INTERNATIONAL STANDARD

ISO 19014-2

First edition
2022-06

Earth-moving machinery — Functional safety —

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

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 commande

Reference number
ISO 19014-2:2022(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 (see 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 (see 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 of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 127, *Earth-moving machinery*, Subcommittee SC 2, *Safety, ergonomics and general requirements,* in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/TC 151, *Construction equipment and building material machines - Safety*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition, together with ISO 19014-1, ISO 19014-3, ISO 19014-4 and ISO 19014-5 cancels and replaces the first editions (ISO 15998:2008 and ISO/TS 15998-2:2012), which have been technically revised.

The main changes are as follows:

— elimination of alternative procedures ECE R79, Annex 6, and IEC 62061;

— application of ISO 13849-1 to mobile Earth-moving machinery, including analysis of non-electronic control systems used in Earth-moving machine applications.

A list of all parts in the ISO 19014 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document addresses systems comprising all technologies 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 document is a type-C standard as stated in ISO 12100.

This document is of relevance, in particular, for the following stakeholder groups representing the market players with regard to machinery safety:

— machine manufacturers (small, medium and large enterprises);

— health and safety bodies (regulators, accident prevention organisations, market surveillance etc.)

Others can be affected by the level of machinery safety achieved with the means of the document by the above-mentioned stakeholder groups:

— machine users/employers (small, medium and large enterprises);

— machine users/employees (e.g. trade unions, organizations for people with special needs);

— service providers, e. g. for maintenance (small, medium and large enterprises);

— consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate at the drafting process of this document.

The machinery concerned and the extent to which hazards, hazardous situations or hazardous events are covered are indicated in the Scope of this document.

When requirements of this type-C standard are different from those which are stated in type-A or type-B standards, the requirements of this type-C standard take precedence over the requirements of the other standards for machines that have been designed and built according to the requirements of this type-C standard.

This document is the adaptation of ISO 13849 to provide a type-C standard to address the specific application of functional safety to earth-moving machinery.

This document is to be used in conjunction with the ISO 13849 series when applied to earth-moving machinery (EMM) and supersedes ISO 15998.

This document 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 document specifies general principles for the development and evaluation of the machine performance level achieved (MPL_a) of safety-control systems (SCS) using components powered by all energy sources (e.g. electronic, electrical, hydraulic, mechanical) used in earth-moving machinery and its equipment, as defined in ISO 6165.

The principles of this document apply to machine control systems (MCS) that control machine motion or mitigate a hazard; such systems are assessed for machine performance level required (MPL_r) per ISO 19014-1 or ISO/TS 19014-5.

Excluded from the scope of this document 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.

In addition, this document addresses the significant hazards as defined in ISO 12100 mitigated by the hardware components within the SCS.

This document is not applicable to EMM manufactured before the date of its publication.

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 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 19014-4:2020, *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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 12100, ISO 13849-1, ISO 19014-1 and the following apply.

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

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

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

3.1
ESCS
electronic safety control system
safety control system made of electronic components from input device to output device

3.2
function
defined behaviour of one or more MCS

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

3.3
N/ESCS
non-electronic safety control system
safety control system made of non-electronic components from input device to output device

3.4
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 behaviour or the potentially hazardous release of stored energy

Note 1 to entry: A safe state can also include maintaining the *function* (3.2) 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, modified – "malfunction" has been replaced by "fault"; "performance" has been replaced by "behaviour"; Note 1 to entry has been added.]

3.5
well-tried component
component for a safety-related application that has been widely used in the past with successful results in the same or similar 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