ABB INDUSTRIAL DRIVES

ACS880 drives

Cyber security guide

ACS880 drives

Cyber security guide

Table of contents 

3AXD50001159429 Rev A
EN
Original instructions
EFFECTIVE: 2025-03-21

Table of contents

Further information

1

Introduction to the guide

Contents of this chapter

This chapter gives information on the guide.

Applicability

This guide applies to ACS880 drives.

This guide applies to the following versions of the ACS880 primary control program:

- ACS880 primary control program for UCU control units (loading package name YINLX, version 1.30 or later)
- ACS880 primary control program for BCU and ZCU control units (loading package name AINLX, version 3.47 or later).

Parameter references

This manual uses the primary control program parameters as reference. Some control programs, such as supply unit control programs, have corresponding parameters, but the parameter group numbering starts from 101 instead of 1.

For example, parameter 96.102 in primary control program is parameter 196.102 in supply unit control program.

Target audience

This guide is intended for persons responsible for cyber security throughout the service life of the product. Readers are expected to have expertise in cyber security.

IEC 62443-4-1 security guidelines

IEC 62443 is an international series of standards on cyber security of operational technology in automation and control systems.

This guide complies with the requirements of Practice 8 - Security Guidelines of the IEC 62443-4-1 standard.

For more information, refer to https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards.

Terms and abbreviations

Term	Description
BCU	Type of control unit
Control board	Circuit board in which the control program runs
Control unit	Enclosure that contains the control board and related connector boards. The term is also used as a synonym for the control board.
DDCS	Distributed Drives Communication System. Optical fiber-based industrial protocol.
Defense in depth	An approach to defend the system against any particular attack using several independent methods (IEC 62443-4-1:2018)
Drive	Frequency converter for controlling AC motors
DSAC	Device security assurance center in ABB
EDR	Endpoint detection and response
EWS	Engineering working station
HTTP(S)	Hypertext transfer protocol (secure variant)
IDS	Intrusion detection systems
Inverter module	Inverter bridge, related components and drive DC link capacitors enclosed in a metal frame or enclosure. Intended for cabinet installation.
Inverter unit	Inverter module(s) under control of one control unit, and related components. One inverter unit typically controls one motor.
IPS	Intrusion prevention systems
OEM	Original Equipment Manufacturer
OPC UA	Open Platform Communications Unified Architecture
PLC	Programmable logic controller
RBAC	Role-based access control
RTU	Remote Terminal Unit
Supply module	Rectifier bridge and related components enclosed in a metal frame or enclosure. Intended for cabinet installation.
Supply unit	Supply module(s) under control of one control unit, and related components.
TCP	Transmission Control Protocol
TLS	Transport Layer Security. Secure communication protocol.
UCU	Type of control unit
VLAN	Virtual local area network
ZCU	Type of control unit

Related documents

White papers

Cybersecurity for ABB drives white paper

Protecting operations through cyber security: ABB Drives solutions white paper

Drive manuals and documents

You can find manuals on the Internet. See below for the relevant code/link. For more documentation, go to www.abb.com/drives/documents.

ACS880-01 manuals

ACS880-04 manuals

ACS880-07 (45 to 710 kW) manuals

ACS880-07 (560 to 2800 kW) manuals

ACS880-07CLC manuals

ACS880-07LC manuals

ACS880-11 manuals

ACS880-14 manuals

ACS880-17 (45 to 400 kW) manuals

ACS880-17 (160 to 3200 kW) manuals

ACS880-17LC manuals

ACS880-34 manuals

ACS880-37 (45 to 400 kW) manuals

ACS880-37 (160 to 3200 kW) manuals

ACS880-37LC manuals

ACS880 multidrives manuals

ACS880 multidrives modules manuals

2

ABB approach to cyber security

Contents of this chapter

This chapter gives information on ABB's approach to cyber security. For more information, refer to https://global.abb/group/en/technology/cyber-security.

Cyber security of the drive system

ABB has a comprehensive cyber security approach to protect its drives and other critical systems. Refer to:

- Protecting operations through cyber security: ABB Drives solutions white paper (9AKK108469A4323 [English])
- Cybersecurity for ABB drives white paper (3AXD10000492137 [English]).

Device Security Assurance Center (DSAC)

The ABB Device Security Assurance Center (DSAC) examines ABB products and communicates any cyber security weaknesses to product development for corrective actions.

The DSAC Cyber Security Test Process was certified by exida for IEC 62443 Part 4-1: 2018 Secure Product development lifecycle requirements. Refer to https://www.exida.com/SAEL-Security/abb-cybersecurity-test-process-assessment-of-the-dsac

For information on DSAC, refer to DSAC White Paper (9AKK107680A9866 [English]).

Suppliers

Refer to:

- ABB Cyber Security Requirements for Suppliers: https://global.abb/group/en/about/supplying/cybersecurity
- ABB Supplier Code of Conduct: https://global.abb/group/en/about/supplying/code-of-conduct.

Vulnerability handling and security notifications

ABB supplies firmware updates and security patches to address newly discovered vulnerabilities and to maintain a secure environment. ABB recommends that customers apply the updates and patches to keep the drives protected.

For more information, refer to ABB's approach to Software Vulnerability Handling (9ADB005059 [English]).

To report a vulnerability in the ABB offerings, go to https://global.abb/group/en/technology/cyber-security.

To see a list of latest cyber security alerts and notifications, and to subscribe the future ones, go to https://global.abb/group/en/technology/cyber-security/alerts-and-notifications.

Cyber security disclaimer

This product is designed to be connected to and to communicate information and data via a network interface. It is Customer's sole responsibility to provide and continuously ensure a secure connection between the product and Customer network or any other network (as the case may be). Customer shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

ABB and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

3

Product security context

Contents of this chapter

This chapter gives conditions that the operational environment of the drive must meet. This defines the security context of the drive which, according to IEC 62443, refers to the specific cyber security conditions under which an industrial automation and control system is expected to perform.

The guidelines are intended for the asset owners (a person or organization that owns or is responsible for one or more products or systems) and authorized users (a person who is authorized to change the settings of the drive).

Organizational measures

ABB recommends to obey these organizational best practices:

1. Establish security policies and procedures. Security policies and procedures, such as access control policies, patch management processes, and incident response plans, help to ensure consistent security practices and rapid response to security incidents.
2. Organize training and awareness programs. Regular training and awareness programs for employees on cyber security best practices, such as phishing awareness, password hygiene, and social engineering defense, strengthens the human element of defense in depth and reduces the risk of insider threats.
3. Implement continuous monitoring and threat intelligence. Continuous monitoring solutions and threat intelligence feeds help organizations to stay vigilant against evolving cyber threats and adapt their defenses to mitigate emerging risks.
4. Ensure regulatory compliance. Compliance with relevant industry regulations and standards (for example, NERC CIP, IEC 62443) helps to maintain a baseline level of security and shows commitment to protect critical infrastructure assets.

Physical security

Install the drive in a physically secure location that only authorized users can access. Refer to section Limiting the physical access (page 43).

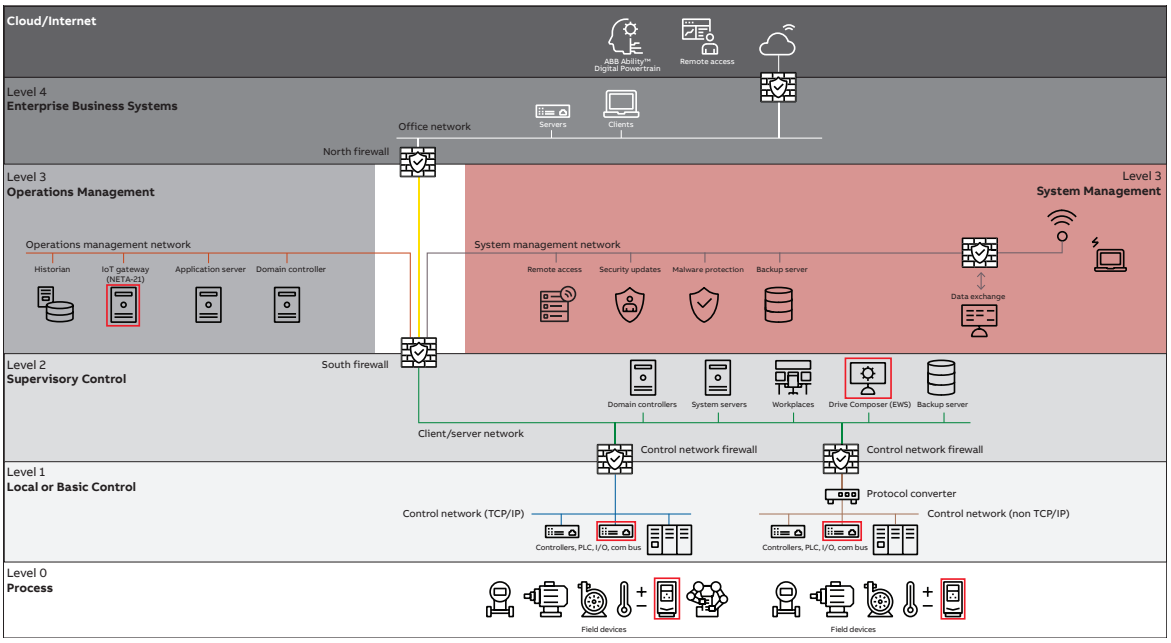
Location in the network

According to ABB ICS Cyber Security Reference Architecture (9AKK107992A6181 [English]), the drive components operate on these levels of the IEC 62443 reference model:

- Level 0: Process. The drive that controls the motor or generator.
- Level 1: Local or basic control. The control unit and other components that communicate through serial communication (such as the control panel and fieldbus adapters).
- Level 2: Supervisory control. Drive Composer that runs on an engineering workstation. If Drive Composer only connects to the drive through the USB port of the control panel, it is an extension of the control panel at level 1.
- Level 3: Operations management. Optional gateway that connects the drive to the cloud. Refer to ABB Ability™ Digital Powertrain.

