BS EN 50325-5:2010

BSI Standards Publication

Industrial communications subsystem based on ISO 11898 (CAN) for controller-device interfaces

Part 5: Functional safety communication based on EN 50325-4

raising standards worldwide™

National foreword

This British Standard is the UK implementation of EN 50325-5:2010.

The UK participation in its preparation was entrusted to Technical Committee AMT/7, Industrial communications: process measurement and control, including fieldbus.

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.

ISBN 978 0 580 65883 9

ICS 25.040.40; 35.240.50; 43.040.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2010.

Amendments issued since publication

Date	Text affected

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50325-5

July 2010

ICS 43.040.15

English version

Industrial communications subsystem based on ISO 11898 (CAN) for controller-device interfaces - Part 5: Functional safety communication based on EN 50325-4

Sous-système de communications industriel basé sur l'ISO 11898 (CAN) pour les interfaces des dispositifs de commande - Partie 5: Communication de sécurité fonctionnelle basée sur EN 50325-4

Industrielles Kommunikationssubsystem basierend auf ISO 11898 (CAN) - Teil 5: Funktional sichere Kommunikation basierend auf EN 50325-4

This European Standard was approved by CENELEC on 2010-07-01. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

Management Centre: Avenue Marnix 17, B - 1000 Brussels

Ref. No. EN 50325-5:2010 E

Foreword

This European Standard was prepared by the Technical Committee CENELEC TC 65CX, Fieldbus.

It was submitted to the formal vote and was approved by CENELEC as EN 50535-5 on 2010-07-01.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

– latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	2011-07-01
– latest date by which the national standards conflicting with the EN have to be withdrawn	(dow)	2013-07-01

Contents

Figures

Tables

Introduction

The EN 50325-4 fieldbus standard defines a communication protocol that enables distributed control of automated applications. Fieldbus technology is now considered well accepted and well proven. Thus many fieldbus enhancements are emerging, addressing not yet standardized areas such as real time, safety-related and security-related applications.

This European Standard specifies a safety communication layer (profile and corresponding protocols) based on the communication profile and protocol layer of EN 50325-4. The relevant principles for functional safety communication with reference to EN 61508 series are explained in EN 61784–3. Differently to EN 61784–3 this standard uses a white channel approach. It does not cover electrical safety and intrinsic safety aspects. Figure 1 shows the safety-related definitions in this standard. In implementing this standard additional measures to ensure integrity with the requirements of EN 61508 series shall be taken care (marked blue and dashed-blue in Figure 1).

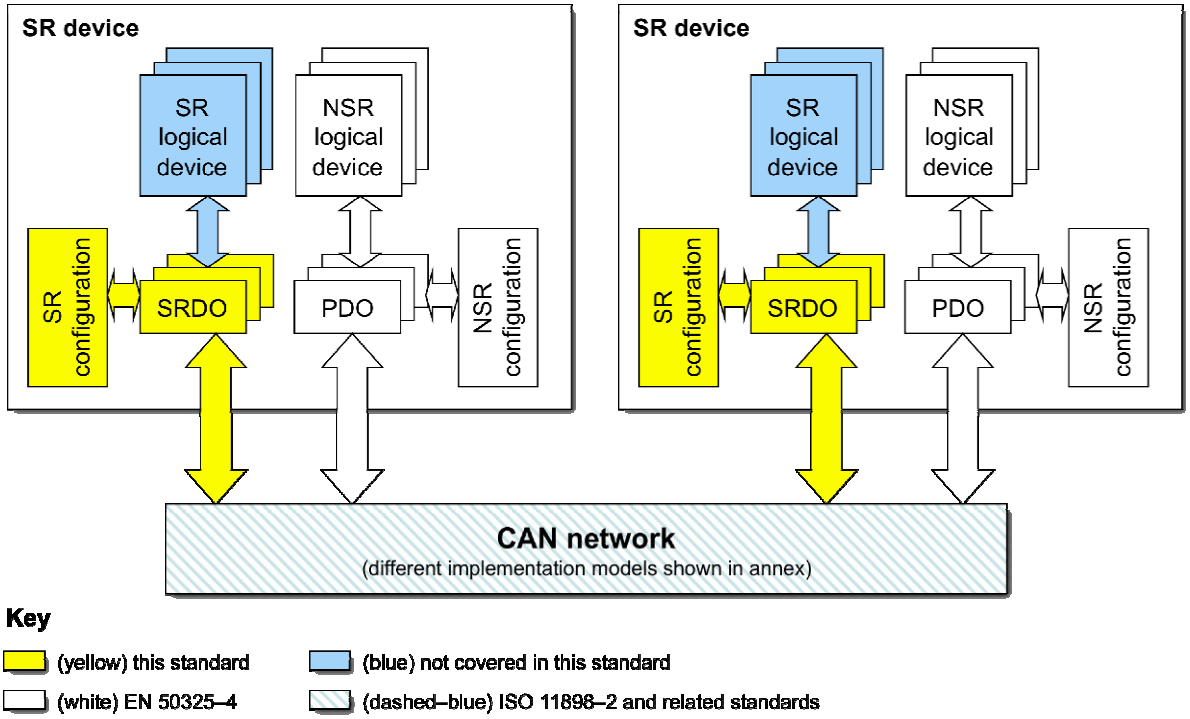
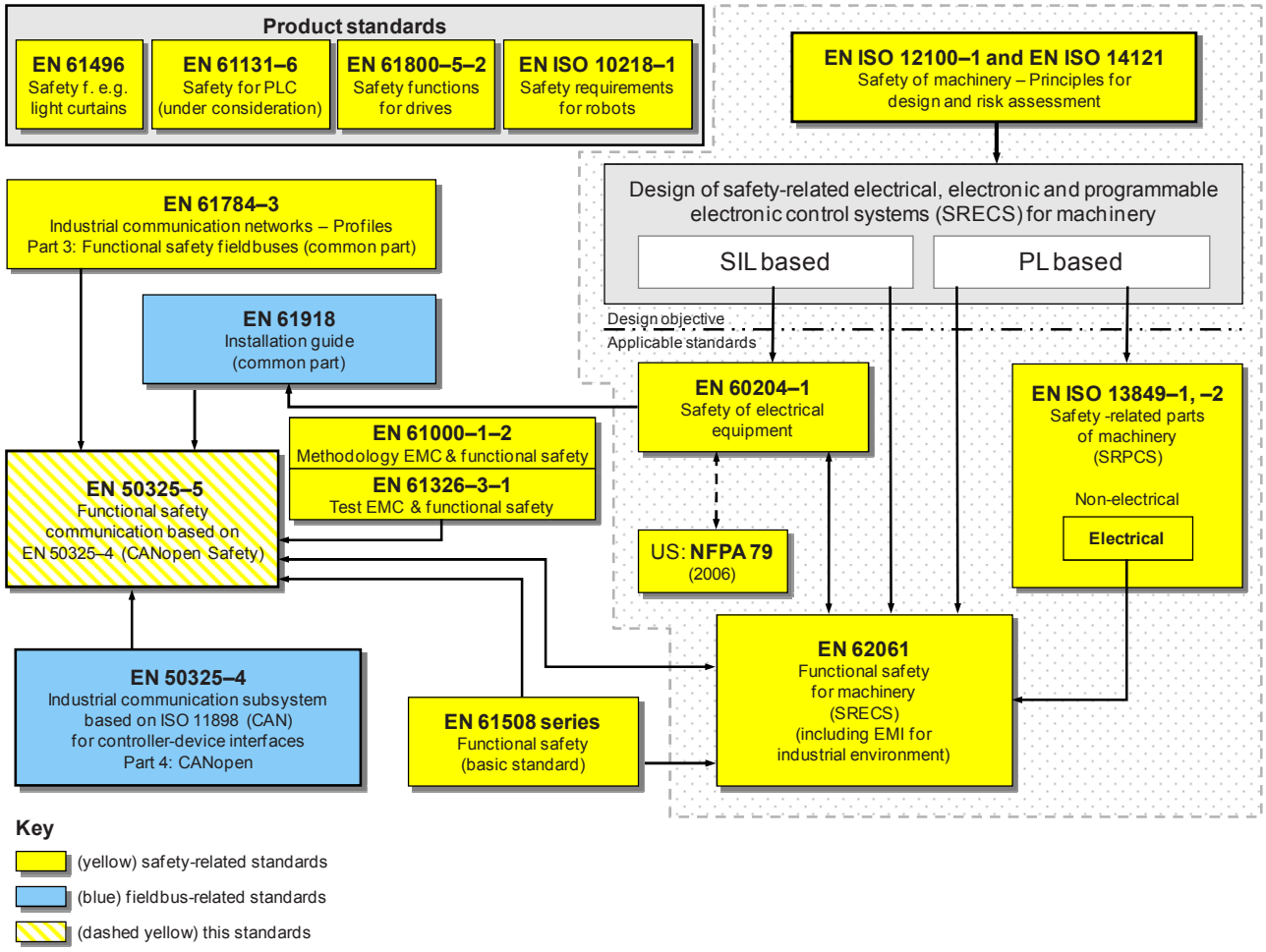


