

Redline version
compare la Quatrième
édition à la Troisième édition



**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*

*STANDARD PREVIEW
(standards.itech.ai)*

[ISO 13849-1:2023](https://standards.itech.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f-0a883595198b/iso-13849-1-2023)

<https://standards.itech.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f-0a883595198b/iso-13849-1-2023>



Numéro de référence
ISO13849-1:redline:2023(F)

IMPORTANT — PLEASE NOTE

This is a provisional mark-up copy and uses the following colour coding:

- Text example 1 — indicates added text (in green)
- ~~Text example 2~~ — indicates removed text (in red)
- indicates added graphic figure
- indicates removed graphic figure
- 1.x ... — Heading numbers containing modifications are highlighted in yellow in the Table of Contents

All changes in this document have yet to reach consensus by vote and as such should only be used internally for review purposes.

DISCLAIMER

This Redline version is not an official IEC Standard and is intended only to provide the user with an indication of what changes have been made to the previous version. Only the current version of the standard is to be considered the official document.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. A vertical bar appears in the margin wherever a change has been made. Additions and deletions are displayed in red, with deletions being struck through.



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2023

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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

Publié en Suisse

Sommaire

Page

Avant-propos	vii
Introduction	ix
1 Domaine d'application	1
2 Références normatives	2
3 Termes, définitions, symboles et abréviations	2
3.1 Termes et définitions	2
3.2 Symboles et abréviations	15
4 Présentation	16
4.1 Processus d'appréciation et de réduction du risque de la machine	16
4.2 Contribution à la réduction du risque	18
4.3 Processus de conception d'une SRP/CS	19
4.4 Méthodologie	21
4.5 Informations requises	21
4.6 Réalisation de la fonction de sécurité en utilisant les sous-systèmes	22
5 Spécification des fonctions de sécurité	22
5.1 Identification et description générale de la fonction de sécurité	22
5.2 Spécification des exigences de sécurité	23
5.2.1 Exigences générales	23
5.2.2 Exigences relatives aux fonctions de sécurité spécifiques	26
5.2.3 Réduction le plus possible de l'incitation à neutraliser les fonctions de sécurité	30
5.2.4 Accès à distance	31
5.3 Détermination du niveau de performance requis (PL _r) pour chaque fonction de sécurité	31
5.4 Examen de la spécification des exigences de sécurité (SRS)	31
5.5 Décomposition de la SRP/CS en sous-systèmes	32
6	34
6 Considérations relatives à la conception	34
 4.1 Objectifs de sécurité lors de la conception	34
 4.2 Stratégie de réduction du risque	36
 4.2.1 Généralités	36
 4.2.2 Contribution à la réduction du risque par le système de commande	36
 4.3 Détermination du niveau de performance requis (PL_r)	39
 4.4 Conception des SRP/CS	40
 4.5 6.1	41
 Évaluation du niveau de performance PL atteint et relation avec le SIL atteint	41
 4.5.1 6.1.1	41
 Niveau Présentation générale du niveau de performance PL	41
 6.1.2 Corrélation entre le niveau de performance (PL) et le niveau d'intégrité de sécurité (SIL)	44
 6.1.3 Architecture — Catégories et leur relation aux MTTF_D de chaque canal, couverture du diagnostic moyenne et défaillance de cause commune (CCF)	45
 4.5.2 6.1.4	52
 Temps moyen avant défaillance dangereuse pour chaque canal (MTTF_D)	52
 4.5.3 6.1.5	53
 Couverture du diagnostic (DC)	53
 6.1.6 Défaillances de cause commune (CCF)	54
 6.1.7 Défaillances systématiques	54
 4.5.4 6.1.8	55
 Procédure simplifiée pour l'estimation des aspects quantifiables d'un PL	55

