NORME INTERNATIONALE

ISO 25119-4

Première édition
2010-06-01

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

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

Part 4: Production, operation, modification and supporting processes

Numéro de référence
ISO 25119-4:2010(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 25119-4 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 4: Procédés de production, de fonctionnement, de modification et d'entretien

1 Domaine d'application

La présente partie de l'ISO 25119 fournit des principes généraux pour les procédés de production, de fonctionnement, de modification et d'entretien 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 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).

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

ISO 25119-1:2010, *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 25119-2:2010, *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*

3 Termes et définitions

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

4 Termes abrégés

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

AgPL	niveau de performance agricole (*agricultural performance level*)
$AgPL_r$	niveau de performance agricole requis (*required agricultural performance level*)
CAD	conception assistée par ordinateur (*computer-aided design*)
Cat	catégorie de matériel
CCF	défaillance de cause commune (*common-cause failure*)
DC	couverture de diagnostic (*diagnostic coverage*)
DC_{avg}	couverture moyenne de diagnostic (*average diagnostic coverage*)
UCE	unité de commande électronique
ETA	analyse par arbre d'événements (*event tree analysis*)
E/E/PES	systèmes électriques/électroniques/électroniques programmables *(electrical/electronic/ programmable electronic systems*)
CEM	compatibilité électromagnétique
EUC	équipement commandé (*equipment under control*)
AMDE	analyse des modes de défaillance et de leurs effets
AMDEC	analyse des modes de défaillance, de leurs effets et de leur criticité
EPROM	mémoire morte reprogrammable (*erasable programmable read-only memory*)
FSM	gestion de la sécurité fonctionnelle (*functional safety management*)
FTA	analyse par arbre de panne (*fault tree analysis*)
HAZOP	étude des phénomènes dangereux et de l'exploitabilité (*hazard and operability study*)
HIL	matériel incorporé (*hardware in the loop*)
MTTF	temps moyen avant défaillance (*mean time to failure*)
$MTTF_d$	temps moyen avant défaillance dangereuse (*mean time to dangerous failure*)
PES	système électronique programmable (*programmable electronic system*)
QM	management (mesures) de la qualité (*quality measures*)
RAM	mémoire vive (*random-access memory*)
SOP	démarrage de la production (*start of production*)

SRL niveau d'exigence du logiciel (*software requirement level*)

SRP parties relatives à la sécurité (*safety-related parts*)

SRP/CS parties relatives à la sécurité d'un système de commande (*safety-related parts of control systems*)

SRS système relatif à la sécurité (*safety-related system*)

5 Gestion de la configuration

5.1 Objectifs

Le premier objectif est de s'assurer que les SRP/CS et les documents associés pour une fonction donnée peuvent être identifiés de manière unique et reproduits à tout moment.

Le second objectif est de s'assurer que les relations et les différences entre les versions antérieures et la version en vigueur des SRP/CS et documents associés peuvent être tracées.

5.2 Généralités

Tous les produits fabriqués de l'ISO 25119 doivent être traités par un système de gestion de la configuration.

5.3 Conditions préalables

Se reporter aux conditions préalables pour chaque phase du cycle de vie de sécurité.

5.4 Exigences

Les outils logiciels et les environnements de développement de logiciel doivent faire l'objet d'une gestion de la configuration.

Les données de gestion de la configuration doivent être conservées conformément à la politique de la société en matière de conservation des documents.

5.5 Produits fabriqués

Les produits fabriqués applicables sont les listing des SRP/CS, avec référence aux documents associés pour une configuration donnée.

6 Vérification et validation

6.1 Objectifs

Un objectif est de démontrer que les exigences relatives à la sécurité sont appropriées au système E/E/PES et qu'elles sont satisfaites.

Un autre objectif est de démontrer que les buts relatifs à la sécurité au niveau de la machine sont atteints.

6.2 Généralités

Les précédentes étapes de vérification (par exemple revues, analyses de sécurité, essais d'intégration des composants) avaient pour objectif de démontrer que les résultats de chaque phase particulière étaient conformes aux exigences de conception et de spécification pertinentes décrites dans l'ISO 25119-3.

