IEC 62061

Edition 2.0 2021-03

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Safety of machinery – Functional safety of safety-related control systems

Sécurité des machines – Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-8322-9333-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SAFETY OF MACHINERY – FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62061 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects. It is an International Standard.

This second edition cancels and replaces the first edition, published in 2005, Amendment 1:2012 and Amendment 2:2015. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

– structure has been changed and contents have been updated to reflect the design process of the safety function,
– standard extended to non-electrical technologies,
– definitions updated to be aligned with IEC 61508-4,
– functional safety plan introduced and configuration management updated (Clause 4),
– requirements on parametrization expanded (Clause 6),
– reference to requirements on security added (Subclause 6.8),
– requirements on periodic testing added (Subclause 6.9),

– various improvements and clarification on architectures and reliability calculations (Clause 6 and Clause 7),
– shift from "SILCL" to "maximum SIL" of a subsystem (Clause 7),
– use cases for software described including requirements (Clause 8),
– requirements on independence for software verification (Clause 8) and validation activities (Clause 9) added,
– new informative annex with examples (Annex G),
– new informative annexes on typical $MTTF_D$ values, diagnostics and calculation methods for the architectures (Annex C, Annex D and Annex H).

The text of this International Standard is based on the following documents:

Draft	Report on voting
44/885/FDIS	44/888/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

As a result of automation, demand for increased production and reduced operator physical effort, Safety-related Control Systems (referred to as SCS) of machines play an increasing role in the achievement of overall machine safety. Furthermore, the SCS themselves increasingly employ complex electronic technology.

IEC 62061 specifies requirements for the design and implementation of safety-related control systems of machinery. This document is machine sector specific within the framework of IEC 61508.

NOTE While IEC 62061 and ISO 13849-1 are using different methodologies for the design of safety related control systems, they intend to achieve the same risk reduction.

This International Standard is intended for use by machinery designers, control system manufacturers and integrators, and others involved in the specification, design and validation of an SCS. It sets out an approach and provides requirements to achieve the necessary performance and facilitates the specification of the safety functions intended to achieve the risk reduction.

This document provides a machine sector specific framework for functional safety of an SCS of machines. It only covers those aspects of the safety lifecycle that are related to safety requirements allocation through to safety validation. Requirements are provided for information for safe use of SCS of machines that can also be relevant to later phases of the lifecycle of an SCS.

There are many situations on machines where SCS are employed as part of safety measures that have been provided to achieve risk reduction. A typical case is the use of an interlocking guard that, when it is opened to allow access to the danger zone, signals the safety related parts of the machine control system to stop hazardous machine operation. In automation, the machine control system that is used to achieve correct operation of the machine process often contributes to safety by mitigating risks associated with hazards arising directly from control system failures. This document gives a methodology and requirements to:

- assign the required safety integrity for each safety function to be implemented by SCS;
- enable the design of the SCS appropriate to the assigned safety (control) function(s);
- integrate safety-related subsystems designed in accordance with other applicable functional safety-related standards (see 6.3.4);
- validate the SCS.

This document is intended to be used within the framework of systematic risk reduction, in conjunction with risk assessment described in ISO 12100. Suggested methodologies for a safety integrity assignment are given in informative Annex A.

SAFETY OF MACHINERY – FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

1 Scope

This International Standard specifies requirements and makes recommendations for the design, integration and validation of safety-related control systems (SCS) for machines. It is applicable to control systems used, either singly or in combination, to carry out safety functions on machines that are not portable by hand while working, including a group of machines working together in a co-ordinated manner.

This document is a machinery sector specific standard within the framework of IEC 61508 (all parts).

The design of complex programmable electronic subsystems or subsystem elements is not within the scope of this document. This is in the scope of IEC 61508 or standards linked to it; see Figure 1.

NOTE 1 Elements such as systems on chip or microcontroller boards are considered complex programmable electronic subsystems.

The main body of this sector standard specifies general requirements for the design, and verification of a safety-related control system intended to be used in high/continuous demand mode.

