

---

---

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

Partie 1:  
**Principes généraux de conception**

iTeh STANDARD PREVIEW

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

[ISO 13849-1:2006](https://standards.iso.org/standards/catalog/standards/sist/8e204c20-5912-4ffe-b59b-294c99dd8a1b/iso-13849-1-2006)

<https://standards.iso.org/standards/catalog/standards/sist/8e204c20-5912-4ffe-b59b-294c99dd8a1b/iso-13849-1-2006>



**PDF – Exonération de responsabilité**

Le présent fichier PDF peut contenir des polices de caractères intégrées. Conformément aux conditions de licence d'Adobe, ce fichier peut être imprimé ou visualisé, mais ne doit pas être modifié à moins que l'ordinateur employé à cet effet ne bénéficie d'une licence autorisant l'utilisation de ces polices et que celles-ci y soient installées. Lors du téléchargement de ce fichier, les parties concernées acceptent de fait la responsabilité de ne pas enfreindre les conditions de licence d'Adobe. Le Secrétariat central de l'ISO décline toute responsabilité en la matière.

Adobe est une marque déposée d'Adobe Systems Incorporated.

Les détails relatifs aux produits logiciels utilisés pour la création du présent fichier PDF sont disponibles dans la rubrique General Info du fichier; les paramètres de création PDF ont été optimisés pour l'impression. Toutes les mesures ont été prises pour garantir l'exploitation de ce fichier par les comités membres de l'ISO. Dans le cas peu probable où surviendrait un problème d'utilisation, veuillez en informer le Secrétariat central à l'adresse donnée ci-dessous.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO 13849-1:2006](https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ff6-b59b-294c99dd8a1b/iso-13849-1-2006)

<https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ff6-b59b-294c99dd8a1b/iso-13849-1-2006>

© ISO 2006

Droits de reproduction réservés. Sauf prescription différente, 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 et les microfilms, sans l'accord écrit de l'ISO à l'adresse ci-après ou du comité membre de l'ISO dans le pays du demandeur.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax. + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Publié en Suisse