6.3 Conditions préalables

Pour cette phase, les conditions préalables sont les suivantes:

— plan de projet, conformément à l'ISO 25119-1:2010, 5.4.7 — délais, ressources, équipements, degré de maturité, etc.;

— plan d'essai de machine — partie du processus d'assurance qualité existant;

— analyse du risque, conformément à ISO 25119-2:2010, Article 6 — identification des phénomènes dangereux potentiels;

— objectifs de sécurit et états de sécurité;

— concept de sécurité technique, conformément à ISO 25119-3:2010, Article 5 — exigences de sécurité technique.

6.4 Exigences

6.4.1 Validation/vérification de la conception des SRP

La conception des SRP du système de commande doit être validée/vérifiée (voir l'ISO 25119-1:2010, Figure 1).

La validation/vérification doit démontrer que chaque SRP satisfait

— à toutes les exigences de la catégorie spécifiée (voir l'ISO 25119-2:2010, Annexe A), et

— aux caractéristiques de sécurité spécifiées pour la partie considérée, comme établi dans les exigences de conception.

6.4.2 Domaine d'application de la validation/vérification de sécurité

Dans le cadre du cycle de vie de sécurité, la validation/vérification des attributs de sécurité doivent être réalisées pour les éléments suivants:

— le système complet au niveau de la machine (par exemple essais au banc, essais du matériel incorporé, machine d'essai);

— le matériel;

— le logiciel.

6.4.3 Activités

Dans le cadre d'une validation/vérification de sécurité structurée, la séquence suivante doit être suivie:

— planification de la validation/vérification;

— spécification de la validation/vérification;

— exécution de la validation/vérification;

— rapport du résultat de la validation/vérification.

Toutes les variantes ou versions du système E/E/PES ayant fait l'objet des activités de validation/vérification doivent être clairement identifiées.

6.4.4 Plan de validation/vérification

Un plan de validation/vérification doit être élaboré pour les objectifs de sécurité et les exigences de sécurité technique, y compris les éléments suivants:

— objet de la validation/vérification et variantes possibles;

— degré de maturité du système;

— buts de la validation/vérification;

— techniques de validation/vérification;

— déclaration d'indépendance de la personne en charge de la validation/vérification à l'égard du développeur;

— équipements et conditions environnementales requis, y compris les spécifications d'étalonnage des outils;

— référence spécifiée au plan de projet global;

— critères d'échec/réussite pour tous les essais.

6.4.5 Validation/vérification, spécification d'essai du matériel et du logiciel

La fonction de l'élément doit être validée/vérifiée au niveau du système E/E/PES, en fonction de la conformité aux exigences de sécurité du matériel/logiciel.

6.4.6 Spécification d'essai de validation/vérification du système complet

Les caractéristiques des SRP/CS doivent être validées/vérifiées au niveau de la machine, en fonction de la conformité au concept de sécurité fonctionnelle.

6.4.7 Spécification d'essai de validation/vérification

Les méthodes et les mesures suivantes doivent être utilisées et spécifiées:

— essais (par exemple boîte noire, HIL, essais de machine, essais sur le terrain, etc.);

— analyse (par exemple simulation);

— revues des documents pertinents (données d'entrée du matériel/logiciel, par exemple AMDE, schéma de circuit).

6.5 Produits fabriqués

Les produits fabriqués suivants sont applicables à cette phase:

a) Un plan de validation/vérification détaillé.

b) Une spécification d'essai.

c) Un rapport de validation/vérification qui doit comprendre la preuve que les buts de la validation/vérification ont été atteints pour

   1) le système complet au niveau de la machine,

   2) le matériel, et

   3) le logiciel.

7 Libération du produit

7.1 Objectifs

Cette phase a pour objectif de spécifier les conditions de libération du produit à l'achèvement du développement du système E/E/PES. La libération du produit confirme que les exigences relatives à la sécurité fonctionnelle de la machine ont été satisfaites.

