NORME INTERNATIONALE

ISO 13849-1

Troisième édition
2015-12-15

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

Numéro de référence
ISO 13849-1:2015(F)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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 (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour l'élaboration du 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 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. 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 sur la liste ISO des déclarations de brevets reçues (voir www.iso.org/patents).

Les éventuelles appellations commerciales utilisées dans le présent document sont données pour information à l'intention des utilisateurs et ne constituent pas une approbation ou une recommandation.

Pour une explication de 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 aux principes de l'OMC concernant les obstacles techniques au commerce (OTC) voir le lien URL suivant: Foreword - Supplementary information

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

Cette troisième édition annule et remplace la deuxième édition (ISO 13849-1:2006), dont elle constitue une révision technique. Elle comprend également le Rectificatif Technique ISO 13849-1:1/Cor 1:2009. Les modifications par rapport à l'édition précédentes incluent

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

— mise à jour et ajout de références normatives,

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

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

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

— 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.

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*

Introduction

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

a) **normes de type A** (normes fondamentales de sécurité), précisant des notions fondamentales, des principes de conception et des aspects généraux relatifs aux machines;

b) **normes de type B** (normes génériques de sécurité), traitant d'un aspect de la sécurité ou d'un type de dispositif conditionnant la sécurité valable pour toutes les machines ou pour une large gamme de machines:

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

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

c) **normes de type C** (normes de sécurité par catégorie de machines), traitant des exigences de sécurité détaillées s'appliquant à une machine particulière ou à un groupe de machines particulier.

La présente partie de l'ISO 13849 est une norme de type B1 telle que définie dans l'ISO 12100.

Lorsque des dispositions de la norme de type C diffèrent de celles indiquées dans une norme de type A ou B, ces dispositions prévalent sur celles des autres normes, et ce pour les machines conçues et fabriquées conformément aux spécifications de la norme de type C.

La présente partie de l'ISO 13849 est destinée à donner des conseils au cours de la conception et de l'évaluation des systèmes de commande ainsi qu'aux Comités Techniques élaborant des normes de type B2 ou de type C présumées conformes aux exigences essentielles de sécurité de l'Annexe I de la Directive 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.

Les parties des systèmes de commande de machines affectées à la réalisation des fonctions de sécurité sont appelées parties d'un système de commande relatives à la sécurité (SRP/CS), et peuvent être constituées de matériels et de logiciels et peuvent être séparées ou intégrées au système de commande. En plus de fournir des fonctions de sécurité, les SRP/CS peuvent faire partie d'une fonction opérationnelle (par exemple commandes bimanuelles comme moyen de mise en marche d'un cycle ou d'un processus).

L'aptitude des parties relatives à la sécurité à exécuter une fonction de sécurité dans des conditions prévisibles est classée en cinq niveaux appelés niveaux de performance (PL). Ces niveaux de performance sont définis en termes de probabilité de défaillance dangereuse du système (voir Tableau 2).

La probabilité de défaillance dangereuse des fonctions de sécurité dépend de plusieurs facteurs, tels que structure matérielle et logicielle du système, étendue des mécanismes de détection des défauts [couverture du diagnostic (DC)], fiabilité des composants [temps moyen avant défaillance dangereuse ($MTTF_D$), défaillance de cause commune (CCF)], processus de conception, contrainte de fonctionnement, conditions environnementales et méthodes de fonctionnement.

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

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

— les équipements de protection (par exemple dispositifs de commande bimanuelle, dispositifs de verrouillage), dispositifs de protection électrosensibles (par exemple barrières photoélectriques), dispositifs sensibles à la pression,

— les unités de commande (par exemple unité logique pour les fonctions de commande, traitement des données, surveillance, etc.), et

— les dispositifs de commande de l'énergie (par exemple relais, distributeurs, etc.),

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

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

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

L'IEC 62061 et la présente partie de l'ISO 13849 spécifient les exigences pour 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.