This document:

– is concerned only with functional safety requirements intended to reduce the risk of hazardous situations;
– is restricted to risks arising directly from the hazards of the machine itself or from a group of machines working together in a co-ordinated manner;

NOTE 2 Requirements to mitigate risks arising from other hazards are provided in relevant sector standards. For example, where a machine(s) is part of a process activity, additional information is available in IEC 61511.

This document does not cover

– electrical hazards arising from the electrical control equipment itself (e.g. electric shock – see IEC 60204-1);
– other safety requirements necessary at the machine level such as safeguarding;
– specific measures for security aspects – see IEC TR 63074.

This document is not intended to limit or inhibit technological advancement.

Figure 1 illustrates the scope of this document.

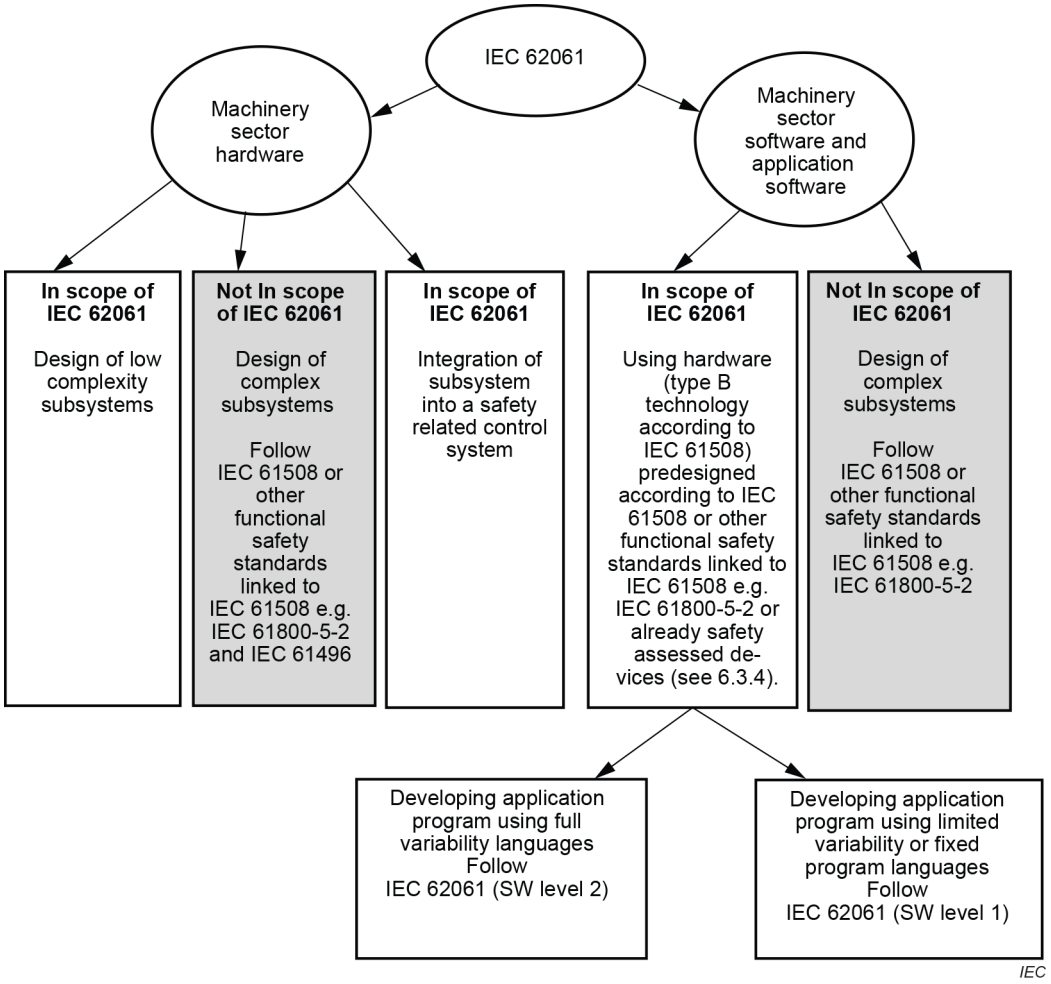

Figure 1 – Scope of this document

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60204-1:2016, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-1-2:2016, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

