SLOVENSKI STANDARD
oSIST prEN ISO 19014-2:2019

01-november-2019

Stroji za zemeljska dela - Funkcijska varnost - 2. del: Oblikovanje in vrednotenje strojnih in arhitekturnih zahtev za varnostne dele krmilnega sistema (ISO/DIS 19014-2:2019)

Earth-moving machinery - Functional safety - Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system (ISO/DIS 19014-2:2019)

Erdbaumaschinen - Funktionale Sicherheit - Teil 2: Entwurf und Bewertung von Hardware- und Architekturanforderungen für sicherheitsrelevante Teile des Steuerungssystems (ISO/DIS 19014-2:2019)

Engins de terrassement - Sécurité fonctionnelle - Partie 2: Conception et évaluation des exigences de matériel et d'architecture pour les parties relatives à la sécurité du système de commandeé (ISO/DIS 19014-2:2019)

Ta slovenski standard je istoveten z: **prEN ISO 19014-2**

ICS:

53.100	Stroji za zemeljska dela	Earth-moving machinery

oSIST prEN ISO 19014-2:2019 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 19014-2

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

Voting begins on: **2019-09-19**

Voting terminates on: **2019-12-12**

Earth-moving machinery — Functional safety —

Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system

ICS: 53.100

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 19014-2:2019(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: 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.

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.

The ISO 19014 series replaces ISO 15998.

Introduction

This document addresses systems comprising 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.

ISO 19014-2 is the adaptation of ISO 13849 to provide a Type –C standard to address the specific application of functional safety to Earth Moving Machinery.

ISO 19014-2 complements the safety life cycle activities of safety control systems per ISO 13849-1:2015 and ISO 13849-2:2012 on earth moving machinery as defined in ISO 6165.

Earth-moving machinery — Functional safety —

Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system

1 Scope

This part of ISO 19014 specifies general principles for the development and evaluation of the achieved machine performance level (MPL_a) of safety-control systems (SCS) using components powered by all energy sources used in earth-moving machinery and its equipment, as defined in ISO 6165. This document is used in conjunction with the other parts in the series.

ISO 19014 is to be used in conjunction with ISO 13849 when applied to Earth Moving Machinery (EMM) and supersedes ISO 15998. Where specific requirements are given in ISO 19014, they take precedence over the requirements in ISO 13849.

The principles of this standard apply to control systems that control machine motion or mitigate a hazard. Such systems are assessed for performance level requirements per ISO 19014-1 or ISO/TS 19014-5.

Excluded from the scope of ISO 19014 are the following systems:

— Awareness systems that do not impact machine motion (e.g., cameras and radar detectors)

— Fire suppression systems, unless the activation of the system interferes with, or activates, another SCS.

Other systems or components whereby the operator would be aware of failure (e.g., windscreen wipers, head lights, etc.), or are primarily used to protect property, are excluded from this document. Audible warnings are excluded from the requirements of diagnostic coverage. Refer to Clause 7.4.3.

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

ISO 13849-1:2015, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation*

ISO 19014-1, *Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related parts of the control system and performance requirements*

ISO 19014-3, *Earth-moving machinery — Functional safety — Part 3: Environmental performance and test requirements of electronic and electrical components used in safety-related parts of the control system*

ISO 19014-4, *Earth-moving machinery – Functional safety – Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system*

ISO/TS 19014-5, *Earth-moving machinery – Functional safety – Part 5: Table of Machine Performance Levels*

IEC 61508, *2, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

3 Terms and Definitions

For the purposes of this document, the terms and definitions given in ISO 19014-1, ISO 12100, ISO 13849-1:2015 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

electronic safety control system

ESCS

machine control system made of electronic components from input device to output device

function

defined behavior of one or more control units

Note 1 to entry A control unit (electronic control units) can execute more than one function. When multiple safety functions are contained in a control unit, each safety function and the associated circuit is analyzed separately.

