# 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 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 It also gives information on projects, withdrawn and replaced publications.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.

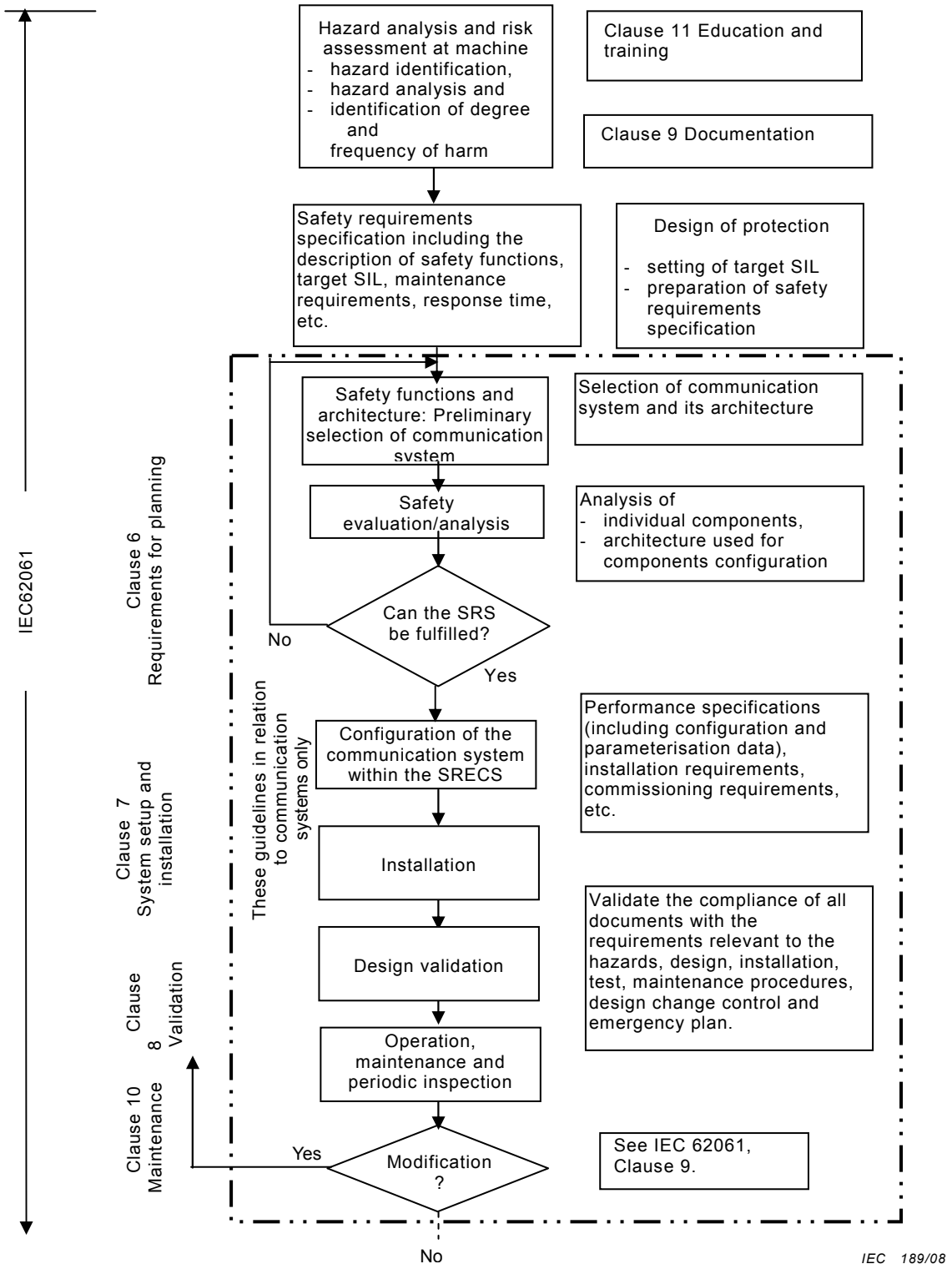
The relevant activities particularly applicable to safety-related communication systems include:

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.

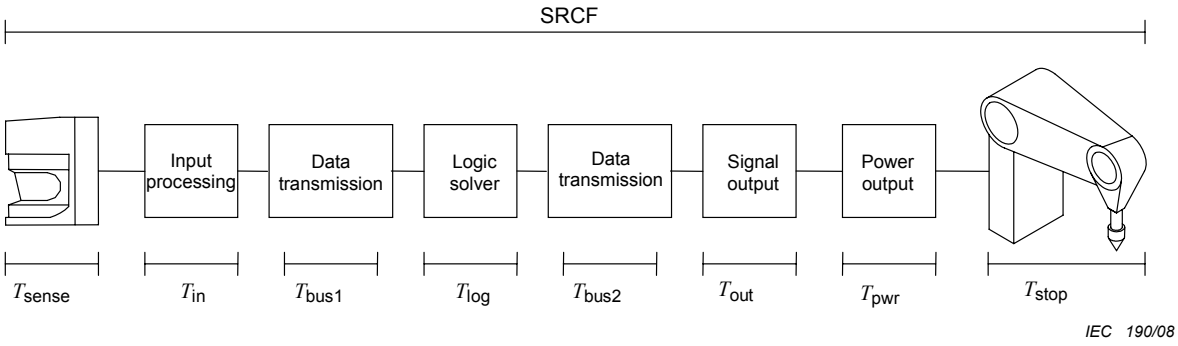



**Figure 2 – System response time components**

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.

NOTE Other delays can occur due for example to unsynchronized processes within the SRCF, and should be taken into account in calculating the worst-case response time.

It is also important to note that $T_{bus1}$ does not correlate directly to $T_{bus2}$. The values for these two parameters can be equal or different, depending for example on the upstream and downstream devices and communication settings that can affect response times.

Conforming to the response time requirement is essential. It should be checked. A sufficient margin should be considered in the design to allow for any foreseeable variations in the specified response time, including variations caused by foreseeable modifications.

### 6.1.4 Fault monitoring and alarm indication

Information about faults and their location within a SRECS can be transmitted via the communication system. It is recommended to centralize fault monitoring to enable troubleshooting in a shorter time.

For centralized fault monitoring, it is recommended that:

- any information available related to fault conditions be sent to the master station;
- the master station surveys such information;
- fault conditions are displayed in a manner that the fault is easily located and analyzed.

Other forms of fault monitoring (e.g. distributed) can also be possible.

Alarm indication should have priority over other indications and be emphasized taking ergonomic principles into account. Alarm indication should not impact the ability to perform any safety function.

### 6.1.5 Assuring functional safety in case of SRECS failure

Consideration should be given to failures that can occur in the SRECS including the safety-related communication system. Countermeasures against the effects of such failures should be included at the design stage.

The safety-related communication system should be selected and integrated within a SRECS considering the following:

- intended use including foreseeable misuse;
- malfunctions (failures), and
- foreseeable human errors while the machine is operated as intended.

Examples of malfunctions (failures) are as follows:

- error of data input from various switches and sensing devices;
- error of data processing due to the malfunction of node;
- actuator operation in case of erroneous output from the network;
- node input and output in case of network failure;
- input and output in case of master failure, etc.

The behaviour of the SRECS in relation to the SRS in case of these communication failures should be assessed at an early stage and the system should be so designed that countermeasures (e.g. fault reaction functions) against such failures are incorporated.

### 6.2 Selection criteria of the safety-related communication system

#### 6.2.1 Architecture and application fields

An adequate safety-related communication system for the application should be selected since different safety-related communication systems have different data transmission capabilities.

When selecting the safety-related communication system, at least the following items should be considered:

- maximum response time;
- number of nodes required to perform the safety-related control functions, and
- application fields;
- transmission speed;
- transmission distance;
- spare nodes for future use.

NOTE These items are not listed in order of priority.

#### 6.2.2 Maximum response time

The required response time for the SRCF should not be exceeded under any circumstances (e.g. including transmission errors and any adverse effects of EMI on the safety-related communication system). The maximum response time of the safety-related communication system can vary depending on a number of characteristics associated with both its design and application.

NOTE The maximum response time of the safety-related communication system is equivalent to the fieldbus safety response time given in IEC 61784-3.

The items that affect the maximum response time include, but are not limited to, the following:

- delay time of the safety input device (include input delay timer);
- delay time of safety communication;
- processing time of safety controller;
- delay time of the safety output device;
- behaviour of the communication system in case of failure.

In addition, the following need to be considered:

- the number of nodes connected to the network;
- processing time of logic in host controller;
- processing time in the slave controller (turn on time/turn off time, etc.);
- network settings such as number of retries;
- repeater delay if applicable;
- asynchronous/synchronous communication;
- response time of devices.

In order to select a safety-related communication system that satisfies the maximum response time required by the SRS, the maximum response time should be calculated before installation in accordance with the instruction manual of the safety-related communication system.

Any modification of the system (including network or nodes) should be assessed for any impact on the response time of the system.

#### 6.2.3 Transmission distance, transmission speed and the number of nodes

The settings for transmission distance and transmission speed should be in accordance with the supplier's specification for the type and length of the cable to be used. Check the particular safety-related communication system for the variability of the maximum response time depending on the number of nodes to be incorporated. If it varies, the network needs to be developed with the number of nodes required to fulfil the safety-related control function while providing an adequate response time.

For safety-related communication systems in which multiple transmission speeds are provided, the maximum transmission distance depends on the transmission speed selected. It should be noted that a higher speed corresponds to a shorter maximum transmission distance.

#### 6.2.4 Environmental conditions

The safety-related communication system should be selected considering the environmental conditions such as ambient temperature, vibration, shock, and electromagnetic interference. In order to avoid malfunctions, such as fading of output signals, the general rules on wiring for immunity to external disturbances, for example separation of the communication cables and the power cables should be observed (see IEC 60204-1).

For environmental requirements, the specifications provided by the manufacturer need to be considered.

NOTE 1 See also IEC 60204-1, IEC 62061, and IEC 61131-2.

NOTE 2 Consideration of manufacturer's specifications and environmental conditions by the system designer is very important to ensure an adequate safety performance level, due to the diversity of safety buses and their associated performance.

#### 6.2.5 Setting and configuration tools

The tools used for settings of the safety-related communication system should be checked for the provision of security means such as passwords for multiple control levels. The management method for these security means should also be defined clearly.

The setting tools used should be as recommended by the manufacturer for use with the safety-related communication system.

## 7 System installation and setup (configuration)

### 7.1 System installation

#### 7.1.1 System confirmation

Prior to system installation, it should be confirmed that the subsystems and subsystem elements are suitable for use with the safety-related communication system.

NOTE See IEC 62061, 6.12.

#### 7.1.2 Safety-related communication system wiring

##### 7.1.2.1 Communication cable specification

The following points should be followed when selecting cables:

- only cables designated or recommended by the manufacturer should be used;

- if the communication system includes both safety-related and non-safety-related devices, use the cable required by the safety-related devices;
- the type of cable is compatible with the transmission speed. The safety-related communication system can require different types of cable depending on the transmission speed;
- the type of cable is compatible with the transmission distance. The safety-related communication system can require different types of cable depending on the maximum transmission distance and/or distances between the nodes;
- possible difference in the transmission error rates for different types of cable should be checked.

