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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-6da54f2a0bfc/iso-13849-2-2012

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

© ISO 2012

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-6da54f2a0bfc/iso-13849-2-2012

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**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/8b0aa05-95aa-4f08-9137-6da54f2a0bfc/iso-13849-2-2012

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-
6ad54f2a0bfc/iso-13849-2-2012

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-6da54f2a0bfc/iso-13849-2-2012

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-6da54f2a0bfc/iso-13849-2-2012

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-
b4a5f2b0d0ac/iso-13849-2-2012

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

b) les exigences du niveau de performance spécifié (voir l'ISO 13849-1:2006, 4.5):

   1) les exigences de la catégorie spécifiée (voir l'ISO 13849-1:2006, 6.2),

   2) les mesures pour la maîtrise et la prévention des défaillances systématiques (voir l'ISO 13849-1:2006, Annexe G),

   3) le cas échéant, les exigences du logiciel (voir l'ISO 13849-1:2006, 4.6),

   4) l'aptitude à exécuter une fonction de sécurité dans des conditions d'environnement prévues;

c) la conception ergonomique de l'interface opérateur, en empêchant, par exemple, que l'opérateur ne soit tenté d'agir de manière dangereuse, en neutralisant le SRP/CS par exemple (voir l'ISO 13849-1:2006, 4.8).

Il convient que la validation soit effectuée par des personnes qui sont indépendantes de la conception système de commande (SRP/CS).

NOTE «Personne indépendante» ne veut pas nécessairement dire qu'une tierce partie soit exigée pour l'essai.

La validation consiste en l'application d'une analyse (voir Article 5) et la réalisation d'essais de fonctionnement (voir Article 6) dans les conditions prévisibles, conformément au plan de validation. La Figure 1 donne une vue d'ensemble du processus de validation. Le dosage entre l'analyse et les essais dépend de la technologie utilisée pour les parties relatives à la sécurité et du niveau de performance exigé. Pour les catégories 2, 3 et 4, la validation de la fonction de sécurité doit également inclure des essais dans les conditions de défaut.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Il convient que l'analyse soit entreprise aussi tôt que possible et en parallèle avec le processus de conception. Les problèmes peuvent être corrigés précocement pendant qu'il est encore relativement aisé de le faire, c'est-à-dire durant les phases «Conception et réalisation technique des fonctions de sécurité» et «Déterminer le niveau de performance PL» (cadres 4 et 5 de la Figure 3 de l'ISO 13849-1:2006). Il peut être nécessaire de retarder certaines parties de l'analyse jusqu'à ce que la conception soit bien avancée.