N/ESCS

Non-electronic safety control system

machine control system made of non-electronic components from input device to output device

safe state

condition in which after a fault of the safety control system, the controlled equipment process or system is automatically or manually stopped or switched into a mode that prevents unintended behavior or the potentially hazardous release of stored energy.

Note 1 to entry A safe state can also include maintaining the function of the safety control system (e.g. steering) in the presence of a single fault depending on the hazard being mitigated .

[SOURCE: ISO 3450:2011 3.15 mod.] modified – note 1 to entry has been added.

well-tried components

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

4 Symbols and Abbreviated Terms

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

a, b, c, d, e	Graduation of machine performance levels
ASIC	Application Specific Integrated Circuit
B, 1, 2, 3, 4	Denotation of categories
CCF	Common Cause Failure
DC	Diagnostic Coverage
DCavg	Average Diagnostic Coverage
ECM	Electronic Control Module
EMM	Earth Moving Machine
ESCS	Electronic Safety Control System
FMEA	Failure Modes and Effects Analysis
FMEDA	Failure Modes, Effects and Diagnostics Analysis
FPGA	Field Programmable Gate Array
HFT	Hardware Fault Tolerance
ILO	Input Logic Output
MCS	Machine Control System
MPL	Machine Performance Level
MPLa	Achieved Machine Performance Level
MPLr	Required Machine Performance Level
MTTF	Mean Time To Failure
MTTFd	Mean Time to Dangerous Failure
N/ESCS	Non-Electronic Safety Control System
OTE	Output of Test Equipment
QM	Quality Management
RC	Reliability Coverage
SCS	Safety Control System
SRP/CS	Safety-Related Parts of Control System
TE	Test Equipment

5 General Requirements

ISO 19014 series shall be used in conjunction with ISO 13849 when applied to Earth Moving Machinery (EMM) and supersedes ISO 15998. Where specific requirements are given in ISO 19014, they take precedence over the requirements in ISO 13849.

The principles of this standard shall be applied to control systems that control machine motion or mitigate a hazard. Such systems shall be assessed for performance level requirements per ISO 19014-1 series or ISO/TS 19014-5. Other machine control systems that interfere with or mute a safety function of the safety control system shall be assigned the same performance level as the system it is interfering with or muting.

5.1 Existing SCS

Where an existing SCS has been developed to a previous standard and demonstrated through application usage and validation to reduce the likelihood of a hazard to as low as reasonably practicable, there shall be no requirement to update the lifecycle documentation. When the previously utilized SCS is modified, an impact assessment of the modifications shall be performed and an action plan developed and implemented to ensure that the safety requirements are met.

6 System Design

6.1 General

A safety function which relies on a control system to provide necessary hazard mitigation for the machine can be implemented by an SCS within the scope of ISO 19014-2. An SCS can contain one or more SRP/CS, and several SCS can share one or more SRP/CS (e.g. a logic unit, power control elements) as illustrated in Figure 1. It is also possible that one SRP/CS implements both safety functions and standard control functions.

NOTE For immediate action warning indicators refer to ISO 19014-1, Annex B.

