RAPPORT TECHNIQUE

ISO/TR 23849

Première édition
2010-05-01

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

Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery

Numéro de référence
ISO/TR 23849:2010(F)

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

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.

Exceptionnellement, lorsqu'un comité technique a réuni des données de nature différente de celles qui sont normalement publiées comme Normes internationales (ceci pouvant comprendre des informations sur l'état de la technique par exemple), il peut décider, à la majorité simple de ses membres, de publier un Rapport technique. Les Rapports techniques sont de nature purement informative et ne doivent pas nécessairement être révisés avant que les données fournies ne soient plus jugées valables ou utiles.

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/TR 23849 a été élaboré conjointement par le comité technique ISO/TC 199, *Sécurité des machines*, et le comité technique CEI/TC 44, *Sécurité des machines — Aspects électrotechniques*. Le projet a été soumis aux organismes nationaux de l'ISO et de la CEI pour vote. Les comités techniques concernés ont convenu de n'apporter aucune modification au présent Rapport technique sans accord mutuel.

Introduction

Le présent Rapport technique a été préparé par des experts du CEI/TC 44/GT 7 et de l'ISO/TC 199/GT 8 en réponse aux demandes de leurs comités techniques pour expliquer la relation entre la CEI 62061 et l'ISO 13849-1. Il est en particulier destiné à aider les utilisateurs de ces Normes internationales concernant les interactions qui peuvent exister entre les normes, afin de garantir que la conception des systèmes de sécurité élaborés conformément à l'une ou l'autre norme soit fiable.

Il est prévu d'intégrer le présent Rapport technique dans la CEI 62061 et dans l'ISO 13849-1, au moyen de rectificatifs faisant référence à la version publiée du présent document. Ces rectificatifs retireront également les informations du Tableau 1, *Utilisation recommandée de la CEI 62061 et de l'ISO 13849-1*, fournies dans l'introduction commune aux deux normes et aujourd'hui reconnues comme n'étant plus d'actualité. Par la suite, il est prévu de fusionner l'ISO 13849-1 et la CEI 62061 par le biais d'un groupe de travail mixte de l'ISO/TC 199 et du CEI/TC 44.

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

1 Domaine d'application

Le présent Rapport technique a pour objet d'expliquer l'application de la CEI 62061 et de l'ISO 13849-1[1)] dans la conception des systèmes de commande des machines relatifs à la sécurité.

2 Généralités

2.1 La CEI 62061 et l'ISO 13849-1 spécifient des exigences de conception et de mise en œuvre des systèmes de commande relatifs à la sécurité des machines[2)]. Les méthodes développées dans ces deux normes sont différentes mais, correctement mises en œuvre, elles permettent des réductions du risque comparables.

2.2 Ces normes classent les systèmes de commande relatifs à la sécurité mettant en œuvre des fonctions de sécurité selon des niveaux définis en termes de probabilité de défaillance dangereuse par heure. L'ISO 13849-1 possède cinq niveaux de performance (PL, *performance levels*), a, b, c, d et e, tandis que la CEI 62061 comprend trois niveaux d'intégrité de sécurité (SIL, *safety integrity levels*), 1, 2 et 3.

2.3 Les comités de normes de produit (type C) spécifient les exigences de sécurité pour les systèmes de commande relatifs à la sécurité et il est recommandé que ces comités classifient les «degrés de confiance» qu'ils requièrent en termes de PL et SIL.

2.4 Les concepteurs de machines sont libres d'utiliser soit la CEI 62061, soit l'ISO 13849-1, selon les caractéristiques spécifiques de l'application.

2.5 Il est fort probable que le choix et l'utilisation d'une norme plutôt que l'autre soient déterminés par exemple comme suit:

— le fait d'avoir des connaissances et une expérience préalables dans le domaine de la conception de systèmes de commande relatifs à la sécurité des machines qui reposent sur le concept des catégories décrites dans l'ISO 13849-1:1999 peut signifier que l'emploi de l'ISO 13849-1:2006 est plus approprié;

— des systèmes de commande relatifs à la sécurité dont le moyen d'action n'est pas électrique peuvent signifier que l'emploi de l'ISO 13849-1:2006 est plus approprié;

— le fait que le client réclame que l'intégrité de sécurité d'un système de commande de machine relatif à la sécurité soit démontrée en termes de SIL peut signifier que l'emploi de la CEI 62061 est plus approprié;

---

1) Le présent Rapport technique s'appuie sur l'ISO 13849-1:2006 plutôt que sur l'ISO 13849-1:1999 qu'elle remplace.