Reference architecture for industrial production networks

For information about ABB's production network reference architecture, refer to ABB ICS Cyber Security Reference Architecture (9AKK107992A6181 [English]). This figure shows ABB's standard reference network architecture.



Network isolation

ABB recommends to isolate the subnetworks where the drive components are installed from the rest of the automation system. Refer to ABB ICS Cyber Security Reference Architecture (9AKK107992A6181 [English]). ABB recommends to segment the local network where the drive is. Set up at least the following virtual networks (VLANs) for:

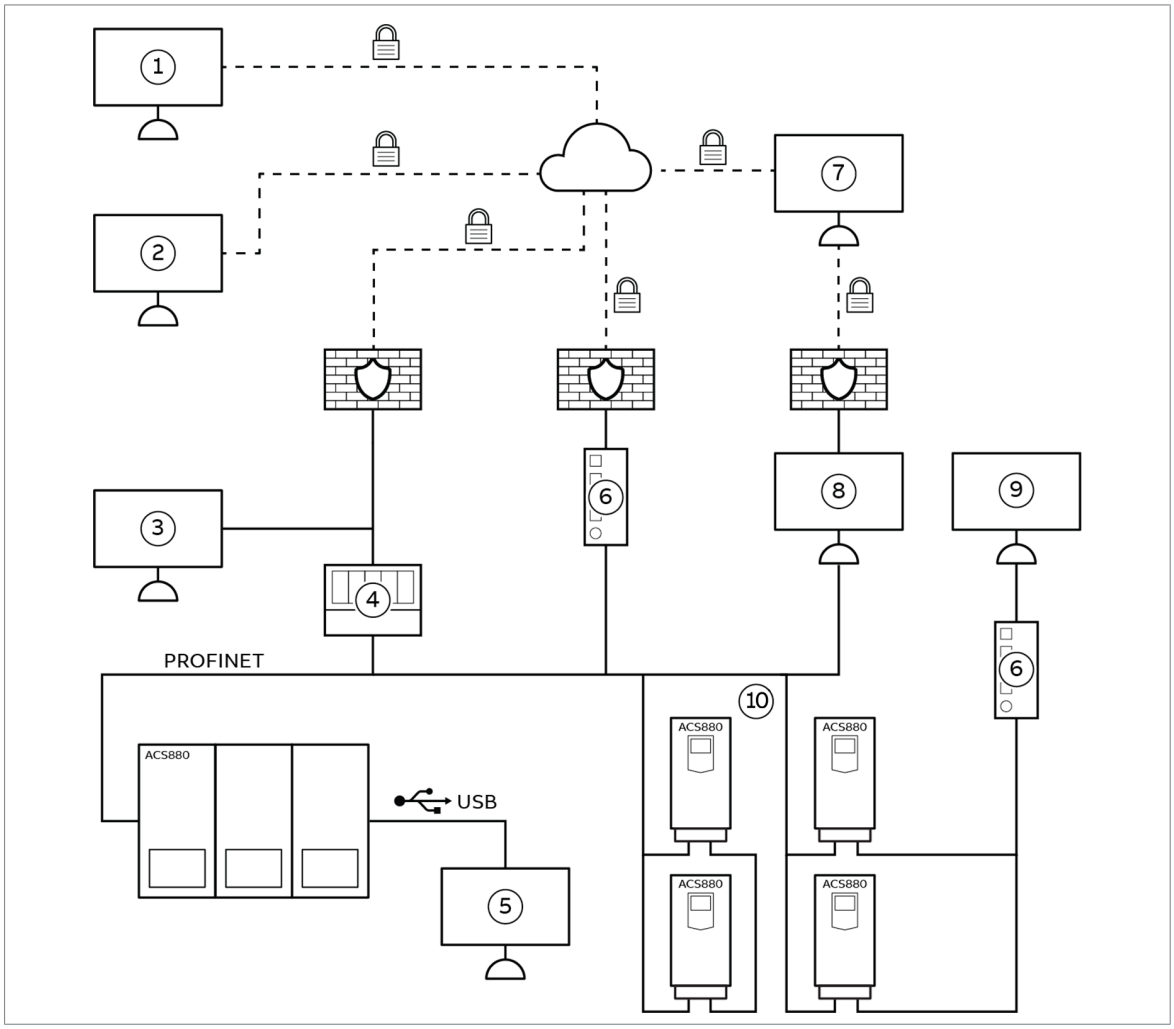
- drive to the EWS (running software tools)
- EWS to the global network
- drive to NETA-21 (if in use for condition monitoring)
- drive to the PLC (control).

Further recommendations at the network level:

- Implement network segmentation to isolate critical systems from less secure or non-essential components. This helps to contain potential security breaches and minimizes the impact of attacks on essential operations.
- Implement firewalls and Intrusion Detection/Prevention Systems (IDS/IPS). Firewalls and IDS/IPS systems at network boundaries and critical junctures help filter and monitor network traffic. They also help detect and block malicious activities in real-time.
- Implement endpoint protection. Endpoint protection solutions, such as antivirus software and endpoint detection and response (EDR) tools help detect and mitigate malware threats targeting drives and other endpoints.

Network connection example

This diagram shows an example of a secure network connection referring to ABB's reference architecture in production environment.



——	Trusted network
- - -	Untrusted network
	Secure connection
1	Customer portal
2	Gateway web page access
3	Local PC with Automation Builder, Drive Application Builder or Drive Manager for SIMATIC
4	Programmable logic controller (PLC)
5	Local PC with Drive Composer
6	Gateway
7	Remote desktop connection
8	Local PC with access to drive’s communication configuration web page
9	Local PC with Drive Composer (or Modbus TCP master)
10	Drive

Trust relationships of the drive

This section describes the trust relationships between the drives and the components of the drive system.

Memory unit

The drive firmware has a trust relationship with the memory unit. The drive firmware does not check the integrity and authenticity of the contents of the memory unit cryptographically.

Software tools

The drive firmware does not authenticate the connection to software tools (such as Drive Composer (page 26) and Drive Application Builder (page 26)) by default. You can connect software tools through USB (not encrypted) or Ethernet connection. Ethernet connectivity can use encrypted protocol (HTTPS). It is possible to restrict Ethernet tool connectivity by downloading user certificates to enable authentication.

Firmware updates

A firmware update is cryptographically authenticated in the UCU control units. In BCU and ZCU control units, a firmware update is not cryptographically authenticated. Apply file download restrictions with the User lock (page 39) to prevent unexpected firmware change. ABB recommends to deactivate firmware download if the drive is in normal operation. Make sure to physically secure the drive to narrow the attack surface. Refer to Limiting the physical access (page 43).

Potential impact of malfunction

It is possible to install drives in critical infrastructure applications where a cyber security attack can have serious impacts, such as:

- physical damage to production systems
- loss of production
- injury
- loss of life.

4

Cyber security related information on ACS880 drives

Contents of this chapter

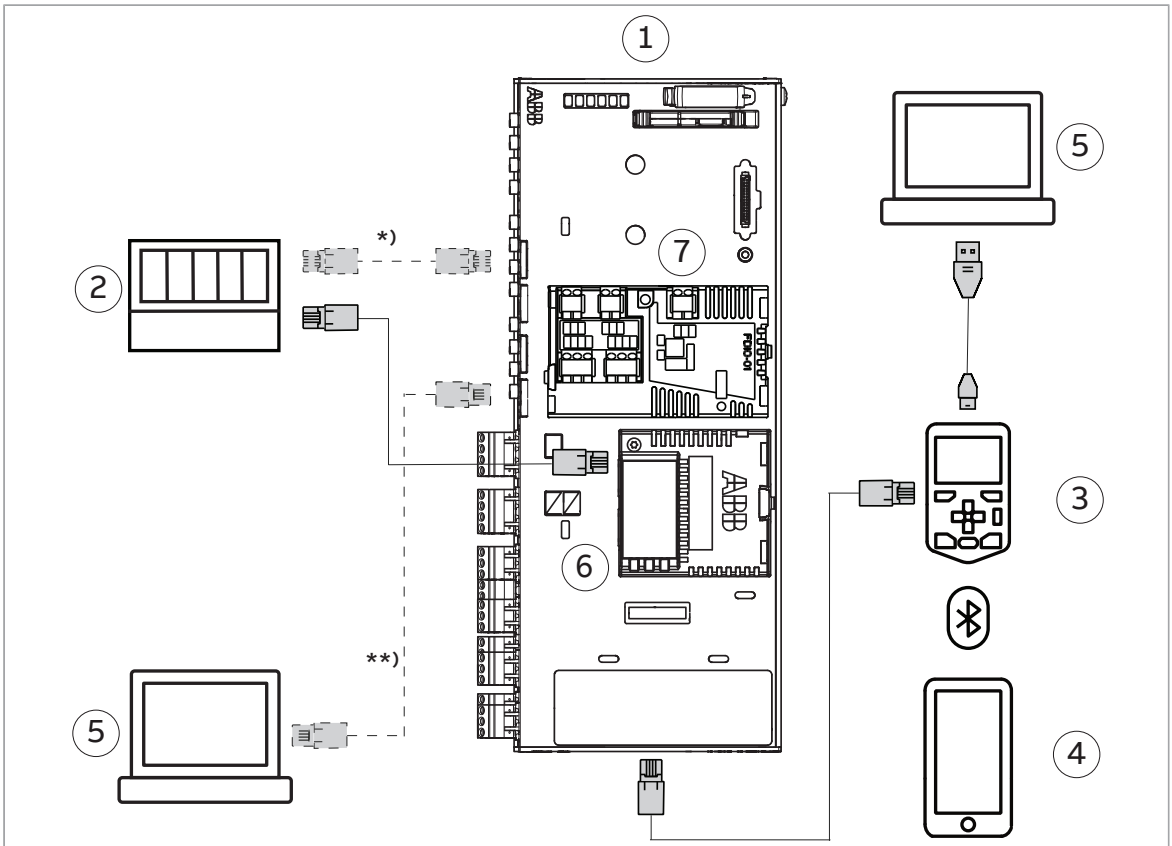
This chapter gives information on ACS880 drives and their components from a cyber security perspective.

