Options for ABB drives

Original user's manual
Prevention of unexpected start-up (option +Q957) for DCS8x0-A enclosed converters equipped with DCS880 modules

POUS option

	E-Stop cat.0	E-Stop cat.1	POUS	forced MC opening
+Q951	x			x
+Q952		x		x
+Q963	x			
+Q964		x		
+Q957			x	

List of related manuals

General	Publication number	EN	DE	IT	ES	FR	PL	ZH	RU
DCS880 Quick guide	3ADW000545	EN	DE	IT	ES	FR			
Safety instructions all languages	3ADW000481	EN	DE	IT	ES	FR	PL	ZH	RU
DCS880 Manual set	-	EN							
DCS880 Units									
DCS880 Flyer	3ADW000475	EN	DE	IT	ES	FR		ZH	RU
DCS880 Technical catalog	3ADW000465	EN	DE	IT	ES	FR	PL	ZH	RU
DCS880 Hardware manual	3ADW000462	EN	DE	IT	ES	FR	PL		RU
DCS880 Firmware manual	3ADW000474	EN	DE	IT	ES	FR	PL		RU
DCS880 Service manual	3ADW000488	EN							
DCS880 Hardparallel manual (on request only)	3ADW000530	EN							
DCS880 12-pulse manual	3ADW000533	EN							
DCS880 Current measurement aid (SDCS-CMA-2) manual	3ADW000745	EN							
ACS-AP-x assistant control panels user's manual	3AUA0000085685	EN							
DCS Thyristor power converter – Technical guide	3ADW000163	EN							
Functional safety									
Supplement for functional safety	3ADW000452	EN		IT	ES	FR	PL		RU
FSPS-21 PROFIsafe safety functions module	3AXD50000158638	EN							
FSO-21 Safety functions module	3AXD50000015614	EN							
Functional safety for enclosed converter									
+Q957 Prevention of unexpected Start Up	3ADW000504	EN							
+Q951 Emergency stop, category 0 with MC opening	3ADW000505	EN							
+Q952 Emergency stop, category 1 with MC opening	3ADW000506	EN							
+Q963 Emergency stop, category 0 without MC opening	3ADW000507	EN							
+Q964 Emergency stop, category 1 without MC opening	3ADW000508	EN							
Enclosed converter									
DCS880-A Catalog	3ADW000531	EN							
DCS880-A Installation manual	3ADW000627	EN							
DCS800-A +S880 Enclosed converters, flyer	3ADW000523	EN							
Rebuild and upgrade systems									
DCS880-R Rebuild manual	3ADW000599	EN							
DCS880-U Upgrade manual	3ADW000719	EN							
Door mounting kits									
DPMP-01 mounting platform for ACS-AP control panel	3AUA0000100140	EN							
DPMP-02 mounting platform for ACS-AP control panel	3AUA0000136205	EN							
Serial communication									
FCAN-01 CANopen adapter module	3AFE68615500	EN	DE						
FDNA-01 DeviceNet™ adapter module	3AFE68573360	EN							
FECA-01 EtherCAT adapter module	3AUA0000068940	EN	DE		ES				
FENA-11/-21 Ethernet adapter module	3AUA0000093568	EN						ZH	
FEPL-02 Ethernet POWERLINK adapter module	3AUA0000123527	EN	DE						
FPBA-01 PROFIBUS DP adapter module	3AFE68573271	EN	DE				PL	ZH	
FSCA-01 RS-485 adapter module	3AUA0000109533	EN						ZH	
FDCO-01/02 DDCS communication modules	3AUA0000114058	EN							
FPNO-21 PROFINET fieldbus adapter module	3AXD50000158614	EN							
Tool and maintenance manuals and guides									
Drive Composer PC tool	3AUA0000094606	EN							
Drive application programming (IEC61131-3) manual	3AUA0000127808	EN							
Adaptive programming, Application guide	3AXD50000028574	EN							
NETA-21 remote monitoring tool	3AUA0000096939	EN							
NETA-21 remote monitoring tool guide	3AUA0000096881	EN							
DDCS branching unit NDBU-95 user's manual	3BFE64285513	EN							
Extension modules									
FIO-11 Analog extension module	3AFE68784930	EN	DE	IT					
FIO-01 Digital extension module	3AFE68784921	EN	DE	IT					
FAIO-01 Analog extension module	3AUA0000124968	EN	DE						
FDIO-01 Digital extension module	3AUA0000124966	EN							
FEN-01 TTL encoder interface	3AFE68784603	EN	DE	IT				ZH	
FEN-31 HTL encoder interface	3AUA0000031044	EN						ZH	
FSE-31 pulse encoder interface module user's manual	3AXD50000016597	EN							
FEA-03 F series extension adapter	3AUA0000115811	EN							
Ethernet tool network for ACS880 drives appl. guide	3AUA0000125635	EN							

Table of contents

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.

WARNING!
This safety function does not disconnect the voltage of the main and auxiliary circuits from the drive. You must not work on the electrical parts of the drive or the motor before you have also disconnected the drive system from the electric supply and ensured by measuring that there is no dangerous voltage present.

WARNING!
After making additions to the drive safety circuit or modifying it, or changing circuit boards inside the drive, always test the functioning of the safety circuit according to the acceptance test procedure. Any changes in the electrical installations of the drive may affect the safety performance or operation of the drive 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.

