Options for ABB drives

# User's manual
# Emergency stop, stop category 0 (option +Q951) for ACS880-07CLC drives


Power and productivity
for a better world™

# User's manual

Emergency stop, stop category 0 (option +Q951) for ACS880-07CLC drives





3AXD50000123384 A
EN
EFFECTIVE: 2017-09-12

# Table of contents

1

# Safety instructions

## Contents of this chapter

Only a qualified electrician who has appropriate knowledge on functional/machine/process safety is allowed to install, start up and maintain the safety circuit.

**WARNING!**

After you have made additions to the drive safety circuit or modified it, changed circuit boards inside the drive, always test the operation of the safety circuit according to its acceptance test procedure. The change can affect unexpectedly. All customer-made changes are on the customer's responsibility.

**WARNING!**

Read and obey all safety instructions given for the drive in its hardware manual. If you ignore them, injury or death, or damage to the equipment can occur.

This manual does not repeat the complete safety instructions of the drive but it only includes the instructions related to the scope of this manual.

2

# Introduction to the manual

## Contents of this chapter

This chapter describes the manual in short and gives some general information for the reader. This chapter also contains a quick reference for implementing a safety system.

## Applicability

The manual applies to the ACS880-07CLC drives which have the option: Emergency stop, stop category 0, with safety relays (option +Q951).

## Target Audience

The manual is intended for people who install, start up, use and service the safety option of the drive. Read the manual before working on the drive. You are expected to know the fundamentals of electricity, wiring, electrical components, electrical schematic symbols, and functional safety.

## Exclusion of liability

ABB is not responsible for the implementation, verification and validation of the overall safety system. It is the responsibility of the system integrator (or other party) who is responsible for the overall system and system safety.

The system integrator (or other responsible party) must make sure that the entire implementation complies with all relevant standards, directives and local electrical code, and that the system is tested, verified and validated correctly.

# Quick reference guide for implementing a safety system

| Task | ☑ |
|---|---|
| Select the appropriate functional safety standard for the implementation: EN ISO 13849-1, EN/IEC 62061, IEC 61511 or other. | ☐ |
| If you select EN/IEC 62061 or IEC 61511, make a safety plan. See EN/IEC 62061 or IEC 61511. | ☐ |
| Assess safety: analyze and evaluate risks (estimate SIL/PL) and define risk reduction strategies. Define the safety requirements. | ☐ |
| Design the safety system. The part of the design made by ABB is described in section Option description and instructions. | ☐ |
| If you made any changes to the delivered safety system, verify the achieved SIL/PL with, for example, FSDT-01 Functional safety design tool or similar. See *Functional safety design tool user's manual* (3AXD10000102417 [English]). | ☐ |
| Connect the wiring. See section Wiring. | ☐ |
| Set the parameters. See section Parameter settings. | ☐ |
| Validate that the implemented system meets the safety requirements:<br>Do the acceptance test. See section Start-up and acceptance test. | ☐ |
| Write the necessary documentation. | ☐ |

# Terms and abbreviations

| Term/Abbr. | Description |
|---|---|
| Cat. | Classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behavior in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability. The categories are: B, 1, 2, 3 and 4. (EN ISO 13849-1) |
| CCF | Common cause failure (%) (EN ISO 13849-1) |
| DC | Diagnostic coverage (EN ISO 13849-1) |
| EMC | Electromagnetic compatibility |
| HFT | Hardware fault tolerance (IEC 61508) |
| $PFD_{avg}$ | Average probability of dangerous failure on demand (IEC 61508) |
| PFH | Average frequency of dangerous failures per hour (IEC 61508) |
| PL | Performance level. Levels a...e correspond to SIL (EN ISO 13849-1) |
| SC | Systematic capability (IEC 61508) |
| SIL | Safety integrity level (1...3) (IEC 61508) |
| SILCL | Maximum SIL (level 1...3) that can be claimed for a safety function or subsystem (IEC/EN 62061) |
| STO | Safe torque off (IEC/EN 61800-5-2) |
| T1 | Proof test interval. Defines the probabilistic failure rate (PFH or PFD) for the safety function or subsystem. Performing a proof test at a maximum interval of T1 is required to keep the SIL capability valid. The same interval must be followed to keep the PL capability (EN ISO 13849) valid. Note that any T1 values given cannot be regarded as a guarantee or warranty. |