Components of the drive system

Refer to the drive hardware manual for the description of its components. Each drive has or can have the following control and monitoring components:

- Control unit (type BCU, UCU or ZCU)
- Power module (such as drive, inverter or supply module)
- Control panel (several types available)
- Fieldbus adapter module (optional, several types available)
- Functional safety module (optional, type FSO, FSPS, or FSCS)
- Remote monitoring module (optional, type NETA-21)
- I/O extension modules, and encoder or resolver adapter modules (optional, several types available)
- Software tools (optional, such as Drive Composer, Drive Application Builder)
- Mobile application Drivetune (optional, operational with a Bluetooth control panel).

This figure shows a connection example of the control and monitoring components of the drive:



1	Control unit
2	Programmable logic controller
3	Control panel
4	Mobile device with Drivetune
5	PC with Drive Composer
6	Fieldbus adapter module/functional safety module
7	I/O extension and encoder modules

*) Embedded control Ethernet. The port exists on all UCU control units but is only used in some firmware versions and drive variants. Refer to the applicable hardware and firmware manuals.

**) Embedded tool Ethernet. The port exists on all UCU control units but is only used in some firmware versions and drive variants. Refer to the applicable hardware and firmware manuals.

Control unit

The control unit controls the operation of the drive. It is also the interface for the external control and monitoring of the drive. The control unit runs the drive firmware.

There are several control unit types in use in the ACS880 product series.

For more information, refer to:

- section External interfaces of the control unit and control panel (page 27)
- drive hardware manuals

- UCU-22, UCU-23 and UCU-24 control units hardware manual (3AXD50000817726 [English])
- BCU-02, BCU-12 and BCU-22 control units hardware manual (3AUA0000113605 [English]).

Control panel

The control panel of the drive is the user interface for configuration and monitoring of drives. The panel has a keypad for manual input and control, and a display that gives real-time feedback on the drive's status and performance. The panel also has USB and Bluetooth interfaces for PC or mobile connectivity, to enable the use of Drive composer or Drivetune.

A single control panel can be used for multiple drives with the panel bus connection. The control panel can be mounted directly to the drive or cabinet door.

With a control panel, a user can:

- use commissioning wizard for easy configuration
- start and stop the drive and control a drive reference signal, for example, motor speed reference
- view and edit parameters, do parameter backups, and restore settings and parameters
- view active warnings and faults and warning and fault history
- reset faults
- switch between local and remote control.

These functions limit the use of the control panel:

- Parameter 19.17 Local control disable disables the start and stop keys of the control panel.
- Parameter lock (page 38) prevents parameter changes.
- Bluetooth pairing is not active as default. Bluetooth connectivity can be disabled with the User lock (page 39).

These panels are available for the ACS880 drives:

- ACS-AP-I assistant control panel
- ACS-AP-W assistant control panel with Bluetooth
- ACS-DCP-11 drive connectivity panel. Refer to Drive connectivity panel for remote connection (page 25).

For more information, refer to:

- ACS-AP-I, -S, -W and ACH-AP-H, -W Assistant control panels user's manual (3AUA0000085685 [English])
- FDPI-02 diagnostics and panel interface user's manual (3AUA0000113618 [English])
- https://new.abb.com/drives/connectivity/user-interface-options.

Fieldbus adapter modules

Optional fieldbus adapters are designed for seamless integration. The fieldbus adapter is a plug-in module that connects the drive to an external controller. Once the adapter is installed, the drive automatically recognizes and activates it, ensuring efficient setup process.

Through the fieldbus adapter module, it is possible to:

- give control commands to the drive (such as start, stop and run enable)
- set a motor speed or torque reference to the drive
- give a process actual value or a process reference to the PID controller of the drive
- read status information and actual values from the drive
- read warnings and faults, reset faults
- view and edit parameters of the drive
- synchronize the real time clock
- connect a PC with the Drive Composer.

Ethernet-based fieldbus adapter modules have a web page for configuration, including certificate management. Username and password restrict the access to the web page.

For more information on a fieldbus adapter module, refer to its user manual. For more information on the fieldbus communication in general, refer to https://new.abb.com/drives/connectivity/fieldbus-connectivity.

Functional safety modules

Functional safety modules are designed to enhance safety and reliability in industrial applications. FSO-12 and FSO-21 are optional functional safety modules that extend the safety functions of the drive. These plug-in modules are installed and cabled inside the drive. Drive Composer pro runs a password-protected functional safety configurator.

The FSO-12 and FSO-21 modules enable several safety functions, such as:

- Safe Stop 1 (SS1), available as SS1-r and SS1-t implementations
- Safe Stop Emergency (SSE)
- Safe Brake Control (SBC)
- Safely Limited Speed (SLS)
- Safe Maximum Speed (SMS)
- Prevention Of Unexpected Start-up (POUS).

For functional safety over fieldbus communication, the FSPS-21 module supports PROFINET and PROFIsafe. FSCS-21 module supports CIP Safety over EtherNet/IP connections, which allows the drive to safely stop using either the STO function or the SS1-t function via PROFIsafe.

For more information, refer to the appropriate safety function module's user manual.

Remote monitoring module - NETA-21

An optional NETA-21 remote monitoring module is designed for remote monitoring and management of the drives. It has an embedded web server, data collection and access interfaces.

The module collects and stores drive performance data in both internal memory and on an SD memory card. This data includes parameters, event lists, and data loggers, which can be accessed remotely. The module supports configurable user access levels and secure access protocols, such as HTTPS, which makes sure that data is protected and accessible only to authorized users.

The module also has event, warning, and fault notifications via email or FTP, allowing for timely responses to any issues that may arise. This feature reduces the time required to access the drives for troubleshooting.

NETA-21 module can connect drives to the ABB Ability™ Digital Powertrain for comprehensive monitoring and management of the entire powertrain.

The module has interfaces for optical, serial, and Ethernet connections. It also supports access through a web page.

Ethernet communication between NETA-21 and drives using HTTP is disabled by default on the drive. HTTP can be enabled through network services.

For more information, refer to NETA-21 remote monitoring tool user's manual (3AUA0000096939 [English]).

Drive connectivity panel for remote connection

The ACS-DCP-11 drive connectivity panel has the same basic features as the assistant control panel used in most drive types as standard. In addition, the drive connectivity panel has these connectivity features:

- Narrowband IoT (NB-IoT) modem and SIM card. If NB-IoT network is available, it is possible to connect the drive to Internet. The NB-IoT connection allows the upload of drive data to ABB Ability™ Digital Powertrain service. User can monitor the data with a browser.
- Bluetooth interface. The Bluetooth interface enables wireless connection to a mobile phone with the Drivetune application. Bluetooth connectivity can be disabled with the User lock (page 39).

For more information, refer to ACS-DCP-11 and ACH-DCP-11 Drive Connectivity Panel User’s manual (3AXD50000718689 [English]).

I/O extension modules and encoder or resolver adapter modules

The optional I/O extension module adds digital and analog inputs and outputs, or relay outputs to the drive. An optional encoder or resolver adapter module connects a motor encoder or resolver to the drive to monitor the speed or position of the motor (or process). The modules are configured with drive parameters, thus software updates are not necessary.

For option modules available, refer to drive hardware manual. For more information on the option module, refer to its user’s manual.

Drive Composer

Drive Composer is a software tool for commissioning and maintenance of drives.

Drive Composer supports these interfaces for connecting to drives: USB cable to the control panel and Ethernet RJ45 cable to an Ethernet adapter module. Drive Composer can also connect to drives through a Bluetooth control panel.

Drive Composer offers secure communication options, including support for HTTPS (TLS 1.2) for encrypted communication. This makes sure that the data transmitted between the PC and the drive is protected from unauthorized access.

Drive Composer has a firmware update feature, which allows users to update the drive's firmware directly from the tool.

Equipping a drive with an Ethernet fieldbus adapter allows the use of Drive Composer over an Ethernet network. This enables remote access and management of drives.

For more information, refer to Drive Composer start-up and maintenance PC tool user's manual (3AUA0000094606 [English]) or go to https://new.abb.com/drives/software-tools/drive-composer.

