NORME INTERNATIONALE

ISO 19014-1

Première édition
2018-06

Version corrigée
2019-02

Engins de terrassement — Sécurité fonctionnelle —

Partie 1: Méthodologie pour la détermination des parties relatives à la sécurité des systèmes de commande et les exigences de performance

Earth-moving machinery — Functional safety —

Part 1: Methodology to determine safety-related parts of the control system and performance requirements

Numéro de référence
ISO 19014-1:2018(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 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. 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 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/foreword.html.

Le comité chargé de l'élaboration du présent document est l'ISO/TC 127, *Engins de terrassement*, sous-comité SC 2, *Sécurité, ergonomie et exigences de sécurité*.

Cette première édition de l'ISO 19014-1, avec l'ISO 19014-2, l'ISO 19014-3, l'ISO 19014-4 et l'ISO/TS 19014-5, annule et remplace l'ISO 15998 et l'ISO/TS 15998-2 qui ont fait l'objet d'une révision technique.

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

— la méthode pour la détermination des niveaux de performance et l'analyse de sécurité du système de commande de la machine,

— les exigences supplémentaires pour les machines mobiles,

— les exigences d'essai environnementaux pour les composants des systèmes de commande relatifs à la sécurité, et

— les exigences pour la validation du logiciel et la vérification des niveaux de performance de la machine.

La présente version corrigée de l'ISO 19014-1:2018 inclut les corrections suivantes:

— en 4.2 c) 2), 4.2 d) 1), 6.1 et l'Annexe C, les références croisées aux étapes définies en 4.2 ont été corrigées.

Une liste de toutes les parties de la série ISO 19014 peut être trouvée sur le site internet de l'ISO. Au moment de la publication du présent document, la Partie 2, *Conception et évaluation des systèmes de commande de la machine relatifs à la sécurité*, la Partie 4, *Conception et évaluation du logiciel et de la*

transmission pour les parties relatives à la sécurité du système de commande, et la Partie 5, *Tableaux de niveaux de performance*, sont en cours d'élaboration.

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

Le présent document traite des systèmes de tout type d'énergie utilisés pour assurer la sécurité fonctionnelle des engins de terrassement.

Dans le domaine de la sécurité des machines, les normes sont articulées de la façon suivante.

Les normes de type A (normes fondamentales de sécurité), contiennent des notions fondamentales, des principes de conception et des aspects généraux relatifs aux machines;

Les normes de type B (normes génériques de sécurité), traitent d'un aspect de la sécurité ou d'un moyen de protection valable pour une large gamme de machines:

— normes de type B1, traitant d'aspects particuliers de la sécurité (par exemple distances de sécurité, température superficielle, bruit);

— normes de type B2, traitant de moyens de protection (par exemple commandes bimanuelles, dispositifs de verrouillage, dispositifs sensibles à la pression, protecteurs);

Les normes de type C (normes de sécurité par catégorie de machines), traitent 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 C, comme indiqué dans l'ISO 12100.

Le contenu du 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);

— organismes de santé et de sécurité (autorités réglementaires, organismes de prévention des risques professionnels, surveillance du marché, etc.)

D'autres groupes peuvent être concernés par le niveau de sécurité des machines atteint à l'aide du document par les parties prenantes mentionnées 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);

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

Les machines concernées et l'étendue des phénomènes dangereux, situations dangereuses ou événements dangereux couverts sont indiquées dans le Domaine d'application du présent document.

Lorsque des exigences de la présente norme de type C sont différentes de celles énoncées dans les normes de type A ou les normes de type B, les exigences de la présente norme de type C ont priorité sur celles des autres normes pour les machines ayant été conçues et fabriquées conformément aux exigences de la présente norme de type C.

Engins de terrassement — Sécurité fonctionnelle —

Partie 1: Méthodologie pour la détermination des parties relatives à la sécurité des systèmes de commande et les exigences de performance

1 Domaine d'application

Le présent document fournit une méthode pour la détermination des niveaux de performance requis pour les engins de terrassement (EMM), comme définit dans l'ISO 6165.

