INTERNATIONAL STANDARD

ISO 15998

First edition
2008-04-15

Earth-moving machinery — Machine-control systems (MCS) using electronic components — Performance criteria and tests for functional safety

Engins de terrassement — Systèmes de contrôle-commande utilisant des composants électroniques — Critères et essais de performances de sécurité fonctionnelle

Reference number
ISO 15998:2008(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

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.

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 15998 was prepared by Technical Committee ISO/TC 127, *Earth-moving machinery*, Subcommittee SC 3, *Operation and maintenance*.

Introduction

Systems consisting of electrical and/or electronic components have been used for many years to perform safety functions in most application sectors. Computer-based systems, generically referred to as programmable electronic systems (PES), are at present being used in all application sectors to perform non-safety-related and, increasingly, safety-related functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to base these decisions.

This International Standard addresses systems comprising electrical and/or electronic and/or programmable electronic components [electrical/electronic/programmable electronic systems (E/E/PES)] used for functional safety in earth-moving machinery.

In most situations, safety is achieved by a number of protective systems which rely on many technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements within an individual system, such as sensors, controlling devices and actuators, but also all the safety-related systems. Therefore, while this International Standard is concerned with safety-related E/E/PES, it could also provide guidance for safety-related systems based on other technologies.

This International Standard

— has been conceived with a rapidly developing technology in mind, with a framework sufficiently robust and comprehensive to meet the demands of that technology,

— provides a method for the development of safety requirement specifications necessary to define the required functional safety for E/E/PES, and

— presents a methodology for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PES, using a risk-based approach.

Earth-moving machinery — Machine-control systems (MCS) using electronic components — Performance criteria and tests for functional safety

1 Scope

This International Standard specifies performance criteria and tests for functional safety of safety-related machine-control systems (MCS) using electronic components in earth-moving machinery and its equipment, as defined in ISO 6165. The procedures of ECE R79, Annex 6, ISO 13849-1 or IEC 62061 can be used as an alternative, provided verification and testing is carried out by the manufacturer using Clause 7 of this International Standard.

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 6165:2006, *Earth-moving machinery — Basic types — Identification and terms and definitions*

ISO 13766, *Earth-moving machinery — Electromagnetic compatibility*

IEC 60529, *Degrees of protection provided by enclosures (IP Code)*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms, definitions and abbreviations given in IEC 61508-4 and the following apply.

3.1 Terms and definitions

3.1.1
earth-moving machinery
self-propelled or towed machine on wheels, crawlers or legs, having equipment or attachment (working tool), or both, primarily designed to perform excavation, loading, transportation, drilling, spreading, compacting or trenching of earth, rock and other materials

[ISO 6165:2006]

3.1.2
machine-control system
MCS
system consisting of the components needed to fulfil the function of the system, including sensors, signal processing unit, monitor, controls and actuators or several of these

NOTE The extent of the system is not limited to the electronic controls, but is defined by the machine-related function of the complete system. It therefore consists generally of electronic, non-electronic and connection devices. This can include mechanical, hydraulic, optical or pneumatic components/systems.

3.1.3
system unit
part of a machine-control system that contains any given number of components and/or parts integrated in one or more units

EXAMPLE Control unit of the power shift transmission.

NOTE Generally, components and/or parts are installed in a common enclosure, but the system unit can also be built as a mechanical composite with several functional elements.

3.1.4
connection devices
devices used for power supply and for the transmission of signals and data

3.1.5
basic function
⟨machine-control system⟩ controlling task

3.1.6
basic function
⟨system unit⟩ receiving of signals and data, processing and/or actuation

3.1.7
system function
any function that has to be processed by a machine-control system or system unit

NOTE In addition to the basic function, system functions include diagnostics, self-monitoring, signal processing and data transmission to other systems.

3.1.8
safety concept
concept contained in a description of the methods designed into the system to address system performance and safe operation in the event of a failure

3.1.9
safety-related machine-control systems
machine-control systems that control the safety-related functions of the machine

3.1.10
safe state
state automatically or manually applied after a malfunction of the machine-control system, where the controlled equipment, process or system is stopped or switched to a safe mode to prevent unexpected movements or the potentially hazardous build-up of stored energy (e.g. high-voltage electricity, hydraulic pressures or compressed springs)

3.1.11
well-tried component
component for a safety-related application which has been widely used in the past with successful results in similar applications, and which has been made and verified using principles which demonstrate its suitability and reliability for safety-related applications

NOTE 1 In some well-tried components, certain faults can also be excluded because the fault rate is known to be very low.

