

NORME INTERNATIONALE

ISO 25119-3

Deuxième édition
2018-10

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

Partie 3: Développement en série, matériels et logiciels

Tractors and machinery for agriculture and forestry — Safety-related parts of control systems —
Part 3: Series development, hardware and software

ISO 25119-3:2018

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



Numéro de référence
ISO 25119-3:2018(F)

© ISO 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>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2018

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos	v
Introduction	vii
1 Domaine d'application	1
2 Références normatives	2
3 Termes et définitions	2
4 Termes abrégés	2
5 Conception du système	3
5.1 Objectifs	3
5.2 Généralités	3
5.3 Conditions préalables	4
5.4 Exigences	4
5.4.1 Structuration des exigences de sécurité	4
5.4.2 Concept de sécurité technique	5
5.5 Produits fabriqués	7
6 Matériel	7
6.1 Objectifs	7
6.2 Généralités	7
6.3 Conditions préalables	7
6.4 Exigences	7
6.5 Catégories de matériel	9
6.6 Produits fabriqués	9
7 Logiciel	10
7.1 Planification de développement du logiciel	10
7.1.1 Objectifs	10
7.1.2 Généralités	10
7.1.3 Conditions préalables	10
7.1.4 Exigences	10
7.1.5 Produits fabriqués	13
7.2 Spécification relative aux exigences de sécurité du logiciel	13
7.2.1 Objectifs	13
7.2.2 Généralités	13
7.2.3 Conditions préalables	13
7.2.4 Exigences	13
7.2.5 Produits fabriqués	17
7.3 Architecture et conception du logiciel	17
7.3.1 Objectifs	17
7.3.2 Généralités	17
7.3.3 Conditions préalables	17
7.3.4 Exigences	17
7.3.5 Produits fabriqués	19
7.4 Conception et mise en œuvre du composant du logiciel	19
7.4.1 Objectifs	19
7.4.2 Généralités	19
7.4.3 Conditions préalables	19
7.4.4 Exigences	20
7.4.5 Produits fabriqués	30
7.5 Essai du composant du logiciel	30
7.5.1 Objectifs	30
7.5.2 Généralités	30
7.5.3 Conditions préalables	30
7.5.4 Exigences	30
7.5.5 Produits fabriqués	39

7.6	Intégration et essai du logiciel.....	39
7.6.1	Objectifs.....	39
7.6.2	Généralités.....	39
7.6.3	Conditions préalables.....	39
7.6.4	Exigences.....	40
7.6.5	Produits fabriqués.....	41
7.7	Essai de sécurité du logiciel.....	42
7.7.1	Objectifs.....	42
7.7.2	Généralités.....	42
7.7.3	Exigences.....	42
7.7.4	Produits fabriqués.....	46
7.8	Paramétrage fondé sur le logiciel.....	46
7.8.1	Objectifs.....	46
7.8.2	Généralités.....	46
7.8.3	Conditions préalables.....	47
7.8.4	Exigences.....	47
7.8.5	Produits fabriqués.....	48
Annexe A (informative) Exemple de programme relatif à une évaluation de la sécurité fonctionnelle au niveau AgPL = e.....		49
Annexe B (normative) Indépendance par partitionnement du logiciel.....		51
Bibliographie.....		62

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>

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/iso/fr/avant-propos.html.

Le présent document a été élaboré par le comité technique ISO/TC 23, *Tracteurs et matériels agricoles et forestiers*, sous-comité SC 19, *Électronique en agriculture*. 4989-9c6a-97acddef44b4/iso-25119-3-2018

Cette deuxième édition annule et remplace la première édition (ISO 25199-3:2010), qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

- l'introduction a été modifiée pour ajouter des informations spécifiques sur les normes de sécurité;
- les conditions préalables à la sécurité fonctionnelle ont été spécifiées;
- l'[Article 5](#) a été révisé pour:
 - spécifier les conditions préalables à la sécurité fonctionnelle, et
 - simplifier les exigences générales des concepts techniques de sécurité;
- des instructions supplémentaires ont été ajoutées dans l'ensemble du document pour vérifier la cohérence des spécifications et des rapports d'essai;
- l'[Annexe B](#) a été changée en une annexe normative;
- le présent document a fait l'objet d'une révision rédactionnelle.

Une liste de toutes les parties de la série ISO 25119 se trouve sur le site web de l'ISO.

