NORME INTERNATIONALE

ISO 13849-1

Quatrième édition
2023-04

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité —

Partie 1: Principes généraux de conception

Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design

Numéro de référence
ISO 13849-1:2023(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 ..... **vi**
Introduction ..... **viii**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes, définitions, symboles et abréviations **2**
3.1 Termes et définitions 2
3.2 Symboles et abréviations 11
4 Présentation **13**
4.1 Processus d'appréciation et de réduction du risque de la machine 13
4.2 Contribution à la réduction du risque 14
4.3 Processus de conception d'une SRP/CS 15
4.4 Méthodologie 17
4.5 Informations requises 17
4.6 Réalisation de la fonction de sécurité en utilisant les sous-systèmes 18
5 Spécification des fonctions de sécurité **18**
5.1 Identification et description générale de la fonction de sécurité 18
5.2 Spécification des exigences de sécurité 19
5.2.1 Exigences générales 19
5.2.2 Exigences relatives aux fonctions de sécurité spécifiques 22
5.2.3 Réduction le plus possible de l'incitation à neutraliser les fonctions de sécurité 26
5.2.4 Accès à distance 27
5.3 Détermination du niveau de performance requis (PL_r) pour chaque fonction de sécurité 27
5.4 Examen de la spécification des exigences de sécurité (SRS) 28
5.5 Décomposition de la SRP/CS en sous-systèmes 28
6 Considérations relatives à la conception **30**
6.1 Évaluation du niveau de performance atteint 30
6.1.1 Présentation générale du niveau de performance 30
6.1.2 Corrélation entre le niveau de performance (PL) et le niveau d'intégrité de sécurité (SIL) 31
6.1.3 Architecture — Catégories et leur relation aux $MTTF_D$ de chaque canal, couverture du diagnostic moyenne et défaillance de cause commune (CCF) 32
6.1.4 Temps moyen avant défaillance dangereuse ($MTTF_D$) 39
6.1.5 Couverture du diagnostic (DC) 41
6.1.6 Défaillances de cause commune (CCF) 41
6.1.7 Défaillances systématiques 42
6.1.8 Procédures simplifiées pour estimer le niveau de performance de sous-systèmes 42
6.1.9 Autre procédure pour déterminer le niveau de performance et la PFH sans $MTTF_D$ 44
6.1.10 Prise en compte et exclusion des défauts 46
6.1.11 Composant éprouvé 47
6.2 Combinaison des sous-systèmes pour atteindre un niveau de performance global de la fonction de sécurité 47
6.2.1 Généralités 47
6.2.2 Valeurs PFH connues 48
6.2.3 Valeurs PFH inconnues 48
6.3 Paramétrage manuel lié au logiciel 49
6.3.1 Généralités 49
6.3.2 Influences sur les paramètres relatifs à la sécurité 49
6.3.3 Exigences relatives au paramétrage manuel lié au logiciel 50

6.3.4 Vérification de l'outil de paramétrage ... 51
6.3.5 Documentation de paramétrage manuel lié au logiciel ... 51

7 Exigences concernant les logiciels ... 52
7.1 Généralités ... 52
7.2 Langage de variabilité limitée (LVL) et langage de variabilité totale (FVL) ... 53
7.2.1 Langage de variabilité limitée (LVL) ... 53
7.2.2 Langage de variabilité totale (FVL) ... 54
7.2.3 Décision pour le langage de variabilité limitée (LVL) ou le langage de variabilité totale (FVL) ... 54
7.3 Logiciel intégré relatif à la sécurité (SRESW) ... 56
7.3.1 Conception du logiciel intégré relatif à la sécurité (SRESW) ... 56
7.3.2 Autres procédures pour le logiciel intégré non accessible ... 57
7.4 Logiciel applicatif relatif à la sécurité (SRASW) ... 57

8 Vérification du niveau de performance atteint ... 60

9 Aspects ergonomiques de la conception ... 61

10 Validation ... 61
10.1 Principes de validation ... 61
10.1.1 Généralités ... 61
10.1.2 Plan de validation ... 63
10.1.3 Listes des défauts génériques ... 64
10.1.4 Listes des défauts spécifiques ... 64
10.1.5 Informations pour la validation ... 64
10.2 Validation de la spécification des exigences de sécurité (SRS) ... 65
10.3 Validation par analyse ... 66
10.3.1 Généralités ... 66
10.3.2 Techniques d'analyse ... 66
10.4 Validation par essais ... 67
10.4.1 Généralités ... 67
10.4.2 Exactitude des mesures ... 67
10.4.3 Exigences supplémentaires relatives aux essais ... 68
10.4.4 Nombre d'échantillons ... 68
10.4.5 Méthodes d'essai ... 68
10.5 Validation des fonctions de sécurité ... 69
10.6 Validation de l'intégrité de sécurité de la SRP/CS ... 69
10.6.1 Validation du (des) sous-système(s) ... 69
10.6.2 Validation des mesures prises contre les défaillances systématiques ... 71
10.6.3 Validation du logiciel relatif à la sécurité ... 71
10.6.4 Validation de la combinaison des sous-systèmes ... 72
10.6.5 Validation globale de l'intégrité de sécurité ... 72
10.7 Validation des exigences d'environnement ... 73
10.8 Rapport de validation ... 73
10.9 Validation des exigences de maintenance ... 73

11 Maintenabilité des SRP/CS ... 74

12 Documentation technique ... 74

13 Informations pour l'utilisation ... 75
13.1 Généralités ... 75
13.2 Informations relatives à l'intégration de SRP/CS ... 75
13.3 Informations destinées à l'utilisateur ... 76

Annexe A (informative) **Lignes directrices pour la détermination du niveau de performance requis (PL_r) ... 78**

Annexe B (informative) **Méthode bloc et diagramme bloc relatif à la sécurité ... 83**

Annexe C (informative) **Calcul ou évaluation des valeurs $MTTF_D$ pour des composants uniques ... 85**

Annexe D (informative) **Méthode simplifiée pour estimer le $MTTF_D$ pour chaque canal** **94**

Annexe E (informative) **Estimations pour la couverture du diagnostic (DC) des fonctions et des sous-systèmes** **96**

Annexe F (informative) **Méthode de quantification des mesures contre les défaillances de cause commune (CCF)** **100**

Annexe G (informative) **Défaillance systématique** **104**

Annexe H (informative) **Exemple d'une combinaison de plusieurs sous-systèmes** **108**

Annexe I (informative) **Exemples de procédure simplifiée pour estimer le PL de sous-systèmes** **111**

Annexe J (informative) **Exemple d'élaboration de SRESW** **120**

Annexe K (informative) **Représentation numérique de la Figure 12** **125**

Annexe L (informative) **Immunité aux interférences éléctromagnétiques (IEM)** **130**

Annexe M (informative) **Informations supplémentaires pour la spécification des exigences de sécurité (SRS)** **134**

Annexe N (informative) **Évitement des défaillances systématiques lors de la conception logicielle** **137**

Annexe O (informative) **Valeurs relatives à la sécurité de composants ou de parties de systèmes de commande** **158**

Bibliographie **161**

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/avant-propos.html.

Le présent document a été élaboré par le Comité technique ISO/TC 199, *Sécurité des machines*, en collaboration avec le Comité technique CEN/TC 114 du Comité européen de normalisation (CEN), *Sécurité des machines*, conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette quatrième édition annule et remplace la troisième édition (ISO 13849-1:2015), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— l'ensemble du document a été réorganisé pour mieux suivre le processus de conception et de développement des systèmes de commande;

— nouvel Article 4 sur une recommandation d'appréciation du risque;

— spécification des fonctions de sécurité (Article 5 mis à jour);

— combinaison de plusieurs sous-systèmes (Article 6 mis à jour);

— nouvel Article 7 sur les exigences de sécurité logicielle;

— nouvel Article 9 sur les aspects ergonomiques de la conception;

— validation (Article 8 mis à jour et transfert à l'Article 10);

— nouveau G.5 sur la gestion de la sécurité fonctionnelle;

— nouvelle Annexe L sur l'immunité aux interférences électromagnétiques (IEM);

— nouvelle Annexe M contenant des informations complémentaires sur la spécification des exigences de sécurité;

— nouvelle Annexe N sur les mesures de prévention des pannes pour la conception de logiciels relatifs à la sécurité;

— nouvelle Annexe O avec valeurs relatives à la sécurité de composants ou de parties des systèmes de commande.

Une liste de toutes les parties de la série ISO 13849 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/members.html.

