Norme internationale

ISO 19014-2

Deuxième édition
2026-10

Engins de terrassement — Sécurité fonctionnelle —

Partie 2: Conception et évaluation des exigences de matériel et d'architecture pour les parties du système de commande relatives à la sécurité

Earth-moving machinery — Functional safety —

Part 2: Design and evaluation of hardware and architecture requirements for safety-related parts of the control system

Sample Document
get full document from standards.iteh.ai

Numéro de référence
ISO 19014-2:2026(fr)

© ISO 2026

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026

Sample Document

get full document from standards.iteh.ai



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2026

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
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026

Sommaire

Page

Avant-propos ..... **iv**
Introduction ..... **v**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **2**
4 Symboles et abréviations **3**
5 Exigences générales **4**
5.1 Application 4
5.2 Système de commande de sécurité (SCS) existant 5
5.3 Prescriptions de sécurité et mesures de prévention ou de réduction du risque 5
6 Conception du système **5**
6.1 Présentation 5
6.2 Exigences générales 5
6.3 Conception du matériel 6
7 Évaluation des performances de sécurité du système **7**
7.1 Niveau de performance de machine obtenu (MPL_a) 7
7.2 Évaluation de la sécurité du matériel 8
7.2.1 Généralités 8
7.2.2 Prise en compte des défauts 8
7.2.3 Exclusion de défauts 8
7.2.4 Temps moyen avant une défaillance dangereuse ($MTTF_d$) 9
7.3 Couverture de diagnostic (DC) 9
7.3.1 Couverture de diagnostic (DC) du système de commande électronique de sécurité (ESCS) 9
7.3.2 Couverture de diagnostic (DC) du système de commande non électronique de sécurité (N/ESCS) 9
7.4 Exigences pour MPL_a = d pour les systèmes de direction et de freinage hydrauliques 9
7.4.1 Généralités 9
7.5 Classifications par catégories 10
7.5.1 Généralités 10
7.5.2 Catégorie B/Catégorie 1 13
7.5.3 Catégorie 2 15
7.5.4 Fonctions de sécurité en conflit 15
7.5.5 Considérations relatives aux SRP/CS des systèmes opérationnels après défaillance 15
7.6 Combinaison de SCS pour obtenir un MPL_a global 16
8 Informations pour l'utilisation et la maintenance **17**
8.1 Généralités 17
8.2 Manuel de l'opérateur 17
Annexe A (informative) **Exemples de systèmes et d'évaluations** **18**
Annexe B (normative) **Compatibilité avec d'autres normes de sécurité fonctionnelle** **34**
Annexe C (informative) **Évaluation de la fonction de sécurité** **35**
Annexe D (normative) **Exceptions, exclusions, ajouts à l'ISO 13849-1:2023 et l'ISO 13849-2:2012** **37**
Bibliographie **40**

Sample Document
Generated document from standards.iteh.ai

© ISO 2026 – Tous droits réservés

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026

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'ISO attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de propriété revendiqué à cet égard. À la date de publication du présent document, l'ISO n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié tout ou partie de tels droits de propriété.

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.

Sample Document

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 www.iso.org/avant-propos.

get full document from standards.iteh.ai

Le présent document a été élaboré par le comité ISO/TC 127, *Engins de terrassement,* sous-comité SC 2, *Sécurité, ergonomie et exigences générales,* en collaboration avec le comité technique CEN/TC 151, *Machines de génie civil et de production de matériaux de construction — Sécurité*, du Comité européen de normalisation (CEN), conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette deuxième édition annule et remplace la première édition (ISO 19014-2:2022), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— correction de l'erreur de niveau de performance de machine (MPL) dans l'Annexe C

— correction des erreurs typographiques à la Figure C.1;

— suppression de la catégorie 2M;

— suppression de la robustesse du système hydraulique (HSR);

— suppression de l'Annexe B;

— ajout d'exigences relatives au MPL_a = d dans la Catégorie 1.

Une liste de toutes les parties de la série ISO 19014 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.

