ABB MACHINERY DRIVES

ACS380-E drives

Cyber security guide

ACS380-E drives

Cyber security guide

Table of contents

3AXD50001145798 Rev A
EN
Original instructions
EFFECTIVE: 2025-05-14

Table of contents

1 Introduction to the document

2 ABB approach to cyber security

3 Cyber security information on ACS380-E drives

4 Cyber security guidelines

1

Introduction to the document

This document is the cyber security guide for ACS380-E drives and has information on the installation, use, service, and decommissioning of the drive. It contains cyber security recommendations for the service life of the drive.

Applicability

This manual applies to the ACS380-E drives.

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.

Personnel definitions

In this guide, we use these personnel roles.

Role	Definition
Asset owner	A person or organization that owns or is responsible for one or more products or systems.
Authorized person	A person authorized to access and control the security policies and capabilities of the product or system.
End user	An end user of the product or system.

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.

Product information

The ACS380-E machinery drive is a low-voltage AC variable-speed drive for motor control in industrial applications. It operates in the power range from 0.55 kW to 22 kW. It has embedded Ethernet connectivity and functional safety features.

Terms and abbreviations

Abbreviation	Explanation
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 that controls AC motors
HTTP(S)	Hypertext Transfer Protocol (secure variant)
LAN	Local Area Network
Panelbus	ABB proprietary industrial protocol
SG	Security Guideline (requirements according to IEC 62443-4-1)
TCP	Transmission Control Protocol
TLS	Transport Layer Security, a secure communications protocol
USB	Universal Serial Bus
WAN	Wide Area Network

Related documents

For more documentation, go to www.abb.com/drives/documents.

	ACS380-E documentation list

2

ABB approach to cyber security

This is information on the ABB approach to cyber security. For more information, go 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.