Figure 1 — Safety-related definitions in this standard

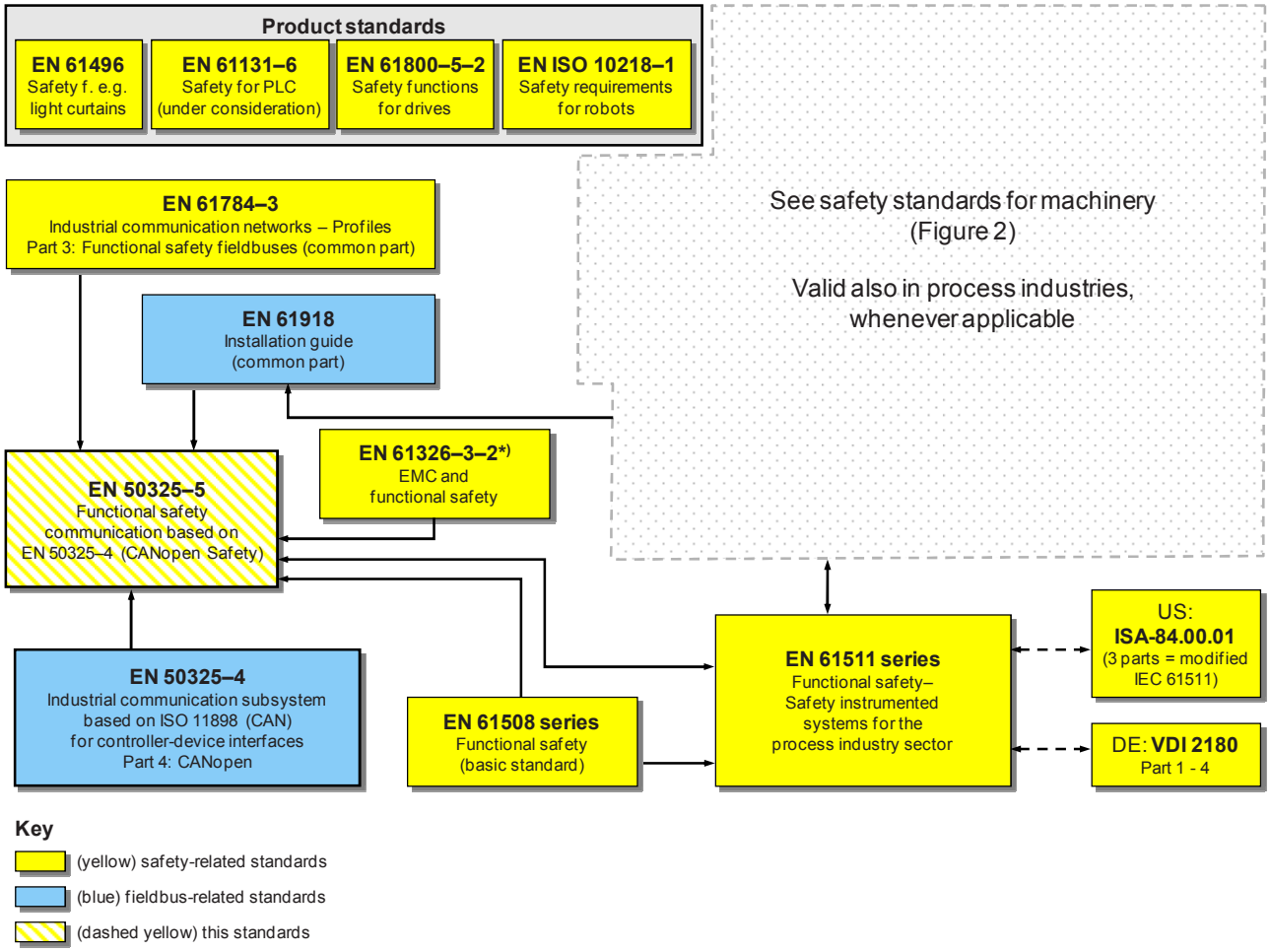
Figure 2 shows the relationships between this standard and relevant safety and fieldbus standards in a machinery environment.



NOTE Subclauses 6.7.6.4 (high complexity) and 6.7.8.1.6 (low complexity) of EN 62061 specify the relationship between PL (category) and SIL.

Figure 2 — Relationships of EN 50325–5 with other standards (machinery)

Figure 3 shows the relationships between this standard and relevant safety and fieldbus standards in a process environment.



* For specified electromagnetic environments; otherwise EN 61326-3-1.

Figure 3 — Relationships of EN 50325–5 with other standards (process)

In other environments than machinery and process control, like for example medical devices or railway systems, other standards instead may apply. The user of this standard has to take care that all related standards for the corresponding environment are considered.

Safety communication layers, which are implemented as part of safety-related systems according to EN 61508 series, provide the necessary confidence in the transportation of messages (information) between two or more participants on a field bus in a safety-related system, or sufficient confidence of safe behaviour in the event of fieldbus errors or failures.

The safety communication layer specified in this standard do this in such a way that a fieldbus can be used for applications requiring functional safety up to the Safety Integrity Level (SIL) specified by its corresponding safety communication profile.

The resulting SIL claim of a system depends on the implementation of the functional safety communication profile within this system – implementation of the functional safety communication profile in a regular device is not sufficient to qualify it as a safety device.

This European Standard covers:

— individual description of the functional safety profile for the communication profile defined in EN 50325-4;

— safety layer extensions to the communication object and object dictionary sections in EN 50325-4.

1 Scope

This European Standard specifies a safety-related communication layer (services and protocol) based on EN 50325-4.

This European Standard applies to networks based on EN 50325-4 providing safety-related communication capabilities between devices in a safety-related system in accordance with the requirements of EN 61508 series for functional safety. The services and protocols defined in this standard are intended to extend those defined in EN 50325-4. These services and protocols may be used in various applications such as manufacturing, machinery, medical, mobile machinery and process control.

NOTE 1 This European Standard does not cover the procedures for the safety-related configuration and for the safety-related setup of safety-related systems. The definition and implementation of such procedures depends on the kind of the safety-related system. For example flexible safety-related systems like operating theatres as found in medical systems require different procedures than for fixed safety-related systems like cranes in the mobile machinery. This European Standard does not cover electrical safety, intrinsic safety and security aspects. Electrical safety relates to hazards such as electrical shock. Intrinsic safety relates to hazards associated with potentially explosive atmospheres. Security relates to enforcing policies to prevent changes in the safety-related system by unauthorized personnel.

NOTE 2 The resulting safety integrity level claim of a system depends on the implementation of the services and protocols within the devices and the system. The implementation of the services and protocols defined in this European Standard in a device is not sufficient to qualify the device as a safety-related device.

2 Normative references

EN 50325-4, *Industrial communications subsystem based on ISO 11898 (CAN) for controller-device interfaces - Part 4: CANopen*

EN 61000–6–2, *Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments* (IEC 61000-6-2)

EN 61326–3–1, Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: *Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications* (IEC 61326-3-1)

EN 61326–3–2, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified electromagnetic environment* (IEC 61326-3-2)

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

EN 61784–3:2008, *Industrial communication networks - Profiles – Part 3: Functional safety fieldbuses - General rules and profile definitions* (IEC 61784-3:2007)

EN 61918, *Industrial communication networks - Installation of communication networks in industrial premises* (IEC 61918)

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

ISO 11898-1, *Road vehicles - Controller area network (CAN) – Part 1: Data link layer and physical signalling*

3 Terms, definitions, symbols, abbreviated terms and conventions

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

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 61784–3, EN 50325-4 and the following apply.

3.1.1
logical device
representation of a program in terms of its objects from one device profile segment (see EN 50325-4) and behaviour as viewed through a network

3.1.2
SR application object
application object in accordance with EN 50325-4 that includes all necessary measures to ensure its integrity with the requirements of EN 61508 series

3.1.3
SR communication profile and protocols
communication profile and protocols that include all the necessary measures to ensure safe transmission of data and the necessary measures to ensure safe configuration with the requirements of EN 61508 series

3.1.4
SR device
composition of regular communication profile and protocols as defined in EN 50325-4, SR communication profile and protocols, regular logical devices and SR logical devices

3.1.5
SR logical device
logical device that includes all necessary measures to ensure safe operation with the requirements of EN 61508 series

3.2 Symbols and abbreviated terms

For the purposes of this document, the following abbreviations apply.

3.2.1 Common symbols

CAN	Controller Area Network	[ISO 11898-1]
CAN-ID	CAN Identifier	[ISO 11898-1]
COB	Communication Object	[EN 50325-4]
COB-ID	COB Identifier	[EN 50325-4]
CRC	Cyclic Redundancy Check	
DLL	Data Link Layer	[ISO/IEC 7498-1]
E/E/PE	Electrical/Electronic/Programmable Electronic	[EN 61508-4]
EMC	Electromagnetic Compatibility	
EUC	Equipment Under Control	[EN 61508-4]
FAL	Fieldbus Application Layer	[EN 61784–3]
FCS	Frame Check Sequence	
FSCP	Functional Safety Communication Profile	[EN 61784–3]

NMT	Network Management	[EN 50325-4]
NSR	Non-safety-related	
PDU	Protocol Data Unit	[ISO/IEC 7498-1]
PES	Programmable electronic system	[EN 61508 series]
PFD	Average probability of failure on demand	[EN 61508-6]
PFH	Probability of failure per hour	[EN 61508-6]
PhL	Physical Layer	[ISO/IEC 7498-1]
RTR	Remote Transmission Request	[ISO 11898-1]
SCL	Safety Communication Layer	[EN 61784–3]
SFRT	Safety Function Response Time	[EN 61784–3]
SIL	Safety Integrity Level	[EN 61508 series]
SR	Safety-related	

3.2.2 Additional symbols

GFC	Global Failsafe Command
PDO	Process Data Object
SCT	Safeguard Cycle Time
SDO	Service Data Object
SRCP	Safety-related communication profile and protocols
SRD	SR device
SRDO	SR Data Object
SRLD	SR logical device
SRVT	SR Validation Time

3.3 Conventions

The conventions used for the descriptions of objects, services and protocols are described in EN 50325-4 and EN 61784–3.

