NORME INTERNATIONALE

ISO 25119-1

Première édition
2010-06-01

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 25119-1:2010(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 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 (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée 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.

L'ISO 25119-1 a été élaborée par le comité technique ISO/TC 23, *Tracteurs et matériels agricoles et forestiers*, sous-comité SC 19, *Électronique en agriculture*.

L'ISO 25119 comprend les parties suivantes, présentées sous le titre général *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*

— *Partie 2: Phase de projet*

— *Partie 3: Développement en série, matériels et logiciels*

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

Introduction

L'ISO 25119 établit une approche pour la conception et l'évaluation de toutes les activités relatives au cycle de vie de sécurité des systèmes relatifs à la sécurité constitués de composants 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 remorquées utilisées en agriculture. Elle est également applicable aux équipements municipaux. Elle couvre les éventuels phénomènes dangereux dus au comportement fonctionnel des systèmes E/E/PES relatifs à la sécurité, indépendamment des phénomènes dangereux dus à l'équipement E/E/PES lui-même (par exemple choc électrique, incendie, niveau de performance nominal du E/E/PES dédié à la sécurité passive et active).

Les parties des systèmes de commande des machines concernées sont fréquemment prévues pour assurer les fonctions critiques 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 critiques, 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 de prévention (aussi bien SRP/CS que non-SRP/CS) dans le but final de réaliser une condition de sécurité.

L'ISO 25119 aborde la capacité des parties relatives à la sécurité à réaliser une fonction critique 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 considérées: les défaillances systématiques, les défaillances de cause commune et les défaillances aléatoires.

Afin de guider le concepteur pendant la conception et faciliter l'évaluation du niveau de performance atteint, l'ISO 25119 définit une approche fondée sur une classification de structures 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 adopte une approche fondée sur le risque du client pour déterminer les risques, tout en fournissant un moyen permettant de spécifier le niveau de performance cible 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.

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

La présente partie de l'ISO 25119 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 remorquées utilisées en agriculture. Elle peut être également applicable aux équipements municipaux (par exemple machines de balayage des rues). Elle spécifie les caractéristiques et les catégories requises des SRP/CS pour réaliser leurs fonctions de sécurité.

La présente partie de l'ISO 25119 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 ne spécifie ni les fonctions de sécurité ni les catégories censées être utilisées dans un cas particulier.

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

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

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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 (y compris les éventuels amendements) s'applique.

ISO 25119-2:2010, *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 2: Phase de projet*

ISO 25119-3:2010, *Tracteurs et matériels agricoles et forestiers — Parties des systèmes de commande relatives à la sécurité — Partie 3: Développement en série, matériels et logiciels*

ISO 25119-4:2010, *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.

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

NOTE Pour les besoins de l'ISO 25119, la performance pour chaque situation dangereuse est divisée en cinq niveaux, a, b, c, d et e, où la sécurité fonctionnelle assurée par le SRP/CS dans «a» est faible et dans «e» est élevée.

3.2
niveau de performance agricole requis
$AgPL_r$
niveau de performance (AgPL) nécessaire pour obtenir la sécurité fonctionnelle requise pour chaque fonction de sécurité

3.3
catégorie
classification des parties relatives à la sécurité d'un système de commande en fonction de sa résistance aux défaillances et de son comportement subséquent dans les conditions de défaillance, et qui est réalisée par la disposition de la structure des parties et/ou par leur fiabilité

3.4
canal
combinaison en série d'éléments d'entrée, logiques et de sortie

3.5
défaillance de cause commune
CCF
défaillances qui affectent plusieurs entités à partir d'un seul événement et qui ne résultent pas les unes des autres

NOTE Il convient de ne pas confondre les défaillances de cause commune avec les défaillances de mode commun. (voir l'ISO 12100).

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 dangereuse des composants faisant l'objet d'une détection de défaut

3.8
défaillance dangereuse
défaillance par laquelle un SRP/CS n'est plus en mesure de maintenir le niveau de performance requis, même si la fonction de sécurité est maintenue par d'autres composants (redondants) du système (du fait de la réduction du niveau de performance qui en résulte)

3.9
taux de défaillance dangereuse
λ_d
fraction de tous les composants qui subissent une défaillance dangereuse par unité de temps

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, exprimée par

$$DC = \sum \lambda_{dd} / \sum \lambda_d$$

NOTE 1 La couverture de diagnostic peut exister pour tout ou partie d'un système à risque fonctionnel élevé, par exemple pour les capteurs et/ou le système logique et/ou les entités finales.