# Related documents

| Manual | Code |
|---|---|
| **Drive hardware manuals and guides** | |
| ACS880-07CLC drives hardware manual | 3AXD50000131457 |
| ACX-AP-x assistant control panels user’s manual | 3AUA0000085685 |
| **Drive firmware manuals and guides** | |
| ACS880 primary control program firmware manual | 3AUA0000085967 |
| ACS880 primary control program quick start-up guide | 3AUA0000098062 |
| ACS880 diode supply control program firmware manual | 3AUA0000103295 |
| ACS880 distributed I/O bus supplement | 3AXD50000126880 |
| **General safety guides** | |
| Functional safety design tool user’s manual | 3AXD10000102417 |
| Functional safety; Technical guide No. 10 Safety and functional safety; A general guide | 3AUA0000048753 |
| **Option manuals and guides** | |
| Drive composer start-up and maintenance PC tool user's manual | 3AUA0000094606 |
| Emergency stop, stop category 0 (option +Q951) for ACS880-07CLC drives user's manual | 3AXD50000123384 |
| Manuals and quick guides for I/O extension modules, fieldbus adapters, etc. | |
| **Other documents** | |
| Circuit diagrams delivered with the drive | |
| Part lists delivered with the drive | |

You can find manuals and other product documents in PDF format on the Internet. See Document Library. For manuals not available in the Document library, contact your local ABB representative.

For additional ABB safety information and solutions visit http://www.abb.com/safety.

3

# Option description and instructions

## Contents of this chapter

This chapter describes the safety function and instructs how to wire, start up, test, validate, use and maintain it. The safety data is also given.

## Overview

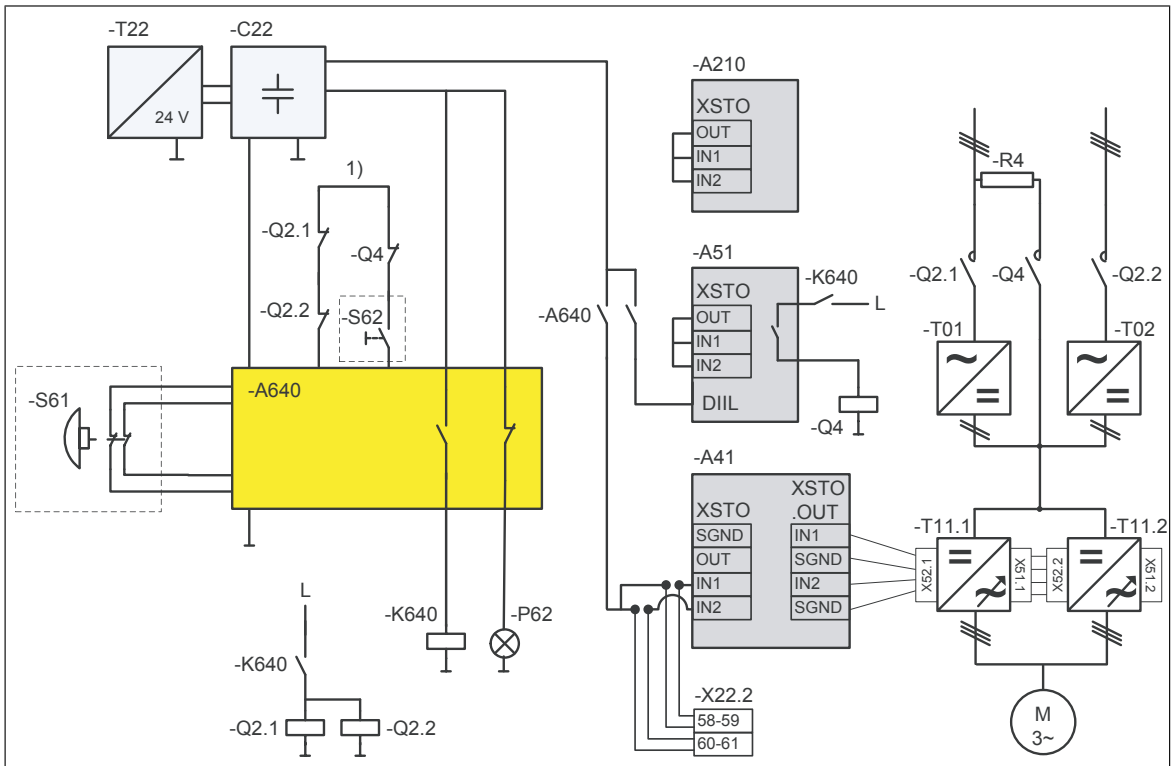
This emergency stop function corresponds to an uncontrolled stop in accordance with stop category 0 (EN/IEC 60204-1). After the emergency stop command has been given, the drive trips the main contactors which cut off the input power of the drive. The motor coasts to a stop.