This document follows the document structure as proposed in EN 61784–3, Annex C.

As appropriate this standard uses diagrams in accordance with EN 50325-4.

“Mandatory” categorizes functionalities that shall be used or implemented; “optional” categorizes functionalities that may be used or implemented.

4 Overview of CANopen Safety

CANopen defines communication profiles based on ISO 11898-1.

The basic profiles are defined in EN 50325-4. The SRCP (CANopen Safety) is based on the basic profiles in EN 50325-4 and the SCL specification defined in this standard.

The SRCP is based on the producer/consumer model. The pairing of producers and consumers is an important part of the relationship that provides the high integrity needed for SRLD.

The SCL is specified using SR data objects (SRDO). These objects are serving as the interface between the SR application objects and the link layer connections, as shown in Figure 4. An SRDO ensures the integrity of the safety data transfers.

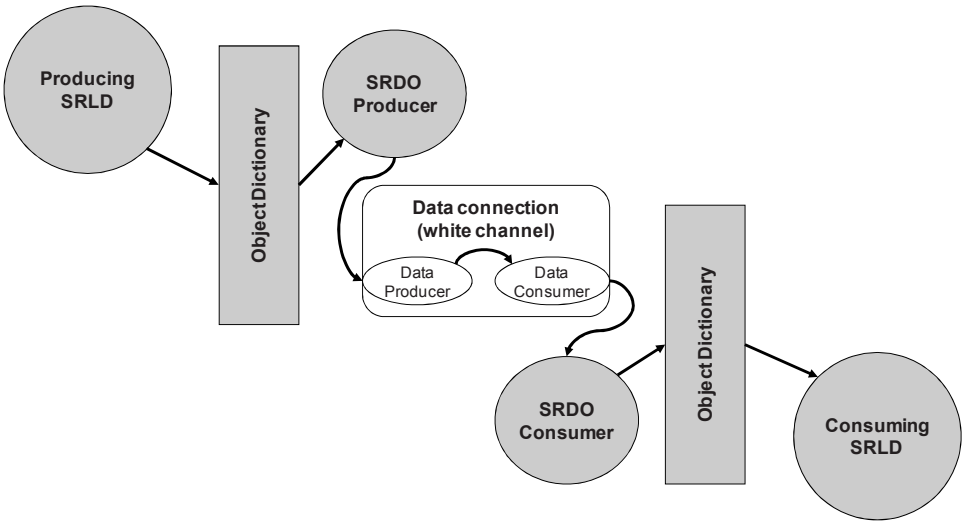


Figure 4 — Relationship of SR data objects

The safety data transfer is executed as follows:

a) the producing SRLD uses the object dictionary to pass the safe data to the SRDO producer;

b) the SRDO producer uses a link data producer to transmit the data;

c) the consuming SRLD uses the object dictionary to receive the safe data from the SRDO consumer;

d) the SRDO consumer uses a link data consumer to receive data.

The SRCP utilizes the white channel concept, which is different to the FSCP protocols defined in EN 61784–3-X. The link data producers and consumers have no knowledge of the safety packet and implement no safety function. The link data producers and consumers implementing data integrity check on per frame basis (see [17]) that are utilized by the SRCP. The responsibility for high-integrity transfer and checking of safety data lies within the SRDO.

The SRCP uses the following measures to ensure the integrity of safety messaging:

a) time expectation;

b) connection authentication;

c) redundancy with cross checking by means of two CAN messages;

d) different integrity assurance systems.

SR data is sent redundantly and cyclically. Diverse measures for producing SR messages are used to ensure that NSR messages are not interpreted as SR messages.

5 General

5.1 External documents providing specifications for the profile

The following documents are especially useful in understanding the design of this SRCP:

— EN 61508 series;

— GS-ET-26;

— EN 50325-4;

— EN 61784–3.

5.2 Safety functional requirements

The following requirements shall apply for the implementation of SRDO and safety configuration. The same requirements are used in the development of this SRCP.

— The SRCP is designed that SRDO and safety configuration are able to support SRD up to SIL3 (according to EN 61508 series) and up to category 4 (according to EN ISO 13849-1).

— The safe state for discrete data and analogue values shall be defined by the SRLD.

— The SRCP is implemented using the white channel approach.

— Implementations of this SRCP shall comply with EN 61508 series.

— Environmental conditions shall be according to EN 61000-6-2 for the basic levels, and EN 61326-3-1 and EN 61326-3-2 for the increased EMC tests, unless there are other specific product standards.

— SR communication shall be independent from NSR communication. However, NSR communication defined in EN 50325-4 may use SR communication for transmission.

— Unless specified in this standard, the requirements specified in EN 50325-4 shall be unchanged for safety communication.

5.3 Safety measures

Table 1 contains the measures used to detect communication errors and the coverage provided by each measure as used.

Table 1 — Communication errors and safety measures matrix

Communication errors	Safety measures							
	Sequence number	Time stamp	Time expectation	Connection authentication	Feedback message	Data integrity assurance	Redundancy with cross checking	Different data integrity assurance system
Corruption (see EN 61784–3)							X	
Unintended repetition (see EN 61784–3)							X	
Incorrect sequence (see EN 61784–3)							X	
Loss (see EN 61784–3)							X	
Unacceptable delay (see EN 61784–3)			X					
Insertion (see EN 61784–3)				X			X	
Masquerade (see EN 61784–3)				X				X
Addressing (see EN 61784–3)				X				X

5.4 Safety communication layer structure

The safety protocol is layered on top of the NSR data link layer (the NSR data link layer and the safety communication layer are building together a “White Channel”, i.e. the SCL takes benefit from the error detection mechanisms of the underlying NSR data link layer). Figure 5 shows how the SCL is related to the EN 50325-4 based layers.

The SCL accepts data from the SRLD. The SCL compiles a SR message and transmits it over the white channel. The SCL on the other SR device receives the SR message over the white channel and decompiles its content and performs validation checks. After the data is verified it is given to the SRLD.

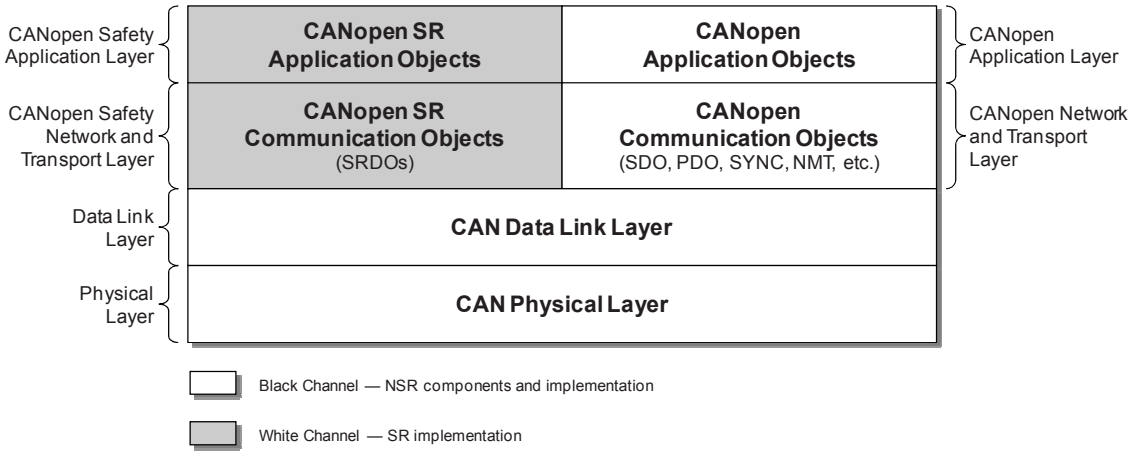


Figure 5 — Communication layers

5.5 Relationships with FAL

5.5.1 General

This SCL shall only be used in conjunction with EN 50325-4. There are no requirements other than those defined in this standard.

5.5.2 Data types

Profiles defined in this standard support all of the data types defined in EN 50325-4.

6 Safety communication layer services

6.1 Introduction

This subclause defines the extensions to EN 50325-4 for SR communication. This includes the SR data objects (SRDO; see 6.2) for use of SR data transfer between SRLD, and the global fail-safe command (GFC; see 6.3) to switch the SRLDs into the safe state immediately.

NOTE 1 The GFC itself is NSR. If a switch of a SRLD into the safe state is required and requested, then a SRDO should be used in any case (see 6.3.1).

This subclause defines also the SR communication objects. These SR communication objects are using the object dictionary as defined in EN 50325-4.

The SR application object shall not exceed a length of 8 octets. The more detailed definition of SR application objects does not fall into the scope of this standard.

NOTE 2 Depending on the SRLD different standards can apply, e.g. EN 61800-5-2 for a drive application.

6.2 SR data object (SRDO)

6.2.1 Introduction

The SR data transfer is performed by means of an SRDO. An SRDO shall be transmitted cyclically. The cyclic transmission is monitored. An SRDO may be transmitted event-driven in addition to the cyclic transmission, if required. An SRDO shall not be transmitted or requested by use of a RTR.

NOTE 1 The event-driven transmission is used to ensure a fast reaction for NSR application. Figure 6 shows a cyclic SRDO transmission with the cycle time t_{cycle} and an event-driven SRDO in between.

NOTE 2 The maximum number of SRDO producers in the system is limited to 64.

