PROJET DE NORME INTERNATIONALE

ISO/DIS 13849-1

ISO/TC **199**	Secrétariat: **DIN**
Début de vote: **2020-06-08**	Vote clos le: **2020-08-31**

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

ICS: 13.110

Le présent document est distribué tel qu'il est parvenu du secrétariat du comité.

TRAITEMENT PARALLÈLE ISO/CEN

Numéro de référence
ISO/DIS 13849-1:2020(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Website: www.iso.org

Publié en Suisse

Sommaire

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 de 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.

Le présent document a été élaboré par le comité technique ISO/TC 199, *Sécurité des machines*.

La première édition de l'ISO 13849-1 a été publiée en 1999 basée sur l'EN 954-1:1996.

La deuxième édition de l'ISO 13849-1 a été révisée en 2006.

La troisième édition a été amendée et publiée en 2015.

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

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

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

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

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

c) Les 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.

La présente partie ISO 13849 est une norme de type-B-1 comme stipulé dans l'ISO 12100.

Le présent document concerne, en particulier, les groupes de parties prenantes suivants, représentant les acteurs du marché dans le domaine de la sécurité des machines:

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

— organismes d'hygiène et de sécurité (autorités réglementaires, organismes de prévention des accidents, surveillance du marché, etc.).

D'autres groupes peuvent être affectés par le niveau de sécurité des machines atteint avec les moyens du document par les groupes de parties prenantes susmentionnés:

— 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);

— consommateurs (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 au processus d'élaboration du présent document.

De plus, le présent document est destiné aux organismes de normalisation élaborant des normes de type C.

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

Lorsque des dispositions de la norme de type C diffèrent de celles indiquées dans une norme de type A ou B, ces dispositions prévalent sur celles des autres normes pour les machines conçues et fabriquées conformément aux spécifications de la norme de type C.

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 élaboré dans le but d'être utilisé dans la plupart des industries de machines et comme base pour les rédacteurs de normes de type C.

La présente partie de l'ISO 13849 est destinée à donner des conseils au cours de la conception et de l'évaluation des systèmes de commande ainsi qu'aux Comités Techniques élaborant des normes de type B2 ou de type C.

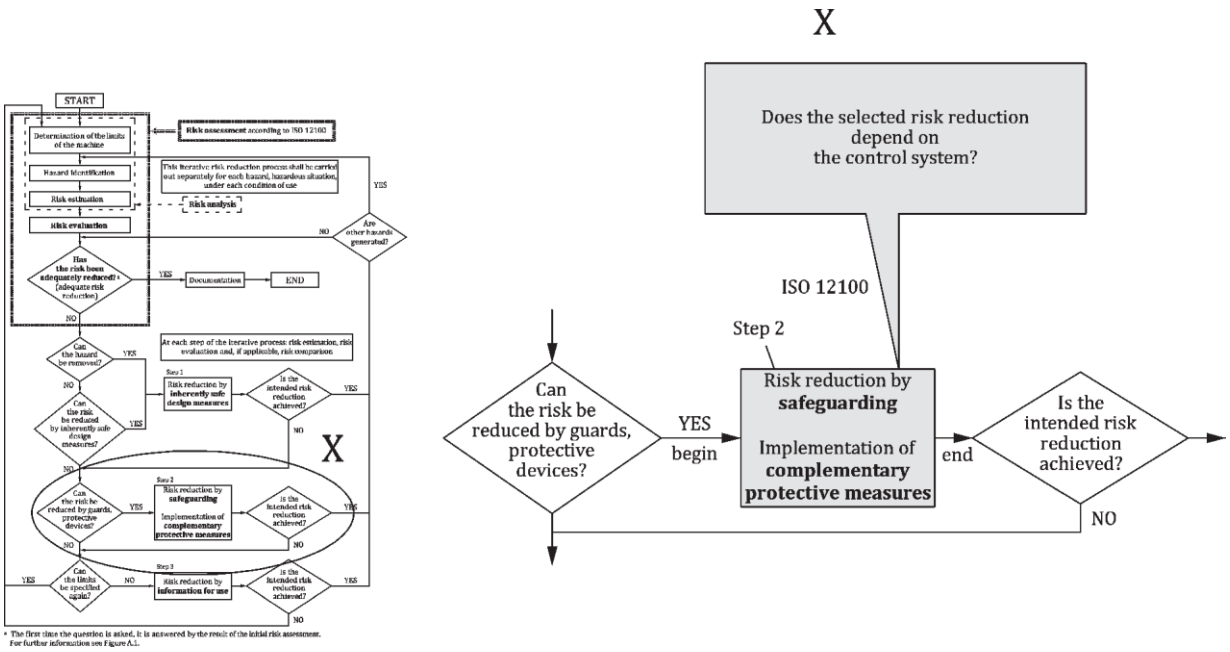
La réduction des risques selon l'ISO 12100:2010, Article 6, s'effectue en appliquant, dans la séquence suivante, les mesures de prévention intrinsèque, les mesures de sauvegarde et/ou de réduction des risques complémentaires et les informations pour l'utilisation. Un concepteur peut réduire les risques au moyen de mesures de réduction des risques en recourant à des fonctions de sécurité. Les parties des systèmes de commande de machines affectées à la réalisation des fonctions de sécurité sont appelées parties d'un système de commande relatives à la sécurité (SRP/CS), et peuvent être constituées de matériels et/ou de logiciels, et séparées ou intégrées au système de commande. En plus de fournir des fonctions de sécurité, les SRP/CS peuvent également mettre en œuvre des fonctions opérationnelles.