NOTE 2 The decision to accept a particular component as well-tried depends on the application.

3.1.12
substitute function
function which allows a continuous process in the case of a malfunction or failure of the system

3.1.13
emergency motion function
function to be adopted in the case of a malfunction or failure of the system to allow the operator an emergency motion

EXAMPLE Moving a machine off a public road.

3.1.14
programmable electronic system
PES
system for control, protection or monitoring based on one or more programmable electronic devices, including all elements of the system, such as power supplies, sensors and other input devices, data busses and other communication paths, and actuators and other output devices

3.2 Abbreviated terms

PES	programmable electronic system
MCS	machine-control systems
FMEA	failure modes and effects analysis
FTA	fault tree analysis
ETA	event tree analysis
SIL	safety integrity level (see IEC 61508-4:1998, 3.5.6)
IP Code	international protection code
EMC	electromagnetic compatibility (see ISO 13766:2006, 3.1)
OSI	open systems interconnection
ASIC	application-specific integrated circuit
RF	radio-frequency

4 General safety requirements

4.1 Application

The following performance criteria are valid for all safety-related machine-control systems using electronic components. These performance criteria are applicable to any type of MCS.

4.2 Description of machine-control system

The system description and overview shall contain

— a list of all system units used by the safety-related functions, and

— a schematic layout of the connection devices and system units, representing the safety-related functions of the machine-control system.

An example of the structure and content of the system description is given in Annex B.

The basic functions and their interfaces to other system units shall be specified for each system unit. This may be done in schematic form or through a block diagram.

The connection shall be illustrated in a suitable way; for the electrical system, a circuit diagram is suitable.

The illustration shall unambiguously classify each connection device (e.g. wires) in relation to the system units (e.g. by terminal identification).

The system units shall be marked by an identification code (e.g. numbers, symbols, characters), so that the correlation between the illustration of the system and the MCS installed in the machine can be verified.

By using the identification code, the manufacturer proves that the system units are in agreement with the documentation with regard to the basic function, safety concept and interfaces. The structure of the identification code (e.g. alphanumerical) may be specified by the manufacturer, but shall be unambiguous.

The system description shall also include requirements for the environmental conditions during the intended operation of the machine:

— climatic conditions (temperature, humidity);

— mechanical conditions (vibration, shock);

— corrosion conditions (salt spray, gas pollution);

— electrical conditions (over- and under-voltage);

— electromagnetic conditions;

— power-source-voltage fluctuation.

4.3 Description of basic function

The basic function of the machine-control system shall be specified in a short description, which may be supported by graphical tools, such as functional schematic or block diagrams. The description shall contain

— an enumeration of the input types and values of the MCS,

— an enumeration of the controlled output types and values of the MCS,

— the open-loop- and closed-loop-control objectives and data/sensors used, and

— the permissible operating and adjusting ranges.

4.4 Risk analysis and assessment

A risk analysis and assessment of the MCS shall be carried out using the systems description in accordance with 4.2 to evaluate the hazards. This may be made in accordance with risk assessment methodologies such as ISO 14121-1 or IEC 61508-5:1998, Annex D. An example is given in Annex A of this International Standard.

4.5 Performance criteria for the safety concept

The basic concept and system functions specified by the manufacturer for the safety concept of the machine shall be taken into account during development and production of the machine-control system. The safety concept includes all measures which provide for safe operation beyond the standard operation (for guidance, see IEC 61508-2:2000, 7.2.3.1). These shall be listed in a generally understandable way, such as in the following examples:

— redundancy;

— fault-detection procedures;

— “safe state”, a safe state may initiate, for example, an emergency motion function (see 5.4).

A documented analysis shall be included, indicating the realization of the safety concept as described. This may be done by an analysis (e.g. FMEA, FTA, ETA) or using equivalent methods suitable for the safety concept of the MCS.

The manufacturer shall document the manner in which the validation of the systems logic has been made during the development stage.

The transition from standard operation mode to safe state shall take into account the stability of the machine and the minimization of the risk of injury to people.