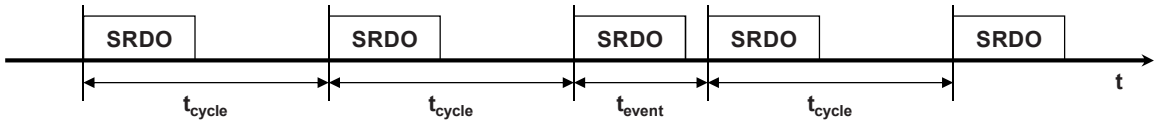


Figure 6 — Example of SRDO transmission

Two types of SRDOs are distinguished:

— the SRDO producer shall be used to transmit SR application data; and

— the SRDO consumer shall be used to receive SR application data.

An SRDO shall have the following attributes:

— SRDO number: SRDO number [1.64] for every user type on the local SRD;

— user type (6.4.1.3): one of the values {consumer, producer};

— data type (6.4.1.4): according to the SRDO mapping;

— refresh-time (6.4.1.3): n in multiples of millisecond, n > 0, for the user type producer;

— SCT (6.4.1.3): n in multiples of millisecond, n > 0, for the user type consumer;

— validation-time (6.4.1.3): n in multiples of millisecond, n > 0, for the user type *consumer.*

The SRDO services are defined in 6.2.2 and 6.2.3. The SRDO protocol is defined in 7.1. The SRDO communication objects are defined in 6.4.1.

6.2.2 SRDO write

The SCL service SRDO write shall use the push model as defined in EN 50325-4 and shall be unconfirmed. An SRDO shall have exactly one SRDO producer and shall have one or more SRDO consumers. The successful reception of an SRDO by the SRDO consumer shall be signalled by a local event to the SRLD.

The SCL service SRDO write shall be used to transmit mapped SR application data from the SRDO producer to the SRDO consumer(s). Table 2 defines the parameters for this service.

Table 2 — SRDO write

Parameter	Request / Indication
Argument	**Mandatory**
SRDO number	Mandatory
SR application data	Mandatory

6.2.3 SRDO read

The SCL service SRDO read is not allowed.

6.3 Global fail-safe command (GFC)

6.3.1 Introduction

The GFC may be used to switch the SRLDs into the safe state. This improves the overall system reaction time in case of an error. The GFC itself is NSR and shall be transmitted event-driven. The GFC itself is NSR and as such the SRDO corresponding to the failure shall be transmitted to maintain safety.

EXAMPLE In the detection of a failure the detection SRLD may transmit the GFC. Based on the GFC all SRLDs are switching into the safe state before the cycle time for the next SRDO has elapsed. Thus the SR system switches into the safe state with an improved reaction time.

The GFC shall have the following attributes:

— user type: one of the values {consumer, producer};

— data type: nil.

The GFC service is defined in 6.3.2. The GFC protocol is defined in 7.2. The GFC communication object is defined in 6.4.2.

6.3.2 GFC write

The SCL service GFC write shall use the push model as defined in EN 50325-4 and shall be unconfirmed. The GFC shall have one or more SR producers and shall have one or more SR consumers.

The SCL service GFC write shall be used to switch the SRLDs into the safe state. This service has no parameters.

6.4 SR communication objects

6.4.1 SRDO communication objects

6.4.1.1 Introduction

The SRDO communication objects are used to configure an SRDO on the SRD. An SRDO is configured by means of its communication behaviour with the SRDO communication parameter and by means of its content with the SRDO mapping parameter. The validity of the configuration is guaranteed by means of the safety configuration signature (see 6.4.1.5).

6.4.1.2 SRDO communication parameter record

Table 3 defines the complex data type used to describe the SRDO communication parameter.

Table 3 — SRDO communication parameter record

Index	Sub-index	Description	Data type
0026_h	00_h	Highest sub-index supported	UNSIGNED8
	01_h	Information direction	UNSIGNED8
	02_h	Refresh-time / SCT	UNSIGNED16
	03_h	SRVT	UNSIGNED8
	04_h	Transmission type	UNSIGNED8
	05_h	COB-ID 1	UNSIGNED32
	06_h	COB-ID 2	UNSIGNED32

6.4.1.3 SRDO communication parameter

This object indicates the communication behaviour of an SRDO. Each supported SRDO from SRDO 1 to SRDO 64 shall have its own object with an index from 1301_h to 1340_h, where SRDO 1 shall correspond to the object at index 1301_h, SRDO 2 shall correspond to the object at index 1302_h, and so on.

The sub-index 00_h shall indicate the highest supported sub-index and shall be set to 06_h.

The sub-index 01_h shall indicate if the SRDO shall be produced, shall be consumed, or shall be not valid and deleted. If this entry is set to produce the SRDO the SRLD shall request the SCL service SRDO write with the mapped SR application data. If this entry is set to consume the SRDO the SRLD shall move the received SR application data from the SRDO to the SRLD if the reception is indicated from the SCL service SRDO write and the verification of the SR data is successful.

The sub-index 02_h shall indicate the refresh-time and SCT for the SRDO as defined in 7.1.2.

The sub-index 03_h shall indicate the SRVT for the SRDO as defined in 7.1.2.

The sub-index 04_h shall indicate the transmission type as defined in EN 50325-4.

The sub-index 05_h shall indicate the CAN-ID that shall be used by the SRDO for the plain SR data (first CAN data frame). This CAN-ID shall be an odd number (see 7.1.1).

The sub-index 06_h shall indicate the CAN-ID that shall be used by the SRDO for the bitwise inverted SR data (second CAN data frame). This CAN-ID shall be the even number following the CAN-ID indicated in sub-index 05_h (see 7.1.1).

The objects are defined in Table 4 and the entries of these objects are defined in Table 5.

Table 4 — Object definition

Attribute	Definition
Index	1301_h to 1340_h
Name	SRDO communication parameter
Object code	RECORD
Data type	SRDO communication parameter record (0026_h)
Category	Mandatory for each supported SRDO

Table 5 — Entry definition

Attribute	Definition
Sub-index	00_h
Name	Highest sub-index supported
Entry category	Mandatory
Access	ro
PDO mapping	No
Value range	06_h
Default value	06_h
Sub-index	01_h
Name	Information direction
Entry category	Mandatory
Access	ro, if NMT state is Operational rw, if NMT state is Pre-operational
PDO mapping	No
Value range	00_h — does not exist / is not valid 01_h — Exists / is valid for transmit (tx, SRDO producer) 02_h — Exists / is valid for receive (rx, SRDO consumer) 03_h to FF_h — reserved
Default value	1301_h : Node-ID = 1_d to 32_d — 01_h Node-ID = 33_d to 64_d — 02_h Node-ID = 65_d to 127_d — 00_h 1302_h to 1340_h : 00_h
Sub-index	02_h
Name	tx : refresh-time rx : SCT
Entry category	Mandatory
Access	ro, if NMT state is Operational rw, if NMT state is Pre-operational
PDO mapping	No
Value range	UNSIGNED16
Default value	tx : 25_d rx : 50_d

Table 5 — Entry definition *(continued)*

Attribute	Definition
Sub-index	03_h
Name	tx : reserved rx : SRVT
Entry category	Conditional; Mandatory, if 02_h in Sub-index 01_h is supported
Access	ro, if NMT state is Operational rw, if NMT state is Pre-operational
PDO mapping	No
Value range	UNSIGNED8
Default value	20_d
Sub-index	04_h
Name	Transmission type
Entry category	Mandatory
Access	ro
PDO mapping	No
Value range	254_d
Default value	254_d
Sub-index	05_h
Name	COB-ID 1
Entry category	Mandatory
Access	ro, if NMT state is Operational rw, if NMT state is Pre-operational
PDO mapping	No
Value range	257_d to 383_d; odd values only
Default value	1301_h : Node-ID ≤ 64_d — 0000 $00FF_h$ + (2 • Node-ID) Node-ID > 64_d — manufacturer-specific 1302_h to 1340_h : manufacturer-specific
Sub-index	06_h
Name	COB-ID 2
Entry category	Mandatory
Access	ro, if NMT state is Operational rw, if NMT state is Pre-operational
PDO mapping	No
Value range	258_d to 384_d; even values only
Default value	1301_h : Node-ID ≤ 64_d — 0000 0100_h + (2 • Node-ID) Node-ID > 64_d — manufacturer-specific 1302_h to 1340_h : manufacturer-specific

6.4.1.4 SRDO mapping parameter

This object indicates the SR application objects that are mapped into an SRDO. Each supported SRDO from SRDO 1 to SRDO 64 shall have its own object with an index from 1381_h to $13C0_h$, where the SRDO 1 shall correspond to the object at index 1301_h, the SRDO 2 shall correspond to the object at index 1381_h and so on.

The value of the entry with sub-index 00_h shall indicate the highest valid sub-index as defined in Table 6. The SRDO shall be deleted by setting the SRDO invalid before changing sub-index 00_h of this object. The structure of the entries with sub-index greater than 00_h and the procedure of the mapping are both defined at PDO mapping in EN 50325-4.

The objects are defined in Table 7 and the entries of these objects are defined in Table 8.

