Options for ABB drives

User's manual
Emergency stop, stop category 0 (+Q951+Q984) for ACS880-07CLC drives

Power and productivity
for a better world™

User's manual

Emergency stop, stop category 0 (+Q951+Q984) for ACS880-07CLC drives

Table of contents

1. Safety instructions

© 2018 ABB Oy. All Rights Reserved.

3AXD50000207848 Rev A
EN
EFFECTIVE: 2018-02-23

Table of contents

1 Safety instructions

Contents of this chapter 7
Use of warnings and notes 7
Safety instructions 8

2 Introduction to the manual

Contents of this chapter 9
Applicability 9
Target audience 9
Exclusion of liability 9
Quick reference guide for implementing a safety system 10
Terms and abbreviations 10
Related documents 11

3 Description and instructions for option +Q951

Contents of this chapter 13
Overview 13
Operation principle 14
Fault reaction function 15
Parameter settings 16
Hardware settings 16
Wiring 16
Start-up and acceptance test 17
Use of the safety function 18
Activating 18
Resetting 18
Emergency stop indications 18
Fault tracing 18

4 Description and instructions for option +Q951+Q984

Contents of this chapter 19
Overview 19
Operation principle 20
Fault reaction function 22
Parameter settings 22
Hardware settings 22
Wiring 23
Start-up and acceptance test 23
Emergency stop button 23
Push button monitoring 24
Use of the safety function 25
Activating 25
Resetting 25
Emergency stop indications 25
Fault tracing 25

5 Maintenance

Proof test interval 28
Competence 28
Residual risk 28
Intentional misuse 28
Decommissioning 28

6 Technical data

Contents of this chapter 29
Safety data 30
Safety data values 30
Safety component types 30
Safety block diagram 31
Relevant failure modes 31
Fault exclusions 31
Operation delays 31
General rules, notes and definitions 32
Validation of the safety functions 32
Validation procedure 32
Acceptance test reports 32
Competence 32
Ambient conditions 32
Reporting problems and failures related to safety functions 32
Related standards and directives 33
Compliance with the European Machinery Directive 33

Further information

1

Safety instructions

Contents of this chapter

This chapter contains the safety instructions which you must obey when you install, operate and do maintenance on the unit and the safety circuit.

Use of warnings and notes

Warnings tell you about conditions which can cause injury or death, or damage to the equipment. They also tell you how to avoid danger. Notes draw attention to a particular condition or fact, or give information on a subject.

The manual uses these warning symbols:

WARNING!

Electricity warning tells about hazards from electricity which can cause injury or death, or damage to the equipment.

WARNING!

General warning tells about conditions, other than those caused by electricity, which can cause injury or death or damage to the equipment.

Safety instructions

Only a qualified electrician who has appropriate knowledge on functional/machine/process safety is allowed to install, start up and maintain the safety circuit. All user-made changes are on the user's responsibility.

WARNING!

After you have made additions to the safety circuit or modified it (e.g. replaced a component), always test the operation of the safety circuit according to its acceptance test procedure.

WARNING!

Read and obey all safety instructions given for the unit. 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 unit 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 guide 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)
- Emergency stop, stop category 0 with push button monitoring (option +Q951+Q984).

Target audience

The manual is intended for people who install, start up, use and service the safety option. Read the manual before working on the unit. 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 appropriate safety function manual.	☐
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 the safety function manual and the circuit diagrams delivered with the drive.	☐
Set the parameters. See the safety function manual.	☐
Validate that the implemented system meets the safety requirements: Do the acceptance test. See the safety function manual.	☐
Write the necessary documentation.	☐

Terms and abbreviations

Term	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 (+Q951+Q984) for ACS880-07CLC drives user's manual	3AXD50000207848
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

Description and instructions for option +Q951

Contents of this chapter

This chapter describes the safety function and instructs how to wire, start up, test, validate and use it.