ISO 12100:2010, *Safety of machinery – General principles for design – Risk assessment and risk reduction*

ISO 13849 (all parts), *Safety of machinery – Safety-related parts of control systems*

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ DES MACHINES – SÉCURITÉ FONCTIONNELLE DES SYSTÈMES DE COMMANDE RELATIFS À LA SÉCURITÉ

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

L'IEC 62061 a été établie par le comité d'études 44 de l'IEC: Sécurité des machines – Aspects électrotechniques. Il s'agit d'une Norme internationale.

Cette deuxième édition annule et remplace la première édition parue en 2005, l'Amendement 1:2012 ainsi que l'Amendement 2:2015. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

– la structure a été modifiée et le contenu a été mis à jour pour refléter le processus de conception de la fonction de sécurité,
– la norme a été étendue aux technologies non électriques,
– définitions mises à jour pour être alignées sur l'IEC 61508-4,

- plan de sécurité fonctionnelle introduit et gestion de configuration mise à jour (Article 4),
- exigences relatives au paramétrage étendues (Article 6),
- référence aux exigences relatives à la sécurité ajoutée (Paragraphe 6.8)
- exigences relatives aux essais périodiques ajoutées (Paragraphe 6.9),
- différentes améliorations et clarifications relatives aux architectures et aux calculs de fiabilité (Article 6 et Article 7),
- décalage entre le "SILCL" et le "SIL maximal" d'un sous-système (Article 7),
- cas d'utilisation pour les logiciels décrits, y compris les exigences (Article 8),
- exigences relatives à l'indépendance des activités de vérification (Article 8) et de validation (Article 9) du logiciel ajoutées,
- nouvelle annexe informative avec des exemples (Annex G),
- nouvelles annexes informatives relatives aux valeurs $MTTF_D$, aux diagnostics et aux méthodes de calcul des architectures (Annex C, Annex D et Annex H).

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
44/885/FDIS	44/888/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer ce document en utilisant une imprimante couleur.

INTRODUCTION

Par suite de l'automatisation, ainsi que de la demande d'une production plus élevée avec une réduction des efforts physiques des opérateurs, les systèmes de commande relatifs à la sécurité (appelés SCS ci-après) des machines jouent un rôle croissant dans la réalisation de la sécurité d'ensemble des machines. De ce fait, les SCS eux-mêmes utilisent de plus en plus souvent une technologie électronique complexe.

L'IEC 62061 spécifie les exigences pour la conception et la réalisation des systèmes de commande des machines relatifs à la sécurité. Le présent document est spécifique au secteur des machines dans le cadre de l'IEC 61508.

NOTE Bien que l'IEC 62061 et l'ISO 13849-1 utilisent des méthodologies différentes en matière de conception des systèmes de commande relatifs à la sécurité, elles visent à réaliser le même objectif de réduction de risque.

La présente Norme internationale est destinée à être utilisée par les concepteurs de machines, les fabricants et les intégrateurs de systèmes de commande, et autres, impliqués dans la spécification, la conception et la validation d'un SCS. Elle présente une approche et donne les exigences nécessaires à la réalisation du fonctionnement requis et facilite la spécification des fonctions de sécurité destinées à réaliser la réduction de risque.

Le présent document donne un cadre spécifique au secteur des machines pour la sécurité fonctionnelle d'un SCS de machine. Il couvre uniquement les aspects du cycle de vie de sécurité relatifs à l'allocation des exigences de sécurité jusqu'à la validation de la sécurité. Des exigences sont données pour information pour une utilisation sûre des SCS de machines, lesquelles peuvent aussi être appropriées pour des phases ultérieures de la vie d'un SCS.