Introduction to the manual

Contents of this chapter

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

Applicability

The manual applies only to DCS880-A cabinet drives and to DCS800-A cabinet drives with option +S880 (exchange of DCS800 with DCS880 drives modules) which have the option: +Q957: Prevention of unexpected start-up (POUS). It also applies to group drives with this option. To achieve POUS for a group of drives, the plus code is added to the incomer cabinet / empty cabinet, which contains the safety circuit. This option is realized with safety relays.

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.

Contents

The chapters of this manual are briefly described below.
Introduction to the manual (this chapter) introduces this manual.
Option description and instructions describes the safety option and instructs how to wire, start-up, test, validate, use and maintain it. The chapter also contains the safety data.

Related documents

- Product manuals (see the inside of the front cover)
- Circuit diagrams delivered with the drive
- Safety data (if the safety circuit is application engineered)

Abbreviations

Abbreviations used in this manual are listed below.

Abbreviation	Description	Reference
Cat.	Category 1. Stop category according to EN/IEC 60204-1 The stop categories are: 0 (uncontrolled stop) and 1 (controlled stop) 2. 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/IEC 60204-1 EN ISO 13849-1
CCF	Common cause failure (%)	EN ISO 13849-1
DC	Diagnostic coverage	EN ISO 13849-1
DI	Digital input	
E-stop	Emergency stop	
Frame (size)	Relates to the construction type of the drive in question. For example, several drive types with different power ratings can have the same basic construction, and a frame size is used in reference to all those drive types.	
HFT	Hardware fault tolerance	IEC 61508, EN/IEC 62061
PFH	Probability of dangerous failures per hour	IEC 61508, EN ISO 13849-1, EN/IEC 62061, EN/IEC 61800-5-2
PL	Performance level (levels are: a, b, c, d and e). Corresponds to SIL.	EN ISO 13849-1
POUS	Prevention of unexpected start-up	EN ISO 14118: 2018
RO	Relay output	
SC	Systematic capability	IEC 61508
SIL	Safety integrity level	IEC 61508, IEC 61511, EN/IEC 62061, EN/IEC 61800-5-2
SILCL	Maximum SIL that can be claimed for a safety function or subsystem	EN/IEC 62061
SS1	Safe stop 1	EN/IEC 61800-5-2
STO	Safe torque off	EN/IEC 61800-5-2
T1	Proof test interval or lifetime (the smaller one)	IEC 61508, EN/IEC 62061

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.
☐	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 chapter Option description and instructions on page 9.
☐	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 Customer wiring on page 15.
☐	Set the parameters. See section Parameter settings on page 14.
☐	Validate that the implemented system meets the safety requirements: – Do the acceptance test. See section Start-up and acceptance test on page 16.
☐	Write the necessary documentation.

Option description and instructions

Contents this chapter

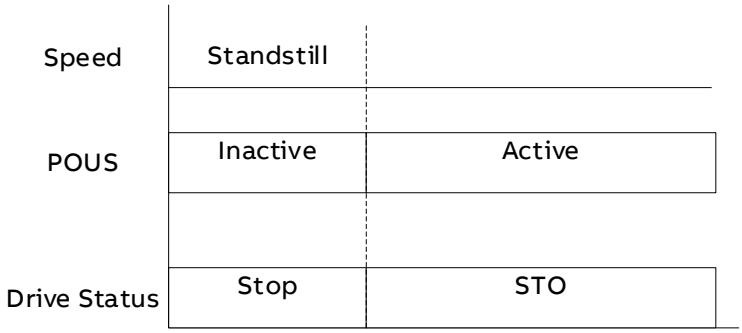
This chapter describes the +Q957 Prevention of unexpected start-up option and instructs how to wire, start-up, test, validate, use and maintain it.