#### 7.1.2.2 Wiring

The following points should be followed for wiring:

- there should be sufficient margin in cable length to avoid intolerable stress at the connection terminals and/or connectors;
- it should be checked whether the shield of wiring is to be terminated or not. In many cases, shield termination is essential to reduce the effects from external disturbances. The instruction manual must be followed;
- wiring should not be bent beyond the allowable range specified by the cable manufacturer. Especially for optical fibres, special care should be taken since communication can totally be disabled if a cable is bent beyond the allowable range;
- the termination of optical fibres should be done in accordance with the instructions given by the cable manufacturer and using the designated tool;
- the communication cables and the power cables, and the cables for AC I/O if applicable, should be laid in separate ducts. The separation distance should be in accordance with the safety-related communication system supplier's recommendation. These are essential to reduce the effect of external noise;
- each apparatus should be checked for its compatibility to the two types of wiring, branching and multi-dropped connection;
- if the safety-related communication system requires termination, termination should be in accordance with the supplier's specification.

#### 7.1.2.3 Wiring distance

The following points should be verified:

- the cable length between nodes and/or the total length of the cable in accordance with the safety-related communication system supplier's specification;
- the fact that the distance between every pair of nodes is within the allowable range does not guarantee that the total length of the cable is within the allowable range. The actual cable length should be checked after wiring work;
- the check for the cable length should be done referring to the appropriate specification that corresponds to the type of cable used.

### 7.1.3 Selection of power supply

Power supply units should be as specified by the safety-related communication system supplier. The effect of voltage fluctuation should be considered when selecting a power supply unit for the safety-related communication system:

- it should be checked during the preparation of the specification whether the power supply for I/O needs to be separated from that for safety-related communication;
- it is recommended that power supplies complying with SELV or PELV be selected when applicable, including power supplies used for diagnostic and monitoring equipment which is connected permanently or temporarily.

### 7.1.4 Environmental conditions

Check that the environmental conditions of the installation are within specified values. If any exceeds the specification, an appropriate countermeasure should be taken before operating the system.

The following items should be checked:

- if operating temperature/humidity exceeds the specified limit value, add heaters or fans and so on to regulate it within the specified values;
- if vibration and impact exceeds the value specified for the network components, use vibration or shock absorbers to regulate them within the specified value;
- if the equipment is installed in a dusty area, a protective measure such as enclosing the control panel should be taken;

NOTE If heaters, fans, shock absorbers, dustproof enclosures, etc. are necessary to achieve the target SIL then they become part of the SRCF and require suitable integrity.

- if appropriate, carry out an EMI measurement and check that the electromagnetic environment is within the limits specified by the safety-related communication system supplier.

## 7.2 Setting

### 7.2.1 System configuration

Setting and modification of system configuration data should be done by suitably competent persons who are sufficiently trained and experienced and have responsibility for that safety system.

The system configuration can be performed using hardware and/or software. It is essential to follow the safety-related communication system manufacturer's instructions. In safety-related communication systems, most settings are performed using dedicated tools. Special attention should be paid to the management of configuration data. In order to prevent modification of settings of the system by non-authorized persons, modification of system configuration should be protected by a password.

The responsible person should control at least the following:

- passwords,
- the latest configuration data.

In the dedicated tool, the data used (e.g. a set of parameters that was set beforehand) and the information associated with the safety-related parameters, such as the identity of the operator who carried out parameter settings, date of setting and other relevant information are recorded. The responsible person should control these data as the master data.

### 7.2.2 Setting for operation

Before applying the power to the machine, the following should be set for safety-related communication.

- Operation mode
  - check the specification of modes and the method of modifying modes referring to the manufacturer's instructions.
- Transmission speed
- Node number

There are two methods for setting; using the switches built in the apparatus supporting safety-related communication and using the dedicated setting tool. Follow the manufacturer's instructions for each method.

#### 7.2.3 Setting and modification of configuration data

Attention should be paid to the following subjects when the configuration data is changed.

- There are two methods in the system configuration setting; hardware setting and software setting. It is important to check the manufacturer's instructions in advance to understand the function subject to the configuration.
- The setting data stored in the apparatus need to be verified by comparing them with the setting data following the verification procedure provided in the manufacturer's instructions.
- After changing configuration, a functional test should be carried out.

These are the responsibility of the safety system administrator.

Changing of the settings during, for example, modification must not lead to a hazardous situation.

## 8 Validation

### 8.1 Checks before applying the power

The following are the points to be checked before applying the power:

- the safety-related communication system should be checked for wiring errors such as incorrect polarity, short-circuits or earth faults by using appropriate test equipment;
- check that earthing is secure including that of other equipment;
- check that the load (e.g. machine actuators) is isolated from the power source before applying power to the safety-related communication system.

NOTE See IEC 62061, Clause 9.

### 8.2 Validation after applying the power

The following are the initial points to be checked after applying the power:

- if possible, signal waveforms in the safety-related communication system should be monitored to verify that the noise level is sufficiently low;
- all power supply voltages should be measured to check whether they are in the allowable range;
- when there is a power supply for communication separate from the power supply for control, the check mentioned above should be carried out on both supplies;
- verify that each apparatus starts up properly by checking indicators according to the instruction manual. At this stage, since parameters have not been set completely, no other check is made.

NOTE See IEC 62061, Clause 9.

### 8.3 Functional tests

During the system commissioning phase and whenever a modification is applied, functional tests should be made on each safety function to validate its conformance with the safety requirements specification.

The behaviour of the communication system should be checked in accordance with the safety requirements specification under the following circumstances:

- power supply interruption and restoration;
- wiring break;
- input/output failure;
- replacement of a slave;
- response time.

NOTE See IEC 62061, Clause 9.

### 8.4 Baseline

Following validation, the configuration data, including but not limited to the parameter settings, identity of the person who carried out parameter settings, date of setting, results of tests, version information, and other relevant data should be recorded as a baseline. This baseline should be updated whenever the safety-related communication system is modified. It can be useful to archive a copy of the previous configuration(s).

NOTE See IEC 62061, Clause 9.

## 9 Documentation

The documentation should:

- be accurate and concise;
- be easy to understand by those persons having to make use of it;
- suit the purpose for which it is intended;
- be accessible and maintainable.

The documents needed for validation of a safety-related communication system used as a subsystem of a SRECS can include:

a) safety requirements specification;
b) system specification (including system configuration, applicable standards, etc.);
c) system management plan;
d) hardware specification;
e) software specification;
f) wiring diagrams;
g) probability of hardware failure (PFH) and probability of dangerous hardware failure ($PFH_D$) estimation;
h) test plan and test report;
i) installation and operation manual;
j) baseline.

If a safety-related device, function block, or software tool to be used in a safety-related communication system has certification for its conformance to IEC 61508, the certificate should be included in the documentation. This applies also to the application software. Information on the configuration tool should also be included in the documentation.

## 10 Operation, maintenance and repair

### 10.1 Appointment of responsible person

A responsible person should be appointed to take responsibility for all maintenance activities involving the safety-related communication system. The responsible person should control operation, maintenance and repair of the safety-related communication system.

### 10.2 Developing a maintenance plan

Maintenance of the safety-related communication system should be carried out according to the maintenance plan. The maintenance plan should include the routine activities (such as periodic inspection and start test) that are required to maintain the functional safety of safety-related communication systems. The procedures for maintenance work should be documented.

The safety of the test program that is used for maintenance work and/or failure analysis should be verified.

It should be noted that the system modification plan has to be independent of the maintenance plan since the purpose of these plans is clearly different.

### 10.3 Implementing periodic maintenance

Periodic maintenance activities should be performed as long as the safety-related communication system is operated. The system should be maintained in order to keep the safety integrity level specified in the safety requirements specification until the time of disposal of the system. This clause specifies the items needed for proper maintenance.

Periodic maintenance should be carried out at intervals not longer than that of the proof test specified in the safety requirements specification and described in the maintenance plan or the manual of the manufacturer.

### 10.4 Items of maintenance work

All proof tests described in the safety requirements specification or manufacturer's specifications should be carried out. Since it is usually not possible to restore the safety-related communication system to an "as-new" condition without replacement of devices, it is recommended that where practicable devices are used in the communication system that have a lifetime or proof test interval greater than twenty years.

Where the $PFH_D$ is highly dependent on proof testing (i.e. tests intended to reveal faults not detected by diagnostic functions) then the proof test interval needs to be shown as realistic and practicable in the context of the expected use of the safety-related communication system. For example, proof test intervals of less than 10 years can be unreasonably short for many machinery applications, and a proof test interval of 20 years is often recommended. It is acknowledged that some subsystems and/or subsystem elements (for example electromechanical components with high duty cycles) will require replacement within the proof test interval.

### 10.5 Record of maintenance results

The results of maintenance procedures should be recorded and stored. The storage period should be defined in the maintenance plan. Any changes to the baseline should be recorded.

# 11 Education and training

## 11.1 General

The responsible person should implement and enforce safety education and training programs in order to maintain the safe operation of safety-related communication systems. The required items for such training are shown in the following subclauses.

## 11.2 Scope

Safety education and training should be enforced to all the persons who are involved in the operation of safety-related communication systems, for example operators, maintenance personnel, program installer, their supervisors and administrators.

## 11.3 Performing continual education and training

Periodic education and training should be carried out for all persons involved in the operation of safety-related communication systems.

Appropriate education and training should also be provided:

- when a person is appointed;
- when a safety-related communication system is modified, and
- before the system is restarted after an accident or near-miss.

## 11.4 Contents of education and training

The following items should be included in the curriculum:

- regulations and standards relevant to the safety of workers;
- principles of the protective measures;
- safety-related devices and their functions;
- operating procedures of each device;
- safe work procedures (for normal operation);
- operation procedures in case of emergency.

## 11.5 Planning of educational activities and storage of education records

Educational activities should be carried out according to the education plan, and records should be kept for a defined period.

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

## A.1 General

As mentioned above, a safety-related communication system is only a subsystem within a SRECS. According to IEC 61508 and IEC 62061, the SRECS usually consists of the components shown in Figure A.1. Instead of using conventional wiring, a safety-related communication system is used. The SILCL is usually documented in the information for use document of the supplier of the safety-related communication system.

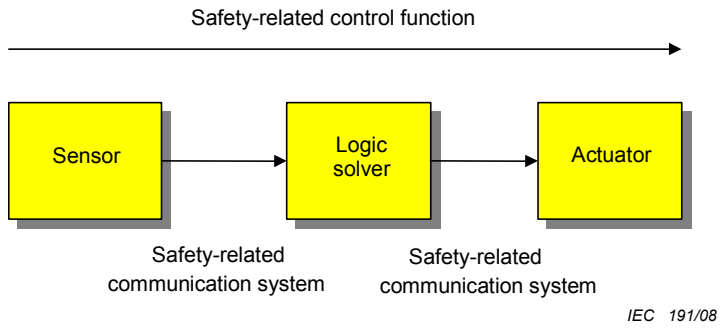



**Figure A.1 – Components of a SRECS**

A safety-related communication system performs only a part of a safety function specified for a safety relevant electrical control system. For this, sensors (e.g. guard door switch), actuators (e.g. contactor), and usually application software are also required.

The safety function of a safety-related communication system is to transmit safety relevant data from an input to an output and/or vice versa within a specified time and at a specified integrity. In this example, for simplicity the logic solver is considered to be incorporated in the safety-related communication system. This device can be a separate unit within a SRECS or a part of the safety input device or the safety output device. This depends on the architecture of the safety-related communication system.