The design principles of the safety function comply with EN ISO 13850.

For a list of related standards and European directives, see section *Related standards and directives (page 24)*.

# Operation principle

Initial status: The drive is in operation and the motor is running.




| | | | |
|---|---|---|---|
| 1) | Reset circuit | P62 | Emergency stop indication lamp |
| A41 | Control unit (inverter unit) | T01/T02 | Supply module |
| A51 | Control unit (supply unit) | T11.1/T11.2 | Inverter module |
| A210 | Control unit (liquid cooling unit) | T22 | 24 V DC power supply |
| A640 | Emergency stop safety relay | C22 | Buffer module |
| K640 | Auxiliary safety relay | X22.2 | Customer terminal |
| Q2.1/Q2.2 | Main contactors | X5x.x | Inverter STO terminals |
| Q4 | Charging contactor | L | Line voltage |
| S61 | Emergency stop button | M | Motor |
| S62 | Emergency stop reset | | |
| The dash line indicates a customer-defined installation. | | | |

| Step | Operation |
|---|---|
| 1. | The user activates emergency stop, for example, by pushing the emergency stop button [S61]. |
| 2. | The emergency stop safety relay [A640] switches off the XSTO inputs IN1 and IN2 of the inverter control unit [A41]. The XSTO.OUT terminal delivers the signal to the inverter modules and opens the STO circuit of the inverter modules.<br>The emergency stop safety relay [A640] de-energizes the main contactors [Q2.1/Q2.2] and the charging contactor [Q4] and activates the DIIL input on the supply control unit [X51]<br>The main contactors [Q2.1/Q2.2] switch off the power supply to the inverter modules [T11.1/T11.2]. |
| 3. | The emergency stop indication lamp [P62] switches on. |
| 4. | The motor coasts to zero speed and remains at zero speed while the emergency stop is active. |
| 5. | Normal operation resumes after the user:<br>• releases the emergency stop button [S61] to normal (up) position<br>• resets the emergency stop circuit (customer-defined)<br>• resets the inverter unit (if the STO indication parameter *31.22* has been set so that a fault is generated).<br>If the drive is used in remote control mode, see the firmware manual for more information. |

# Fault reaction function

**Definition**: A safety function requires a “fault reaction function” that attempts to initiate a safe state if the safety function's diagnostics detect a fault within the hardware/software that performs the safety function.

The fault reaction function of the emergency stop safety relay trips if it detects a failure (short circuit between signals, open circuits, redundancy fault when the emergency stop button is pushed) in the safety circuit. The fault reaction function shifts the drive immediately into the safe state by switching on the drive emergency stop command, opening the main contactor, and keeping them on until the detected fault has been repaired. The indication lamp of the reset button is on until the fault has been repaired.

The emergency stop reset circuit must be open when the user releases the emergency stop button. The emergency stop safety relay detects if the reset circuit is closed and the relay does not close.

# Parameter settings

The parameter setting in the inverter control program:

- parameter *31.22 STO indication run/stop* is set to value *Warning/Warning* (recommended).

