IEC/TR 62513

Edition 1.0 2008-02

TECHNICAL REPORT

RAPPORT TECHNIQUE

Safety of machinery – Guidelines for the use of communication systems in safety-related applications

Sécurité des machines – Lignes directrices pour l'usage de systèmes de communication dans les applications liées à la sécurité

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

U

ICS 13.110; 29.020; 35.100

ISBN 2-8318-9614-2

CONTENTS

FOREWORD 4
INTRODUCTION 6

1 Scope 7
2 Normative references 7
3 Terms and definitions 7
4 Management of functional safety 11
4.1 Requirements of IEC 62061 11
5 Realisation of a safety-related electrical control system (SRECS) using a safety-related communication system 12
6 Planning of the safety-related communication system 13
6.1 System design 13
6.1.1 Safety integrity level (SIL) assigned to the SRCF(s) and the safety-related communication system 13
6.1.2 Configuration and parameterisation of the safety-related communication system 13
6.1.3 Response time and protective measures 13
6.1.4 Fault monitoring and alarm indication 14
6.1.5 Assuring functional safety in case of SRECS failure 14
6.2 Selection criteria of the safety-related communication system 15
6.2.1 Architecture and application fields 15
6.2.2 Maximum response time 15
6.2.3 Transmission distance, transmission speed and the number of nodes 16
6.2.4 Environmental conditions 16
6.2.5 Setting and configuration tools 16
7 System installation and setup (configuration) 16
7.1 System installation 16
7.1.1 System confirmation 16
7.1.2 Safety-related communication system wiring 16
7.1.3 Selection of power supply 17
7.1.4 Environmental conditions 18
7.2 Setting 18
7.2.1 System configuration 18
7.2.2 Setting for operation 18
7.2.3 Setting and modification of configuration data 19
8 Validation 19
8.1 Checks before applying the power 19
8.2 Validation after applying the power 19
8.3 Functional tests 19
8.4 Baseline 20
9 Documentation 20
10 Operation, maintenance and repair 21
10.1 Appointment of responsible person 21
10.2 Developing a maintenance plan 21
10.3 Implementing periodic maintenance 21
10.4 Items of maintenance work 21

10.5 Record of maintenance results 21
11 Education and training 22
11.1 General 22
11.2 Scope 22
11.3 Performing continual education and training 22
11.4 Contents of education and training 22
11.5 Planning of educational activities and storage of education records 22

Annex A (informative) Design of a SRECS using a safety-related communication system – Function blocks concept 23

Bibliography 28

Figure 1 – SRECS design and development flow 12
Figure 2 – System Response Time Components 13
Figure A.1 – Components of a SRECS 23
Figure A.2 – SRECS using a safety-related communication system 24
Figure A.3 – Different views of the safety-related communication system 25
Figure A.4 – Examples of typical architectures of safety-related communication systems 26

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SAFETY OF MACHINERY – GUIDELINES FOR THE USE OF COMMUNICATION SYSTEMS IN SAFETY-RELATED APPLICATIONS

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 62513, which is a technical report, has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects.

This Technical Report is to be used in conjunction with IEC 62061.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
44/551/DTR	44/555/RVC

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result 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.

INTRODUCTION

International standards exist that can be used to determine the integrity of communication systems. This Technical Report was developed to give guidance on the design and operation of control systems using suitable communication systems that contribute to safety-related control functions of machines.

SAFETY OF MACHINERY – GUIDELINES FOR THE USE OF COMMUNICATION SYSTEMS IN SAFETY-RELATED APPLICATIONS

1 Scope

This Technical Report addresses the application of closed serial digital communications systems (often termed fieldbuses) used for transmission of safety-related data in the realisation of safety functions at machinery. It offers guidance on the issues that need to be considered during the specification, system design, installation, commissioning, modification and maintenance of such applications.

NOTE A closed serial digital communications system is considered to have a fixed number or fixed maximum number of participants linked by a transmission system with well-known and fixed properties, and where the risk of unauthorized access is considered negligible.

This Technical Report assumes that the SRECS safety requirements specification (SRS) has been developed and the design of the SRECS (Safety-Related Electrical Control Systems) is intended to include a safety-related communication system. This Technical Report is intended to be used in conjunction with IEC 62061.

This Technical Report does not address the design of the safety-related communication system itself.

2 Normative references

The following referenced documents are indispensable for the application 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, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