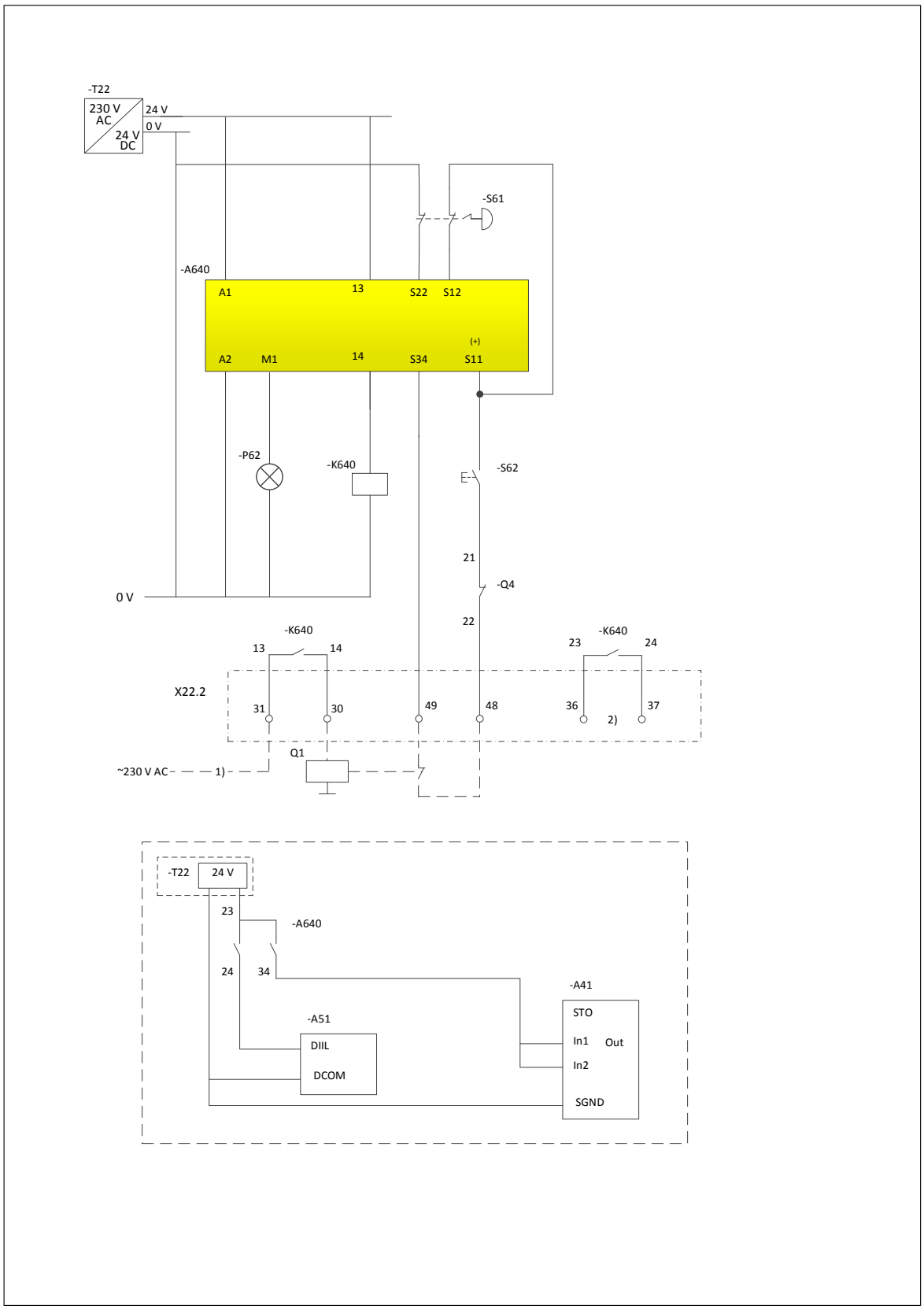
Overview

This emergency stop function corresponds to an uncontrolled stop in accordance with stop category 0 (EN/IEC 60204-1). After the drive receives the emergency stop command, it activates the Safe Torque Off function and trips the main contactor which cuts off the input power of the drive. The motor coasts to a stop.

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

For a list of related standards and European directives, see section *Related standards and directives (page 33)*.

Operation principle



ID	Description	ID	Description
A640	Safety relay	S61	Emergency stop button
S62	Reset button	P62	Reset pilot light
K640	Auxiliary safety relay	A51	Supply control unit
A41	Inverter control unit	Q4	Charging contactor
Q1	Main contactor or breaker	X22.2	Terminal block (eg, for user connections)
1)	Main contactor control circuit. For details, see delivery-specific circuit diagrams.	2)	Emergency stop indication for user-defined use