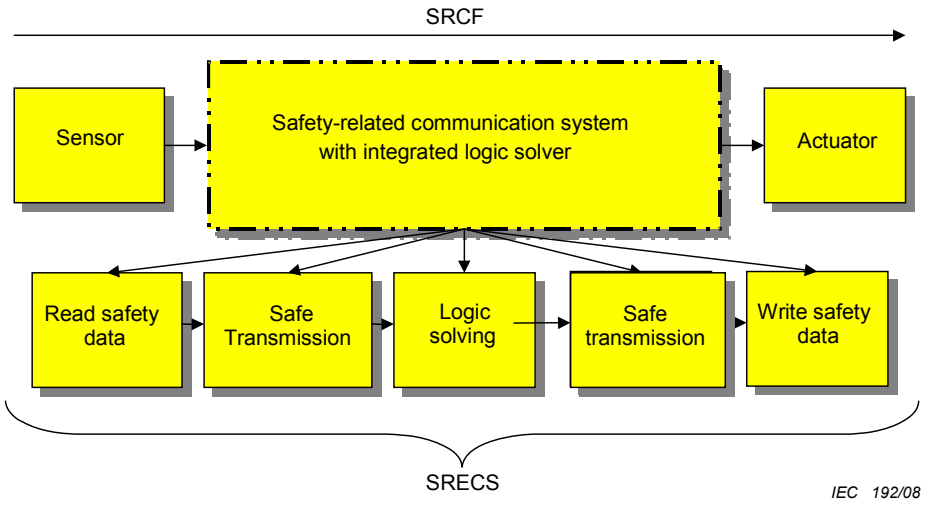



**Figure A.2 – SRECS using a safety-related communication system**

NOTE Implementation of a function block usually requires a detailed safety requirement specification. Also, a safety requirements specification for the subsystems performing the function blocks is needed. These specifications are made by the supplier of the safety-related communication system and are outwith the scope of these guidelines. Usually the supplier of a safety-related communication systems defines the maximum SILCL that can be achieved by correct parameterization of the safety-related communication system and the devices used.

The safe transmission function block ensures the safe transmission of safety relevant data from a source to a sink (e.g. transmitter to receiver): it can be divided into two additional function blocks:

– safe transmission master function block;
– safe transmission slave function block.

NOTE According to IEC 62061, a function block is performed by a single subsystem (e.g. device) only. Each function block is assigned to a subsystem within the architecture of the safety function. Several function blocks may be assigned to a single subsystem. A function block is only performed by a single subsystem.

Communication systems usually use master and slave devices. In some systems, these devices are called producer and consumer. Also multi-master communication systems usually have a unit sending a safety-related message and one or more units receiving this messages. In these guidelines, it is assumed that a master device (producer) and slave devices (consumers) are used.

Under this pre-condition, a safety-related communication system is based on the following two main subsystems (devices):

– safety relevant slave (input, output, input and output);
– safety relevant master (e.g. with safety relevant controller).

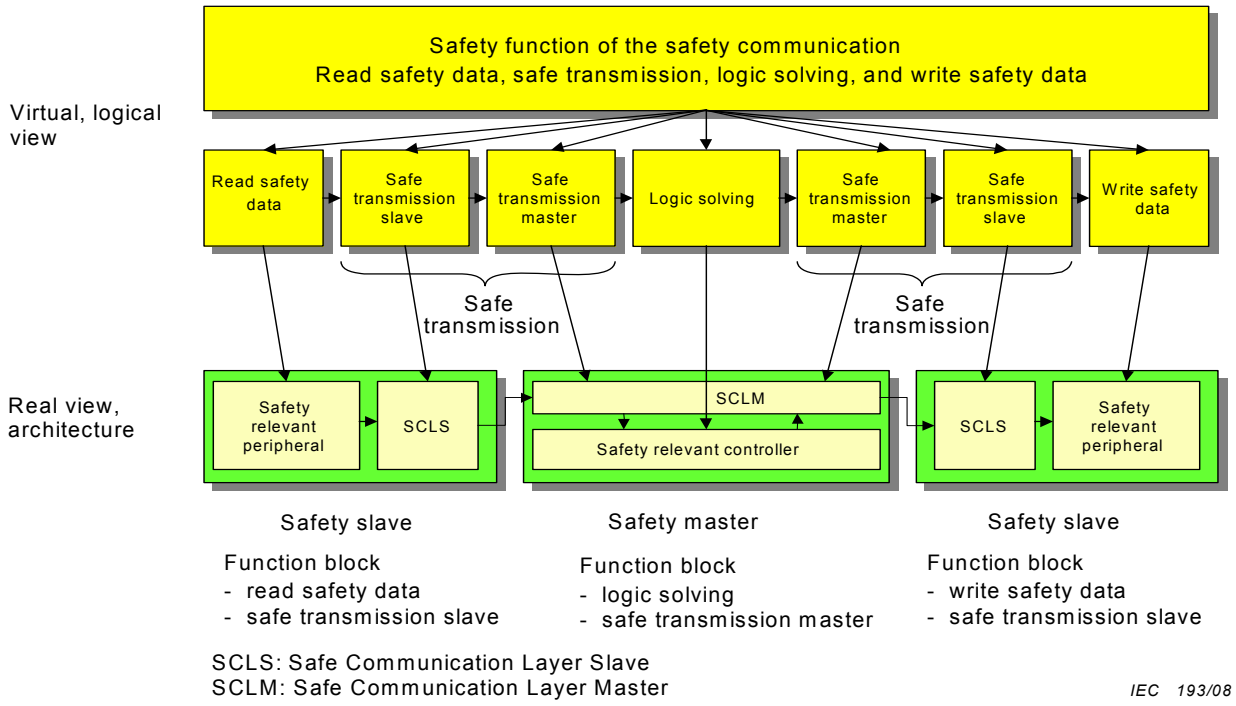



**Figure A.3 – Different views of the safety-related communication system**

Each of the subsystems (devices) performs one or more function blocks. As shown in Figure A.3, the subsystems safety-related peripheral and the SCLS are performed on a safety-related slave. Both subsystems can be separate devices too (e.g. chip set performing the SCLS services and a safety input device).

## A.2 Architecture of the safety-related communication system

In safety-related communication systems, the sensors and actuators are wired to corresponding input and output devices. These devices may be connected either locally or remotely to the logic solving unit. Typical architectures of safety-related communication systems include the following examples.

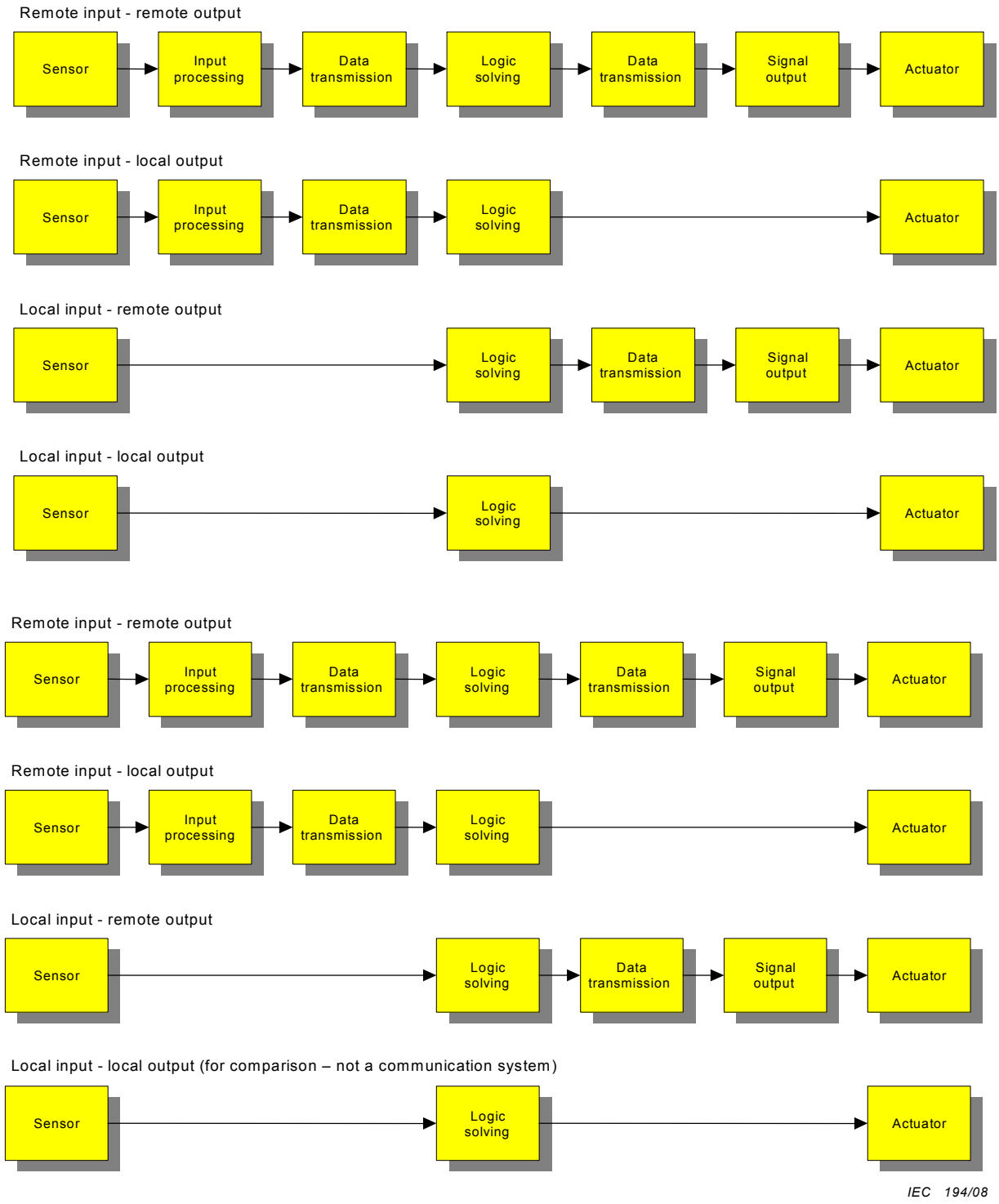



**Figure A.4 – Examples of typical architectures of safety-related communication systems**

## A.3 Calculation of the $PFH_D$ of the SRECS

For the calculation of the $PFH_D$ of the SRECS information is needed on the values which have to be taken into account. Usually, the supplier of the safety-related communication system provides these values for each safety-related device. In most cases, the $PFH_D$ of the SRECS is the summation of the $PFH_D$ of each device used within a safety loop (sensor – safety-related communication system – logic solver – actuator).

The $PFH_D$ of the sensor part depends on the parameterization of the device and the architecture (one or more sensors, with or without test pulses, …). This should be explained in the information for use document of the supplier of the safety-related devices or communication systems.

The connection of the sensors and actuators to a safety-related device of a safety-related communication system is an important aspect of achieving the required SIL of the SRCF. It is highly recommended to take into account the information for use document of the supplier.

## Bibliography

IEC 61131-2:2007, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61784-3, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile*

IEC 61918, *Industrial communication networks – Installation of communication networks in industrial premises*

IEC 62280-1: 2002, *Railway applications – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems*

ISO 12100-1:2003, *Safety of machinery – Basifc concepts, general principles for design – Part 1: Basic terminology, methodology*

ISO 12100-2:2003, *Safety of machinery – Basic concepts, general principles for design – Part 2: Technical principles*

ISO 13849-1: 2006, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 14121-1:2007, *Safety of machinery – Risk assessment – Part 1: Principles*

_____

# SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

## AVANT-PROPOS

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

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

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

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

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

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

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

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

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

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

# INTRODUCTION

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

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

## 1 Domaine d'application

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

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

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

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

## 2 Références normatives

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

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

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

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

## 3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

**3.1**
**catégorie**
classification de la partie d'un système de commande relative à la sécurité en termes de résistance aux défauts et de comportement prévisible en condition de défaut, et qui est obtenue par la disposition structurelle des parties et/ou par leur fiabilité

[ISO 13849-1, 3.1.2]

**3.2**
**système de communication**
configuration du matériel, du logiciel et des supports de propagation pour le transfert des messages entre les dispositifs, comme par exemple les capteurs, les organes de commande et les dispositifs de commande des machines

**3.3**
**configuration (réglage des paramètres)**
réglage et/ou modification de toute donnée, nécessaire(s) pour le fonctionnement du système

**3.4**
**perturbation électromagnétique**
**EMI (e*lectromagnetic interference*)**
perturbation entraînant une dégradation des performances, un dysfonctionnement ou une défaillance des dispositifs électriques et électroniques, des appareils et/ou des systèmes

NOTE Les brouillages radioélectriques sont un exemple type de telles perturbations.