Une analyse de sécurité des systèmes de commande de la machine (MCSSA) détermine le degré de réduction des phénomènes dangereux associés aux systèmes de commande requis pour les systèmes de commande de sécurité (SCS). Cette réduction est quantifiée par le niveau de performance de la machine (MPL), les phénomènes dangereux sont identifiés selon les principes d'évaluation des risques définis dans la norme ISO 12100 ou par d'autres moyens.

NOTE 1 La deuxième étape, comme présenté dans l'Annexe A, démontre la relation entre l'ISO 12100 et l'ISO 19014 en tant que mesure complémentaire.

NOTE 2 L'ISO 19014 peut également être utilisée pour évaluer les exigences de sécurité fonctionnelle d'autres machines mobiles non routières.

Pour ce qui est des commandes déterminées comme étant relatives à la sécurité, les caractéristiques d'exigences et de performances environnementales de l'architecture, du matériel et du logiciel sont couvertes dans d'autres parties de l'ISO 19014.

L'ISO 19014 couvre les phénomènes dangereux dus au disfonctionnement fonctionnel d'un système de commande lié à la sécurité, et exclut les phénomènes dangereux dus à l'équipement lui-même (par exemple, choc électrique, incendie, etc.).

Les autres commandes qui ne sont pas des systèmes de commande de sécurité (SCS), qui n'atténuent pas un phénomène dangereux ni ne réalisent une fonction de commande, et les cas où les défaillances pourraient être constatées par l'opérateur, sont exclus de la présente norme (par exemple, les essuie-glaces, les phares, l'éclairage de cabine, etc.).

NOTE 3 Une liste de fonctions de sécurité est incluse dans l'Annexe D.

NOTE 4 Les avertisseurs sonores sont exclus des exigences de la couverture de diagnostic.

2 Références normatives

Les documents suivants, en tout ou partie, sont référencés de façon normative dans le présent document et sont indispensables à son application. 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 6165, *Engins de terrassement — Principaux types — Identification et termes et définitions*

ISO 12100:2010, *Sécurité des machines — Principes généraux de conception — Appréciation du risque et réduction du risque*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO 6165 et l'ISO 12100 ainsi que les suivants s'appliquent.

L'ISO et l'IEC maintiennent des bases de données terminologiques pour utilisation dans le domaine de la normalisation aux adresses suivantes:

— IEC Electropedia: disponible à l'adresse http://www.electropedia.org/

— ISO Online browsing platform: disponible à l'adresse http://www.iso.org/obp

3.1
niveau de performance de machine
MPL
niveau discret d'aptitude de *parties relatives à la sécurité des systèmes de commande* (3.3.2) à réaliser une fonction de sécurité dans des conditions raisonnablement prévisibles

Note 1 à l'article: Le terme MPL est utilisé pour désigner le niveau de performance requis d'une partie du système de commande relative à la sécurité. «M» fait référence à la machine et désigne les engins de terrassement couverts par le domaine d'application du présent document, et est utilisé pour faire la distinction avec les autres normes de sécurité fonctionnelle (par exemple PL, AgPL, ASIL, etc.).

3.1.1
niveau de performance de machine requis
MPL_r
niveau discret requis tel que déterminé par des processus dans le présent document

3.1.2
niveau de performance de machine obtenu
MPL_a
niveau discret obtenu par les *systèmes de commande de sécurité* (3.3.1)

Note 1 à l'article: Le processus pour la détermination du MPL_a sera couvert dans l'ISO 19014-2 et l'ISO 19014-4 qui sont en cours d'élaboration.

3.2
sécurité fonctionnelle
partie de la sécurité globale relative à l'équipement commandé et à son système de commande qui dépend du fonctionnement correct des systèmes de commande liés à la sécurité (SCS) et autres mesures de réduction des risques

[SOURCE: IEC 61508-4:2010, 3.1.12 modifié]

3.3
système de commande de la machine
MCS
système qui répond aux signaux d'entrée de parties de machines, des *opérateurs* (3.4.1), des équipements de commande externes ou de toute combinaison de ceux-ci et qui génère des signaux de sorties imposant à la machine un comportement attendu

[SOURCE: ISO 13849-1:2015, 3.1.32]

3.3.1
système de commande de sécurité
SCS
sous-système ou système utilisé par un *MCS* (3.3) pour assurer la *sécurité fonctionnelle* (3.2) en influençant le comportement de la machine ou en atténuant un phénomène dangereux

Note 1 à l'article: Un système pouvant être sujet à une défaillance qui génère un phénomène dangereux est considéré comme un SCS.

