

Deuxième édition
2018-10

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

**Partie 4:
Procédés de production, de
fonctionnement, de modification et
d'entretien**

**iTEH Standards
(<https://standards.iteh.ai>)**

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

Part 4: Production, operation, modification and supporting processes

[ISO 25119-4:2018](#)

<https://standards.iteh.ai/catalog/standards/iso/d44357e9-26e0-4bf8-8645-99b25a4ff582/iso-25119-4-2018>



Numéro de référence
ISO 25119-4:2018(F)

© ISO 2018

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

[ISO 25119-4:2018](#)

<https://standards.iteh.ai/catalog/standards/iso/d44357e9-26e0-4bf8-8645-99b25a4ff582/iso-25119-4-2018>



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	vi
1 Domaine d'application	1
2 Références normatives	2
3 Termes et définitions	2
4 Termes abrégés	2
5 Système de management de la qualité	3
6 Vérification et validation	4
6.1 Objectifs	4
6.2 Généralités	4
6.3 Conditions préalables	4
6.4 Exigences	4
6.4.1 Validation et vérification de la conception des SRP/CS	4
6.4.2 Domaine d'application de la validation et de la vérification de sécurité	5
6.4.3 Activités	5
6.4.4 Plan de validation et de vérification	5
6.4.5 Spécification d'essai de validation et de vérification	5
6.5 Produits fabriqués	6
7 Gestion de la configuration	6
7.1 Objectifs	6
7.2 Conditions préalables	6
7.3 Exigences	6
7.4 Produits fabriqués	6
8 Libération du produit	6
8.1 Objectifs	6
8.2 Généralités	7
8.3 Conditions préalables	7
8.4 Exigences	8
8.4.1 Conditions de libération du produit	8
8.4.2 Documentation de libération du produit	8
8.5 Produits fabriqués	8
9 Planning de production, production et essais de production	8
9.1 Objectifs	8
9.2 Généralités	8
9.3 Conditions préalables	8
9.4 Exigences	9
9.4.1 Plan de production	9
9.4.2 Plan d'essai de la production	9
9.4.3 Personnel	9
9.4.4 Capacité du processus	9
9.4.5 Documentation	9
9.4.6 Non-conformité	9
9.4.7 Conditions de stockage et de transport	9
9.5 Produits fabriqués	10
10 Planification de fonctionnement et maintenance (instructions de fonctionnement, entretien, réparation et démantèlement)	10
10.1 Objectifs	10
10.2 Généralités	10
10.3 Conditions préalables	10
10.4 Exigences	10

10.4.1	Généralités	10
10.4.2	Programme d'entretien.....	10
10.4.3	Instructions de réparation	11
10.4.4	Instructions relatives aux services techniques.....	11
10.4.5	Informations pour l'utilisation	11
10.4.6	Observation sur le terrain.....	11
10.4.7	Conditions de stockage et de transport	11
10.4.8	Démantèlement et démontage.....	11
10.5	Produits fabriqués.....	12
11	Modifications (gestion des modifications).....	12
11.1	Objectif	12
11.2	Généralités.....	12
11.3	Conditions préalables	12
11.4	Exigences	12
11.4.1	Procédures de modification et d'amélioration du produit.....	12
11.4.2	Demande de modification.....	14
11.4.3	Évaluation de l'impact de la modification.....	15
11.4.4	Autorisation de modification	15
11.5	Produits fabriqués.....	15
12	Procédure relative aux fournisseurs de SRP/CS, sous-systèmes et composants.....	16
12.1	Objectifs	16
12.2	Généralités.....	16
12.3	Conditions préalables	16
12.4	Exigences	16
12.4.1	Généralités	16
12.4.2	Domaine d'application des exigences	17
12.4.3	Sélection du fournisseur	17
12.4.4	Initiation du projet.....	17
12.4.5	Planification du projet.....	17
12.4.6	Exécution du projet	18
12.4.7	Mesures de confirmation de la sécurité fonctionnelle des partenaires au développement.....	18
12.4.8	Validation du système	18
12.5	Produits fabriqués.....	18
13	Documentation technique	18
13.1	Objectifs	18
13.2	Exigences	19
13.2.1	Conservation des documents	19
13.2.2	Structure des documents	19
Annexe A (informative) Liste de vérification de la documentation technique	20	
Bibliographie	23	

