

NORME INTERNATIONALE

ISO 25119-2

Troisième édition
2019-08

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

Partie 2: Phase de projet

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

Part 2: Concept phase

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

ISO 25119-2:2019

<https://standards.iteh.ai/catalog/standards/iso/1ee51eb5-6179-4eef-b8e4-92c731d85585/iso-25119-2-2019>



Numéro de référence
ISO 25119-2:2019(F)

© ISO 2019

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

ISO 25119-2:2019

<https://standards.iteh.ai/catalog/standards/iso/1ee51eb5-6179-4eef-b8e4-92c731d85585/iso-25119-2-2019>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2019

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	vi
1 Domaine d'application	1
2 Références normatives	2
3 Termes et définitions	2
4 Termes abrégés	2
5 Concept — UoO	3
5.1 Objectifs	3
5.2 Conditions préalables	3
5.3 Exigences	3
5.3.1 Exigences fondamentales et conditions ambiantes	3
5.3.2 Limites de l'UoO et ses interfaces avec d'autres UoO	4
5.3.3 Mise en correspondance et affectation des fonctions pertinentes aux UoO impliquées, sources de contrainte	4
5.3.4 Déterminations supplémentaires	4
5.4 Produits fabriqués	5
6 HARA: Détermination de l'AgPLr	5
6.1 Objectifs	5
6.2 Conditions préalables	5
6.3 Exigences	5
6.3.1 Procédures de préparation d'une analyse HARA	5
6.3.2 Les tâches d'une analyse HARA	5
6.3.3 Participants à l'analyse HARA	5
6.3.4 Classification d'un dommage potentiel	6
6.3.5 Classification de l'exposition dans la situation observée	6
6.3.6 Classification des possibilités d'éviter un dommage	7
6.3.7 Sélection de l'AgPLr	7
6.4 Produits fabriqués	8
7 Concept de sécurité fonctionnelle	9
7.1 Objectifs	9
7.2 Conditions préalables	9
7.3 Exigences	9
7.3.1 Objectifs de sécurité	9
7.3.2 Exigences de sécurité fonctionnelle	9
7.3.3 Valeur de MTTF _D	9
7.3.4 Valeur de DC	10
7.3.5 Sélection des catégories MTTF _{DC} , DC et SRL	10
7.3.6 Obtention de l'AgPLr	11
7.3.7 Compatibilité avec d'autres fonctions de sécurité	12
7.3.8 Combinaison d'E/E/PES	12
7.3.9 Variantes de combinaisons de SRP/CS pour atteindre l'AgPL global	12
7.4 Produits fabriqués	12
Annexe A (normative) Architectures désignées pour les SRP/CS	13
Annexe B (informative) Méthode simplifiée d'estimation du MTTF_{DC} d'un canal	21
Annexe C (informative) Détermination de la couverture de diagnostic (DC)	25
Annexe D (informative) Estimations relatives à la défaillance de cause commune (CCF)	31
Annexe E (informative) Défaillance systématique	33
Annexe F (informative) Caractéristiques des fonctions relatives à la sécurité souvent fondamentales pour la réduction des risques	36

Annexe G (informative) Exemple d'analyse du risque	39
Annexe H (normative) Compatibilité avec les autres normes relatives à la sécurité fonctionnelle	44
Annexe I (informative) Méthode alternative de conformité des systèmes assemblés	47
Annexe J (normative) Autres combinaisons de SRP/CS pour atteindre l'AgPL global	48
Bibliographie	50

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

[ISO 25119-2:2019](https://standards.iteh.ai/catalog/standards/iso/1ee51eb5-6179-4eef-b8e4-92c731d85585/iso-25119-2-2019)

<https://standards.iteh.ai/catalog/standards/iso/1ee51eb5-6179-4eef-b8e4-92c731d85585/iso-25119-2-2019>

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*.

Cette troisième édition annule et remplace la deuxième édition (ISO 25119-2:2018), qui a fait l'objet d'une révision technique.

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

- Une révision mineure a été faite sur l'[Annexe H](#) pour améliorer la clarté et la compréhension des exigences à suivre par l'utilisateur final concernant les sous-systèmes ou composants conçus suivant l'ISO 26262.

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

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

L'ISO 25119 (toutes ses parties) établit une approche pour l'évaluation, la conception et la vérification, pour toutes les activités relatives au cycle de vie de sécurité, des parties relatives à la sécurité comprenant les 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 ses 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 chargé d'assurer des fonctions relatives à la sécurité, créant des parties de systèmes de commande relatives à la sécurité (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 ses 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 défaillance susceptibles de provoquer des dysfonctionnements des systèmes E/E/PES conduisant à des situations potentiellement dangereuses sont considérés: la défaillance systématique, la défaillance de cause commune et la défaillance aléatoire.

Afin de guider le concepteur pendant la conception et la vérification, et de faciliter l'évaluation du niveau de performance atteint, l'ISO 25119 (toutes ses 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 ses 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 structure des normes de sécurité dans le domaine des machines 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 génériques de sécurité) traitant d'un ou plusieurs aspects de la sécurité, ou d'un ou plusieurs types de protecteur 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);

- normes de type B2 traitant de dispositifs conditionnant la sécurité (par exemple: commandes bi-manuelles, dispositifs de verrouillage, dispositifs sensibles à la pression, protecteurs).
- c) Normes de type C (normes de sécurité par catégorie de machines) indiquant des spécifications de sécurité détaillées s'appliquant à une machine particulière ou à un groupe de machines particulier.

Le présent document est une norme de type B1 comme mentionné dans l'ISO 12100.

Le présent document concerne, en particulier, les groupes de parties prenantes suivants représentant les acteurs du marché en ce qui concerne la sécurité des machines:

- fabricants de machines (petites, moyennes et grandes entreprises);
- les organismes de santé et de sécurité (autorités réglementaires, organismes de prévention des risques professionnels, surveillance du marché, etc.).

D'autres partenaires peuvent être concernés par le niveau de sécurité des machines atteint à l'aide du document par les groupes de parties prenantes mentionnés ci-dessus:

- utilisateurs de machines/employeurs (petites, moyennes et grandes entreprises);
- utilisateurs de machines/salariés (par exemple: syndicats de salariés, organisations représentant des personnes ayant des besoins particuliers);
- prestataires de services, par exemple pour la maintenance (petites, moyennes et grandes entreprises);
- consommateurs (dans le cas de machines destinées à être utilisées par des consommateurs).

Les groupes de parties prenantes mentionnés ci-dessus ont eu la possibilité de participer à l'élaboration du présent document.

De plus, le présent document est destiné aux organismes de normalisation élaborant des normes de type C.

Les exigences du présent document peuvent être complétées ou modifiées par une norme de type C.

<https://standards.iteh.ai/> Pour les machines couvertes par le domaine d'application d'une norme de type C et qui ont été conçues et construites conformément aux exigences de cette norme, les exigences de la norme de type C prévalent.