Table 6 — Value definition

Value	Definition
00_h	Mapping invalid (disabled)
01_h	reserved
02_h	Sub-indexes 01_h and 02_h valid (mapping valid, enabled)
03_h	reserved
04_h	Sub-indexes from 01_h to 04_h valid (mapping valid, enabled)
05_h	reserved
06_h	Sub-indexes from 01_h to 06_{hh} valid (mapping valid, enabled)
to	
$0F_h$	reserved
10_h	Sub-indexes from 01_h to 10_h valid (mapping valid, enabled)
11_h	reserved
12_h	Sub-indexes from 01_h to 12_h valid (mapping valid, enabled)
to	
$7F_h$	reserved
80_h	Sub-indexes from 01_h to 80_h valid (mapping valid, enabled)

Table 7 — Object definition

Attribute	Definition
Index	1381_h to $13C0_h$
Name	SRDO mapping parameter
Object code	ARRAY
Data type	UNSIGNED32
Category	Mandatory for each supported SRDO

Table 8 — Entry definition

Attribute	Definition
Sub-index	00_h
Name	Highest sub-index supported
Entry category	Mandatory
Access	ro, if NMT state is Operational or variable mapping is not supported rw, if NMT state is Pre-operational and variable mapping supported
PDO mapping	No
Value range	see Table 6
Default value	manufacturer-specific
Sub-index	01_h
Name	SR application data object 1 (plain data)
Entry category	Mandatory
Access	ro, if NMT state is Operational, variable mapping is not supported, or sub-index 00_h is set to a value unequal 00_h rw, if NMT state is Pre-operational, variable mapping supported, and sub-index 00_h is set to 00_h
PDO mapping	No
Value range	see PDO mapping parameter in EN 50325-4
Default value	manufacturer-specific
Sub-index	02_h
Name	SR application data object 1 (bitwise inverted data)
Entry category	Mandatory
Access	ro, if NMT state is Operational, variable mapping is not supported, or sub-index 00_h is set to a value unequal 00_h rw, if NMT state is Pre-operational, variable mapping supported, and sub-index 00_h is set to 00_h
PDO mapping	No
Value range	see PDO mapping parameter in EN 50325-4
Default value	manufacturer-specific
Sub-index	03_h
Name	SR application data object 2 (plain data)
Entry category	Optional
Access	ro, if NMT state is Operational, variable mapping is not supported, or sub-index 00_h is set to a value unequal 00_h rw, if NMT state is Pre-operational, variable mapping supported, and sub-index 00_h is set to 00_h
PDO mapping	No
Value range	see PDO mapping parameter in EN 50325-4
Default value	manufacturer-specific

Table 8 — Entry definition *(continued)*

Attribute	Definition
Sub-index	04_h
Name	SR application data object 2 (bitwise inverted data)
Entry category	Optional
Access	ro, if NMT state is Operational, variable mapping is not supported, or sub-index 00_h is set to a value unequal 00_h rw, if NMT state is Pre-operational, variable mapping supported, and sub-index 00_h is set to 00_h
PDO mapping	No
Value range	see PDO mapping parameter in EN 50325-4
Default value	manufacturer-specific
to	
Sub-index	$0F_h$
Name	SR application data object 8 (plain data)
Entry category	Optional
Access	ro, if NMT state is Operational, variable mapping is not supported, or sub-index 00_h is set to a value unequal 00_h rw, if NMT state is Pre-operational, variable mapping supported, and sub-index 00_h is set to 00_h
PDO mapping	No
Value range	see PDO mapping parameter in EN 50325-4
Default value	manufacturer-specific
Sub-index	10_h
Name	SR application data object 8 (bitwise inverted data)
Entry category	Optional
Access	ro, if NMT state is Operational, variable mapping is not supported, or sub-index 00_h is set to a value unequal 00_h rw, if NMT state is Pre-operational, variable mapping supported, and sub-index 00_h is set to 00_h
PDO mapping	No
Value range	see PDO mapping parameter in EN 50325-4
Default value	manufacturer-specific
to	
Sub-index	$7F_h$
Name	SR application data object 64 (plain data)
Entry category	Optional
Access	ro, if NMT state is Operational, variable mapping is not supported, or sub-index 00_h is set to a value unequal 00_h rw, if NMT state is Pre-operational, variable mapping supported, and sub-index 00_h is set to 00_h
PDO mapping	No
Value range	see PDO mapping parameter in EN 50325-4
Default value	manufacturer-specific

Table 8 — Entry definition *(continued)*

Attribute	Definition
Sub-index	80_h
Name	SR application data object 64 (bitwise inverted data)
Entry category	Optional
Access	ro, if NMT state is Operational, variable mapping is not supported, or sub-index 00_h is set to a value unequal 00_h rw, if NMT state is Pre-operational, variable mapping supported, and sub-index 00_h is set to 00_h
PDO mapping	No
Value range	see PDO mapping parameter in EN 50325-4
Default value	manufacturer-specific

6.4.1.5 Safety configuration signature

This object is used to secure and verify the configuration of an SRDO. To each SRDO a safety configuration signature is applied. An external SR configuration tool downloads the configuration data of an SRDO into the SRD. The SR configuration tool then calculates a CRC signature based on the configuration data of the SRDO and downloads this calculated CRC signature into the SRD. The SRD also calculates the CRC based on the configuration data of the SRDO and then compares the downloaded CRC signature with the calculated CRC signature. If both matches the configuration is valid.

The SRD and the SR configuration tool shall use the CRC algorithm (see [20]) with the generator polynomial as defined in (1) and the data as defined in (2) and Table 9 to calculate the CRC signature. Table 9 defines the parameters and the order of them used to calculate the CRC signature if SRDO 1 (object 1301_h and 1381_h) is supported. The highest sub-index of object 1381_h that shall be included into the CRC calculation is indicated by sub-index 00_h. For the CRC calculation of the CRC signature for SRDO 2 to SRDO 64 the objects from 1302_h to 1340_h and from 1382_h to $13C0_h$ shall be used accordingly. The starting seed value for the CRC calculation shall be 0000_h.

The object is defined in Table 10 and the entries of the object are defined in Table 11.

$$g(x) = x^{16} + x^{12} + x^5 + 1 \qquad (1)$$

$$\begin{aligned} d(x) = {} & a_{7\ to\ 0} \\ & + b_{7\ to\ 0} + b_{15\ to\ 8} \\ & + c_{7\ to\ 0} \\ & + d_{7\ to\ 0} + d_{15\ to\ 8} + d_{23\ to\ 16} + d_{31\ to\ 24} \\ & + e_{7\ to\ 0} + e_{15\ to\ 8} + e_{23\ to\ 16} + e_{31\ to\ 24} \\ & + f_{7\ to\ 0} \\ & + g^{1}{}_{7\ to\ 0} \\ & + h^{1}{}_{7\ to\ 0} + h^{1}{}_{15\ to\ 8} + h^{1}{}_{23\ to\ 16} + h^{1}{}_{31\ to\ 24} \\ & + g^{2}{}_{7\ to\ 0} \\ & + h^{2}{}_{7\ to\ 0} + h^{2}{}_{15\ to\ 8} + h^{2}{}_{23\ to\ 16} + h^{2}{}_{31\ to\ 24} \\ & \quad \text{to} \\ & + g^{128}{}_{7\ to\ 0} \\ & + h^{128}{}_{7\ to\ 0} + h^{128}{}_{15\ to\ 8} + h^{128}{}_{23\ to\ 16} + h^{128}{}_{31\ to\ 24} \end{aligned} \qquad (2)$$

Table 9 — SR parameter data for SRDO 1 for CRC calculation

Order	Index	Sub-index	Name	Size	Value
	1301_h		**SRDO communication parameter**		
1		01_h	Information direction	1 octet	a_7 to a_0
2		02_h	Refresh-time / SCT	2 octets	b_{15} to b_0
3		03_h	SRVT	1 octet	c_7 to c_0
4		05_h	COB-ID 1	4 octets	d_{31} to d_0
5		06_h	COB-ID 2	4 octets	e_{31} to e_0
	1381_h		**SRDO mapping parameter**		
6		00_h		1 octet	f_7 to f_0
7		01_h	Sub-index	1 octet	g^1_7 to g^1_0 (01_h)
8		01_h	SR application data object 1 (plain data)	4 octets	h^1_{31} to h^1_0
9		02_h	Sub-index	1 octet	g^2_7 to g^2_0 (02_h)
10		02_h	SR application data object 1 (bitwise inverted data)	4 octets	h^2_{31} to h^2_0
11		03_h	Sub-index	1 octet	g^3_7 to g^3_0 (03_h)
12		03_h	SR application data object 2 (plain data)	4 octets	h^3_{31} to h^3_0
13		04_h	Sub-index	1 octet	g^4_7 to g^4_0 (04_h)
14		04_h	SR application data object 2 (bitwise inverted data)	4 octets	h^4_{31} to h^4_0
to		to			
259		$7F_h$	Sub-index	1 octet	g^{127}_7 to g^{127}_0 ($7F_h$)
260		$7F_h$	SR application data object 64 (plain data)	4 octets	h^{127}_{31} to h^{127}_0
261		80_h	Sub-index	1 octet	g^{128}_7 to g^{128}_0 (80_h)
262		80_h	SR application data object 64 (bitwise inverted data)	4 octets	h^{128}_{31} to h^{128}_0

Table 10 — Object definition

Attribute	Definition
Index	$13FF_h$
Name	Safety configuration signature
Object code	ARRAY
Data type	UNSIGNED16
Category	Mandatory

Table 11 — Entry definition

Attribute	Definition
Sub-index	00_h
Name	Highest sub-index supported
Entry category	Mandatory
Access	ro
PDO mapping	No
Value range	01_h to 40_h
Default value	manufacturer-specific
Sub-index	01_h
Name	SRDO1 signature
Entry category	Mandatory, if index 1301_h is supported
Access	ro, if NMT state is Operational rw, if NMT state is Pre-operational
PDO mapping	No
Value range	UNSIGNED16
Default value	0000_h
Sub-index	02_h
Name	SRDO2 signature
Entry category	Mandatory, if index 1302_h is supported
Access	ro, if NMT state is Operational rw, if NMT state is Pre-operational
PDO mapping	No
Value range	UNSIGNED16
Default value	0000_h
to	
Sub-index	40_h
Name	SRDO64 signature
Entry category	Mandatory, if index 1340_h is supported
Access	ro, if NMT state is Operational rw, if NMT state is Pre-operational
PDO mapping	No
Value range	UNSIGNED16
Default value	0000_h

6.4.1.6 Configuration valid

This object indicates if the current configuration of the SRD is valid. The SRD shall switch its SRLDs into the safe state and shall set the value of the object to 00_h if the configuration is not valid. Any change of the content of at least one of the SR communication objects shall lead to a not valid configuration (the SRD shall set the value to 00_h). When the configuration of the SRD is finished the SR configuration tool downloads a value of $A5_h$. This shall signal the SRD that the configuration is finished and depending on additional SR verification may switch its SRLDs from the safe state into the working state.