Overview

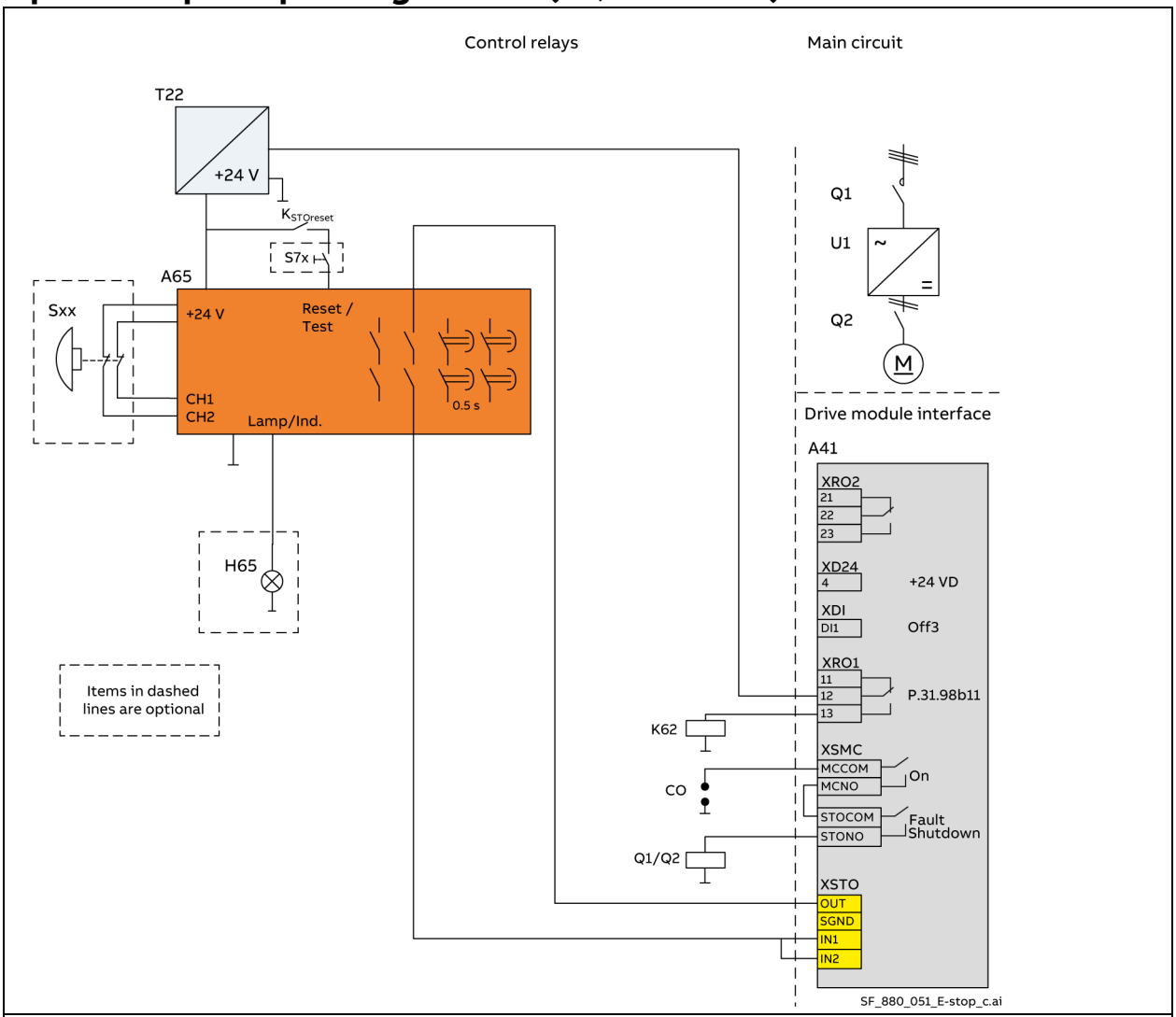
The Prevention of unexpected start -up (POUS) function disables the drive(s) output stage by utilizing the STO function.
This prevents the drive(s) from generating the torque required to rotate the motor(s). The POUS function activates the Safe torque off (STO) function of the drive(s). By using this function, short-time operations (such as cleaning, loading or unloading) or maintenance work on the non-electrical parts of the machinery can be performed without switching off and disconnecting the drive.
The user activates the Prevention of unexpected start-up function using a (key) switch mounted on a control desk. When the switch is open (off), the POUS function is active and the POUS indication lamp is on.
The customer is responsible for installing and connecting the operating switch on site. It can be included in the delivery as an option. See the machine-specific C-type standards whether an indication lamp is required.
For a detailed description of the Safe torque off function, see the appropriate hardware manual
The design principles of the option +Q957 comply with EN ISO 14118: 2018.
The STO function complies with EN/IEC 61800-5-2:2007.
For a complete list of related standards and European directives, see section Related standards and directives on page 23.

Warning: Drives with the Emergency stop, stop category 1 function (option +Q952 or +Q964): If the user activates the POUS function during the emergency stop deceleration ramp, it overrides the emergency stop function. This activates the STO function the drive(s) immediately and each motor coasts to a stop. This normally means, that the machine cannot be stopped sufficiently fast. For more information on the emergency stop function, see the appropriate user's manual.

Basic timing diagram



Operation principle Single Drive (+Q957 POUS)



A41	Drive Control board	H65	POUS indication lamp
A65	POUS safety relay	S7x	POUS reset button (for manual reset)
Sxx	POUS (key) switch / button	Q1/Q2	Mains breaker / DC breaker
T22	24 V power supply	K62	Reset indication for safety relay
U1	DCS880 converter	XSMC:MC	Relay opens at any drive fault
CO	24 V from T22 or functional control from any source	XSMC:STO	Relay for fault reaction function

Note: The DCDS880-A cabinet-internal wiring is done with single wires, (see chapter Single wiring inside cabinets (fault exclusion)).

Operation sequence

Initial status: The drive is in operation and the motor is at a standstill.

Step	Operation
1.	The user activates Prevention of unexpected start-up by switching off the POUS (key) switch [Sxx].
2.	The POUS safety relay [A65] trips and the relay switches off the Safe torque off (STO) control signals on the drive control board(s) [A41]. The STO cuts off the drive control pulses preventing motor control and generation of torque.
3.	The aux. contact of safety relay [A65] energizes the indication lamp [P7x].
4.	The motor does not (motors do not) generate torque and remain(s) at zero speed while the POUS is active.
5.	Normal operation resumes after the user: – releases the POUS switch [Sxx] to normal (up) position – resets the POUS circuit with the POUS reset button [S7x] (if installed; the user must push the reset button for 0.1 to 3 seconds) – resets the drive(s) (if the STO indication parameter 31.22 has been set so that a fault is generated) – makes sure that the (group) drive has received the start signal (depends on the configuration, see the firmware manual).