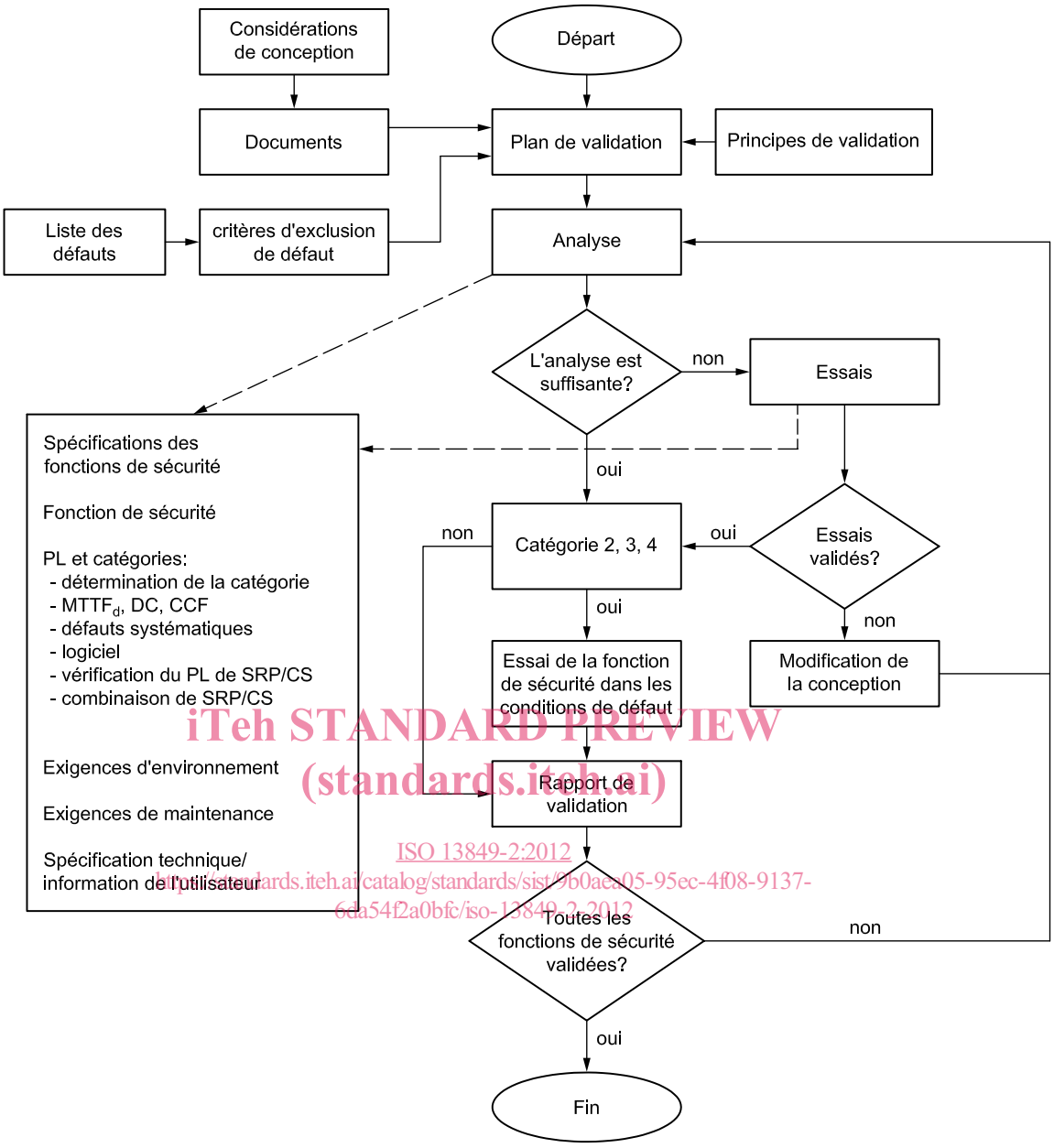
ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea03-95ec-4108-9137-6da54f2a0bfc/iso-13849-2-2012

Si cela est nécessaire en raison de la taille du système, de la complexité ou des effets de l'intégration au système de commande (de la machine), il convient d'adopter des dispositions particulières pour

— la validation des SRP/CS séparément avant l'intégration, y compris la simulation des signaux d'entrée et de sortie appropriés, et

— la validation des effets de l'intégration des parties relatives à la sécurité au reste du système de commande dans le contexte de son utilisation dans la machine.

 © ISO 2012 – Tous droits réservés



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-6da54f2a0bfc/iso-13849-2-2012

Figure 1 — Vue d'ensemble du processus de validation

«Modification de la conception» dans la Figure 1 se rapporte au processus de conception. Si la validation ne peut pas être effectuée avec succès, il est nécessaire de modifier la conception. Il convient de répéter la validation des parties modifiées relatives à la sécurité. Il convient de réitérer ce processus jusqu'à ce que toutes les parties relatives à la sécurité des fonctions de sécurité aient été validées.

4.2 Plan de validation

Le plan de validation doit identifier et décrire les exigences de mise en œuvre du processus de validation des fonctions de sécurité spécifiées, de leurs catégories et de leurs niveaux de performance.

Le plan de validation doit également identifier les moyens à employer pour valider les fonctions de sécurité spécifiées, les catégories et les niveaux de performance. Lorsque cela est approprié, il doit établir:

a) l'identité des documents de spécification;

b) les conditions de fonctionnement et d'environnement pendant les essais;

c) les analyses et les essais à réaliser;

d) la référence aux normes d'essai à appliquer;

e) les personnes ou parties responsables de chaque partie de la validation.

Pour les parties relatives à la sécurité qui ont été validées précédemment pour la même spécification, une référence à cette précédente validation suffit.