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

Step	Operation
1.	The user activates emergency stop by pushing the emergency stop button [S61]. Safety relay [A640] receives the emergency stop command.
2.	The safety relay [A640] switches off the XSTO inputs IN1 and IN2 of the inverter control unit [A41]. The XSTO.OUT terminal opens the STO circuit of the inverter modules. This disables the inverter operation. The safety relay [A640] de-energizes the main contactor and the charging contactor [Q4] and activates the DIIL input on the supply control unit [A51]. The main contactor [Q1] opens and switches off the AC power supply to the drive.
3.	The emergency stop indication lamp [P62] switches on.
4.	The motor coasts to a stop and remains stopped while the emergency stop is active.
5.	Normal operation resumes after the user: • releases the emergency stop button [S61] to normal (up) position • resets the emergency stop circuit (reset button [S62]). • resets the inverter unit with a control panel (if the STO indication parameter *31.22* has been set to cause a fault trip). 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 the drive if it detects a failure (short circuit between signals, open circuits, redundancy fault when the emergency stop button is pushed) in the primary safety circuit (i.e. emergency stop button [S61] and the contacts wired to it). The fault reaction function shifts the drive immediately into the safe state by switching on the emergency stop command, opening the main contactor/breaker [Q1], and keeping this state on until the detected fault has been fixed and the emergency stop function has been reset. The indication lamp of the reset button [P62] is on until the fault has been fixed and the user has pushed the reset button [S62].

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 is wired to the manual reset mode at the factory. Do not change the wiring.

Wiring

One emergency stop button is installed on the cabinet door and wired to the safety relay [A640] at the factory. No user connections are needed or allowed. Also, the user may not install any additional emergency stop buttons.

The user must wire the main contactor/breaker control circuit [X22.2:30…31]… and the main contactor/breaker feedback circuit [X22.2:48…49].

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.

Note: The safety system and user-made wirings are on the user'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 [S61], reset circuit, STO circuits and connections to the main contactor/breaker [Q1].	☐
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 run and stop 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 [S61].	☐
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 [P62] switches on.	☐
Make sure that you cannot switch the power on with the operating switch, or by any other possible means.	☐
Make sure that you cannot start the drive and motor from any control location: the motor does not start when you switch the external drive start signal off and on or change the control panel (or Drive composer) to local control mode (Loc key) and try to start by the panel start key. Restore the default control location (local or remote) after the test.	☐
Turn the emergency stop button [S61] until it releases and returns to the up position.	☐
Reset the emergency stop circuit [S62].	☐
Make sure that the indication lamp [P62] switches off.	☐
If you configured the emergency stop command to cause a fault trip, reset the related fault message with a control panel.	
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.	☐
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 [S61]. The emergency stop activates and the button locks in “ON” (open) position.

Resetting

1. Turn the emergency stop button [S61] until it releases.
2. Reset the emergency stop circuit from the reset button [S62].
   The indication lamp [P62] switches off. The emergency stop function deactivates.
3. Reset the drive if necessary.
4. Close the main contactor/breaker [Q1] with the operating switch if necessary (see the hardware and firmware manuals).
   The main contactor/breaker [Q1] closes and the drive is powered up.
5. You can now restart the drive.
6. Make sure that the drive has received the start signal (depends on the configuration, see the firmware manual).

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

Emergency stop indications

When the parameter settings has been set according to section Parameter settings and 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 [P62] on the cabinet door is illuminated.

Fault tracing

The emergency stop safety relay type is Phoenix Contact PSR-MC34 [A640]. For the error indications of the relay, see the data sheet of the relay (www.phoenixcontact.com).

This table describes the general states of the safety relay LEDs during its normal operation. The same LEDs also indicate errors.

PWR LED	IN1/2 LED	K1 LED	K2 LED	State
ON	OFF	OFF	OFF	All internal relays are not activated. The sensor circuit is off. Possible error.
ON	ON	OFF	OFF	The sensor circuit is active. Relays K1 and K2 are ready to start and await reset/start command [S34].
ON	ON	ON	ON	The sensor circuit is active. All relays are picked up.

4

Description and instructions for option +Q951+Q984

Contents of this chapter

This chapter describes the safety function and instructs how to wire, start up, test, validate and use it.

Overview

The emergency stop function corresponds to an uncontrolled stop in accordance with stop category 0 (EN/IEC 60204-1). After the drive receives the emergency stop command, it activates the Safe Torque Off function, and trips the main contactor/breaker which cuts off the input power of the drive. The motor coasts to a stop.