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/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*.
http://www.iso.org/iso/iso_25119-4/-/iso-25119-4-2018

Cette deuxième édition annule et remplace la première édition (ISO 25119-4:2010), 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;
- le domaine d'application a été légèrement modifié;
- un nouvel Article 5 (système de management de la qualité) a été ajouté;
- l'ancien Article (gestion de la configuration) a été déplacé après l'Article 6;
- l'Article 6 a été révisé;
- l'exemple de la liste de contrôle de la documentation technique a été modifié;
- 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.

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 systématisques, 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:

- 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.
- 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);

- 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 tel que spécifié dans l'ISO 12100.

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

- fabricants de machines (petites, moyennes et grandes entreprises);
- 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 sociétés de maintenance (petites, moyennes et grandes entreprises);
- consommateurs (dans le cas de machines destinées à être utilisées par des consommateurs).

Les groupes de parties prenantes mentionnées ci-dessus ont eu la possibilité de participer au processus d'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.

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

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

Partie 4: Procédés de production, de fonctionnement, de modification et d'entretien

1 Domaine d'application

Le présent document établit des principes généraux pour la conception et le développement des parties relatives à la sécurité des systèmes de commande (SRP/CS) 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 peut également être applicable aux équipements municipaux mobiles (par exemple machines de nettoiement). Elle spécifie les caractéristiques et les catégories requises des SRP/CS pour réaliser leurs fonctions de sécurité.

Le présent document n'est pas applicable aux:

- véhicules aéroportés et sur cousin d'air utilisées en agriculture;
- équipements pour jardins et pelouses.

Le présent document spécifie les caractéristiques et les catégories requises des SRP/CS pour réaliser leurs fonctions relatives à la sécurité. Il n'identifie pas de niveaux de performance pour des applications spécifiques.

NOTE 1 Les normes spécifiques à une machine donnée (normes de type C) peuvent spécifier des niveaux de performance (AgPL) pour des fonctions relatives à la sécurité dans des machines relevant de leur domaine d'application. Sinon, la spécification de l'AgPL est de la responsabilité du fabricant.

Le présent document est applicable aux parties relatives à la sécurité des systèmes électriques/électroniques/électroniques programmables (E/E/PES), dans la mesure où celles-ci sont liées aux systèmes mécatroniques. Elle couvre les éventuels phénomènes dangereux dus au comportement fonctionnel des systèmes E/E/PES liés à la sécurité, y compris les interactions entre ces systèmes. Elle ne traite pas des phénomènes dangereux dus à l'équipement lui-même (choc électrique, incendie, fumées, chaleur, rayonnement, toxicité inflammabilité, réactivité, corrosion, libération de l'énergie, et phénomènes dangereux similaires, à moins d'être causés directement par une défaillance du comportement des systèmes E/E/PES liés à la sécurité. Elle traite également de la défaillance du comportement des systèmes E/E/PES liés à la sécurité impliqués dans les mesures de protection, protecteurs ou fonctions liées à la sécurité en réponse aux phénomènes dangereux hors E/E/PES.

Exemples inclus dans le domaine d'application du présent document:

- Parties de machines relatives à la sécurité (SRP/CS) qui limitent le flux de courant dans les hybrides électriques pour empêcher les phénomènes dangereux de panne d'isolement/choc;
- interférence électromagnétique avec les SRP/CS;
- SRP/CS conçus pour empêcher les incendies.