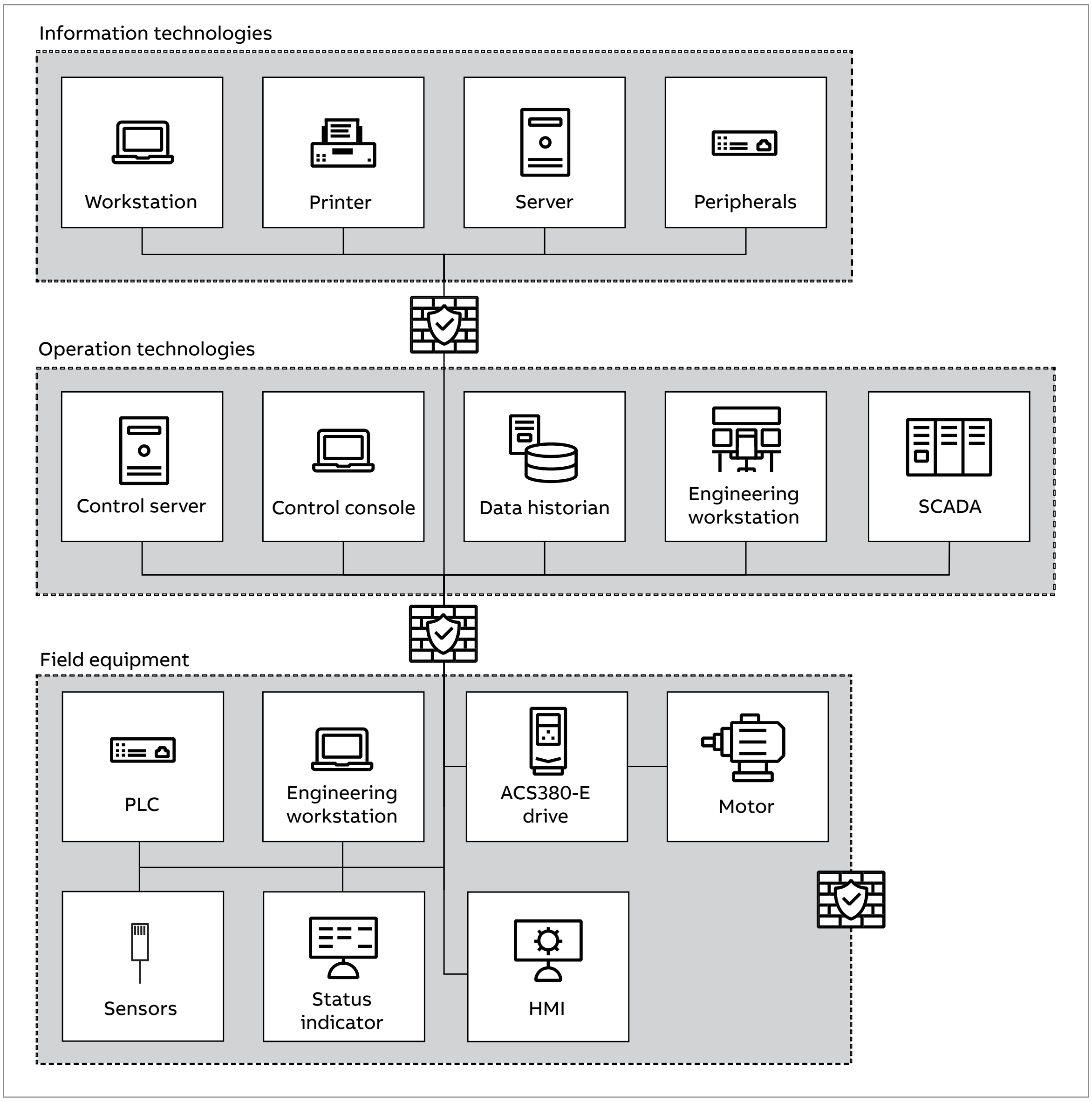
3

Cyber security information on ACS380-E drives

Information on the ACS380-E drive from a cyber security perspective.

Operating environment

The illustration shows an example of the operating environment of an ACS380-E drive.



Product security

Physical security

Install the drive in a secure location that only authorized persons can access, for example, in a locked cabinet or a restricted area. For more information, refer to Defense-in-depth measures expected in the environment (SG-2) (page 21).

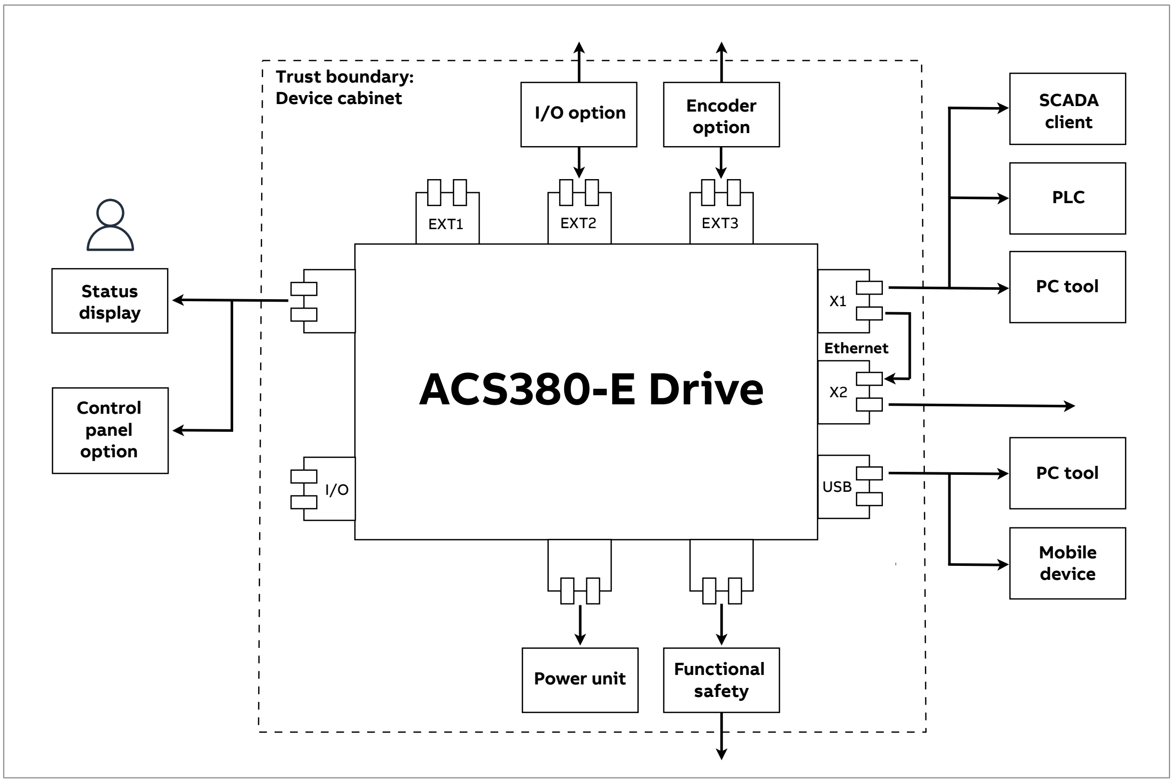
Software security

It is possible to change the configuration settings of the drive with Drive Composer, PLC control, or an optional control panel. Make sure that only authorized persons can change the configuration settings of the drive. Refer to User lock (page 17).

