NORME INTERNATIONALE

ISO 19014-2

Première édition
2022-06

Engins de terrassement — Sécurité fonctionnelle —

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

Earth-moving machinery — Functional safety —

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

Numéro de référence
ISO 19014-2:2022(F)

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

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.html.

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

Cette première édition, avec l'ISO 19014-1, l'ISO 19014-3, ISO 19014-4 et ISO 19014-5, annule et remplace les premières éditions (ISO 15998:2008 et l'ISO/TS 15998-2:2012) qui ont fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— élimination de procédures alternatives ECE R79, Annexe 6, et IEC 62061;

— application de l'ISO 13849-1 aux Engins de terrassement mobiles, y compris l'analyse de systèmes de commande non électroniques utilisés dans les applications d'Engins de terrassement.

Une liste de toutes les parties de la série ISO 19014 est disponible sur le site Internet 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 complète de ces organismes peut être consultée à l'adresse www.iso.org/fr/members.html.

Introduction

Le présent document traite des systèmes comprenant toutes les technologies utilisées 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 aspect(s) de la sécurité ou d'un ou de plusieurs type(s) de moyens de protection qui peuvent être utilisés 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).

— 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.

Le présent document est pertinent, en particulier, pour les groupes de parties prenantes suivants représentant les acteurs du marché à l'égard de 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 peuvent être affectés par le niveau de sécurité des machines obtenu au moyen du document par les groupes de parties prenantes mentionnées ci-dessus:

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

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

— prestataires de services, par exemple, sociétés de 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 au processus d'élaboration du présent document.

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

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

Le présent document est l'adaptation de l'ISO 13849 visant à fournir une norme de type C destinée à une application spécifique de sécurité fonctionnelle des engins de terrassement.

Le présent document doit être utilisé conjointement avec la série ISO 13849 lorsqu'elle s'applique aux engins de terrassement (EMM) et remplace l'ISO 15998.

Le présent document complète les activités du cycle de vie de sécurité des systèmes de commande de sécurité conformes à l'ISO 13849-1:2015 et à l'ISO 13849-2:2012 qui traitent des engins de terrassement comme défini dans l'ISO 6165.

Engins de terrassement — Sécurité fonctionnelle —

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

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, électronique, électrique, hydraulique, mécanique) utilisées dans les engins de terrassement et leur équipement, comme défini dans l'ISO 6165.

Les principes du présent document s'appliquent aux systèmes de commande d'engins (MCS) qui commandent le mouvement d'un engin ou atténuent un phénomène dangereux; ces systèmes sont évalués pour vérifier que les exigences de niveau de performance des engins (MPL_r) sont conformes à l'ISO 19014-1 ou à l'ISO/TS 19014-5.

Les systèmes suivants sont exclus du domaine d'application du présent document:

— systèmes de connaissance n'ayant aucun impact sur le mouvement de l'engin (par exemple, caméras et détecteurs radar);

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

Les autres systèmes ou composants pour lesquels les défaillances pourraient être constatées par l'opérateur (par exemple, les essuie-glaces, les phares, l'éclairage de la cabine, etc.) ou ceux qui servent essentiellement à protéger la propriété sont exclus du présent document. 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 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 12100, *Sécurité des machines — Principes généraux de conception — Appréciation du risque et réduction du risque*

ISO 13849-1:2015, *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, *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*

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

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

ISO/TS 19014-5, *Engins de terrassement — Sécurité fonctionnelle — Partie 5: Tableaux des niveaux de performance*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO 12100, l'ISO 13849-1, l'ISO 19014-1, 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:

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

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

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

3.2
fonction
comportement défini d'un ou de plusieurs MCS

Note 1 à l'article: Une unité de commande (par exemple, unité de commande électronique) peut exécuter plusieurs d'une fonction. 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
N/ESCS
système de commande non-électronique de sécurité
système de commande de sécurité constitué de composants non-électroniques du dispositif d'entrée au dispositif de sortie

3.4
état de sécurité
condition telle que, après une défaillance du système de commande de sécurité, le processus ou le système de l'équipement commandé est automatiquement ou manuellement arrêté ou désactivé de manière à empêcher tout comportement intempestif ou la libération d'énergie accumulée potentiellement dangereuse

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

[SOURCE: ISO 3450:2011, 3.15, modifiée – "dysfonctionnement" a été remplacé par "défaut"; "performance" a été remplacée par "comportement"; Note 1 à l'article a été ajouté.]