**3.5**
**tolérance aux anomalies**
aptitude d'un SRECS, d'un sous-système ou d'un élément de sous-système à continuer d'accomplir une fonction requise en présence d'anomalies ou d'erreurs

[CEI 62061, 3.2.31]

**3.6**
**nœud**
point d'un système de communication au niveau duquel une ou plusieurs unités fonctionnelles interconnectent des voies de données ou des circuits de données

**3.7**
**mode de fonctionnement**
méthode ou mode de fonctionnement

**3.8**
**TBTP (très basse tension de protection)**
circuits mis à la terre, qui sont isolés de la tension dangereuse par une double isolation ou une meilleure isolation quelconque, et dans lesquels la tension ne peut pas dépasser la TBT spécifiée dans la CEI 61201 : 1992, dans les conditions normales et dans les conditions de premier défaut

[CEI 61140]

**3.9**
**essai de validité**
essai qui peut détecter les défaillances et la dégradation d'un SRECS et de ses sous-systèmes de telle sorte que, lorsque nécessaire, le SRECS et ses sous-systèmes puissent être rétablis dans une condition "comme neuf" ou dans une condition aussi proche que possible de celle-ci

[CEI 62061, 3.2.37, modifié]

NOTE Un essai de validité est prévu afin de confirmer que le SRECS est en condition d'assurer l'intégrité de sécurité spécifiée.

**3.10**
**mesure de prévention**
mesure destinée à réduire le risque, mise en œuvre:

– par le concepteur (prévention intrinsèque, mesures de protection et complémentaires, informations pour l'utilisation) et
– par l'utilisateur (organisation, méthodes de travail sûres, surveillance, système du permis de travailler, moyens de protection supplémentaires, équipements de protection individuelle, formation)

[ISO 13849-1, 3.28]

**3.11**
**mauvais usage raisonnablement prévisible**
utilisation d'une machine d'une manière ne correspondant pas aux intentions du concepteur, mais pouvant résulter d'un comportement humain aisément prévisible

[ISO 13849-1, 3.20]

**3.12**
**fonction de sécurité**
fonction d'une machine dont la défaillance peut provoquer un accroissement immédiat du (des) risque(s)

[CEI 62061, 3.2.15, et ISO 12100-1:2003, 3.28]

NOTE Cette définition diffère des définitions de la CEI 61508-4 et de l'ISO 13849-1.

**3.13**
**spécification des exigences concernant les fonctions de sécurité**
spécification qui contient les exigences nécessaires aux fonctions de sécurité qui doivent être exécutées par les systèmes relatifs à la sécurité

[CEI 61508-4, 3.5.9]

**3.14**
**intégrité de sécurité**
probabilité pour qu'un SRECS ou ses sous-systèmes exécutent de manière satisfaisante les fonctions de commande relatives à la sécurité requises dans toutes les conditions spécifiées

[CEI 62061, 3.2.19]

NOTE 1 Plus le niveau d'intégrité de sécurité de l'entité est élevé, plus la probabilité d'une défaillance de cette entité dans l'exécution de la fonction de commande relative à la sécurité requise est faible.

NOTE 2 L'intégrité de sécurité comprend l'intégrité de sécurité du matériel (voir CEI 62061, 3.2.20) ainsi que l'intégrité de sécurité systématique (voir CEI 62061, 3.2.22).

**3.15**
**niveau d'intégrité de sécurité**
**SIL (s*afety integrity level*)**
niveau discret (parmi trois possibles) permettant de spécifier les exigences concernant l'intégrité de sécurité des fonctions de commande relatives à la sécurité à allouer aux SRECS, le niveau 3 d'intégrité de sécurité possédant le plus haut degré d'intégrité et le niveau 1 possédant le plus bas

[CEI 62061, 3.2.23]

NOTE Le SIL 4 n'est pas pris en compte dans la présente norme, car il n'est pas approprié aux exigences de réduction du risque normalement associées aux machines. Pour les exigences applicables au SIL 4, voir la CEI 61508-1 et la CEI 61508-2.

**3.16**
**fonction de commande relative à la sécurité**
**SRCF (*safety-related control function*)**
fonction de commande avec un niveau d'intégrité spécifié, mise en œuvre par un SRECS, prévue pour maintenir la condition de sécurité de la machine ou empêcher un accroissement immédiat du (des) risque(s)

[CEI 62061, 3.2.16]

**3.17**
**système de commande électrique relatif à la sécurité (SRECS)**
partie électrique, électronique ou électronique programmable d'un système de commande de machine dont la défaillance peut provoquer un accroissement immédiat du (des) risque(s)

[CEI 62061, 3.2.4]

**3.18**
**spécification des exigences concernant la sécurité**
spécification contenant toutes les exigences liées aux fonctions de sécurité qui doivent être exécutées par les systèmes relatifs à la sécurité

NOTE Cette spécification se divise en deux parties, une spécification des exigences concernant les fonctions de sécurité, et une spécification des exigences concernant l'intégrité de sécurité.

[CEI 61508-4, 3.5.8]

**3.19**
**TBTS (très basse tension de sécurité)**
circuits non mis à la terre, qui sont isolés de la tension dangereuse par une double isolation ou une meilleure isolation quelconque, et dans lesquels la tension ne peut pas dépasser la TBT spécifiée dans la CEI 61201 : 1992, dans les conditions normales et dans les conditions de premier défaut

[CEI 61140]

**3.20**
**proportion de défaillances en sécurité**
**SFF (*safe failure fraction*)**
proportion du taux global des défaillances d'un sous-système qui n'entraînent pas une défaillance dangereuse

[CEI 62061, 3.2.42]

**3.21**
**limite de revendication de SIL (pour un sous-système)**
**SILCL (*SIL Claim Limit*)**
SIL maximal qui peut être revendiqué pour un sous-système de SRECS en relation avec des contraintes architecturales et l'intégrité de sécurité systématique

[CEI 62061, 3.2.24]

**3.22**
**sous-système**
entité de la conception de l'architecture générale du SRECS dans laquelle une défaillance d'un sous-système quelconque entraînera une défaillance d'une fonction de commande relative à la sécurité

NOTE 1 Un sous-système complet peut être constitué à partir d'un nombre d'éléments de sous-système identifiables et séparés qui, lorsqu'ils sont associés, réalisent les blocs fonctionnels alloués au sous-système.

NOTE 2 Cette définition est une restriction à la définition générale donnée dans la CEI 61508-4: ensemble d'éléments qui interagissent selon un modèle précis, un élément pouvant être un autre système, appelé sous-système, lequel peut être composé de matériel, de logiciel en interaction avec l'être humain.

NOTE 3 Cette définition diffère du langage courant, où le terme « sous-système » peut signifier une quelconque partie subdivisée d'une entité; le terme « sous-système » est utilisé dans la présente norme dans une hiérarchie terminologique bien déterminée: le « sous-système » est le premier niveau de subdivision d'un système. Les parties résultant de subdivisions ultérieures d'un sous-système sont appelées "éléments de sous-systèmes".

[CEI 62061, 3.2.5]

**3.23**
**validation**
confirmation par examen (par exemple essais, analyses) que les exigences de sécurité fonctionnelle de l'application spécifique sont satisfaites

[CEI 62061, 3.2.52, modifiée]

## 4 Gestion de la sécurité fonctionnelle

### 4.1 Exigences de la CEI 62061

La CEI 62061 exige qu'un plan de sécurité fonctionnelle soit dressé et documenté pour chaque projet de conception de SRECS, et qu'il soit mis à jour autant que nécessaire. Le plan inclut les procédures de contrôle des activités spécifiées dans les Articles 5 à 9 de la CEI 62061.

Le présent rapport technique suppose que la gestion des exigences de sécurité fonctionnelle spécifiée dans la CEI 62061 a été mise en application, et attire l'attention sur les questions qui sont en particulier applicables aux systèmes de communication relatifs à la sécurité.

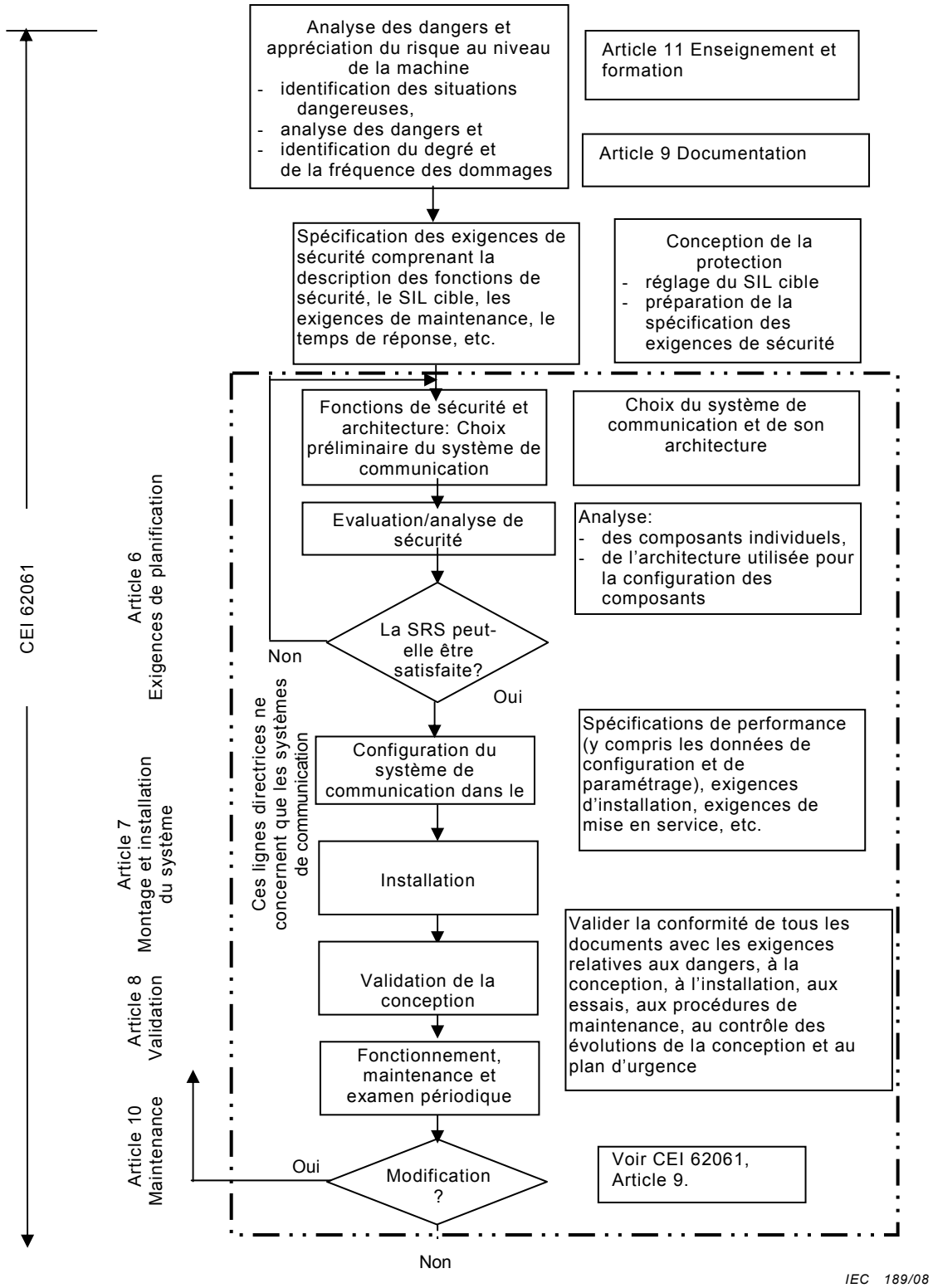
Les activités appropriées en particulier applicables aux systèmes de communication relatifs à la sécurité sont les suivantes:

a) gestion de la sélection
   – voir 6.2 ;
b) gestion de l'installation
   – voir 7.1 ;
c) gestion de la configuration et du paramétrage
   – voir 7.2 ;
d) gestion de la validation
   – voir l'Article 8 ;
e) gestion du fonctionnement, de la maintenance et des examens périodiques
   – voir l'Article 10 ;
f) gestion des modifications
   – voir la CEI 62061, Article 9.