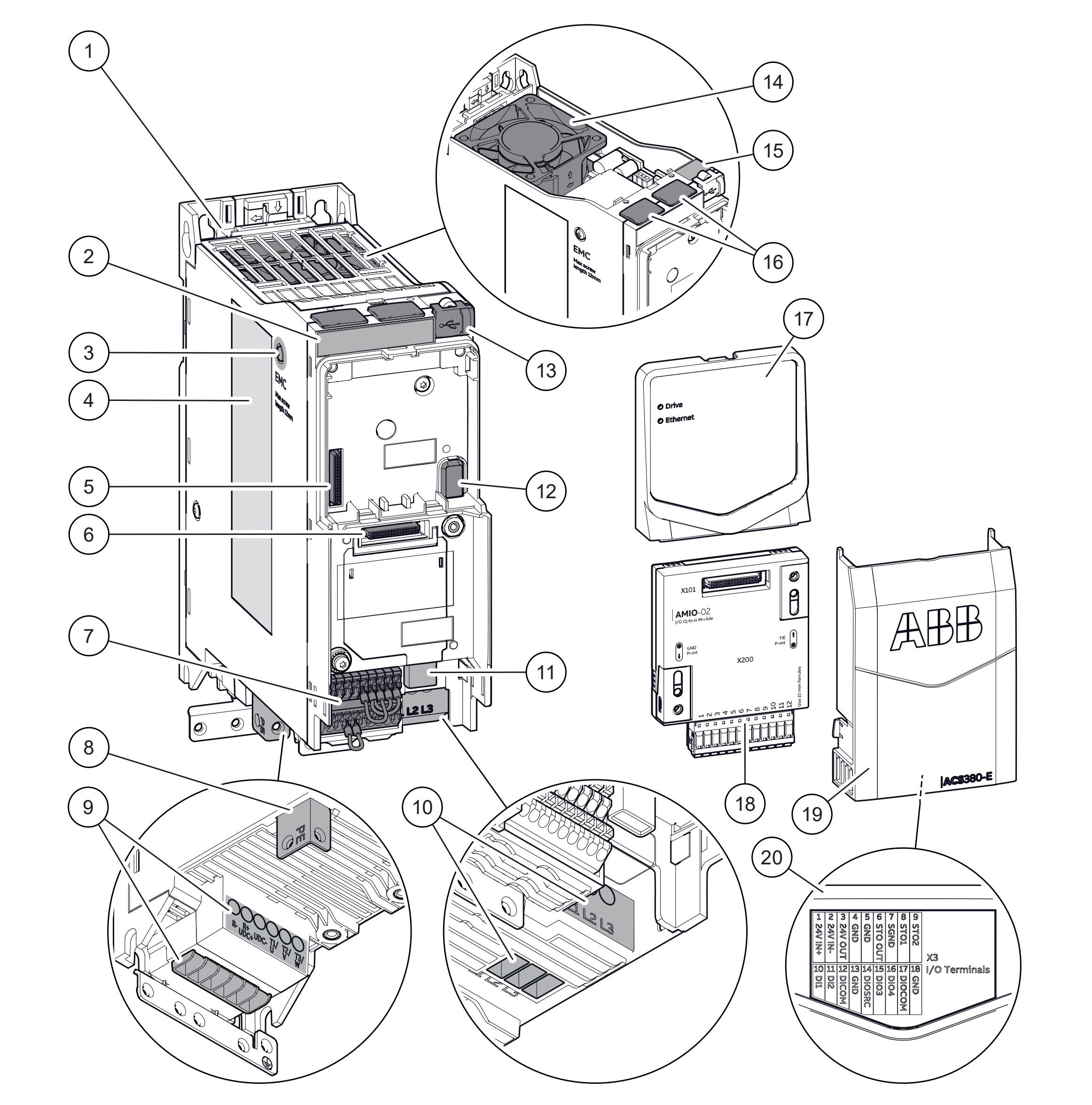
Drive system components

The ACS380-E drive is described in detail in the drive hardware manual: ACS380-E drives hardware manual (3AXD50001141677)