## Sommaire

Page

Avant-propos.....	v
Introduction.....	vi
<b>1</b> <b>Domaine d'application.....</b>	<b>1</b>
<b>2</b> <b>Références normatives.....</b>	<b>1</b>
<b>3</b> <b>Termes, définitions, symboles et abréviations.....</b>	<b>2</b>
3.1 <b>Termes et définitions.....</b>	<b>2</b>
3.2 <b>Symboles et abréviations.....</b>	<b>8</b>
<b>4</b> <b>Considérations relatives à la conception.....</b>	<b>9</b>
4.1 <b>Objectifs de sécurité lors de la conception.....</b>	<b>9</b>
4.2 <b>Stratégie de réduction du risque.....</b>	<b>11</b>
4.2.1 <b>Généralités.....</b>	<b>11</b>
4.2.2 <b>Contribution à la réduction du risque par le système de commande.....</b>	<b>11</b>
4.3 <b>Détermination du niveau de performance requis (PL<sub>r</sub>).....</b>	<b>14</b>
4.4 <b>Conception des SRP/CS.....</b>	<b>14</b>
4.5 <b>Évaluation du niveau de performance PL atteint et relation avec le SIL.....</b>	<b>15</b>
4.5.1 <b>Niveau de performance PL.....</b>	<b>15</b>
4.5.2 <b>Temps moyen avant défaillance dangereuse pour chaque canal (MTTF<sub>d</sub>).....</b>	<b>17</b>
4.5.3 <b>Couverture du diagnostic (DC).....</b>	<b>18</b>
4.5.4 <b>Procédure simplifiée pour l'estimation d'un PL.....</b>	<b>18</b>
4.6 <b>Exigences pour le logiciel de sécurité.....</b>	<b>21</b>
4.6.1 <b>Généralités.....</b>	<b>21</b>
4.6.2 <b>Logiciel intégré relatif à la sécurité (SRESW).....</b>	<b>21</b>
4.6.3 <b>Logiciel applicatif relatif à la sécurité (SRASW).....</b>	<b>22</b>
4.6.4 <b>Paramétrage lié au logiciel.....</b>	<b>25</b>
4.7 <b>Vérification de l'atteinte du PL requis.....</b>	<b>26</b>
4.8 <b>Aspects ergonomiques de la conception.....</b>	<b>26</b>
<b>5</b> <b>Caractéristiques des fonctions de sécurité.....</b>	<b>27</b>
5.1 <b>Spécification des fonctions de sécurité.....</b>	<b>27</b>
5.2 <b>Détails des fonctions de sécurité.....</b>	<b>29</b>
5.2.1 <b>Fonction d'arrêt liée à la sécurité.....</b>	<b>29</b>
5.2.2 <b>Fonction réarmement manuel.....</b>	<b>29</b>
5.2.3 <b>Fonction mise en marche et remise en marche.....</b>	<b>30</b>
5.2.4 <b>Fonction commande locale.....</b>	<b>30</b>
5.2.5 <b>Fonction d'inhibition.....</b>	<b>31</b>
5.2.6 <b>Temps de réponse.....</b>	<b>31</b>
5.2.7 <b>Paramètres relatifs à la sécurité.....</b>	<b>31</b>
5.2.8 <b>Variations, perte et rétablissement des sources d'énergie.....</b>	<b>31</b>
<b>6</b> <b>Catégories et leur relation aux MTTF<sub>d</sub> de chaque canal, DC<sub>avg</sub> et CCF.....</b>	<b>32</b>
6.1 <b>Généralités.....</b>	<b>32</b>
6.2 <b>Spécifications des catégories.....</b>	<b>32</b>
6.2.1 <b>Généralités.....</b>	<b>32</b>
6.2.2 <b>Architectures désignées.....</b>	<b>33</b>
6.2.3 <b>Catégorie B.....</b>	<b>33</b>
6.2.4 <b>Catégorie 1.....</b>	<b>34</b>
6.2.5 <b>Catégorie 2.....</b>	<b>35</b>
6.2.6 <b>Catégorie 3.....</b>	<b>37</b>
6.2.7 <b>Catégorie 4.....</b>	<b>38</b>
6.3 <b>Combinaison des SRP/CS pour atteindre un PL global.....</b>	<b>40</b>

7	Prise en compte des défauts, exclusion de défauts .....	41
7.1	Généralités .....	41
7.2	Prise en compte des défauts .....	41
7.3	Exclusion de défauts .....	42
8	Validation .....	42
9	Maintenance.....	42
10	Documentation technique .....	43
11	Informations pour l'utilisation .....	44
Annexe A (informative) Détermination du niveau de performance requis (PL <sub>r</sub> ) .....		45
Annexe B (informative) Méthode bloc et diagramme bloc relatif à la sécurité .....		48
Annexe C (informative) Calcul ou évaluation du MTTF <sub>d</sub> pour des composants uniques .....		50
Annexe D (informative) Méthode simplifiée pour estimer le MTTF <sub>d</sub> pour chaque canal.....		58
Annexe E (informative) Estimations pour la couverture du diagnostic (DC) pour les fonctions et les modules.....		60
Annexe F (informative) Estimations pour les défaillances de cause commune (CCF) .....		63
Annexe G (informative) Défaillance systématique .....		66
Annexe H (informative) Combinaison de plusieurs parties du système de commande relatives à la sécurité (SRP/CS).....		69
Annexe I (informative) Exemples .....		72
Annexe J (informative) Logiciel.....		79
Annexe K (informative) Représentation numérique de la Figure 5 .....		83
Bibliographie .....		86

ISO 13849-1:2006  
<https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4f6e-b59b-294c99dd8a1b/iso-13849-1-2006>

