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. This is a preview. Click here to purchase the full publication.



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.

This is a preview. Click here to purchase the full publication.

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

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 This is a preview. Click here to purchase the full publication.

First published as AS ISO 19014.4:2022.

COPYRIGHT

© ISO 2022 — All rights reserved © Standards Australia Limited 2022

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

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 whe This is a preview. Click here to purchase the full publication.

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

Preface			ii
Fo	reword		iv
In	troductio	n	v
1	Scope		1
2	Normat	ive references	
3	Terms a	nd definitions	
4	Software development		4
-	4.1	General	4
	4.2	Planning	5
	4.3	Artifacts	6
	4.4 4 5	Software architecture design	/ 8
	4.6	Software module design and coding	
	4.7	Language and tool selection	9
	This	is a preview. Click here to purchase the full publication.	
	4 10	Software validation	
F	Software-based narameterization		10
5	5 1	General	12 12
	5.2	Data integrity	
	5.3	Software-based parameterization verification	13
6	Transm	ission protection of safety-related messages on bus systems	
7	Indepe	ndence by software partitioning	
	7.1	General	
	7.2	Several partitions within a single microcontroller	
•	7.5	several partitions within the scope of an Eco network	
8	Informa 8 1	Coneral	17 17
	8.2	Instruction handbook	
Ar	inex A	(informative) Description of software methods/measures	
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	
Δr	nev F	(informative) Methods and measures for data protection internal to	
Л	IIICA L	microcontroller	
Bi	Bibliography		

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 r This is a preview. Click here to purchase the full publication. 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 <u>www.iso</u> .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 <u>www.iso.org/members.html</u>.