L'ISO 12100 est utilisée pour apprécier le risque de la machine. L'ISO 13849-1, Annexe A, peut être utilisée pour déterminer le niveau de performance requis d'une fonction de sécurité réalisée par les SRP/CS, où PL_r n'est pas spécifié dans la norme de type C applicable.

L'ISO 13849-1 est pertinente pour les fonctions de sécurité SRP/CS utilisées pour réduire les risques, si une appréciation du risque menée selon l'ISO 12100 a initié une mesure de réduction des risques (par exemple, protecteur avec dispositif d'interverrouillage) s'appuyant sur un système de commande relatif à la sécurité. Dans ces cas, le système de commande relatif à la sécurité doit réaliser une fonction de sécurité. Il convient d'utiliser l'ISO 13849-1 pour concevoir et évaluer les parties du système de commande relatives à la sécurité. Seule la partie du système de commande relative à la sécurité relève de l'ISO 13849-1.

La Figure 1 illustre la relation entre l'ISO 12100 et l'ISO 13849-1.

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



Does the selected risk reduction depend on the control system?	La réduction des risques sélectionnés dépend-elle du système de commande?
Step 2	Étape 2
Risk reduction by safeguarding	Réduction des risques par protection
Implementation of complementary protective measures	Mise en œuvre de mesures de protection complémentaires
YES	OUI
begin	début
Can the risk be reduced by guards, protective devices?	Le risque peut-il être réduit par des protecteurs, des dispositifs de protection?
end	fin
Is the intended risk reduction achieved?	La réduction prévue du risque est-elle atteinte?
NO	NON

Figure 1 — Intégration de l'ISO 13849-1 dans le processus de réduction des risques de l'ISO 12100

NOTE 3 La Figure 1 présente la manière dont les SRP/CS contribuent au processus de réduction des risques de l'ISO 12100: Étape 2. Les SRP/CS supportent les mesures de réduction des risques combinées par la mise en œuvre des fonctions de sécurité.

L'aptitude des parties 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 est déterminé par l'estimation du risque.

La probabilité de défaillance dangereuse des fonctions de sécurité dépend de plusieurs facteurs, tels que structure matérielle et logicielle du système, étendue des mécanismes de détection des défauts [couverture du diagnostic (DC)], fiabilité des composants [temps moyen avant défaillance dangereuse ($MTTF_D$)], défaillance de cause commune (CCF)], processus de conception, contrainte de fonctionnement, conditions environnementales et méthodes de fonctionnement.

La sécurité fonctionnelle inclut une catégorisation d'architecture selon une conception spécifique et des comportements spécifiés dans des conditions de défaut. Cette architecture est classée dans l'une des cinq catégories B, 1, 2, 3 ou 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 probabilité de défaillance dangereuse par heure (PFH_D).

L'estimation du risque montre une variance du fait de la nature subjective des critères d'évaluation. Les normes de type C peuvent présenter des méthodes d'estimation du risque plus spécifiques pour des applications spécifiques de la machine, qui peuvent être de nature moins subjective. Par conséquent, il convient donc de considérer l'utilisation de la méthodologie dans ce document comme une orientation précieuse pour la conception des parties du système de commande relatives à la sécurité plutôt que comme une exigence stricte. Les niveaux de performance et les catégories peuvent s'appliquer aux parties d'un système de commande relatives à la sécurité telles que

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

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

Les niveaux de performance peuvent être calculés, et les catégories déterminées pour

— les SRP/CS assurant des fonctions de sécurité pour les machines,

— les sous-systèmes de SRP/CS utilisant des parties de sécurité (composants) telles que

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

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

— Capteurs et éléments IHM (capteurs de position, interrupteurs d'activation).