## 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 (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO 13849-1 a été élaborée par le comité technique CEN/TC 114, *Sécurité des machines et appareils*, du Comité européen de normalisation (CEN) en collaboration avec le comité technique ISO/TC 199, *Sécurité des machines*, 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 13849-1:1999), dont elle constitue une révision technique. <https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ffc-b59b-294c99dd8a1b/iso-13849-1-2006>

L'ISO 13849 comprend les parties suivantes, présentées sous le titre général *Sécurité des machines — Parties des systèmes de commande relatives à la sécurité*:

- *Partie 1: Principes généraux de conception*
- *Partie 2: Validation*
- *Partie 100: Lignes directrices pour l'utilisation et l'application de l'ISO 13849-1* [Rapport technique]

## Introduction

Dans le domaine de la sécurité des machines, les normes sont structurées de la manière 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 aspect de la sécurité ou d'un type de dispositif conditionnant la sécurité valable pour toutes les machines ou 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 dispositifs conditionnant la sécurité (par exemple commandes bimanuelles, dispositifs de verrouillage, dispositifs sensibles à la pression, protecteurs);
- c) **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 de l'ISO 13849 est une norme de type B1 telle que définie dans l'ISO 12100-1.

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, et ce pour les machines conçues et fabriquées conformément aux spécifications de la norme 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 présumées conformes aux exigences essentielles de sécurité de l'Annexe I de la Directive du Conseil 98/37/CE. Elle ne donne pas de conseils spécifiques pour la conformité à d'autres Directives CE.

En tant que partie de la stratégie globale de réduction des risques pour une machine, un concepteur voudra souvent choisir de réaliser certaines mesures de réduction des risques par l'application de mesures de protection employant une ou plusieurs 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 de logiciels et peuvent être séparées ou intégrées au système de commande. En plus de fournir des fonctions de sécurité, les SRP/CS peuvent faire partie d'une fonction opérationnelle (par exemple commandes bimanuelles comme moyen de mise en marche d'un cycle ou d'un processus).

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). Ces niveaux de performance sont définis en termes de probabilité de défaillance dangereuse du système (voir Tableau 3).

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<sub>d</sub>), défaillance de cause commune (CCF)], processus de conception, contrainte de fonctionnement, conditions environnementales et méthodes de fonctionnement.

Afin d'aider le concepteur et de faciliter l'estimation du PL atteint, la présente partie de l'ISO 13849 définit une approche reposant sur la classification des structures selon des critères de conception spécifiques et un comportement spécifiés en cas de défaut. Ces catégories sont classées en cinq niveaux, appelés Catégories B, 1, 2, 3 et 4.

Les niveaux de performance et les catégories peuvent s'appliquer aux parties d'un système de commande relatives à la sécurité telles que

- les équipements de protection (par exemple dispositifs de commande bimanuelle, dispositifs de verrouillage), dispositifs de protection électrosensibles (par exemple barrières photoélectriques), dispositifs sensibles à la pression,
- les unités de commande (par exemple unité logique pour les fonctions de commande, traitement des données, surveillance, etc.), et
- les dispositifs de commande de l'énergie (par exemple relais, distributeurs, etc.),

ainsi qu'aux systèmes de commande exécutant des fonctions de sécurité pour tout type de machines, de la plus simple (par exemple matériel de cuisine ou portes et barrières automatiques) aux installations manufacturières (par exemple machines d'emballage, machines d'impression, presses).

L'objectif de la présente partie de l'ISO 13849 est de fournir une base claire permettant l'évaluation de la conception et des performances de toute application de SRP/CS (et de la machine) par une tierce partie ou en interne ou par un laboratoire d'essai indépendant, par exemple.

**Information sur l'utilisation recommandée de la CEI 62061 et la présente partie de l'ISO 13849**

La CEI 62061 et la présente partie de l'ISO 13849 spécifient les exigences pour la conception et la mise en œuvre des systèmes de commande électriques relatifs à la sécurité des machines. L'utiliser de l'une de ces deux Normes internationales, en accord avec leurs domaines d'application, peut présumer de satisfaire aux exigences essentielles de sécurité appropriées. Le Tableau 1 résume les domaines d'application de la CEI 62061 et de la présente partie de l'ISO 13849.

