IEC 62745

Edition 1.0 2017-03

INTERNATIONAL STANDARD

colour inside

Safety of machinery – Requirements for cableless control systems of machinery

IEC 62745:2017-03(en)

International Electrotechnical Commission

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

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

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC 62745

Edition 1.0 2017-03

INTERNATIONAL STANDARD

colour inside

Safety of machinery – Requirements for cableless control systems of machinery

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 29.020; 35.100.01

ISBN 978-2-8322-4013-7

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SAFETY OF MACHINERY – REQUIREMENTS FOR CABLELESS CONTROL SYSTEMS OF MACHINERY

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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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.

International Standard IEC 62745 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects.

The text of this standard is based on the following documents:

FDIS	Report on voting
44/783/FDIS	44/785/RVD

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

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

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

Cableless control systems (CCS) are increasingly being used to provide an operator interface on a wide range of machinery. The functionality of a CCS and the way in which it interfaces with the overall machine control system can therefore affect the safety of the machinery.

IEC 62745 specifies requirements for the functionality of a CCS that is interfaced with or is part of a machine control system for use as an operator control station on a machine.

The extent to which the functionality of a CCS is relied upon to minimise risk on a machine is a key selection criterion. It is therefore important to select a CCS that provides suitable control functions with an appropriate safety integrity in accordance with the risk assessment at the machine.

In some particular applications, the requirements for a CCS can exceed those specified in this document.

SAFETY OF MACHINERY – REQUIREMENTS FOR CABLELESS CONTROL SYSTEMS OF MACHINERY

1 Scope

This standard specifies requirements for the functionality and interfacing of cableless (for example, radio, infra-red) control systems that provide communication between operator control station(s) and the control system of a machine. Specific requirements are included for such operator control stations that are portable by the operator.

NOTE The part of the cableless control system that is used as an operator control station is sometimes referred to as the 'transmitter' and the part that interfaces with the machine control system is sometimes referred to as the 'receiver'. However, to take account of the possibility of bi-directional communication, this standard refers to these individual parts as the 'remote station' and the 'base station' respectively.

This document does not deal with cableless communication between parts of a machine(s) that are not operator control stations.

This document is not intended to specify all of the requirements that are necessary for the design and construction of a cableless control system. For example, it does not specify communication protocols, frequency or bandwidth aspects, nor the full range of constructional requirements such as impact resistance, ingress protection, electromagnetic compatibility, etc.

The provisions of this document are intended to be applied in addition to the requirements for electrical equipment in the IEC 60204-1.

This document is a type-B2 standard as stated in ISO 12100.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 60068-2-31:2008, *Environmental testing – Part 2-31: Tests – Test Ec – Rough handling shocks, primarily for equipment-type specimens*

IEC 60204-1:2005, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 60947-5-1:2016, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

IEC 60947-5-5, *Low-voltage switchgear and controlgear – Part 5-5: Control circuit devices and switching elements – Electrical emergency stop device with mechanical latching function*

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

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

ISO 13849-2, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

ISO 13850, *Safety of machinery – Emergency stop function– Principles for design*

3 Terms, definitions and abbreviations

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

For an alphabetical list of definitions, see Table 1.

For list of abbreviations see Table 2.

Table 1 – Alphabetical list of definitions

Term	Definition number
active stop	3.17
address code	3.7
automatic stop (ATS)	3.19
base station	3.13
cableless control	3.1
cableless control system (CCS)	3.2
disabling of a remote station	3.22
error detection code	3.9
frame	3.6
Hamming distance	3.11
manual stop	3.20
neutral frame	3.10
OFF-state	3.15
operating command signal	3.8
operator control station	3.5
passive stop	3.18
receiver	3.3
remote station	3.12
safety-related stop function	3.16
stop output	3.14
transmitter	3.4
valid signal	3.21

Table 2 – Abbreviations

Term	Abbreviation
automatic stop (4.7.3.5)	ATS
cableless control system (3.2)	CCS
emergency stop (4.7.3.4)	EMS
general safe stop (4.7.3.3)	GSS

3.1
cableless control
transmission of the machine operator's commands without any wired connection

3.2
cableless control system
CCS
system consisting of at least one remote station and one base station, which uses cableless control to transmit commands between them

3.3
receiver
part of a cableless control system which receives frames from a transmitter

3.4
transmitter
part of a cableless control system which sends frames to a receiver

3.5
operator control station
assembly of one or more control actuators (part of a device to which an external manual action is to be applied) fixed on the same panel or located in the same enclosure

Note 1 to entry: An operator control station can also contain related equipment, for example, potentiometers, signal lamps, instruments, display devices, etc.

3.6
frame
“package” of information exchanged between a remote station and a base station, and consisting of, for example:

a) address code;

b) operating commands;

c) error detection code;

d) other commands, signals or information

Note 1 to entry: A “frame” is sometimes referred to as a “telegram” or “message”.

3.7
address code
part of a frame that enables a base station or a remote station to recognise frames that are intended to convey commands to it

Note 1 to entry: The base station or remote station respond to commands that are recognised as having the relevant address code.

3.8
operating command signal
control signal that is intended to initiate, modify or maintain a machine function

3.9
error detection code
additional information added to each frame to enable the detection of transmission errors

3.10
neutral frame
frame in which all operating command signals are in a state such that when it is received at the base station it does not activate any outputs intended for control of hazardous operations of the machine

Note 1 to entry: Neutral frames can be used to maintain communication (i.e. a valid signal) between a transmitter and receiver, for example to preclude automatic initiation of the stop function at a machine.