Group drive safety: Information and operation principle

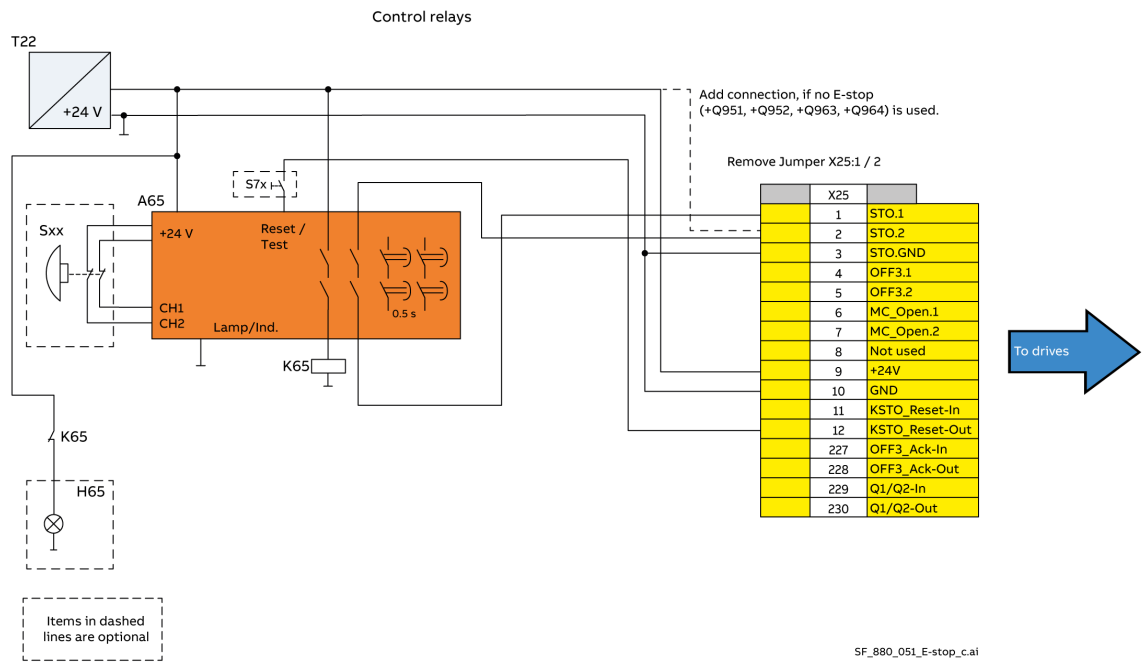
DCS880-A cabinet drives are structured in line-ups. Functional safety group drives behave like single drives with regard to functional safety.

If more than one drive can pose a danger at a specific place according to functional safety standards, a functional safety group drive is required. It behaves like a single drive with regards to functional safety. This means that a (ramp) stop command (+Q951, +Q952, +Q963, +Q964) or POUS command (+Q957) is valid for all drives at once. Examples of functional safety group drives are drives working on the same roll / shaft, such as a master follower drive. For more information on possible safety configurations, please refer to the DCS880-A catalog. The POUS function can be implemented for each individual drive (individual POUS) or for the whole group (group POUS).

For individual POUS, option +Q957 needs to be added to each drive. The operation sequence (see section above) is identical to that of a single drive with the POUS option.

For group POUS, option +Q957 needs to be added only to the incomer cabinet or empty cabinet. The operation sequence is similar to that of a single drive with the POUS option. However, for transmitting the signals to more than one drive, a safety bus is used. It consists of multiple X25 terminals with wired connections. For each drive, plus code +S925 is required. The safety relays of the safety option provide the required signals such as STO, ramp start (Off3) and open MC command to the safety bus. Also, diagnostic information is returned to the safety relays using the safety bus, such as the STO reset indication and Off3 acknowledge.

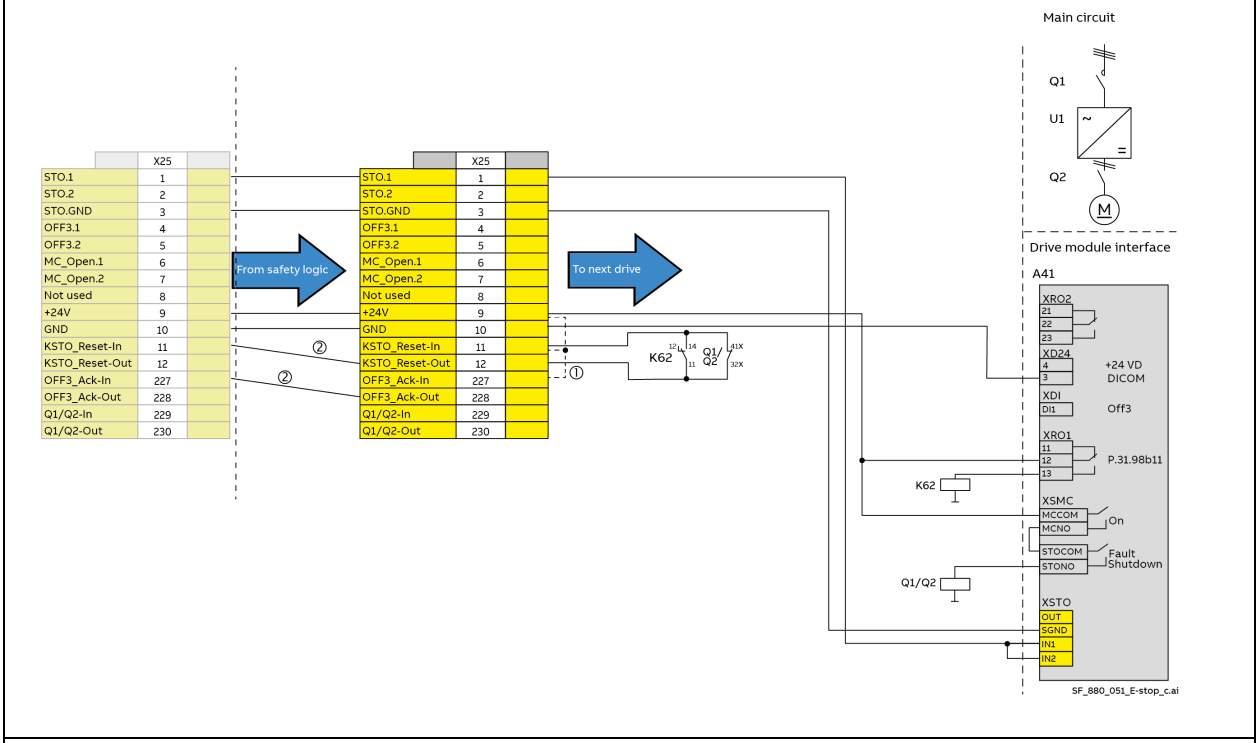
Connection to safety bus X25 (Q957)