**Tableau 1 — Utilisation recommandée de la CEI 62061 et de la présente partie de l'ISO 13849**

	Technologie mettant en œuvre la(les) fonction(s) de commande relative(s) à la sécurité	ISO 13849-1	CEI 62061
A	Non électrique, par exemple hydraulique	X	Non couvert
B	Électromécanique, par exemple relais, et/ou électronique non complexe	Limité aux architecture désignées <sup>a</sup> et jusqu'à PL = e	Toutes architectures et jusqu'à SIL 3
C	Électronique complexe, par exemple programmable	Limité aux architecture désignées <sup>a</sup> et jusqu'à PL = d	Toutes architectures et jusqu'à SIL 3
D	A combiné avec B	Limité aux architecture désignées <sup>a</sup> et jusqu'à PL = e	X <sup>c</sup>
E	C combiné avec B	Limité aux architecture désignées et jusqu'à PL = d	Toutes architectures et jusqu'à SIL 3
F	C combiné avec A, ou C combiné avec A et B	X <sup>b</sup>	X

X indique que ce cas est traité par la Norme internationale indiquée en tête de colonne

<sup>a</sup> Les architectures désignées sont définies en 6.2 afin de fournir une approche simplifiée de la quantification du niveau de performance.

<sup>b</sup> Pour l'électronique complexe: utilisation des architectures désignées conformes à la présente partie de l'ISO 13849 jusqu'à PL = d ou toute architecture conforme à la CEI 62061.

<sup>c</sup> Pour la technologie non électrique, utilisation des parties en tant que sous-systèmes conformes à la présente partie de l'ISO 13849.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[ISO 13849-1:2006](https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ffe-b59b-294c99dd8a1b/iso-13849-1-2006)

<https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ffe-b59b-294c99dd8a1b/iso-13849-1-2006>

# 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 fournit des exigences de sécurité et des conseils relatifs aux principes de conception et d'intégration des parties des systèmes de commande relatives à la sécurité (SRP/CS) incluant la conception du logiciel. Pour ces parties, elle spécifie les caractéristiques, incluant le niveau de performance requis, pour réaliser ces fonctions de sécurité. Elle s'applique aux SRP/CS de tous les types de machines, indépendamment de la technologie et du type d'énergie utilisés (électrique, hydraulique, pneumatique, mécanique, etc.).

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

La présente partie de l'ISO 13849 fournit des exigences spécifiques pour les SRP/CS utilisant un (des) système(s) électronique(s) programmable(s).

Elle ne donne pas d'exigences spécifiques pour la conception de composants intégrés dans les SRP/CS. Néanmoins, les principes donnés, tels que les catégories ou les niveaux de performance, peuvent être utilisés.

NOTE 1 Exemples de composants intégrés dans les SRP/CS: relais, distributeur solénoïde, interrupteur de position, PLC, unité de commande de moteurs, dispositifs de commande bimanuelle, dispositifs de protection électrosensibles. Pour la conception de tels composants, il est recommandé de se référer aux normes spécifiques, par exemple l'ISO 13851, l'ISO 13856-1 et l'ISO 13856-2.

NOTE 2 Pour la définition du *niveau de performance requis*, voir 3.1.24.

NOTE 3 Les exigences fournies dans la présente partie de l'ISO 13849 pour les systèmes électroniques programmables sont compatibles avec la méthodologie pour la conception et le développement des systèmes, pour les machines, de commande électriques, électroniques et électroniques programmables relatifs à la sécurité donnés dans la CEI 61061.

NOTE 4 Pour le logiciel embarqué relatif à la sécurité pour des composants de PL<sub>r</sub> = e, voir la CEI 61508-3:1998, Article 7.

NOTE 5 Voir également le Tableau 1.