7.2 Généralités

La Figure 1 montre les étapes d'approbation nécessaires pour le développement d'un système E/E/PES et leur ordre de réalisation afin de respecter les conditions requises pour la libération du produit.

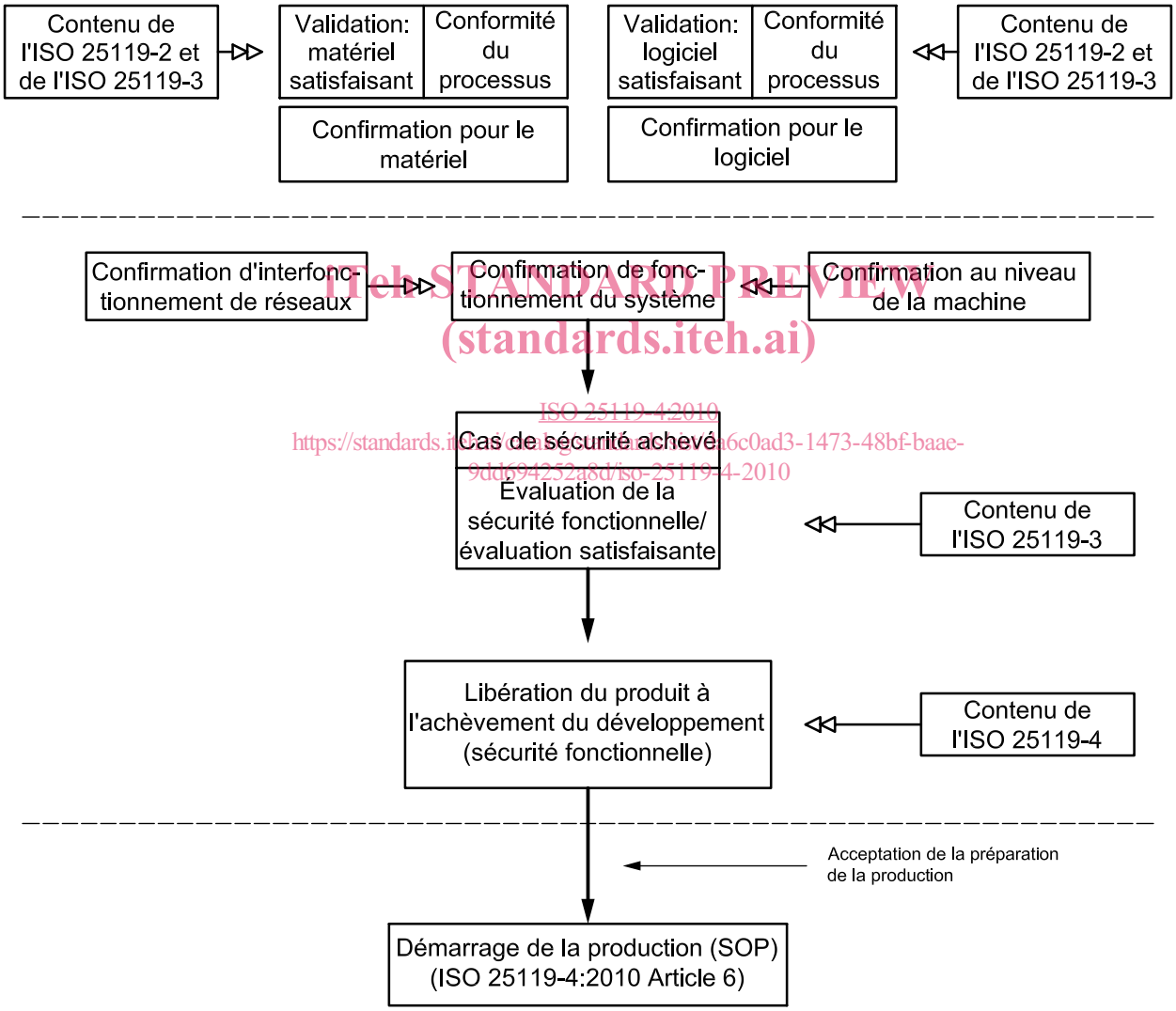

Figure 1 — Hiérarchie d'approbation