DRAFT INTERNATIONAL STANDARD

ISO/DIS 19014-1

ISO/TC **127**/SC **2**

Secretariat: **ANSI**

Voting begins on:
2016-08-26

Voting terminates on:
2016-11-17

Earth-moving machinery — Safety —

Part 1:
Methodology to determine safety-related parts of the control system and performance requirements

Engins de terrassement — Sécurité —

Partie 1: Méthodologie·permettant de déterminer les parties du système de commande et les exigences de performance liés à la sécurité

ICS: 53.100

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 19014-1:2016(E)

COPYRIGHT PROTECTED DOCUMENT

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. 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. 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 the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 127.

ISO 19014 consists of the following parts, under the general title *Earth-moving machinery — Safety*:

— *Part 1: Methodology to determine safety-related parts of the control system and performance requirements*

— *Part 2: Design and evaluation of safety-related electrical and electronic machine control systems*

— *Part 3: Environmental performance and test requirements of electronic and electrical components used in safety-related parts of the control system*

— *Part 4: Design and evaluation of software and data transmission for safety related parts of the control system*

ISO 19014- series replaces ISO 15998.

Introduction

This International Standard addresses systems comprising of all energy types used for functional safety in earth-moving machinery.

The structure of safety standards in the field of machinery is as follows.

Type-A standards (basis standards) give basic concepts, principles for design and general aspects that can be applied to machinery.

Type-B standards (generic safety standards) deal with one or more safety aspects, or one or more types of safeguards that can be used across a wide range of machinery:

— type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);

— type-B2 standards on safeguards (e.g. two-hands controls, interlocking devices, pressure sensitive devices, guards).

Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This part of ISO 19014 is a type B-1 standard as stated in ISO 12100.

Earth-moving machinery — Safety —

Part 1:
Methodology to determine safety-related parts of the control system and performance requirements

1 Scope

This part of ISO 19014 provides guidance and a methodology for determination of performance levels required for earth moving machinery (EMM), as described in ISO 6165 after a hazard is identified by risk assessment and a control is determine as a safety related part of the control system (SRP/CS).

Hazard identification is determined by risk assessment using the method described in ISO 12100 or by other means and is not covered by this document.

Where a control is determined as safety related a Machine Performance Level (MPL) is determined by the method described.

NOTE 1 The term MPL is used to describe the level of performance required from a safety related part of a control system. The 'M' refers to machine and is applicable to all Earth Moving Machinery covered by the scope of this document.

For those controls determined as safety related, the characteristics for architecture, hardware, software environmental requirements and performance are covered by other parts in this series.

A safety related control system that addresses hazards as identified by a machine or system risk assessment includes but is not limited to systems that control machine movement. (for example powered motion, braking, steering, attachments and working tool control systems).

Control systems that protect against rapid thermal events, electrical shock, requirements for explosive atmospheres etc are also included.

The principles of this standard can also be applied to immediate action warning indicator intended to warn the operator of a possible hazard and requiring immediate action from the operator to correct and prevent such a hazard.

Other safety related devices that the operator would be aware of failure are excluded from this standard (e.g. windscreen wipers, head lights etc.).

NOTE 2 Audible warnings are excluded from the requirements of diagnostic coverage.

This standard supersedes ISO 15998:2008.

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 3411, *Earth-moving machinery — Physical dimensions of operators and minimum operator space envelope*

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

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

ISO 14121-1:2007, *Safety of machinery — Principles of risk assessment*

ISO 19014-2, *Earth-moving machinery — Safety — Control system performance level architecture and requirements*

ISO 19014-3, *Earth-moving machinery — Safety — Control system performance level environmental requirements*

ISO 19014-4, *Earth-moving machinery — Safety — Design and evaluation of software and data transmission for safety related parts of the control system*

ISO 20474-1, *Earth Moving Machinery — Safety — General Requirements*

3 Terms and definitions

For the purposes of this document, the following terms and definitions in ISO 6165, ISO 13849-1, ISO 12100 and ISO 20474-1 apply, in addition to the definitions listed below.

3.1
Machine Performance Level (MPL)
discrete level to specify the ability of safety-related parts of control systems to perform a safety function under reasonably foreseeable conditions

3.2
functional safety
part of the overall safety that depends on a system or equipment operating correctly in response to its inputs

3.3.1
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 1 to entry: 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.

3.3.2
safety related part of the control system (SRP/CS)
part of a control system that responds to safety-related input signals and generates safety-related output signals

Note 1 to entry: The combined safety-related parts of a control system start at the point where the safety-related input signals are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contractor).