Drive Application Builder

Drive Application Builder is a tool for drive-based application programming. With the drive application programming, you can create application specific features on top of the drive firmware functionality. For more information, refer to https://new.abb.com/drives/software-tools/drive-application-programming.

Drivetune mobile application

Drivetune is a mobile app to manage drives remotely. The mobile device can be paired through Bluetooth to the drive control panel if the control panel supports Bluetooth.

ABB recommends to disable the Bluetooth in normal use to prevent unauthorized access to the drive. Refer to Guidelines to secure the drive with access levels, user lock and parameter lock (page 47).

For more information, refer to https://new.abb.com/drives/mobile-tools/drivetune.

External interfaces of the control unit and control panel

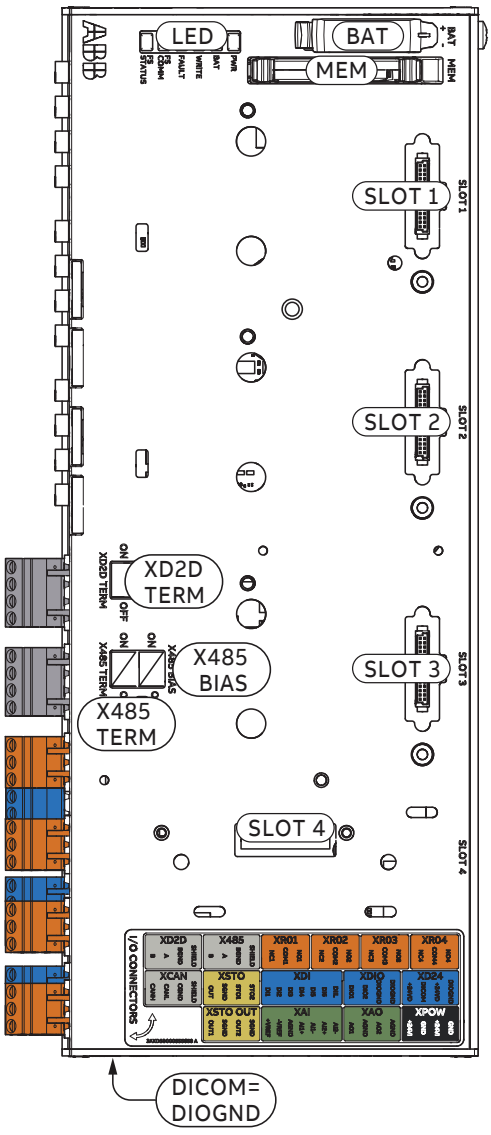
External serial communication interfaces

Interface	Control unit type		
	UCU-22 UCU-23 UCU-24	**BCU-02 BCU-12 BCU-22**	**ZCU-12 ZCU-14**
Ethernet	4 [1)]	1 [1)]	-
Power unit connection	Optical fiber	Optical fiber	Copper wire
Option module slots	4	4	3
Embedded serial RS-485	D2D link or Modbus/RTU [2)]	Modbus/RTU [2)]	D2D link or Modbus/RTU
Embedded serial RS-485	Liquid-cooled units: CIO-01 module connection Air-cooled units: not in use	Liquid-cooled units: CIO-01 module connection Air-cooled units: not in use	-
Embedded serial CAN interface	1 [3)]	-	-
Control panel connection	Assistant control panel/FDPI-02 diagnostics and panel interface unit	Assistant control panel/FDPI-02 diagnostics and panel interface unit	Assistant control panel/FDPI-02 diagnostics and panel interface unit
USB connection	Only through ACS-AP-I or ACS-AP-W control panel		
Wireless connection	Only through ACS-AP-W or ACS-DCP-11 control panel		

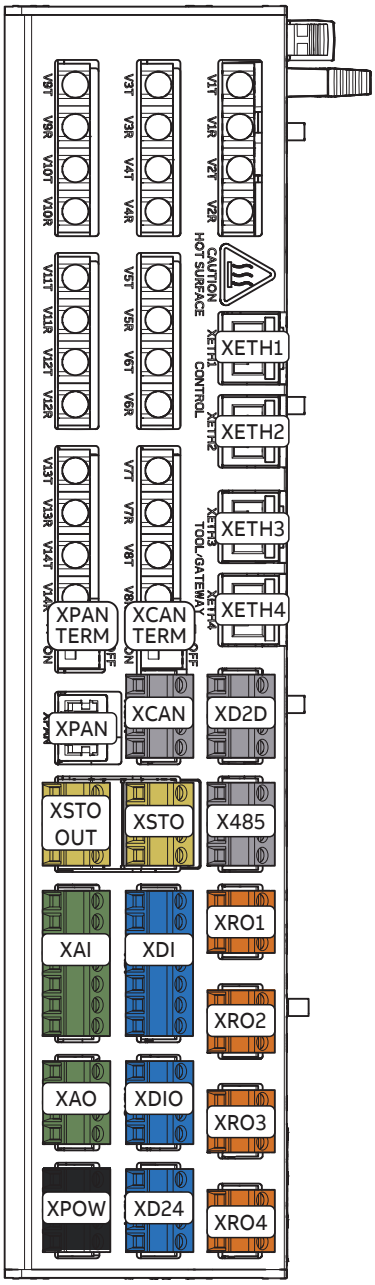
1) The port is only used in some firmware versions and drive variants. Refer to applicable hardware and firmware manuals.
2) Available in some firmware versions. Refer to applicable firmware manuals.
3) Not in use.

Control unit connectors (UCU-22...UCU-24)

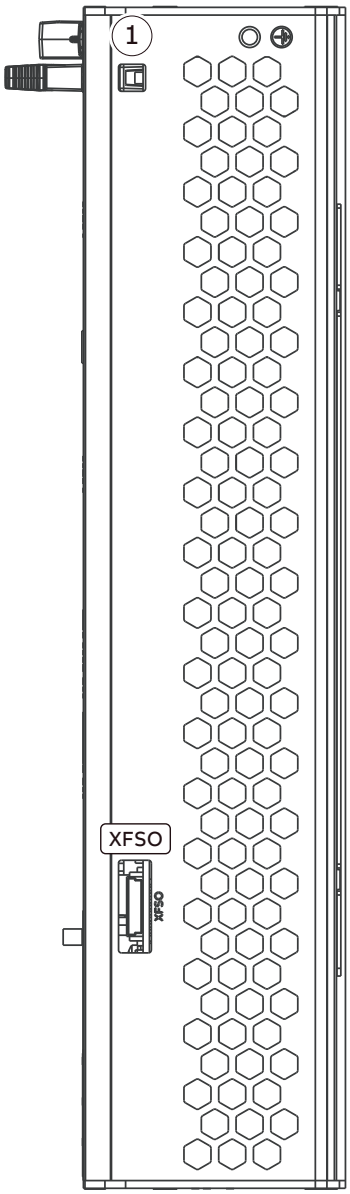
The figures below show the layout of the UCU-24 control unit.



Item	Description
SLOT 1	I/O extension, encoder interface or fieldbus adapter module connection. For F-type modules with USCA-02 adapter.
SLOT 2	
SLOT 3	
SLOT 4	RDCO DDCS communication option module connection
MEM	UMU-01 memory unit connection. A data logger microSDHC memory card is inside the memory unit.
BAT	Holder for real-time clock battery (BR2032)
XD2D TERM	Termination switches for drive-to-drive link (XD2D)
X485 TERM	RS-485 link termination switch
X485 BIAS	RS-485 link bias switch.
DICOM= DIOGND	Ground selection. Determines whether DICOM is separated from DIOGND (ie. the common reference for the digital inputs floats). Refer to the ground isolation diagram.
PWR LED	When the PWR LED is on, the voltage supply is sufficient.
BAT LED	When the BAT LED is on, the real-time clock battery voltage is higher than 2.5 V. If the LED is off when the control unit is energized, the battery must be replaced.
WRITE LED	When the WRITE LED is on, writing to the microSDHC memory card is in progress. Do not remove the microSDHC memory card.
FAULT LED	If the FAULT LED is on, the control program has generated a fault. Refer to the firmware manual.
FS COMM LED	Reserved
FS STATUS LED	Reserved