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, et 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

4 Symboles et termes abrégés

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

a, b, c, d, e	niveaux de performance requis des machines
ASIC	circuit intégré spécifique à l'application
B, 1, 2, 3, 4	dénomination des catégories
CCF	défaillance de cause commune
DC	couverture du diagnostic
DCavg	couverture du diagnostic moyenne
ECU	unité de commande électronique
EMM	engin de terrassement
ESCS	système de commande électronique de sécurité
FMEA	analyse des modes de défaillance et de leurs effets
FMEDA	analyse des modes de défaillance, de leurs effets et de leurs diagnostics
FPGA	circuit logique programmable
HFT	tolérance à la défaillance du matériel
HSR	robustesse du système hydraulique
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
SCS	système de commande de sécurité
SRP/CS	partie d'un système de commande relative à la sécurité
TE	équipement d'essai

5 Exigences générales

5.1 Application

La série ISO 19014 doit être utilisée conjointement avec l'ISO 13849 lorsqu'elle s'applique aux engins de terrassement (EMM) et remplace l'ISO 15998. 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 E.1 et E.2 dans l'Annexe E.

Les principes du présent document doivent être appliqués aux MCS considérés comme SCS dans l'ISO 19014-1 ou l'ISO/TS 19014-5. Les autres systèmes de commande de machine qui perturbent ou inhibent une fonction de sécurité du système de commande de sécurité doivent se voir attribuer le même niveau de performance de machine que le système qu'ils perturbent ou inhibent.

Les machines doivent être conformes aux exigences de sécurité et/ou aux mesures de prévention/réduction des risques du présent article. De plus, les machines doivent être conçues 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. Les logiciels liés à la sécurité dans tous les composants du SCS doivent répondre aux exigences de la norme ISO 19014-4:2020.

5.2 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, il n'est pas nécessaire de mettre à jour la documentation du cycle de vie. Lorsque le SCS utilisé précédemment est modifié, une analyse d'impact (voir ISO 19014-4:2020, 3.28) 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.

6 Conception du système

6.1 Présentation

De nombreuses fonctions de sécurité des machines mobiles ne sont pas équipées de sorties marche/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 l'ISO 13849, les concepteurs doivent tenir compte de la manière dont les caractéristiques des fonctions de sécurité peuvent différer sur une machine mobile (par exemple, le système a-t-il besoin d'une commande en boucle fermée ou en boucle ouverte pour traiter les taux d'applications incorrectes, le système doit-il traiter les phénomènes dangereux associés à une activation non commandée ainsi que les pannes sur demande, etc.).

Une fonction de sécurité qui repose sur un système de commande visant à fournir l'atténuation des phénomènes dangereux nécessaire pour l'engin peut être mise en œuvre par un SCS dans le cadre de du présent document. Un SCS peut contenir un ou plusieurs SRP/CS, et plusieurs SCS peuvent partager un 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 de non sécurité.

NOTE Pour les indicateurs d'avertissement d'action immédiate, voir l'ISO 19014-1:2018, Annexe B.

Certains systèmes sur les machines mobiles doivent maintenir un état de fonctionnement même en cas de panne. Même si l'ISO 13849-1:2015 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 C définit les exigences minimales à respecter 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.

Les aspects de conception suivants doivent être pris en compte:

— signaux d'entrée ou de sortie contradictoires;

— 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 UCE);

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

— les systèmes qui exigent un concept de fonctionnement à sécurité intégrée;

— 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.

NOTE Un exemple EMM de cette synchronisation est une flèche, un bras et un godet d'une pelle hydraulique qui doivent être 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 défaillances. Les mesures pratiques peuvent inclure la redondance, la diversité et la surveillance.

Le processus de développement matériel doit suivre l'ISO 13849-1:2015, tel que mentionné à l'Annexe E. Il convient que le concepteur commencer 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. Tout processus éprouvé organisé qui satisfait aux exigences de l'ISO 19014 peut être utilisé pour compléter le processus de conception.