© ISO 2026 – Tous droits réservés

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026

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:

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

— normes de type B (normes génériques de sécurité), traitant d'un ou de plusieurs aspects de la sécurité ou d'un ou de plusieurs types de moyens de protection qui peuvent être utilisés pour une large gamme de machines:

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

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

— 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 C telle que définie dans l'ISO 12100:2010.

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:

— fabricants de machines et de composants (petites, moyennes et grandes entreprises);

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

Sample Document
Get full document from standards.iteh.ai

D'autres partenaires peuvent être concernés par le niveau de sécurité des machines atteint à l'aide du document:

— utilisateurs de machines et employeurs (petites, moyennes et grandes entreprises);

— utilisateurs de machines et employés (par exemple, syndicats, organisations pour les personnes ayant des besoins spéciaux);

— prestataires de services, par exemple, pour la maintenance (petites, moyennes et grandes entreprises);

— consommateurs (dans le cas de machines destinées à l'utilisation par les consommateurs).

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, situations ou événements dangereux couverts sont indiquées dans le domaine d'application du présent document.

Lorsque les prescriptions de la présente norme de type C diffèrent de celles spécifiées dans les normes de type A ou B, les exigences de la présente norme de type C prévalent sur celles des autres normes pour les machines qui ont été conçues et construites conformément aux exigences de la présente norme de type C.

© ISO 2026 – Tous droits réservés

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026

Sample Document

get full document from standards.iteh.ai

Engins de terrassement — Sécurité fonctionnelle —

Partie 2:
Conception et évaluation des exigences de matériel et d'architecture pour les parties du système de commande relatives à la sécurité

1 Domaine d'application

Le présent document spécifie les principes généraux d'élaboration et d'évaluation du niveau de performance de machine obtenu (MPL_a) des systèmes de commande de sécurité (SCS) utilisant des composants alimentés par toutes les sources d'énergie (par exemple, électrique, hydraulique, mécanique) utilisées dans les engins de terrassement et leur équipement, comme défini dans l'ISO 6165:2022.

Les principes du présent document s'appliquent aux systèmes de commande de la machine (MCS) qui commandent le mouvement d'une machine ou atténuent un phénomène dangereux; ces systèmes sont évalués pour vérifier que les exigences de niveau de performance de machine requis (MPL_r) sont conformes à l'ISO 19014-1:2026[1)] ou à l'ISO 19014-5:2026.[2)].

NOTE 1 Les exigences relatives à l'application de la sécurité fonctionnelle tout au long du cycle de vie du développement logiciel sont traitées dans l'ISO 19014-4:2026.[3)]

Sample Document

Afin de couvrir l'ensemble des exigences de sécurité pertinentes pour les produits entrant dans son domaine d'application, le présent document est utilisé conjointement avec l'ISO 19014-1:2026, l'ISO 19014-3:2026, l'ISO 19014-4:2026 et l'ISO 19014-5:2026.

Preview document from standards.iteh.ai

Le présent document exclut les systèmes suivants:

— systèmes de perception de l'environnement n'ayant aucun impact sur le mouvement de la machine (par exemple, caméras et détecteurs radar);

— systèmes de lutte contre l'incendie, excepté si l'activation du système interfère ou active un autre SCS.

Le présent document ne s'applique pas aux autres systèmes ou composants pour lesquels des défaillances pourraient être constatées par l'opérateur (par exemple, les essuie-glaces, les phares, l'éclairage de la cabine) ou ceux qui servent essentiellement à protéger la propriété.

NOTE 2 Les avertisseurs sonores sont exclus des exigences de la couverture de diagnostic.

De plus, le présent document traite des phénomènes dangereux significatifs tels que définis dans l'ISO 12100:2010 atténués par les composants matériels dans le SCS.

