AS ISO 19014.4:2022
ISO 19014-4:2020

Australian STANDARD®

STANDARDS Australia

Earth-moving machinery — Functional safety

Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system

AS ISO 19014.4:2022

This Australian Standard ® was prepared by ME-063, Earthmoving Equipment. It was approved on behalf of the Council of Standards Australia on 16 February 2022.

This Standard was published on 25 February 2022.

The following are represented on Committee ME-063:

Australasian Institute of Mining & Metallurgy
Australian Industry Group
Better Regulation Division — Safework NSW
Construction and Mining Equipment Industry Group
Department of Regional NSW
Engineers Australia
Institute of Instrumentation, Control & Automation
Minerals Council of Australia
Mining Electrical and Mining Mechanical Engineering Society
Resources Health & Safety Queensland
University of Queensland

This Standard was issued in draft form for comment as DR AS ISO 19014.4:2021.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76113 670 2

AS ISO 19014.4:2022
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

First published as AS ISO 19014.4:2022.

Preface

This Standard was prepared by the Standards Australia Committee ME-063, Earthmoving Equipment.

The objective of this document is to specify 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.

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

This document is identical with, and has been reproduced from, 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*.

As this document has been reproduced from an International Standard, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

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.

NOTES

Australian Standard®

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.