4.5.4	6.1.8	55
	Procédures simplifiées pour estimer le niveau de performance de sous-systèmes	
4.5.5	6.1.9	58
	Description du dispositif de sortie du SRP/CS par catégorie	
4.5.5	6.1.9	59
	Autre procédure pour déterminer le niveau de performance et la PFH sans MTTF _D	
6.1.10	Prise en compte et exclusion des défauts	61
6.1.11	Composant éprouvé	62
6.2	Combinaison des sous-systèmes pour atteindre un niveau de performance global de la fonction de sécurité	62
6.2.1	Généralités	62
6.2.2	Valeurs PFH connues	63
6.2.3	Valeurs PFH inconnues	63
4.6	6.3	64
	Exigences pour le logiciel de sécurité	
4.6.1	Généralités	64
4.6.2	Logiciel intégré relatif à la sécurité (SRESW)	65
4.6	6.3	66
	Paramétrage manuel lié au logiciel	
4.6.3	6.3.1	66
	Logiciel applicatif relatif à la sécurité (SRASW)	
4.6.3	6.3.1	68
	Généralités	
6.3.2	Influences sur les paramètres relatifs à la sécurité	69
4.6.4	6.3.3	69
	Paramétrage Exigences relatives au paramétrage manuel lié au logiciel	
6.3.4	Vérification de l'outil de paramétrage	72
6.3.5	Documentation de paramétrage manuel lié au logiciel	72
4.7	Vérification de l'atteinte du PL requis	72
4.8	Aspects ergonomiques de la conception	72
7	Exigences concernant les logiciels	73
7.1	Généralités	73
7.2	Langage de variabilité limitée (LVL) et langage de variabilité totale (FVL)	74
7.2.1	Langage de variabilité limitée (LVL)	74
7.2.2	Langage de variabilité totale (FVL)	75
7.2.3	Décision pour le langage de variabilité limitée (LVL) ou le langage de variabilité totale (FVL)	75
7.3	Logiciel intégré relatif à la sécurité (SRESW)	77
7.3.1	Conception du logiciel intégré relatif à la sécurité (SRESW)	77
7.3.2	Autres procédures pour le logiciel intégré non accessible	78
7.4	Logiciel applicatif relatif à la sécurité (SRASW)	78
8	Vérification du niveau de performance atteint	81
5	Caractéristiques des fonctions de sécurité	82
5.1	Spécification des fonctions de sécurité	82
5.2	Détails des fonctions de sécurité	84
5.2.1	Fonction d'arrêt liée à la sécurité	84
5.2.2	Fonction réarmement manuel	84
5.2.3	Fonction mise en marche et remise en marche	85
5.2.4	Fonction commande locale	85
5.2.5	Fonction d'inhibition	86
5.2.6	Temps de réponse	86
5.2.7	Paramètres relatifs à la sécurité	86
5.2.8	Variations, perte et rétablissement des sources d'énergie	86

5	9	Aspects ergonomiques de la conception	86
6	6	Catégories et leur relation aux $MTTF_p$ de chaque canal, DC_{avg} et CCF	87
6	10	Validation	87
6.1	10.1	Généralités	87
6.1	10.1	Principes de validation	87
	10.1.1	Généralités	87
	10.1.2	Plan de validation	89
	10.1.3	Listes des défauts génériques	90
	10.1.4	Listes des défauts spécifiques	90
	10.1.5	Informations pour la validation	90
	10.2	Validation de la spécification des exigences de sécurité (SRS)	91
	10.3	Validation par analyse	92
	10.3.1	Généralités	92
	10.3.2	Techniques d'analyse	92
	10.4	Validation par essais	93
	10.4.1	Généralités	93
	10.4.2	Exactitude des mesures	93
	10.4.3	Exigences supplémentaires relatives aux essais	94
	10.4.4	Nombre d'échantillons	94
	10.4.5	Méthodes d'essai	94
	10.5	Validation des fonctions de sécurité	95
6.2	10.6	Spécifications des catégories	95
	6.2.1	Généralités	95
	6.2.2	Architectures désignées	96
6.2	10.6	Validation de l'intégrité de sécurité de la SRP/CS	96
	6.2.3	10.6.1	96
		Catégorie B	
	6.2.3	10.6.1	96
		Validation du (des) sous-système(s)	
	10.6.2	Validation des mesures prises contre les défaillances systématiques	98
	6.2.4	10.6.3	99
		Catégorie 1	
	6.2.4	10.6.3	99
		Validation du logiciel relatif à la sécurité	
	6.2.5	Catégorie 2	101
	6.2.6	Catégorie 3	102
	6.2.7	10.6.4	103
		Catégorie 4	
	6.2.7	10.6.4	104
		Validation de la combinaison des sous-systèmes	
	10.6.5	Validation globale de l'intégrité de sécurité	107
6.3	10.7	Combinaison des SRP/CS pour atteindre un PL global	107
6.3	10.7	Validation des exigences d'environnement	108
	10.8	Rapport de validation	109
	10.9	Validation des exigences de maintenance	109
7	7	Prise en compte des défauts, exclusion de défauts	110
	7.1	Généralités	110
	7.2	Prise en compte des défauts	110
	7.3	Exclusion de défauts	110

