
**Tractors and machinery for
agriculture and forestry — Safety-
related parts of control systems —**

**Part 3:
Series development, hardware and
software**

*Tracteurs et matériels agricoles et forestiers — Parties des systèmes
de commande relatives à la sécurité —*

Partie 3: Développement en série, matériels et logiciels

ISO 25119-3:2018

<https://standards.iteh.ai/catalog/standards/iso/283017c5-70a4-4989-9c6a-97acddef44b4/iso-25119-3-2018>



iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

ISO 25119-3:2018

<https://standards.iteh.ai/catalog/standards/iso/283017c5-70a4-4989-9c6a-97acddef44b4/iso-25119-3-2018>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2018

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
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	2
3 Terms and definitions	2
4 Abbreviated terms	2
5 System design	3
5.1 Objectives	3
5.2 General	3
5.3 Prerequisites	4
5.4 Requirements	4
5.4.1 Structuring safety requirements	4
5.4.2 Technical safety concept	5
5.5 Work products	7
6 Hardware	7
6.1 Objectives	7
6.2 General	7
6.3 Prerequisites	7
6.4 Requirements	7
6.5 Hardware categories	9
6.6 Work products	9
7 Software	10
7.1 Software development planning	10
7.1.1 Objectives	10
7.1.2 General	10
7.1.3 Prerequisites	10
7.1.4 Requirements	10
7.1.5 Work products	13
7.2 Software safety requirements specification	13
7.2.1 Objectives	13
7.2.2 General	13
7.2.3 Prerequisites	13
7.2.4 Requirements	13
7.2.5 Work products	17
7.3 Software architecture design	17
7.3.1 Objectives	17
7.3.2 General	17
7.3.3 Prerequisites	17
7.3.4 Requirements	17
7.3.5 Work products	19
7.4 Software component design and implementation	19
7.4.1 Objectives	19
7.4.2 General	19
7.4.3 Prerequisites	19
7.4.4 Requirements	19
7.4.5 Work products	29
7.5 Software component testing	29
7.5.1 Objectives	29
7.5.2 General	29
7.5.3 Prerequisites	29
7.5.4 Requirements	29
7.5.5 Work products	37

7.6	Software integration and testing.....	37
7.6.1	Objectives.....	37
7.6.2	General.....	38
7.6.3	Prerequisites.....	38
7.6.4	Requirements.....	38
7.6.5	Work products.....	39
7.7	Software safety testing.....	40
7.7.1	Objectives.....	40
7.7.2	General.....	40
7.7.3	Prerequisites.....	40
7.7.4	Requirements.....	40
7.7.5	Work products.....	44
7.8	Software-based parameterisation.....	44
7.8.1	Objective.....	44
7.8.2	General.....	44
7.8.3	Prerequisites.....	45
7.8.4	Requirements.....	45
7.8.5	Work products.....	46
Annex A	(informative) Example of agenda for assessment of functional safety at AgPL = e.....	47
Annex B	(normative) Independence by software partitioning.....	49
Bibliography		59

iTeh Standards
(<https://standards.itih.ai>)
Document Preview

ISO 25119-3:2018

<https://standards.itih.ai/catalog/standards/iso/283017c5-70a4-4989-9c6a-97acddef44b4/iso-25119-3-2018>

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 Technical Committee ISO/TC 23, *Tractors and machinery for agriculture and forestry*, Subcommittee SC 19, *Agricultural electronics*.

This second edition cancels and replaces the first edition (ISO 25119-3:2010), which has been technically revised. The main changes compared to the previous edition are as follows:

- the introduction has been modified to add specific information on safety standards;
- the prerequisites of functional safety have been specified;
- Clause 5 has been revised to:
 - specify the prerequisites of functional safety, and
 - simplify the general requirements of technical safety concepts;
- additional instructions have been added throughout the document to verify consistency of test specifications and reports;
- Annex B has been changed to a normative annex;
- the document has been editorially revised.

A list of all parts in the ISO 25119 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

ISO 25119 (all parts) sets out an approach to the assessment, design and verification, for all safety life cycle activities, of safety-related parts comprising electrical and/or electronic and/or programmable electronic systems (E/E/PES) on tractors used in agriculture and forestry, and on self-propelled ride-on machines and mounted, semi-mounted and trailed machines used in agriculture. It is also applicable to mobile municipal equipment.

A prerequisite to the application of ISO 25119 (all parts) is the completion of a suitable hazard identification and risk analysis (e.g. ISO 12100) for the entire machine. As a result, an E/E/PES is frequently assigned to provide safety-related functions that create safety-related parts of control systems (SRP/CS). These can consist of hardware or software, can be separate or integrated parts of a control system, and can either perform solely safety-related functions or form part of an operational function.

In general, the designer (and to some extent, the user) will combine the design and validation of these SRP/CS as part of the risk assessment. The objective is to reduce the risk associated with a given hazard (or hazardous situation) under all conditions of use of the machine. This can be achieved by applying various measures (both SRP/CS and non-SRP/CS) with the end result of achieving a safe condition.

ISO 25119 (all parts) allocates the ability of safety-related parts to perform a safety-related function under foreseeable conditions into five performance levels. The performance level of a controlled channel depends on several factors, including system structure (category), the extent of fault detection mechanisms (diagnostic coverage), the reliability of components (mean time to dangerous failure, common-cause failure), design processes, operating stress, environmental conditions and operation procedures. Three types of failures that can cause E/E/PES malfunctions leading to potential hazardous situations are considered: systematic, common-cause and random.

In order to guide the designer during design, verification, and to facilitate the assessment of the achieved performance level, ISO 25119 (all parts) defines an approach based on a classification of architecture with different design features and specific behaviour in case of a fault.

The performance levels and categories can be applied to the control systems of all kinds of mobile machines: from simple systems (e.g. auxiliary valves) to complex systems (e.g. steer by wire), as well as the control systems of protective equipment (e.g. interlocking devices, pressure sensitive devices).

ISO 25119 (all parts) adopts a risk-based approach for the determination of the risks, while providing a means of specifying the required performance level for the safety-related functions to be implemented by E/E/PES safety-related channels. It gives requirements for the whole safety life cycle of E/E/PES (design, validation, production, operation, maintenance, decommissioning), necessary for achieving the required functional safety for E/E/PES that are linked to the performance levels.

The structure of safety standards in the field of machinery is as follows.

- a) Type-A standards (basic safety standards) give basic concepts, principles for design and general aspects that can be applied to machinery.
- b) 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-hand controls, interlocking devices, pressure sensitive devices, guards).
- c) Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This document is a type-B1 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 organizations, 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);
- consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate at the drafting process of this document.

In addition, this document is intended for standardization bodies elaborating type-C standards.

The requirements of this document can be supplemented or modified by a type-C standard.

For machines which are covered by the scope of a type-C standard and which have been designed and built according to the requirements of that standard, the requirements of that type-C standard take precedence.

Itch Standards
(<https://standards.itech.ai>)
Document Preview

ISO 25119-3:2018

<https://standards.itech.ai/catalog/standards/iso/283017c5-70a4-4989-9c6a-97acddef44b4/iso-25119-3-2018>