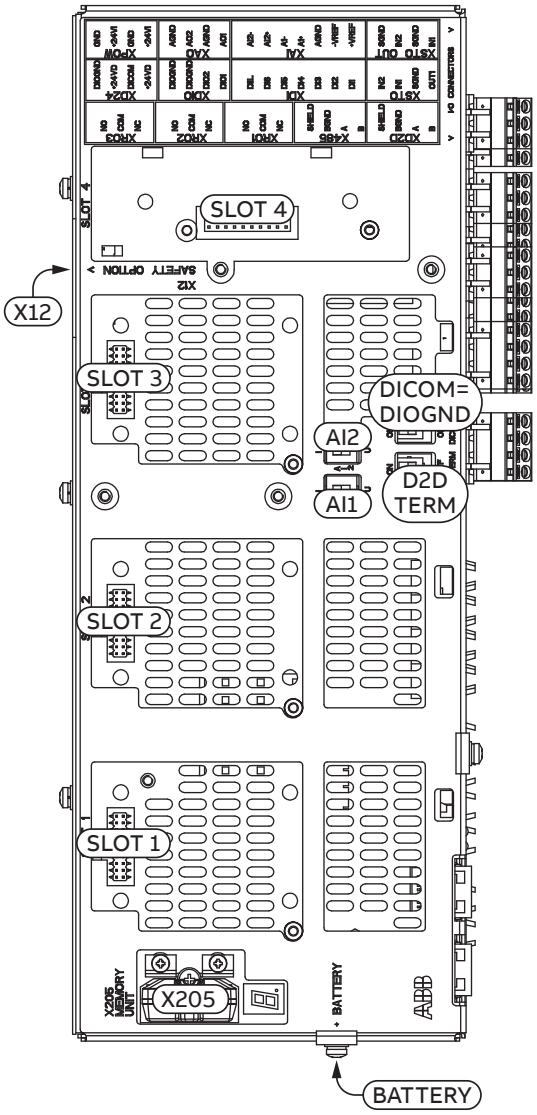
Item	Description
XAI	Analog input
XAO	Analog output
XCAN	Not in use
XCAN TERM	CAN bus termination switch
XDI	Digital input
XDIO	Digital input/output
XD2D	Drive-to-drive link or Modbus/RTU
XD24	+24 V output (for digital input)
XETH1	Ethernet ports for fieldbus, internal switch
XETH2	
XETH3	Ethernet ports for tool communication, internal switch
XETH4	
XPAN	Control panel connection
XPAN TERM	Panel bus termination switch
XPOW	External power input
XRO1	Relay output RO1
XRO2	Relay output RO2
XRO3	Relay output RO3
XRO4	Relay output RO4, reserved
XSTO	Safe torque off connection (input signals)
XSTO OUT	Safe torque off connection (to inverter modules)
X485	RS-485 link
V1T/V1R … V14T/V14R	Fiber optic connections (VxT = transmitter, VxR = receiver) UCU-22: V1T/V1R … V2T/V2R UCU-23: V1T/V1R … V8T/V8R UCU-24: V1T/V1R … V14T/V14R



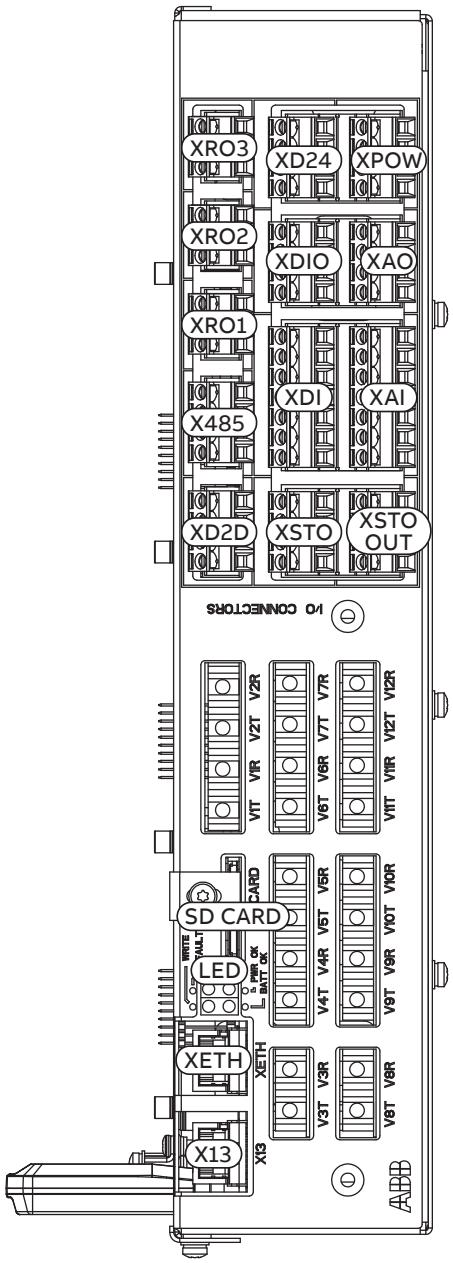
Item	Description
XFSO	Optional connection for FSO safety functions module (supported only in inverter units)
1	Humidity and temperature measurements

Control unit connectors (BCU-02, -12, -22)

The figures below show an example layout of the BCU control unit.



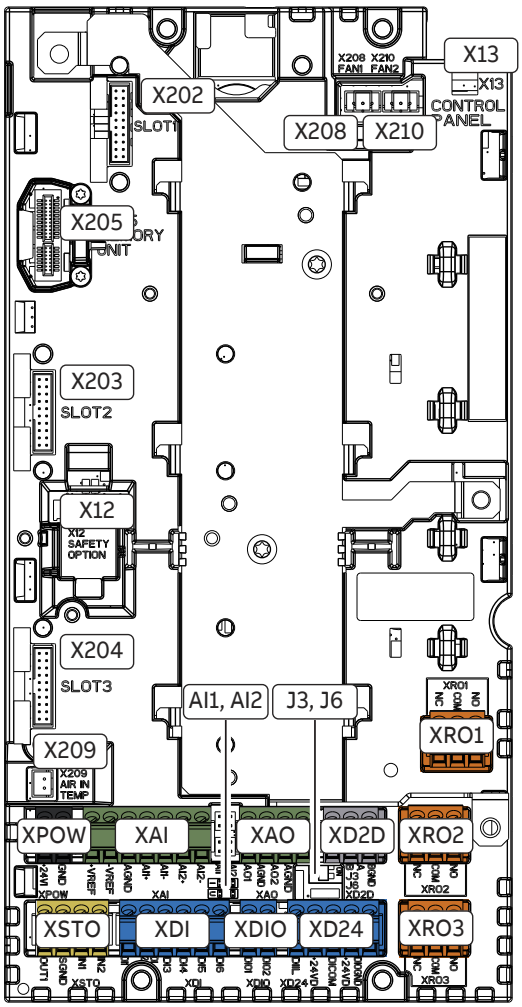
Item	Description
SLOT 1	I/O extension, encoder interface or fieldbus adapter module connection. (This is the only location for an FDPI-02 diagnostics and panel interface module.)
SLOT 2	I/O extension, encoder interface or fieldbus adapter module connection
SLOT 3	I/O extension, encoder interface, fieldbus adapter or FSO safety functions module connection
SLOT 4	RDCO DDCS communication option module connection
X12	Optional connection for FSO safety functions module (supported only in inverter units)
X205	Memory unit connection
BATTERY	Holder for real-time clock battery (BR2032)
AI1	Mode selector for analog input AI1 (I = current, U = voltage)
AI2	Mode selector for analog input AI2 (I = current, U = voltage)
D2D TERM	Termination switch for drive-to-drive link (D2D)
DICOM= DIOGND	Ground selection. Determines whether DICOM is separated from DIOGND (ie. the common reference for the digital inputs floats). Refer to the ground isolation diagram.
7-segment display Multicharacter indications are displayed as repeated sequences of characters.	
o	(“U” is indicated briefly before “o”.) Control program running
U	Control program startup in progress
E	(Flashing) Firmware cannot be started. Memory unit is missing or corrupted.
F	Firmware download from PC to control unit in progress
2	At power-up, the display can show short indications of eg. “1”, “2”, “b” or “U”. These are normal indications immediately after power-up. If the display ends up showing any other value than those described, it indicates a hardware failure.



Item	Description
XAI	Analog input
XAO	Analog output
XDI	Digital input
XDIO	Digital input/output
XD2D	Drive-to-drive link or Modbus/RTU
XD24	+24 V output (for digital input)
XETH	Ethernet port (not in use)
XPOW	External power input
XRO1	Relay output RO1
XRO2	Relay output RO2
XRO3	Relay output RO3
XSTO	Safe torque off connection (input signals)
XSTO OUT	Safe torque off connection (to inverter modules)
X13	Control panel connection (PC connection through control panel)
X485	Not in use by default
V1T/V1R … V12T/V12R	Fiber optic connections (VxT = transmitter, VxR = receiver) BCU-02: V1T/V1R … V2T/V2R BCU-12: V1T/V1R … V7T/V7R BCU-22: V1T/V1R … V12T/V12R
SD CARD	Data logger memory card
BATT OK LED	When the BATT OK LED is on, the real-time clock battery voltage is higher than 2.8 V. If the LED is off when the control unit is energized, the battery must be replaced.
PWR OK LED	When the PWR OK LED is on, the voltage supply is sufficient.
FAULT LED	If the FAULT LED is on, the control program has generated a fault. Refer to the firmware manual.
WRITE LED	When the WRITE LED is on, writing to the memory card is in progress. Do not remove the memory card.

Control unit connectors (ZCU-12)

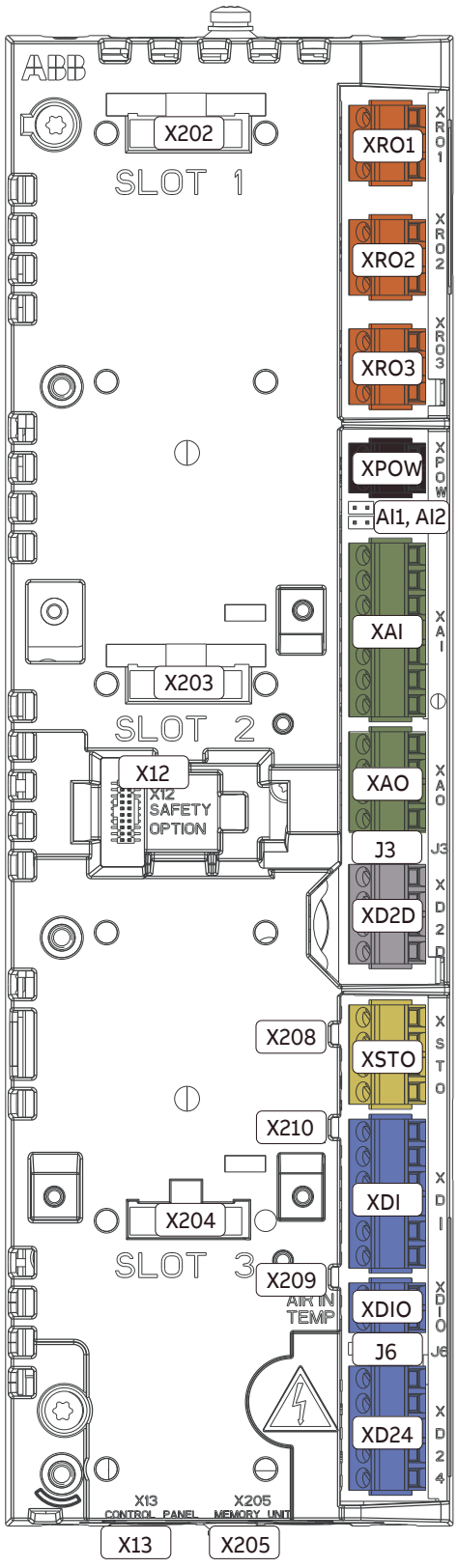
This figure shows the layout of the ZCU-12 control unit.