Note 2 to entry: If monitoring systems are used for diagnostics, they are also considered as SRP/CS.

3.4
operator
person operating an EMM with high level of skills, training and awareness

3.5
co-worker
person working in the vicinity of a machine assumed to have a medium level of training (site induction) and awareness

3.6
bystander
person including non-employee, child or member of the public with little or no awareness of machine hazards and no training

3.7
maintainer
person whose function is to perform maintenance tasks on the machine being analysed. These personnel are normally trained, and are familiar with the machine

3.8
controllability
involved individual's possibility of avoiding harm in the situation that is putting him/her at risk

3.9
exposure
duration of time and frequency in which an individual is in a situation in which the potential hazard exists

3.10
severity
degree of harm to an endangered individual

3.11
warning indicator
visual or audible indications were an action from the operator or control system is required

Note 1 to entry: Note to entry: The action required can be immediate for urgent warnings such as tip over indicators or advisory such as low oil – action required is generally determined by colour of indicator or urgency of alarm.

3.11.1
immediate action warning indicator
warning Indicator requiring immediate action from the operator to mitigate hazard or system failure

Note 1 to entry: Note to entry: Annex C provides a list of warning indicators and guidance on those considered requiring immediate action.

3.12
operation indicator
visual indicator used to show mode of operation

3.13
application profile
breakdown of time a machine is used for a given application in a work cycle (expressed in %)

EXAMPLE Machine application profile = 100 %:

20 % road use,

40 % bucket/jobsite application,

30 % back hoe use,

10 % idle.

4 Method to determine MPLr for SRP/CS of EMM

4.1 General

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 therefore considers not only all the elements within an individual system, such as sensors, controlling devices and actuators, but also all the safety-related parts of the control systems.

ISO 19014- series sets out an approach to the design and assessment, for all safety life cycle activities, of safety-relevant control systems of all energy types on earth moving machines as defined in ISO 6165.

It covers the possible hazards caused by the functional behaviour of safety-related systems, as distinct from hazards arising from the equipment itself (electric shock, fire, nominal performance level of components dedicated to active and passive safety, etc.).

Parts of the control systems of the machines concerned which provide safety functions are called safety-related parts of control systems (SRP/CS). These can consist of hardware or software, can be separate or integrated parts of a control system, and can either perform solely critical functions or form part of an operational function.

In general, the designer (and to some extent, the user) may combine the design and validation of these SRP/CS as part of the risk assessment. The objective is to reduce the risk associated with a given hazard (or hazardous situation) under all conditions of use of the machine. This can be achieved by applying various protective measures (both SRP/CS and non-SRP/CS) with the end result of achieving a safe condition.

In order to guide the designer during design, and to facilitate the assessment of the achieved performance level, ISO 19014 defines an approach based on a classification of structures with different design features and specific behaviour in case of a fault.

The performance levels and categories can be applied to the control systems of all kinds of mobile machines: from simple systems (e.g. auxiliary valves) to complex systems (e.g. steer by wire), as well as to the control systems of protective equipment (e.g. interlocking devices, pressure sensitive devices).

ISO 19014 adopts a customer risk-based approach for the determination of the risks, while providing a means of specifying the target performance level for the safety-related functions to be implemented by safety-related channels. It gives requirements for the whole safety life cycle of SRP/CS (design, validation, production, operation, maintenance, decommissioning), necessary for achieving the required functional safety for SRP/CS that are linked to the performance levels.

4.2 Method

The following key stages apply to determining MPLr for Safety Related Part of the Control System SRP/CS:

a) Determine the intended EMM limits as per EN ISO 12100:2010. (Clause 5)

b) Complete a risk assessment using a suitable tool and identifying the hazards associated with the function or application of the machine.

c) Determine how the hazards identified in the risk assessment process are mitigated or protected against. (This may require additional control systems or means of ensuring the integrity of inherent control systems.)

d) Determine if the hazard mitigation/protective measure used is dependent upon a control system and if this is a SRP/CS. (This shall include control systems added to the machine to mitigate a hazard, control systems that control the movement of the machine or control systems used if failure creates a hazardous situation.)

e) If a control system is not determined as a SRP/CS the process stops and MPL determination is not required. The control systems which are not subject to the requirements of ISO 19014-1 MPL are covered by the requirements for quality management systems (QM) (clause 6.1.7) and the integrity is to be ensured by following quality management tools, relevant technical requirements and standards as applicable.

f) If the protective measure is dependent upon a SRP/CS, use the performance level determination calculation to decide the MPL(s) required for the SRP/CS to perform the safety function. (Clause 6)

g) For a system to achieve a determined MPL refer to other parts in this series.