4.3 Listes des défauts génériques

Le processus de validation implique l'examen du comportement des SRP/CS pour tous les défauts à considérer. Une base pour la considération des défauts est donnée dans les tableaux des listes de défauts dans les Annexes A à D, qui s'appuient sur l'expérience et qui comprennent:

— les composants/éléments à inclure, par exemple les conducteurs/câbles (voir l'Annexe D);

— les défauts à prendre en compte, par exemple les courts-circuits entre conducteurs;

— les exclusions de défaut autorisées en tenant compte des aspects environnementaux, fonctionnels et d'application;

— une section de remarques justifiant les exclusions de défaut.

Dans les listes de défauts, seuls les défauts permanents sont pris en compte.

4.4 Listes des défauts spécifiques

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Si nécessaire une liste des défauts spécifiques se rapportant au produit doit être établie pour servir de document de référence au processus de validation de la (des) partie(s) relative(s) à la sécurité. La liste peut s'appuyer sur la (les) liste(s) générique(s) appropriée(s) données dans les annexes.

ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-
6825f4a0b0ca/iso-13849-2-2012

Lorsque la liste des défauts spécifiques se rapportant au produit est basée sur une (des) liste(s) générique(s), elle doit mentionner:

a) les défauts extraits de la (des) liste(s) générique(s) à inclure;

b) tout autre défaut pertinent à inclure mais non donné dans la liste générique (par exemple défaillances de cause commune);

c) les défauts extraits de la (des) liste(s) générique(s) qu'il est possible d'exclure sur la base de la satisfaction des critères donnés dans la (les) liste(s) générique(s) (voir l'ISO 13849-1:2006, 7.3);

et, exceptionnellement

d) tous les autres défauts pour lesquels la (les) liste(s) générique(s) ne permet(tent) pas d'exclusion, mais pour lesquels une justification et un raisonnement pour exclusion sont présentés (voir l'ISO 13849-1:2006, 7.3).

Lorsque cette liste n'est pas basée sur une (des) liste(s) générique(s), le concepteur doit donner la justification pour les exclusions de défaut.

4.5 Informations pour la validation

Les informations requises pour la validation varient avec la technologie utilisée, la (les) catégorie(s) et le(s) niveau(x) de performance à démontrer, le raisonnement suivi lors de la conception du système et la contribution des SRP/CS à la réduction des risques. Les documents contenant des informations suffisantes et issus de la liste suivante doivent être inclus dans le processus de validation afin de

 © ISO 2012 – Tous droits réservés

démontrer que des parties relatives à la sécurité exécutent les fonctions de sécurité spécifiées par le(s) niveau(x) de performance et catégorie(s) exigés:

a) spécification des caractéristiques requises de chaque fonction de sécurité, sa catégorie et son niveau de performance requis;

b) plans et spécifications, par exemple pour les parties mécaniques, hydrauliques et pneumatiques, cartes de circuits intégrés et cartes assemblées, câblage intérieur, enveloppe, matériaux, montage;

c) schéma(s) fonctionnel(s) avec description fonctionnelle des blocs;

d) schéma(s) de circuits y compris les interfaces/connexions;

e) description fonctionnelle du (des) schéma(s) de circuits;

f) diagramme(s) séquentiel(s) des composants de commutation, signaux relatifs à la sécurité;

g) description des caractéristiques pertinentes des composants préalablement validés;

h) pour les parties relatives à la sécurité autres que celles listées en g), listes des composants avec désignation des éléments, valeurs nominales, tolérances, contraintes en fonctionnement pertinentes, désignation du type, données relatives au taux de défaillance, fabricant des composants et toute autre donnée relative à la sécurité;

i) analyse de tous les défauts pertinents (voir aussi 4.3 et 4.4), tels que ceux énumérés dans les tableaux des Annexes A à D, y compris la justification de toute exclusion de défaut;

j) analyse de l'influence des matériaux traités;

k) informations pour l'utilisation, par exemple le manuel d'installation et d'exploitation/notice d'emploi.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-6da5412a0b1c/iso-13849-2-2012

Lorsque cela est approprié, la documentation relative au logiciel doit inclure:

— une spécification claire, et sans ambiguïté établissant les performances de sécurité que le logiciel doit réaliser;

— la preuve que le logiciel est conçu pour réaliser les performances de sécurité requises (voir 9.5);

— les détails des essais (en particulier les rapports d'essai) effectués pour prouver que les performances de sécurité requises sont réalisées.