2) Ces normes ont été adoptées par les organismes européens de normalisation CEN et CENELEC sous les références respectives ISO 13849-1 et EN 62061, où elles ont le statut de normes harmonisées au titre de la transposition de la directive Machines (98/37/CE et 2006/42/CE). Dans les conditions de leur publication, l'utilisation correcte de l'une de ces deux normes implique la conformité aux exigences de sécurité essentielles de la directive Machines (98/37/CE et 2006/42/CE).

— le fait que les machines comprenant les systèmes de commande relatifs à la sécurité en question soient utilisées, par exemple dans les industries de transformation où d'autres systèmes relatifs à la sécurité (tels que des systèmes de sécurité conformes à la CEI 61511) sont définis en termes de SIL, peut signifier que l'emploi de la CEI 62061 est plus approprié.

3 Comparaison des normes

3.1 Une comparaison des exigences techniques de l'ISO 13849-1 et de la CEI 62061 a été menée sur les aspects suivants:

— terminologie;

— estimation du risque et détermination d'objectif de performance;

— spécification des exigences de sécurité;

— exigences d'intégrité systématique;

— fonctions de diagnostic;

— exigences de sécurité logicielle.

3.2 En outre, une évaluation de l'utilisation des formules mathématiques simplifiées pour déterminer la probabilité des défaillances dangereuses (PFH_D, *probability of a dangerous failure per hour*) et le temps moyen avant défaillance dangereuse ($MTTF_d$, *mean time to dangerous failure*) suivant les deux normes a aussi été effectuée.

3.3 Les conclusions de ce travail sont les suivantes.

— Les systèmes de commande relatifs à la sécurité peuvent être conçus de manière à atteindre des niveaux de sécurité fonctionnelle acceptables avec l'une ou l'autre norme, en intégrant des sous-systèmes de commande électriques relatifs à la sécurité (SRECS, *safety-related electrical control system*) ou des parties de systèmes de commande relatives à la sécurité (SRP/CS, *safety-related parts of a control system*) non complexes[3)] conçus respectivement conformément à la CEI 62061 et à l'ISO 13849-1.

— Ces deux normes peuvent également fournir des solutions de conception pour des SRECS et SRP/CS complexes en intégrant des sous-systèmes électriques/électroniques/programmables électroniques conçus conformément à la CEI 61508.

— Chaque norme est déjà appréciée par les utilisateurs du secteur des machines, qui tireront avantage de l'expérience acquise à l'usage. Une certaine période d'observation de leur application pratique est nécessaire à toute initiative future d'évolution vers une norme qui fusionne les contenus de la CEI 62061 et de l'ISO 13849-1.

— Des différences de détail existent et il est reconnu que certains concepts (par exemple celui de la gestion de la sécurité fonctionnelle) nécessitent encore du travail pour établir une équivalence entre les méthodologies de conception respectives et certaines exigences techniques.

3) Bien qu'il n'y ait aucune définition pour les termes SRECS ou SRP/CS «non complexes», il convient de le considérer comme l'équivalent de la faible complexité dans le contexte de la CEI 62061:2005, 3.2.7.

4 Estimation du risque et détermination de la performance requise

4.1 Une comparaison a été effectuée sur l'utilisation des méthodes pour attribuer un SIL et/ou un PL_r à une fonction de sécurité particulière. Elle a établi qu'il existe un bon niveau de correspondance entre les méthodes fournies dans l'Annexe A de chaque norme.

4.2 Il est important, quelle que soit la méthode utilisée, de veiller à ce que des jugements corrects soient émis sur les paramètres de risque pour déterminer le SIL et/ou PL_r supposé s'appliquer à une fonction de sécurité particulière. Ces jugements sont souvent plus justes lorsqu'ils sont émis par un panel de professionnels (par exemple des concepteurs, du personnel de maintenance, des opérateurs) pour s'assurer que les dangers éventuellement présents sur une machine soient bien compris.

4.3 D'autres renseignements sur le processus d'estimation du risque et de la détermination des objectifs de performance se trouvent dans l'ISO 14121-1 et la CEI 61508-5.

5 Spécification des exigences de sécurité

5.1 Dans l'ISO 13849-1 comme dans la CEI 62061, la première étape de la méthodologie consiste à préciser la (les) fonction(s) de sécurité que le système de commande relatif à la sécurité est censé remplir.