Introduction

La structure des normes de sécurité dans le domaine des machines est la suivante:

a) Normes de type A (normes fondamentales de sécurité), précisant des notions fondamentales, des principes de conception et des aspects généraux relatifs aux machines.

b) 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 protection qui peut ou peuvent être utilisé(s) pour une large gamme de machines:

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

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

c) normes de type C (normes de sécurité des machines), traitant des exigences de sécurité détaillées pour une machine particulière ou un groupe de machines.

Le présent document est une norme de type B1 tel que défini dans l'ISO 12100:2010.

La première édition du présent document a été publiée en 1999 sur la base de l'EN 954-1:1996 (norme annulée). La deuxième édition a été révisée en 2006, et la troisième édition a été révisée en 2015.

Le présent document est pertinent, en particulier, pour les groupes de parties prenantes suivants, dans le domaine 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).

D'autres personnes peuvent être concernées par le niveau de sécurité des machines obtenu au moyen du présent document:

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

— utilisateurs de machines/salariés (par exemple, syndicats);

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

— consommateurs (c'est-à-dire, dans le cas de machines destinées à être utilisées par des consommateurs).

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

De plus, le présent document est destiné aux organismes de normalisation élaborant des normes de type C, telles que définies dans l'ISO 12100:2010.

Les exigences du présent document peuvent être complétées ou modifiées par une norme de type C.

Pour les machines couvertes par le domaine d'application d'une norme de type C et qui ont été conçues et construites suivant les exigences de cette norme, les exigences de ladite norme de type C sont prioritaires.

NOTE 1 Les exemples et la base de la majeure partie du contenu reposent sur des machines fixes servant à des applications industrielles. Cependant, d'autres machines ne sont pas exclues. Le présent document a été rédigé sans tenir compte des exigences particulières de certaines machines (par exemple, machines mobiles). Cependant, le présent document est destiné à être utilisé dans de nombreuses industries de machines et comme base pour les développeurs de normes de type C, dans la mesure du possible.

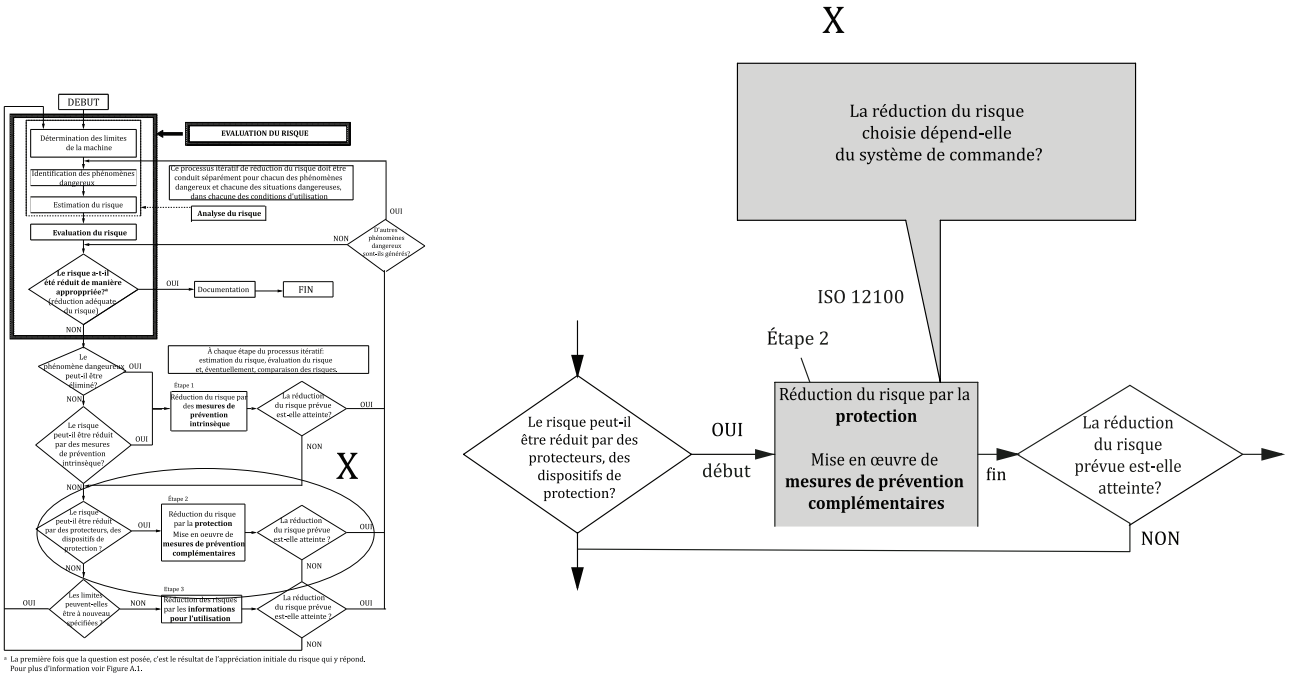
Le présent document est destiné à donner des conseils au cours de la conception et de l'évaluation des systèmes de commande ainsi qu'au cours de l'élaboration des normes de type B2 ou de type C.

La réduction du risque selon l'ISO 12100:2010, Article 6, s'effectue en appliquant, dans la séquence suivante, les mesures de prévention intrinsèque, les mesures de sauvegarde et/ou de réduction du risque complémentaires et les informations pour l'utilisation. Un concepteur peut réduire les risques au moyen de mesures de réduction du risque qui peuvent avoir des fonctions de sécurité. Les parties des systèmes de commande de machine qui sont assignées pour fournir des fonctions de sécurité sont appelées parties des systèmes de commande relatives à la sécurité (SRP/CS). Celles-ci peuvent être constituées de matériel ou d'une combinaison de matériel et de logiciel et peuvent être séparées du système de commande de la machine ou en faire partie intégrante. En plus de fournir des fonctions de sécurité, les SRP/CS peuvent également mettre en œuvre des fonctions opérationnelles.

L'ISO 12100:2010 est utilisée pour l'appréciation du risque de la machine. L'Annexe A du présent document peut être utilisée pour la détermination du niveau de performance requis (PL_r) d'une fonction de sécurité réalisée par la SRP/CS, lorsque son PL_r n'est pas spécifié dans la norme de type C applicable. Le présent document concerne les fonctions de sécurité SRP/CS qui sont utilisées pour remédier aux risques dans les cas où une appréciation du risque conduite selon l'ISO 12100:2010 détermine qu'une mesure de réduction du risque s'appuyant sur une fonction de sécurité (par exemple, protecteur avec dispositif de verrouillage) est nécessaire. Dans ces cas, le système de commande relatif à la sécurité réalise une fonction de sécurité. Le présent document est destiné à être utilisé pour concevoir et évaluer la SRP/CS. Seule la partie du système de commande relative à la sécurité relève du présent document.

La Figure 1 illustre la relation entre l'ISO 12100:2010 et le présent document. Pour un aperçu détaillé, voir Figure 2.

NOTE 2 Voir également l'ISO/TR 22100-2:2013 pour plus d'informations.



NOTE Basé sur l'ISO/TR 22100-2:2013, Figure 2.

Figure 1 — Intégration du présent document (ISO 13849-1) dans le processus de réduction du risque de l'ISO 12100:2010

NOTE 3 La Figure 1 présente la manière dont les SRP/CS contribuent au processus de réduction du risque de l'ISO 12100:2010: Étape 2. La SRP/CS supporte les mesures de réduction du risque combinées par la mise en œuvre de fonctions de sécurité. L'aptitude des parties des systèmes de commande relatives à la sécurité à exécuter une fonction de sécurité dans des conditions prévisibles est classée en cinq niveaux, appelés niveaux de performance (PL). Le niveau de performance requis (PL_r) pour une fonction de sécurité particulière (en fonction de la réduction du risque requise) sera déterminé par une estimation du risque.

L'Annexe A informative du présent document contient une méthode d'estimation du risque et peut être utilisée pour la détermination du PL_r d'une fonction de sécurité exécutée par la SRP/CS. Toute méthode d'estimation du risque montrera une variance du fait de la nature subjective des critères d'évaluation. Comparé à l'Annexe A, les normes de type C peuvent présenter des méthodes d'estimation du risque plus spécifiques pour des applications spécifiques de la machine.

La fréquence de défaillance dangereuse des fonctions de sécurité dépend de plusieurs facteurs, y compris, mais sans y être limité, la structure matérielle et logicielle du système, l'étendue des mécanismes de détection des défauts [couverture du diagnostic (DC)], la fiabilité des composants [temps moyen avant défaillance dangereuse ($MTTF_D$), la défaillance de cause commune (CCF)], le processus de conception, la contrainte de fonctionnement, les conditions environnementales et les méthodes de fonctionnement.