Logical connections



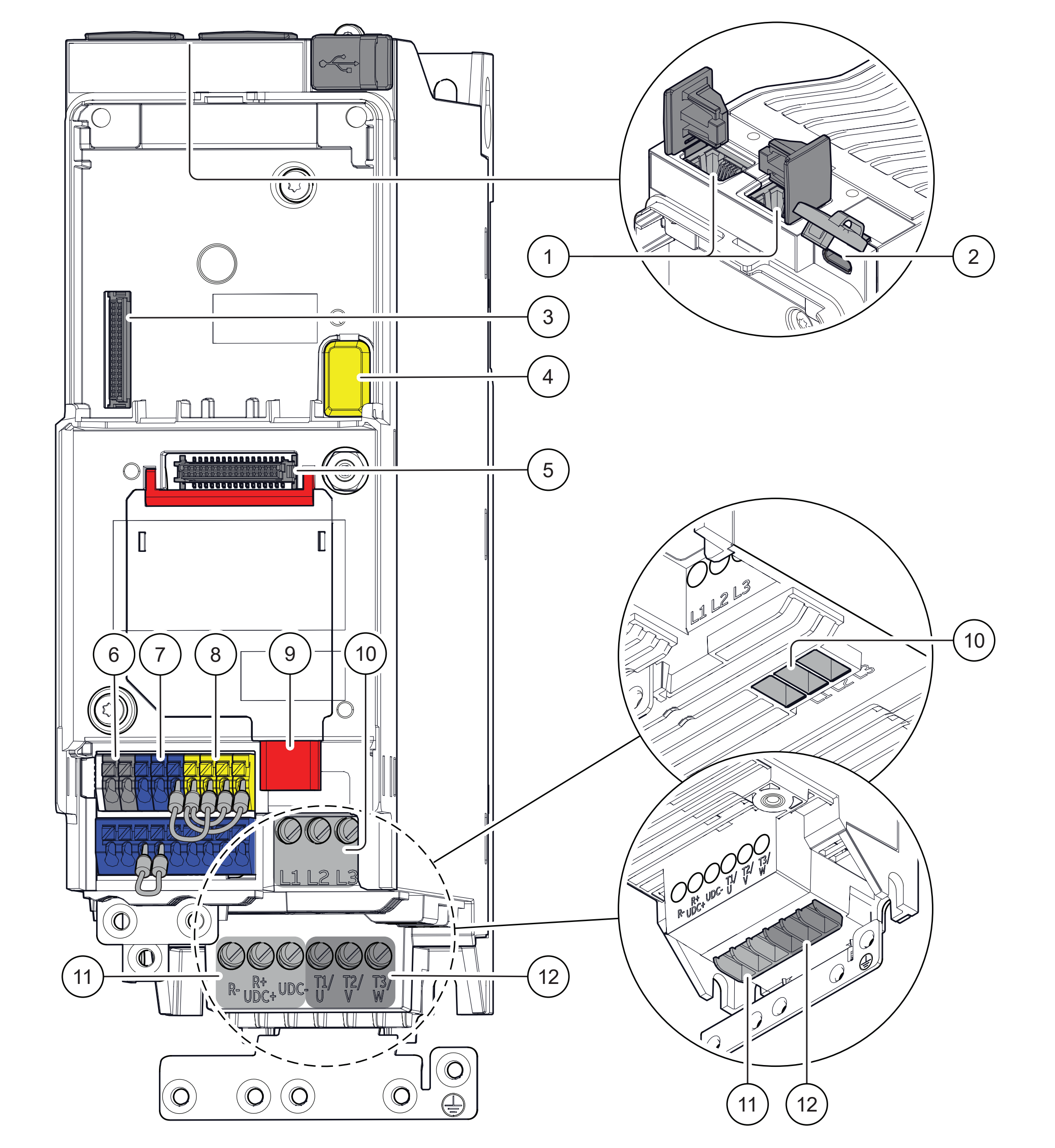
Drive components



1. Drive base unit
2. MAC address label
3. EMC filter grounding screw
4. Type designation label
5. Front panel/safety option connector
6. Option module connector
7. Control terminals
8. PE connection (motor)
9. Brake resistor and motor terminals
10. Input power terminals
11. Eject button for option module
12. Safety option connector
13. USB-C port
14. Cooling fan
15. Model information label
16. Ethernet ports (X1 and X2)
17. Front panel (Status display or option)
18. Option module
19. Front cover
20. Control terminal designations