NOTE Before the SRD switches its SRLDs from the safe state into the working state the SRLDs on the SRD performs self-tests to guarantee that in addition to the SR validation of the SCL the SRLDs have no faults. The SRLD does not fall into the scope of this standard and such the additional self-tests to test the SRLDs does not fall into the scope of this standard.

The object is defined in Table 12 and the entry of the object is defined in Table 13.

Table 12 — Object definition

Attribute	Definition
Index	$13FE_h$
Name	Configuration valid
Object code	VAR
Data type	UNSIGNED8
Category	Mandatory

Table 13 — Entry definition

Attribute	Definition
Sub-index	00_h
Access	ro, if NMT state is Operational rw, if NMT state is Pre-operational
PDO mapping	No
Value range	00_h to $A4_h$ — configuration is not valid $A5_h$ — configuration is valid $A6_h$ to FF_h — configuration is not valid
Default value	00_h

6.4.2 GFC communication objects

6.4.2.1 GFC parameter

This object indicates if the SRD has requested a GFC or a GFC has been indicated. The SRD shall set the value of the GFC parameter to 01_h if the SRD has requested the SCL service GFC write (see 6.3). The SRD shall set the value to 01_h if the SCL service GFC write (see 6.3) has been indicated at the SRD. Otherwise the value shall be set to 00_h.

The object is defined in Table 14 and the entry of the object is defined in Table 15.

Table 14 — Object definition

Attribute	Definition
Index	1300_h
Name	Global fail-safe command parameter
Object code	VAR
Data type	UNSIGNED8
Category	Optional

Table 15 — Entry definition

Attribute	Definition
Sub-index	00_h
Access	rw
PDO mapping	No
Value range	00_h — GFC is not valid 01_h — GFC is valid 02_h to FF_h — reserved
Default value	00_h

7 Safety communication layer protocol

7.1 SRDO

7.1.1 General

An SRDO shall consist of two CAN data frames with CAN-IDs, which shall be different in at least two bit positions. The second CAN data frame shall be transmitted immediately after the transmission of the first CAN data frame is finished. The SR application data of the second CAN data frame shall be the bitwise inverted SR application data of the first CAN data frame. The reception of both CAN data frames shall be monitored.

NOTE The implementation of the SR logical device should take care that the SR data is safely transferred to this SRCP, because this is not covered by this standard as shown in Figure 1.

7.1.2 Timing requirements

The SRDO is transmitted as defined in 6.2.1 and the reception is monitored. The cyclic transmission rate is defined by the refresh-time and monitored with the safety cycle-time (SCT). If the SCT is elapsed before the corresponding SRDO is received the SRDO consumer shall signal the event *SCT event* to the SRLD and the SRLD shall switch into the safe state. Figure 7 shows the timing relation.

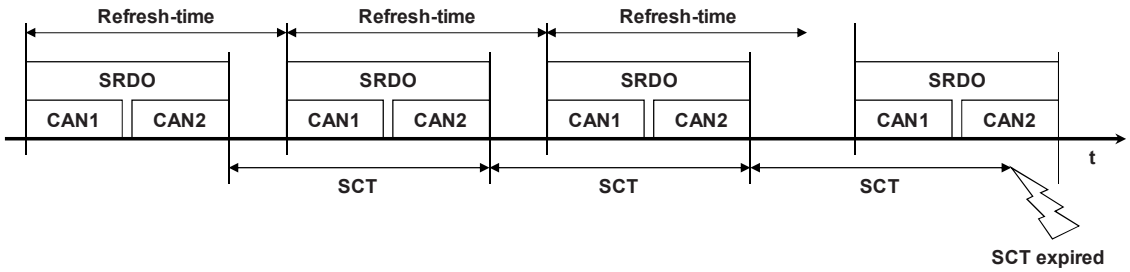


Figure 7 — Example of SCT timing

The SRDO consists of two CAN frames that are transmitted subsequently as defined in 7.1.1 and the reception is monitored. The reception is monitored with the SR validation time (SRVT). If the SRVT is elapsed before the second CAN data frame is received the SRDO consumer shall signal the event *SRVT event* to the SRLD and the SRLD shall switch into the safe state. Figure 8 shows the timing relation.

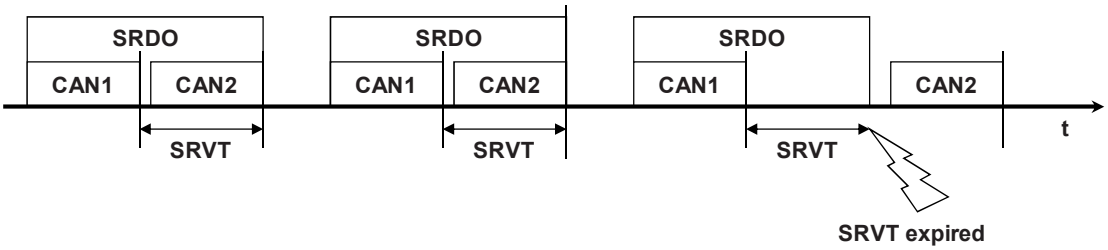
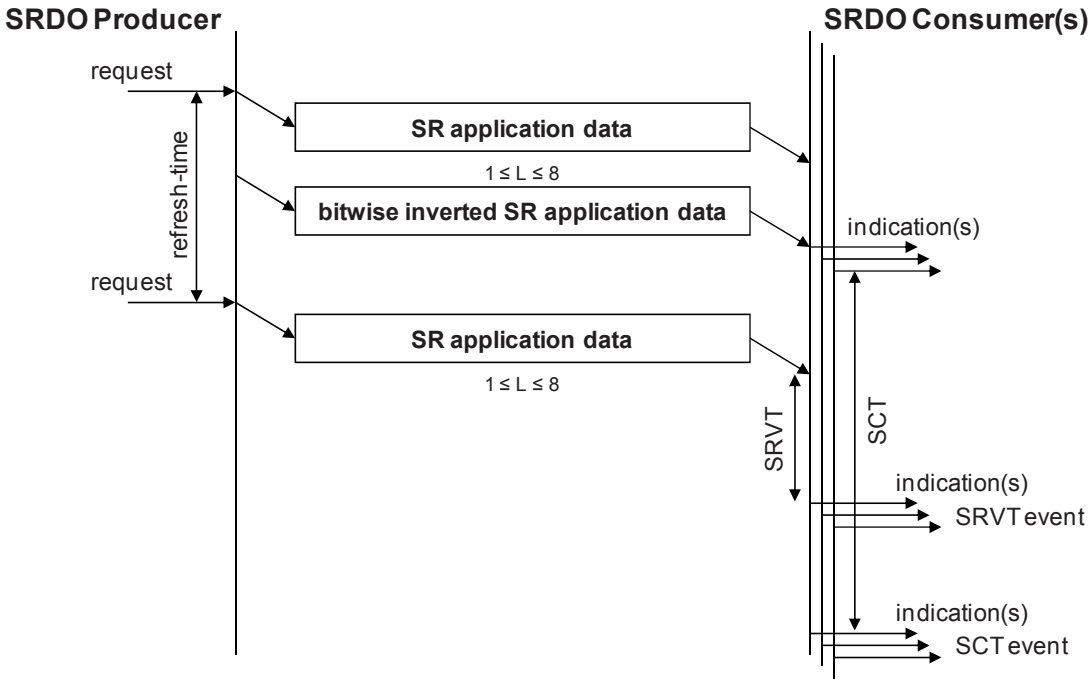


Figure 8 — Example of SRVT timing

NOTE The SCT and SRVT timer values need to be chosen in consideration of the amount of possible telegrams with higher priority than the SRDO. Using the GFC allows to choose a longer interval for SCT and SRVT.

7.1.3 SRDO write

Figure 9 defines the protocol for the SCL service SRDO write as defined in 6.2.2 and 7.1.1 including the timing requirements as defined in 7.1.2.



SR application data: up to *L* bytes of SR application data according to the SRDO mapping (see 6.4.1.4).

Figure 9 — SRDO write

If *L* exceeds the number 'n' defined by the actual SRDO mapping length, only the first 'n' data bytes shall be processed by the SRDO consumer. If *L* is less than the number 'n' the data of the received SRDO shall not be processed and an Emergency message (see EN 50325-4) with error code 8210_h shall be produced, if Emergency is supported.

NOTE 1 As defined in 6.2.1 no RTR is allowed on an SRDO.

NOTE 2 The Emergency message is defined in EN 50325-4 and is NSR.