5.2 Il convient que, pour chaque fonction de sécurité remplie par un circuit de commande, une évaluation ait été réalisée s'appuyant, par exemple, sur l'Annexe A de l'ISO 13849-1 ou sur l'Annexe A de la CEI 62061. Il convient que cette évaluation ait déterminé quelle est la réduction du risque nécessaire pour chaque fonction de sécurité d'une machine et, ensuite, quel est le degré de confiance nécessaire pour le circuit de commande qui accomplit cette fonction de sécurité.

5.3 Le degré de confiance, spécifié sous forme de PL et/ou SIL, est attaché à une fonction de sécurité particulière.

5.4 Ci-après se trouvent les informations, relatives aux fonctions de sécurité, qu'il convient qu'une norme de produit (type C) fournisse.

Fonction(s) de sécurité qu'un circuit de commande doit remplir:

Nom de la fonction de sécurité

Description de la fonction

Niveau de performance requis conformément à l'ISO 13849-1: PL_r, a à e

et/ou

Intégrité de sécurité requise conformément à la CEI 62061: SIL, 1 à 3

6 Détermination des objectifs de performance: PL ou SIL

Le Tableau 1 donne la relation entre le PL et le SIL d'après la probabilité moyenne d'une défaillance dangereuse par heure. Les deux normes fournissent toutefois des exigences (par exemple d'intégrité de sécurité systématique) qui viennent s'ajouter à ces objectifs probabilistes et qui doivent aussi s'appliquer à un système de commande relatif à la sécurité. La rigueur de ces exigences dépend du PL et SIL en question.

Tableau 1 — Relation entre PL et SIL basée sur la probabilité moyenne d'une défaillance dangereuse par heure

Niveau de performance (PL)	Probabilité moyenne d'une défaillance dangereuse par heure (1/h)	Niveau d'intégrité de sécurité (SIL)
a	$\geqslant 10^{-5}$ à $< 10^{-4}$	Aucune exigence de sécurité particulière
b	$\geqslant 3 \times 10^{-6}$ à $< 10^{-5}$	1
c	$\geqslant 10^{-6}$ à $< 3 \times 10^{-6}$	1
d	$\geqslant 10^{-7}$ à $< 10^{-6}$	2
e	$\geqslant 10^{-8}$ à $< 10^{-7}$	3

7 Conception du système

7.1 Exigences générales pour la conception des système selon la CEI 62061 et l'ISO 13849-1

Lors de la conception d'un SRECS ou d'une SRP/CS, il convient de prendre en compte les aspects suivants.

— Lorsqu'elles sont appliquées dans les limites de leur domaine d'application, les deux normes peuvent servir à concevoir des systèmes de commande relatifs à la sécurité avec une sécurité fonctionnelle acceptable, indiquée par le PL ou le SIL obtenu.

— Les parties non complexes relatives à la sécurité, conçues pour atteindre le PL approprié conformément à l'ISO 13849-1, peuvent être intégrées en tant que sous-système dans un système de commande électrique relatif à la sécurité (SRECS) conçu conformément à la CEI 62061. Toute partie complexe relative à la sécurité, conçue pour atteindre le PL approprié conformément à l'ISO 13849-1, peut être intégrée dans les pièces relatives à la sécurité d'un système de commande (SRP/SC) conçu conformément à l'ISO 13849-1.

— Tout sous-système non complexe conçu conformément à la CEI 62061 pour atteindre le SIL approprié peut être intégré en tant que pièce(s) relative(s) à la sécurité dans une combinaison de SRP/SC conçue conformément à l'ISO 13849-1.

— Tout sous-système complexe conçu conformément à la CEI 61508 pour atteindre le SIL approprié peut être intégré en tant que pièce(s) relative(s) à la sécurité dans une combinaison de SRP/SC conçue conformément à l'ISO 13849-1 ou en tant que sous-système dans un SRECS conçu conformément à la CEI 62061.

7.2 Estimation de la PFH_D et du $MTTF_d$ et utilisation des exclusions d'anomalie

7.2.1 PFH_D et $MTTF_d$

7.2.1.1 Dans le contexte de l'ISO 13849-1, la valeur du $MTTF_d$ correspond à une SRP/CS à canal unique sans diagnostic et, dans ce cas seulement, est l'inverse de la PFH_D de la CEI 62061.

7.2.1.2 Le $MTTF_d$ est un paramètre de composant et/ou de canal unique ne tenant aucun compte de facteurs tels que le diagnostic et l'architecture, tandis que la PFH_D est un paramètre de sous-système qui prend en compte la contribution de ces facteurs, selon la structure de conception.