	Description
XAI	Analog inputs
XAO	Analog outputs
XDI	Digital inputs
XDIO	Digital input/outputs
XD24	Digital input interlock (DIIL) and +24 V output
XD2D	Drive-to-drive link or Modbus/RTU
XPOW	External power input
XRO1	Relay output RO1
XRO2	Relay output RO2
XRO3	Relay output RO3
XSTO	Safe torque off connection
X12	Connection for FSO safety functions module
X13	Control panel connection
X202	Option slot 1
X203	Option slot 2
X204	Option slot 3
X205	Memory unit connection
X208	Cooling fan 1 connection
X209	Connection for ambient temperature sensor (at air inlet). Connected at the factory.
X210	Cooling fan 2 connection
AI1, AI2	Current/Voltage selection jumpers (J1, J2) for analog inputs
J3	Drive-to-drive link termination switch (J3)
J6	Common digital input ground selection switch (J6)

Control unit connectors (ZCU-14)

This figure shows the layout of the ZCU-14 control unit.



	Description
XPOW	External power input
XAI	Analog inputs
XAO	Analog outputs
XD2D	Drive-to-drive link or Modbus/RTU
XRO1	Relay output RO1
XRO2	Relay output RO2
XRO3	Relay output RO3
XD24	Digital input interlock (DIIL) and +24 V output
XDIO	Digital input/outputs
XDI	Digital inputs
XSTO	Safe torque off connection (inverter unit only). **Note:** This connection only acts as a true Safe torque off input when the ZCU is controlling an inverter unit. When the ZCU is controlling a supply unit, de-energizing the inputs will stop the unit but will not constitute a true safety function.
X12	Connection for FSO safety functions module (inverter unit only).
X13	Control panel connection
X202	Option slot 1
X203	Option slot 2
X204	Option slot 3
X205	Memory unit connection
X208	Cooling fan 1 connection
X209	Connection for ambient temperature sensor (at air inlet). Connected at the factory.
X210	Cooling fan 2 connection
AI1, AI2	Voltage/Current selection jumpers (AI1, AI2) for analog inputs
J3	Drive-to-drive link termination switch (J3)
J6	Common digital input ground selection jumper (J6).

Protocols for external communication

This table shows a list of protocols that can be used in communication between the drive and external equipment. For each protocol, the table shows the connection interface, ie, a terminal on the control unit or a reference to an optional device of the drive.

Protocol	Interface	Additional information
CANopen®	Fieldbus adapter module[1)]	Fieldbus connection
CIP Safety		
ControlNet™		
DDCS[2)]	RDCO-0x adapter module	Drive-to-drive connection, connection to ABB controller
DeviceNet™	Fieldbus adapter module[1)]	Fieldbus connection
EtherCAT®		
EtherNet/IP™		
HTTPS/TLS 1.2	Fieldbus adapter module[1)]	PC tool connection
Modbus/RTU	XD2D	Fieldbus connection, drive-to-drive connection
Modbus TCP®	Fieldbus adapter module[1)]	Fieldbus connection
Ethernet POWERLINK		
PROFIBUS DP®		
PROFIsafe		
PROFINET IO®		
OPC UA		
USB	Control panel (USB mini connector)	PC tool connection

1) Refer to https://new.abb.com/drives/connectivity.
2) ABB proprietary protocol.

Network communication ports

This is a list of possible network communication ports of the drive fieldbus interfaces (embedded or when equipped with a fieldbus adapters). Available ports depend on the fieldbus interface type in use. For each port, the supported services and protocol are given.

- port 443 for HTTPS communication (web page and Drive Composer)
- port 80 HTTP traffic is routed to port 443
- ports 34962, 34963, and 34964 (UDP) for the PROFINET protocol
- port 161 (UDP) for the Simple Network Management Protocol (SNMP)
- port 502 for the Modbus (TCP) protocol
- port 44818 (TCP) / 2222 (UDP) for the EtherNet/IP protocol
- port 24576 to set IP addresses with the ABB IP Configuration Tool
- port 123 (UDP) for the Simple Network Time Protocol (SNTP)
- port 68 (UDP) DHCP client
- port 4840 (TCP) OPC UA Server.

Additional services that are available through Ethernet interface:

- web server
- Ethernet adapter firmware update through web page
- Ethernet adapter firmware update through Drive Composer
- connection to Drive Composer over Ethernet interface
- connection to NETA-21 over Ethernet interface via HTTP
- response to ICMP (Internet Control Message Protocol) message.

There are parameters to activate/deactivate each service or protocol (51.02 and 51.15).

For more information, refer to the manual applicable for the fieldbus interface, for example FPNO-21 PROFINET IO fieldbus adapter module user's manual (3AXD50000158614 [English]).

5

Security features

Contents of this chapter

This chapter gives information on the security features of the ACS880 drives.

Secure storage (UCU control units)

Secure storage is a system that keeps certificates, private keys, and encryption keys in a drive, serving multiple use cases. Certificates are used for authenticating data and communications. To make sure unique authentication for devices, data, or configurations, users require unique certificates for each device. The users can utilize an existing Public Key Infrastructure (PKI) to manage all certificate needs on-site. The PKI can generate certificates for devices with private keys or can provide both private keys and certificates for devices.

Secure boot (UCU control units)

The secure boot system authenticates all software executables including boot binary, control firmware, and FPGA logic. The system runs executables produced and signed by ABB. A secure boot is accomplished by using the hardware root of a trusted boot mechanism. Software that has been modified or downloaded maliciously cannot be executed during the startup

R&D access and debugging (UCU control units)

ABB R&D personnel uses the control token system to get access to internal features. These features are mainly for debugging purposes. The control token is a loading package that ABB personnel can download to the control unit. The system verifies the authenticity before it downloads the loading package. The system accepts only control tokens generated with ABB build tools.

Use the user lock function to disable control token download: set parameter 96.102 to bit 2 Disable file download.

To remove all active control tokens from the control unit, activate any bit in parameter 07.63. Reboot the control unit.

Passcode-protected features

The drive control program has these passcode-protected features: access levels, parameter lock and user lock. Ethernet-based fieldbus adapters and NETA-21 gateway have a password-protected web page for configuration.

Access levels

The drive control program has several access levels. Parameter 96.03 shows the status of each access level (active or inactive). On each access level, the user has visibility and access only to predefined content:

Access level	Description
Read only	Read only access is active when parameter lock is activated, or access to control panel is limited. The user has visibility to the content that is available for all users.
End user	The user has read and write access to the content that is available for all users.
Service	The user has read and write access to the same content as the End user, and to the service parameters. This access level is for the ABB authorized users only.
Advanced programmer	The user has read and write access to the same content as End user, and to some additional functions. This access level is for advanced programmers only.
OEM access level 1	The user has read and write access to the same content as End user, and to additional functions for OEM users. These access levels are for OEM customers only.
OEM access level 2	
OEM access level 3	
Fieldbus communication	Access to all visible parameters.

End user access level is active as default. To activate another access level, user must enter the access level pass code to the drive. Refer to Guidelines to secure the drive with access levels, user lock and parameter lock (page 47).

Parameter lock

The drive control program has a parameter lock function. When user activates it, it prevents parameter changes through the control panel and Drive Composer.

Note: Parameter lock does not prevent parameter changes through fieldbus interface.

The parameter lock is only effective against accidental change of parameter settings. Any user can open the parameter lock with its default pass code and change parameters. To prevent this, activate the user lock function.

For instructions on how to activate or deactivate the parameter lock, refer to Guidelines to secure the drive with access levels, user lock and parameter lock (page 47).

User lock

The user lock can be locked or unlocked with a user-defined pass code.