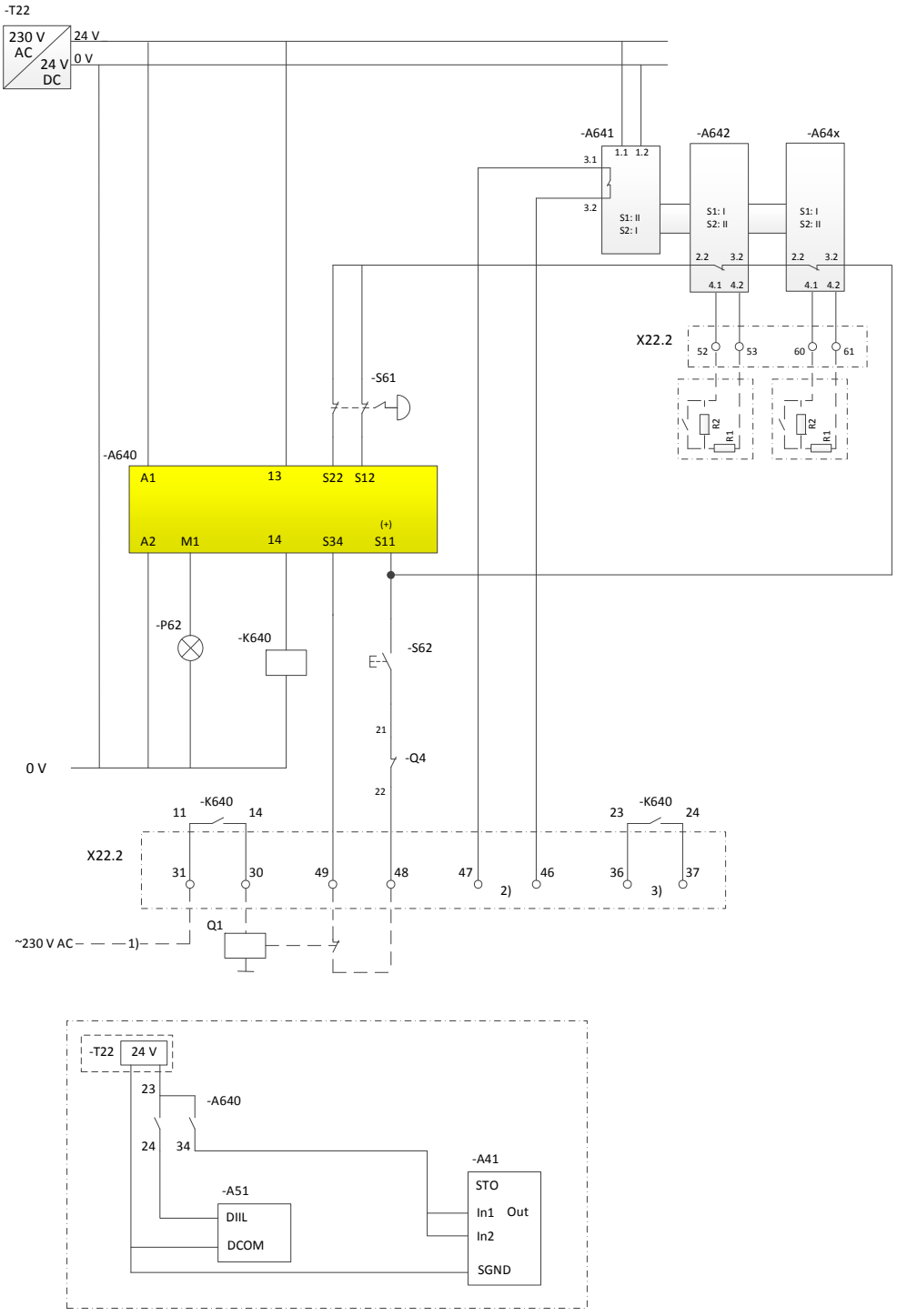
The design principles of the safety function comply with EN ISO 13850.

For a list of related standards and European directives, see section *Related standards and directives (page 33)*.

The user can install additional push buttons to the system. The system monitors the status of each button individually and triggers the emergency stop when any button is pushed. The system also detects possible line faults in any individual button circuit. If there is a short circuit or a broken wire, the system indicates it via a normally-closed relay contact. However these errors do not trigger the emergency stop or trip the drive.

Note: The related standards apply only to emergency stop, stop category 0 (+Q951) emergency stop button. Push button monitoring (+Q984) push buttons are marine emergency stops.