Il existe de nombreuses circonstances dans les machines où les SCS sont utilisés comme partie des mesures de sécurité développées pour réaliser la réduction de risque. Un exemple typique est l'utilisation d'un protecteur avec dispositif de verrouillage qui, lorsqu'il est ouvert pour permettre l'accès à la zone dangereuse, signale aux parties relatives à la sécurité du système de commande de la machine d'arrêter le fonctionnement dangereux de la machine. En automatisation, le système de commande de la machine utilisé pour réaliser le fonctionnement correct du processus machine contribue souvent à la sécurité en réduisant les risques associés aux phénomènes dangereux résultant directement de défaillances du système de commande. Le présent document donne une méthodologie et les exigences pour:

- assigner le niveau d'intégrité de sécurité exigé pour chaque fonction de sécurité devant être mise en œuvre par les SCS;
- permettre la conception des SCS appropriés à la ou aux fonctions de commande assignées relatives à la sécurité;
- intégrer les sous-systèmes relatifs à la sécurité conçus selon d'autres normes applicables relatives à la sécurité fonctionnelle (voir 6.3.4);
- valider les SCS.

Le présent document est destiné à être utilisé dans le cadre de la réduction systématique du risque, conjointement avec l'appréciation du risque décrite dans l'ISO 12100. Les méthodologies conseillées pour l'attribution d'intégrité de sécurité sont données dans l'Annex A informative.

SÉCURITÉ DES MACHINES – SÉCURITÉ FONCTIONNELLE DES SYSTÈMES DE COMMANDE RELATIFS À LA SÉCURITÉ

1 Domaine d'application

La présente Norme internationale spécifie les exigences et donne des recommandations pour la conception, l'intégration et la validation des systèmes de commande relatifs à la sécurité (SCS) pour les machines. Elle s'applique aux systèmes de commande utilisés, séparément ou en combinaison, pour assurer les fonctions de sécurité de machines qui ne sont pas portables à la main en fonctionnement, y compris un groupe de machines fonctionnant ensemble d'une manière coordonnée.

Le présent document est spécifique au secteur des machines dans le cadre de l'IEC 61508 (toutes les parties).

La conception de sous-systèmes ou d'éléments de sous-système électroniques programmables complexes ne relève pas du domaine d'application du présent document. Ces éléments relèvent du domaine d'application de l'IEC 61508 ou de normes qui lui sont associées (voir la Figure 1).

NOTE 1 Les éléments tels que les systèmes sur puce ou les cartes de microcontrôleur sont considérés comme des sous-systèmes électroniques programmables complexes.

Le corps principal de la présente norme sectorielle spécifie les exigences générales en matière de conception et de vérification d'un système de commande relatif à la sécurité destiné à être utilisé en mode à forte sollicitation/continu.

Le présent document:

– ne concerne que les exigences de sécurité fonctionnelle destinées à réduire le risque de situations dangereuses;
– se limite aux risques résultant directement des phénomènes dangereux de la machine elle-même ou d'un groupe de machines fonctionnant ensemble d'une manière coordonnée;

NOTE 2 Les exigences pour réduire les risques provenant d'autres phénomènes dangereux sont données dans les normes sectorielles appropriées. Par exemple, pour une ou plusieurs machines qui font partie d'une activité processus, des informations supplémentaires sont disponibles dans l'IEC 61511.

Le présent document ne concerne pas

– les phénomènes dangereux électriques provenant du matériel de commande électrique lui-même (par exemple choc électrique – voir l'IEC 60204-1);
– les autres exigences relatives à la sécurité nécessaires au niveau de la machine (la protection par protecteur, par exemple);
– les mesures particulières pour les aspects liés à la sécurité – voir l'IEC TR 63074.

Le présent document n'est pas destiné à limiter ou inhiber les progrès technologiques.

La Figure 1 donne une représentation du domaine d'application du présent document.

