SLOVENSKI STANDARD
oSIST prEN ISO 19014-1:2017

01-julij-2017

Stroji za zemeljska dela - Varnost - 1. del: Metodologija ugotavljanja delov krmilnega sistema, ki so povezani z varnostjo in zahtevanimi lastnostmi (ISO/DIS 19014-1:2017)

Earth-moving machinery - Safety - Part 1: Methodology to determine safety-related parts of the control system and performance requirements (ISO/DIS 19014-1:2017)

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 (ISO/DIS 19014-1:2017)

Ta slovenski standard je istoveten z: **prEN ISO 19014-1**

ICS:

53.100	Stroji za zemeljska dela	Earth-moving machinery

oSIST prEN ISO 19014-1:2017 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 19014-1.2

ISO/TC **127**/SC **2** Secretariat: **ANSI**

Voting begins on: **2017-05-17**

Voting terminates on: **2017-07-11**

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

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 19014-1.2:2017(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. 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 — Functional Safety:

— Part 1: Risk assessment methodology to determine control system performance requirements

— Part 2: Design and Evaluation of Safety-Related Machine Control Systems

— Part 3: Environmental Testing Requirements

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

— Part 5: Technical report: Guidance and table of MPLr for EMM

ISO 19014- series replaces ISO 15998

Introduction

This document addresses systems 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 C 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.

NOTE This series can also be used to assess the functional safety requirements of other off-road mobile machinery

Hazard identification is determined by risk assessment (herein also known as machine control system safety analysis MCSSA) using the method described in ISO 12100 or by other means and is not covered by this document.

If a sub-system is determined to be a safety control system (SCS), a Machine Performance Level (MPL) is allocated to that sub-system.

NOTE The term MPL is used to describe the performance level required from a safety-related part of a control system. The 'M' refers to machine and denotes Earth Moving Machinery covered by the scope of this document and is used to differentiate from other functional safety standards (e.g PL, AgPL, ASIL, etc) .

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.

ISO 19014 covers the hazards caused by the functional behaviour of safety-related systems and excludes hazards arising from the equipment itself (for example, electric shock, fire, etc.)

The principles of this standard shall 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. . (e.g. vision systems, proximity detection systems etc)

NOTE A normative list of immediate action warning indicators is included in Annex B

Other controls that are not safety control systems (SCS), that do not mitigate a hazard or perform a control function and where the operator would be aware of a failure, are excluded from this standard (e.g. windscreen wipers, head lights, cab light etc.)

NOTE 1 An informative list of safety functions is included in Annex E.

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

This standard supersedes ISO 15998:2008.

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 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 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 terms and definitions given in ISO 12100 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp"

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

3.1.1
Machine Performance Level required
MPL_r
discrete level required as determined by processes in this document

3.1.2
Machine Performance Level achieved
MPL_a
discrete level achieved as determined by processes in ISO 19014-2 and ISO 19014-4

3.2
functional safety
part of the overall safety relating to the equipment under control and its control system that depends on the correct functioning of the safety-related systems and other risk reduction measures

[SOURCE: 3.1.12 of IEC 61508-4:2010]

3.3
Machine control system
MCS
system which responds to input signals from parts of machine elements, operators, external control equipment or any combination of these and generates output signals causing the machine to behave in the intended manner

[SOURCE: ISO 13849-1:2015, 3.1.32]

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.

3.3.1
safety control system
SCS
a sub-system or component used by a MCS to achieve functional safety by affecting machine behaviour or mitigating a hazard

Note 1 to entry: A system which can fail in a way that creates a hazard is considered a SCS.

Note 2 to entry: for example, SCS for propulsion may include throttle, gear shift, start/stop etc

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

[SOURCE: ISO 13849-1:2015, 3.1.1]

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

Note 3 to entry: SRP/CS is a part or component within the specific MCS

3.4
operator
Person operating the EMM

3.5
co-worker
Person working in the vicinity of a machine

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

Note 1 to entry: A maintainer is trained and familiar with the machine

3.8
controllability
ability to avoid harm to the person group at risk through the timely reactions of the operator, possibly with the support of alternative controls

3.9
exposure
percentage of time a person group is exposed to the hazard

3.10
severity
estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation

[SOURCE: ISO 26262-1:2011, 3.120]

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

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

3.12
indicator
means by which the state of the equipment or machinery is represented to an observer

[SOURCE: ISO 22555:2007, 3.2]

3.13
application
different industries that a machine is used in, that may have different hazard from one another

Note 1 to entry: Applications can include, general construction, road construction, waste management, quarry etc

3.14
use case
uses of a machine within an application

Note 1 to entry: An example of this is that a dozer can have dozing, ripping, travel and maintenance use cases within an application.

3.15
application use case
highest percentage of time a machine is used in a use case within a given application during the intended use of the life cycle of the machine

Note 1 to entry: because the application use case represents the highest percentage of time a machine spends in a use case, the sum of application use cases across an application can be greater than 100%.

3.16
hazard time
percentage of time within the work cycle where it is reasonably foreseeable that a hazard may exist should the control system being assessed fail

Note 1 to entry: For example, a dozer pushing material off a high wall is only exposed to the hazard of going over the high wall for the time where the machine is traveling towards the high wall within the stopping distance of the machine.

3.16.1
hazard zone
any space within or around machinery in which a person can be exposed to a hazard from the SCS under analysis

[SOURCE: ISO 12100:2010, 3.11(MOD)]

3.17
machine control system safety analysis
MCSSA
risk assessment used to determine the required MPL_r for the SCS on a machine as outlined in this document

3.18
person group
groups of people analyzed in the MCSSA

Note 1 to entry: The four person groups are operators, maintainers, bystanders and co-workers