NORME INTERNATIONALE

ISO 25119-1

Deuxième édition
2018-10

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

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

Part 1: General principles for design and development

Numéro de référence
ISO 25119-1:2018(F)

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

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.

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 deuxième édition annule et remplace la première édition (ISO 25119-1:2010), 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 Tableaux 1 à 3 ont été supprimés et les tableaux suivants ont été renumérotés;

— L'Article 5 (Système de management de la qualité) a été inséré et les articles suivants ont été renumérotés;

— dans le paragraphe 8.5, les produits fabriqués issus des activités de gestion de la sécurité après que les SOP ont été spécifiés;

— la Figure 2 a été modifiée;

— le document a été révisé sur le plan rédactionnel.

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 fondamentales de sécurité), contenant des notions fondamentales, des principes de conception et des aspects généraux relatifs aux machines;

b) normes de type B (normes génériques de sécurité), traitant d'un aspect de la sécurité ou d'un type de dispositif conditionnant la sécurité valable pour toutes les machines ou 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), traitant des exigences 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:

— les 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.

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.

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

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) utilisées 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. Il peut également s'appliquer aux équipements municipaux mobiles (par exemple machines de nettoiement).

Le présent document ne s'applique pas:

— aux véhicules aéroportés et sur coussin d'air utilisés en agriculture,

— aux équipements de jardinage ou horticoles.

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 s'applique 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. Il couvre les éventuels phénomènes dangereux dus au dysfonctionnement de systèmes E/E/PES relatifs à la sécurité, y compris l'interaction entre ces systèmes. Il ne traite pas des phénomènes dangereux associés aux événements suivants: choc électrique, incendie, fumées, chaleur, rayonnement, toxicité, inflammabilité, réactivité, corrosion, libération d'énergie, et phénomènes dangereux similaires, à moins qu'ils ne soient causés directement par un dysfonctionnement des systèmes E/E/PES relatifs à la sécurité. Il couvre également le dysfonctionnement des systèmes E/E/PES relatifs à la sécurité qui sont impliqués dans les mesures de protection, protecteurs ou fonctions relatives à la sécurité en réponse aux phénomènes dangereux hors E/E/PES.

Exemples faisant partie du domaine d'application du présent document:

— SRP/CS limitant 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 conçues pour empêcher les incendies.

Exemples ne faisant pas partie du domaine d'application du présent document:

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

— rayonnement électromagnétique nominal qui impacte 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 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*

ISO 25119-4:2018, *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*

3 Termes et définitions

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

L'ISO et la CEI tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables 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/

3.1
niveau de performance agricole
AgPL
niveau qui spécifie l'aptitude des parties de systèmes de commande relatives à la sécurité à accomplir une fonction relative à la sécurité dans des conditions prévisibles

Note 1 à l'article: Pour les besoins de l'ISO 25119 (toutes ses parties), la performance pour chaque fonction est divisée en cinq niveaux (a, b, c, d et e), où la sécurité fonctionnelle assurée par la SRP/CS est faible dans «a» et élevée dans «e».

3.2
niveau de performance agricole requis
$AgPL_r$
niveau(x) de performance (AgPL) nécessaire(s) pour chaque fonction relative à la sécurité

Note 1 à l'article: En fonction des comportements potentiels d'une UoO défectueuse, une fonction relative à la sécurité peut avoir plusieurs $AgPL_r$. Par exemple, une perte partielle d'une fonction, la perte complète soudaine d'une fonction et l'inaptitude à activer une fonction peuvent avoir trois $AgPL_r$ différents.

3.3
catégorie
classification des parties relatives à la sécurité d'un système de commande en fonction de sa résistance aux défaillances dangereuses, en tenant compte de leur comportement subséquent en état de défaut, obtenue par un arrangement structurel (architecture) des parties

3.4
canal
combinaison d'éléments d'entrée, logiques et de sortie nécessaire à l'exécution d'une ou plusieurs fonctions

3.5
défaillance de cause commune
CCF
défaillances multiples au sein d'une UoO, qui proviennent d'un seul événement et qui ne résultent pas les unes des autres

Note 1 à l'article: Il convient de ne pas confondre les défaillances de mode commun avec les défaillances de cause commune. En effet, les défaillances de mode commun peuvent résulter de différentes causes.

3.6
contrôlabilité
possibilité pour un individu impliqué d'éviter un dommage dans la situation qui l'expose à un risque

3.7
taux de défaillance dangereuse détectée
λ_{DD}
taux de défaillance détecté au sein de l'UoO, n'impliquant qu'une augmentation du risque nulle ou minime mais si non détecté, provoquerait une augmentation de risque immédiate

3.8
défaillance dangereuse
défaillance (et défaillance multiple due à une cause commune) par laquelle une SRP/CS n'est plus en mesure de maintenir la fonction de sécurité et dont le comportement de la machine qui en résulte pourrait faire apparaître une situation dangereuse

3.9
taux de défaillance dangereuse
λ_D
fraction de tous les composants qui subissent une *défaillance dangereuse* (3.8) par unité de temps

Note 1 à l'article: λ_D est la valeur inverse du $MTTF_D$.

3.10
couverture de diagnostic
DC
fraction de la probabilité de défaillances dangereuses détectées, λ_{DD}, et de la probabilité de défaillances dangereuses totales, λ_D, (3.9)

3.11
intervalle entre essais de diagnostic
intervalle entre les essais en ligne utilisé pour détecter les défauts dans un système relatif à la sécurité ayant une *couverture de diagnostic* (3.10) spécifiée

3.12
architecture E/E/PES
affectation de fonctions relatives à la sécurité à des unités de commande électronique (UCE) et classification en matériel et logiciel, y compris la communication

3.13
condition environnementale
condition physique dans laquelle un système est utilisé

3.14
exposition
durée et fréquence à laquelle un individu se trouve exposé à un phénomène dangereux potentiel