Note 2 to entry: Neutral frame transmission is intended to prevent hazardous operations of the machine resulting from establishment or re-establishment of communication.

Note 3 to entry: Neutral frames can contain data, for example parameterisation data, and commands that are not intended to cause hazardous operations of the machine.

3.11
Hamming distance
number of bit positions in which two frames of the same length differ from each other

3.12
remote station
part of a cableless control system via which an operator interfaces with the cableless control system

Note 1 to entry: The remote station of a cableless control system is sometimes referred to as a “transmitter”, but a remote station that is part of a bi-directional cableless control system will incorporate both a transmitter and a receiver.

Note 2 to entry: The remote station forms the operator control station of a cableless control system.

Note 3 to entry: The remote station can be portable (by the operator), mobile (e.g. installed separately from the machine on a vehicle or trolley) or fixed (e.g. installed on or near to the machine).

3.13
base station
part of the cableless control system that interfaces with the machine control system

Note 1 to entry: The base station of a cableless control system is sometimes referred to as a “receiver”, but a base station that is part of a bi-directional cableless control system will incorporate both a receiver and a transmitter.

Note 2 to entry: The base station may be installed on static or mobile machinery.

Note 3 to entry: The base station is not necessarily a discrete physical entity, but it includes all of the components that fulfill the requirements specified in this standard for the base station.

3.14
stop output
output circuit of the base station that interfaces with the control system of the machine to initiate a stop function

Note 1 to entry: Stop outputs can be safety-related or non-safety-related. See also Table 3.

Note 2 to entry: Interfaces to field bus part of a CCS base station can also be considered as an output circuit.

3.15
OFF-state
state of safety-related stop output(s) of the base station, which is intended to be used to initiate one or more stop functions of a machine

3.16
safety-related stop function
stop function provided by the CCS that results in an OFF-state and whose failure can result in an immediate increase of the risk(s)

3.17
active stop
stop resulting from transmission of a stop signal from the remote station to the base station

3.18
passive stop
safety-related stop resulting from absence of a valid signal at the base station

Note 1 to entry: A passive stop can be initiated by, for example, an out of range condition, battery failure, electromagnetic interference.

3.19
automatic stop
safety-related stop initiated without manual actuation of a device by an operator

3.20
manual stop
stop initiated by actuation of a device by an operator

3.21
valid signal
any received frame, including a neutral frame, that is accepted by the error checking routines of the receiver and contains the relevant address code for the receiver

3.22
disabling of a remote station
deliberate operation that renders a remote station incapable of sending signals to the base station

4 Functional requirements

4.1 General

Figure 1 illustrates an example of the main elements of a CCS and its interaction with the machine control system.

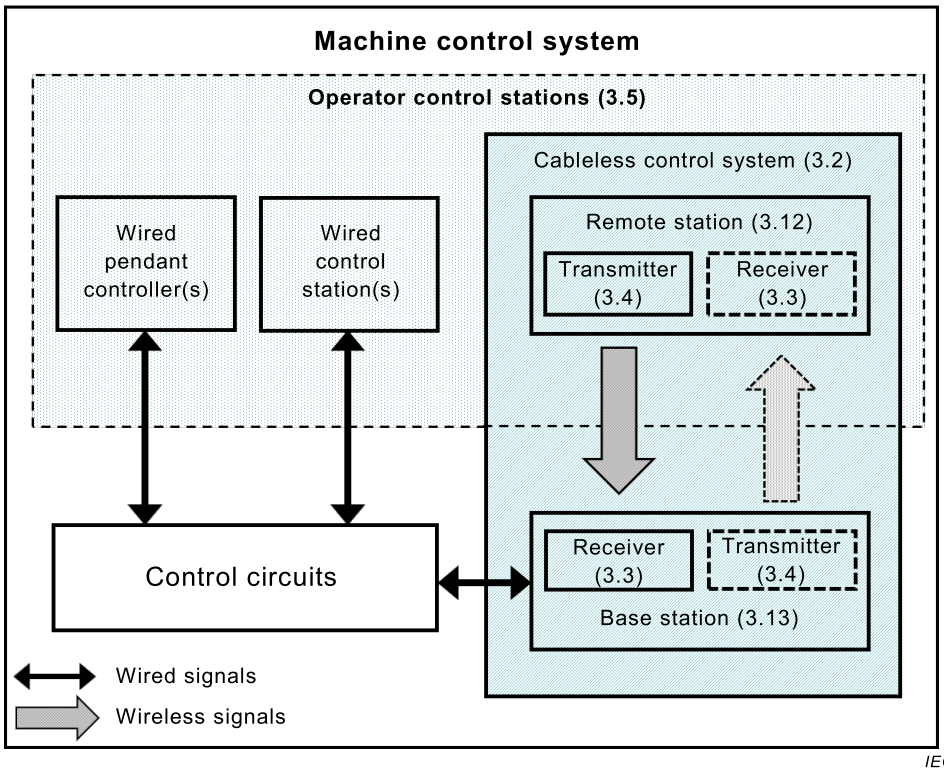

Figure 1 – Block diagram example of a cableless control system and its interaction with the machine control system

NOTE The references to IEC 60204-1 in this standard could have corresponding requirements in other relevant parts of IEC 60204 series.

4.2 Operational preventions

4.2.1 Prevention of inadvertent actuation

The remote station and its control actuators shall be designed and arranged so as to minimise the possibility of inadvertent actuation (for example, caused by dropping to the floor or striking an obstruction, failure of electronics) generating an unintended hazardous command.