		K65	Relay for indication lamp
A65	POUS safety relay	H65	POUS indication lamp
Sxx	POUS (key) switch / button	S7x	POUS reset button (for manual reset)
T22	24 V power supply	X25	Safety bus terminal

Note: If the cabinets of the drives of a group are not physically connected with each other, the electrical drawing of the safety bus is more complex. For this so-called line-up split, the extra plus codes +S926 safety transmitter and +S927 safety receiver are needed. The safety transmitter can connect one safety group via two channel field wiring to one or two safety receivers. Please see circuit diagrams delivered with the drive for reference.

Connection of safety bus X25 to drives (Q957)



A41	Drive Control board	K62	Reset indication for safety relay
U1	DCS880 converter	Q1/Q2	Mains breaker / DC breaker
X25	Safety bus terminal	XSMC:MC	Relay opens at any drive fault
①	Bus termination (in last drive only)	XSMC:STO	Relay for fault reaction function
②	drive feedback signals daisy chain		

Each individual drive in a group is connected in the same way to the safety bus:
The safety bus X25 provides these signals to all drives and collects the feedback signals from these drives (daisy chain structure). The interconnections of these terminals are created according to the grouping in document 3ADT077036 Safety function configuration for group drives protected, which has to be filled in as a part of the project specification for all safety groups.

+Q957 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 POUS safety relay [A65] trips if it detects a failure (short circuit between signals, open circuits, redundancy fault) in the safety circuit. The fault reaction function shifts the drive immediately into the safe state by activating the STO function. The STO function is active until the fault is repaired. The POUS indication lamp is on until the fault is repaired.

The STO function has its own internal fault diagnostics and fault reaction function (see Supplement for functional safety).

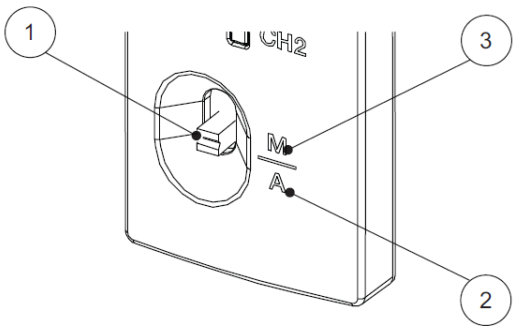
Parameter settings

This table lists the drive parameters settings for the +Q957 option. For more information, see the firmware manual.

No.	Name	Value	Description
10.24	RO1 source	31.98.b11 STO Reset indication	Selects a drive signal to be connected to relay output RO1. In this case, the RO1 is energized if the Drive is in STO state and no STO related fault is active.
31.22	STO indication run / stop	3: Fault / Warning	Selects which indications are given when the Safe torque off (STO) signals are switched off, depending on whether the drive is Running / Stopped, when they occur. When a fault occurs in the drive, the mains contactor AC-B or DC-B is opened by the XSMC-MC relay. Fault/Warning is the recommended setting. Use Warning / Warning if E-Stop, stop category 0 (+Q951 or +Q963) is used.

Hardware settings

Appropriate hardware settings have been preset at the factory for the safety function.
The hardware reset of the safety relay A65 [SSR32] is preset to automatic (Dip Switch).

Use the switch (1) to change settings between automatic reset (2) and manual reset (3). Power cycle (power off and on) the safety relay when a setting has been changed.	

To change the reset behavior to manual, follow the instructions (see electrical drawings):

1. Connect POUS reset button.
2. Remove jumper between -X971:2 and -X971:3
3. Change safety relay switch position on -A65 from [x]A to [x]M

Customer wiring

One POUS (key) switch and one reset button (for manual reset only) need to be installed and wired to the drive at the factory. There must be double contacts in the POUS switch and double wiring (two-channel connection) between the button and the POUS safety relay [A65]. The safety relay detects cross faults and faults across one contact from the POUS (key) switch.

If needed, install additional POUS (key) switches on site and wire them to the appropriate terminal block inside the drive cabinet. See the circuit diagrams delivered with the drive. Follow the rules below:

1. Use only double-contact buttons approved for the POUS circuits.
2. Connect the POUS (key) switches 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 POUS safety relay trips and activates the POUS command of the drive as it detects a redundancy fault.

3. Use shielded, twisted pair cable. We recommend a double-shielded cable and gold-plated contacts in the POUS (key) switch.
4. Ensure that the sum resistance for one channel (loop resistance) does not exceed 850 Ω and that the used cable does not exceed a capacity of 100 nF to ground. If very long cables are required, see chapter Long cables for POUS loop.
5. Follow the general control cable installation instructions given in the drive hardware manual.