## 5 Réalisation d'un système de commande électrique relatif à la sécurité (SRECS) à l'aide d'un système de communication relatif à la sécurité

La Figure 1 présente le processus de sélection ou de conception et de fabrication d'un SRECS satisfaisant aux fonctions de sécurité et à l'intégrité de sécurité exigées par la spécification des exigences de sécurité.

NOTE Pour le détail de la spécification des exigences de sécurité (SRS), se reporter à la CEI 62061, 5.2.




NOTE Les références aux articles se rapportent au présent document, sauf indication contraire.

**Figure 1 – Diagramme de conception et de développement d'un SRECS**

# 6 Planification du système de communication relatif à la sécurité

## 6.1 Conception du système

### 6.1.1 Niveau d'intégrité de sécurité (SIL) attribué à la (aux) SRCF(s) et au système de communication relatif à la sécurité

Le présent rapport technique suppose que la spécification des exigences de sécurité du SRECS a été élaborée conformément à la CEI 62061 et que le SIL requis a été déterminé pour chaque fonction de sécurité qui utilise le système de communication relatif à la sécurité.

Il convient que la limite de revendication de SIL (SILCL) d'un système de communication relatif à la sécurité candidat soit suffisante pour obtenir le SIL requis pour toute fonction de commande relative à la sécurité (SRCF).

NOTE L'Annexe A fournit une indication de la conception d'un SRECS utilisant un système de communication relatif à la sécurité fondé sur le concept des blocs fonctionnels.

### 6.1.2 Configuration et paramétrage du système de communication relatif à la sécurité

A l'étude.

### 6.1.3 Temps de réponse et mesures de protection

Il convient que le temps de réponse le plus défavorable (voir aussi 6.2.2) de l'entrée à la sortie du SRECS, y compris le système de communication relatif à la sécurité, soit suffisamment court pour que toutes les fonctions de sécurité de l'application spécifique puissent être réalisées pendant la durée spécifiée dans la SRS. Lorsque le temps de réponse le plus défavorable n'est pas suffisamment court pour permettre une performance adéquate des fonctions de sécurité (par exemple en raison des contraintes liées à la machine), il convient alors de prendre d'autres mesures (par exemple mesure(s) de protection supplémentaire(s), choix d'une forme alternative de système de communication relatif à la sécurité ayant amélioré le temps de réponse), afin de satisfaire aux exigences applicables de la SRS.

Le schéma ci-dessous présente les divers composants du temps de réponse du système qu'il convient de prendre en compte en ce qui concerne la communication des données à partir d'une entrée relative à la sécurité à distance d'un poste de commande, jusqu'à une sortie relative à la sécurité à distance.

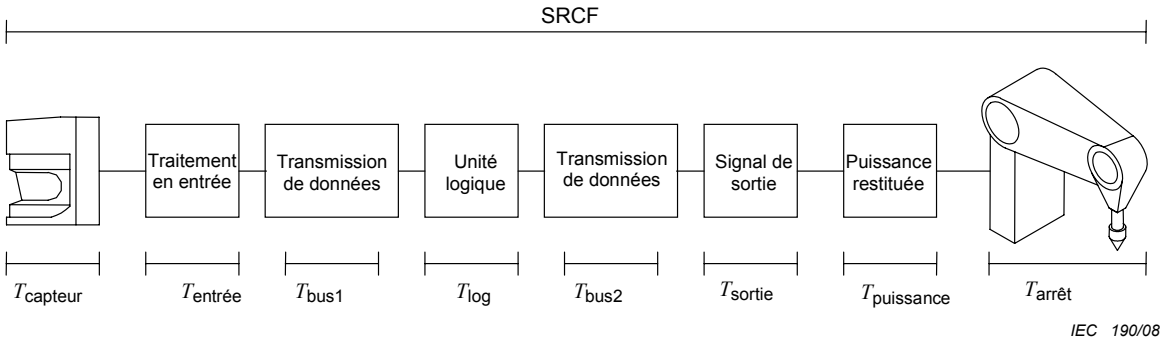



**Figure 2 – Composants du temps de réponse du système**

Le temps de réponse du système de communication relatif à la sécurité est défini par:

Temps de réponse du système de communication = $T_{bus1} + T_{bus2}$

Il est important de noter que $T_{bus1}$ et $T_{bus2}$ ne dépendent pas seulement du temps pour un cycle de bus ou un message, mais qu'ils peuvent également contenir des répétitions, des erreurs de manipulation, des temps de réponse de synchronisation, etc. Pour les détails, voir la spécification du système de communication relatif à la sécurité.

NOTE D'autres temps de réponse peuvent se produire, dus par exemple à des processus non synchronisés dans la SRCF, et il convient de les prendre en compte dans le calcul du temps de réponse le plus défavorable.

Il est également important de noter que $T_{bus1}$ n'est pas directement en corrélation avec $T_{bus2}$. Les valeurs pour ces deux paramètres peuvent être égales ou différentes, en fonction par exemple des dispositifs en amont et en aval et des réglages de communication qui peuvent affecter les temps de réponse.

La conformité à l'exigence du temps de réponse est essentielle. Il est recommandé qu'elle soit vérifiée. Il convient de prendre en compte une marge suffisante dans la conception, pour tenir compte des variations prévisibles du temps de réponse spécifié, y compris les variations provoquées par des modifications prévisibles.

### 6.1.4 Surveillance des défauts et indication d'alarme

Les informations sur les défauts et leur emplacement dans un SRECS peuvent être transmises par l'intermédiaire du système de communication. Il est recommandé de centraliser la surveillance des défauts, afin de permettre une recherche des défauts dans un laps de temps plus court.

Pour la surveillance des défauts centralisée, il est recommandé:

- que toutes les informations disponibles relatives aux conditions de défaut soient envoyées au poste maître,
- que le poste maître examine les informations de ce type,
- que les conditions de défaut soient affichées de manière à situer et analyser facilement le défaut.

D'autres formes de surveillance des défauts (par exemple distribuée) peuvent également être possibles.

Il convient que l'indication d'alarme soit prioritaire sur d'autres indications et qu'elle soit mise en valeur en tenant compte des principes ergonomiques. Il convient que l'indication d'alarme n'influence pas l'aptitude à réaliser toute fonction de sécurité.

### 6.1.5 Garantie d'une sécurité fonctionnelle en cas de défaillance du SRECS

Il convient de prendre en considération les défaillances qui peuvent se produire dans le SRECS, y compris dans le système de communication relatif à la sécurité. Il est recommandé d'inclure des contre-mesures contre les effets de telles défaillances au stade de la conception.

Il convient que le système de communication relatif à la sécurité soit choisi et intégré dans un SRECS en tenant compte des éléments suivants:

- l'utilisation prévue, y compris le mauvais usage prévisible ;
- les dysfonctionnements (défaillances) ; et
- les erreurs humaines prévisibles lorsque la machine est mise en fonctionnement comme prévu.

Parmi les dysfonctionnements (défaillances), on peut citer par exemple:

- les erreurs de données d'entrée provenant de divers interrupteurs et dispositifs de détection ;
- les erreurs de traitement des données dues au dysfonctionnement du nœud ;
- le fonctionnement de l'organe de commande en cas de données de sortie erronées en provenance du réseau ;
- l'entrée et la sortie du nœud en cas de défaillance du réseau ;
- l'entrée et la sortie en cas de défaillance du maître, etc.

Il convient que le comportement du SRECS par rapport à la SRS dans le cas de ces défaillances de communication soit évalué à un stade précoce, et que le système soit conçu de telle sorte que des contre-mesures (par exemple fonctions de réaction aux défauts) par rapport à de telles défaillances soient intégrées.

## 6.2 Critères de sélection du système de communication relatif à la sécurité

### 6.2.1 Architecture et domaines d'application

Il convient de choisir un système de communication relatif à la sécurité adéquat pour l'application, étant donné que différents systèmes de communication relatifs à la sécurité ont différentes capacités de transmission de données.

Lors de la sélection du système de communication relatif à la sécurité, il convient de prendre en considération au moins les éléments suivants:

- le temps de réponse maximal ;
- le nombre de nœuds exigés pour réaliser les fonctions de commande relatives à la sécurité ; et
- les domaines d'application ;
- la vitesse de transmission ;
- la distance de transmission ;
- les nœuds disponibles pour une utilisation ultérieure.

NOTE Ces éléments ne sont pas énumérés dans l'ordre de priorité.

### 6.2.2 Temps de réponse maximal

Il convient que le temps de réponse requis pour la SRCF ne soit pas dépassé, quelles que soient les circonstances (par exemple, y compris les erreurs de transmission et tous les effets néfastes de la perturbation électromagnétique sur le système de communication relatif à la sécurité). Le temps de réponse maximal du système de communication relatif à la sécurité peut varier en fonction d'un certain nombre de caractéristiques associées à la fois à sa conception et à son application.

NOTE Le temps de réponse maximal du système de communication relatif à la sécurité est équivalent au temps de réponse de sécurité du bus de terrain donné dans la CEI 61784-3.

Les éléments qui affectent le temps de réponse maximal comprennent, sans que l'énumération ne soit exhaustive, les éléments suivants:

- le temps de réponse du dispositif d'entrée de sécurité (y compris le temporisateur d'entrée);
- le temps de réponse de la communication de sécurité;
- le temps de traitement du poste de commande de sécurité;
- le temps de réponse du dispositif de sortie de sécurité;
- le comportement du système de communication en cas de défaillance.

En outre, il convient de prendre en compte les éléments suivants:

- le nombre de nœuds reliés au réseau;
- le temps de traitement de l'unité logique dans le poste de commande hôte;
- le temps de traitement dans le poste de commande esclave (temps d'établissement/temps de coupure, etc.);
- les réglages du réseau, comme par exemple le nombre d'essais;
- le temps de réponse du répétiteur, si applicable;
- la communication asynchrone/synchrone;
- le temps de réponse des dispositifs.

Afin de choisir un système de communication relatif à la sécurité qui satisfait au temps de réponse maximal exigé par la SRS, il convient de calculer le temps de réponse maximal avant l'installation, conformément au manuel d'instruction du système de communication relatif à la sécurité.

Il convient d'évaluer toute modification du système (y compris le réseau ou les nœuds) concernant tout impact sur le temps de réponse du système.