NOTE Voir l'ISO 13849-1:2006, 4.6.2 et 4.6.3, pour les exigences.

Des informations sont nécessaires concernant la manière de déterminer le niveau de performance et la probabilité moyenne d'une défaillance dangereuse par heure. La documentation des aspects quantifiables doit comprendre:

— le diagramme bloc relatif à la sécurité (voir l'ISO 13849-1:2006, Annexe B) ou l'architecture désignée (voir l'ISO 13849-1:2006, 6.2);

— la détermination du $MTTF_d$, de la DC_{avg} et de la CCF;

— la détermination de la catégorie (voir Tableau 2).

Des informations sont requises pour la documentation des aspects systématiques des SRP/CS.

Des informations sont requises concernant la manière dont l'association de plusieurs SRP/CS réalise un niveau de performance conforme au niveau de performance exigé.

© ISO 2012 – Tous droits réservés

Tableau 2 — Exigences de documentation pour les catégories en tant que partie des niveaux de performance

Exigence de documentation	Catégorie pour laquelle une documentation est requise				
	B	1	2	3	4
Principes de sécurité de base	X	X	X	X	X
Contraintes de fonctionnement prévues	X	X	X	X	X
Influences du matériau traité	X	X	X	X	X
Performances sous d'autres influences extérieures	X	X	X	X	X
Composants éprouvés	—	X	—	—	—
Principes de sécurité éprouvés	—	X	X	X	X
Temps moyen avant défaillance dangereuse ($MTTF_d$) pour chaque canal	X	X	X	X	X
Procédure de contrôle de la (des) fonction(s) de sécurité	—	—	X	—	—
Mesures de diagnostic effectuées, y compris la réaction au défaut	—	—	X	X	X
Intervalles de contrôle, lorsque spécifiés	—	—	X	X	X
Couverture du diagnostic (DC_{avg})	—	—	X	X	X
Défauts uniques prévisibles pris en compte à la conception et méthode de détection utilisée	—	—	X	X	X
Défaillances de cause commune identifiées et mode de prévention	—	—	X	X	X
Exclusions de défauts uniques prévisibles	—	—	—	X	X
Défauts à détecter	—	—	X	X	X
Manière dont la fonction de sécurité est assurée pour chaque défaut	—	—	—	X	X
Manière dont la fonction de sécurité est assurée pour chaque combinaison de défauts	—	—	—	—	X
Mesures de prévention des défauts systématiques	X	X	X	X	X
Mesures de prévention des défauts logiciels	X	—	X	X	X
X documentation requise — aucune documentation requise					
NOTE Les catégories mentionnées dans le Tableau 2 sont celles données dans l'ISO 13849-1:2006.					

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-6da54f2a0bfc/iso-13849-2-2012

4.6 Rapport de validation

La validation par analyse et essais doit faire l'objet d'un rapport. Le rapport doit décrire le processus de validation de chaque exigence de sécurité. Il est possible de faire référence à de précédents rapports de validation, à condition qu'ils soient convenablement identifiés.

Pour toute partie relative à la sécurité qui a échoué à une partie du processus de validation, le rapport de validation doit indiquer quelle(s) partie(s) de l'analyse/des essais de validation a (ont) échoué. Toutes les parties relatives à la sécurité doivent être revalidées avec succès après leur modification.

5 Validation par analyse

5.1 Généralités

La validation des SRP/CS doit être réalisée par analyse. Les données d'entrée de l'analyse comprennent:

— la (les) fonctions de sécurité, leurs caractéristiques et le(s) niveau(x) de performance requis identifiés lors de l'analyse du risque (voir l'ISO 13849-1:2006, Figures 1 et 3);

 © ISO 2012 – Tous droits réservés

— les aspects quantifiables ($MTTF_d$, DC_{avg} et CCF);

— la structure du système (par exemple, les architectures désignées) (voir l'ISO 13849-1:2006, Article 6);

— les aspects non quantifiables et qualitatifs qui affectent le comportement du système (si applicable, les aspects du logiciel);

— les arguments déterministes.