4.2.2 Prevention of unauthorised operation

Where prevention of unauthorised operation of the CCS is required, remote stations shall be provided with means to prevent unauthorised use (for example, key-operated switch, access code).

4.2.3 Prevention of unintended commands

Measures shall be taken to ensure that operating command signals:

- affect only the intended base station or remote station (for example, using address code);
- initiate only the intended functions in that base station or remote station.

Such measures shall be resistant to accidental or unintentional change.

Upon detection of malfunction or faults, all relevant safety-related output shall be controlled to OFF-state with an appropriate safety integrity.

Where hardware switches (for example, DIP) are used for device addressing, additional measures such as parity checking may be necessary to fulfil the requirements in case of a fault.

NOTE Typical methods include factory-set coding, which are more robust than user-configurable methods because they cannot be defeated (either intentionally or inadvertently) by the user.

4.3 Serial data transfer

The serial data transfer shall satisfy one of the following requirements:

- means shall be provided that ensure the probability of an erroneous frame being received undetected, $R(P_e)$, is less than 1×10^{-8}, given an input bit error probability of $P_e = 10^{-3}$, if no better input bit error probability can be proven, or
- the Hamming distance shall be either 4 or the total number of bits in a frame divided by 20, whichever is greater.

NOTE 1 An input bit error probability of $P_e = 10^{-3}$ can be assumed as typical estimate for a wireless channel disturbed by Additive White Gaussian Noise (AWGN) and electromagnetic interference (EMI).

NOTE 2 IEC 60870-5-1 defines a set of possible transmission frame formats.

NOTE 3 Increasing the reliability of serial data transmission only reduces the possibility of errors than can be occurring in the transmission media.

In addition for safety-related functions of a CCS the residual error probability Λ of undetected error per hour shall be less than 1 % of the specified PFHD value for the respective function of the CCS. Residual probability of undetected error per hour Λ shall be calculated by:

$$\Lambda(P_e) = R(P_e) \times v \times b \ [1/h]$$

where:

$\Lambda(P_e)$: residual probability of undetected error per hour in relation to the input bit error probability

$R(P_e)$: residual probability of undetected error per frame in relation to the input bit error probability

P_e: input error probability. If no better input bit error probability can be proven, $P_e = 1 \times 10^{-3}$ applies

v: maximum number of safety-related messages per hour

b: maximum number of listening base stations

NOTE 4 For a definition of PFH_D see IEC 62061 or ISO 13849-1.

NOTE 5 $\Lambda(P_e)$ calculation is based on IEC 61784-3; this approach is valid for cyclic transmission of safety-related messages.

NOTE 6 When using CRC as hash-function, Equation (B.3) or (B.4) from IEC 61784-3:2016 can be applied in order to determine $R(P_e)$ with an input bit error probability of $P_e = 1 \times 10^{-3}$.

The CCS can be equipped with indicator of transmission reliability.

NOTE 7 It is not necessary to provide a separate warning indicator for each condition that can affect transmission reliability.

4.4 Removal of remote station transmission

Means shall be provided to readily stop transmission from the remote station. This shall be achieved by one or more of the following:

- a device that interrupts the power supply of transmission for the remote station, where such a device shall have direct opening action (see IEC 60947-5-1:2016, Annex K), or
- removal of the battery without the use of a tool, or

- a dedicated transmission removal function in accordance with IEC 61508, IEC 62061 or ISO 13849-1 and ISO 13849-2, with an integrity in accordance with 4.7.2.

NOTE A passive stop will result from the removal of transmission power.

4.5 Establishment and indication of transmission and communication

Power up of the remote station or re-establishment of communication (for example, after power supply interruption, remote station battery replacement, lost signal condition) shall not activate any output that is intended for control of hazardous operations of the machine. Initiation or re-initiation of such operations shall require a deliberate action (for example, releasing a control actuator from its energised position and then pressing it again).

The base station shall not respond to operating command signals that can activate outputs intended for control of hazardous operations of the machine until a neutral frame has been received (i.e. following re-establishment of communication).

When transmission from a remote station is taking place, this shall be indicated on the remote station (for example, by an indicating light, a visual display indication, etc.).

NOTE It can also be useful to provide a means of indicating when a base station is receiving transmissions from an associated remote station. For example, an output(s) on the base station can be designated for this purpose, and/or a confirmation signal can be transmitted to the remote station if bi-directional communication is available. Where the base station does not provide a designated means of indication, it is important that the information for use of the CCS includes instructions on how to implement this functionality (for example, using base station stop outputs).

4.6 Safety-related functions of the CCS

Functions of the CCS that are intended for safety-related applications shall have an appropriate safety integrity. The requirements of IEC 62061 and/or ISO 13849-1, ISO 13849-2 shall apply.

Upon detection of faults, all relevant safety-related output shall be controlled to OFF-state. In addition the detection of a fault in the remote station that can lead to the loss of a safety related function, shall cease the transmission.

NOTE Further information on the design of safety-related aspects of control functions is given in ISO 12100 and IEC 61508.

4.7 Stop functions of the CCS

4.7.1 General

The CCS shall provide an automatic stop (ATS) function and at least one safety related stop function that is initiated by a deliberate human action on a control device provided specifically for that purpose.

Information about logic of stop functions are given in Annex A.

NOTE In most applications this manually-initiated stop function is either a GSS or EMS (see 4.7.3).