Le présent document n'est pas applicable aux engins de terrassement fabriqués avant la date de sa publication.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils 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 2026 – Tous droits réservés

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026

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

ISO 13849-1:2023, *Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux de conception*

ISO 13849-2:2012, *Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 2: Validation*

ISO 19014-1:2026, *Engins de terrassement — Sécurité fonctionnelle — Partie 1: Méthodologie pour la détermination des parties du système de commande relatives à la sécurité et les exigences de performance*

ISO 19014-3:2026, *Engins de terrassement — Sécurité fonctionnelle — Partie 3: Exigences pour la performance environnementale et l'essai des composants électroniques et électriques utilisés dans les parties du système de commande relatives à la sécurité*

ISO 19014-4:2026, *Engins de terrassement — Sécurité fonctionnelle — Partie 4: Conception et évaluation du logiciel et de la transmission des données pour les parties du système de commande relatives à la sécurité*

ISO 19014-5:2026, *Engins de terrassement — Sécurité fonctionnelle — Partie 5: Tableau des niveaux de performance*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO 12100:2010, l'ISO 13849-1:2023 et l'ISO 19014-1:2026 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

Sample Document

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

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

get full document from standards.iteh.ai

3.1
système de commande électronique de sécurité
ESCS
système de commande de sécurité constitué de composants électroniques, du dispositif d'entrée au dispositif de sortie

3.2
fonction
réponse définie d'un ou de plusieurs systèmes de commande de la machine (MCS)

Note 1 à l'article: Une unité de commande (par exemple, unité de commande électronique) peut exécuter plusieurs fonctions. Lorsque plusieurs fonctions de sécurité sont contenues dans une unité de commande, chaque fonction de sécurité et le circuit associé sont analysés de façon séparée.

3.3
système de commande non électronique de sécurité
N/ESCS
système de commande de sécurité constitué de composants non électroniques, du dispositif d'entrée au dispositif de sortie

© ISO 2026 – Tous droits réservés

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026

3.4
état de sécurité
état dans lequel l'équipement, le processus ou le système commandé est automatiquement ou manuellement arrêté ou basculé dans un mode permettant d'empêcher un comportement inattendu ou le dégagement potentiellement dangereux d'énergie accumulée à la suite d'un défaut du système de contrôle-commande de l'engin

Note 1 à l'article: Un état de sécurité peut inclure également le maintien de la *fonction* (3.2) du système de commande de sécurité (par exemple, la direction) en cas de défaut unique, selon le type de danger devant être réduit.

[SOURCE: ISO 3450:2011, 3.15, modifié — «dysfonctionnement» a été remplacé par «défaut», «fonctionnement» a été remplacé par «comportement» et la Note 1 à l'article a été ajoutée.]

3.5
composant éprouvé
composant pour utilisation relative à la sécurité qui a été largement utilisé dans le passé avec des résultats satisfaisants pour les mêmes utilisations ou des utilisations similaires, ou qui a été fabriqué et vérifié en utilisant les principes qui démontrent qu'il est adapté et fiable pour les utilisations relatives à la sécurité

3.6
tolérance aux anomalies du matériel
HFT
aptitude d'un sous-système à la perte potentielle de la fonction de sécurité en cas de N+1 anomalies au moins

Note 1 à l'article: Une tolérance aux anomalies du matériel (HFT) de N signifie que N+1 anomalies d'un sous-système peuvent provoquer la perte de la fonction de sécurité.

[SOURCE: IEC 62061:2021, 3.2.35, modifié — «(HFT)» ajouté dans la Note 1 à l'article]

Sample Document

3.7
système opérationnel après défaillance
système capable de fonctionner après une défaillance

get full document from standards.iteh.ai

3.8
analyse d'impact
documentation qui rend compte de la compréhension et des implications d'un changement proposé

3.9
fonction de sécurité conflictuelle
fonction de sécurité dans laquelle un type de défaillance conduit à un état de sécurité qui entre en conflit avec l'état de sécurité d'un autre type de défaillance relevant de la même fonction de sécurité

EXEMPLE L'état de sécurité en cas de défaillance du freinage consiste à arrêter la machine, mais l'état de sécurité en cas d'actionnement non commandé du frein consiste à desserrer le frein.