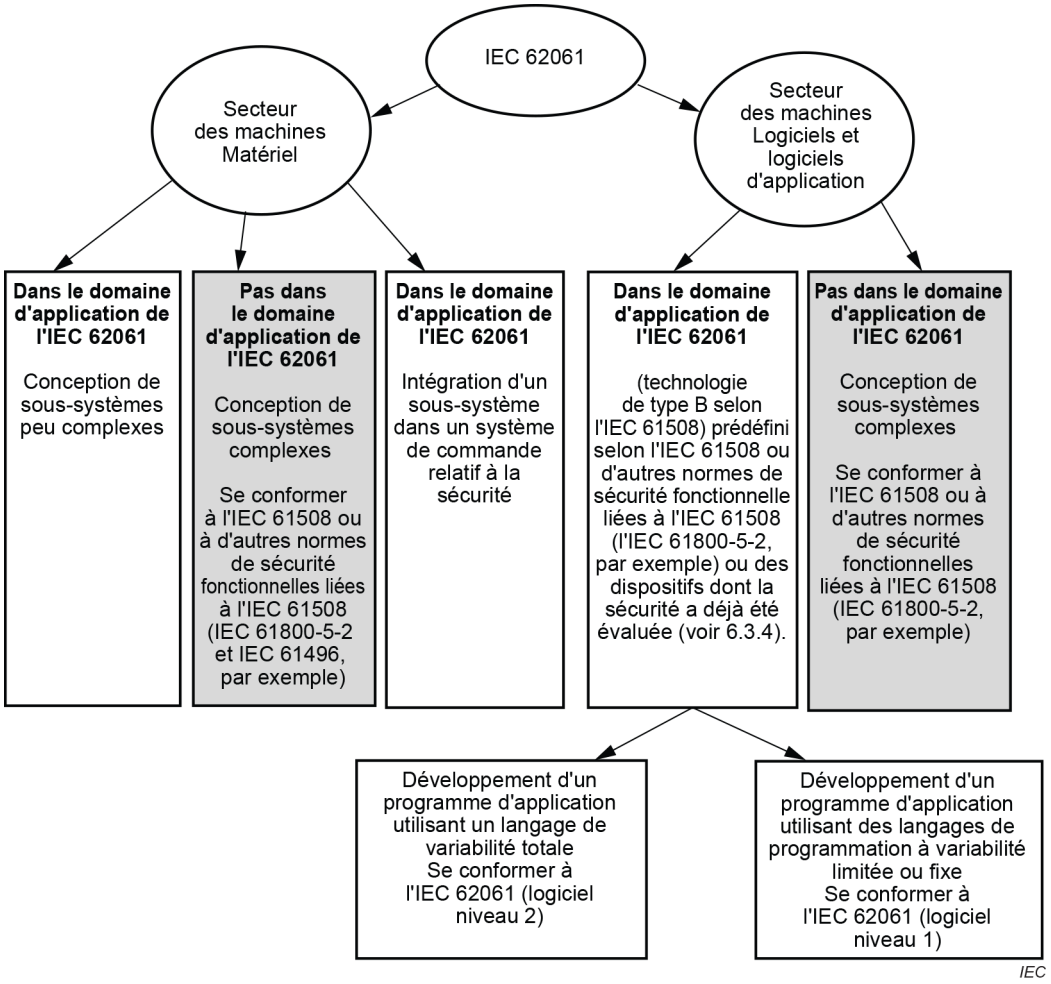

Figure 1 – Domaine d'application du présent document

2 Références normatives

Les documents 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. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60204-1:2016, *Sécurité des machines – Équipement électrique des machines – Partie 1: Exigences générales*

IEC 61000-1-2:2016, *Compatibilité électromagnétique (CEM) – Partie 1-2: Généralités – Méthodologie pour la réalisation de la sécurité fonctionnelle des systèmes électriques et électroniques, y compris les équipements, du point de vue des phénomènes électromagnétiques*

IEC 61508 (toutes les parties), *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité*

IEC 61508-2:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité*

IEC 61508-3:2010, *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité – Partie 3: Exigences concernant les logiciels*

ISO 12100:2010, *Sécurité des machines – Principes généraux de conception – Appréciation du risque et réduction du risque*

ISO 13849 (toutes les parties), *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité*

ISO 13849-1:2015, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 13849-2:2012, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 2: Validation*