You can also install additional reset buttons and indication lamps for the POUS circuit on site. We recommend gold-plated contacts in the reset button. Wire the buttons to the appropriate terminal block inside the drive cabinet. See the circuit diagrams delivered with the drive.
Follow the rules below:

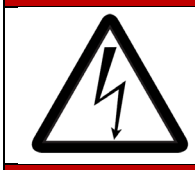
1. Sum resistance of the external reset circuit may not exceed 800 Ω.
2. Follow the general control cable installation instructions given in the drive hardware manual.

+Q957 Start-up and acceptance test checklist

This acceptance test has to be done as part of the testing procedure whenever an STO function is in use. It is valid for functional safety single drives and functional safety group drives. You need the Drive composer PC tool or a control panel to perform the start-up and acceptance test.

For group drives, this test must be done for each group. The assignment of the drives to each group can be found in document 3ADT077036 Safety function configuration for group drives protected. This document must be signed together with the test.
See also document 3ADP078580 (on request) with further test instructions for transport splits and line-up splits (applicable to group drives with plus codes +S926 and +S927).

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! Follow the Safety instructions, page 5. Otherwise, serious injury, death, or damage to the equipment can occur.	
Checks and settings with no voltage connected	
If any connections of the POUS circuit have been changed on site (such as wiring of additional POUS switches, connection of shipping splits of large drives, etc.), verify that the connections are correct with the appropriate circuit diagrams.	☐
Check that the hardware setting relevant to the safety function are set as defined in section Hardware settings on page 15.	☐ M ☐ A
Settings with voltage connected	
Check that the parameters of the drive(s) relevant to the safety function are set as defined in section Parameter settings on page 14.	☐
Ensure that the motor(s) can run and be stopped freely during the test.	☐
Close the main contactor and switch on the power. The POUS function should be activated only when the motor is stopped.	☐
Activate the POUS function by turning off the POUS switch.	☐
Ensure that each drive indicates POUS as defined in section POUS indications on page 17.	☐ Event:
Ensure that the POUS indication lamp [H65] switches on.	☐
Ensure that you cannot start the (group) drive and motor from any control location: Switch the external start signal off and on (in the external control mode) and press the start key of the panel (in the local control mode).	☐
Deactivate the POUS function by switching on the POUS switch. Ensure that the drive does not restart directly after deactivation.	☐
Reset the POUS safety relay by pushing the POUS reset button [S7x] (if installed, not necessary for automatic reset).	☐
Ensure that the POUS indication lamp [H65] switches off.	☐
If there are drives that are part of the group but not in operation (switched off, e.g. via Q1, Q10, …), they must not affect the reset process described above.	
Switch off the (group) drive start signal. If a fault message is generated, reset the affected drive(s). See section Parameter settings on page 17.	☐
Restart the drive and motor and check that they operate normally.	☐
Repeat the test from each operating location (each POUS switch and reset button)	☐
Fill in and sign the acceptance test report which verifies that the safety function is safe and approved for operation.	☐

Use of the safety function

Activating

1. Lock the POUS key switch. The switch locks in “ON” (open) position.

Resetting

1. Unlock the POUS switch until it releases.
2. Push the POUS reset button [S7x] (if installed). The indication lamp [H65] goes out, the POUS deactivates.
   Note: You must push the reset button [S7x] for 0.1 to 3 seconds.
3. Reset the drive(s) if necessary.
4. Make sure that the drive has (drives have) received the start signal (depends on the configuration, see the firmware manual).
5. You can now restart the drive(s).

Note: You have to reset the POUS circuit with the reset button [S7x] also after you have powered up the drive, in case of manual reset.

Note for group drives: If one or more drive are switched off via mains contactor, AC-breaker or DC-breaker (see Q1/Q2 in chapter Group drive safety: Information and Operation principle), resetting the safety relay is possible. This allows to use the other drives of a group drive, even if a drive is faulted or under maintenance.

POUS indications

When the POUS is on:

- the drive control program has the warning Safe torque off active,
- the POUS indication lamp [H65] is illuminated,
- the mode LED of the safety relay [A65] is steady blue.

+Q957 Fault tracing

This table describes the status LEDs of the emergency stop safety relay A65 [SSR32].

CH1	Mode	CH2	Status	Action
off	off	off	The safety relay is not powered.	Check A1–A2 voltage and connections.
green	green	green	CH1 and CH2 accepted. Reset made and outputs activated.	
off	flash green	off	CH1 and CH2 unaccepted. A timer function is counting down while the safety relay remains activated.	
off	flash green	green	CH1 unaccepted and CH2 accepted. A timer function is counting down while the safety relay remains activated.	
green	flash green	off	CH1 accepted and CH2 unaccepted. A timer function is counting down while the safety relay remains activated.	
off	blue	off	No channels accepted.	Check CH1 and CH2
off	blue	green	CH1 unaccepted, CH2 accepted	Check CH1
green	blue	off	CH1 accepted, CH2 unaccepted	Check CH2
green	blue	green	CH1 and CH2 accepted, the safety relay waits for reset.	Check reset settings, wiring and reset/test circuit

green	blue	fast flash green	Two-channels error: CH2 has been unaccepted and then accepted again while CH1 remained accepted.	Check installation. Restore by opening and closing both CH:s at the same time.
fast flash green	blue	green	Two-channels error: CH1 has been unaccepted and then accepted again while CH2 remained accepted.	Check installation. Restore by opening and closing both CH:s at the same time.
fast flash green	blue	fast flash green	Reading error on R1 and R2.	Check installation. Restore by opening and closing both CH:s at the same time.
red	fast flash blue	red	Failsafe mode, a new setting has been stored.	Power cycle the unit to use the new setting.
red	flash red	red	Failsafe mode, the system is waiting for a new setting.	Change the timer setting switch.
red	fast flash red	red	The safety relay is in failsafe mode.	Check installation and power cycle.
red	fast flash red	fast flash red	Failsafe mode due to short circuit between CH2 and 24 VDC or T1	Check and remove the short circuit.
fast flash red	fast flash red	red	Failsafe mode due to short circuit between CH1 and 24 VDC or T2	Check and remove the short circuit.