### 6.2.3 Distance de transmission, vitesse de transmission et nombre de nœuds

Il convient que les réglages de la distance de transmission et de la vitesse de transmission soient conformes à la spécification du fournisseur pour le type et la longueur du câble à utiliser. Vérifier le système de communication relatif à la sécurité particulier concernant la variabilité du temps de réponse maximal, en fonction du nombre de nœuds à intégrer. Si celui-ci varie, il est nécessaire d'élaborer le réseau avec le nombre de nœuds exigé pour remplir la fonction de commande relative à la sécurité, tout en fournissant un temps de réponse adéquat.

Pour les systèmes de communication relatifs à la sécurité dans lesquels des vitesses de transmission multiples sont fournies, la distance de transmission maximale dépend de la vitesse de transmission choisie. Il convient de noter qu'une vitesse plus élevée correspond à une distance de transmission maximale plus courte.

### 6.2.4 Conditions environnementales

Il convient que le système de communication relatif à la sécurité soit choisi en tenant compte des conditions environnementales telles que la température ambiante, les vibrations, les chocs et les perturbations électromagnétiques. Afin d'éviter des dysfonctionnements, tels que l'affaiblissement des signaux de sortie, il convient d'observer les règles générales sur le câblage pour l'immunité aux perturbations externes, par exemple la séparation des câbles de communication et des câbles de puissance (voir CEI 60204-1).

Pour les exigences environnementales, les spécifications fournies par le fabricant doivent être prises en compte.

NOTE 1 Voir également la CEI 60204-1, la CEI 62061, et la CEI 61131-2.

NOTE 2 La prise en compte des spécifications du fabricant et des conditions environnementales par le concepteur du système est très importante pour garantir un niveau de performance de sécurité adéquat, en raison de la diversité des bus de sécurité et de leur performance associée.

### 6.2.5 Outils de réglage et de configuration

Il convient de vérifier que les outils utilisés pour les réglages du système de communication relatif à la sécurité sont équipés de moyens de sécurité tels que des mots de passe pour des niveaux de contrôle multiples. Il est recommandé que la méthode de gestion de ces dispositifs de sécurité soit également définie clairement.

Il convient que les outils de réglage utilisés soient conformes aux recommandations du fabricant relatives à l'utilisation avec le système de communication relatif à la sécurité.

# 7 Installation et montage du système (configuration)

## 7.1 Installation du système

### 7.1.1 Confirmation du système

Avant l'installation du système, il convient de confirmer que les sous-systèmes et les éléments de sous-systèmes sont adaptés à une utilisation avec le système de communication relatif à la sécurité.

NOTE Voir la CEI 62061, 6.12.

### 7.1.2 Câblage du système de communication relatif à la sécurité

#### 7.1.2.1 Spécification des câbles de communication

Il convient de suivre les points suivants lors du choix des câbles:

- il convient d'utiliser uniquement les câbles désignés ou recommandés par le fabricant ;
- si le système de communication comprend à la fois des dispositifs relatifs à la sécurité et non relatifs à la sécurité, utiliser le câble requis par les dispositifs relatifs à la sécurité ;
- le type de câble est compatible avec la vitesse de transmission. Le système de communication relatif à la sécurité peut exiger différents types de câbles en fonction de la vitesse de transmission,
- le type de câble est compatible avec la distance de transmission. Le système de communication relatif à la sécurité peut exiger différents types de câbles en fonction de la distance de transmission maximale et/ou des distances entre les nœuds ;
- il convient de vérifier les différences possibles dans les taux d'erreurs de transmission pour différents types de câbles.

#### 7.1.2.2 Câblage

Il convient de suivre les points suivants pour le câblage:

- il convient qu'il y ait une marge suffisante dans la longueur du câble, afin d'éviter les contraintes intolérables au niveau des bornes de connexion et/ou des connecteurs ;
- il convient de vérifier si le blindage du câble doit être raccordé ou non. Dans de nombreux cas, la terminaison du blindage est essentielle pour réduire les effets provenant des perturbations externes. S'assurer de bien suivre le manuel d'instruction ;
- il convient de ne pas plier le câblage au-delà de la plage autorisée spécifiée par le fabricant du câble. En particulier pour les fibres optiques, il convient de prendre les précautions nécessaires, étant donné que la communication peut être totalement interrompue si un câble est plié au-delà de la plage autorisée ;
- il convient que le raccord des fibres optiques soit effectué conformément aux instructions données par le fabricant du câble et à l'aide de l'outil désigné ;
- il convient que les câbles de communication et les câbles de puissance, ainsi que les câbles pour l'entrée/la sortie en courant alternatif si applicable, soient disposés dans des conduits distincts. Il est recommandé que la distance de séparation soit conforme à la recommandation du fournisseur du système de communication relatif à la sécurité. Ceci est essentiel pour réduire l'effet du bruit extérieur ;
- il convient de vérifier la compatibilité de chaque appareil avec les deux types de câblages, le branchement et la connexion multipoints ;

- si le système de communication relatif à la sécurité nécessite un raccord, il est recommandé que ce dernier soit conforme à la spécification du fournisseur.

#### 7.1.2.3 Distance de câblage

Il convient de vérifier les points suivants:

- la longueur de câble entre les nœuds et/ou la longueur totale du câble, conformément à la spécification du fournisseur du système de communication relatif à la sécurité ;
- le fait que la distance entre chaque paire de nœuds se situe dans la plage autorisée ne garantit pas que la longueur totale du câble se situe dans la plage autorisée. Il convient de vérifier la longueur de câble réelle après le câblage ;
- il convient de vérifier la longueur de câble en faisant référence à la spécification appropriée qui correspond au type de câble utilisé.

### 7.1.3 Choix de l'alimentation

Il est recommandé que les alimentations soient telles que spécifiées par le fournisseur du système de communication relatif à la sécurité. Il convient de tenir compte de l'effet de la fluctuation de tension lors du choix d'une alimentation pour le système de communication relatif à la sécurité :

- il convient de vérifier au cours de l'élaboration de la spécification s'il est nécessaire ou non que l'alimentation pour l'entrée/sortie soit séparée de celle pour le système de communication relatif à la sécurité ;
- il est recommandé que les alimentations conformes à la TBTS ou à la TBTP soient choisies si applicable, y compris les alimentations utilisées pour les appareils de diagnostic et de surveillance qui sont reliés de façon permanente ou temporairement.

### 7.1.4 Conditions environnementales

Vérifier que les conditions environnementales de l'installation se situent dans les valeurs spécifiées. Si l'une d'elles se situe en dehors de la spécification, il convient de prendre une contre-mesure appropriée avant de faire fonctionner le système.

Il convient de vérifier les éléments suivants:

- si la température de fonctionnement/l'humidité dépassent la valeur limite spécifiée, ajouter des dispositifs de chauffage ou des ventilateurs, etc., pour les réguler et pour qu'elles se situent dans les valeurs spécifiées ;
- si les vibrations et les impacts dépassent la valeur spécifiée pour les composants du réseau, utiliser des amortisseurs de vibrations ou de chocs pour les réguler et pour qu'ils se situent autour de la valeur spécifiée ;
- si l'appareil est installé dans une zone poussiéreuse, il convient de prendre une mesure de protection, comme par exemple envelopper le poste de commande ;

NOTE Si les dispositifs de chauffage, les ventilateurs, les amortisseurs de chocs, les enveloppes étanches aux poussières, etc., sont nécessaires pour obtenir le SIL cible, ils font alors partie de la SRCF et exigent une intégrité adaptée.

- si cela est approprié, réaliser une mesure des perturbations électromagnétiques et vérifier que l'environnement électromagnétique se situe dans les limites spécifiées par le fournisseur du système de communication relatif à la sécurité.

## 7.2 Réglage

### 7.2.1 Configuration du système

Il convient que le réglage et la modification des données de configuration du système soient effectués par des personnes compétentes suffisamment qualifiées et expérimentées et ayant la responsabilité de ce système de sécurité.

La configuration du système peut être effectuée à l'aide d'un matériel et/ou d'un logiciel. Il est essentiel de suivre les instructions du fabricant du système de communication relatif à la sécurité. Dans les systèmes de communication relatifs à la sécurité, la plupart des réglages sont réalisés à l'aide d'outils dédiés. Il convient de porter une attention particulière à la gestion des données de configuration. Afin d'empêcher la modification des réglages du système par des personnes non autorisées, il convient de protéger la modification de la configuration du système par un mot de passe.

Il est recommandé que la personne responsable contrôle au moins les informations suivantes:

- les mots de passe;
- les dernières données de configuration.

Dans l'outil dédié, les données utilisées (par exemple un ensemble de paramètres qui ont été fixés préalablement) et les informations associées aux paramètres relatifs à la sécurité, comme par exemple l'identité de l'opérateur qui a effectué les réglages des paramètres, la date du réglage et d'autres informations appropriées, sont enregistrées. Il est recommandé que la personne responsable contrôle ces données comme les données d'origine.

### 7.2.2 Réglage pour le fonctionnement

Avant d'appliquer la puissance à la machine, il convient d'établir les éléments suivants pour le système de communication relatif à la sécurité.

- Mode de fonctionnement
  - vérifier la spécification des modes et la méthode de modification des modes en se référant aux instructions du fabricant.
- Vitesse de transmission
- Nombre de nœuds

Il existe deux méthodes de réglage: l'utilisation des interrupteurs intégrés à l'appareil, soutenant le système de communication relatif à la sécurité, et l'utilisation de l'outil de réglage dédié. Suivre les instructions du fabricant pour chaque méthode.

### 7.2.3 Réglage et modification des données de configuration

Il convient de porter une attention particulière aux sujets suivants lorsque les données de configuration sont modifiées.

- Il existe deux méthodes de réglage de la configuration du système: le réglage matériel et le réglage logiciel. Il est important de vérifier les instructions du fabricant à l'avance, pour comprendre la fonction soumise à la configuration.
- Il est nécessaire de vérifier les données de réglage stockées dans l'appareil en les comparant aux données de réglage en suivant la procédure de vérification fournie dans les instructions du fabricant.
- Après la modification de la configuration, il convient de réaliser un essai fonctionnel.

Ceci incombe à l'administrateur du système de sécurité.

Le changement des réglages au cours d'une modification, par exemple, ne doit pas entraîner de situation dangereuse.

## 8 Validation

### 8.1 Vérifications avant l'application de la puissance

Avant d'appliquer la puissance à la machine, il convient de vérifier les points suivants :

- il convient de vérifier les erreurs de câblage du système de communication relatif à la sécurité, comme par exemple une polarité incorrecte, des courts-circuits ou des défauts à la terre, en utilisant l'équipement d'essai approprié ;
- vérifier que la mise à la terre est sûre, y compris celle des autres appareils ;
- vérifier que la charge (par exemple les organes de commande de la machine) est isolée de la source d'alimentation avant d'appliquer la puissance au système de communication relatif à la sécurité.

NOTE Voir CEI 62061, Article 9.

### 8.2 Validation après l'application de la puissance

Les éléments suivants sont les points initiaux à vérifier après l'application de la puissance :

- si possible, il convient de surveiller les formes d'ondes des signaux dans le système de communication relatif à la sécurité, afin de vérifier que le niveau de bruit est suffisamment bas ;
- il convient de mesurer toutes les tensions d'alimentation pour vérifier si elles se situent ou non dans la plage autorisée ;
- lorsqu'il y a une alimentation pour la communication distincte de l'alimentation pour le contrôle, il convient que la vérification mentionnée ci-dessus soit effectuée sur les deux alimentations ;
- vérifier que chaque appareil démarre correctement en vérifiant les indicateurs conformément au manuel d'instruction. A ce stade, étant donné que les paramètres n'ont pas été fixés complètement, aucune autre vérification n'est effectuée.