8	Validation	110
9	Maintenance	111
9	11	
	Maintenabilité des SRP/CS	111
10	12	
	Documentation technique	111
11	13	
	Informations pour l'utilisation	112
	13.1 Généralités	113
	13.2 Informations relatives à l'intégration de SRP/CS	113
	13.3 Informations destinées à l'utilisateur	114
Annexe A (informative)	Détermination Lignes directrices pour la détermination du niveau de performance requis (PL _r)	115
Annexe B (informative)	Méthode bloc et diagramme bloc relatif à la sécurité	122
Annexe C (informative)	Calcul ou évaluation de des valeurs MTTF _D pour des composants uniques	125
Annexe D (informative)	Méthode simplifiée pour estimer le MTTF _D pour chaque canal	138
Annexe E (informative)	Estimations pour la couverture du diagnostic (DC) pour les fonctions et les modules des fonctions et des sous-systèmes	141
Annexe F (informative)	Estimations pour Méthode de quantification des mesures contre les défaillances de cause commune (CCF)	146
Annexe G (informative)	Défaillance systématique	152
Annexe H (informative)	Combinaison de plusieurs parties du système de commande relatives à la sécurité (SRP/CS) Exemple d'une combinaison de plusieurs sous-systèmes	157
Annexe I (informative)	Exemples de procédure simplifiée pour estimer le PL de sous-systèmes	161
Annexe J (informative)	Logiciel Exemple d'élaboration de SRESW	174
Annexe K (informative)	Représentation numérique de la Figure 5-12	180
Annexe L (informative)	Immunité aux interférences électromagnétiques (IEM)	185
Annexe M (informative)	Informations supplémentaires pour la spécification des exigences de sécurité (SRS)	189
Annexe N (informative)	Évitement des défaillances systématiques lors de la conception logicielle	192
Annexe O (informative)	Valeurs relatives à la sécurité de composants ou de parties de systèmes de commande	213
Bibliographie	216

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/patents).

Les éventuelles appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne constituent pas une approbation ou une recommandation saurait 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, aussi bien que pour des informations au sujet de l'adhésion de l'ISO 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 URL suivant: [Foreword - Supplementary information www.iso.org/iso/avant-propos.html](http://www.iso.org/iso/avant-propos.html).

Le comité chargé de l'élaboration du présent document est l'ISO/TC 199, *Sécurité des machines*.

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 13849-1:2006/2015), dont elle constitue une qui a fait l'objet d'une révision technique. Elle comprend également le Rectificatif Technique ISO 13849-1.1/Cor 1:2009. Les modifications par rapport à l'édition précédente incluent

Les principales modifications sont les suivantes:

— suppression de l'ancien Tableau 1 contenu dans l'Introduction;

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;

— mise à jour et ajout de références normatives;

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

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

~~modification de la définition des termes *situation dangereuse* et *mode de demande élevée ou mode continu*,~~

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;

~~ajout d'un nouveau terme et définition, *utilisation éprouvée*,~~

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

~~modification éditoriale, mais pas technique, de la Figure 1,~~

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;

~~un nouveau paragraphe, 4.5.5, mais également des modifications aux sections existantes dont les annexes, notamment des modifications substantielles de l'Annexe C et une nouvelle Annexe I.~~

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

~~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~~

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

~~Dans le domaine de la sécurité des machines, les normes sont structurées de la manière suivante.~~

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

- a) **normes de type 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 de type B (normes génériques de sécurité), traitant d'un aspect ou de plusieurs aspect(s) de la sécurité, ou d'un type de dispositif conditionnant la sécurité valable pour toutes les machines 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 dispositifs conditionnant la sécurité,~~ 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.
- ~~e) 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~~ Le présent document est une norme de type B1 telle que définie dans ~~tel que défini dans l'ISO 12100:2010.~~

~~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 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.