The parameter settings in the supply control program:

- parameter *121.04 Emergency stop mode* is set to value *Stop and warning*
- parameter *121.05 Emergency stop source* is set to value *DIIL*.

For more information, see the firmware manuals.

# Hardware settings

Appropriate hardware settings have been preset at the factory for the safety function.

The emergency stop safety relay [A640] is wired to the manual reset mode at the factory.

# Wiring

The customer must wire an emergency stop button to the safety system. One emergency stop button is installed on the cabinet door.

There are double contacts in the emergency stop button and double wiring (two-channel connection) between the button and the emergency stop safety relay. The safety relay detects cross faults and faults across one contact from the emergency stop button. This function must be used in a redundant manner, that is, the emergency stop button must be connected to both terminals with a separate contact.

If needed, install additional emergency stop buttons on site and wire them to the appropriate terminal block inside the drive cabinet. See the circuit diagrams delivered with the drive. Obey these rules:

1. Use only double-contact buttons approved for the emergency stop circuits.
2. Connect the emergency stop buttons with two conductors (two-channel connection).

   **Note:**

   Keep the channels separate. If you use only one channel, or if the first and second channels are connected together (for example, in a chain), the cross fault detection of the emergency stop safety relay trips and activates the emergency stop command of the drive as it detects a redundancy fault.

3. Use a shielded, twisted pair cable. We recommend a double-shielded cable and gold-plated contacts in the emergency stop button.
4. Ensure that the sum resistance for one channel (loop resistance) from the field to the safety relay does not exceed 70 ohm.
5. Obey the general control cable installation instructions given in the drive hardware manual.

You must install and wire a reset button (or similar) to terminal block [X22.2] on the drive. See the circuit diagrams delivered with the drive. We recommend gold-plated contacts in the reset button. Obey these rules:

1. Sum resistance of the external reset circuit must not exceed 70 ohm.
2. Obey the general control cable installation instructions given in the drive hardware manual.

**Note:**

The safety system and customer-made wirings are on the customer’s responsibility.

# Start-up and acceptance test

You need the Drive composer PC tool or a control panel to perform the start-up and acceptance test.

Initial status: Make sure that the drive is ready for use, that is, you have done the tasks of the drive start-up procedure. See the hardware manual.

| Action | ☑ |
|---|---|
| **WARNING!** Obey the safety instructions. If you ignore them, injury or death, or damage to the equipment can occur. | ☐ |
| **Checks and settings with no voltage connected** | |
| Check the connections against the appropriate circuit diagrams: the emergency stop button, reset circuit, STO circuits, and connections to the contactors. | ☐ |
| Check that the hardware settings relevant to the safety function are set as defined in section Hardware settings. | ☐ |
| **Settings with voltage connected** | |
| Check that the parameters relevant to the safety function are set as defined in section Parameter settings. | ☐ |
| **Acceptance test** | |
| Make sure that you can ran and strop the motor freely during the test. | ☐ |
| Start the drive and make sure that the motor is running. If possible, use a motor speed close to the maximum speed of the application. | ☐ |
| Push the emergency stop button. | ☐ |
| Make sure that the drive stops the motor by coasting and displays the correct warnings. See section Emergency stop indications. | ☐ |
| Make sure that the indication lamp switches on. | ☐ |
| Make sure that you cannot switch the power on with the operating switch. | ☐ |
| Make sure that you cannot start the drive and motor from any control location:<br>Make sure that the motor does not start even if you switch the start signal off and on or push the start key of the panel. | ☐ |
| Turn the emergency stop button until it releases and returns to the up position. | ☐ |
| Reset the emergency stop circuit. | ☐ |
| Make sure that the indication lamp switches off. | ☐ |
| Switch off the drive start signal. | ☐ |
| Power up the drive (see the hardware and firmware manuals). | ☐ |
| Restart the drive and motor and check that they operate normally. | ☐ |
| Repeat the test from each operating location (every emergency stop button and reset button). | ☐ |
| Fill in and sign the acceptance test report which verifies that the safety function is safe and accepted to operation. | ☐ |

# Use of the safety function

## Activating

1. Push the emergency stop button. The emergency stop activates and the button locks in “ON” (open) position.

## Resetting

1. Turn the emergency stop button until it releases.
2. Reset the emergency stop circuit (customer-defined).
   The indication lamp switches off. The emergency stop function deactivates.
3. Reset the drive if necessary.
4. Close the main contactors with the operating switch if necessary (see the hardware and firmware manuals).
   The main contactors close and the drive is powered up.
5. Make sure that the drive has received the start signal (depends on the configuration, see the firmware manual).
6. You can now restart the drive.