NOTE 2 La valeur de DC est définie conformément au Tableau 1.

NOTE 3 Pour le SRP/CS comprenant plusieurs parties, une valeur moyenne, DC_{avg}, est utilisée (voir l'ISO 25119-2:2010, Annexe C).

Tableau 1 — Couverture de diagnostic (DC)

Notation	Plage
Faible	DC < 60 %
Moyenne	60 % ⩽ DC < 90 %
Élevée	90 % ⩽ DC

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 spécifiée

3.12
architecture de système E/E/PES
affectation de fonctions critiques 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

3.15
défaillance
cessation de l'aptitude d'une entité à accomplir une fonction requise

NOTE 1 Les défaillances qui n'affectent pas la disponibilité du processus en commande ne s'inscrivent pas dans le domaine d'application de l'ISO 25119.

NOTE 2 Après défaillance, l'entité présente un défaut.

NOTE 3 Une «défaillance» est un passage d'un état à un autre, par opposition à un défaut, qui est un état.

NOTE 4 La notion de défaillance, telle qu'elle est définie, ne s'applique pas à une entité constituée seulement de logiciel.

3.16
défaut
état d'une entité inapte à accomplir une fonction requise, non comprise l'inaptitude due à la maintenance préventive ou à d'autres actions programmées ou due à un manque de moyens externes

NOTE 1 Un défaut est souvent la conséquence d'une défaillance de l'entité elle-même, mais il peut exister sans défaillance préalable.

NOTE 2 Pour les besoins de l'ISO 25119, le terme défaut signifie un *défaut aléatoire*.

3.17
fonction
comportement défini d'une ou de plusieurs unités de commande électronique

3.18
concept fonctionnel
fonctions de base et interactions nécessaires pour obtenir un comportement souhaité

NOTE Le concept fonctionnel est élaboré durant la phase de projet du cycle de vie de sécurité.

3.19
exigence fonctionnelle
exigence relative à une fonction prévue du système E/E/PES

3.20
sécurité fonctionnelle
système qui fonctionne de sorte à ne présenter aucun risque de dommage intolérable aux opérateurs ou à des tiers

3.21
concept de sécurité fonctionnelle
ensemble des fonctions relatives à la sécurité et interactions nécessaires pour obtenir un comportement souhaité

NOTE Le concept de sécurité fonctionnelle est élaboré durant la phase de projet du cycle de vie de sécurité.

3.22
exigence de sécurité fonctionnelle
exigence d'une fonction relative à la sécurité du système E/E/PES

3.23
exigence de sécurité du matériel
exigence qui s'applique au matériel relatif à la sécurité, et qui est incluse comme élément d'une exigence de sécurité technique

3.24
dommage
blessure physique

3.25
phénomène dangereux
source potentielle de dommage

3.26
situation dangereuse
circonstance dans laquelle une personne est exposée à un (des) phénomène(s) dangereux(s) pouvant entraîner des effets, immédiatement ou à plus long terme

3.27
utilisation normale
⟨d'une machine⟩ utilisation conformément aux indications données dans les manuels d'utilisation

3.28
inspection
méthode de vérification formelle et systématique utilisée pour examiner la qualité des produits

NOTE Lors d'une inspection, les produits fabriqués sont vérifiés par un ou plusieurs inspecteurs pour s'assurer de leur conformité aux exigences. L'inspection est organisée et dirigée par un responsable de l'inspection. L'auteur des produits fabriqués participe à l'inspection mais ne peut diriger le processus.

3.29
durée de vie de la machine
cycle de vie
temps écoulé entre la production et le démantèlement

3.30
réinitialisation manuelle
fonction au sein des parties relatives à la sécurité du système de commande utilisée pour restaurer manuellement une ou plusieurs fonctions de sécurité avant le redémarrage de la machine

3.31
fabricant
fabricant de la machine
fabricant de tracteurs agricoles et forestiers, de machines automotrices à conducteur porté, de machines portées, semi-portées et remorquées utilisées en agriculture, et d'équipements municipaux

Voir **fournisseur** (3.50).