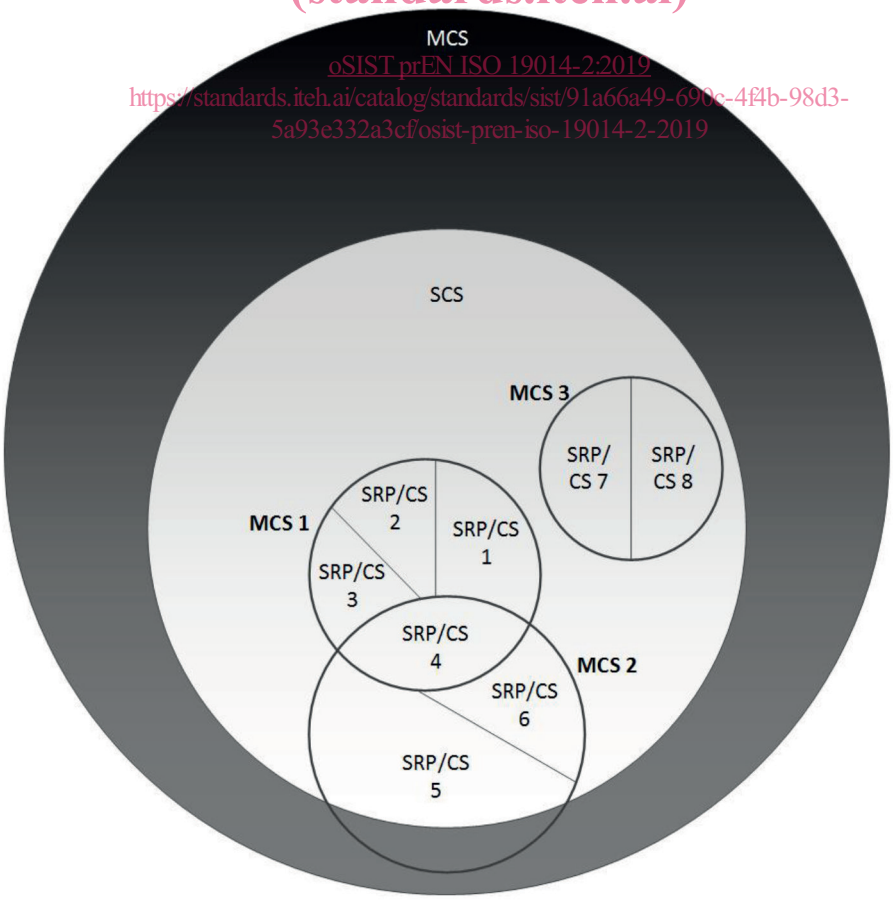

Figure 1 — Composition of safety-related MCS

Having identified the safety functions of the control system, the designer shall determine and document the requirements of each SCS which performs a safety function. During the safety lifecycle, safety requirements are detailed and specified in greater detail at hierarchical levels. All safety requirements shall be written such that they are unambiguous, consistent with other requirements, and feasible to implement.

6.1.1 Interaction between different SRP/CS

When machine functions are designed to be used in a synchronized manner (e.g., task automation), the control system shall be designed to mitigate hazards due to lack of synchronization.

Note An EMM example of this synchronization is an excavator boom, arm, and bucket being controlled simultaneously by a grade control system.

6.1.2 Differences between safety functions of mobile and stationary machines

Many safety functions on mobile machines do not have run / stop outputs like stationary machine safety functions normally do, and are not always added to a machine purely to mitigate a hazard. Steering, service brakes, swing and equipment controls may have modulated or variable outputs within a certain range. While these types of systems can fit into the ISO 13849 architectures, designers need to consider how the safety concepts and safety functions may differ on a mobile machine (e.g. does the system need closed loop control rather than open loop to address incorrect application rates, does the system need to address hazards associated with uncommanded activation as well as failure on demand etc.).

Some systems on mobile machines need to maintain an operable state during a failure. While ISO 13849-1:2015 allows for this, additional measures will need to be taken to ensure this can happen safely and that parallel channels do not conflict with each other and that the systems function as the requirements for the claimed architecture specifies

The following design considerations shall be taken into account:

— Conflicting input or output signals

— Loss of signal and actuation energies to either system (e.g. separate oil supplies for each channel, redundant power supplies for ECMs)

— Conflicting safe states required by multiple failure types that are being addressed by the system

— Systems that require a fail operable safety concept

6.1.3 Assessment process

Assessment processes should be independent from the design process.

6.2 Hardware design

The hardware structure of the SCS can provide measures for avoiding, detecting or tolerating faults. Practical measures can include redundancy, diversity, and monitoring.

The hardware development process shall begin at the system level where safety functions and associated requirements are identified (see Figure 2). The system can be decomposed into subsystems for easier development.

Where applicable, each phase of the development cycle shall be verified.

See Figure 2 for a depiction of the hardware development process in the form of a V-model.

The design procedure for the hardware system architecture is as follows:

a) identify the component operating environment and stress level