**Note:**

You have to reset the emergency stop circuit also after you have powered up the drive.

# Emergency stop indications

When the emergency stop is on:

- the inverter control program has the *Safe torque off* warning active,
- the supply control program has the *Emergency stop* warning active,
- the emergency stop indication lamp on the cabinet door is illuminated.

# Fault tracing

The emergency stop safety relay type is Phoenix Contact PSR-MC34. For more information, see the data sheet of the relay (www.phoenixcontact.com).

This table describes the status LEDs of the safety relay.

| PWR LED | IN1/2 LED | K1 LED | K2 LED | LED is lit and steady |
|---|---|---|---|---|
| ON | OFF | OFF | OFF | All relays are not activated. The sensor circuit is off. Possible error. For more information, see the data sheet of the relay. |
| ON | ON | OFF | OFF | Relay K1 is energized. |
| ON | ON | ON | ON | Relay K2 is energized. |

# Maintenance

After the operation of the safety function is tested at start-up, it does not need any scheduled maintenance, excluding the main contactor which has a limited lifetime. Replace the contactor before the end of its lifetime. See the contactor data sheet or manual. Repeat the acceptance test for the function after the replacement. See section Start-up and acceptance test.

In addition to proof testing, it is a good practice to check the operation of the function when other maintenance routines of the machinery are carried out. Do acceptance test described in section Start-up and acceptance test.

If you change any wiring or component after the start-up, or restore parameters to their default values:

- Use only ABB approved spare parts.
- Register the change to the change log for the safety circuit.
- Test the safety function again after the change. Obey the rules given in section Start-up and acceptance test.
- Document the tests and store the report into the logbook of the machine.

## Proof test interval

After the operation of the safety function is validated at start-up, the safety function must be maintained by periodic proof testing. In high demand mode of operation, the maximum proof test interval is 20 years. In low demand mode of operation, the maximum proof test interval is 1 year (high or low demand as defined in IEC 61508, EN/IEC 62061 and EN ISO 13849-1). Regardless of the mode of operation, it is a good practice to check the operation of the safety function at least once a year. Do the test as described in section Start-up and acceptance test.

The person responsible for the design of the complete safety function should also note the Recommendation of Use CNB/M/11.050 published by the European co-ordination of Notified Bodies for Machinery concerning dual-channel safety-related systems with electromechanical outputs:

- When the safety integrity requirement for the safety function is SIL 3 or PL e (cat. 3 or 4), the proof test for the function must be performed at least every month.
- When the safety integrity requirement for the safety function is SIL 2 (HFT = 1) or PL d (cat. 3), the proof test for the function must be performed at least every 12 months.

This is a recommendation and depends on the required (not achieved) SIL/PL. For example, safety relays, contactor relays, emergency stop buttons, switches etc. are typically safety devices which contain electromechanical outputs.

## Competence

The maintenance and proof test activities of the safety function must be carried out by a competent person with expertise and knowledge of the safety function as well as functional safety, as required by IEC 61508-1 clause 6.

## Residual risk

The safety functions are used to reduce the recognized hazardous conditions. In spite of this, it is not always possible to eliminate all potential hazards. Therefore the warnings for the residual risks must be given to the operators.

## Intentional misuse

The safety circuit is not designed to protect a machine against intentional misuse.

## Decommissioning

When you decommission an emergency stop circuit or a drive, make sure that the safety of the machine is maintained until the decommissioning is complete.

# Safety data

The safety data given below is valid for the default design of the safety circuit. In case the final design differs from the default, ABB calculates new safety data and delivers it separately to the customer.

