

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

ICS 13.110; 29.020; 35.100.01

National foreword

This Published Document is the UK implementation of IEC/TR 62513:2008.
The UK participation in its preparation was entrusted to Technical Committee MCE/3, Safeguarding of machinery.
A list of organizations represented on this committee can be obtained on request to its secretary.
This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 September 2008

© BSI 2008

ISBN 978 0 580 62291 5

Amendments/corrigenda issued since publication

Date	Comments

TECHNICAL REPORT

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

CONTENTS

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

10.5	Record of maintenance results	19
11	Education and training.....	20
11.1	General.....	20
11.2	Scope.....	20
11.3	Performing continual education and training	20
11.4	Contents of education and training	20
11.5	Planning of educational activities and storage of education records.....	20
Annex A (informative) Design of a SRECS using a safety-related communication system – Function blocks concept.....		21
Bibliography.....		26
Figure 1 – SRECS design and development flow		10
Figure 2 – System Response Time Components		11
Figure A.1 – Components of a SRECS.....		21
Figure A.2 – SRECS using a safety-related communication system		22
Figure A.3 – Different views of the safety-related communication system.....		23
Figure A.4 – Examples of typical architectures of safety-related communication systems		24

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]