7.2 GFC

7.2.1 General

The GFC shall be one CAN data frame with the CAN-ID 001_h. The SRLD, which detects a failure or an error, shall request the transmission of a GFC by the GFC producer. The GFC consumer shall signal via an event the reception of a GFC to their SRLD and the SRLD shall switch into the safe state.

7.2.2 GFC write

Figure 10 defines the protocol for the SCL service GFC write as defined in 6.3 and 7.2.1.

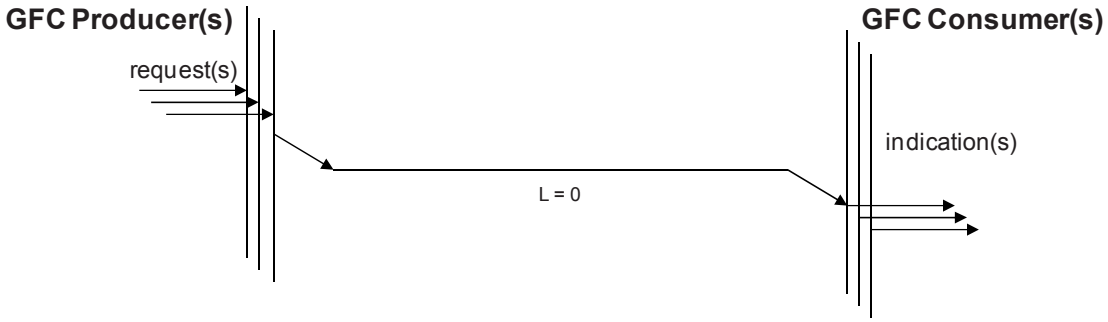


Figure 10 — GFC write

8 Safety communication layer management

8.1 Overview

This subclause refers to EN 50325-4 with respect to detailed descriptions of how to establish connections. It therefore focuses on the features used and the extensions required to support SR connections.

All SRDO connections between SRLD shall be established using SDO download as defined in EN 50325-4 by using a SR configuration tool for verification. The definition of the verification methods implemented in the SR configuration tool does not fall into the scope of this standard.

8.2 SR network initialization and system boot-up

8.2.1 Introduction

The network initialization process is controlled by the NMT master application or configuration application.

8.2.2 NMT states for SRDs

The definition for NMT of EN 50325-4 shall apply. The transmission and reception of SRDOs shall be enabled in the NMT state “Operational” and shall be disabled in all other NMT states. The SRLDs may be in the working state in the NMT state “Operational” and shall be in the safe state in all other NMT states. All SR communication objects (see 6.4) are read-only in the NMT state “Operational”, except the GFC parameter (see 6.4.2.1) and are read/write in the other NMT states, if supported. The definition of the relation between the SR application objects (see 6.1) and the NMT states does not fall into the scope of this standard.

8.3 SR device and network configuration

8.3.1 SR device configuration

The SRD shall perform the SR device configuration verification. The SR device shall calculate a CRC signature as defined in 6.4.1.5. The calculated CRC signature shall be compared with the safety configuration signature (see 6.4.1.5) written by the SR configuration tool, the SR NMT master application, or the SR configuration application. If both values are equal the configuration shall be valid (see 6.4.1.6).

NOTE The SR configuration tool, the SR NMT master application, or the SR configuration application that configures the SRD should read and compare the current configuration data including the safety configuration signature (see 6.4.1.5) from the SRD with the written configuration data, before writing the configuration valid flag (see 6.4.1.6) to the SRD. The read access should be done by use of diversified methods within the SR configuration tool, the SR NMT master application, or the SR configuration application.

8.3.2 SR network configuration

The methods and algorithms required to verify the validity of the SR network configuration do not fall into the scope of this standard. This shall be provided by a different data integrity assurance system.

9 System requirements

9.1 Indicators and switches

Indicators and switches are depending on the individual SRD.

9.2 Installation guidelines

There are no special installation requirements for this protocol. Appropriate standards shall be considered depending on the application field. In machinery and process environment the principles defined in the common part of EN 61918 shall apply.

9.3 Safety function response time

9.3.1 Introduction

The safety function response time (SFRT) is the worst-case time from a SR event as input to the system or as a fault within the system, until the time the system is in the safe state. The scope of the reaction time is shown in Figure 11 as an example.

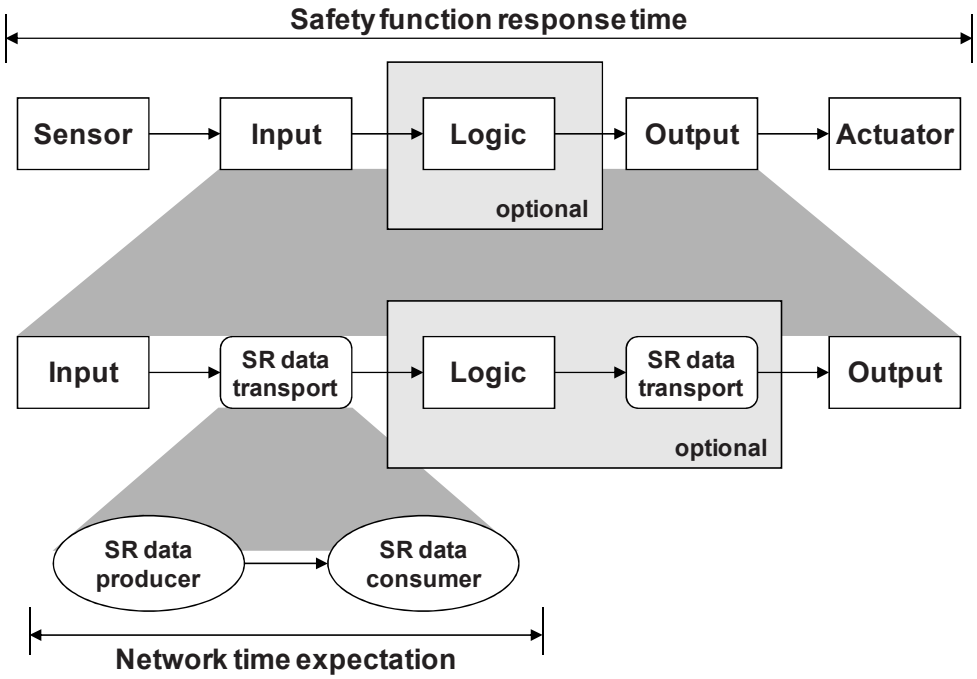


Figure 11 — Safety function response time

To determine the worst case SFRT of any SR control loop the user shall add up all the worst case safety reaction times of each subsystem of the SR control loop (see definitions in EN 61784–3).

EXAMPLE

The SFRT as shown in Figure 11 consists of the:

- sensor reaction time;
- input reaction time;
- network reaction time;
- controller reaction time, if a controller is present;
- network reaction timer, if a controller is present;
- output reaction time; and
- actuator reaction time.

Then the SFRT is the sum of the above mentioned worst case reaction times:

+ worst case sensor reaction time
+ worst case input reaction time
+ worst case network reaction time
+ worst case controller reaction time
+ worst case network reaction time
+ worst case output reaction time
+ worst case actuator reaction time
+ worst case delta time of a subsystem that fails when the safety function trips

= safety function response time (3)

9.4 Constraints for the calculation of system characteristics

9.4.1 Number of SRDOs

The number of SRDO producers is limited to 64 in a SR system. The number of SRDO consumers is not limited.

NOTE The number of SRDO producers is limited, because of compatibility reasons with EN 50325-4, which has only 128 high priority CAN identifiers reserved, and the limited available bandwidth. Allowing more SRDO producers will increase the probability of too much traffic on CAN resulting in SR reactions by mere overload.

9.4.2 Residual error probability for SRDO

This subclause will describe the calculations used for the determination of the residual error probability for SRDO.

The worst-case residual error probability for CAN according to [17], [18] and [19] is given in (4). This worst-case residual error probability is used because the data link layer is used as part of the white channel approach in difference to the black channel approach defined by the FSCPs defined in EN 61784–3-X.

$$R(P_{CAN}) = 7 \bullet 10^{-9} \approx 1 \bullet 10^{-8} \quad (4)$$

The worst-case residual error probability is squared according to GS-ET-26 for the use of Model III (see A.4) as shown in (5). The other models may be used, but then it shall be shown that the following formula is still valid.

$$R_{SL}(P) = R(P_{CAN})^2 = 4{,}9 \bullet 10^{-17} \quad (5)$$

NOTE 1 The definition for white channel (EN 61784–3) requires an assessment of the complete solution with all possible errors and failures of the transmission channel according to EN 61508 series.

NOTE 2 The residual error probability calculated in this subclause and the formula used is based on the assumption that an implementation of this SRCP uses redundant mechanisms or diversified methods to maintain safety.

9.5 Maintenance

There are no special maintenance requirements for this protocol.

9.6 Safety manual

Implementers of this part shall supply a safety manual with the following information at a minimum:

a) the safety manual shall inform the users of constraints for calculation of system characteristics (see 9.4);
b) the safety manual shall inform the users of their responsibilities in the proper parameterization of the devices (6.4);
c) the safety manual shall contain advises on calculating the expected maximum network reaction time.

In addition to the requirements of this clause the safety manual shall follow all requirements in the EN 61508 series.

10 Assessment

It is highly recommended that implementers of SRCP obtain verification from an independent assessor for all functional safety aspects of the product, both the protocol and any application. It is highly recommended that implementers of SRCP obtain proof that an independent assessor has performed a suitable conformance test.

Information on assessment services can be inquired by the following institution:

CAN in Automation (CiA)
Kontumazgarten 3
90429 Nuremberg
Germany
www.can-cia.org

NOTE See EN 61508, for the definition of independent assessor.