Pour faciliter la conception des SRP/CS et l'évaluation du PL atteint, le présent document emploie une méthodologie basée sur la catégorisation d'architectures avec des critères de conception spécifiques (par exemple, $MTTF_D$, DC_{avg}) et un comportement spécifié dans des conditions de défaut. Ces architectures sont classées en cinq niveaux, appelés catégories B, 1, 2, 3 et 4.

La sécurité fonctionnelle tient compte des caractéristiques de défaillance d'éléments/de composants réalisant une fonction de sécurité. Pour chaque fonction de sécurité, cette caractéristique de défaillance s'exprime en fréquence de défaillance dangereuse par heure (PFH).

Les niveaux et catégories de performance peuvent être appliqués à la SRP/CS, par exemple:

— les unités de commande (par exemple, unité logique pour les fonctions de commande, traitement des données, surveillance continue);

— les dispositifs de protection électrosensibles (par exemple, barrières photoélectriques), dispositifs sensibles à la pression.

Les niveaux de performance peuvent être définis, et les catégories déterminées pour les sous-systèmes de SRP/CS en utilisant des parties de sécurité (composants), par exemple:

— les dispositifs de protection (par exemple, dispositifs de commande bimanuelle, dispositifs de verrouillage);

— les pré-actionneurs (par exemple, relais, vannes);

— les capteurs et éléments IHM (par exemple, capteurs de position, interrupteurs d'activation).

Les machines couvertes par le présent document vont des plus simples (par exemple, petits électroménagers de cuisine ou portes et portails automatiques) aux plus complexes (par exemple, machines d'emballage, machines d'impression, presses, et machines intégrées dans un système).

Le présent document et l'IEC 62061 spécifient tous deux une méthodologie, et fournissent des conseils portant sur la conception et la mise en œuvre des systèmes de commande relatifs à la sécurité des machines.

Les exigences de l'Article 10 du présent document remplacent les exigences de l'ISO 13849-2:2012 (à l'exception des annexes informatives).

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité —

Partie 1: Principes généraux de conception

1 Domaine d'application

Le présent document spécifie une méthodologie et fournit des exigences, des recommandations et des conseils portant sur la conception et l'intégration des parties des systèmes de commande relatives à la sécurité (SRP/CS) qui réalisent des fonctions de sécurité, incluant la conception de logiciels.

Le présent document s'applique aux SRP/CS pour les modes de fonctionnement à forte sollicitation et continu, incluant leurs sous-systèmes, indépendamment du type de technologie et d'énergie utilisé (par exemple, électrique, hydraulique, pneumatique et mécanique). Le présent document ne s'applique pas au mode de fonctionnement à faible sollicitation.

NOTE 1 Voir 3.1.44 et la série IEC 61508 pour le mode de fonctionnement à faible sollicitation.

Le présent document ne spécifie pas les fonctions de sécurité et les niveaux de performance requis (PL_r) qui doivent être utilisés dans un cas particulier.

NOTE 2 Le présent document spécifie une méthodologie pour la conception des SRP/CS sans tenir compte d'exigences spécifiques pour certaines machines (par exemple, machines mobiles). Ces exigences spécifiques peuvent être prises en compte dans une norme de type-C.

Le présent document ne donne pas d'exigences spécifiques pour la conception de produits/composants intégrés dans les SRP/CS. Les exigences spécifiques pour la conception de certains composants de SRP/CS sont couvertes par les normes ISO et IEC applicables.

Le présent document ne fournit pas de mesures spécifiques pour les aspects de sécurité (par exemple, physique, sécurité informatique (IT-security), cybersécurité).

NOTE 3 Les problèmes de sécurité peuvent avoir un effet sur les fonctions de sécurité. Voir l'ISO/TR 22100-4 et l'IEC/TR 63074 pour d'autres informations.

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

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

ISO 13855:2010, *Sécurité des machines — Positionnement des dispositifs de protection par rapport à la vitesse d'approche des parties du corps*

ISO 20607:2019, *Sécurité des machines — Notice d'instructions — Principes rédactionnels généraux*

IEC 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité — Partie 3: Exigences concernant les logiciels*

IEC 62046:2018, *Sécurité des machines — Application des équipements de protection à la détection de la présence de personnes*

IEC 62061:2021, *Sécurité des machines — Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité*

IEC/IEEE 82079-1:2019, *Élaboration des informations d'utilisation (instructions d'utilisation) des produits — Partie 1: Principes et exigences générales*

3 Termes, définitions, symboles et abréviations

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO 12100:2010, 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/

3.1.1
partie d'un système de commande relative à la sécurité
SRP/CS
partie d'un système de commande qui réalise une *fonction de sécurité* (3.1.27) répondant à un ou des signaux d'entrée et générant un ou des signaux de sortie relatifs à la sécurité

Note 1 à l'article: Les parties d'un système de commande relatives à la sécurité commencent au point où sont générés les signaux d'entrée 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 d'un contacteur).