Exemples non inclus dans le domaine d'application du présent document:

- panne d'isolement due au frottement qui engendre des phénomènes de chocs électriques;

- rayonnement électromagnétique nominal qui impactent les systèmes de commande environnants de la machine;
- corrosion engendrant une surchauffe des câbles électriques.

Le présent document n'est pas applicable aux systèmes non-E/E/PES (par exemple hydraulique, mécanique et pneumatique).

NOTE 2 Pour les principes de conception relatifs à la sécurité des machines, voir également l'ISO 12100.

Le présent document n'est pas applicable aux parties relatives à la sécurité des systèmes de commande fabriqués avant la date de sa publication.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 3600, *Tracteurs, matériels agricoles et forestiers, matériel à moteur pour jardins et pelouses — Manuels d'utilisation — Contenu et présentation*

ISO 25119-1:2018, *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux pour la conception et le développement*

ISO 25119-2:2018, *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 2: Phase de projet*

ISO 25119-3:2018, *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 3: Développement en série, matériels et logiciels*

3 Termes et définitions

[ISO 25119-4:2018](#)

Pour les besoins du présent document, les termes et définitions de l'ISO 25119-1 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques pour l'utilisation en normalisation aux adresses suivantes:

- ISO Online browsing platform: disponible à l'adresse <https://www.iso.org/obp>
- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>

4 Termes abrégés

Pour les besoins du présent document, les termes abrégés suivants s'appliquent.

AgPL	niveau de performance agricole (<i>agricultural performance level</i>)
AgPL _r	niveau de performance agricole requis (<i>required agricultural performance level</i>)
CAD	conception assistée par ordinateur (<i>computer-aided design</i>)
Cat	catégorie de matériel
CCF	défaillance de cause commune (<i>common-cause failure</i>)
DC	couverture de diagnostic (<i>diagnostic coverage</i>)

DC _{avg}	couverture moyenne de diagnostic (<i>average diagnostic coverage</i>)
UCE	unité de commande électronique
ETA	analyse par arbre d'événements (<i>event tree analysis</i>)
E/E/PES	systèmes électriques/électroniques/électroniques programmables (<i>electrical/electronic/programmable electronic systems</i>)
CEM	compatibilité électromagnétique
FMEA	analyse des modes de défaillance et de leurs effets
FSM	gestion de la sécurité fonctionnelle (<i>functional safety management</i>)
FTA	analyse par arbre de panne (<i>fault tree analysis</i>)
HARA	hazard analysis and risk assessment
HIL	matériel incorporé (<i>hardware in the loop</i>)
MTTF	temps moyen avant défaillance (<i>mean time to failure</i>)
MTTF _D	temps moyen avant défaillance dangereuse (<i>mean time to dangerous failure</i>)
MTTF _{DC}	temps moyen avant défaillance dangereuse pour chaque canal (<i>mean time to dangerous failure for each channel</i>)
PES	système électronique programmable (<i>programmable electronic system</i>)
QM	management (mesures) de la qualité (<i>quality measures</i>)
RAM	mémoire vive (<i>random-access memory</i>)
SOP	démarrage de la production (<i>start of production</i>)
SRL	niveau d'exigence du logiciel (<i>software requirement level</i>)
SRP	parties relatives à la sécurité (<i>safety-related parts</i>)
SRP/CS	parties relatives à la sécurité d'un système de commande (<i>safety-related parts of control systems</i>)
UoO	unité d'observation

5 Système de management de la qualité

Un système de management de la qualité est une partie importante de la sécurité fonctionnelle. Les utilisateurs du présent document doivent démontrer la conformité avec les [Articles 7, 8, 9 et 11](#)

- en appliquant les principes de management de la qualité tels que ceux qui figurent dans l'ISO 9001, en prenant pour recommandation les [Articles 7, 8, 9 et 11](#), ou
- en appliquant les spécifications des [Articles 7, 8, 9 et 11](#) tels qu'ils sont rédigés dans le présent document.