11 Conformance

The safety related communication profile and protocols (SRCP) within this standard is based on EN 50325-4.

A statement of conformance to this SRCP shall be stated as conformance to EN 50325-5.

Conformance means that all mandatory requirements of this SRCP for the particular SR system, SRD, or SRLD shall be fulfilled.

Product standards shall not include any Conformity Assessment aspects (including QM provisions), either normative or informative, other than provisions for product testing (evaluation and examination).

Annex A
(informative)

Example SR communication models

A.1 General

This clause considers some but not all models of implementation structure for implementing the SR communication profile and protocols in this standard. These models provide different fault detection mechanisms. Models shown below are only intended to illustrate possible implementation structures. EN 61508 series shall be considered for the overall system design.

A.2 Model I

Model I shown in Figure A.1 shows a system where all communication layers (SCL, DLL, and PhL) exist twice.

The messages from both safety communication channels are verified and crosschecked. If crosschecking shows discrepancy, an appropriate action is initiated to maintain safety.

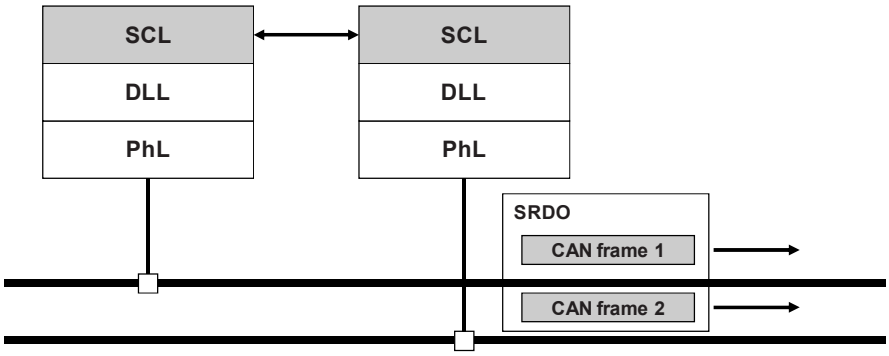


Figure A.1 — Model I

A.3 Model II

Model II shown in Figure A.2 describes a redundancy approach similar to Model I. This model uses only one transmission medium.

The messages from both safety communication channels are verified and crosschecked. If crosschecking shows discrepancy, an appropriate action is initiated to maintain safety.

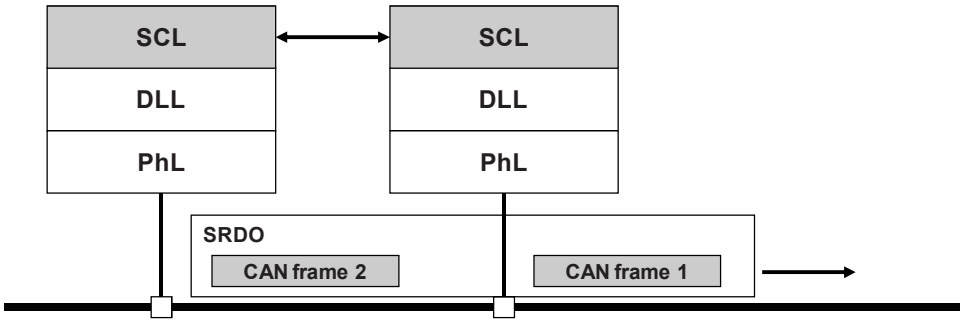


Figure A.2 —Model II

A.4 Model III

Model III shown in Figure A.3 describes a redundancy approach similar to Model II. This model uses only one PhL implementation. The PhL implementation is regarded as part of the very same black channel like to the transmission medium itself.

The messages from both safety communication channels are verified and crosschecked. If crosschecking shows discrepancy, an appropriate action is initiated to maintain safety.

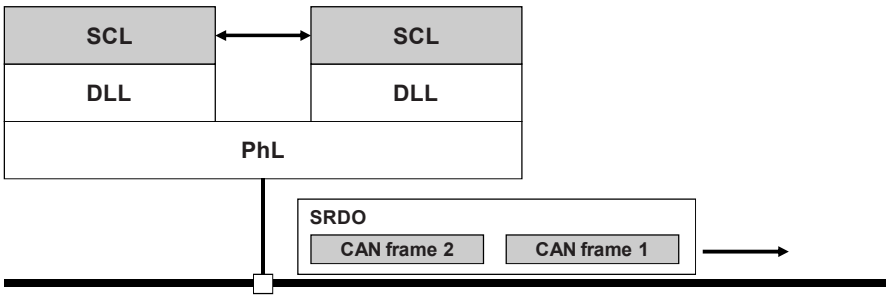


Figure A.3 — Model III

A.5 Model IV

Model IV shown in Figure A.4 describes a redundancy approach similar to Model III. This model uses only one DLL implementation. The DLL implementation is regarded as part of the very same black channel like to the PhL implementation and transmission medium. Both SCL access the DLL implementation independently.

The messages from both safety communication channels are verified and crosschecked. If crosschecking shows discrepancy, an appropriate action is initiated to maintain safety.

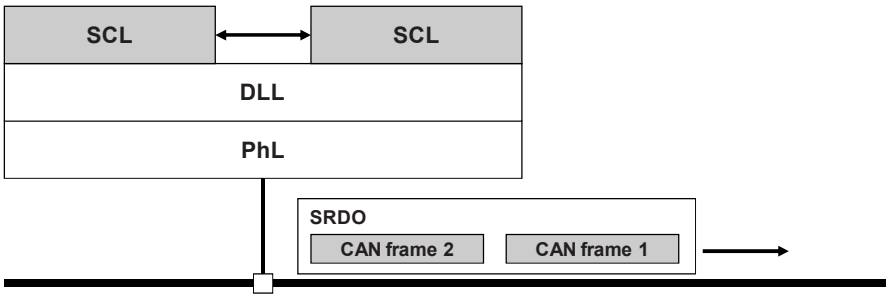


Figure A.4 — Model IV

Bibliography

[1] EN 60204-1, *Safety of machinery — Electrical equipment of machines — Part 1: General requirements*

[2] EN 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 1: General requirements*

[3] EN 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations*

[4] EN 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 6: Guidelines on the application of IEC 61508–2 and IEC 61508–*3

[5] EN 61511 (series), *Functional safety – Safety instrumented systems for the process industry sector* (IEC 61511 series)

[6] EN 61800-5-2, *Adjustable speed electrical power drive systems — Part 5-2: Safety Requirements — Functional*

[7] EN 62061, *Safety of machinery — Functional safety of safety-related electrical, electronic and programmable electronic control systems* (IEC 62061)

[8] EN/CLC/TS 61496 (series), *Safety of machinery — Electro-sensitive protective equipment*

[9] EN ISO 10218-1, *Robots for industrial environments — Safety requirements - Part 1: Robot* (ISO 10218-1)

[10] EN ISO 12100-1, *Safety of machinery — Basic concepts, general principles for design — Part 1: Basic terminology, methodology* (ISO 12100-1)

[11] EN ISO 13849-1, *Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design* (ISO 13849-1)

[12] EN ISO 13849-2, *Safety of machinery — Safety-related parts of control systems — Part 2: Validation* (ISO 13849-2)

[13] EN ISO 14121-1, *Safety of machinery — Risk assessment — Part 1: Principles* (ISO 14121-1)

[14] EN 61131-6 [1)], *Programmable controllers — Part 6: Functional safety*

[15] ISO/IEC 7498 (series), *Information processing systems — Open Systems Interconnection — Basic Reference Model*

[16] GS-ET-26, *"Grundsatz für die Prüfung und Zertifizierung von Bussystemen für die Übertragung sicherheitsrelevanter Nachrichten",* May 2002; HVBG, Gustav-Heinemann-Ufer 130, D-50968 Köln ("Principles for Test and Certification of Bus Systems for Safety relevant Communication") [2)]

[17] J. Charzinski, *"Performance of the Error Detection Mechanisms in CAN",* Proceedings of the 1st International CAN Conference, Mainz, Sep. 1994; CiA, Kontumazgarten 3, 90429 Nuremberg, Germany

---

1) Under consideration.

2) An English version of this document is in preparation, which will replace this reference when published.

[18] Dr.-Ing. H.-J. Mathony, Dr. rer. nat. J. Unruh, Dr.-Ing. K.-H. Kaiser, *"On the Data Integrity in Automotive Networks",* VDI Berichte Nr. 819, Sep. 1990, VDI-Verlag ISBN 3-18-090819-X

[19] N. Navet, Y.-Q. Song, *"Performance and Fault Tolerance of Real-Time Applications Distributed over CAN (Controller Area Network)"*, CiA Research Award 1997, 1997; CiA, Kontumazgarten 3, 90429 Nuremberg, Germany

[20] W. Wesley Peterson, "Error-Correction Codes", 2nd edition 1981, MIT-Press, ISBN 0-262-16-039-0

[21] NFPA79 (2002), *Electrical Standard for Industrial Machinery*

[22] ANSI/ISA-84.00.01-2004 (series), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*

[23] VDI/VDE 2180 (series), *Safeguarding of industrial process plants by means of process control engineering*

This page deliberately left blank

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services.
It presents the UK view on standards in Europe and at the international level.

It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop.** In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

Various BSI electronic information services are also available which give details on all its products and services.

Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048
Email: info@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at **www.bsigroup.com/BSOL**

Further information about BSI is available on the BSI website at **www.bsigroup.com/standards**

Copyright

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/standards

raising standards worldwide™