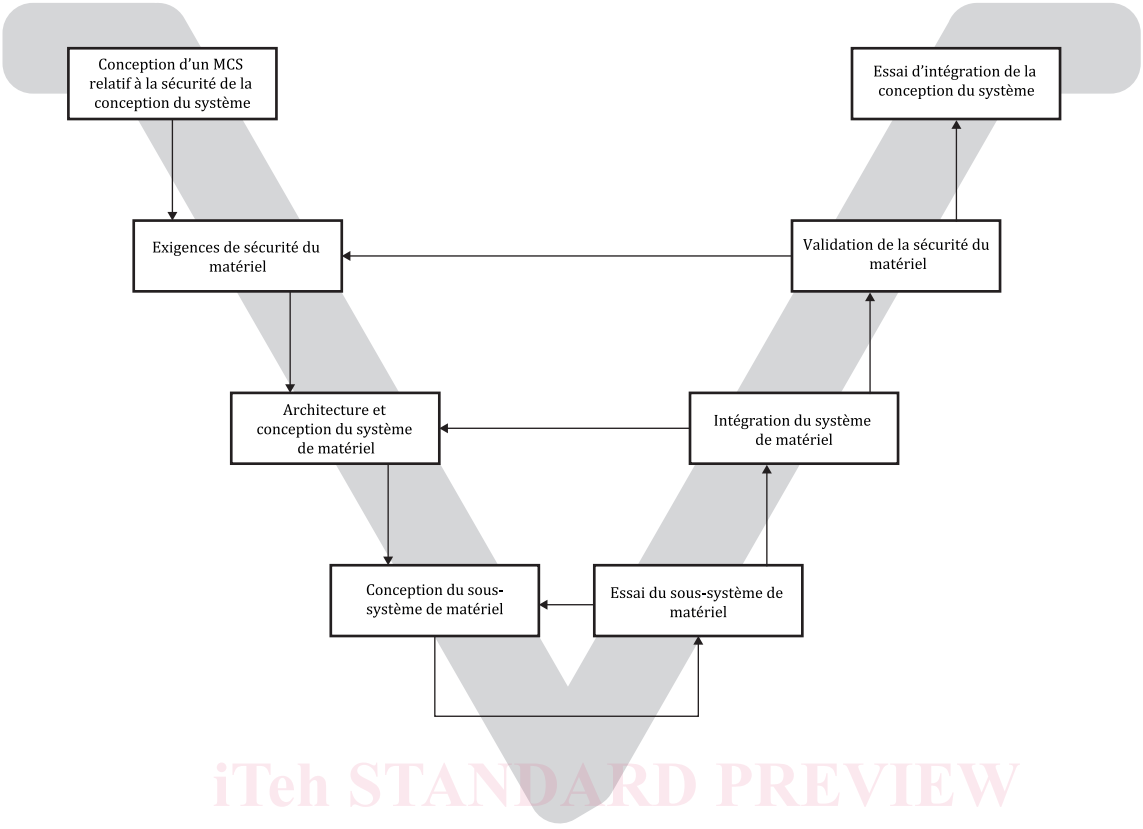

Figure 1 — Développement matériel — Modèle en V

7 Évaluation des performances de sécurité du système

7.1 Niveau de performance de machine obtenu (MPL_a)

L'intégrité obtenue des parties relatives à la sécurité à réaliser une fonction de sécurité est exprimée via la détermination du MPL_a.

L'aptitude à réaliser une fonction de sécurité dans les conditions environnementales escomptées comme le prévoit l'ISO 19014-3, doit être démontrée et documentée.

La procédure d'évaluation de MPL_a est la suivante:

a) identifier l'environnement de fonctionnement du composant et le niveau de contrainte;

b) choisir les composants;

c) identifier et documenter les exclusions de défaillances (7.2) ou utiliser l'analyse du système appropriée (par exemple, AMDE, analyse par arbre de défaillances, etc.);

d) calculer le $MTTF_d$ (voir ISO 13849-1:2015, Annexe D), et vérifier que le $MTTF_d$ satisfait aux niveaux requis (voir ISO 13849-1:2015);

e) déterminer si le matériel peut fournir le niveau de DC requis (ISO 13849-1:2015, Annexe E). Pour les systèmes reposant sur une interaction logicielle pour déterminer une couverture de diagnostic, cette analyse vise à déterminer uniquement si le matériel est en mesure de supporter la DC et non pas à vérifier que les exigences de DC du système sont satisfaites;

f) si nécessaire, prendre en compte la CCF (voir ISO 13849-1:2015, Annexe F);

g) prendre en compte la défaillance systématique (ISO 13849-1:2015, Annexe G);

h) prendre en compte une éventuelle interaction avec d'autres fonctions de sécurité;

i) pour une conception de FPGA et d'ASIC, voir IEC 61508-2:2010, Annexes E ou F.

Voir l'Annexe D pour des informations supplémentaires concernant l'évaluation de la fonction de sécurité.