For more information see 2TLC010002M0201.

+Q957 Maintenance

After the operation of the circuit is tested at start-up and it needs scheduled maintenance testing during its specified lifetime depending on its usage.

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.
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.
  Follow the rules given in section +Q957 Startup and acceptance test on page 16.
- 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 one year (high or low demand as defined in IEC 61508, EN/IEC 62061 and EN ISO 13849-1).

Diagnostic test interval

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 +Q957 Start-up and acceptance test on page 16.

The person responsible for the design of the complete safety function should also note the Requirements from IEC61800-5-2:2016 / EN61800-5-2:2017 for the drives STO circuit:

6.2.2.1.4: Diagnostic test interval when the hardware fault tolerance is greater than zero

The diagnostic test interval of any subsystem of the PDS (SR) shall be appropriate to meet the required PFH (see 6.2.2.1.1).

NOTE 2: For redundant parts of a PDS (SR) which cannot be tested without disrupting the application in which the PDS (SR) is used (machine or plant) and where no justifiable technical solution can be implemented, the following maximum diagnostic test intervals can be considered as acceptable:

- one test per year for SIL 2, PL d / category;
- one test per three months for SIL 3, PL e / category 3;
- one test per day for SIL 3, PL e / category 4 (not applicable).

PL and category according to ISO 13849-1.

The noted DC Values are taken from SS-EN ISO 13849-1:2016 (E) chapter 4.5.3.

Competence

The maintenance and proof test activities of the safety function must be carried out by a competent person with adequate 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 a POUS 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, it is obligation of the changing person to calculate new safety data and deliver it separately to the customer.

Safety data values

Drive module frame size	SIL① / SILCL	SC	PL①	PFH②[1/h]	DC [%]	Cat.	HFT	CCF	Lifetime [a]	T1③④ [a]
H1 … H8	3	3	e	4.8 E-8	>90	3	1	80	20	20/1
(Hard) parallel drive, Master-Follower	3	3	e	< 5.3E-8	>90	3	1	80	20	20/1

① The drive may be used for applications with the given SIL / PL only if the function is tested regularly (see chapter: test interval above).
② PFH values are according to EN ISO 13849. PFH assumes a standard POUS key switch with a lifetime of 500,000 operations, that is used 10 times per day. Differing from these assumptions can change the PFH value. The system integrator (or other responsible party) must redo the calculation, if the lifetime of the used E-Stop button is shorter, the button is used more often, additional drives and / or additional safety relays are added to the safety system.
③ See the recommendation of use CNB/M/11.050 published by the European coordination of notified bodies for lower T1 requirement and also IEC61800-5-2:2016 / EN61800-5-2:2017 6.2.2.1.4 Note 2 for guidance.
④ T1 = 20a is used with high demand mode of operation.
See also section Proof test interval on page 18.

Note for functional safety group drives: To calculate the total PFH value of a group, the PFH values of the drives (see safety supplement) excluding the first have to be added to the PFH value above.
PL e requires the PFH value to remain below 1.0E-7.
Including a safety margin, the following number of drives of any frame size can be in one group with performance level e:

Option+Q957: Possible number of drives with SIL 3 / Pl e

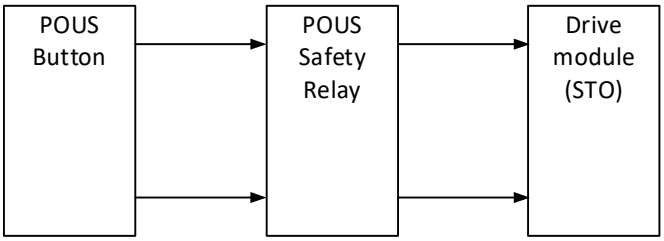
Single line-up	1 split	2 splits
30	27	20

Single line-up means that all drives are next to each other (no field wiring in between).
The splits refer to the so-called line-up split with 1 split (plus codes +S926 and +S927) and 2 splits (plus codes +S926 and twice +S927).

Safety component types

Safety component types as defined in IEC 61508-2:
- POUS (key) switch: type A
- safety relays: type A
- drive STO circuit:
- frame sizes H1 ... H8: type A

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



Relevant failure modes
Internal failures of safety relays, the POUS switch and STO. 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 inside the cabinet
- any short and open circuits in the cabinet terminal blocks of the safety circuits.

Operation delays
POUS total delay: max. 520 ms (measured from the time, when the input to the safety relay is 0 V)

Note: If plus code +S927 is used in the incomer (line-up-split), an additional response time of 40 ms has to be added.

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 on page 16:
- 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 adequate 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.