4.7.2 Safety-related stop functions of a CCS

Each safety-related stop function of a CCS shall initiate an OFF-state of the relevant stop output(s) at the base station.

Each safety-related stop function of a CCS shall have a safety integrity of at least SIL1/PLc.

In addition, a single fault in any part of the CCS shall not lead to the loss of any safety-related stop function, and whenever reasonably practicable, the single fault shall be detected at or before the next demand on the safety-related stop function.

4.7.3 Classification of stop functions

4.7.3.1 General

Stop functions of a CCS are classified as:

- control stop;
- general safe stop (GSS);
- emergency stop (EMS);
- automatic stop (ATS).

Table 3 describes the characteristics of the different stop functions.

Table 3 – Overview of stop functions of the CCS

Function	Clause	Safety-related function	Type of stop (see Fig.2)	Effect on CCS	Availability & operability	Control actuator	
						Type	Colour
Control stop	4.7.3.2	Either	Active, passive, or active followed by passive	Defined state of (a) stop output(s), or of another output associated with release of a hold-to-run control actuator or, if safety-related: OFF-state of all safety-related stop output(s)	Operational when the CCS is in control of the machine	See IEC 60204-1	Black White Grey
General safe stop (GSS)	4.7.3.3	Yes	Active, passive, or active followed by passive	OFF-state of all safety-related stop output(s)	Operational when the CCS is in control of the machine	See 4.7.3.3	Black (preferred) or red. Red shall not have a yellow background
Emergency stop (EMS)	4.7.3.4				Operational at all times	Device that complies with IEC 60947-5-5	Red with a yellow background
Automatic stop (ATS)	4.7.3.5				Operational when the CCS is in control of the machine	Not applicable	Not applicable

4.7.3.2 Control stop function

A control stop function is always initiated manually by the operator and is available only when the CCS is in control of the machine.

A control stop function shall be designed in accordance with IEC 60204-1:2005, 9.2.5.3.

NOTE A control stop function can be initiated by releasing a hold-to-run control actuator or by an enabling device that is not in the run position.

4.7.3.3 General safe stop (GSS) function

The GSS function of a CCS is a safety-related control function.

Where the GSS function is provided on a CCS, the remote station shall include a separate and clearly identifiable means of manually initiating this function, which shall result in an OFF-state of all safety-related stop output(s) at the base station. See Table 3.

The device that initiates the GSS function shall have direct opening action (see IEC 60947-5-1:2003, Annex K).

When active operation of the actuator has ceased following initiation of the GSS function, the effect of the command shall be sustained by engagement of the device until it is disengaged by a manual action at the remote station. It shall not be possible to generate the stop command without latching the actuator, and latching of the actuator shall not occur without generation of the stop command. In case of failure of the latching mechanism, actuation of the device shall generate a stop command regardless of the latching of the actuator.

When active operation of the control actuator has ceased following initiation of the GSS function, the effect of the command shall be sustained by engagement of the device until it is disengaged by an intentional manual action at the remote station.

NOTE 1 The signal produced by the GSS function is intended to be used to initiate either a stop category 0 or a stop category 1 of the machine in accordance with IEC 60204-1, as determined by the risk assessment.

NOTE 2 Some CCSs perform the GSS function by transmitting a stop command before ceasing transmission (i.e. an active stop), whereas others only cease transmission (i.e. a passive stop). An active stop can deliver a quicker stop command to the machine's control system, because the time delay associated with recognising the loss of a valid signal before initiating an automatic stop command is absent.

4.7.3.4 Emergency stop (EMS) function

A CCS that provides an EMS function shall comply with the requirements of 4.7.2, 4.7.3.3 and the following additional requirements (see also Table 3):

a) the actuator shall be marked and/or labelled as an emergency stop device (see IEC 60204-1:2005, 10.7.3 and shall conform to IEC 60947-5-5;
b) the function shall be available and operational at all times;
c) the initiation of EMS function shall result in an OFF-state of all safety-related stop output(s) at the base station;
d) relevant requirements of ISO 13850 are satisfied;
e) the information for use (see Clause 6) shall instruct the system integrator who incorporates the CCS into the machine control system to ensure that the requirements of this clause are complied with;
f) in the case of multiple remote stations that are concurrently communicating with a base station, the disabling of a remote station (unavailability of the EMS function of the disabled remote station) initiates an automatic stop (ATS) function.

NOTE It can be useful to provide an indication on the remote station that the emergency stop is available and operational, where bi-directional communication facilitates this.

4.7.3.5 Automatic stop (ATS) function

The ATS function of the CCS shall initiate an OFF-state of all safety-related stop output(s) at the base station, so as to prevent hazardous operation(s) of the machine. See Table 3.

NOTE 1 The stop outputs affected by the ATS function can be the same as those that are switched to the OFF-state by the GSS function and/or the EMS function.

The ATS function of a CCS is a safety-related control function. The ATS function shall have a safety integrity that is not less than the highest safety integrity of any other safety-related stop functions provided by the CCS.

The ATS function of the CCS shall be automatically initiated under conditions that include, but are not limited to:

- when a fault in a safety-related part of the CCS is detected;
- when no valid signal has been detected at a base station (and where necessary in accordance with risk assessment at a remote station in a CCS with bi-directional communication) within a time period declared by the CCS manufacturer. This time period shall be determined by a risk assessment at the machine, but should not exceed 0,5 s;
- when transmission ceases (see 4.9).