7.2 Évaluation de la sécurité du matériel

7.2.1 Généralités

L'ISO 13849-2:2012, Annexes A à D énumère les défauts, les exclusions de défauts, et les défaillances pour plusieurs types de composants. Ces listes ne sont pas exhaustives. Si nécessaire, d'autres défauts, exclusions de défauts, et défaillances doivent être pris en compte et être énumérés; dans de tels cas, il convient également d'élaborer clairement la méthode d'évaluation.

Une analyse des modes de défaillance et de leurs effets (AMDE), une analyse de l'arbre des défaillances, ou une analyse du système équivalente, doit être réalisée pour établir les défaillances et les exclusions de défaillances.

7.2.2 Prise en compte des défaillances

En général, les critères de défaillance suivants peuvent être pris en compte:

— si, en conséquence d'une défaillance, des composants supplémentaires sont défectueux, la première défaillance et toutes les suivantes sont considérées comme constituant une défaillance unique;

— deux défaillances ou plus ayant une cause commune doivent être considérées comme constituant une seule défaillance (désignée défaillance de cause commune);

— l'occurrence simultanée de deux défaillances ou plus ayant pour origine des causes séparées est considérée comme étant hautement improbable et n'est donc pas prise en compte.

7.2.3 Exclusion de défaillances

Les exclusions de défaillances sont utilisées dans le développement matériel comme moyen d'atténuer les mécanismes de défaillance entraînant des phénomènes dangereux connus conformément aux meilleures pratiques de l'industrie. Une exclusion de défaillance constitue un compromis entre des exigences techniques de sécurité et la possibilité théorique de l'occurrence de la défaillance.

L'exclusion de défaillances peut reposer sur les critères suivants:

— l'improbabilité technique de l'occurrence de certaines défaillances;

— l'expérience technique généralement admise qui peut s'appliquer indépendamment de l'application considérée; et

— des exigences techniques relatives à l'application et au phénomène dangereux spécifique.

La documentation technique doit justifier de manière détaillée toutes les défaillances exclues.

Les exclusions de défaillances peuvent s'appliquer à travers la hiérarchie suivante:

1. Sur la base de chaque défaillance examinée l'une après l'autre - une fois toutes les défaillances identifiées, certaines d'entre elles peuvent être exclues sur la base des critères ci-dessus; les autres défaillances peuvent être gérées par diagnostic au sein du système de commande.

2. Au niveau du composant - si toutes les défaillances de SCS connues peuvent être exclues au niveau du composant, l'exclusion de la défaillance peut s'appliquer à la totalité du composant.

3. Au niveau du système – si toutes les défaillances dans tous les composants ont été traitées par exclusions de défaillances, une analyse des systèmes hydrauliques peut être réalisée en utilisant le processus HSR dans 7.4. Des systèmes purement mécaniques peuvent être exclus de défaillances au niveau du système si des composants sont conçus selon un coefficient de sécurité approprié et que des exigences de maintenance pour conserver la fonctionnalité correcte du système sont incluses dans la littérature de service selon l'Article 8.

7.2.4 Temps moyen avant défaillance dangereuse ($MTTF_d$)

Le processus de détermination du $MTTF_d$ est mentionné dans l'ISO 13849-1:2015, 4.5.2. Tandis que l'ISO 13849-1 recommande l'hypothèse de principe de 50 % de défaillance dangereuse (par exemple, $B_{10d} = 2 \times B_{10}$), des taux de défaillance inférieurs peuvent être utilisés s'ils sont pris en charge par des analyses (par exemple, données empiriques, AMDE).

7.3 Couverture de diagnostic (DC)

7.3.1 DC de l'ESCS

Voir l'ISO 13849-1:2015, 4.5.3

7.3.2 DC de N/ESCS

La DC des systèmes non-électriques est déterminée de la, ou des façon(s) suivante(s).

1.) En sélectionnant le type analogue le plus applicable de la note de couverture de diagnostic dans l'ISO 13849-1:2015, Annexe E. Par exemple, une vanne sélecteur de circuit qui compare les pressions d'huile et exécute une action sur la base de ces pressions est comparable à une surveillance continue. Dans ce cas, une note de 99 % peut lui être attribuée.

2.) Calcul du pourcentage de la DC via une AMDE.

3.) L'exclusion de défaillances peut être appliquée à toutes les défaillances ou seulement à certaines d'entre elles. Si elle devait s'appliquer uniquement à certaines défaillances, il faudrait alors calculer la DC appropriée.