The movement (active or passive) of the machine or its working equipment/attachment out of the hazardous area or position in the case of a malfunction of the MCS should be possible.

4.6 Physical environment and operating conditions

4.6.1 General

The environmental conditions in which the machines are used shall be the basis for the specification of the MCS.

4.6.2 Environment temperature and humidity

The machine-control system shall operate safely under the conditions described in 7.2.2.

Restrictions not having any influence on the safe functioning of the MCS are acceptable.

For special operating conditions of the machine and installation conditions of the electronic parts, other environmental conditions may be specified by the manufacturer.

4.6.3 Degree of protection (IP Code)

Based on the installation conditions, the parts of the MCS carrying out the functional safety shall meet at least the following degrees of protection, in accordance with IEC 60529:

— IP 66 [1)] for all electronic parts, which are fitted outside the machine or are exposed directly to environmental influences.

For special operating conditions of the machine and installation conditions of the electronic parts, other environmental conditions may be specified by the manufacturer.

4.6.4 Electromagnetic compatibility (EMC)

The machine-control system shall fulfil the requirements of ISO 13766.

4.6.5 Mechanical vibration and shock

The system units, components and parts of the MCS shall be designed and fitted so that their safe function is maintained for vibration and shock loads during the typical operation of the machine.

See 7.2.3 and 7.2.4 for test conditions.

For special operating conditions of the machine and installation conditions of the electronic parts, other environmental conditions may be specified by the manufacturer.

4.7 Emergency stop function

An emergency stop function shall be provided if the safety concept requires it. The emergency stop shall shift the MCS or the system unit or the machine into a defined safe state, in the case of failure that could lead to a hazardous motion or condition of the machine.

5 Additional requirements for safety-related machine-control systems

5.1 General

This clause applies to machine-control systems with safety-related functions that have a minimum SIL-Level 1 or equivalent (see A.3.2).

Machine-control systems with safety-related functions shall fulfil the following additional requirements in accordance with the risk assessment.

5.2 Fault avoidance and fault control

5.2.1 IEC 61508-2:2000, Annexes A and B, or other comparable methods, shall be used as a guide to measures and the techniques for the avoidance and control of faults.

5.2.2 Failures in a safety-related system vary essentially according to the time of their origin:

a) failures caused by faults originating before or during system installation, for example, software faults include specification and program faults, hardware faults include manufacturing faults and incorrect selection of components;

1) For special installation conditions, other degrees of protection may be selected, e.g. in the case of higher voltage, malfunction by moisture, dirt or foreign-conductor particles which could lead to an unacceptable situation (risk).

b) failures caused by faults or human errors originating during machine life/operation and, in general, after system installation (e.g. random hardware failures, failures caused by incorrect use).

Failures of the type mentioned in a) can be detected, corrected and avoided by measures made during the different phases of the life-cycle (see IEC 61508-2:2000, Annex B). The measures for failure avoidance are primarily design and analytical procedures.

Failures of the type mentioned in b) can only be controlled during normal operation (see IEC 61508-2:2000, Annex A). The measures for the control of those failures shall be integrated in the safety concept.

Some of the measures and techniques given in IEC 61508-2 are of basic importance (see Annexes A and B), thus they should be used independently from the safety integrity level. Others should also be used independently of this level. The effort required to realize these measures should be chosen such that the effectiveness demanded by IEC 61508-2:2000, Tables B.1 to B.5 (low/medium/high), is achieved. All other measures are replaceable in principle. They can be replaced individually or in connection with other measures.

5.3 Requirements for programmable electronic systems (PES)

The software shall be developed and validated according to appropriate measures (see, for example, IEC 61508-3:1998, Annex A or ISO 13849-1:2006).

The concepts and the development methods and tools for programmable electronic systems (PES) used in machine-control systems shall be documented.

5.4 Malfunction or failure of the electronic components used in machine-control systems

The entering of a safe state shall be achieved in the case of a malfunction or failure of the electronic components used on machine-control systems, in accordance with risk assessment. Reduced system performance or (a) substitute function(s) may be used to achieve a safe state as a part of the safety concept.

The safe state may be achieved by an automatic shift into a substituting function (see Figure 1). If this transition is automatically applied by the MCS, then there shall be some form of indication to the operator, such as alarms, indicators or derated performance (e.g. slow motion).