Note 2 à l'article: Par exemple, les SCS pour la propulsion peuvent inclure la manette des gaz, le réducteur, le démarrage/arrêt, etc.

3.3.2
partie d'un système de commande relative à la sécurité
SRP/CS
partie d'un *SCS* (3.3.1) qui répond à des signaux d'entrée et génère des signaux de sortie relatifs à la sécurité

Note 1 à l'article: Les parties combinées d'un système de commande relatives à la sécurité commencent au point où sont générés les signaux relatifs à la sécurité (y compris, par exemple, la came de commande et le galet de l'interrupteur de position) et se terminent à la sortie des pré-actionneurs (y compris, par exemple, les contacts principaux du contacteur).

Note 2 à l'article: Si des systèmes de surveillance sont utilisés pour la couverture du diagnostic, ceux-ci sont considérés comme des SRP/CS.

Note 3 à l'article: Une SRP/CS est une pièce ou un composant dans un MCS spécifique.

[SOURCE: ISO 13849-1:2015, 3.1.1 modifié – La Note 3 à l'article a été ajoutée.]

3.4
groupe de personnes
groupes de personnes analysés dans la *MCSSA* (3.14)

3.4.1
opérateur
personne faisant fonctionner l'engin de terrassement et conscient des phénomènes dangereux associés

3.4.2
collaborateur
personne travaillant à proximité de la machine et conscient des phénomènes dangereux associés

3.4.3
tiers
personne, y compris celles ne faisant pas partie du personnel, les enfants ou les membres du public n'ayant que peu ou pas de connaissance des phénomènes dangereux liés à la machine et aucune formation

3.4.4
technicien de maintenance
personne dont la fonction est d'effectuer les tâches de maintenance sur la machine

Note 1 à l'article: Un technicien de maintenance a reçu une formation et connaît bien la machine.

3.5
contrôlabilité
capacité d'éviter un dommage au *groupe de personnes* (3.4) exposées à un risque grâce aux réactions rapides de l'opérateur, éventuellement avec l'aide d'autres commandes

3.6
exposition
pourcentage de temps durant lequel un *groupe de personnes* (3.4) est exposé au phénomène dangereux

Note 1 à l'article: L'exposition est le produit des probabilités dépendantes suivantes; *cas d'utilisation d'application* (3.11), *durée du phénomène dangereux* (3.12), et *exposition d'un groupe de personnes* (3.15).

3.7
gravité
estimation de l'étendue du dommage à un ou plusieurs individus qui peut se produire dans une situation potentiellement dangereuse

[SOURCE: ISO 26262-1:2011, 1.120]

3.8
indicateur
moyen par lequel l'état de l'équipement ou de la machine est représenté à un observateur

[SOURCE: ISO 22555:2007, 3.2]

3.8.1
indicateur d'avertissement
indications visuelles, sensorielles ou sonores lorsqu'une action est requise de l'*opérateur* (3.4.1) ou du système de commande

3.8.2
indicateur d'avertissement d'action immédiate
indicateur d'avertissement (3.8.1) nécessitant une action immédiate de l'*opérateur* (3.4.1) afin d'atténuer les phénomènes dangereux ou les défaillances du système

3.9
application
différents secteurs industriels au sein desquels une machine est utilisée, dont les situations dangereuses peuvent différer de l'un à l'autre

Note 1 à l'article: Les applications peuvent comprendre la construction générale, la construction de route, la gestion des déchets, l'exploitation de carrière, etc.

3.10
cas d'utilisation
utilisation prévue d'une machine dans le cadre d'une *application* (3.9)

Note 1 à l'article: Par exemple, un bouteur peut être utilisé pour sa lame, pour le délignage, les déplacements et la maintenance dans le cadre d'une application.