7.2.1.3 L'Annexe K de l'ISO 13849-1 décrit la relation entre le $MTTF_d$ et la PFH_D d'une SRP/CS, pour différentes architectures classées en termes de catégorie et de couverture du diagnostic (DC, *diagnostic coverage*).

7.2.1.4 L'estimation de la PFH_D pour une combinaison de SRP/CS en série conforme à l'ISO 13849-1 peut aussi être réalisée en ajoutant des valeurs de PFH_D (par exemple déduites de l'Annexe K de l'ISO 13849-1) de chaque SRP/CS d'une manière similaire à celle utilisée avec des sous-systèmes dans la CEI 62061.

7.2.2 Usage des exclusions d'anomalie

7.2.2.1 Chacune des deux normes permet l'usage des exclusions d'anomalie (voir la CEI 62061, 6.7.7, et l'ISO 13849-1, 7.3). La CEI 62061 ne permet pas l'utilisation d'exclusions d'anomalie pour un SRECS sans tolérance aux anomalies matérielles devant atteindre un SIL 3 sans tolérance aux anomalies matérielles.

7.2.2.2 Lorsque des exclusions d'anomalie sont utilisées, il est important qu'elles soient correctement justifiées et valables pour la durée de vie prévue d'une SRP/CS ou d'un SRECS.

7.2.2.3 En général, lorsque, pour une fonction de sécurité devant être accomplie par une SRP/CS ou un SRECS, le niveau PL e ou SIL 3 est exigé, il n'est pas acceptable de s'appuyer uniquement sur les exclusions d'anomalies pour atteindre ce niveau de performance. Cela dépend de la technologie utilisée et de l'environnement de fonctionnement prévu. Il est donc essentiel que le concepteur accorde un soin supplémentaire à l'usage des exclusions d'anomalie en même temps que le PL ou SIL augmente.

7.2.2.4 En général, les exclusions d'anomalies ne sont pas applicables aux aspects mécaniques des interrupteurs électromécaniques de fin de course et des interrupteurs à commande manuelle (par exemple dispositif d'arrêt d'urgence) dans l'obtention du niveau PL e ou SIL 3 lors de la conception d'une SRP/CS ou d'un SRECS. Les exclusions d'anomalies qui peuvent être appliquées à des conditions de défaut mécanique particulières (par exemple usure/corrosion, rupture) sont décrites dans l'ISO 13849-2.

7.2.2.5 Par exemple, un système d'inter-verrouillage de porte qui doit atteindre le PL e ou le SIL 3 aura besoin de posséder une tolérance minimale aux anomalies égale à 1 (par exemple avec deux interrupteurs de fin de course mécaniques conventionnels) pour atteindre ce niveau de performance, car il n'est normalement pas justifiable d'exclure des anomalies telles que des actionneurs d'interrupteurs cassés. Il peut toutefois être acceptable d'exclure des anomalies telles que le court-circuit de câblage dans un tableau de commande conforme aux normes pertinentes.

7.2.2.6 La prochaine révision de l'ISO 13849-2 actuellement en cours d'élaboration par l'ISO/TC 199/GT 8 apportera davantage de renseignements sur l'usage des exclusions d'anomalie.

7.3 Conception de système à partir de sous-systèmes ou de SRP/CS conformes à la CEI 62061 ou à l'ISO 13849-1

7.3.1 Dans tous les cas où des sous-systèmes ou des parties de système de commande relatives à la sécurité sont conçus conformément à l'ISO 13849-1 ou à la CEI 62061, la conformité à la norme relative au niveau de système ne peut être affirmée que si toutes les exigences de la norme relative au niveau de système (selon le cas) sont satisfaites.

7.3.2 Pour la conception d'un sous-système ou d'une partie de système de commande relative à la sécurité, soit la CEI 62061, soit l'ISO 13849-1, respectivement, doit être observée. Il est permis de satisfaire plus d'une de ces normes à condition que les normes utilisées soient entièrement respectées.

7.3.3 Lors de la conception d'un sous-système ou d'une partie de système de commande relative à la sécurité, il n'est pas permis de mélanger les exigences des normes.

7.4 Conception de système à partir de sous-systèmes ou de SRP/CS conçus d'après d'autres normes CEI ou ISO

7.4.1 Il est possible de choisir des sous-systèmes, par exemple des matériels de protection électro-sensibles, de conception conforme aux normes de produit CEI ou ISO correspondantes et à l'une ou l'autre des normes CEI 61508, CEI 62061 ou ISO 13849-1. Il convient que le(s) vendeur(s) de ces types de