NOTE 2 Potential consequences of loss of ability to control the machine during this time period and the effect on the overall machine stopping time can be considered by the machine control system designer or manufacturer.

4.8 Reset

Reset after a GSS or EMS initiated at a remote station shall require a deliberate action at that remote station (and at every remote station where the safety-related stop has been initiated) before base station outputs that are intended for control of hazardous operations of the machine can be activated.

If the disengagement of the latched GSS or EMS device results in communication re-establishment, an additional manual reset action at the remote station can be necessary.

NOTE Depending on the risk assessment, in addition to the reset action(s) at the remote station, it can be opportune to consider the addition of one or more supplementary fixed reset devices (e.g. pushbuttons) at location(s) from which the hazard zone(s) can be seen to be clear of persons.

Particular consideration is necessary when the remote station is mobile or portable.

Interruption and reconnection of power (at either the remote or base station), or a single fault in any part of the CCS shall not result in the reset of a previously initiated safety-related stop function such as a GSS or EMS function.

Reset shall not be possible while a detected fault exists within the CCS.

See also 6.2 q) for information to be provided by manufacturer.

4.9 Cessation of transmission from the remote station

Where the CCS is provided with automatic cessation of transmission, neutral frames shall be transmitted for a period after operating command signal have ceased. The duration of this period of neutral frame transmission shall be stated by the CCS manufacturer. The CCS shall initiate an ATS function at the end of this pre-determined period of neutral frame transmission.

Where automatic cessation of transmission is not provided, neutral frames shall be transmitted until the next operating command signal.

NOTE Automatic cessation of transmission with an insufficient period of neutral frame transmission will cause the stop output (and hence for example, the main contactor of a machine) to go to the OFF-state more frequently, which will increase the number of switching operations for the stop output(s) and any components that it switches.

4.10 Latching control functions

For reasons of ergonomics and functionality, it can be useful for some CCS control functions to have latching capability (i.e. not hold-to-run) implemented in either the remote station or the base station.

NOTE 1 Latching of particular control functions can be achieved by a control actuator on the remote station (for example, a bi-stable switch or a potentiometer), or in the control logic of the base station.

Latching in the control logic of the remote station shall only be used to control outputs intended for non-hazardous operations of the machine.

Latching control functions in the base station shall not be used to sustain hazardous operations of the machine, unless supported by the risk assessment and realized as safety related functions. Information on this restriction shall be provided in the CCS instructions for use (see Clause 6).

NOTE 2 In some cases, for example when the CCS is used to control magnetic or vacuum lifting devices, the ability to latch a command in the base station can be a useful feature.

4.11 Behaviour on loss of supply

A variation in the battery voltage or power supply of the CCS shall not cause unintended output commands from the base station.

A visual warning shall be given to the operator when a variation in battery voltage exceeds specified limits; acoustic and/or haptic may additionally be provided. Under these circumstances, the CCS shall remain functional for a specific time declared in the information for use.

NOTE A time period of 10 min can be considered sufficient to enable the machine to be put into a non-hazardous condition. This time period can vary with battery ageing and environmental factors such as temperature.

When the battery voltage becomes so low that a reliable transmission cannot be guaranteed, the transmission power shall be removed. It shall not be possible for the remote station to transmit further frames until the battery voltage has been restored to acceptable levels and a manual reset operation has been performed (see 4.5 and 4.8).

Where information such as configuration data or address codes is stored in the CCS (see also 4.15), the retention of such data shall not depend on the presence of the supply voltage.

4.12 Multiple remote stations

Where a CCS is provided with more than one remote station, the CCS shall be designed such that the use of any one remote station precludes the use of the others, except for the initiation of the EMS function.

NOTE This requirement is not applicable to remote station(s) that are not in service.

There should be a means of indicating which remote station is in control of the base station (see also 4.5).

Transfer of control from one remote station to another shall require a deliberate action specifically designed for that purpose at the remote station that has control, in order to minimise the possibility of hazardous situations that might otherwise result from such transfer.

4.13 Multiple base stations

When a remote station can be used to communicate with one of several base stations, means shall be provided on the remote station to select which base station(s) is(are) to be connected. Selecting connection to a particular base station shall not, by itself, result in control commands at that base station.

When a remote station can be used to control more than one base station, an indication shall be provided on the base and/or on the remote station to confirm which base station(s) is(are) under the control of the remote station.

4.14 Suspension of CCS control

A suspension mode may be provided to allow the control of the machine to be switched from a CCS to another operator control station, without having OFF-state on the base station. See also 4.13.

NOTE This typical mode/feature when a machine can operate while the remote station is switched off, for example, to preserve battery charge, or while the machine is controlled by another operator control station or by the machine control system (e.g. automatic mode).

Means shall be provided within the CCS to enable the remote station to surrender and regain control of the machine. These actions shall be performed by a deliberate action on the remote station specifically designed for that purpose, for example, a special task involving the use of a designated switch or a key switch may be used.

After the surrending has been completed, the remote station is no longer in control of the machine. After the regain has been completed, the remote station is in control of the machine.

The suspension shall:

- be indicated on the remote station and
- activate an output signal at the base station for the machine control system.

Where this mode is available, EMS is not allowed on the remote station.

4.15 Configurability protection

Measures shall be taken to ensure that any configurable functionality of a CCS is protected against unauthorised modification. Example of such configurable functionality are, the duration of neutral frame transmission (see 4.9), or the communication pairing of remote and base stations, including allocation of control actuators to outputs (see 4.2.3).