Operation principle



ID	Description	ID	Description
A640	Safety relay	S61	Emergency stop button
S62	Reset button	P62	Reset pilot light
K640	Auxiliary safety relay	A51	Supply control unit
A41	Inverter control unit	Q4	Charging contactor
Q1	Main contactor or breaker	A641	Push button monitoring relay
A642...A646	Push button safety relays (2 to 5 relays)	X22.2	Terminal block (eg, for user connections)
1)	Main contactor/breaker control circuit	2)	Push button monitoring and fault indication (for user-defined use)
3)	Emergency stop indication for user-defined use	R1, R2	Push button resistors
S1, S2	DIP switches		

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

Step	Operation
1.	The user activates emergency stop, for example, by pushing the emergency stop button [S61].
2.	The safety relay [A640] switches off the XSTO inputs IN1 and IN2 of the inverter control unit [A41]. The XSTO.OUT terminal opens the STO circuit of the inverter modules. This disables the inverter operation. The safety relay [A640] de-energizes the main contactor and the charging contactor [Q4] and activates the DIIL input on the supply control unit [A51]. The main contactor [Q1] opens and switches off the AC power supply to the drive.
3.	The emergency stop indication lamp [P62] switches on.
4.	The motor coasts to a stop and remains stopped while the emergency stop is active.
5.	Normal operation resumes after the user: • releases the emergency stop button [S61] or the user-defined button to normal (up) position • resets the emergency stop circuit [S62] • resets the inverter unit with a control panel (if the STO indication parameter *31.22* has been set to cause fault trip). If the drive is used in remote control mode, see the firmware manual for more information.
6.	If there is a wiring fault in any individual push button circuit, the fault will trigger a fault signal [X22.2:46, X22.2:47].

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 the drive if it detects a failure (short circuit between signals, open circuits, redundancy fault when the emergency stop button is pushed) in the primary safety circuit (i.e. emergency stop button [S61] and the contacts wired to it). The fault reaction function shifts the drive immediately into the safe state by switching on the emergency stop command, opening the main contactor/breaker [Q1], and keeping this state on until the detected fault has been fixed and the emergency stop function has been reset. The indication lamp of the reset button [P62] is on until the fault has been fixed and the user has pushed the reset button [S62].

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.

Note: A line fault in the push button monitoring circuit does not cause a fault reaction function.

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 is wired to the manual reset mode at the factory. Do not change the wiring.

The DIP switches [S1…S4] of the push button monitoring relay [A641…A646] have been preset at the factory as follows:

DIP switch	S1	S2	S3	S4
K641	II	I	-	-
K642…K646	I	II	I	I

Wiring

One emergency stop button [S61] and a reset button [S62] with an indication LED [P62] are installed on the cabinet door and wired at the factory.

There is a one-channel contact between the button and the emergency stop safety relay. The safety relay detects 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.

The user must install...

- push buttons with resistors [X22.2:52...61].
- wiring for the push button fault indication [X22.2:46...47].
- main contactor/breaker control circuit [X22.2:30...31].
- main contactor/breaker feedback circuit [X22.2:48...49].

Values for the push button resistors [R1, R2] are:

Resistor	Value [ohm]
R1	1000
R2	10000

Note: The safety system and user-made wirings are on the user's responsibility.

Start-up and acceptance test

Emergency stop button

Do the acceptance test as described in *Start-up and acceptance test (page 17)*.

Push button monitoring

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 and section *Wiring (page 23)*: the push buttons, reset circuit, STO circuits, and connections to the main contactor/breaker [Q1].	☐
Check that the hardware settings relevant to the safety functions are set as defined in section *Hardware settings (page 22)*.	☐
Settings with voltage connected	
Check that the parameters relevant to the safety functions are set as defined in section *Parameter settings (page 16)*.	☐
Acceptance test	
Make sure that you can run and stop 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 a push button.	☐
Make sure that the drive stops the motor by coasting and displays the correct warnings. See section *Emergency stop indications (page 18)*.	☐
Make sure that the indication lamp [P62] switches on.	☐
Make sure that you cannot switch the power on with the operating switch on the cabinet door, or by any other possible means.	☐
Make sure that you cannot start the drive and motor from any control location: The motor does not start when you switch the external drive start signal off and on or push the start key of the panel.	☐
Turn the emergency stop button [S61] until it releases and returns to the up position.	☐
Reset the emergency stop circuit [S61].	☐
Make sure that the indication lamp [P62] 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.	☐
WARNING! Do not exceed the maximum number of drive power-ups which is five in ten minutes. Too frequent power-ups can damage the charging circuit for the safety circuits.	
Repeat the test from each operating location (every push 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 [S61]. The emergency stop activates and the button locks in “ON” (open) position.

