NORME INTERNATIONALE

ISO 13849-2

Deuxième édition
2012-10-15

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

Partie 2: Validation

Safety of machinery — Safety-related parts of control systems — Part 2: Validation

Numéro de référence
ISO 13849-2:2012(F)

© ISO 2012



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2012

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
Web www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **iv**

Introduction ..... **v**

1 Domaine d'application **1**

2 Références normatives **1**

3 Termes et définitions **1**

4 Processus de validation **1**
4.1 Principes de validation 1
4.2 Plan de validation 3
4.3 Listes des défauts génériques 4
4.4 Listes des défauts spécifiques 4
4.5 Informations pour la validation 4
4.6 Rapport de validation 6

5 Validation par analyse **6**
5.1 Généralités 6
5.2 Techniques d'analyse 7

6 Validation par essais **7**
6.1 Généralités 7
6.2 Précision des mesures 8
6.3 Exigences supérieures 9
6.4 Nombre d'échantillons 9

7 Validation de la spécification des exigences de sécurité pour les fonctions de sécurité **9**

8 Validation des fonctions de sécurité **10**

9 Validation des niveaux de performance et des catégories **10**
9.1 Analyse et essais 10
9.2 Validation des spécifications relatives aux catégories 11
9.3 Validation du $MTTF_d$, de la DC_{avg} et de la CCF 13
9.4 Validation des mesures de prévention des défaillances systématiques relatives au niveau de performance et à la catégorie des SRP/CS 14
9.5 Validation du logiciel relatif à la sécurité 14
9.6 Validation et vérification du niveau de performance 15
9.7 Validation d'une combinaison de parties relatives à la sécurité 15

10 Validation des exigences d'environnement **16**

11 Validation des exigences de maintenance **16**

12 Validation de la documentation technique et des informations pour l'utilisation **17**

Annexe A (informative) **Outils de validation pour les systèmes mécaniques** **18**

Annexe B (informative) **Outils de validation pour les systèmes pneumatiques** **23**

Annexe C (informative) **Outils de validation pour les systèmes hydrauliques** **33**

Annexe D (informative) **Outils de validation pour les systèmes électriques** **42**

Annexe E (informative) **Exemple de validation du comportement des défauts et des moyens de diagnostic** **56**

Bibliographie **84**

© ISO 2012 – Tous droits réservés

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 13849-2 a été élaborée par le comité technique ISO/TC 199, *Sécurité des machines*.

Cette deuxième édition annule et remplace la première édition (ISO 13849-2:2003), qui a fait l'objet d'une révision technique pour correspondre à l'ISO 13849-1:2006. De plus, la nouvelle Annexe E fournit un exemple de la validation du comportement des défauts et des moyens de diagnostic.

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*

Les Annexes A à D sont fournies à titre informatif et sont organisées comme indiqué dans le Tableau 1.

Tableau 1 — Structure des Annexes A à D de la présente partie de l'ISO 13849

Annexe	Technologie	Liste des principes de sécurité de base	Liste des principes de sécurité éprouvés	Liste des composants éprouvés	Liste des défauts et exclusions de défaut
		Tableau(x)			
A	Mécanique	A.1	A.2	A.3	A.4, A.5
B	Pneumatique	B.1	B.2		B.3 à B.18
C	Hydraulique	C.1	C.2		C.3 à C.12
D	Électrique (y compris électronique)	D.1	D.2	D.3	D.4 à D.21

© ISO 2012 – Tous droits réservés

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), contenant 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 moyen de protection valable pour une large gamme de machines:

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

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

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.

Le présent document est une norme de type B1, telle que définie dans l'ISO 12100.

Les exigences du présent document peuvent faire l'objet de compléments ou être modifiées dans 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 conformément aux exigences de cette norme, les exigences de la norme de type C prévalent.

La présente partie de l'ISO 13849 spécifie le processus de validation, pour les fonctions, catégories et niveaux de performance de sécurité des parties des systèmes de commande relatives à la sécurité. Elle identifie que la validation des pièces relatives à la sécurité du système de commande peut être réalisée par une combinaison d'analyse (voir Article 5) et d'essai (voir Article 6), et spécifie les circonstances particulières dans lesquelles il convient d'effectuer l'essai.

La plupart des modes opératoires et des conditions de la présente partie de l'ISO 13849 s'appuient sur l'hypothèse que le mode opératoire simplifié pour l'estimation du niveau de performance (PL), décrit dans l'ISO 13849-1:2006, 4.5.4, est utilisé. La présente partie de l'ISO 13849 ne fournit pas de lignes directrices pour les situations dans lesquelles d'autres modes opératoires sont utilisés pour estimer la PL (par exemple la modélisation de Markov), auquel cas il se peut que certaines dispositions ne soient pas applicables et que des exigences supplémentaires soient nécessaires.

Des lignes directrices sur les principes généraux de conception (voir l'ISO 12100) des parties des systèmes de commande relatives à la sécurité indépendamment du type de technologie utilisé (électrique, hydraulique, pneumatique, mécanique, etc.) sont fournies dans l'ISO 13849-1. Cela comprend des descriptions de quelques fonctions de sécurité typiques, la détermination de leurs niveaux de performances exigés, et des conditions générales des catégories et niveaux de performance.

Dans la présente partie de l'ISO 13849, certaines des conditions de validation sont générales, tandis que d'autres sont spécifiques au type de technologie utilisé.

© ISO 2012 – Tous droits réservés

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

Partie 2: Validation

1 Domaine d'application

La présente partie de l'ISO 13849 spécifie les modes opératoires et conditions à suivre pour la validation par analyse et par essais

— des fonctions de sécurité spécifiées,

— de la catégorie atteinte, et

— du niveau de performance atteint

par les parties d'un système de commande relatives à la sécurité (SRP/CS) conçu conformément à l'ISO 13849-1.

NOTE Des exigences supplémentaires pour les systèmes électroniques programmables, y compris les logiciels intégrés, sont données dans l'ISO 13849-1:2006, 4.6 et dans la série CEI 61508.

2 Références normatives

Les documents de référence 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 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 13849-1:2006, *Sécurité des machines — Parties des systèmes de commande relatives à la sécurité — Partie 1: Principes généraux de conception*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO 12100 et l'ISO 13849-1 s'appliquent.

4 Processus de validation

4.1 Principes de validation

Le but du processus de validation est de confirmer que la conception des SRP/CS soutient les exigences de sécurité globales des machines.

La validation doit démontrer que chaque SRP/CS remplit les exigences de l'ISO 13849-1 et, en particulier, les points suivants:

a) les caractéristiques de sécurité spécifiées des fonctions de sécurité assurées par cette partie, conformément au raisonnement de conception;

© ISO 2012 – Tous droits réservés