~~La présente partie de l'ISO 13849~~ Le présent document est ~~destinée~~ destiné à donner des conseils au cours de la conception et de l'évaluation des systèmes de commande ainsi ~~qu'aux Comités Techniques élaborant~~ qu'au cours de l'élaboration des normes de type B2 ou de type C ~~présupposées conformes aux exigences essentielles de sécurité de l'Annexe I de la Directive 2006/42/CE relative aux machines. 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.~~

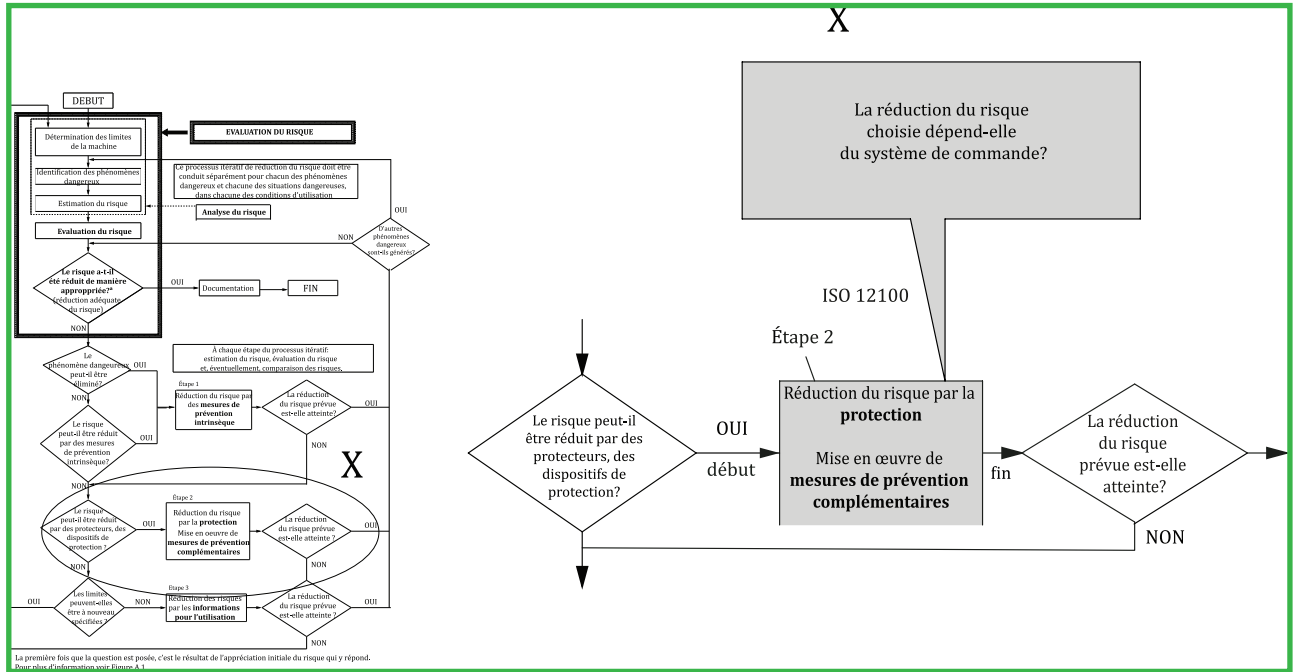
La réduction du risque selon l'ISO 12100:2010, Article 6, s'effectue en appliquant, dans la séquence suivante, les mesures de prévention intrinsèque, les mesures de sauvegarde et/ou de réduction du risque complémentaires et les informations pour l'utilisation. Un concepteur peut réduire les risques au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

~~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 2).~~

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 probabilité fréquence de défaillance dangereuse des fonctions de sécurité dépend de plusieurs facteurs, tels que y compris, mais sans y être limité, la structure matérielle et logicielle du système, étendue 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.

~~Afin d'aider le concepteur et l'estimation~~ Pour faciliter la conception des SRP/CS et l'évaluation du PL atteint, la présente partie de l'ISO 13849 définit une approche reposant sur la classification des structures selon 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 spécifiés en cas spécifié dans des conditions de défaut. Ces catégories architectures sont classées en cinq niveaux, appelés Catégories 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 ~~et les catégories peuvent s'appliquer aux parties d'un système de commande relatives à la sécurité telles que~~ peuvent être appliqués à la SRP/CS, par exemple:

- ~~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 continue**);
- les dispositifs de ~~commande de l'énergie~~ **protection électrosensibles** (par exemple ~~relais, distributeurs, etc.~~), **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).