Tout retour ou question sur le présent document doit être adressée à l'organisme national de normalisation de l'utilisateur. Une liste complète de ces organismes peut être consultée à l'adresse www.iso.org/members.html.

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>

Introduction

L'ISO 25119 (toutes les parties) établit une approche pour l'évaluation, la conception et la vérification de toutes les activités relatives au cycle de vie de sécurité des parties relatives à la sécurité constituées de systèmes électriques et/ou électroniques et/ou électroniques programmables (E/E/PES) utilisés sur les tracteurs agricoles et forestiers, sur les machines automotrices à conducteur porté et sur les machines portées, semi-portées et traînées utilisées en agriculture. Elle est également applicable aux équipements municipaux mobiles.

Le prérequis pour l'application de l'ISO 25119 (toutes les parties), est la réalisation d'une identification des risques et d'une analyse de risque (par exemple ISO 12100) adaptées pour la totalité de la machine. Il en résulte qu'un système E/E/PES est fréquemment prévu pour assurer des fonctions relatives à la sécurité, créant des *parties relatives à la sécurité des systèmes de commande* (SRP/CS). Ces parties peuvent être constituées de matériels et de logiciels, elles peuvent être des parties isolées du système de commande ou en faire partie intégrante, et elles peuvent soit assurer uniquement des fonctions relatives à la sécurité, soit faire partie d'une fonction opérationnelle.

En général, le concepteur (et, dans une certaine mesure, l'utilisateur) associe la conception et la validation de ces SRP/CS dans le cadre de l'appréciation du risque. L'objectif est de réduire le risque lié à un phénomène dangereux donné (ou à une situation dangereuse) dans toutes les conditions d'utilisation de la machine. Cela peut être réalisé en appliquant diverses mesures (aussi bien SRP/CS que non-SRP/CS) dans le but final de réaliser une condition de sécurité.

L'ISO 25119 (toutes les parties) aborde la capacité des parties relatives à la sécurité à réaliser une fonction relative à la sécurité dans des conditions prévisibles en cinq niveaux de performance. Le niveau de performance d'un canal contrôlé dépend de plusieurs facteurs, tels que la structure du système (catégorie), l'étendue du mécanisme de détection de défaut (couverture de diagnostic), la fiabilité des composants (temps moyen avant défaillance dangereuse, défaillances de cause commune), le processus de conception, la contrainte en service, les conditions environnementales et les procédures de fonctionnement. Trois types de défaillances sont susceptibles de provoquer des dysfonctionnements des systèmes E/E/PES conduisant à des situations potentiellement dangereuses sont considérés: les défaillances systématiques, les défaillances de cause commune et les défaillances aléatoires.

Afin de guider le concepteur pendant la conception, la vérification, et faciliter l'évaluation du niveau de performance atteint, l'ISO 25119 (toutes les parties) définit une approche fondée sur une classification d'architecture avec différentes caractéristiques de conception et un comportement spécifique en cas de défaut.

Les niveaux et catégories de performance peuvent être appliqués aux systèmes de commande de tous les types de machines mobiles, des systèmes simples (par exemple valves auxiliaires) aux systèmes complexes (par exemple transmission par fil), ainsi qu'aux systèmes de commande d'équipements de protection (par exemple dispositifs de verrouillage ou dispositifs sensibles à la pression).

L'ISO 25119 (toutes les parties) adopte une approche fondée sur le risque pour déterminer les risques, tout en fournissant un moyen permettant de spécifier le niveau de performance requis pour les fonctions relatives à la sécurité à mettre en œuvre par les canaux E/E/PES relatifs à la sécurité. Elle fournit les exigences pour tout le cycle de vie de sécurité des E/E/PES (conception, validation, production, fonctionnement, maintenance, démantèlement) nécessaires pour assurer la sécurité fonctionnelle requise pour les E/E/PES liés aux niveaux de performance.

La hiérarchie des normes est la suivante:

- a) Normes de type A (normes de sécurité fondamentales) précisant des notions fondamentales, des principes de conception et des aspects généraux valables pour tous les types de machines.
- b) Normes de type B (normes de sécurité relatives à un groupe) traitant d'un aspect de la sécurité ou d'un type de dispositif conditionnant la sécurité valable pour une large gamme de machines:
 - normes de type B1 traitant d'aspects particuliers de la sécurité (par exemple, distances de sécurité, température de surface, bruit);