Drive connections

Connections of the drive base unit:



1. Ethernet (RJ45) ports	7. Auxiliary +24 V DC output, and digital I/Os
2. USB-C port	8. Safe torque off connections
3. Front panel connector	9. Option module eject button
4. Safety option connector	10. Input power terminals
5. Option module connector	11. Brake resistor terminals
6. External +24 V DC input	12. Motor terminals

Embedded Ethernet connection

Embedded Ethernet connection specifications:

- **Compatibility:** Ethernet Standard IEEE802.3/u devices
- **Medium:** 10/100Base-TX with auto-negotiation and auto-MDIX
- **Topology:** bus, star, or ring
- **Connectors:** RJ45

I/O extension modules

The drive has an optional AMIO-02 I/O extension module. For information on the module, refer to the drive hardware manual.

Control panel option module

The drive has an optional control panel module. For information on the module, refer to the drive hardware manual.

Commissioning and maintenance tools

Drive Composer is a start-up and maintenance tool for ABB drives. With Drive Composer, the user can read and set parameters, and monitor and control process performance.

Drive Composer connects to the drive through:

- USB connection (USB-C port)
- Embedded Ethernet connection (RJ45 ports X1 and X2)

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

Communication interfaces

- Ethernet ports: X1 and X2 LAN ports for wired local area connection
- USB-C port

Communication protocols

Standard protocols:

- Hypertext Transfer Protocol Secure (HTTPS/TLS 1.2) for commissioning and maintenance communication with the web interface over the embedded Ethernet connection.
- USB communication device class (CDC) for commissioning and maintenance communication through the USB-C connection.

The embedded Ethernet connection supports these industrial Ethernet protocols to monitor and control the drive:

- PROFINET (protocol information: www.profibus.com) (Enabled by default.)
- EtherNet/IP (protocol information: www.odva.org)
- Modbus/TCP (protocol information: modbus.org)

Security features

Security features of the ACS380-E drive:

Secure boot

The drive control unit examines the integrity and authenticity of the drive firmware with a secure boot mechanism. The drive firmware is digitally signed and handled by industry best practices for data security.

If the drive cannot authenticate the firmware, it shows a permanent fault and does not start. Refer to the drive firmware manual for more information.

User lock

The drive has a user lock feature. With it, the user can:

- Set limits on drive functionality
- Prevent changes to drive parameter values
- Prevent firmware updates

The user lock can be locked and opened with a user-defined passphrase. Refer to Account management (SG-6) (page 24). For more information, refer to the drive firmware manual.

4

Cyber security guidelines

These are the security guidelines of the ACS380-E drives according to IEC 62443-4-1:2018.

Product defense in depth (SG-1)

ACS380-E drives implement a defense-in-depth approach. This strategy uses multiple layers of protection against cyber security threats. This section has information on the methods for the defense-in-depth approach for ACS380-E drives.

Access security

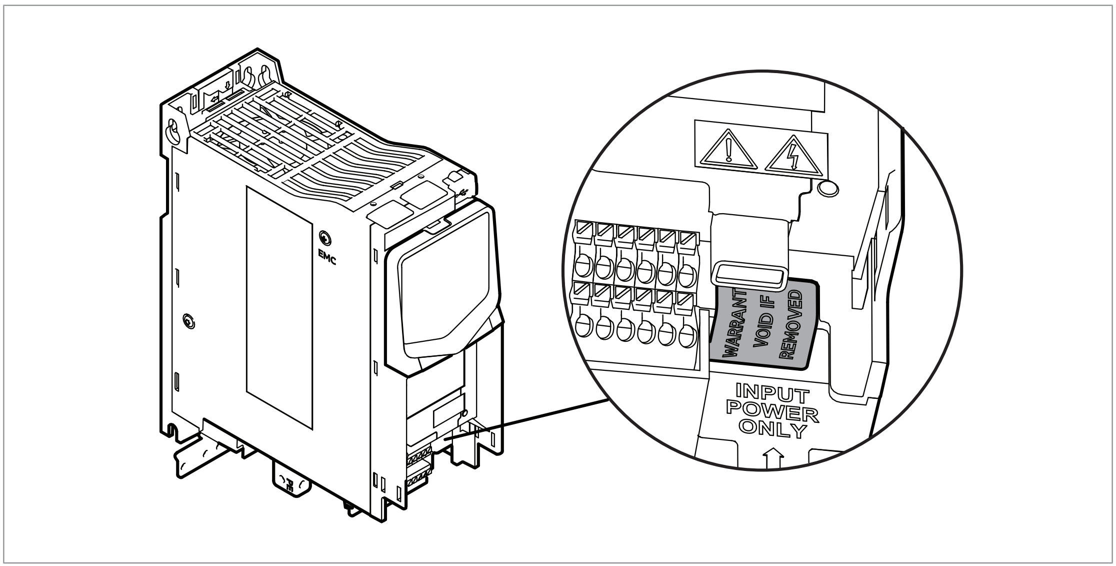
Give access to the drive cabinets and drives only to a limited authorized group of persons.

Hardware security features

ACS380-E drives have hardware security features to resist physical tampering and unauthorized access. This includes secure enclosures, tamper-evident seals, and strong components to withstand harsh industrial environments.

Before you use the ACS380-E drive:

1. Examine the product package for signs of tampering or damage.
2. Make sure that the anti-tamper seals of the product packages are intact.
3. Make sure that the anti-tamper label of the drive is intact and that there is no damage to the drive. If there is damage, do not use the drive and contact your supplier.



The anti-tamper label on the drive

Embedded security mechanisms

ACS380-E drives have embedded security mechanisms such as secure boot, which makes sure that only authenticated firmware can be loaded onto the device. This prevents unauthorized modifications or tampering with the drive firmware.

Network security

ACS380-E drives use advanced network security measures to protect against cyber security threats and unauthorized access over communication channels. This includes support for secure communication protocols, and encryption and authentication mechanisms for data confidentiality and integrity during transmission.

Network communication ports

NOTICE Do not connect the drive to a public or unsecured data network.

The ACS380-E drive uses these network ports:

Default ports:

- Port 443 for HTTPS communication.
- 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).

Configurable ports:

- 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.

Security updates and patch management

ABB releases regular security updates and patches to address vulnerabilities and enhance the resilience of ACS380-E drives against emerging threats. These updates are thoroughly tested and validated before deployment to minimize the risk of disruption to industrial operations.

You can look for new firmware versions and update the drive firmware with Drive Composer.

Defense-in-depth measures expected in the environment (SG-2)

Install the drive in a secure location that only authorized persons can access, for example, an area with restricted and monitored access.

ABB recommends that you obey these guidelines to restrict unauthorized access to the drive:

- Set the user lock and change the default password.
- Disable unused Ethernet ports.
- If applicable, disable the Bluetooth function of a connected Bluetooth-enabled control panel.
- Use port blockers to prevent unauthorized connections to the Ethernet and USB connectors of the drive.
- If the drive is in a cabinet, use cabinet locks with unique keys.

In addition to the defense-in-depth measures implemented in the ABB drives, ABB recommends these measures in the installation environment:

1. **Network segmentation**
   Make sure that industrial networks are segmented to isolate critical systems, such as ABB drives, from less secure or non-essential components. This helps contain potential security breaches and decreases the impact of attacks on essential operations.
2. **Firewalls and intrusion detection/prevention systems (IDS/IPS)**
   Install firewalls and IDS/IPS systems at network boundaries and critical junctures to filter and monitor network traffic, and detect and prevent malicious activities in real time.
3. **Endpoint protection**
   Use network endpoint protection, such as antivirus software and endpoint detection and response (EDR) tools, on devices in the industrial network environment to detect and decrease malware threats on ABB drives and other network endpoints.
4. **Security policies and procedures**
   Establish and enforce robust security policies and procedures, such as access control, patch management, and incident response plans.

5. **Employee training and awareness**
   Give training to employees on cyber security best practices, phishing awareness, password hygiene, and social engineering defense. This increases the strength of the human element of defense-in-depth and decreases the risk of insider threats.

6. **Physical security measures**
   Use physical security measures, such as access control, surveillance, and security patrols, to prevent unauthorized access to ABB drives and other critical infrastructure components.

7. **Continuous monitoring and threat intelligence**
   Use continuous monitoring and threat intelligence against new cyber security threats and develop defenses to mitigate emerging risks.