Les machines prises en compte dans cette norme 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).

L'IEC 62061 et la présente partie de l'ISO 13849, à la fois, spécifient 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.

NOTE L'ISO/TR 23849 donne des conseils sur la relation entre les deux normes, et la manière dont elles se complètent.

Les exigences de l'Article 10 de l'ISO 13849-1 remplacent les exigences de l'ISO 13849-2:2012 à l'exception des annexes informatives. Une SRP/CS qui répond aux exigences de l'Article 10 est réputée satisfaire aux exigences de l'ISO 13849-2:2012.

Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux de conception

1 Domaine d'application

La présente partie de l'ISO 13849 spécifie une méthodologie et donne des conseils portant sur la conception et l'intégration des parties des systèmes de commande, relatives à la sécurité (SRP/CS), incluant la conception du logiciel. Le présent document spécifie les caractéristiques nécessaires pour déterminer le niveau de performance requis des fonctions de sécurité. Le présent document s'applique aux SRP/CS pour le mode à sollicitation élevée et le mode continu, incluant leurs sous-systèmes, indépendamment du type de technologie et d'énergie utilisé (par exemple, électrique, hydraulique, pneumatique, mécanique), quelles que soient les machines. La norme ne s'applique pas au mode à faible sollicitation.

Le présent document ne spécifie pas quelles fonctions de sécurité et quels niveaux de performance doivent être utilisés dans un cas particulier.

Le présent document ne donne pas d'exigences spécifiques pour la conception de composants intégrés dans les SRP/CS.

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

NOTE 1 Le présent document spécifie une méthodologie pour la conception des SRP/CS sans tenir compte de la nécessité d'exigences spécifiques pour certaines machines (par exemple, machines mobiles). Ces exigences spécifiques peuvent être prises en compte dans une norme de type-C.

NOTE 2 Pour le mode à faible sollicitation, voir l'IEC 61508.

NOTE 3 Voir également l'ISO/TR 22100-4 pour les aspects de sécurité TI et l'IEC/TR 63074 pour les aspects liés de sécurité.

2 Références normatives

Les documents suivants cités dans le texte 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 13849-2:2013, *Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 2: Validation*

IEC 60204-1:2016, *Sécurité des machines — Équipement électrique des machines — Partie 1: Exigences générales*

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 62061:2015, *Sécurité des machines — Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

3 Termes et définitions

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

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

— Plate-forme de consultation en ligne ISO: disponible à l'adresse https://www.iso.org/obp

3.1 Termes et définitions

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 répondant à des signaux d'entrée et générant 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 aux points 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).

3.1.2
spécification des exigences de sécurité
SRS
spécification renfermant les exigences relatives aux fonctions de sécurité qui doivent être assurées 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

[SOURCE: IEC 61508-4:2010, 3.5.11 et 3.5.12, modifiée, Note ajoutée]

3.1.3
catégorie
classification du sous-système liée à sa résistance aux défauts et à son comportement consécutif à des défauts, qui est obtenue par l'architecture des parties, la détection des défauts et/ou leur fiabilité

3.1.4
défaut
état d'un dispositif caractérisé par son inaptitude à accomplir une fonction requise, non comprise l'inaptitude due à la maintenance préventive ou à d'autres actions programmées, ou due à un manque de moyens extérieurs

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

Note 2 à l'article: Dans la présente partie de l'ISO 13849-1, «défaut» signifie un défaut aléatoire ou un défaut causé par une défaillance systématique.

[SOURCE: IEC 60050-192:2015; modifiée: Note 2 à l'article modifiée]

3.1.5
exclusion de défauts
exclusion de certains défauts dans une SRP/CS, si elle est justifiée en raison de leur improbabilité et de leur contribution négligeable à la fiabilité des SRP/CS

3.1.6
défaillance
cessation de l'aptitude d'un dispositif à accomplir une fonction requise

Note 1 à l'article: Après défaillance d'un dispositif, celui-ci est en état de défaut.

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 de la présente partie de l'ISO 13849.

[SOURCE: IEC 60050-192:2015; modifiée: Note 4 à l'article modifiée]

3.1.7
défaillance dangereuse
défaillance qui peut potentiellement mettre une SRP/CS dans un état dangereux ou défectueux

Note 1 à l'article: La réalisation ou non du «potentiellement» peut dépendre de l'architecture de canal du système; dans des systèmes redondants, une défaillance dangereuse du système matériel présente moins de risque d'aboutir à un état global dangereux ou défectueux.