La validation des fonctions de sécurité par analyse plutôt que par essais exige la formulation d'arguments déterministes.

NOTE 1 Un argument déterministe est un argument fondé sur des aspects qualitatifs (par exemple qualité de fabrication, expérience d'utilisation). Cette analyse dépend de l'application, qui, avec d'autres facteurs, peut affecter les arguments déterministes.

NOTE 2 Les arguments déterministes diffèrent des autres justifications en cela qu'ils montrent que les propriétés exigées du système découlent logiquement d'une modélisation du système. De tels arguments peuvent être construits sur la base de notions simples, bien comprises.

5.2 Techniques d'analyse

La sélection d'une technique d'analyse dépend d'un objectif particulier. Deux techniques fondamentales existent, comme indiqué ci-après.

a) Les techniques descendantes (déductives) conviennent pour déterminer les événements déclencheurs qui peuvent conduire à des événements supérieurs identifiés et pour calculer la probabilité des événements supérieurs à partir de la probabilité des événements déclencheurs. Elles peuvent également servir à rechercher les conséquences de défauts multiples identifiés.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

EXEMPLE Analyse par arbre des défaillances (ADD, voir la CEI 61025) et analyse par arbre des événements (AAE).

ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-6da54f2e0b6f/iso-13849-2-2012

b) Les techniques ascendantes (inductives) conviennent pour rechercher les conséquences de défauts uniques identifiés.

EXEMPLE Analyse des modes de défaillance et de leurs effets (AMDE, voir la CEI 60812) et analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC).

6 Validation par essais

6.1 Généralités

Lorsque la validation par analyse ne permet pas d'atteindre une conclusion, des essais doivent être réalisés pour achever la validation. Les essais sont toujours complémentaires à l'analyse et sont souvent nécessaires.

Les essais de validation doivent être programmés et réalisés de façon logique. En particulier:

a) un plan des essais doit être présenté avant le début des essais qui doit inclure:

   1) les spécifications des essais,

   2) les résultats d'essai exigés pour la conformité des essais, et

   3) la chronologie des essais;

b) des rapports d'essai doivent être fournis qui comprennent

   1) le nom de la personne ayant réalisé le contrôle,

   2) les conditions d'environnement (voir Article 10),

© ISO 2012 – Tous droits réservés

3) les procédures d'essais et les équipements utilisés,

4) la date de l'essai, et

5) les résultats d'essai;

c) les rapports d'essai doivent être comparés avec le plan des essais pour s'assurer que les objectifs de fonctionnement et de performances spécifiés sont atteints.

L'échantillon d'essai doit être utilisé dans des conditions aussi proches que possible de sa configuration opérationnelle définitive, c'est-à-dire avec tous les dispositifs périphériques et capots fixés.

Les essais peuvent être effectués manuellement ou automatiquement (par exemple par ordinateur).

Lorsqu'elle est pratiquée, la validation des fonctions de sécurité par essais doit être effectuée en introduisant des signaux d'entrée, combinés de diverses manières, dans les SRP/CS. La réponse résultant des données de sortie doit être comparée aux données de sortie spécifiées.

Il est recommandé d'appliquer systématiquement la combinaison de ces signaux d'entrée au système de commande et à la machine. Voici un exemple de cette logique: mise sous tension, mise en marche, fonctionnement, inversion de mouvement, remise en marche. Si nécessaire, une gamme étendue de données d'entrée doit être introduite pour prendre en compte les situations anormales ou inhabituelles et vérifier comment les SRP/CS répondent. Ces combinaisons de données d'entrée doivent prendre en compte tout dysfonctionnement prévisible.

Les objectifs de l'essai déterminent les conditions d'environnement pour cet essai. Il peut s'agir:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

— des conditions d'environnement pour l'utilisation prévue;

— des conditions spécifiques;

— d'une gamme donnée de conditions si une dérive est attendue.

ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aea05-95ec-4f08-9137-
b8e4ea0c0bb1/iso-13849-2-2012

Il convient que la plage de conditions considérée comme stable et dans laquelle les essais sont valides fasse l'objet d'un accord entre le concepteur et la (les) personne(s) responsable(s) de l'exécution des essais et soit inscrite dans le rapport.

6.2 Précision des mesures

La précision des mesures au cours de la validation par essais doit être adaptée à l'essai effectué. En général, ces précisions de mesure doivent être effectuées à 5 K pour les températures et à 5 % pour les mesures suivantes:

a) mesures de temps;

b) mesures de pression;

c) mesures de force;

d) mesures électriques;

e) mesures hygrométriques;

f) mesures linéaires.

Les écarts par rapport à ces précisions de mesure doivent être justifiés.

 © ISO 2012 – Tous droits réservés

6.3 Exigences supérieures

Si, selon la documentation d'accompagnement, les SRP/CS répondent à des exigences supérieures à celles de la présente partie de l'ISO 13849, les exigences supérieures doivent s'appliquer.

NOTE De telles exigences supérieures peuvent s'appliquer si le système de commande doit résister à des conditions de fonctionnement particulièrement difficiles, par exemple manipulation brutale, effets de l'humidité, hydrolyse, variations de la température ambiante, effets d'agents chimiques, corrosion, forte intensité de champs électromagnétiques, par exemple du fait de la proximité d'émetteurs.

6.4 Nombre d'échantillons

Sauf spécification contraire, les essais doivent être réalisés sur un seul échantillon de série de la (des) partie(s) relative(s) à la sécurité qui est (sont) soumise(s) à essai.

La (les) partie(s) relative(s) à la sécurité soumise(s) aux essais ne doi(ven)t pas être modifiée(s) au cours des essais.

Certains essais peuvent modifier de manière permanente les performances de certains composants. Lorsque la modification permanente d'un composant rend la partie relative à la sécurité incapable de remplir les exigences pour les autres essais, un ou plusieurs nouveaux échantillons doivent être utilisés pour les essais qui suivent.

Lorsqu'un essai particulier est destructif, et que des résultats équivalents peuvent être obtenus en procédant à des essais sur une partie isolée de la SRP/CS, un échantillon de cette partie relative à la sécurité peut être utilisé à la place de l'intégralité de la (des) partie(s) relative(s) à la sécurité pour parvenir aux résultats de l'essai. Cette approche ne doit être appliquée que lorsqu'il a été établi par l'analyse que l'essai de la (des) partie(s) relative(s) à la sécurité est suffisant pour démontrer les performances de sécurité de l'intégralité de la partie relative à la sécurité réalisant la fonction de sécurité.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 13849-2:2012
https://standards.iteh.ai/catalog/standards/sist/9b0aec95-95ce-4f08-8137-6da54f2a0bfc/iso-13849-2-2012

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

Avant la validation de la conception de la SRP/CS ou de la combinaison de SRP/CS réalisant la fonction de sécurité, la spécification des exigences pour la fonction de sécurité doit être vérifiée pour assurer l'uniformité et la perfection pour son usage prévu.

Il convient d'analyser la spécification des exigences de sécurité avant de commencer la conception, puisque toutes les autres activités s'appuient sur ces exigences.

La documentation des exigences pour toutes les fonctions de sécurité du système de commande de la machine doit être assurée.

Afin de valider la spécification, il convient d'appliquer des mesures appropriées de prévention des défauts systématiques (erreurs, omissions ou incohérences).

La validation peut être effectuée par des examens et des inspections des exigences de sécurité de la SRP/CS et de la (des) spécification(s) de conception; surtout pour prouver que tous les aspects

— des exigences pour les applications prévues et des besoins de sécurité, et

— des conditions de fonctionnement et d'environnement et des erreurs humaines possibles (par exemple une mauvaise utilisation)

ont été pris en considération.

Lorsqu'une norme de produit spécifie les exigences de sécurité pour la conception d'une SRP/CS (par exemple l'ISO 11161 pour les systèmes de fabrication intégrés ou l'ISO 13851 pour les dispositifs de commande bimanuelle), celles-ci doivent être prises en compte.

© ISO 2012 – Tous droits réservés