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

IEC 62061, *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*

SOMMAIRE

AVANT-PROPOS 32
INTRODUCTION 34

1 Domaine d'application 35
2 Références normatives 35
3 Termes et définitions 35
4 Gestion de la sécurité fonctionnelle 39
4.1 Exigences de la CEI 62061 39
5 Réalisation d'un système de commande électrique relatif à la sécurité (SRECS) à l'aide d'un système de communication relatif à la sécurité 39
6 Planification du système de communication relatif à la sécurité 41
6.1 Conception du système 41
6.1.1 Niveau d'intégrité de sécurité (SIL) attribué à la (aux) SRCF(s) et au système de communication relatif à la sécurité 41
6.1.2 Configuration et paramétrage du système de communication relatif à la sécurité 41
6.1.3 Temps de réponse et mesures de protection 41
6.1.4 Surveillance des défauts et indication d'alarme 42
6.1.5 Garantie d'une sécurité fonctionnelle en cas de défaillance du SRECS 42
6.2 Critères de sélection du système de communication relatif à la sécurité 43
6.2.1 Architecture et domaines d'application 43
6.2.2 Temps de réponse maximal 43
6.2.3 Distance de transmission, vitesse de transmission et nombre de nœuds 44
6.2.4 Conditions environnementales 44
6.2.5 Outils de réglage et de configuration 44
7 Installation et montage du système (configuration) 45
7.1 Installation du système 45
7.1.1 Confirmation du système 45
7.1.2 Câblage du système de communication relatif à la sécurité 45
7.1.3 Choix de l'alimentation 46
7.1.4 Conditions environnementales 46
7.2 Réglage 46
7.2.1 Configuration du système 46
7.2.2 Réglage pour le fonctionnement 47
7.2.3 Réglage et modification des données de configuration 47
8 Validation 47
8.1 Vérifications avant l'application de la puissance 47
8.2 Validation après l'application de la puissance 48
8.3 Essais fonctionnels 48
8.4 Référentiel 48
9 Documentation 49
10 Fonctionnement, maintenance et réparation 49
10.1 Désignation d'une personne responsable 49
10.2 Elaboration d'un plan de maintenance 49

10.3 Mise en œuvre d'une maintenance périodique 50
10.4 Eléments des travaux de maintenance 50
10.5 Enregistrement des résultats de maintenance 50
11 Enseignement et formation 50
11.1 Généralités 50
11.2 Domaine d'application 50
11.3 Mise en œuvre d'un enseignement et d'une formation continus 50
11.4 Contenu de l'enseignement et de la formation 51
11.5 Planification des activités de formation et conservation des données de formation 51

Annexe A (informative) Conception d'un SRECS utilisant un système de communication relatif à la sécurité – Concept des blocs fonctionnels 52

Bibliographie 57

Figure 1 – Diagramme de conception et de développement d'un SRECS 40
Figure 2 – Composants du temps de réponse du système 41
Figure A.1 – Composants d'un SRECS 52
Figure A.2 – SRECS utilisant un système de communication relatif à la sécurité 53
Figure A.3 – Vues différentes du système de communication relatif à la sécurité 54
Figure A.4 – Exemples d'architectures types des systèmes de communication relatifs à la sécurité 55

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ DES MACHINES – LIGNES DIRECTRICES POUR L'USAGE DE SYSTÈMES DE COMMUNICATION DANS LES APPLICATIONS LIÉES A LA SÉCURITÉ

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La tâche principale des comités d'études de la CEI est l'élaboration des Normes internationales. Toutefois, un comité d'études peut proposer la publication d'un rapport technique lorsqu'il a réuni des données de nature différente de celles qui sont normalement publiées comme Normes internationales, cela pouvant comprendre, par exemple, des informations sur l' « état de la technique ».

La CEI 62513, qui est un rapport technique, a été établie par le comité d'études 44 de la CEI: Sécurité des machines – Aspects électrotechniques.

Le présent rapport technique doit être lu conjointement avec la CEI 62061.

Le texte de ce rapport technique est issu des documents suivants:

Projet d'enquête	Rapport de vote
44/551/DTR	44/555/RVC

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

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

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

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

INTRODUCTION

Il existe des normes internationales qui peuvent être utilisées pour déterminer l'intégrité des systèmes de communication. Le présent rapport technique a été élaboré pour donner un guide sur la conception et le fonctionnement des systèmes de commande utilisant des systèmes de communication adaptés qui contribuent aux fonctions de commande relatives à la sécurité des machines.

SÉCURITÉ DES MACHINES – LIGNES DIRECTRICES POUR L'USAGE DE SYSTÈMES DE COMMUNICATION DANS LES APPLICATIONS LIÉES A LA SÉCURITÉ

1 Domaine d'application

Le présent rapport technique traite de l'application des systèmes de communication numériques de série fermés (souvent désignés par bus de terrain) utilisés pour la transmission des données relatives à la sécurité dans la réalisation des fonctions de sécurité au niveau des machines. Il propose un guide sur les questions qui doivent être prises en compte au cours de la spécification, de la conception du système, de l'installation, de la mise en service, de la modification et de la maintenance de telles applications.

NOTE Un système de communication numérique de série fermé est considéré comme ayant un nombre fixe ou un nombre maximal fixe de participants liés par un système de transmission avec des propriétés bien connues et fixes, et lorsque le risque d'accès non autorisé est considéré comme négligeable.

Le présent rapport technique suppose que la spécification des exigences de sécurité (SRS, *safety requirements specification*) du SRECS (système de commande électrique relatif à la sécurité, *safety-related electrical control system*) a été élaborée et que la conception du SRECS est destinée à inclure un système de communication relatif à la sécurité. Le présent rapport technique est destiné à être utilisé conjointement avec la CEI 62061.

Le présent rapport technique ne traite pas de la conception du système de communication relatif à la sécurité lui-même.

2 Références normatives

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

CEI 60204-1, *Sécurité des machines – Equipement électrique des machines – Partie 1: Règles générales.*

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

CEI 62061, *Sécurité des machines – Sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité*