
Stroji za zemeljska dela - Funkcijska varnost - 4. del: Načrtovanje in vrednotenje programske opreme in prenosa podatkov za dele krmilnega sistema, povezane z varnostjo (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 19014-4:2020)

Erdbaumaschinen - Sicherheit - Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante Steuerungssysteme (ISO 19014-4:2020)

Engins de terrassement - Sécurité - Partie 4: Conception et évaluation du logiciel et de la transmission des données pour les parties relatives à la sécurité du système de commande (ISO 19014-4:2020)

Ta slovenski standard je istoveten z: EN ISO 19014-4:2020

ICS:

35.080	Programska oprema	Software
53.100	Stroji za zemeljska dela	Earth-moving machinery

SIST EN ISO 19014-4:2020

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO 19014-4:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/4c829175-4a82-4262-ae47-755789dd8f3d/sist-en-iso-19014-4-2020>

EUROPEAN STANDARD

EN ISO 19014-4

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2020

ICS 53.100

English Version

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-
4:2020)

Engins de terrassement - Sécurité fonctionnelle - Partie
4: Conception et évaluation du logiciel et de la
transmission des données pour les parties relatives à la
sécurité du système de commande (ISO 19014-4:2020)

Erdbaumaschinen - Funktionale Sicherheit - Teil 4:
Gestaltung und Beurteilung von Software und
Datenübertragung für sicherheitsrelevante
Steuerungssysteme (ISO 19014-4:2020)

This European Standard was approved by CEN on 29 June 2020.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Contents	Page
European foreword.....	3

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO 19014-4:2020](https://standards.iteh.ai/catalog/standards/sist/4c829175-4a82-4262-ae47-755789dd8f3d/sist-en-iso-19014-4-2020)
<https://standards.iteh.ai/catalog/standards/sist/4c829175-4a82-4262-ae47-755789dd8f3d/sist-en-iso-19014-4-2020>

European foreword

This document (EN ISO 19014-4:2020) has been prepared by Technical Committee ISO/TC 127 "Earth-moving machinery" in collaboration with Technical Committee CEN/TC 151 "Construction equipment and building material machines - Safety" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2021, and conflicting national standards shall be withdrawn at the latest by February 2021.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

iTeh STANDARD PREVIEW

The text of ISO 19014-4:2020 has been approved by CEN as EN ISO 19014-4:2020 without any modification.

[SIST EN ISO 19014-4:2020](https://standards.iteh.ai/catalog/standards/sist/4c829175-4a82-4262-ae47-755789dd8f3d/sist-en-iso-19014-4-2020)

<https://standards.iteh.ai/catalog/standards/sist/4c829175-4a82-4262-ae47-755789dd8f3d/sist-en-iso-19014-4-2020>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO 19014-4:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/4c829175-4a82-4262-ae47-755789dd8f3d/sist-en-iso-19014-4-2020>

INTERNATIONAL
STANDARD

ISO
19014-4

First edition
2020-07

**Earth-moving machinery —
Functional safety —**

Part 4:

**Design and evaluation of software and
data transmission for safety-related
parts of the control system**

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Engins de terrassement — Sécurité fonctionnelle —

*Partie 4: Conception et évaluation du logiciel et de la transmission
des données pour les parties relatives à la sécurité du système de
commande*

<https://standards.iteh.ai/catalog/standards/sist/4c829175-4a82-4262-ac47-755789dd8f3d/sist-en-iso-19014-4-2020>



Reference number
ISO 19014-4:2020(E)

© ISO 2020

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO 19014-4:2020

<https://standards.iteh.ai/catalog/standards/sist/4c829175-4a82-4262-ae47-755789dd8f3d/sist-en-iso-19014-4-2020>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

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	1
4 Software development	4
4.1 General.....	4
4.2 Planning.....	5
4.3 Artifacts.....	6
4.4 Software safety requirements specification.....	7
4.5 Software architecture design.....	8
4.6 Software module design and coding.....	8
4.7 Language and tool selection.....	9
4.8 Software module testing.....	10
4.9 Software module integration and testing.....	11
4.10 Software validation.....	12
5 Software-based parameterization	12
5.1 General.....	12
5.2 Data integrity.....	13
5.3 Software-based parameterization verification.....	13
6 Transmission protection of safety-related messages on bus systems	13
7 Independence by software partitioning	14
7.1 General.....	14
7.2 Several partitions within a single microcontroller.....	15
7.3 Several partitions within the scope of an ECU network.....	16
8 Information for use	17
8.1 General.....	17
8.2 Instruction handbook.....	17
Annex A (informative) Description of software methods/measures	18
Annex B (normative) Software validation test environments	31
Annex C (informative) Data integrity assurance calculation	34
Annex D (informative) Methods and measures for transmission protection	36
Annex E (informative) Methods and measures for data protection internal to microcontroller	38
Bibliography	40

ISO 19014-4:2020(E)

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 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 of ISO 19014-4, together with other parts in the ISO 19014 series, cancels and replaces ISO 15998:2008 and ISO/TS 15998-2:2012, which have been technically revised.

The main changes compared to the previous documents are as follows:

- additional requirements for software development,
- requirements for software-based parametrization development,
- requirements for transmission of safety related messages on a communication bus, and
- requirements for software validation and verification of machine performance levels.

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 any combination of electrical, electronic, and programmable electronic components [electrical/electronic/programmable electronic systems (E/E/PES)] 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 aspect(s), or one or more type(s) 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);

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO 19014-4:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/4c829175-4a82-4262-ae47-755789dd8f3d/sist-en-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

1 Scope

This document specifies general principles for software development and signal transmission requirements of safety-related parts of machine-control systems (MCS) in earth-moving machinery (EMM) and its equipment, as defined in ISO 6165. In addition, this document addresses the significant hazards as defined in ISO 12100 related to the software embedded within the machine control system. The significant hazards being addressed are the incorrect machine control system output responses from machine control system inputs.

Cyber security is out of the scope of this document.

NOTE For guidance on cybersecurity, see an appropriate security standard.

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 6750-1, *Earth-moving machinery — Operator's manual — Part 1: Contents and format*

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

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

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

ISO 19014-2:—¹⁾, *Earth-moving machinery — Functional safety — Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system*

3 Terms and definitions

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

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

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

1) Under preparation. Stage at the time of publication: ISO/DIS 19014-2:2020.

ISO 19014-4:2020(E)

- 3.1
bus system**
subsystem used in an electronic control system for the transmission of *messages* (3.6)
- Note 1 to entry: The bus system consists of the system unit (sources and sinks of information), a transmission path/transmission medium (e.g. electrical lines, fiber-optical lines, radio frequency transmission) and the interface between message source/sink and bus electronics (e.g. protocol application specific integrated circuit, transceivers).
- 3.2
encapsulated bus system**
bus system (3.1) comprising a fixed number or a predetermined maximum number of bus participants connected to each other through a transmission medium with well-defined and fixed performance/characteristics
- 3.3
failure of peer communication**
situation in which the communication peer is not available
- 3.4
unintended message repetition**
situation in which the same *message* (3.6) is unintentionally sent again
- 3.5
message repetition**
situation in which the same *message* (3.6) is intentionally sent again
- Note 1 to entry: This technique of resending the same message addresses failures such as message loss (3.10).
- 3.6
message**
electronic transmission of data
- Note 1 to entry: Transmitted data can include user data, address, or identifier data and data to ensure transmission integrity.
- 3.7
ECU
electronic control unit**
electronic device (electronic programmable controller) used in a control system on earth-moving machinery
- [SOURCE: ISO 22448:2010, 3.3, modified — The admitted terms "ECM" and "electronic control module" have been removed.]
- 3.8
reaction time**
time from the detection of a safety-related event until the initiation of a safety reaction
- 3.9
artifact**
work products that are produced and used during a project to capture and convey information
- 3.10
message loss**
unintended deletion of a *message* (3.6) due to a fault of a bus participant

3.11**incorrect sequence**

unintended modification of the sequence of *messages* (3.6) due to a fault of a bus participant

Note 1 to entry: *Bus systems* (3.1) can contain elements with stored messages (first-in, first-out (FIFOs), etc.) that can modify the correct sequence.

3.12**message falsification**

unintended modification of *messages* (3.6) due to an error of a bus participant or due to errors on the transmission channel

3.13**message retardation**

unintended delay or prevention of the safety function, caused by an overload of the transmission path by normal data exchange or by sending incorrect *messages* (3.6)

3.14**alive counter**

accounting component initialised with "0" when the object to be monitored is created or restored

Note 1 to entry: The counter increases from time $t-1$ to time t as long as the object is alive. Finally, the alive counter shows the period of time for which the object has been alive within a network.

3.15**black box testing**

testing of an object that does not require knowledge of its internal structure or its concrete implementation

3.16**partition**

resource entity allocating a portion of memory, input/output devices, and central processing unit usage to one or more *system tasks* (3.21)

Note 1 to entry: The partitions can be assigned to one or more subsystems within the microcontroller network.

3.17**software partitioning**

software fault (3.26) containment method consisting of assigning resources to specific software components with the intention of avoiding the propagation of a software fault to multiple *partitions* (3.16)

3.18**software component**

one or more *software modules* (3.19)

[SOURCE: ISO 26262-1:2018, 3.157, modified — The word "units" has been replaced with "modules".]

3.19**software module**

independent piece of software that can be independently tested and traced to a specification

Note 1 to entry: The software module is an indivisible software component.

3.20**software partitions**

runtime environment with separate system resources assigned

3.21**system task**

runtime entities that are executed within the resource budget of *partitions* (3.16) and with different priorities