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

Partie 1: Principes généraux de conception

1 Domaine d'application

La présente partie de l'ISO 13849 fournit des exigences de sécurité et des conseils relatifs aux principes de conception et d'intégration des parties des systèmes de commande relatives à la sécurité (SRP/CS) incluant la conception du logiciel. Pour ces parties, elle spécifie les caractéristiques, incluant le niveau de performance requis, pour réaliser ces fonctions de sécurité. Elle s'applique aux SRP/CS 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.

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

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

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

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

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

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

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

2 Références normatives

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

ISO 12100:2010, *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.

IEC 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité — Partie 3:Prescriptions concernant les logiciels*. Corrigée 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 62061:2012, *Sécurité des machines — Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*

ISO/TR 22100-2:2013, *Sécurité des machines — Relation avec l'ISO 12100 — Partie 2: Relation entre l'ISO 12100 et l'ISO 13849-1*

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 et la IEC 60050-191 ainsi que les suivants s'appliquent.

3.1.1
partie d'un système de commande relative à la sécurité
SRP/CS
partie d'un système de commande qui répond à des signaux d'entrée et génère des signaux de sortie relatifs à la sécurité

Note 1 à l'article: Les parties combinées d'un système de commande relatives à la sécurité commencent aux points où sont générés les signaux relatifs à la sécurité (y compris, par exemple, la came de commande et le galet de l'interrupteur de position) et se terminent à la sortie des pré-actionneurs (y compris, par exemple, les contacts principaux du contacteur).

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

3.1.2
catégorie
classification des parties relatives à la sécurité d'un système de commande liée à leur résistance aux défauts et à leur comportement consécutif à des défauts et qui est obtenue par l'architecture des parties, la détection des défauts et/ou leur fiabilité

3.1.3
défaut
état d'une entité caractérisée par son inaptitude à accomplir une fonction requise, non comprise l'inaptitude due à la maintenance préventive ou à d'autres actions programmées, ou due à un manque de moyens extérieurs

Note 1 à l'article: Un défaut est souvent le résultat d'une défaillance de l'entité elle-même, mais il peut exister sans défaillance préalable.

Note 2 à l'article: Dans la présente partie de l'ISO 13849, le terme «défaut» signifie «défaut aléatoire».

[SOURCE: IEC 60050-191:1990, 05-01.]

3.1.4
défaillance
cessation de l'aptitude d'une entité à accomplir une fonction requise

Note 1 à l'article: Après défaillance d'une entité, cette entité a un défaut.

Note 2 à l'article: Une défaillance est un passage d'un état à un autre, par opposition à un défaut qui est un état.

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

Note 4 à l'article: Les défaillances n'affectant que la disponibilité du processus commandé ne sont pas couvertes par le domaine d'application de la présente partie de l'ISO 13849.

[SOURCE: IEC 60050-191:1990, 04-01.]

3.1.5
défaillance dangereuse
défaillance qui peut potentiellement mettre une SRP/CS dans un état dangereux ou défectueux

Note 1 à l'article: La réalisation ou non du «potentiellement» peut dépendre de l'architecture de canal du système; dans des systèmes redondants, une défaillance dangereuse du système matériel présente moins de risque d'aboutir à un état global dangereux ou défectueux.

[SOURCE: IEC 61508-4:1998, 3.6.7, modifiée.]

3.1.6
défaillance de cause commune
CCF
défaillances qui affectent plusieurs entités à partir d'un même événement et qui ne résultent pas les unes des autres

Note 1 à l'article: Il convient de ne pas confondre les défaillances de cause commune et les défaillances de mode commun (voir l'ISO 12100:2010, 3.36).

[SOURCE: IEC 60050-191:1990-am1:1999, 04-23.]

3.1.7
défaillance systématique
défaillance associée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés

Note 1 à l'article: La maintenance corrective sans modification n'élimine pas, habituellement, la cause de la défaillance.

Note 2 à l'article: Une défaillance systématique peut être induite en simulant la cause de la défaillance.