## Safety data values

The safety data calculations are based on the following assumptions on the operation of the main contactors [Q2.1/Q2.2]:

- It is switched at low load current (normal use, ~0%, AC-1).
- It is used for the emergency stop once a month.
- It is used for the ordinary on and off once a day.

| ACS880-07CLC type | Contactors | SIL / SILCL | PL | PFH[1] [1/h] | $PFD_{avg}$ | DC[2] [%] | SC | Cat. | HFT | CCF | Life time [a] | T1[3][4] [a] |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| -1470A-7 | AF1250 and AF16 | 2 | d | 9.6E-7 | 4.6E-03 | >90 | 3 | 2 | 0 | 65 | 20 | 20 / 1 |
| | | | | | | | | | | | | 3AXD10000097591 Rev E |

[1] PFH values according to EN ISO 13849.

[2] DC for low demand mode is 0% (determined by the DC of the worst component in the subsystem).

[3] See also the Recommendation of Use CNB/M/11.050 published by the European coordination of Notified Bodies for lower T1 requirement.

[4] T1 = 20 a stands for high demand use. T1 = 1 a is used with low demand mode of operation.

**Note:**

If $T_1$ > 1 a is needed in low demand mode of operation, SIL 1 / PL c levels shall be used and PFD calculated separately.

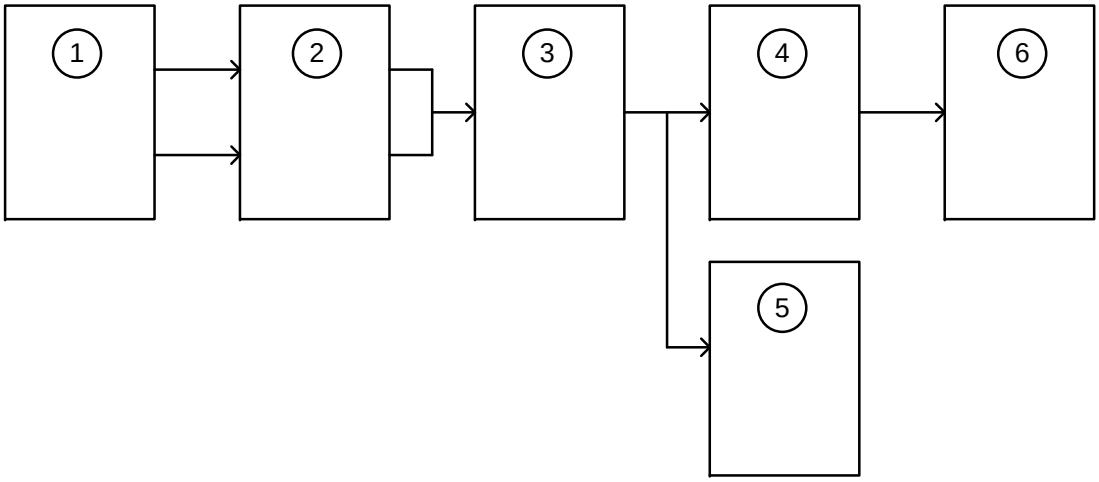
## Safety component types

Safety component types as defined in IEC 61508-2:

- emergency stop button: type A
- emergency stop safety relay: type A
- auxiliary safety relay: type A
- main contactors: type A
- charging contactor: type A

## Safety block diagram

The components that are included in the safety circuit are shown in this safety block diagram.




| No. | Description |
|---|---|
| 1 | Emergency stop button |
| 2 | Emergency stop safety relay |
| 3 | Auxiliary safety relay |
| 4 | Main contactor |
| 5 | Charging supply contactor |
| 6 | Main contactor |

## Relevant failure modes

- The main contactor does not open when requested. (All contactor failures are considered dangerous.)
- Internal failures of safety relays and the emergency stop button. These failures are included in the PFH value of the function.

## Fault exclusions

Fault exclusions (not considered in the calculations):

- any short and open circuits in the cables of the safety circuit
- any short and open circuits in the cabinet terminal blocks of the safety circuits.