### 2 Références normatives

Les documents de références suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition de la publication à laquelle il est fait référence s'applique (y compris les amendements).

ISO 12100-1:2003, *Sécurité des machines — Notions fondamentales, principes généraux de conception — Partie 1: Terminologie de base, méthodologie*

ISO 12100-2:2003, *Sécurité des machines — Notions fondamentales, principes généraux de conception — Partie 2: Principes techniques*

ISO 13849-2:2003, *Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 2: Validation*

ISO 14121:—<sup>1)</sup>, *Sécurité des machines — Principes pour l'appréciation du risque*

CEI 60050-191:1990, *Vocabulaire Électrotechnique International — Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 60050-191:1990-am1:1999-am2:2002, *Vocabulaire Électrotechnique International — Chapitre 191: Sûreté de fonctionnement et qualité de service*

CEI 61508-3:1998 et corr.1:1999, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité — Partie 3: Prescriptions concernant les logiciels*

CEI 61508-4:1998 et corr.1:1999, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité — Partie 4: Définitions et abréviations*

### 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 12100-1 et la CEI 60050-191 ainsi que les suivants s'appliquent.

##### 3.1.1

##### **partie d'un système de commande relative à la sécurité**

##### **SRP/CS**

partie d'un système de commande qui répond à des signaux d'entrée et génère des signaux de sortie relatifs à la sécurité

NOTE 1 Les parties combinées 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).

NOTE 2 Si un système de surveillance est utilisé pour les diagnostics, ceux-ci sont considérés comme des SRP/CS.

##### 3.1.2

##### **catégorie**

classification des parties relatives à la sécurité d'un système de commande liée à leur résistance aux défauts et à leur comportement consécutif à des défauts et qui est obtenue par l'architecture des parties, la détection des défauts et/ou leur fiabilité

##### 3.1.3

##### **défaut**

état d'une entité caractérisée 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 Un défaut est souvent le résultat d'une défaillance de l'entité elle-même, mais il peut exister sans défaillance préalable.

[CEI 60050-191:1990, 05-01]

NOTE 2 Dans la présente partie de l'ISO 13849, le terme «défaut» signifie «défaut aléatoire».

1) À publier. (Révision de l'ISO 14121:1999)

**3.1.4****défaillance**

cessation de l'aptitude d'une entité à accomplir une fonction requise

NOTE 1 Après défaillance d'une entité, cette entité a un défaut.

NOTE 2 Une défaillance est un passage d'un état à un autre, par opposition à un défaut qui est un état.

NOTE 3 La notion de défaillance, telle qu'elle est définie, ne s'applique pas à une entité constituée seulement de logiciel.

[CEI 60050-191:1990, 04-01]

NOTE 4 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.

**3.1.5****défaillance dangereuse**

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

NOTE 1 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.

NOTE 2 Adaptée de la CEI 61508-4:1998, définition 3.6.7.

**3.1.6****défaillance de cause commune****CCF**

défaillances qui affectent plusieurs entités à partir d'un même événement et qui ne résultent pas les unes des autres

[ISO 13849-1:2006](https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ffe-b59b-294c99dd8a1b/iso-13849-1-2006)

[CEI 60050-191:1990-am1:1999, 04-23] <https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ffe-b59b-294c99dd8a1b/iso-13849-1-2006>

NOTE Il convient de ne pas confondre les défaillances de cause commune et les défaillances de mode commun (voir l'ISO 12100-1:2003, 3.34).

**3.1.7****défaillance systématique**

défaillance associée 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 La maintenance corrective sans modification n'élimine pas, habituellement, la cause de la défaillance.

NOTE 2 Une défaillance systématique peut être induite en simulant la cause de la défaillance.

[CEI 60050-191:1990, 04-19]

NOTE 3 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;
- la conception, la mise en œuvre, etc., du logiciel.