~~ainsi qu'aux systèmes de commande exécutant des fonctions de sécurité pour tout type de machines, de la plus simple~~ Les machines couvertes par le présent document vont des plus simples (par exemple ~~matériel, petits électroménagers de cuisine ou portes et barrières portails automatiques~~) aux ~~installations manufacturières plus complexes~~ (par exemple, machines ~~d'emballage d'emballage, machines d'impression, presses d'impression, presses, et machines intégrées dans un système~~).

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 IEC 62061 et la présente partie de l'ISO 13849

~~Le présent document et l'IEC 62061 et la présente partie de l'ISO 13849 spécifient les exigences pour~~ **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.** ~~L'utilisation 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. L'ISO/TR 23849 donne les lignes directrices relatives à l'application de l'ISO 13849-1 et de l'IEC 62061 pour la conception des systèmes de commande des machines relatifs à la sécurité.~~

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

~~La présente partie de l'ISO 13849~~ Le présent document spécifie une méthodologie et fournit des exigences de sécurité, des recommandations et des conseils relatifs aux principes de conception et d'intégration portant sur la conception et l'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 qui réalisent des fonctions de sécurité. Elle s'applique aux SRP/CS pour le mode de demande élevée et le mode continu, indépendamment du type de technologie et d'énergie utilisé (électrique, hydraulique, pneumatique mécanique, etc.), quelques soient les machines, 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.

~~Elle~~ Le présent document ne spécifie pas ~~quelles~~les fonctions de sécurité et ~~quels~~les niveaux de performance requis (PL_r) qui 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).

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.

~~Elle~~ Le présent document ne donne pas ~~d'exigences~~d'exigences spécifiques pour la conception de produits/composants intégrés dans les SRP/CS. Néanmoins, les principes donnés, tels que les catégories ou les niveaux de performance, peuvent être utilisés. Les exigences spécifiques pour la conception de certains composants de SRP/CS sont couvertes par les normes ISO et IEC applicables.

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 IEC 61061.

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

NOTE 4 3 Pour le logiciel embarqué relatif à la sécurité pour des composants de PL_r = e, voir la IEC 61508-3:1998, Article 7.

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 de références suivants sont indispensables pour l'application 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 l'édition citée s'applique. Pour les références non datées, la dernière édition de la publication à laquelle il est fait 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*

~~IEC 60050 191:1990, , Vocabulaire Électrotechnique International — Chapitre 191: Sûreté de fonctionnement et qualité de service. Amendé par IEC 60050 191 am1:1999 et IEC 60050 191 am2:2002:1999.~~

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: Prescriptions Exigences concernant les logiciels. Corrigé par IEC 61508 3/Cor.1:1999*

~~IEC 61508 4:2010, , Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité — Partie 4: Définitions et abréviations. Corrigé par IEC 61508 4/Cor.1:1999~~

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

~~IEC 62061:2012~~ 2021, *Sécurité des machines — Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

~~ISO/TR 22100 2:2013~~ IEC/IEEE 82079-1:2019, *Sécurité des machines — Relation avec l'ISO 12100 — Partie 2: Relation entre l'ISO 12100 et l'ISO 13849-1, Élaboration des informations d'utilisation (instructions d'utilisation) des produits — Partie 1: Principes et exigences générales*

~~ISO/TR 23849, , Lignes directrices relatives à l'application de l'ISO 13849-1 et de la CEI 62061 dans la conception des systèmes de commande des machines relatifs à la sécurité~~

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 et le IEC 60050 191, 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 ~~répond~~ réalise une *fonction de sécurité* (3.1.27) répondant à un ou des signaux d'entrée et ~~génère~~ générant un ou des signaux de sortie relatifs à la sécurité

Note 1 à l'article: Les parties ~~combinées~~ d'un système de commande relatives à la sécurité commencent ~~aux points~~ 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 ~~du~~ d'un contacteur).

~~Note 2 à l'article: Si un système de surveillance est utilisé pour les diagnostics, ceux-ci sont considérés comme des SRP/CS.~~

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) (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.]

ISO 13849-1:2023

<https://standards.iteh.ai/catalog/standards/sist/0ec4d0c2-c2ee-4bac-b69f-0a883595198b/iso-13849-1-2023>

3.1.2**3.1.4****catégorie**

classification ~~des parties~~ du *sous-système* (3.1.45) ~~relatives à la sécurité d'un système de commande liée à leur résistance aux défauts~~ liée à sa résistance aux *défauts* (3.1.8) et à ~~leur son~~ comportement consécutif à des défauts ~~et~~, 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).