5 Verification

5.1 General

The specified requirements of a CCS and its interfacing with the machine control system shall be verified by visual inspection, analysis (i.e. calculations) and/or testing (i.e. type tests, acceptance/routine tests, functional tests and integration tests) carried out by the manufacturer of the CCS and/or the system integrator as appropriate (i.e. as specified in the information for use provided by the CCS manufacturer).

NOTE Some of the verification activities relate to properties of the CCS itself, while others relate to the correct configuration of the CCS and the suitability of its interfacing with the machine control system.

Where any aspect of the configuration of the CCS with the machine control system is changed or modified, appropriate verification shall be repeated.

5.2 Labelling and markings

It shall be verified that there is unambiguous identification on the CCS remote station and the base station and that the nameplates of each include at least the information specified in Clause 7.

5.3 Documentation

Verify that the CCS complies with the information for use (see Clause 6).

5.4 Functional verifications

Compliance with the functional requirements specified in Clause 4 shall be checked by carrying out applicable tests; a test may be omitted if analysis demonstrates conclusively that the CCS would pass the test.

A summary of the functional requirements of the CCS that require verification is provided in Table 4 that also covers verification procedures applicable to the system integrator for the

interfacing of the CCS with the machine control system, as specified in the information for use. See 6.2, x).

Table 4 – Verification of functional requirements

Ref. Clause	Requirement	Method (one or more of the specified methods apply)			Additional verification requirements
		Analysis	Testing	Visual inspection	
4.2.1	Inadvertent actuation		X	X	While the CCS is in an operationally-ready state, the portable remote station shall be tested in accordance with 5.1 (Drop and topple) and 5.2 (Freefall procedure 1) of IEC 60068-2-31:2008. In addition to the final inspection and checks defined in Clause 6 of IEC 60068-2-31:2008, during these tests no signal change shall occur except for that corresponding to GSS, EMS or ATS functions.
4.2.2	Prevention of unauthorized operation		X	X	
4.2.3	Prevention of unintended commands	X[a]	X[a]		
4.3	Serial data transfer	X	X		To test also the incorrect addressing and corruption of frames, for example creating disturbances.
4.4	Removal of remote station transmission power	X	X		
4.5	Establishment and indication of transmission and communication		X	X	
4.6	Safety-related functions of the CCS	X	X		
4.7	Stop functions of the CCS	X	X	X	
4.7.3.4	Additional requirements for the EMS function	X[a]	X[a]	X[a]	
4.8	Reset		X	X	
4.9	Cessation of transmission from the remote station		X		
4.10	Latching control functions	X	X		
4.11	Behaviour on loss of supply		X		
4.11	Battery-powered remote station		X	X	The battery shall initially be fully charged in accordance with the manufacturer's recommendation. During these tests, the charging supply shall be disconnected from the remote station, the remote station shall be communicating with the maximum number of base stations (for example, 1 in single, 2 in tandem) and the remote station shall continue to transmit for the duration of the test.
4.12	Multiple remote stations		X	X	
4.13	Multiple base stations		X	X	
4.14	Suspension of CCS control	X	X		
4.15	Configurability protection		X		

[a] All marked methods apply for this verification

6 Information for use

6.1 General

All information necessary for the identification, transport, installation, use, maintenance and decommissioning and disposal of a CCS shall be supplied in an appropriate format, for example, drawings, diagrams, charts, tables, instructions.

NOTE 1 The technical documentation provided with a CCS will form part of the overall documentation of the machine.

NOTE 2 In some countries, the requirement to use specific language(s) is covered by legal requirements.

6.2 Information to be provided

The documentation made available to the user shall include the following information.

a) The manufacturer's name (trade name, mark of origin) and full address.

b) A general description of the CCS.

c) The environmental and operating conditions (temperature, humidity, etc.) under which the remote station and the base station are intended to be used.

d) The transmission output power or emission level.

e) Details of the rated operating voltage (DC, AC, frequency) and power consumption, including the following details for the battery:

- recommended battery specification for the remote station, if replaceable by the user;
- duration of typical operation on a single battery charge and its reference conditions;
- procedures for replacing and charging batteries;
- approximate time between a low battery warning and the initiation of remote station shutdown and factors (e.g. ageing or temperature of battery) that can affect such a time.

f) Nominal operating distance range in free line of sight.

g) Instructions on how to resolve potential interference problems between the CCS and other systems in use at that location.

h) Details of all control actuators and their associated control functions, including the maximum response time for each control function.

i) Where applicable, instructions on the transfer of control between different remote stations.

j) Whether or not an automatic power-off (removal of transmission power) is provided, and the maximum duration of neutral frame transmission where it is provided.

k) Whether any control functions and associated outputs of the base station have latching functionality (see 4.10) that is either user-configurable or factory preset, and provide configuration instructions as appropriate. Provide instructions on restrictions relating to the use of latching functionality for the control of hazardous operations of the machine including functionality in transitional situations such as power-up or re-establishment of communication.

l) Whether the communication pairing between remote and base stations is factory preset or user-configurable, and provide configuration instructions as appropriate.

m) A functional specification of each safety-related control function (including stop functions) supported by the CCS, to include:

- a description of its functionality;
- the reaction in case of error detection;
- timing information, including any delay time for the safety-related output interface (e.g. contacts) for the EMS, GSS and ATS functions.

n) For the ATS function of the CCS (see 4.7.3.5), specify:

- all conditions that result in its initiation;
- the time interval between the loss of a valid signal and its initiation;
- the maximum response time within the CCS; in case of different time for different reasons, each time has to be declared.

o) For each safety-related control function, a specification of its safety integrity in terms of:
- a SIL if it is designed in accordance with IEC 61508 or IEC 62061, and/or
- a PL if it is designed in accordance with ISO 13849-1.