**3.1.8****inhibition**

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

### 3.1.9

#### **réarmement manuel**

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

### 3.1.10

#### **dommage**

blesseure physique ou atteinte à la santé

[EN ISO 12100-1:2003, 3.5]

### 3.1.11

#### **phénomène dangereux**

source potentielle de dommage

NOTE 1 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, d'incendie).

NOTE 2 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).

[ISO 12100-1:2003, 3.6]

### 3.1.12

#### **situation dangereuse**

situation dans laquelle une personne est exposée à au moins un phénomène dangereux, l'exposition pouvant entraîner un dommage, immédiatement ou à plus long terme

[ISO 12100-1:2003, 3.9]

### 3.1.13

#### **risque**

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

[ISO 12100-1:2003, 3.11]

### 3.1.14

#### **risque résiduel**

risque subsistant après que des mesures de prévention ont été prises

Voir Figure 2.

NOTE Adaptée de l'ISO 12100-1:2003, définition 3.12.

### 3.1.15

#### **appréciation du risque**

processus global d'analyse et d'évaluation du risque

[ISO 12100-1:2003, 3.13]

**3.1.16****analyse du risque**

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

[ISO 12100-1:2003, 3.14]

**3.1.17****évaluation du risque**

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

[ISO 12100-1:2003, 3.16]

**3.1.18****utilisation normale d'une machine**

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

(ISO 12100-1:2003, 3.22)

**3.1.19****mauvais usage raisonnablement prévisible**

utilisation d'une machine d'une manière ne correspondant pas aux intentions du concepteur, mais pouvant résulter d'un comportement humain aisément prévisible

[ISO 12100-1:2003, 3.23]

**3.1.20****fonction de sécurité**

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

[ISO 12100-1:2003, 3.28]

iTeh STANDARD PREVIEW

(standards.iteh.ai)

[ISO 13849-1:2006](https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ff6-b59b-294c99dd8a1b/iso-13849-1-2006)

**3.1.21****surveillance continue**

fonction de sécurité assurant qu'une mesure de prévention est initiée si l'aptitude d'un composant ou d'un élément à exécuter sa fonction diminue ou si les conditions de fonctionnement sont modifiées de telle façon qu'il en résulte une diminution de la réduction du risque

<https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ff6-b59b-294c99dd8a1b/iso-13849-1-2006>

**3.1.22****système électronique programmable****PES**

système de commande, de protection ou de surveillance reposant sur un ou plusieurs dispositifs électroniques programmables, y compris tous les éléments du système tels que les alimentations en énergie, les capteurs et autres dispositifs d'entrée, jusqu'aux actionneurs et autres dispositifs de sortie

NOTE Adaptée de la CEI 61508-4:1998, définition 3.3.2.

**3.1.23****niveau de performance****PL**

niveau discret d'aptitude de parties relatives à la sécurité à réaliser une fonction de sécurité dans des conditions prévisibles

NOTE Voir 4.5.1.

**3.1.24****niveau de performance requis****PL<sub>r</sub>**

niveau de performance (PL) permettant d'atteindre la réduction du risque requise pour chaque fonction de sécurité

NOTE Voir Figures 2 et A.1.

**3.1.25**

**temps moyen avant défaillance dangereuse**

**MTTF<sub>d</sub>**

valeur probable de la durée moyenne avant défaillance dangereuse

NOTE Adaptée de la CEI 62061:2005, définition 3.2.34.

**3.1.26**

**couverture du diagnostic**

**DC**

mesure de l'efficacité du diagnostic, peut être définie comme la fraction de la probabilité de défaillances dangereuses détectées sur la probabilité de toutes les défaillances dangereuses

NOTE 1 La couverture du diagnostic peut se rapporter à tout ou partie d'un système relatif à la sécurité. Elle peut, par exemple, concerner des capteurs et/ou un système logique et/ou des éléments terminaux.

NOTE 2 Adaptée de la CEI 61508-4:1998, définition, 3.8.6.

**3.1.27**

**mesure de prévention**

mesure destinée à réduire le risque

EXEMPLE 1 Mise en œuvre par le concepteur: prévention intrinsèque, protection et mesures de prévention complémentaires, informations pour l'utilisation.