4 Symboles et abréviations

Pour les besoins du présent document, les symboles et abréviations suivants s'appliquent.

a, b, c, d, e	échelons des niveaux de performance de machine
ASIC	circuit intégré spécifique à l'application
B, 1, 2, 3, 4	dénomination des catégories
CCF	défaillance de cause commune
DC	couverture de diagnostic
DC_{moy}	couverture de diagnostic moyenne

© ISO 2026 – Tous droits réservés

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026

ECU	unité de commande électronique
ESCS	système de commande électronique de sécurité
AMDE	analyse des modes de défaillance et de leurs effets
AMDED	analyse des modes de défaillance, de leurs effets et de leurs diagnostics
FPGA	circuit logique programmable
HFT	tolérance aux anomalies du matériel
I-L-O	Entrée-logique-sortie
MCS	système de commande de la machine
MPL	niveau de performance de machine
MPL_a	niveau de performance de machine obtenu
MPL_r	niveau de performance de machine requis
MTTF	temps moyen avant défaillance
$MTTF_d$	temps moyen avant une défaillance dangereuse
N/ESCS	système de commande non électronique de sécurité
OTE	sortie de l'équipement d'essai
A/P	ajout parallèle
PL	niveau de performance
SCS	système de commande de sécurité
SRP/CS	partie d'un système de commande relative à la sécurité
TE	équipement d'essai

Sample Document
get full document from standards.iteh.ai

5 Exigences générales

5.1 Application

La série ISO 19014 doit être utilisée conjointement avec la série ISO 13849 lorsqu'elle s'applique aux engins de terrassement. Lorsque des exigences spécifiques sont données dans le présent document, celles-ci l'emportent sur celles de la série ISO 13849; cependant, lorsqu'aucune exigence spécifique n'est donnée dans le présent document, la série ISO 13849 doit s'appliquer, en utilisant PL à la place de MPL (par exemple, MPL = b est analogue à PL = b). Pour un résumé des articles applicables dans la série ISO 13849 ou le présent document, voir Tableaux D.1 et D.2 à l'Annexe D.

Les principes du présent document doivent être appliqués aux MCS considérés comme des SCS dans l'ISO 19014-1:2026. Si une fonction interagit avec une autre fonction de sécurité et change la réponse de cette autre fonction de sécurité, le niveau de performance le plus élevé de ces fonctions de sécurité pour un même type de défaillance doit être utilisé.

Les logiciels liés à la sécurité dans tous les composants du SCS doivent répondre aux exigences de l'ISO 19014-4:2026.

© ISO 2026 – Tous droits réservés

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026

5.2 Système de commande de sécurité (SCS) existant

Lorsqu'un SCS existant a été élaboré conformément à une norme précédente et qu'il a été démontré à travers l'utilisation et la validation de l'application qu'il réduisait la probabilité d'un phénomène dangereux au niveau le plus bas pouvant raisonnablement être atteint, la mise à jour de la documentation du cycle de vie n'est pas requise. Lorsque le SCS utilisé précédemment est modifié, une analyse d'impact des modifications doit être effectuée et un plan d'action doit être élaboré et mis en œuvre pour vérifier que les exigences de sécurité sont satisfaites.

5.3 Prescriptions de sécurité et mesures de prévention ou de réduction du risque

Les machines doivent être conformes aux exigences de sécurité, aux mesures de prévention et de réduction du risque, ou à ces deux types de dispositions du présent article. De plus, la machine doit être conçue selon les principes de l'ISO 12100:2010 pour les phénomènes dangereux pertinents mais non significatifs qui ne sont pas traités dans le présent document.

6 Conception du système

6.1 Présentation

De nombreuses fonctions de sécurité des machines mobiles ne sont pas équipées de sorties de marche et arrêt comme pour les fonctions de sécurité des machines non mobiles et ces sorties ne sont pas toujours ajoutées sur une machine uniquement pour atténuer les phénomènes dangereux. Par exemple, les commandes de direction, de freins de service, d'orientation et des accessoires peuvent avoir des sorties modulées ou variables dans certaines limites. Même si ce type de systèmes peut s'intégrer dans les architectures de la série ISO 13849, une considération clé pour les concepteurs est la différence entre les fonctions de sécurité d'une machine mobile et d'une machine non mobile.

Sample Document

D'autres considérations incluent:

a) Le système requiert-t-il une commande en boucle fermée ou en boucle ouverte pour traiter les taux d'applications incorrects?

Sample document from standards.iteh.ai

b) Existe-t-il des phénomènes dangereux associés à une activation non commandée ainsi que les défaillances sur demande?

Une fonction de sécurité qui repose sur un système de commande visant à fournir l'atténuation des phénomènes dangereux nécessaire pour la machine peut être mise en œuvre par un SCS dans le cadre du présent document. Un SCS peut contenir une ou plusieurs SRP/CS, et plusieurs SCS peuvent partager une ou plusieurs SRP/CS (par exemple, une unité logique, des pré-actionneurs). Une SRP/CS peut aussi mettre en œuvre à la fois des fonctions de sécurité et des fonctions non liées à la sécurité.

Certains systèmes sur les machines mobiles sont requis pour maintenir un état de fonctionnement même en cas de défaillance. Même si l'ISO 13849-1:2023 le permet, des mesures supplémentaires sont nécessaires pour s'assurer que cela puisse se produire en toute sécurité et que les canaux parallèles ne sont pas en conflit les uns avec les autres et que les systèmes fonctionnent conformément aux exigences de l'architecture déclarée.

L'Annexe B définit les exigences minimales devant être respectées pour utiliser des systèmes, sous-systèmes et SRP/CS développés et évalués par des méthodes autres que celles de la série ISO 19014.

6.2 Exigences générales

Une fois les fonctions de sécurité du SCS identifiées, les exigences correspondant à chaque SCS doivent être documentées. Pendant le cycle de vie de sécurité, les exigences de sécurité sont détaillées et spécifiées de manière plus approfondie selon des niveaux hiérarchiques. Toutes les exigences de sécurité doivent être écrites de manière à ne pas présenter d'ambiguïtés, à être cohérentes avec les autres exigences et à pouvoir être mises en œuvre.

© ISO 2026 – Tous droits réservés

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026

Les aspects de conception suivants doivent être pris en compte:

— les signaux d'entrée ou de sortie contradictoires;

— la perte de signaux et d'énergie d'actionnement pour l'un ou l'autre système (par exemple, alimentation en huile séparée pour chaque canal, alimentation redondante pour les ECU);

— les états de sécurité conflictuels requis par les multiples types de défaillance traités par le système;

— les systèmes qui exigent un concept de fonctionnement opérationnel après défaillance;

— les processus d'évaluation sont indépendants du processus de conception;

— lorsque les SCS sont conçus pour être utilisés de manière synchronisée (par exemple, dans le cadre de l'automatisation d'une tâche), le système de commande doit être conçu de manière à pouvoir atténuer les phénomènes dangereux dus à un manque de synchronisation.

Voir la norme ISO 13849-1: 2023, 5.2.1.3, pour une liste exhaustive des spécifications des exigences de sécurité (SRS); toutefois, les exemples 3, 4 et 5, point j), ainsi que la dernière phrase de ce paragraphe ne s'appliquent pas.

NOTE Un exemple de cette synchronisation pour un engin de terrassement est une flèche, un bras et un godet d'une pelle hydraulique qui sont commandés simultanément par un système de commande de nivellement.

6.3 Conception du matériel

La structure du matériel des SCS peut fournir des mesures (par exemple, redondance, diversité et surveillance) permettant d'éviter, de détecter ou de tolérer les défauts. Les mesures pratiques peuvent inclure la redondance, la diversité et la surveillance.

Sample Document

Le processus de développement matériel doit se conformer à l'ISO 13849-1:2023, tel que mentionné à l'Annexe D du présent document. Tout processus éprouvé organisé qui satisfait aux exigences de la série ISO 19014 peut être utilisé pour compléter le processus de conception.

get full document from standards.iteh.ai

Il convient que le concepteur commence au niveau du système où les fonctions de sécurité et les exigences associées sont identifiées. Le système peut être décomposé en sous-systèmes pour faciliter le développement. Le cas échéant, chaque phase du cycle de développement doit être vérifiée.

La Figure 1 décrit le processus de développement matériel en forme de modèle en V, qui commence par «Conception du système liée à la sécurité (MCS Design)». Sur le côté droit du modèle en V, les flèches horizontales indiquent les exigences par rapport auxquelles le matériel est testé.

© ISO 2026 – Tous droits réservés

ISO 19014-2:2026 • https://standards.iteh.ai/catalog/standards/iso/2ba48efd-a0cb-45cd-ae75-5b6dfd66498b/iso-19014-2-2026