3.1.2
système de commande de la machine
système qui répond aux signaux d'entrée de parties de machines, d'opérateurs, d'équipements de commande externes ou de toute combinaison de ceux-ci et qui génère des signaux de sortie imposant à la machine un comportement attendu

Note 1 à l'article: Le système de commande de la machine peut utiliser toute technologie ou combinaison de différentes technologies (par exemple, électrique/électronique, hydraulique, pneumatique et mécanique).

3.1.3
spécification des exigences de sécurité
SRS
spécification contenant les exigences relatives aux *fonctions de sécurité* (3.1.27) qui doivent être satisfaites par le système de commande relatif à la sécurité en termes de caractéristiques des fonctions de sécurité (exigences fonctionnelles) et de *niveaux de performance requis (PL_r)* (3.1.6)

[SOURCE: IEC 61508-4:2010, 3.5.11, modifié — Les informations de IEC 61508-4:2010, 3.5.12 ont été incluses.]

3.1.4
catégorie
classification du *sous-système* (3.1.45) liée à sa résistance aux *défauts* (3.1.8) et à son comportement consécutif à des défauts, qui est obtenue par l'architecture des parties, la détection des défauts et/ou leur fiabilité

3.1.5
niveau de performance
PL
niveau discret utilisé pour spécifier l'aptitude de *parties de systèmes de commande relatives à la sécurité (SRP/CS)* (3.1.1) à réaliser une *fonction de sécurité* (3.1.27) dans des conditions prévisibles

Note 1 à l'article: Voir 6.1 pour un aperçu général du niveau de performance.

3.1.6
niveau de performance requis
PL_r
niveau de performance (3.1.5) exigé pour atteindre la réduction du *risque* (3.1.19) requise pour chaque *fonction de sécurité* (3.1.27)

Note 1 à l'article: Voir 5.3 et Figure A.1 pour plus d'informations sur le niveau de performance requis (PL_r).

3.1.7
niveau d'intégrité de sécurité
SIL
niveau discret (parmi quatre possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité des *fonctions de sécurité* (3.1.27) à allouer aux systèmes relatifs à la sécurité, le niveau 4 d'intégrité de sécurité ayant le plus haut degré d'intégrité de sécurité et le niveau 1 le plus bas

Note 1 à l'article: Dans le présent document, seuls les SIL 1 à SIL 3 sont pris en compte.

[SOURCE: IEC 61508-4:2010, 3.5.8, modifié — «à allouer aux systèmes relatifs à la sécurité» a été ajouté à la définition, les NOTES ont été supprimées et une nouvelle Note 1 à l'article a été ajoutée.]

3.1.8
défaut
condition anormale qui peut entraîner une réduction ou une perte de la capacité d'une unité fonctionnelle à exécuter une fonction requise

Note 1 à l'article: Un défaut est souvent la conséquence d'une *défaillance* (3.1.10) de l'entité elle-même, mais il peut exister sans défaillance préalable.

Note 2 à l'article: Dans le présent document, «défaut» signifie un défaut aléatoire ou un défaut causé par une *défaillance systématique* (3.1.14).

[SOURCE: IEC 60050-192:2015, modifié — La Note 2 à l'article a été modifiée.]

3.1.9
exclusion de défauts
exclusion de certains *défauts* (3.1.8) dans une partie d'un système de commande relative à la sécurité (SRP/CS), si cette exclusion peut être justifiée par la probabilité négligeable de ces défauts

3.1.10
défaillance
cessation de l'aptitude d'un dispositif à accomplir une fonction requise

Note 1 à l'article: Après une défaillance, le dispositif présente un *défaut* (3.1.8).

Note 2 à l'article: Une «défaillance» est un passage d'un état à un autre, par opposition à un «défaut», qui est un état.

Note 3 à l'article: Les défaillances n'affectant que la disponibilité du processus commandé ne sont pas couvertes par le domaine d'application du présent document.

[SOURCE: IEC 60050-192:2015, modifié — La Note 3 à l'article a été modifiée.]