3.32
temps moyen avant défaillance dangereuse
$MTTF_d$
valeur moyenne du temps prévu avant une défaillance dangereuse

NOTE 1 Elle est définie par les plages faible, moyenne et élevée.

Voir Tableau 2.

NOTE 2 Pour les besoins der l'ISO 25119, il est important que le $MTTF_d$ soit pris en compte individuellement pour chaque canal d'un SRP/CS ($MTTF_{dC}$).

NOTE 3 $MTTF_d$ est la valeur inverse de λ_d.

Tableau 2 — Temps moyen avant défaillance dangereuse ($MTTF_d$)

Notation	Plage
Faible	3 ans < $MTTF_d$ < 10 ans
Moyenne	10 ans < $MTTF_d$ < 30 ans
Élevée	$MTTF_d$ > 30 ans

3.33
contrôle
contrôle automatique
fonction de sécurité qui assure qu'une mesure de prévention est initiée en cas de réduction de l'aptitude d'un composant ou d'une entité à accomplir sa fonction, ou de modifications des conditions du processus telles qu'elles provoquent des phénomènes dangereux

3.34
neutralisation
suspension automatique temporaire d'une fonction relative à la sécurité par des parties relatives à la sécurité du système de commande

3.35
système électronique programmable
PES
système de commande, de protection ou de contrôle, qui utilise un ou plusieurs dispositifs électroniques programmables

NOTE Cela comprend tous les éléments du système, tels que les sources d'alimentation, les capteurs et autres dispositifs d'entrée, les inforoutes et autres voies de communication, et les actionneurs et autres dispositifs de sortie.

3.36
mesure de prévention
mesure destinée à assurer la sécurité fonctionnelle, mise en œuvre par le concepteur (prévention intrinsèque, protection et mesures de prévention complémentaires, informations pour l'utilisation) et par l'utilisateur (organisation, méthodes de travail sûres, surveillance, système du permis de travailler, fourniture et utilisation de moyens de protection supplémentaires, utilisation d'équipements de protection individuelle, formation)

3.37
mauvais usage raisonnablement prévisible
utilisation d'une machine d'une manière ne correspondant pas aux intentions du concepteur, mais pouvant résulter d'un comportement humain aisément prévisible

3.38
temps de réponse
temps maximal susceptible de s'écouler entre l'occurrence d'une erreur et l'atteinte d'un état de sécurité

3.39
risque
combinaison de la probabilité d'un dommage et de la gravité de ce dommage

3.40
analyse du risque
combinaison de la détermination des limites de la machine, de l'identification des phénomènes dangereux et de l'estimation du risque

3.41
appréciation du risque
processus global d'analyse et d'évaluation du risque

3.42
évaluation du risque
jugement destiné à établir, sur la base de l'analyse du risque, si un risque donné est tolérable

3.43
état de sécurité
mode de fonctionnement d'un système avec un niveau acceptable de risque

EXEMPLE Le mode de fonctionnement prévu, le mode de fonctionnement de sauvegarde ou les modes d'interruption.

3.44
objectif de sécurité
description de la manière dont un phénomène dangereux donné doit être évité

NOTE 1 Il s'agit de l'exigence de sécurité de plus haut niveau, dérivée de l'analyse des phénomènes dangereux et de l'appréciation du risque.

NOTE 2 L'existence de plusieurs objectifs de sécurité pour une seule entité est possible.

3.45
fonction de sécurité
fonction d'une machine dont la défaillance peut provoquer un accroissement immédiat du risque

3.46
partie relative à la sécurité d'un système de commande
SRP/CS
partie ou sous-partie d'un système de commande qui répond aux signaux d'entrée et génère des signaux de sortie relatifs à la sécurité

NOTE Les parties combinées relatives à la sécurité d'un système de commande débutent au point où les signaux relatifs à la sécurité sont initiés (par exemple la came de commande et le galet du contacteur de position) et prennent fin à la sortie des éléments de commande de puissance (par exemple les contacts principaux du contacteur); elles comprennent également les systèmes de contrôle.