NOTE Voir CEI 62061, Article 9.

### 8.3 Essais fonctionnels

Au cours de la phase de mise en service du système, et à chaque fois qu'une modification est appliquée, il convient de réaliser des essais fonctionnels sur chaque fonction de sécurité, pour valider sa conformité à la spécification des exigences de sécurité.

Il convient de vérifier le comportement du système de communication, conformément à la spécification des exigences de sécurité, dans les circonstances suivantes:

- coupure et rétablissement de l'alimentation ;
- rupture du câblage ;
- défaillance en entrée/sortie ;
- remplacement d'un esclave ;
- temps de réponse.

NOTE Voir CEI 62061, Article 9.

### 8.4 Référentiel

Après la validation, il convient d'enregistrer comme référentiel les données de configuration, comprenant au moins les réglages des paramètres, l'identité de la personne ayant effectué les réglages des paramètres, la date du réglage, les résultats des essais, les informations sur la version, et d'autres données correspondantes. Il convient de mettre à jour ce référentiel à chaque fois que le système de communication relatif à la sécurité est modifié. Il peut être utile d'archiver une copie de la (des) configuration(s) précédente(s).

NOTE Voir CEI 62061, Article 9.

## 9 Documentation

Il convient que la documentation:

- soit précise et concise;
- soit facile à comprendre pour les personnes devant l'utiliser;
- corresponde à son objectif;
- soit accessible et qu'elle puisse être actualisée.

Les documents nécessaires pour la validation d'un système de communication relatif à la sécurité utilisé comme sous-système d'un SRECS peuvent inclure:

a) une spécification des exigences de sécurité ;

b) une spécification du système (y compris la configuration du système, les normes applicables, etc.) ;

c) un plan de gestion du système ;

d) une spécification matérielle ;

e) une spécification logicielle ;

f) des schémas de câblage ;

g) la probabilité d'estimation d'une défaillance matérielle (PFH, *probability of hardware failure*), et la probabilité d'estimation d'une défaillance matérielle dangereuse ($PFH_D$) ;

h) un plan d'essai et un rapport d'essai ;

i) un manuel d'installation et de fonctionnement ;

j) un référentiel.

Si un dispositif relatif à la sécurité, un bloc fonctionnel, ou un outil logiciel à utiliser dans un système de communication relatif à la sécurité a une certification pour sa conformité à la CEI 61508, il convient d'inclure le certificat dans la documentation. Ceci s'applique également au logiciel d'application. Il convient également d'inclure dans la documentation les informations relatives à l'outil de configuration.

## 10 Fonctionnement, maintenance et réparation

### 10.1 Désignation d'une personne responsable

Il convient de désigner une personne responsable pour prendre la responsabilité de toutes les activités de maintenance, impliquant le système de communication relatif à la sécurité. Il convient que la personne responsable contrôle le fonctionnement, la maintenance et la réparation du système de communication relatif à la sécurité.

### 10.2 Elaboration d'un plan de maintenance

Il convient que la maintenance du système de communication relatif à la sécurité soit effectuée conformément au plan de maintenance. Il est recommandé que le plan de maintenance comprenne les activités courantes (telles que l'examen périodique et l'essai de démarrage) qui sont exigées pour maintenir la sécurité fonctionnelle des systèmes de communication relatifs à la sécurité. Il convient que les procédures pour les travaux de maintenance soient documentées.

Il convient de vérifier la sécurité du programme d'essai qui est utilisé pour les travaux de maintenance et/ou l'analyse des défaillances.

Il convient de noter que le plan de modification du système doit être indépendant du plan de maintenance, étant donné que l'objectif de ces plans est clairement différent.

### 10.3 Mise en œuvre d'une maintenance périodique

Il est recommandé que les activités de maintenance périodique soient effectuées tant que le système de communication relatif à la sécurité fonctionne. Il convient de maintenir le système afin de conserver le niveau d'intégrité de sécurité spécifié dans la spécification des exigences de sécurité, jusqu'à la mise au rebut du système. Cet article spécifie les éléments nécessaires pour une maintenance correcte.

Il convient que la maintenance périodique soit effectuée à des intervalles ne dépassant pas celui de l'essai de validité spécifié dans la spécification des exigences de sécurité et décrit dans le plan de maintenance ou dans le manuel du fabricant.

### 10.4 Eléments des travaux de maintenance

Il est recommandé d'effectuer tous les essais de validité décrits dans la spécification des exigences de sécurité ou dans les spécifications du fabricant. Etant donné qu'il n'est généralement pas possible de rétablir le système de communication relatif à la sécurité dans une condition "comme neuf" sans remplacer les dispositifs, il est recommandé d'utiliser si possible, dans le système de communication, des dispositifs ayant une durée de vie ou un intervalle d'essai de validité supérieur(e) à vingt ans.

Lorsque la $PFH_D$ dépend fortement des essais de validité (c'est-à-dire des essais destinés à révéler des défauts non détectés par des fonctions de diagnostic), il est alors nécessaire de présenter l'intervalle d'essai de validité comme réaliste et réalisable dans le contexte de l'utilisation prévue du système de communication relatif à la sécurité. Par exemple, des intervalles d'essais de validité inférieurs à 10 ans peuvent être exagérément courts pour de nombreuses applications de machines, et un intervalle d'essai de validité de 20 ans est souvent recommandé. Il est reconnu que certains sous-systèmes et/ou éléments de sous-systèmes (par exemple composants électromécaniques avec des cycles d'utilisation élevés) exigeront un remplacement dans l'intervalle d'essai de validité.

### 10.5 Enregistrement des résultats de maintenance

Il convient d'enregistrer et de conserver les résultats des procédures de maintenance. Il convient de définir la période de conservation dans le plan de maintenance. Il convient d'enregistrer toutes les modifications apportées au référentiel.

## 11 Enseignement et formation

### 11.1 Généralités

Il convient que la personne responsable mette en œuvre et en application des programmes d'enseignement et de formation sur la sécurité, afin de maintenir la sécurité de fonctionnement des systèmes de communication relatifs à la sécurité. Les éléments exigés pour une telle formation sont présentés dans les paragraphes suivants.

### 11.2 Domaine d'application

Il convient de mettre en application des programmes d'enseignement et de formation sur la sécurité pour toutes les personnes qui sont impliquées dans le fonctionnement des systèmes de communication relatifs à la sécurité, par exemple les opérateurs, le personnel de maintenance, les installateurs de programmes, leurs responsables et leurs administrateurs.

### 11.3 Mise en œuvre d'un enseignement et d'une formation continus

Il convient qu'un enseignement et une formation périodiques soient réalisés pour toutes les personnes impliquées dans le fonctionnement des systèmes de communication relatifs à la sécurité.

Il convient également de fournir un enseignement et une formation appropriés:

- lorsqu'une personne est désignée ;
- lorsqu'un système de communication relatif à la sécurité est modifié, et
- avant que le système ne soit remis en marche après un accident ou un quasi-accident.

### 11.4 Contenu de l'enseignement et de la formation

Il convient d'inclure les éléments suivants dans le programme d'enseignement:

- réglementations et normes relatives à la sécurité des travailleurs;
- principes des mesures de protection;
- dispositifs relatifs à la sécurité et leurs fonctions;
- procédures de fonctionnement de chaque dispositif;
- procédures de travail sûres (pour un fonctionnement normal);
- procédures de fonctionnement en cas d'urgence.

### 11.5 Planification des activités de formation et conservation des données de formation

Il convient de réaliser les activités de formation conformément au programme de formation, et il est recommandé de conserver les données pendant une période définie.

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

## A.1 Généralités

Comme mentionné ci-dessus, un système de communication relatif à la sécurité est uniquement un sous-système dans un SRECS. Conformément à la CEI 61508 et à la CEI 62061, le SRECS se compose généralement des composants présentés sur la Figure A.1. Au lieu d'utiliser un câblage conventionnel, un système de communication relatif à la sécurité est utilisé. La SILCL est généralement documentée dans le document sur les instructions d'utilisation du fournisseur du système de communication relatif à la sécurité.

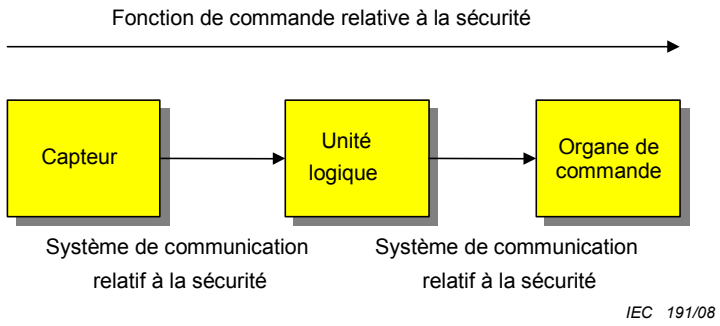



**Figure A.1 – Composants d'un SRECS**

Un système de communication relatif à la sécurité ne réalise qu'une partie d'une fonction de sécurité spécifiée pour un système de commande électrique relatif à la sécurité. Pour cela, les capteurs (par exemple interrupteur protecteur de porte), les organes de commande (par exemple contacteur), et généralement le logiciel d'application, sont également exigés.

La fonction de sécurité d'un système de communication relatif à la sécurité consiste à transmettre des données relatives à la sécurité d'une entrée à une sortie et/ou vice versa, dans une durée spécifiée et à une intégrité spécifiée. Dans cet exemple, dans un souci de simplicité, l'unité logique est considérée comme intégrée au système de communication relatif à la sécurité. Ce dispositif peut être une unité séparée dans un SRECS ou une partie du dispositif d'entrée de sécurité ou du dispositif de sortie de sécurité. Ceci dépend de l'architecture du système de communication relatif à la sécurité.

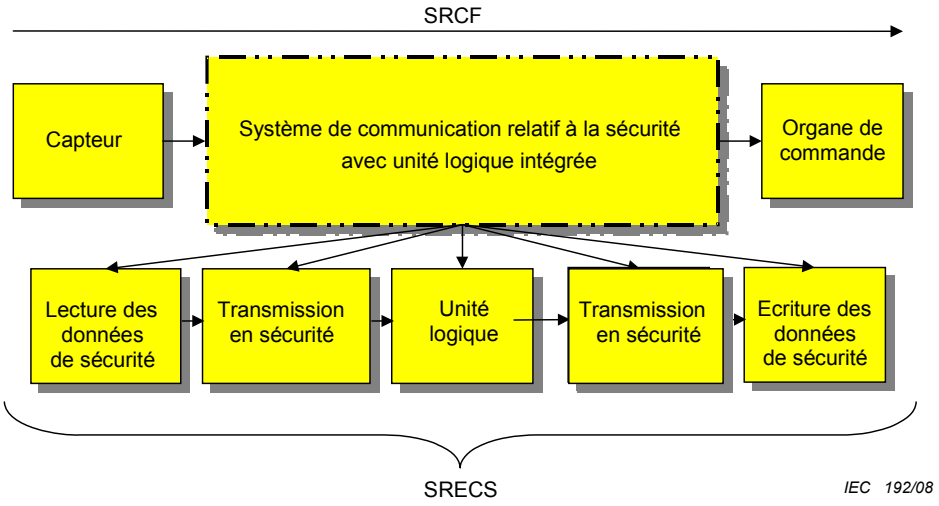



**Figure A.2 – SRECS utilisant un système de communication relatif à la sécurité**

NOTE La mise en œuvre d'un bloc fonctionnel exige généralement une spécification détaillée des exigences de sécurité. Une spécification des exigences de sécurité pour les sous-systèmes réalisant les blocs fonctionnels est également nécessaire. Ces spécifications sont réalisées par le fournisseur du système de communication relatif à la sécurité et n'entrent pas dans le domaine d'application de ces lignes directrices. Le fournisseur d'un système de communication relatif à la sécurité définit généralement la SILCL maximale pouvant être atteinte par un paramétrage correct du système de communication relatif à la sécurité et des dispositifs utilisés.