## Operation delays

Emergency stop total delay: less than 250 ms.

# General rules, notes and definitions

## Validation of the safety functions

You must do an acceptance test (validation) to validate the correct operation of safety functions.

### Validation procedure

You must do the acceptance test using the checklist given in section Start-up and acceptance test.

- at initial start-up of the safety function
- after any changes related to the safety function (wiring, components, safety function related parameter settings etc.)
- after any maintenance action related to the safety function.

The acceptance test must include at least the following steps:

- you must have an acceptance test plan
- you must test all commissioned functions for proper operation, from each operation location
- you must document all acceptance tests.

### Acceptance test reports

You must store the signed acceptance test reports in the logbook of the machine. The report must include, as required by the referred standards:

- a description of the safety application (including a figure)
- a description and revisions of safety components that are used in the safety application
- a list of all safety functions that are used in the safety application
- a list of all safety related parameters and their values
- documentation of start-up activities, references to failure reports and resolution of failures
- the test results for each safety function, checksums, date of the tests and confirmation by the test personnel.

You must store any new acceptance test reports performed due to changes or maintenance in the logbook of the machine.

### Competence

The acceptance test of the safety function must be carried out by a competent person with expertise and knowledge of the safety function as well as functional safety, as required by IEC 61508-1 clause 6. The test procedures and report must be documented and signed by this person.

## Ambient conditions

For the environmental limits for the safety functions and the drive, refer to the hardware manual of your drive.

## Reporting problems and failures related to safety functions

Contact your local ABB representative.

# Related standards and directives

| Standard | Name |
|---|---|
| EN 60204-1:2006 + AC:2010<br>IEC 60204-1:2016 | Safety of machinery – Electrical equipment of machines – Part 1: General requirements |
| IEC 61508 Parts 1-3, Ed. 2.0:2010 | Functional safety of electrical/electronic/programmable electronic safety-related systems |
| IEC 61800-5-2:2016<br>EN 61800-5-2:2007 | Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional |
| IEC 62061:2015 Ed. 1.2<br>EN 62061:2005 +AC:2010+A1:2013+ A2:2015 | Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems |
| EN ISO 12100:2010 | Safety of machinery – General principles for design – Risk assessment and risk reduction |
| EN ISO 13849-1:2015 | Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design |
| EN ISO 13849-2:2012 | Safety of machinery – Safety-related parts of control systems – Part 2: Validation |
| EN 61800-3:2004 + A1:2012 | Adjustable Speed Electrical Power Drive Systems - Part 3: EMC requirements and specific test methods |
| IEC 61326-3-1:2008 | Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – General industrial applications |
| IEC 60533:2015 | Electrical and electronic installations in ships – Electromagnetic compatibility (EMC) – Ships with a metallic hull |
| IEC 61511-1:2016 | Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application programming requirements |
| EN ISO 13850:2015 | Safety of machinery – Emergency stop – Principles for design |
| 2006/42/EC | European Machinery Directive |
| Other | Sector-specific C-type standards |

# Compliance with the European Machinery Directive

The drive is an electronic product which is covered by the European Low Voltage Directive. However, the drive internal safety function of this manual is in the scope of the Machinery Directive as a safety component. This function complies with European harmonized standards such as EN/IEC 61800-5-2. The declaration of conformity is delivered with the drive.

# Further information

## Product and service inquiries

Address any inquiries about the product to your local ABB representative, quoting the type designation and serial number of the unit in question. A listing of ABB sales, support and service contacts can be found by navigating to www.abb.com/searchchannels.

## Product training

For information on ABB product training, navigate to new.abb.com/service/training.

## Providing feedback on ABB manuals

Your comments on our manuals are welcome. Navigate to new.abb.com/drives/manuals-feedback-form.

## Document library on the Internet

You can find manuals and other product documents in PDF format on the Internet at www.abb.com/drives/documents.

a50 (frozen)
PDF-Web
Created 2017-09-12, 16:23:51

# Contact us

**www.abb.com/drives**

3AXD50000123384 A (EN) EFFECTIVE 2017-09-12

3AXD50000123384A

Power and productivity
for a better world™