NOTE Additional relevant data (e.g. PFH_D, $MTTF_D/B10_D$, DC, SFF) can be used to facilitate integration of the CCS into a machine control system.

p) Details of all initiators of a stop function of the CCS, including whether each will result in a stop command that is active, passive, or active followed by passive and the maximum response times within the CCS.

q) Instructions for performing a:
- reset after any safety-related stop function has been initiated;
- recovery after loss of communication, or failure or malfunction of the remote station or the base station.

r) Instructions on the use and availability of the EMS function, where provided, to include an instruction that the emergency stop device of a portable or mobile remote station shall not be the sole means of initiating the EMS function of a machine.

s) An instruction that a reset after an EMS function has been initiated at a portable or mobile remote station shall only be possible when it can be seen that the reason for initiation has been resolved, and that this can require the use of supplementary fixed reset devices.

t) Specify which outputs of the base station can be activated when only a neutral frame is being received (or without receiving a neutral frame following re-establishment of communication) and provide warnings about their use for the control of hazardous operations of the machine.

u) Instructions on the means of preventing unauthorised operation.

v) Description of error code handling and recommended operator reactions.

w) If the EMS function is provided, specify that has to be available and operational at all times, regardless of the operating mode of the machine (for example, automatic/manual, remote/local).

x) Details of all verification activities that it are necessary for the system integrator to perform when the CCS is integrated into the electrical equipment of the machinery (see Table 5 and 5.4).

Table 5 – List of possible verifications to be required to the system integrator

Functional requirement
Inadvertent actuation
Prevention of unauthorized operation
Prevention of unintended commands
Removal of remote station transmission power
Establishment and indication of transmission and communication
Safety-related functions of the CCS
Stop functions of the CCS
Reset
Latching control functions
Behaviour on loss of supply
Battery-powered remote station
Warning indicators
Multiple remote stations
Multiple base stations
Response time
Suspension of CCS control

7 Labelling and markings

The CCS base station and remote station shall each have a nameplate that is legibly and durably marked, and suitable to withstand the application (environment, etc.) and intended use. The nameplate on both the base station and remote station shall contain at least the following information:

- name or trade mark of supplier;
- certification mark, when required;
- serial number and model;
- operating frequency band;
- the rated voltage

and where relevant:

- type and rating of batteries;
- additional markings as necessary to identify matched remote station(s) and base station(s).

Annex A
(informative)

Logic of stop functions

The stop functions of a CCS can be initiated manually or automatically and can be performed by an active stop and/or a passive stop.

NOTE An active stop can be automatically followed by a passive stop.

Figure A.1 shows typical logic sequences for stop functions of a CCS. Numbers 1 to 5 beside the arrows correspond to the sequences.