4.) Le couplage mécanique direct de composants peut être considéré comme constituant une DC de 99 %.

7.4 Mesures de réduction de défaillances au niveau système des systèmes hydrauliques basées sur la robustesse du système hydraulique (HSR)

7.4.1 Généralités

L'évaluation du MPL_a de systèmes de freinage et de direction hydrauliques exige une évaluation des défauts des composants dans le canal principal. En raison des caractéristiques des composants hydrauliques et de leur application aux engins de terrassement, ces défauts ne peuvent pas être traités par des techniques de détection de défauts utilisées dans les systèmes électroniques. L'évaluation de la note de robustesse du système hydraulique (HSR) est déterminée en utilisant les critères du Tableau 1. Cette évaluation repose sur la robustesse de la conception du système hydraulique dans les applications de sécurité sur les engins de terrassement. Les critères du Tableau 1 reposent sur les principes de sécurité de base, sur les critères d'exclusion de défaillances et sur les principes de sécurité éprouvés (par exemple, contenus dans l'ISO 13849-2:2012, ainsi qu'au travers des meilleures pratiques établies en matière de conception, de développement et de fabrication des SCS hydrauliques).

NOTE Ces critères peuvent également être appliqués aux systèmes hydrauliques non utilisés dans les applications de freinage et de direction, mais étant donné que ces systèmes sont généralement de catégorie 1, l'utilisation du Tableau 2 pour calculer une valeur DC ne serait pas nécessaire pour l'analyse d'un système de catégorie 1.

7.4.2 Calcul de la note de la HSR

La note de la HSR est définie en pourcentage à l'aide de la formule ci-dessous:

$$r = \frac{t}{100 - q} \times 100$$

où

r est la robustesse du système hydraulique (HSR);

q est la somme des critères qui ne réduit pas la probabilité de la défaillance dangereuse pour la fonction de sécurité prévue que la fonction de sécurité atténue;

t est la somme des critères applicables restants satisfaits par le système.

Tout critère que le système ne satisfait pas ne doit pas être inclus dans q. (Par exemple, une source d'énergie secondaire ne serait pas un critère applicable à un système de ressort à desserrage hydraulique lorsque l'état de sécurité du système est engagé).

Chaque SRP/CS du système hydraulique en cours d'évaluation doit satisfaire aux exigences des critères donnés pour obtenir une note. Les notes partielles ne sont pas autorisées (par exemple, s'il y a trois distributeurs et que seulement deux d'entre eux répondent aux exigences d'un critère donné, la note serait de zéro pour ce critère).

Les systèmes hydrauliques doivent respecter les exigences de l'ISO 13849-2:2012, C.1 et C.2. L'exclusion de défaillances peut être appliquée au niveau d'un composant si toutes les défaillances applicables peuvent être exclues selon l'ISO 13849-2:2012, Annexe C.

Tableau 1 — Critères de notation de la robustesse d'un système hydraulique

Réf.	Critères	Note
A	Surdimensionnement (par exemple, jeu suffisant, rectitude et cylindricité des distributeurs)	10
B	Contre-mesures de l'adhérence ou de la rotation du tiroir de la valve	10
C	Contre-mesures relatives aux entrées hydrauliques prohibitives (par exemple, pression élevée instantanée sur les deux orifices du moteur hydraulique)	10
D	Source secondaire d'énergie (par exemple, accumulateur piloté) ou conception à sécurité intégrée en cas de perte de la source d'énergie principale	20
E	Défaillance lente ou progressant pas à pas (par exemple, réduction de la force d'assistance de direction avant défaillance importante)	10
F	Atténuation de l'éclatement du flexible (par exemple, cheminement pour éviter un perçage du tuyau en raison de présence de particules/d'abrasion)	10
G	Système conçu pour conserver la propreté nécessaire du fluide hydraulique	10
H	Contre-mesures relatives à la cavitation due à une aération dans le fluide hydraulique ou à sa viscosité	10
I	Contre-mesures relatives aux problèmes de transfert de pression dus à une aération dans le fluide hydraulique ou à sa viscosité (par exemple, circuit de ventilation)	10
	Note totale	

Le Tableau 2 définit la DC à laquelle une note donnée de la HSR est corrélée, et un MPL_a peut être déterminé en utilisant cette valeur DC, une catégorie d'architecture du système, un $MTTF_d$ et une CCF adaptés de l'ISO 13849-1:2015 Tableau 6. Voir Tableau 3 pour une explication de la Catégorie 2M