The user lock has the following cyber security related elements:

- Passcode: number to trigger an action.
- Passcode entry parameter: field to enter a passcode.
- Passcodes in scope:
  - **ABB access levels** passcode: ABB's internal passcode for service access.
  - **Parameter lock** passcode: it enables/disables write protection for product parameters.
  - **User passcode**: passcode to open the user lock and change the lock's functionalities.
- User lock functionalities (parameter 96.102 bits 0…10):
  - **Disable ABB access levels passcode**: Disables ABB's internal passcode for service access, advanced programmer, etc.
  - **Freeze parameter lock state**: Prevents parameter lock state change, parameter lock pass code has no effect.
  - **Disable file download**: Prevents loading files to the drive. This includes:
    - Firmware download.
    - Safety functions module FSO-21 configuration.
    - Parameter restore to default values.
    - Loading of adaptive programs.
    - Loading and debugging application programs through Drive Application Builder.
    - Changing the home view of the control panel.
    - Editing drive texts.
    - Editing the favorite parameters list on the control panel.
    - Configuration settings done through control panel (such as time and date formats).
  - **Disable fieldbus write to hidden parameters**: Disables fieldbus access to hidden parameters on disabled access levels.
  - **Protect AP (Access Point)**: Prevents creating a backup and restoring from a backup.
  - **Disable panel Bluetooth**: Disables Bluetooth of a Bluetooth control panel.
  - **Disable write protection via panel port**: Disables parameter write operations from the panel bus (UCU control units only).

For instructions, refer to Guidelines to secure the drive with access levels, user lock and parameter lock (page 47).

Local control disable

User can enable or disable the local control of the drive (start and stop keys on the control panel, and the local controls on the PC tool). Refer to Disabling the local control (page 48) for instructions.

Parameter checksum

A parameter checksum can be calculated from a user-definable set of parameters to monitor changes in the drive configuration. The calculated checksum is compared to 1…4 reference checksums; in case of a mismatch, an event (a pure event, warning or fault) is generated.

By default, the set of parameters included in the calculation contain most parameters, except:

- actual signals
- parameter group 47
- parameters that are activated to validate new settings (such as 51.27 and 96.07)
- parameters that are not saved to the flash memory (such as 96.24)
- parameters that are internally calculated from others (such as 98.09…98.14)
- dynamic parameters (parameters that vary according to hardware), and
- application program parameters.

The default settings can be edited with the Drive customizer PC tool.

Encrypted communication

A control unit with an Ethernet-based fieldbus adapter can communicate with Drive Composer pro through an encrypted communication channel over HTTPS. The OPC UA server supports encrypted and signed communication with OPC UA clients. Refer to Fieldbus adapter modules (page 24).

For more information, refer to Drive Composer start-up and maintenance PC tool user's manual (3AUA0000094606 [English]).

Firmware update of drive components

Control unit

Control program can be updated only locally by connecting PC to the drive.

Control panel

Control panel software can be updated only locally by connecting it to PC through USB interface.

Fieldbus adapters with Ethernet connectivity

It is possible to install a firmware update on the configuration web pages of the fieldbus adapter, or using a TFTP protocol. User must have the firmware update available in a locally connected PC. Note:

- ABB recommends to protect the access to the configuration web pages with a user-defined password.
- It is possible to prevent the installation of firmware updates on the configuration web pages. For more information, refer to the adapter module user's manuals.

Fieldbus adapters without Ethernet connectivity

Local access with special hardware is required to update fieldbus adapters without Ethernet connectivity.

Functional safety modules

Local access with special hardware is required to update functional safety modules.

With fieldbus functional safety modules (FSPS-21 and FSCS-21), update is done through TFTP protocol. TFTP protocol requires local access to the adapter to disconnect Ethernet cable and activate boot mode.

6

Security guidelines

Contents of this chapter

This chapter gives information on how to implement and maintain the defense-in-depth strategy of the drive. The chapter also gives instructions on the use of the drive cyber security features. These instructions are for the asset owners and authorized users.

Limiting the physical access

Install the drive in a secure location that only authorized users can access, such as a locked room that has limited and tracked access of persons.
If it is not possible to install the drive in a location that only authorized users can access:

- Cabinet-installed drives: Order the drives with custom door locks. Give the keys only to the authorized users. By default, ABB cabinets have standard triangle key locks. Note that in some cabinet installations the control panel is accessible even when the door is closed and locked, and can easily be removed.
- Make sure that unauthorized persons cannot access the communication cables between drive cabinets.
- Make sure that the drive has parameter write protection activated, the default passcode has been changed and the checksum is in use. Refer to section Guidelines to secure the drive with access levels, user lock and parameter lock (page 47).
- Make sure that unauthorized persons cannot access the connectors that can be used to communicate with the drive (for example, control panel connectors, PC connectors and Ethernet connectors). Use plastic port blockers, where applicable.

If the drive has a control panel with Bluetooth, disable Bluetooth, and secure the control panel with a user-defined pass code. Refer to Guidelines to secure the drive with access levels, user lock and parameter lock (page 47).

Configuring secure Ethernet networks

ABB recommends to use restrictive configured firewalls and intrusion prevention and detection systems.

The drive supports multiple network interfaces simultaneously. ABB recommends to separate the service (tool) network and process control network, and to configure each interface according to specific needs.

When the interface is used for process control, disable all additional services and lock the configuration after drive commissioning is complete. Do the fieldbus adapter module settings that follow. The parameters are visible in the drive control program after the Ethernet adapter module is installed.

1. Set bits of parameter 51.15 (53.15) Service configuration:
   - **bit 1** Disable IP config tool (with ABB IP configuration tool it is possible to change IP address of the interface without authentication credentials)
   - **bit 2** Disable ETH tool network (deactivates remote connection of Drive Composer)
   - **bit 3** Disable ping response (response to ICMP (ping) message is prevented)
   - **bit 5** Disable configuring web pages (disables Ethernet adapter's embedded web server access)
   - **bit 6** Web-based firmware update (disables firmware update of interface adapter via Web API)
   - **bit 7** Disable OPC UA (deactivates OPC UA Server. It is not used in process control).
2. After the configuration is done, activate **bit 0** of parameter 51.15 (53.15) to lock it, and apply the new settings with parameter 51.27.

When the interface is used for service (tool) network, that is for connecting Drive Composer or OPC UA, ABB recommends to:

1. Disable fieldbus protocol of the Ethernet adapter. Set parameter 51.02 Protocol/Profile to NONE(200). In addition:
2. Set bits of parameter 51.15 (53.15) Service configuration:
   - **bit 1** Disable IP config tool (with ABB IP configuration tool it is possible to change IP address of the interface without authentication credentials)
   - **bit 3** Disable ping response (response to ICMP (ping) message is prevented)
   - **bit 5** Disable configuring web pages (disables Ethernet adapter's embedded web server access)
   - **bit 6** Web-based firmware update (disables firmware update of interface adapter via Web API).
3. After the configuration is done, activate **bit 0** of parameter 51.15 (53.15) to lock it, and apply new settings with parameter 51.27.

Maintaining the drive system secure

This section contains recommendations on periodic security maintenance activities. The guidelines and recommendations are intended for the asset owners and authorized users.

ABB recommends these periodic security maintenance activities:

- Check known vulnerabilities on https://global.abb/group/en/technology/cyber-security/alerts-and-notifications periodically and obey ABB's guidelines.
- Make sure to update the firmware of the drive, its components and PC software regularly. Refer to Firmware update of drive components (page 41).
- Check ABB Drives life cycle plan changes at least once a year. Go to https://www.abb.com/global/en/product/drives/low-voltage-ac-drives/legacy-drives for product-specific lifecycle statements, or contact ABB. ABB does not supply security patches for obsolete products.
- Perform backups of all components' configuration files and data periodically. Keep the backups in a safe place.
- Check the drive's clock configuration periodically. If using distributed time clock systems check whether the time synchronization is correctly configured.
- Periodically check possible improvement actions on your system. You may want to get the support from ABB services to do so, contact local ABB Services representatives

Secure operation best practices

To make sure that the drive operates correctly with minimum downtime, and is secured against outside threats, obey these best practices:

- Keep up-to-date backups of the drive parameter settings. Use Drive Composer's backup/restore feature.
- Set custom passcode and user account protection for the drive system components. Refer to section Managing passcodes, passwords and user accounts (page 46).
- Disable all unnecessary services, protocols, or ports of the drive to reduce the attack surface. Only enable the services necessary for the operation. Use port blockers where possible.
- Verify your firmware update download before deploying to device. Refer to section Securing the firmware integrity (page 49).
- Install firmware updates regularly. Use the latest loading packages provided by ABB. Test the updates in a controlled environment before you deploy them to production systems.
- Implement strong access controls in the engineering work stations with software tools and overriding control systems to restrict access to the drive. Use role-based access control (RBAC) to assign permissions based on job roles and responsibilities, and limit access to only authorized users. Use account management on the PC where Drive Composer is installed.
- Use physical access control for the control panel.

- Implement physical security measures to prevent unauthorized access to the drive. You can use, for example secure enclosures, access control systems, or surveillance cameras.
- Prefer secure protocols over plain text protocols.
- Check the drive control program event logs periodically. Refer to Using event logs (page 46).
- Use time synchronization. Synchronize the clocks of all the components. This ensures that audit log timestamps are accurate.

Managing passcodes, passwords and user accounts

ABB recommends to set up passcodes of the maximum length possible. Avoid simple series of numbers, such as 1234 or 9999. Renew passcodes regularly and make sure only authorized users have access to the passcodes.

Change the default passcode for the user lock in the drive control program. Refer to Guidelines to secure the drive with access levels, user lock and parameter lock (page 47).

If you have a fieldbus adapter module with Ethernet connectivity in the drive system, change the default password and username for its configuration web page. Refer to Ethernet fieldbus adapter user's manual.

If you have NETA-21 gateway in the drive system, change the default password and username for its configuration web page. Refer to NETA-21 remote monitoring tool user's manual (3AUA0000096939 [English]).

Using event logs

Check the drive control program event logs periodically for events, faults and warnings in the drives, especially the user lock warnings or cyber security related faults, like open user locks warning 1236.

For instructions on how to check events logged in NETA-21, control panel or Drive Composer, refer to applicable user's manual.

Access management

Guidelines to secure the drive with access levels, user lock and parameter lock

For the user lock to be effective and the parameter lock to be bound to the user lock, do the following steps. This procedure allows to harden the drive as described in sections Parameter lock (page 38) and User lock (page 39).

1. Enter the default user passcode 10000000 in 96.02 Passcode.
2. Change the default user passcode. Use parameters 96.100 Change user passcode and 96.101 Confirm user passcode. The new passcode is set when both values of parameter 96.100 and 96.101 are identical. Write down the new user passcode and store it securely. Make sure that only authorized users have access to it.

   NOTICE ABB cannot open the user lock if the passcode is lost. ABB is not liable for damages or losses caused by the failure to change the default pass code.

3. In 96.102 User lock functionality set bits 0, 2, 3 and 6 to 1 (high):
   - Bit 0: Disable ABB access levels
   - Bit 2: Disable file download
   - Bit 3: Disable Fieldbus write to hidden parameters
   - Bit 6: Protect AP.

   Note: Keep bit 1 to value 0 (low).
4. Enter any invalid passcode in 96.02 Passcode to close the user lock.
5. Set parameter 96.02 Passcode to 358 to close the parameter lock.
   - In 96.03 Access Levels Active bit 14 (parameter lock) is set. Parameters can no longer be changed (but for 96.100 to 96.102).
6. Enter your user passcode in 96.02 Passcode to open the user lock.
7. In 96.102 User lock functionality set bit 1 to 1 (high) to freeze the parameter lock state.
8. Enter any invalid passcode in 96.02 Passcode to close the user lock.

Opening the parameter lock

If you need to open the parameter lock after you have frozen its state change with the user lock, do the steps that follow:

1. Enter your pass code to parameter 96.02 to open the user lock.
2. Set bit 1 of parameter 96.102 to 0 to unfreeze the parameter lock state change.
3. Enter the parameter lock pass code (358) to parameter 96.02.

You can do the necessary parameter changes now. After you are done, remember to close the parameter lock and freeze its state change with the user lock.

Disabling the local control

WARNING Before you disable local control, make sure that the control panel is not needed to stop the drive.

To disable local control, set parameter 19.17 to Yes.

Managing the certificates for NETA-21 (if any)

For instructions on setting TLS certificates in NETA-21, refer to NETA-21 remote monitoring tool user's manual (3AUA0000096939 [English]).

Activating the Drive Composer authentication

Refer to Guidelines to secure the drive with access levels, user lock and parameter lock (page 47) to manage the authentications of the drive. These authentications are also valid for the access over Drive Composer.

Drive Composer uses secure HTTPS (TLS 1.2) communication when connected through Ethernet. By default, the Ethernet adapter does not require client authentication for PC tool communication. ABB recommends to use a client certificate to restrict remote access to the drive through the Ethernet interface. Refer to Hardening the authentication for the fieldbus adapter modules with Ethernet connectivity (page 48).

Connectivity restrictions

The connection between Drive Composer and the drive can be restricted to authorized instances only using certificates. Refer to Drive Composer start-up and maintenance PC tool user's manual (3AUA0000094606 [English]) for instructions to set up certificates on both sides.

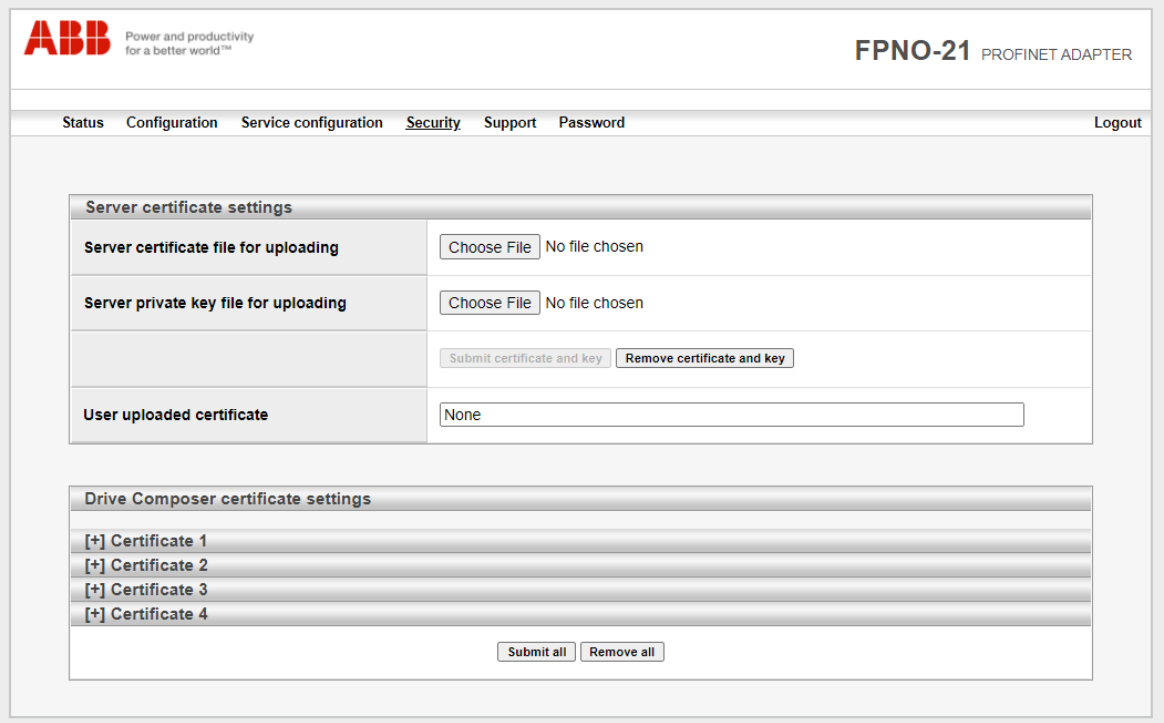
Activating the control panel authentication

Refer to Guidelines to secure the drive with access levels, user lock and parameter lock (page 47) to manage the authentications of the drive. These authentications are also valid for the access over the control panel.

Hardening the authentication for the fieldbus adapter modules with Ethernet connectivity

1. Change the default password for the fieldbus web configuration pages.
2. Deactivate any unused services and secure the configuration to prevent modifications through the fieldbus adapter module.
3. If an Ethernet adapter web page is necessary for the application, ABB recommends to upload the private key and certificates to replace the self-signed certificate utilized by the web server for HTTPS communication. Navigate to security page (in the configuration web pages) to perform the action.

Note: Secure PC tool communication is possible with Drive Composer Pro version 2.7 or later.



For more information, refer to the applicable fieldbus adapter module user's manual.

Securing the firmware integrity

Use only firmware provided by ABB or downloaded from ABB secure websites, such as ABB Library (https://library.abb.com/), which use authentic certificates.

Check firmware loading package integrity before loading it to the drive. Firmware loading package is available from the in-house Maintenance Manual (only available to ABB service engineers and premium partners) or through Drive Composer (refer to Drive Composer manual for detailed instructions).

Check the checksum of the FW loading package against the reference checksum given in SHA-512 checksum summary for ACS880 (9AKK107045A0964) (BCU and ZCU) or Security guidelines (page 43) (UCU). Obey the instructions given at the end of the file. Make sure to get the original document from the ABB library (through HTTPS, if possible).

Securing the parameter integrity

To be aware of any unexpected changes in parameter configuration, ABB recommends to activate the Parameter checksum (page 40) function.

To configure parameter checksum:

1. Define the level of notification by setting parameter 96.54 Checksum action. For better security, use Fault or Warning and prevent start.
2. After parameter 96.54 is configured, check parameter 96.53 Actual checksum.

3. Define Approved checksum in parameters 96.56…96.59.
4. Activate approved checksum with parameter 96.55 Checksum control word.

For more information, refer to applicable firmware manual.

Secure disposal instructions

This section gives instructions on how to securely dispose of the drives.

Note: These operations cannot be undone.

⚠WARNING Obey the safety instructions of the drive. If you ignore them, injury or death, or damage to the equipment can occur. If you are not a qualified electrical professional, do not do electrical installation, commissioning or maintenance work.

⚠WARNING Do not remove the memory unit when the control unit is powered.

1. Erase the content of the secure storage and replace the customer-defined secure storage encryption key with the factory default key: Set parameter 07.75 to Erase and reset.
2. Remove the memory unit from the control unit. Refer to the drive hardware manual or control unit hardware manual.
3. Remove the memory card from the memory unit. Refer to the drive hardware manual or control unit hardware manual.
4. Discard the memory unit and memory card according to company security guidelines.
5. Recycle the drive components. Refer to the drive recycling instructions.

Documentation review and feedback process

ABB has a user documentation review process, and a process for gathering feedback on user documentation. If you find a cyber security related issue in the user documentation, send an e-mail to the ABB cyber security mailbox: cybersecurity@ch.abb.com. For non-urgent feedback on the documentation, use this form: forms.abb.com/form-26567. You can also contact an ABB representative.

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 new.abb.com/contact-centers.

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 forms.abb.com/form-26567.

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.

a4 (frozen)
PDF-A4
Created 2025-03-21, 19:51:59

www.abb.com/drives

3AXD50001159429A

3AXD50001159429 Rev A (EN) 2025-03-21