EXEMPLE 2 Mise en œuvre par l'utilisateur: organisation (méthodes de travail sûres, surveillance, système du permis de travailler), fourniture et utilisation de moyens de protection supplémentaires, équipement de protection individuelle, formation.

ITIH STANDARD PREVIEW  
(standards.iteh.ai)

NOTE Adaptée de l'ISO 12100-1:2003, définition 3.18.

[ISO 13849-1:2006](https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ffe-b59b-294c99dd8a1b/iso-13849-1-2006)

<https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ffe-b59b-294c99dd8a1b/iso-13849-1-2006>

**3.1.28**

**durée de mission**

**T<sub>M</sub>**

laps de temps couvrant l'utilisation normale d'une SRP/CS

**3.1.29**

**taux d'essais**

**r<sub>t</sub>**

fréquence des essais en ligne permettant de détecter les défauts d'un SRP/CS, valeur inverse de l'intervalle entre essais de diagnostic

**3.1.30**

**taux de demande**

**r<sub>d</sub>**

fréquence de sollicitation d'une action relative à la sécurité d'une SRP/CS

**3.1.31**

**taux de réparation**

**r<sub>r</sub>**

valeur inverse de l'intervalle de temps entre la détection d'une défaillance dangereuse par un essai en ligne ou un dysfonctionnement évident du système et la remise en marche après réparation du système/remplacement du composant

NOTE Le temps de réparation ne comprend pas le temps nécessaire à la détection de la défaillance.

**3.1.32****système de commande de la machine**

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

NOTE Le système de commande de la machine peut utiliser toute technologie ou combinaison de différentes technologies (exemple électrique/électronique, hydraulique, pneumatique, mécanique).

**3.1.33****Niveau d'intégrité de sécurité****SIL**

niveau discret (parmi trois possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions de commandes relatives à la sécurité à allouer aux systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité, le niveau 4 d'intégrité de sécurité possédant le plus haut degré d'intégrité et le niveau 1 possédant le plus bas

[CEI 61508-4:1998, 3.5.6]

**3.1.34****langage de variabilité limitée****LVL**

type de langage qui fournit la possibilité de combiner des fonctions de bibliothèques, prédéfinies, spécifiques à une application, pour mettre en œuvre les spécifications des exigences concernant la sécurité

NOTE 1 Adaptée de la CEI 61511-1:2003, définition 3.2.80.1.2

NOTE 2 Des exemples typiques de LVL sont donnés dans la CEI 61131-3. Ils incluent: échelle logique, schéma bloc fonctionnel.

NOTE 3 Un exemple typique de système utilisant le LVL: PLC.

<https://standards.iteh.ai/catalog/standards/sist/8e204c20-5912-4ffc-b59b-294c99dd8a1b/iso-13849-1-2006>

**3.1.35****langage de variabilité totale****FVL**

type de langage qui fournit la possibilité de mettre en œuvre une gamme étendue de fonctions et d'applications

EXEMPLE C, C++, assembleur.

NOTE 1 Adaptée de la CEI 61511-1:2003, définition 3.2.80.1.3.

NOTE 2 Un exemple typique de système utilisant le FVL: ordinateur d'usage général.

NOTE 3 Le FVL se trouve normalement dans les logiciels intégrés et rarement dans les logiciels d'application.

**3.1.36****logiciel d'application**

logiciel spécifique d'application qui a été implémenté par le concepteur de la machine et qui contient généralement des séquences logiques, des limites et des expressions qui commandent l'entrée, la sortie, les calculs appropriés et les décisions nécessaires pour satisfaire aux exigences des SRP/CS

**3.1.37****logiciel intégré**

micrologiciel

logiciel système

logiciel faisant partie du système fourni par le constructeur et non accessible par l'utilisateur en vue d'une modification

NOTE Le logiciel intégré est généralement écrit en FVL.