3.11
cas d'utilisation dans une application
plus grande proportion de temps pendant laquelle il est prévu d'utiliser une machine dans un *cas d'utilisation* (3.10) pour une *application* (3.9) donnée au cours de l'utilisation normale du cycle de vie de la machine

Note 1 à l'article: Étant donné que le cas d'utilisation dans une application représente la plus grande proportion de temps passé et non la moyenne, une machine dans la population passe pour un cas d'utilisation, la somme des cas d'utilisation sur l'ensemble d'une application ce qui peut être supérieur à 100 %.

3.12
période de phénomène dangereux
pourcentage de temps dans le cycle de travail d'utilisation dans une application pendant laquelle il est raisonnablement prévisible qu'un phénomène dangereux puisse exister si le système de commande évalué est sujet à une défaillance

Note 1 à l'article: Par exemple, un bouteur qui pousse de la matière du haut d'un mur élevé n'est exposé au risque de tomber du haut du mur que pendant le temps où la machine se déplace vers le mur élevé dans les limites de la distance d'arrêt de la machine.

3.13
zone dangereuse
tout espace, à l'intérieur ou autour d'une machine, dans lequel une personne peut être exposée à un phénomène dangereux provenant du *SCS* (3.3.1) analysé

[SOURCE: ISO 12100:2010, 3.11 modifié – «provenant du *SCS* (3.3.1) analysé» a été ajouté]

3.14
analyse de sécurité des systèmes de commande de la machine
MCSSA
appréciation du risque permettant de déterminer le *MPLr* (3.1.1) requis pour le *SCS* (3.3.1) sur une machine, comme indiqué dans le présent document

3.15
exposition d'un groupe de personnes
plus grand pourcentage de la *période de phénomène dangereux* (3.12) pendant laquelle un membre du *groupe de personnes* (3.4) évalué est présent dans la *zone dangereuse* (3.13)

Note 1 à l'article: Cette analyse porte sur la somme de toutes les personnes exposées du groupe de personnes, pas sur un seul individu dans ce groupe, c'est-à-dire pas sur une seule voiture passant à proximité, mais sur la circulation.

3.16
type de défaillance
description du type de défaillance pouvant se produire dans un *SCS* (3.3.1)

Note 1 à l'article: Les types de défaillance à considérer comprennent la non-application, le non-desserrage, l'application non commandée, le desserrage non commandé, la vitesse d'application incorrecte, la vitesse de desserrage incorrecte ou une direction incorrecte, etc.

3.17
pire plausible
estimation de la *gravité* (3.7) des plus graves dommages pouvant survenir de façon réaliste à la suite d'un seul événement dangereux

Note 1 à l'article: Le pire plausible n'est pas toujours le pire concevable ou le plus probable, mais il est fondé sur la prise en compte de l'historique des incidents et du résultat potentiel d'un événement dangereux.

4 Méthode de détermination du MPLr pour SRP/CS des engins de terrassement

4.1 Généralités

La sécurité fonctionnelle est assurée par un ou plusieurs SCS qui sont basés sur un grand nombre de technologies (par exemple, mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). Toute stratégie de sécurité doit prendre en compte tous les éléments au sein d'un SCS, comme les capteurs, dispositifs de commande et actionneurs.

Les parties des SCS qui assurent des fonctions de sécurité sont appelées parties des systèmes de commande relatives à la sécurité (SRP/CS). Ces parties peuvent être constituées de matériels ou de logiciels, elles peuvent être des parties isolées du système de commande ou en faire partie intégrante, et le système de commande doit être inclus dans le processus de MCSSA.

L'objectif est de réduire le risque lié à un phénomène dangereux donné (ou à une situation dangereuse) durant l'utilisation normale ou un mauvais usage raisonnablement prévisible de la machine. Cela doit 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'examen des risques liés aux fonctions de sécurité est axé sur l'origine des blessures subies par les personnes. Si, dans l'analyse des dommages potentiels, il peut être établi que les dommages sont clairement limités aux biens et n'impliquent pas de blessures aux personnes, cela n'exigerait pas qu'un MCS soit classé comme un SCS. De plus, il incombe à l'utilisateur (propriétaire) d'effectuer une évaluation des risques sur le lieu de travail et ces évaluations ne font pas partie du processus de la MCSSA.

4.2 Méthode d'analyse de sécurité du Système de Commande de la Machine (MCSSA)

a) Identifier tous les MCS ou toutes les fonctions de la machine à évaluer.