[SOURCE: IEC 61508-4:2010, 3.6.7]

3.1.8
défaillance de cause commune
CCF
défaillance, résultat d'un ou plusieurs événements, entraînant des défaillances simultanées sur deux ou plusieurs canaux séparés dans un sous-système à canaux multiples, entraînant la défaillance d'une fonction de sécurité

Note 1 à l'article: Il convient de ne pas confondre les défaillances de cause commune et les défaillances de mode commun (voir l'ISO 12100:2010, 3.36).

[SOURCE: IEC 61508-4:2010]

3.1.9
défaillance systématique
défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

Note 1 à l'article: La maintenance corrective sans modification n'élimine pas, habituellement, la cause de la défaillance.

Note 2 à l'article: Une défaillance systématique peut être induite en simulant la cause de la défaillance.

Note 3 à l'article: Exemples de causes de défaillances systématiques incluant les erreurs humaines dans

— la spécification des exigences de sécurité,

— la conception, la fabrication, l'installation et l'exploitation du matériel, et

— la conception, la mise en œuvre, etc., du logiciel.

[SOURCE: IEC 60050-192:2015]

3.1.10
inhibition
interruption automatique et temporaire de fonction(s) de sécurité par les SRP/CS

3.1.11
réarmement manuel
fonction de sécurité interne aux SRP/CS permettant de rétablir manuellement des fonctions de sécurité données avant la remise en marche d'une machine

3.1.12
dommage
blessure physique ou atteinte à la santé

[SOURCE: ISO 12100:2010, 3.5]

3.1.13
phénomène dangereux
source potentielle de dommage

Note 1 à l'article: L'expression «phénomène dangereux» peut être qualifiée de manière à faire apparaître l'origine (par exemple, phénomène dangereux mécanique, phénomène dangereux électrique) ou la nature du dommage potentiel (par exemple, risque de choc électrique, de coupure, d'intoxication, et d'incendie).

Note 2 à l'article: Le phénomène dangereux envisagé dans cette définition:

— est présent en permanence pendant l'utilisation normale de la machine (par exemple, déplacement d'éléments mobiles dangereux, arc électrique pendant une phase de soudage, mauvaise posture, émission de bruit, température élevée), ou

— peut apparaître de manière inattendue (par exemple, explosion, risque d'écrasement résultant d'une mise en marche intempestive/inattendue, projection résultant d'une rupture, chute résultant d'une accélération ou d'une décélération).

[SOURCE: ISO 12100:2010, 3.6, modifiée, Note 3 supprimée]

3.1.14
situation dangereuse
situation dans laquelle une personne est exposée à au moins un phénomène dangereux

Note 1 à l'article: L'exposition peut entraîner un dommage, immédiatement ou à plus long terme.

[SOURCE: ISO 12100:2010, 3.10]

3.1.15
risque
combinaison de la probabilité d'un dommage et de la gravité de ce dommage

[SOURCE: ISO 12100:2010, 3.12]

3.1.16
risque résiduel
risque subsistant après que des mesures de réduction du risque (mesures de protection) ont été prises

Note 1 à l'article: Voir Figure 2.

[SOURCE: ISO 12100:2010, 3.13, Note 1 modifiée]

3.1.17
appréciation du risque
processus global d'analyse et d'évaluation du risque

[SOURCE: ISO 12100:2010, 3.17]

3.1.18
analyse du risque
combinaison de la détermination des limites de la machine, de l'identification des phénomènes dangereux et de l'estimation du risque

[SOURCE: ISO 12100:2010, 3.15]

3.1.19
évaluation du risque
jugement destiné à établir, à partir de l'analyse du risque, si les objectifs de réduction du risque ont été atteints

[SOURCE: ISO 12100:2010, 3.16]

3.1.20
utilisation normale d'une machine
utilisation d'une machine conformément aux indications données dans les instructions pour l'utilisation

[SOURCE: ISO 12100:2010, 3.23]

3.1.21
mauvais usage raisonnablement prévisible
utilisation d'une machine dans des conditions non prévues par le concepteur, mais pouvant résulter d'un comportement humain envisageable

[SOURCE: ISO 12100:2010, 3.24]

3.1.22
fonction de sécurité
fonction d'une machine dont la défaillance peut provoquer un accroissement immédiat du (des) risque(s)

Note 1 à l'article: Une fonction de sécurité est une fonction à mettre en œuvre par une partie d'un système de commande relative à la sécurité, qui est nécessaire pour atteindre ou maintenir un état sûr de la machine face à un événement dangereux spécifique.

[SOURCE: ISO 12100:2010, 3.30]

3.1.23
surveillance continue
mesure de diagnostic qui détecte un état et le compare à la valeur prévue