Note 3 à l'article: Exemples de causes de défaillances systématiques incluant les erreurs humaines dans

— la spécification des exigences de sécurité;

— la conception, la fabrication, l'installation et l'exploitation du matériel;

— la conception, la mise en œuvre, etc., du logiciel.

[SOURCE: IEC 60050-191:1990, 04-19]

3.1.8
inhibition
interruption automatique et temporaire de fonction(s) de sécurité par les SRP/CS

3.1.9
réarmement manuel
fonction interne aux SRP/CS permettant de rétablir manuellement des fonctions de sécurité données avant la remise en marche d'une machine

3.1.10
dommage
blessure physique ou atteinte à la santé

[SOURCE: ISO 12100:2010, 3.5]

3.1.11
phénomène dangereux
source potentielle de dommage

Note 1 à l'article: L'expression «phénomène dangereux» peut être qualifiée de manière à faire apparaître l'origine (par exemple phénomène dangereux mécanique, phénomène dangereux électrique) ou la nature du dommage potentiel (par exemple risque de choc électrique, de coupure, d'intoxication, d'incendie).

Note 2 à l'article: Le phénomène dangereux envisagé dans cette définition

— est présent en permanence pendant l'utilisation normale de la machine (par exemple déplacement d'éléments mobiles dangereux, arc électrique pendant une phase de soudage, mauvaise posture, émission de bruit, température élevée), ou

— peut apparaître de manière inattendue (par exemple explosion, risque d'écrasement résultant d'une mise en marche intempestive/inattendue, projection résultant d'une rupture, chute résultant d'une accélération ou d'une décélération).

[SOURCE: ISO 12100:2010, 3.6, modifiée.]

3.1.12
situation dangereuse
situation dans laquelle une personne est exposée à au moins un phénomène dangereux

Note 1 à l'article: L'exposition peut entraîner un dommage, immédiatement ou à long terme.

[SOURCE: ISO 12100:2010, 3.10]

3.1.13
risque
combinaison de la probabilité d'un dommage et de la gravité de ce dommage

[SOURCE: ISO 12100:2010, 3.12]

3.1.14
risque résiduel
risque subsistant après que des mesures de prévention ont été prises

Note 1 à l'article: Voir Figure 2.

[SOURCE: ISO 12100:2010, 3.17, modifiée.]

3.1.15
appréciation du risque
processus global d'analyse et d'évaluation du risque

[SOURCE: ISO 12100:2010, 3.17]

3.1.16
analyse du risque
combinaison de la détermination des limites de la machine, de l'identification des phénomènes dangereux et de l'estimation du risque

[SOURCE: ISO 12100:2010, 3.15]

3.1.17
évaluation du risque
jugement destiné à établir, à partir de l'analyse du risque, si les objectifs de réduction du risque ont été atteints

[SOURCE: ISO 12100:2010, 3.16]

3.1.18
utilisation normale d'une machine
utilisation d'une machine conformément aux indications données dans les instructions pour l'utilisation

[SOURCE: ISO 12100:2010, 3.23]

3.1.19
mauvais usage raisonnablement prévisible
utilisation d'une machine d'une manière ne correspondant pas aux intentions du concepteur, mais pouvant résulter d'un comportement humain aisément prévisible

[SOURCE: ISO 12100:2010, 3.24]

3.1.20
fonction de sécurité
fonction d'une machine dont la défaillance peut provoquer un accroissement immédiat du (des) risque(s)

[SOURCE: ISO 12100:2010, 3.30]

3.1.21
surveillance continue
fonction de sécurité assurant qu'une mesure de prévention est initiée si l'aptitude d'un composant ou d'un élément à exécuter sa fonction diminue ou si les conditions de fonctionnement sont modifiées de telle façon qu'il en résulte une diminution de la réduction du risque

3.1.22
système électronique programmable
PES
système de commande, de protection ou de surveillance reposant sur un ou plusieurs dispositifs électroniques programmables, y compris tous les éléments du système tels que les alimentations en énergie, les capteurs et autres dispositifs d'entrée, jusqu'aux actionneurs et autres dispositifs de sortie

[SOURCE: IEC 61508-4:1998, définition 3.3.2, modifiée.]