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 60204-1:2005 + A1:2008	Safety of machinery – Electrical equipment of machines – Part 1: General requirements
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety related systems - Part 1: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety related systems - Part 2: Requirements for electrical/electronic/ programmable electronic safety related systems.
EN 61800-5-2:2017 IEC 61800-5-2:2016	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional
EN 62061:2005 + AC:2010 + A1:2013 + A2:2015 IEC 62061:2015	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
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 ISO 13850:2015 ISO 13850:2015	Safety of machinery. Emergency stop. Principles for design
IEC 61511-1:2016	Functional safety – Safety instrumented systems for the process industry sector
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
2006/42/EC	European Machinery Directive
EN ISO 14118: 2018	Safety of machinery – Prevention of unexpected start-up
Other	Machine-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 (option +Q957) 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.

Appendix

Single wiring inside cabinets (fault exclusion)

The DCS880-A cabinet safety functions can achieve up to SIL 3 / Pl e.
- Functional safety customer interfaces are designed in double wiring.
- Functional safety devices work with dual channels (double contacts); examples are E-Stop buttons, safety relays and the DCS880 STO function.
- Functional safety relevant connections inside the cabinet are designed with single wires; for example, the connection from the safety relay (orange) to XSTO terminal (yellow), see picture in chapter Operation principle Single Drive (+Q957 POUS)).

Single wiring inside cabinets is permitted based on the following two standards (fault exclusion): According to IEC 62061, claiming Hardware Fault Tolerance (HFT) 1 does not require that two physical channels are needed, but depends on the safe failure fraction of the safety function subsystem (6.7.6). Possible faults are divided into safe and dangerous failures. The only dangerous failure for the STO circuit is a short circuit of a wire to 24 V. This 24 V short circuit is very unlikely, compared to other faults (such as broken cables or connectors or loss of 24 V supply), due to the fixed routing of “separate” isolated cables inside the cabinet.
Similarly, in ISO 13849, architectures 3 and 4 do not necessarily require two physical channels but a fault tolerance of 1. For dangerous failures (short circuit to 24 V) in wiring (and terminals), it is possible to claim a fault exclusion to achieve a fault tolerance of 1, if the requirements of ISO 13849-2 table D.4 (and table D.6) are fulfilled. That means for the wiring, that the cables are permanently fixed, protected against damage, with separate isolation and are located in an electrical enclosure.

Long cables for POUS loop

There are applications which require long cables and might have a higher capacity than 100 nF to ground for each channel, even with low-capacity cables (see chapter Customer wiring). The inputs A61: T1 /T2 are equipped with a test pulse function, which does not work with high-capacity cables, i.e. with long cables. In this case connecting the E-stop button without test pulses (terminal A1 instead of T1/T2)

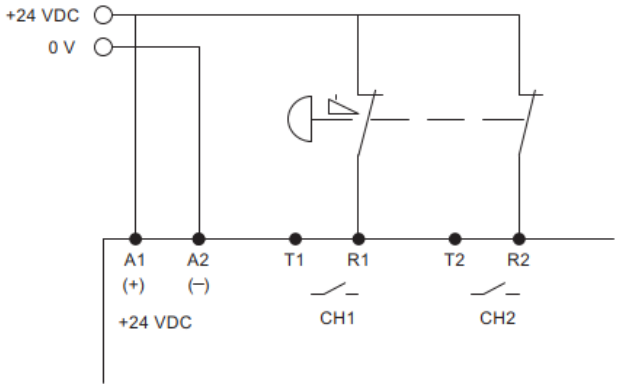


Figure 36: 2 channels connection with equivalent contacts, +24 VDC static signal

according to the picture below is possible.
This solution can achieve PL d level without fault exclusion, see configuration 2-channel sensor (equivalent) of AC500-S manual page 74 3ADR025091M0208 for reference.)

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

DCS Family

DCS550-S modules
The compact drive for machinery application

20 ... 1,000 A_{DC}
0 ... 610 V_{DC}
230 ... 525 V_{AC}
IP00

- Compact
- Robust design
- Adaptive and winder program
- High field exciter current

DCS880 modules
For safe productivity

20 ... 5,200 A_{DC}
0 ... 1,500 V_{DC}
230 ... 1,200 V_{AC}
IP00

- Safe torque off (STO) built in as standard
- Compact and robust
- Single drives, 20 A_{DC} to 5,200 A_{DC}, up to 1,500 V_{DC}
- IEC 61131 programmable
- Intuitive control panel and PC tool with USB connection and start up assistant
- Wide range of options to serve any DC motor application

DCS880-A enclosed converters
Complete drive solutions

20 ... 20,000 A_{DC}
0 ... 1,500 V_{DC}
230 ... 1,200 V_{AC}
IP21 – IP54

- Suitable for motoric and non motoric applications (e.g. electrolysis & hydrogen production)
- Individually adaptable to customer requirements
- User-defined accessories like external PLC or automation systems can be included
- High power solutions in 6- and 12-pulse up to 20,000 A_{DC}, 1,500 V_{DC}
- In accordance to usual standards
- Individually factory load tested
- Detailed documentation

DCT880 modules
Thyristor power controller

20 ... 4,200 A_{AC}
110 ... 990 V_{AC}
IP00

- Precise power control in industrial heating applications
- Two or three phase devices
- Power optimizer for peak load reduction
- Built on ABB's all-compatible drives architecture
- Intuitive control panel and PC tool with USB connection and start up assistant
- Application control programs and drive application programming with IEC 61131 programming

ABB AG
Wallstadter-Straße 59
68526 Ladenburg • Germany
Tel: +49 (0) 6203-71-0
Mail: dc-drives@de.abb.com
Web: www.abb.com/dc-drives

Ident. No.: 3ADW000504R0401 Rev D
02.2023

504R0401A3070000