Le bloc fonctionnel de transmission en sécurité garantit la transmission en sécurité des données relatives à la sécurité d'une source à un bloc récepteur (par exemple, émetteur à récepteur): il peut être divisé en deux blocs fonctionnels supplémentaires :

- bloc fonctionnel maître de transmission en sécurité ;
- bloc fonctionnel esclave de transmission en sécurité.

NOTE Conformément à la CEI 62061, un bloc fonctionnel est réalisé par un seul sous-système uniquement (par exemple, dispositif). Chaque bloc fonctionnel est attribué à un sous-système dans l'architecture de la fonction de sécurité. Plusieurs blocs fonctionnels peuvent être attribués à un seul sous-système. Un bloc fonctionnel est uniquement réalisé par un seul sous-système.

Les systèmes de communication utilisent généralement des dispositifs maîtres et esclaves. Dans certains systèmes, ces dispositifs sont appelés producteur et consommateur. Les systèmes de communication à plusieurs maîtres ont aussi généralement une unité envoyant un message relatif à la sécurité et une ou plusieurs unités recevant ce message. Dans ces lignes directrices, on considère qu'un dispositif maître (producteur) et des dispositifs esclaves (consommateurs) sont utilisés.

Dans cette condition préalable, un système de communication relatif à la sécurité est fondé sur les deux sous-systèmes (dispositifs) principaux suivants:

- esclave relatif à la sécurité (entrée, sortie, entrée et sortie) ;
- maître relatif à la sécurité (par exemple avec un poste de commande relatif à la sécurité).

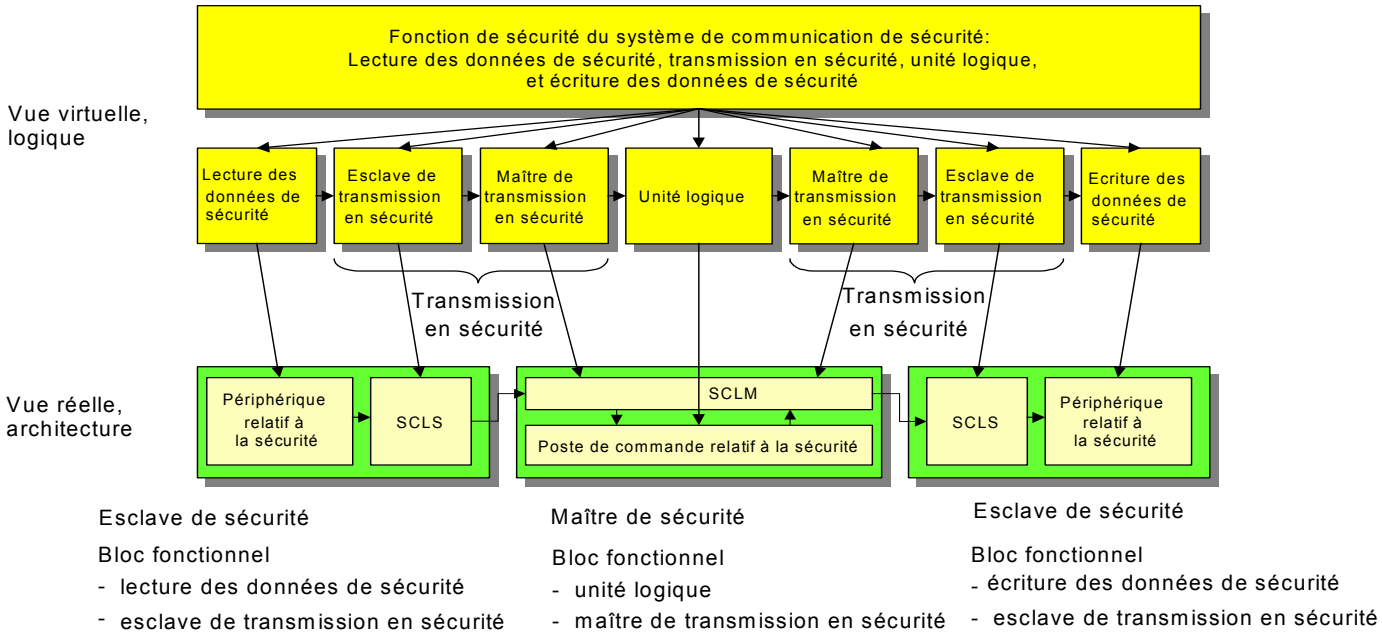



**Figure A.3 – Vues différentes du système de communication relatif à la sécurité**

Chacun des sous-systèmes (dispositifs) réalise un ou plusieurs blocs fonctionnels. Comme représenté sur la Figure A.3, le périphérique relatif à la sécurité et le SCLS des sous-systèmes sont réalisés sur un esclave relatif à la sécurité. Les deux sous-systèmes peuvent aussi être des dispositifs distincts (par exemple, un jeu de puces réalisant les services du SCLS et un dispositif d'entrée de sécurité).

## A.2 Architecture du système de communication relatif à la sécurité

Dans les systèmes de communication relatifs à la sécurité, les capteurs et les organes de commande sont raccordés aux dispositifs d'entrée et de sortie correspondants. Ces dispositifs peuvent être reliés localement ou à distance à l'unité logique. Les architectures types des systèmes de communication relatifs à la sécurité comprennent les exemples suivants.

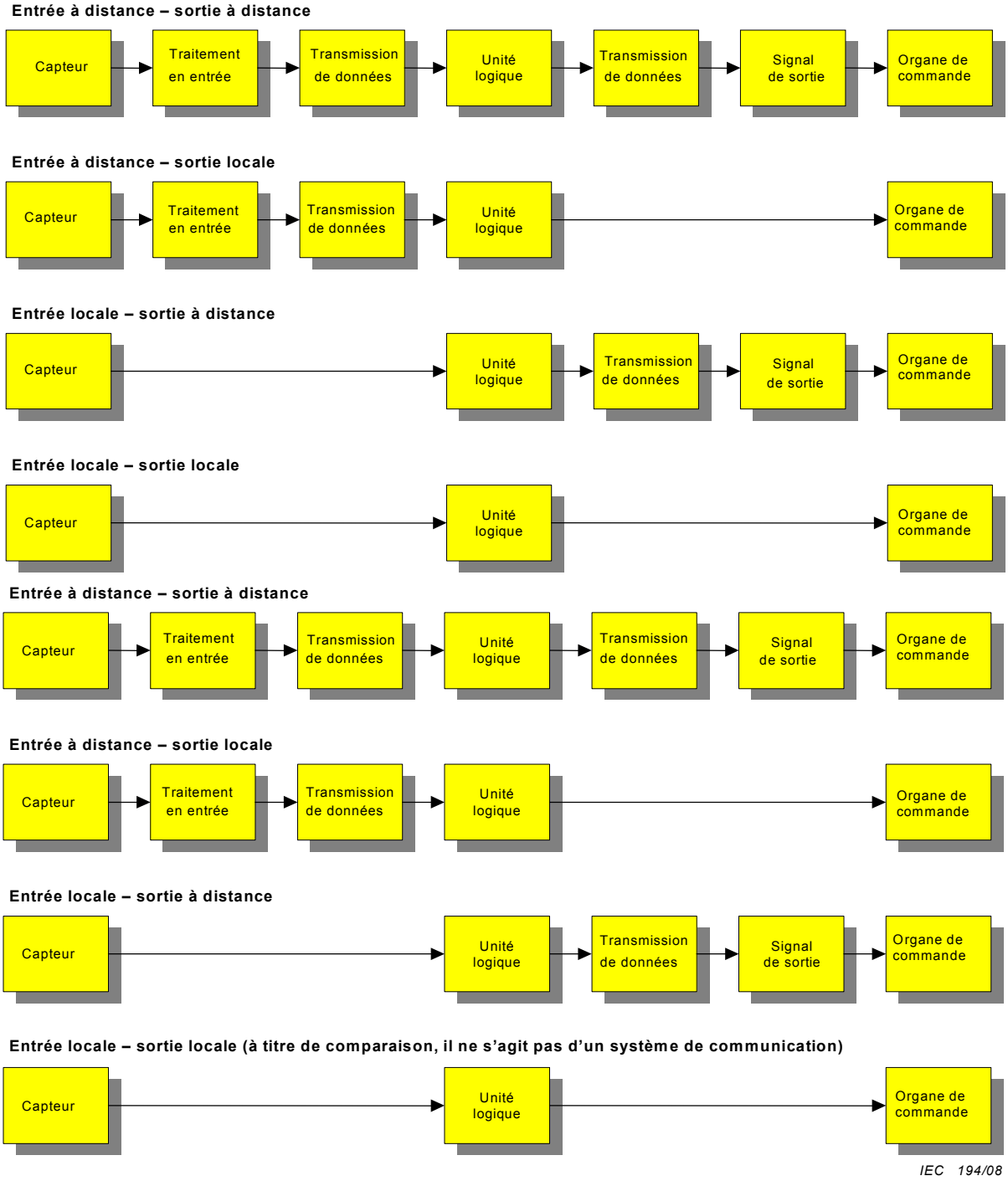



**Figure A.4 – Exemples d'architectures types des systèmes de communication relatifs à la sécurité**

## A.3 Calcul de la $PFH_D$ du SRECS

Pour le calcul de la $PFH_D$ du SRECS, des informations sont nécessaires sur les valeurs qui doivent être prises en compte. Le fournisseur du système de communication relatif à la sécurité fournit généralement ces valeurs pour chaque dispositif relatif à la sécurité. Dans la plupart des cas, la $PFH_D$ du SRECS est la somme de la $PFH_D$ de chaque dispositif utilisé dans une boucle de sécurité (capteur – système de communication relatif à la sécurité – unité logique – organe de commande).

La $PFH_D$ de la partie capteur dépend du paramétrage du dispositif et de l'architecture (un ou plusieurs capteurs, avec ou sans impulsions d'essai, ...). Il convient que ceci soit expliqué dans le document sur les instructions d'utilisation du fournisseur des dispositifs ou des systèmes de communication relatifs à la sécurité.

La connexion des capteurs et des organes de commande à un dispositif relatif à la sécurité d'un système de communication relatif à la sécurité est un aspect important dans l'obtention du SIL requis de la SRCF. Il est fortement recommandé de prendre en compte le document sur les instructions d'utilisation du fournisseur.

## Bibliographie

CEI 61131-2 : 2007, *Programmable controllers – Part 2: Equipment requirements and tests* (anglais seulement)

CEI 61784-3: *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile* (anglais seulement)

CEI 61918, *Industrial communication networks – Installation of communication networks in industrial premises* (anglais seulement)

CEI 62280-1: 2002, *Applications ferroviaires – Systèmes de signalisation, de télécommunication et de traitement – Partie 1: Communication de sécurité sur des systèmes de transmission fermés*

ISO 12100-1:2003, *Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 1: Terminologie de base, méthodologie*

ISO 12100-2:2003, *Sécurité des machines – Notions fondamentales, principes généraux de conception – Partie 2: Principes techniques*

ISO 13849-1 :2006, *Sécurité des machines – Parties des systèmes de commande relatives à la sécurité – Partie 1: Principes généraux de conception*

ISO 14121-1 : 2007, *Sécurité des machines – Appréciation du risque – Principes*

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
P.O. Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch