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

IEC/TR 62513:2008

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

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

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*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
category
classification of the safety-related part of a control system in respect of its resistance to faults and its subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts and/or by their reliability

[ISO 13849-1, 3.1.2]

3.2
communication system
arrangement of hardware, software and propagation media for the transfer of messages between devices, such as sensors, actuators and the controlling devices of machinery

3.3
configuration (parameter setting)
setting and/or modification of any data required for system operation

3.4
electromagnetic interference
EMI
disturbance causing performance degradation, malfunction or failure of electrical and electronic devices, apparatuses and/or systems

NOTE A typical example of such disturbances is radio frequency interference.

3.5
fault tolerance
ability of a SRECS, a subsystem, or subsystem element to continue to perform a required function in the presence of faults or failures

[IEC 62061, 3.2.31]

3.6
node
point of a communication system where one or more functional units interconnect data channels or data circuits

3.7
operation mode
method or way of operation

3.8
protected extra-low-voltage
PELV
earthed circuits which are insulated from hazardous voltage by double insulation or any better insulation, and in which the voltage cannot exceed ELV specified in IEC 61201: 1992, under normal conditions and single fault conditions

[IEC 61140]

3.9
proof test
test that can detect faults and degradation in a SRECS and its subsystems so that, if necessary, the SRECS and its subsystems can be restored to an “as new” condition or as close as practical to this condition

[IEC 62061, 3.2.37]

NOTE A proof test is intended to confirm that the SRECS is in a condition that assures the specified safety integrity.

3.10
protective measure
measure intended to achieve risk reduction, implemented

– by the designer (intrinsic design, safeguarding and complementary measures, information for use) and

– by the user (organization, safe working procedures, supervision, permit to work, system, additional safeguards, personal protective equipment, training)

[ISO 13849-1, 3.1.27]

3.11
reasonably foreseeable misuse
use of a machine in a way not intended by the designer, but which may result from readily predictable human behaviour

[ISO 13849-1, 3.1.19]

3.12
safety function
function of a machine whose failure can result in an immediate increase of the risk(s)

[IEC 62061, 3.2.15, and ISO 12100-1:2003, 3.28]

NOTE This definition differs from the definitions in IEC 61508-4 and ISO 13849-1.

3.13
safety functions requirements specification
specification containing the requirements of the safety functions that have to be performed by safety-related systems

[IEC 61508-4, 3.5.9]

3.14
safety integrity
probability of a SRECS or its subsystem satisfactorily performing the required safety-related control functions under all stated conditions

[IEC 62061, 3.2.19]

NOTE 1 The higher the level of safety integrity of the item, the lower the probability that the item will fail to carry out the required safety-related control function.

NOTE 2 Safety integrity comprises hardware safety integrity (see IEC 62061, 3.2.20) and systematic safety integrity (see IEC 62061, 3.2.22).

3.15
safety integrity level
SIL
discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest

[IEC 62061, 3.2.23]

NOTE SIL 4 is not considered in this standard, as it is not relevant to the risk reduction requirements normally associated with machinery. For requirements applicable to SIL 4, see IEC 61508-1 and IEC 61508-2.

3.16
safety-related control function
SRCF
control function with a specified integrity level to be implemented by a SRECS that is intended to maintain the safe condition of the machine or prevent an immediate increase of the risk(s)

[IEC 62061, 3.2.16]

3.17
safety-related electrical control system
SRECS
electrical, electronic or programmable electronic part of a machine control system whose failure can result in an immediate increase of the risk(s)

[IEC 62061, 3.2.4 modified]

3.18
safety requirements specification
specification containing all the requirements of the safety functions that have to be performed by safety-related systems

NOTE The specification is divided into the safety functions requirements specification and the safety integrity requirements specification.

[IEC 61508-4, 3.5.8]

3.19
safety extra-low-voltage
SELV
unearthed circuits which are insulated from hazardous voltage by double insulation or any better insulation, and in which the voltage cannot exceed ELV specified in IEC 61201: 1992, under normal conditions and single fault conditions

[IEC 61140]

3.20
safe failure fraction
SFF
fraction of the overall failure rate of a subsystem that does not result in a dangerous failure

[IEC 62061, 3.2.42]

3.21
SIL claim limit (for a subsystem)
SILCL
maximum SIL that can be claimed for a SRECS subsystem in relation to architectural constraints and systematic safety integrity

[IEC 62061, 3.2.24]

3.22
subsystem
entity of the top-level architectural design of the SRECS where a failure of any subsystem will result in a failure of a safety-related control function

NOTE 1 A complete subsystem can be made up from a number of identifiable and separate subsystem elements, which when put together implement the function blocks allocated to the subsystem.

NOTE 2 This definition is a limitation of the general definition of IEC 61508-4: `set of elements which interact according to a design, where an element of a system can be another system, called a subsystem, which may include hardware, software and human interaction.

NOTE 3 This differs from common language where “subsystem” may mean any sub-divided part of an entity, the term “subsystem” is used in this standard within a strongly defined hierarchy of terminology: “subsystem” is the first level subdivision of a system. The parts resulting from further subdivision of a subsystem are called “subsystem elements”.

[IEC 62061, 3.2.5]

3.23
validation
confirmation by examination (e.g. tests, analysis) that the functional safety requirements of the specific application are met

[IEC 62061, 3.2.52 modified]

4 Management of functional safety

4.1 Requirements of IEC 62061

IEC 62061 requires that a functional safety plan be drawn up and documented for each SRECS design project, and is updated as necessary. The plan includes procedures for control of the activities specified in Clauses 5 to 9 of IEC 62061.

This Technical Report assumes that the management of functional safety requirements specified in IEC 62061 have been implemented, and draws attention to those issues that are particularly applicable to safety-related communication systems.

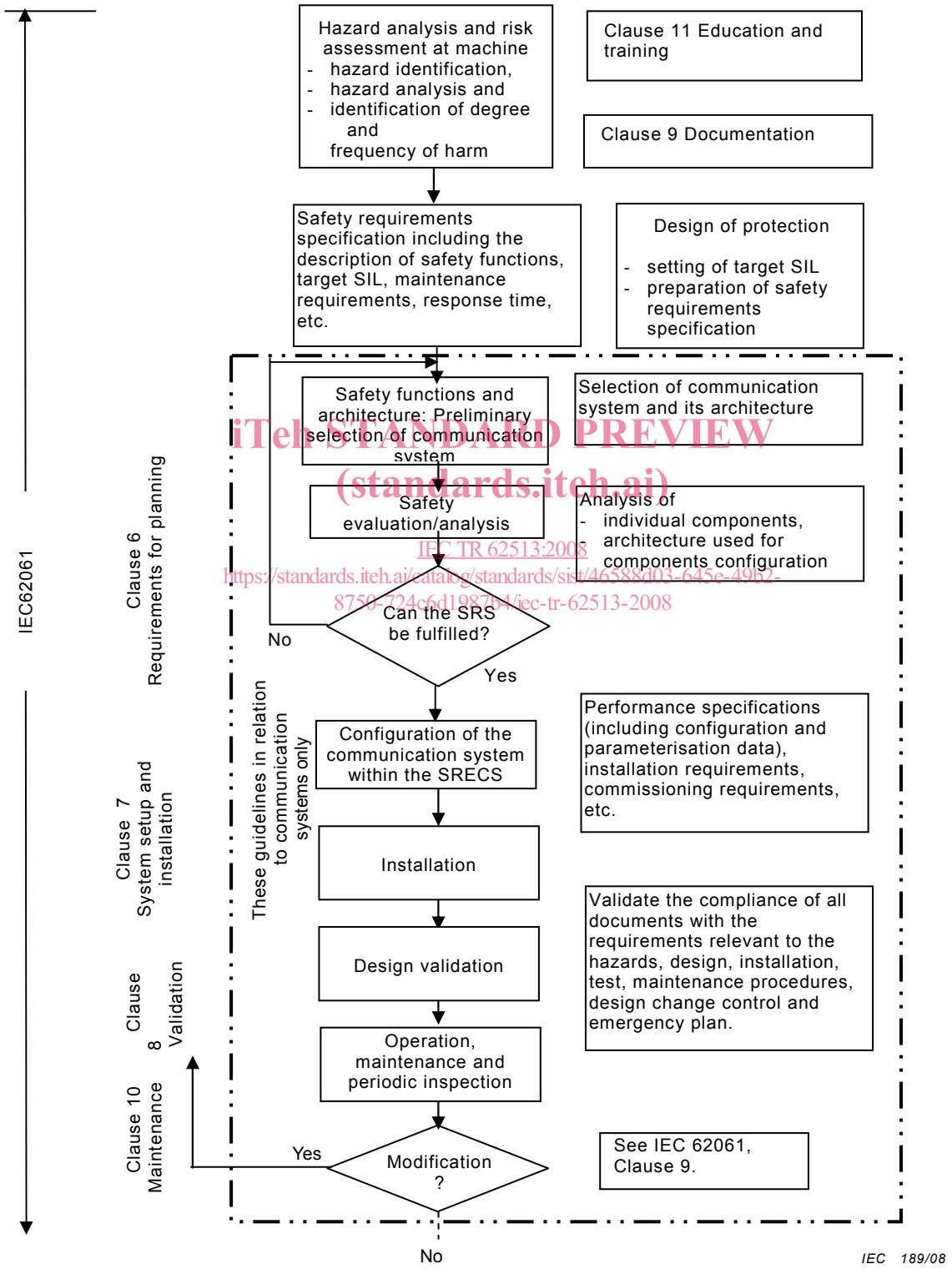
The relevant activities particularly applicable to safety-related communication systems include:

a) selection management
   – see 6.2;
b) installation management
   – see 7.1;
c) configuration and parametrisation management
   – see 7.2;
d) validation management
   – see Clause 8;
e) operation, maintenance and periodic inspection management
   – see Clause 10;
f) modification management
   – see IEC 62061, Clause 9.

5 Realisation of a safety-related electrical control system (SRECS) using a safety-related communication system

Figure 1 shows the process of selection or design and manufacturing of SRECS satisfying the safety functions and safety integrity required by the safety requirements specification.

NOTE For the detail of safety requirements specification (SRS), refer to IEC 62061, 5.2.



NOTE References to clauses refer to this document unless stated otherwise

Figure 1 – SRECS design and development flow

6 Planning of the safety-related communication system

6.1 System design

6.1.1 Safety integrity level (SIL) assigned to the SRCF(s) and the safety-related communication system

This Technical Report assumes that the SRECS safety requirements specification has been developed in accordance with IEC 62061 and the required SIL has been determined for each safety function that utilises the safety-related communication system.

The SIL claim limit (SILCL) of a candidate safety-related communication system should be sufficient to achieve the required SIL for any safety-related control function(s) (SRCFs).

NOTE Annex A provides an outline of the design of a SRECS using a safety-related communication system based on the function blocks concept.

6.1.2 Configuration and parameterisation of the safety-related communication system

Under consideration.

6.1.3 Response time and protective measures

The worst-case response time (see also 6.2.2) from input to output of the SRECS including the safety-related communication system, should be sufficiently short that all safety functions of the specific application can be performed within the time specified in the SRS. Where the worst-case response time is not sufficiently short to allow adequate performance of the safety functions (e.g. due to the constraints of the machinery), then other measures (e.g. additional protective measure(s), selection of an alternative form of safety-related communication system that has improved response time) should be taken to fulfil the relevant requirements of the SRS.

The following diagram outlines the various system response time components that should be considered with regard to the communication of data from a remote safety-related input to a controller to a remote safety-related output.

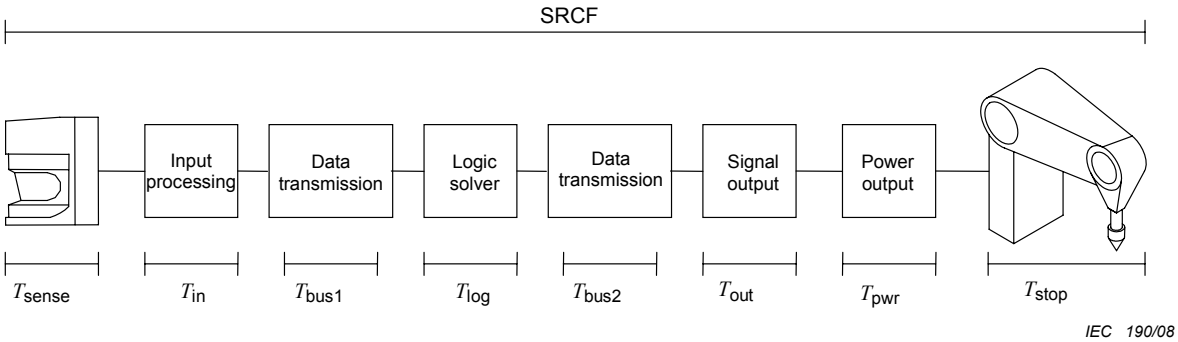


Figure 2 – System response time components

The response time of the safety related communication system is defined by

Communication system response time = $T_{bus1} + T_{bus2}$

It is important to note that T_{bus1} and T_{bus2} are not only dependent on the time for one bus cycle or one message, but can also contain repetition, error handling, synchronization delays, etc. For details, see the safety-related communication system specification.