3.1.23
niveau de performance
PL
niveau discret d'aptitude de parties relatives à la sécurité à réaliser une fonction de sécurité dans des conditions prévisibles

Note 1 à l'article: Voir 4.5.1.

3.1.24
niveau de performance requis
PL_r
niveau de performance (PL) permettant d'atteindre la réduction du risque requise pour chaque fonction de sécurité

Note 1 à l'article: Voir Figures 2 et A.1.

3.1.25
temps moyen avant défaillance dangereuse
$MTTF_D$
valeur probable de la durée moyenne avant défaillance dangereuse

[SOURCE: IEC 62061:2005, 3.2.34, modifiée.]

3.1.26
couverture du diagnostic
DC
mesure de l'efficacité du diagnostic, peut être définie comme la fraction de la probabilité de défaillances dangereuses détectées sur la probabilité de toutes les défaillances dangereuses

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

[SOURCE: IEC 61508-4:1998, 3.8.6, modifiée.]

3.1.27
mesure de prévention
mesure destinée à réduire le risque

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

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

[SOURCE: ISO 12100:2010, 3.30, modifiée.]

3.1.28
durée de mission
T_M
laps de temps couvrant l'utilisation normale d'une SRP/CS

3.1.29
taux d'essais
r_t
fréquence des essais en ligne permettant de détecter les défauts d'un SRP/CS, valeur inverse de l'intervalle entre essais de diagnostic

3.1.30
taux de demande
r_D
fréquence de sollicitation d'une action relative à la sécurité d'une SRP/CS

3.1.31
taux de réparation
r_r
valeur inverse de l'intervalle de temps entre la détection d'une défaillance dangereuse par un essai en ligne ou un dysfonctionnement évident du système et la remise en marche après réparation du système/remplacement du composant

Note 1 à l'article: Le temps de réparation ne comprend pas le temps nécessaire à la détection de la défaillance.

3.1.32
système de commande de la machine
système qui répond aux signaux d'entrée de parties de machines, des opérateurs, des équipements de commande externes ou de toute combinaison de ceux-ci et qui génère des signaux de sorties imposant à la machine un comportement attendu

Note 1 à l'article: Le système de commande de la machine peut utiliser toute technologie ou combinaison de différentes technologies (exemple électrique/électronique, hydraulique, pneumatique, mécanique).

3.1.33
Niveau d'intégrité de sécurité
SIL
niveau discret (parmi trois possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions de commandes relatives à la sécurité à allouer aux systèmes électriques, électroniques et électroniques programmables relatifs à la sécurité, le niveau 4 d'intégrité de sécurité possédant le plus haut degré d'intégrité et le niveau 1 possédant le plus bas

[SOURCE: IEC 61508-4:1998, 3.5.6]

3.1.34
langage de variabilité limitée
LVL

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

Note 1 à l'article: Des exemples typiques de LVL sont donnés dans la IEC 61131-3. Ils incluent: échelle logique, schéma bloc fonctionnel.

Note 2 à l'article: Un exemple typique de système utilisant le LVL: PLC.

[SOURCE: IEC 61511-1:2003, définition 3.2.80.1.2, modifiée.]

3.1.35
langage de variabilité totale
FVL
type de langage qui fournit la possibilité de mettre en œuvre une gamme étendue de fonctions et d'applications

EXEMPLE C, C++, assembleur.

Note 1 à l'article: Un exemple typique de système utilisant le FVL: ordinateur d'usage général.

Note 2 à l'article: Le FVL se trouve normalement dans les logiciels intégrés et rarement dans les logiciels d'application.

[SOURCE: IEC 61511-1:2003, 3.2.80.1.3, modifiée.]

3.1.36
logiciel d'application
logiciel spécifique d'application qui a été implémenté par le concepteur de la machine et qui contient généralement des séquences logiques, des limites et des expressions qui commandent l'entrée, la sortie, les calculs appropriés et les décisions nécessaires pour satisfaire aux exigences des SRP/CS