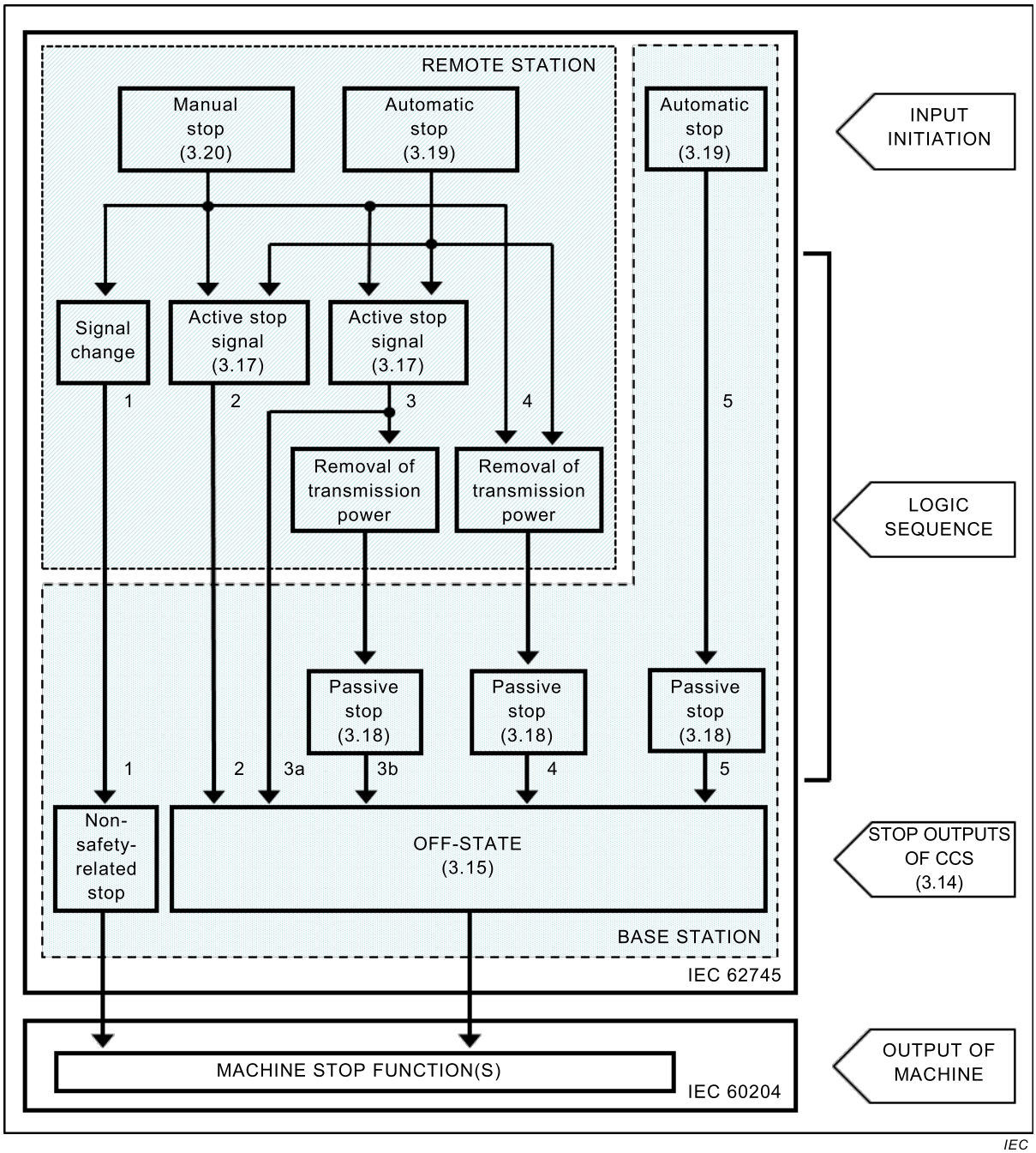

Figure A.1 – Logic for stop functions

Sequence 1 represents a type of manually-initiated stop that results in a stop state of the non-safety-related stop outputs of the CCS. For example, releasing a hold-to-run control actuator results in the CCS performing a control stop function, which causes associated movement of the machine to stop. An OFF-state is not produced at the base station.

Sequences 2, 3 and 4 represent various types of manual stop (3.20) or automatic stop (3.19), all of which ultimately result in an OFF-state at the base station.

a) Sequence 2 – An active stop only:

- Manual stop (3.20) example: Activating a STOP actuator causes a stop signal to be transmitted by the remote station, which produces an OFF-state at the base station. The remote station transmission power is not removed.
- Automatic stop (3.19) example: In response to a particular situation, the remote station transmits a stop signal, which produces an OFF-state at the base station. The remote station transmission power is not removed.

b) Sequence 3 – An active stop automatically followed by removal of remote station transmission power. An OFF-state is initiated at the base station by an active stop (3a) and by a passive stop (3b). The passive stop (3b) therefore initiates an OFF-state even if the active stop (3a) is ineffective:

- Manual stop (3.20) example: Activating a STOP actuator causes a stop signal to be transmitted and it then also removes the remote station transmission power. An OFF-state is initiated at the base station when it receives the stop signal, or when the subsequent absence of a valid signal is detected.
- Automatic stop (3.19) example: In response to a particular situation, the remote station transmits a stop signal before the transmission power is removed. An OFF-state is initiated at the base station when it receives the stop signal, or when the subsequent absence of a valid signal is detected.

c) Sequence 4 – A passive stop resulting from removal of remote station transmission power:

- Manual stop (3.20) example: Activating a STOP actuator removes the remote station transmission power. An OFF-state is initiated at the base station when it detects the resulting absence of a valid signal.
- Automatic stop (3.19) example: In response to a particular situation, the removal of transmission power is triggered in the remote station. An OFF-state is initiated at the base station when it detects the resulting absence of a valid signal.

Sequence 5 represents a further type of automatic stop (3.19), in which a passive stop and the resulting OFF-state is automatically initiated at the base station. For example, the remote station is moved outside of the operating range, i.e. too far from the base station, which automatically initiates an OFF-state at the base station because a valid signal is absent.

Bibliography

IEC 60050 (all parts), *International Electrotechnical Vocabulary* (available at http://www.electropedia.org)

IEC 60050-441:1984, *International Electrotechnical Vocabulary. Switchgear, controlgear and fuses*

IEC 60068-2-1, *Environmental testing – Part 2-1: Tests – Test A: Cold*

IEC 60068-2-2, *Environmental testing – Part 2-2: Tests – Test B: Dry heat*

IEC 60068-2-6, *Environmental testing – Part 2-6: Tests – Test Fc: Vibration (sinusoidal)*

IEC 60068-2-27, *Environmental testing – Part 2-27: Tests – Test Ea and guidance: Shock*

IEC 60068-2-30, *Environmental testing – Part 2-30: Tests – Test Db: Damp heat, cyclic (12 h + 12 h cycle)*

IEC 60068-2-64, *Environmental testing – Part 2-64: Tests – Test Fh: Vibration, broadband random and guidance*

IEC 60204 (all parts), *Safety of machinery – Electrical equipment of machines*

IEC TR 60870-1-3, *Telecontrol equipment and systems – Part 1: General considerations – Section 3: Glossary*

IEC 60870-5-1, *Telecontrol equipment and systems – Part 5: Transmission protocols. Section One – Transmission frame formats*

IEC 60947-5-8, *Low-voltage switchgear and controlgear – Part 5-8: Control circuit devices and switching elements – Three-position enabling switches*

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

IEC 61784-1, *Industrial communication networks – Profiles – Part 1: Fieldbus profiles*

IEC 61784-3:2016, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

ISO 12100, *Safety of machinery – General principles for design – Risk assessment and risk reduction*

EN 13557:2003, *Cranes – Controls and control stations*

———————

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO 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