



**SLOVENSKI STANDARD**  
**oSIST prEN ISO 19014-4:2019**  
**01-julij-2019**

---

**Stroji za zemeljska dela - Funkcijska varnost - 4. del: Načrtovanje in ocenjevanje programske opreme in prenosa podatkov za varnostne dele nadzornega sistema (ISO/DIS 19014-4:2019)**

Earth-moving machinery - Functional safety - Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system (ISO/DIS 19014-4:2019)

Erdbaumaschinen - Sicherheit - Teil 4: Gestaltung und Beurteilung von Software und Datenübertragung für sicherheitsrelevante Steuerungssysteme

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/DIS 19014-4:2019)

**Ta slovenski standard je istoveten z: prEN ISO 19014-4**

---

**ICS:**

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

**oSIST prEN ISO 19014-4:2019**                      **en,fr,de**



# DRAFT INTERNATIONAL STANDARD

## ISO/DIS 19014-4

ISO/TC 127/SC 2

Secretariat: ANSI

Voting begins on:  
2019-05-10Voting terminates on:  
2019-08-02

---

---

### Earth-moving machinery — Functional safety —

Part 4:

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

ICS: 53.100

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>

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

**ISO/CEN PARALLEL PROCESSING**



Reference number  
ISO/DIS 19014-4:2019(E)

© ISO 2019

# 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 2019

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  
Fax: +41 22 749 09 47  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Software development</b> .....	<b>4</b>
4.1 Planning.....	4
4.2 Artifacts.....	6
4.3 Software safety requirements specification.....	7
4.4 Software architecture design.....	7
4.5 Software module design and coding.....	8
4.6 Language, library, and tool selection.....	9
4.7 Software module testing.....	10
4.8 Software module integration and testing.....	11
4.9 Software validation.....	12
<b>5 Software-based parameterization</b> .....	<b>13</b>
5.1 General.....	13
5.2 Data integrity.....	13
5.3 Software-based parameterization verification.....	13
<b>6 Transmission protection of safety-related messages on bus systems</b> .....	<b>13</b>
<b>7 Independence by software partitioning</b> .....	<b>15</b>
7.1 Several partitions within a single microcontroller.....	15
7.2 Several partitions within the scope of an ECU network.....	16
<b>Annex A (informative) Description of software methods/measures</b> .....	<b>17</b>
<b>Annex B (normative) Software validation test environments</b> .....	<b>30</b>
<b>Annex C (informative) Data integrity assurance</b> .....	<b>33</b>
<b>Annex D (informative) Methods and measures for transmission protection</b> .....	<b>34</b>
<b>Annex E (informative) Methods and measures for data protection internal to microcontroller</b> .....	<b>36</b>

## ISO/DIS 19014-4:2019(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: [www.iso.org/directives](http://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](http://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:

- Earth-moving machinery – Functional Safety – Part 1: Risk assessment methodology to determine control system performance requirements
- Earth-moving machinery – Functional Safety – Part 2: Design and Evaluation of Safety-Related Machine Control Systems
- Earth-moving machinery – Functional Safety – Part 3: Environmental Testing Requirements
- Earth-moving machinery – Functional Safety – Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system
- Earth-moving machinery – Functional Safety – Part 5: Table of Performance Levels

ISO 19014 series replaces ISO 15998

## Introduction

This International Standard 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 part of ISO 19014 is a type C standard as stated in ISO 12100.

**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>





# 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 part of ISO 19014 specifies general principles for software development and signal transmission requirements of safety-related parts of machine-control systems (MCS) in earth-moving machinery and its equipment, as defined in ISO 6165.

Cyber security is out of the scope of this document.

## 2 Normative references

For normative references refer to ISO 19014-1.

## 3 Terms and definitions

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

### 3.1 Bus system

Subsystem used in an electronic control system for the transmission of safety-related messages; 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, RF transmission) and the interface between message source/sink and bus electronics (e.g. protocol ASICs, transceivers).

### 3.2 Encapsulated bus system

Bus system 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

communication peer is not available

### 3.4 Unintended message repetition

same message is unintentionally sent again

### 3.5 Incorrect sequence

order in which data has been sent changed during transmission, i.e. the data is not received in the same order as in which it was sent

## ISO/DIS 19014-4:2019(E)

### 3.6 Message repetition

same message is unintentionally sent again

### 3.7 Message

Electronic transmission including user data, an address and data to ensure transmission integrity.

### 3.8 Maximum extension size

Maximum permissible number of senders and receivers that are engaged in the message exchange as defined for the system.

### 3.9 Reaction time

Time from the detection of a safety-related event until the initiation of a safety reaction.

### 3.10 Message repetition

Error due to a fault of a bus participant, whereby old, non-up-to-date messages are repeated at an incorrect point in time.

Note 1 to entry : This activity can cause a hazardous disturbance of the receiver (e.g. signaling “access door closed” when it is already open).

### 3.11 Message loss

Unintended deletion of a message due to a fault of a bus participant.

### 3.12 Insertion of messages

Unintended insertion of a message due to a fault of a bus participant.

### 3.13 Incorrect sequence

Unintended modification of the sequence of messages due to a fault of a bus participant.

Note 1 to entry Bus systems can contain elements with stored messages (FIFOs, etc.) that can modify the correct sequence.

### 3.14 Message falsification

Unintended modification of messages due to an error of a bus participant or due to errors on the transmission channel.

### 3.15 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.

### 3.16 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.

### 3.17 Black-box test

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

### 3.18 Partition

Resource entity allocating a portion of memory, I/O devices and CPU usage to one or more tasks.

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

### 3.19 Software partitioning

Software fault containment method consisting of assigning resources to specific software components with the intention of avoiding the propagation of a software fault to multiple partitions.

### 3.20 Absolute addressing

Explicit identification of a memory location or of a peripheral device.

(cf. [3.17](#) relative addressing)

### 3.21 Relative addressing

Identification of a memory location or a peripheral device as an offset from another address.

(cf. [3.16](#) absolute addressing)

### 3.22 Software component

One or more software modules.

[MOD ISO 26262-1: 2011, 3.123] [SIST EN ISO 19014-4:2020  
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)

### 3.23 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.

### 3.24 Software partitions

Runtime environment with separate system resources assigned.

### 3.25 Task

Runtime entities that are executed within the resource budget of partitions and with different priorities.

### 3.26 Independence of software

Exclusion of unintended interactions between software components, as well as freedom from impact on the correct operation of a software component resulting from errors of another software component.

### 3.27 Operational history

Operating data about a component or a software module during its time in service.

## ISO/DIS 19014-4:2019(E)

### 3.28 Demand profile

Usage scope of components or software modules that characterizes their behavior during the operating experience.

### 3.29 Maximum cycle time

Static time to access a communication bus between nodes at a bus or node level.

Note 1 to entry The application of a Time-Triggered Protocol ensures this cycle time is not exceeded.

### 3.30 Maximum response time

Fixed time assigned to a system activity to exchange globally-synchronised messages on a bus in a Time-Triggered Architecture.

### 3.31 Software fault

An incorrect step, process, or data definition in software which causes the system to produce unexpected results.

### 3.32 Impact Analysis

Documentation that records the understanding and implications of a proposed change.

### 3.33 Configuration Management Process

The task of tracking and controlling changes to the artifacts in the development process.

## 4 Software development

This clause gives recommendations for the design of software and the subsequent related testing. The avoidance of software faults shall be considered during the entire software development process.

### 4.1 Planning

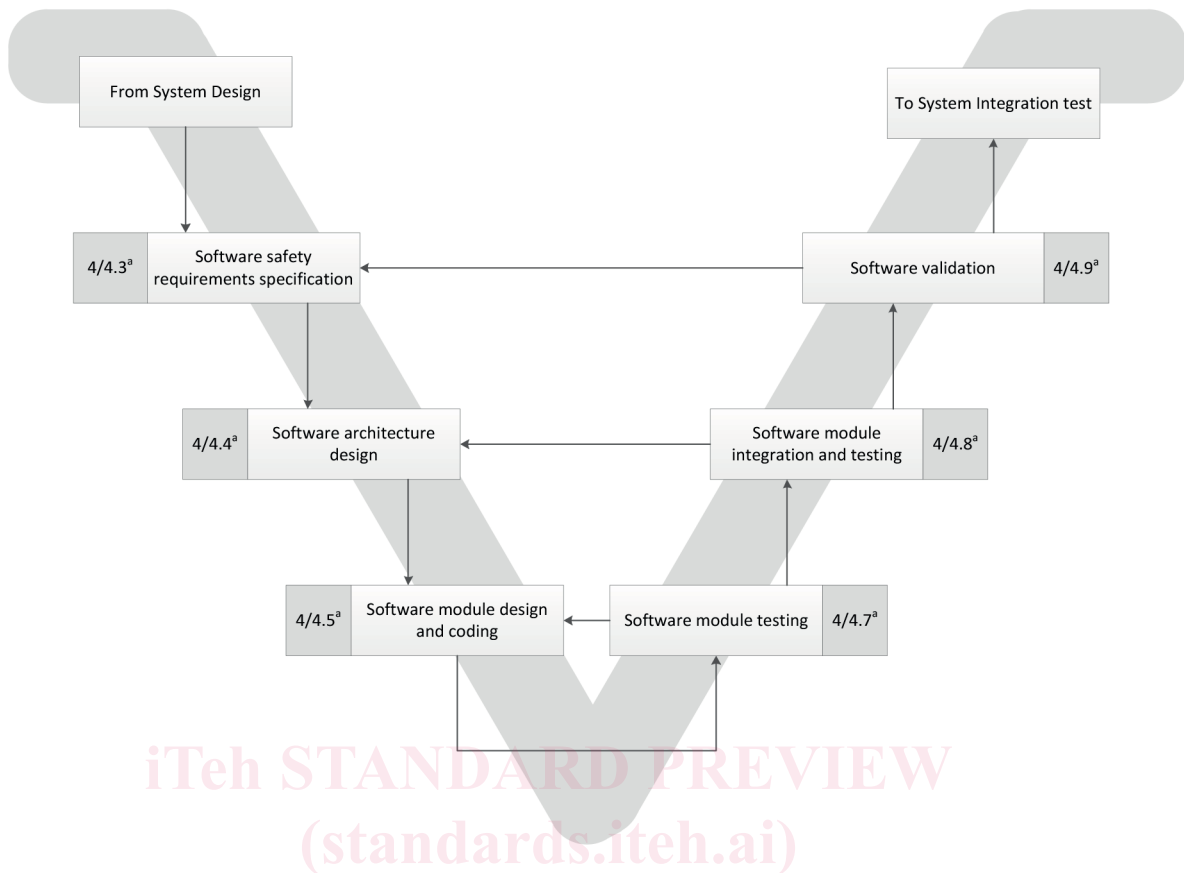
The main objective of the following requirements is to achieve software reliability by means of readable, understandable, testable, and maintainable software.

A plan shall be developed to define the relationship between the individual phases of the software development and the related artifacts.

Appropriate methods and measures shall be selected for software development according to the MPLr.

The MPLr of the system may be achieved by adding, in parallel, two systems of a lower performance level. When adding in parallel, the software can be developed in each system to the lower MPLr requirements. This is only allowable when there are no common cause failures between the two systems.

The suitability of the selected methods or measures to the application area shall be justified and shall be made at the beginning of each planned development phase. For a particular application, the appropriate combination of methods or measures shall be stated during development planning. Methods or measures not listed in [Table 1](#) through [Table 7](#) may be used.



**Figure 1 — Software development V-model**

<sup>a</sup> The first number in this and the other toned boxes signifies the part of ISO 19014, while the second number, separated from the first by a slash, signifies the clause number of that part, (e.g. “4/4.4” signifies ISO 19014-4, Sub-Clause 4.4)

NOTE This figure is a representation of one possible design method (V-Model). Any organized, proven development process that meets the requirements of ISO 19014 can be used for the software development

When selecting methods and measures, in addition to manual coding, model-based development can be applied where the source code is automatically generated from models.

With each method or measure in the tables, there is a different level of recommendation for each performance level. These recommendations are as follows:

+	The method or measure shall be used for this MPLr. In case this method or measure is not used, the related rationale shall be documented during the safety planning phase.
o	The method or measure may be used for this MPLr.
-	The method or measure is not suitable to meet this MPLr.

Methods and measures corresponding to the respective MPLr shall be selected. Alternative or equivalent methods and measures are identified by letters after the number. At least one of the alternatives or equivalent methods and measures marked with a “+” shall be selected, in which case, providing a rationale is not required.

Example