International Standard

ISO 19014-2

Second edition
2026-10

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 du système de commande relatives à la sécurité

Reference number
ISO 19014-2:2026(en)

© ISO 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **2**
4 Symbols and abbreviated terms ... **3**
5 General requirements ... **4**
5.1 Application ... 4
5.2 Existing safety control system (SCS) ... 4
5.3 Safety requirements and/or protective/risk reduction measures ... 4
6 System design ... **4**
6.1 Overview ... 4
6.2 General requirements ... 5
6.3 Hardware design ... 5
7 System safety performance evaluation ... **6**
7.1 Machine performance level achieved (MPL_a) ... 6
7.2 Hardware safety evaluation ... 7
7.2.1 General ... 7
7.2.2 Fault consideration ... 7
7.2.3 Fault exclusion ... 7
7.2.4 Mean time to dangerous failure ($MTTF_d$) ... 7
7.3 Diagnostic coverage (DC) ... 8
7.3.1 Diagnostic coverage(DC) of electronic safety control systems (ESCS) ... 8
7.3.2 Diagnostic coverage (DC) of non-electronic safety control systems (N/ESCS) ... 8
7.4 Requirements for MPL_a = d for hydraulic steering and braking systems ... 8
7.4.1 General ... 8
7.5 Category classifications ... 9
7.5.1 General ... 9
7.5.2 Category B/Category 1 ... 12
7.5.3 Category 2 ... 13
7.5.4 Conflicting safety functions ... 14
7.5.5 Considerations for the SRP/CS of fail-operational systems ... 14
7.6 Combination of SCS to achieve an overall MPL_a ... 14
8 Information for use and maintenance ... **16**
8.1 General ... 16
8.2 Operator's manual ... 16
Annex A (informative) **Example systems and evaluations** ... **17**
Annex B (normative) **Compatibility with other functional safety standards** ... **31**
Annex C (informative) **Safety function evaluation** ... **32**
Annex D (normative) **Exceptions, exclusions, additions to ISO 13849-1:2023 and ISO 13849-2:2012** ... **34**
Bibliography ... **37**

© ISO 2026 – All rights reserved

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 document 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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 second edition cancels and replaces the first edition (ISO 19014-2:2022), which has been technically revised.

The main changes are as follows:

— correction of machine performance level (MPL) error in Annex C;

— correction of typographical errors in Figure C.1;

— removal of Category 2M;

— removal of hydraulic system robustness (HSR);

— removal of Annex B;

— addition of requirements for MPL_a=d within Category 1.

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.

© ISO 2026 – All rights reserved

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 (basic 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 12100:2010.

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

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

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

Others can be affected by the level of machinery safety achieved in accordance with this document:

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

— machine users and 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 in 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 the requirements of this type-C standard differ from those 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.

© ISO 2026 – All rights reserved

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. electrical, hydraulic, mechanical) used in earth-moving machinery and its equipment, as defined in ISO 6165:2022.

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 19014-1:2026[1)] or ISO 19014-5:2026.[2)]

NOTE 1 Requirements for the application of functional safety throughout the software development lifecycle are addressed in ISO 19014-4:2026.[3)]

To cover all the relevant safety requirements for the products in its scope, this document is used in combination with ISO 19014-1:2026, ISO 19014-3:2026, ISO 19014-4:2026, and ISO 19014-5:2026.

This document does not apply to 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.

This document does not apply to other systems or components where the operator would be aware of failure (e.g. windscreen wipers, head lights), or are primarily used to protect property.

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

This document addresses the significant hazards, as defined in ISO 12100:2010, mitigated by the hardware components within the SCS.

This document is not applicable to earth-moving machinery 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 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 13849-1:2023, *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 19014-1:2026, *Earth-moving machinery — Functional safety — Part 1: Methodology to determine safety-related pars of the control system and performance requirements*

© ISO 2026 – All rights reserved

ISO 19014-3: 2026, *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: 2026, *Earth-moving machinery — Functional safety — Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system*

ISO 19014-5: 2026, *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 12100:2010, ISO 13849-1:2023, and ISO 19014-1:2026 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
electronic safety control system
ESCS
safety control system made of electronic components from input device to output device

3.2
function
defined response of one or more machine control systems (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
non-electronic safety control system
N/ESCS
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 functionality 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 "functionality"; 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 or which has been made and verified using principles which demonstrate its suitability and reliability for safety-related applications

3.6
hardware fault tolerance
HFT
property of a subsystem to potentially lose the safety function upon at least N+1 faults

Note 1 to entry: A hardware fault tolerance (HFT) of N means that N+1 faults of a subsystem can cause a loss of the safety function.

© ISO 2026 – All rights reserved

[SOURCE: IEC 62061:2021, 3.2.35, modified – changed “could” to “can” and added “HFT” in Note 1 to entry.]

3.7
fail-operational system
system capable of operating after a failure

3.8
impact analysis
documentation that records the understanding and implications of a proposed change

3.9
conflicting safety function
safety function where one failure type drives a safe state that conflicts with the safe state of another failure type from the same safety function

EXAMPLE The safe state for a failure to brake is to stop the machine, but the safe state of an uncommanded brake application is to release the brake.

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
DC_{avg}	average diagnostic coverage
ECU	electronic control unit
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
I-L-O	Input-logic-output
MCS	machine control system
MPL	machine performance level
MPL_a	machine performance level achieved
MPL_r	machine performance level required
MTTF	mean time to failure
$MTTF_d$	mean time to dangerous failure
N/ESCS	non-electronic safety control system

© ISO 2026 – All rights reserved