Resetting

1. Turn the emergency stop button [S61] until it releases.
2. Reset the emergency stop circuit from the reset button [S62].
   The indication lamp [P62] switches off. The emergency stop function deactivates.
3. Reset the drive if necessary.
4. Close the main contactor/breaker [Q1] with the operating switch if necessary (see the hardware and firmware manuals).
   The main contactor/breaker [Q1] closes and the drive is powered up.
5. You can now restart the drive.
6. Make sure that the drive has received the start signal (depends on the configuration, see the firmware manual).

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

Emergency stop indications

When the parameter settings has been set according to section Parameter settings and 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 [P62] on the cabinet door is illuminated.

Fault tracing

The emergency stop safety relay type is Phoenix Contact PSR-MC34 [A640]. For the error indications of the relay, see the data sheet of the relay (www.phoenixcontact.com).

This table describes the general states of the safety relay LEDs during its normal operation. The same LEDs also indicate errors.

PWR LED	IN1/2 LED	K1 LED	K2 LED	State
ON	OFF	OFF	OFF	All internal relays are not activated. The sensor circuit is off. Possible error.
ON	ON	OFF	OFF	The sensor circuit is active. Relays K1 and K2 are ready to start and await reset/start command [S34].
ON	ON	ON	ON	The sensor circuit is active. All relays are picked up.

The LED status indications of the Phoenix Contact MCR-SL-NAM-R-SP [A642...A646] module are: supply voltage (green), switching state (yellow) and line fault (red).

5

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 the acceptance test described in section Start-up and acceptance test.

If you change any component or wiring 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 acceptance 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.

For proof test intervals for safety functions without SIL classification, see ship's maintenance schedule and main contactor's instructions. For SIL classifications, see section Safety data.

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 the whole unit, make sure that the safety of the machine is maintained until the decommissioning is complete.

6

Technical data

Contents of this chapter

This chapter contains the technical specifications of the option, for example, safety data values, safety block diagram, general rules and related standards and directives.

Safety data

The safety data given is valid for the emergency stop function (+Q951) safety circuit in:

- Emergency stop, stop category 0, with safety relays (option +Q951)
- Emergency stop, stop category 0, with push button monitoring (option +Q951+Q984).

This data is not valid for marine emergency stops (+Q984). In case the final design differs from the default, ABB calculates new safety data and delivers it separately to the user.

Safety data values

The safety data calculations are based on the following assumptions on the operation of the user-controlled main contactors:

- 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.

Option code	Contactors	SIL / SILCL	PL	PFH [1/h] [1)]	PFD_{avg}	DC [%] [2)]	SC	Cat.	HFT	CCF	Life time [a]	T1 [3) 4)] [a]
+Q951	- [5)]	2	d	5.02E-7	7.7E-4	>90	3	2	0	65	20	20 / 1 [6)]
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.
5) ACS880-07CLC does not include contactors. Contactors are assembled and installed by the user and will affect safety values.
6) 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.

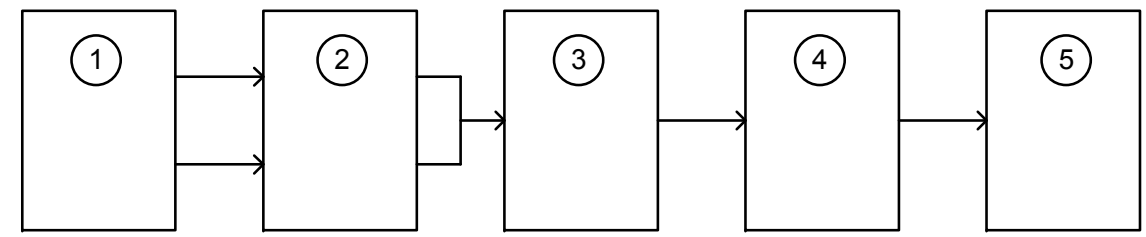
Safety component types

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
- 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

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 environmental limits, see the hardware manual.

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 IEC 60204-1:2016	Safety of machinery – Electrical equipment of machines – Part 1: General requirements
IEC 61508 Parts 1-2, Ed. 2.0:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61800-5-2:2016 EN 61800-5-2:2007	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional
IEC 62061:2015 Ed. 1.2 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 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.

Contact us

www.abb.com/drives

3AXD50000207848 Rev A (EN) EFFECTIVE 2018-02-23

3AXD50000207848A

Power and productivity
for a better world™