8. **Regulatory compliance**
   Make sure that you comply with the relevant industry regulations and standards, such as NERC CIP, IEC 62443, to have a baseline level of security and demonstrate commitment to protect critical infrastructure assets.

These defense-in-depth measures together with the inherent security features of ABB drives, create a robust security posture that mitigates risks and enhances resilience against cyber threats in industrial environments.

Security hardening guidelines (SG-3)

These security hardening guidelines aim to strengthen the security of the drive with best practices and configurations to mitigate potential vulnerabilities.

Secure hardening recommendations:

1. **User lock**

   Use the user lock to prevent unauthorized access to the drive parameters. Refer to Account management (SG-6) (page 24).

   For information on the user lock, refer to parameters 96.100–96.102 in the drive firmware manual.

2. **Disable services and connectors that are not in use**

   Disable the protocols, services, and connectors on the drive that are not in use. Only enable the protocols and services that you require for the intended use of the drive. For example, disable Drive Composer connectivity over an Ethernet connection if it is not required (parameter 51.15 Service configuration).

   ABB recommends port blockers for connectors that are not in use.

   For information on how to enable and disable protocols, refer to the drive firmware manual.

3. **Firmware updates**

   Regularly update the firmware of the drive with the latest patches and security updates from ABB. Do a test install in a controlled environment before you install them on production systems. You can update the drive firmware with Driver Composer.

4. **Access control**

   Use strong access controls to restrict access to the drive. Use role-based access control (RBAC) to set permissions based on job roles and responsibilities, and limits on access for authorized users. Refer to Account management (SG-6) (page 24).

   Use physical access control for HMI panels and PC account management for Drive Composer.

5. **Physical security**

   Use physical security measures to prevent unauthorized access to the drive, such as a secure enclosure, access control, and surveillance.

Recommendations for periodic security maintenance activities

ABB recommends that you:

- Periodically read the known cyber security vulnerabilities at https://global.abb/group/en/technology/cyber-security/alerts-and-notifications and obey ABB guidelines.
- Regularly update all firmware and software components, even if the release notes do not contain security patches.
- Annually examine the ABB Drives Life Cycle Plan: https://library.abb.com/d/4FPS10000105014. ABB does not make security patches for obsolete products.

- Make periodic backups of the configuration files and data for all of the applicable components in the system.
- Make sure that the clocks of the components in the system do not have drift. Synchronize the clocks regularly.

Secure disposal guidelines (SG-4)

Before you dispose of the drive, return the drive firmware to the factory default state. For more information on how to restore the factory default state of the drive, refer to the drive firmware manual: Select Clear all for parameter 96.06.

For decommissioning and hardware disposal information, refer to the drive hardware manual and drive recycling instructions.

Secure operation guidelines (SG-5)

To make sure that the drive operates correctly with minimum downtime, and is secured against outside threats, ABB recommends that you obey these guidelines:

- Change the default passphrase of the drive during commissioning.
- Keep up-to-date backups of the parameter settings and configuration of the drive.
- Make sure that the embedded Ethernet functionality is configured correctly.
- Do not try to open the enclosure of the drive or remove its seals.

Account management (SG-6)

User roles

The ACS380-E has these roles for access control:

- End user (default)
- Read only (parameter lock active)
- Asset owner (configures the user lock)
- Service role (service access level passcode)
- Fieldbus access

Parameter lock

The converter firmware has a parameter lock. When you activate it with parameter 96.02, it prevents changes to parameter settings through the control panel or Drive Composer. You can use the parameter lock with or without the user lock.

Note: The parameter lock without the user lock is effective only against accidental parameter changes.

To activate or deactivate the parameter lock without the user lock, set parameter 96.02 to value 358.

User lock

Use the user lock to prevent unauthorized parameter changes with a custom passphrase. For detailed information on the user lock, refer to the drive firmware manual.

NOTICE Change the default user passphrase. ABB is not liable for damages or losses caused by the failure to change the default passphrase. Keep the passphrase in a safe place. ABB cannot open the user lock if the passphrase is lost.

Setting a custom passphrase

1. Set parameter 96.02 to value 10000000 (default passphrase). This opens the user lock.
2. Use parameter 96.100 to set the new passphrase. Confirm the passphrase with parameter 96.101.
3. Start the control unit again.
4. Set parameter 96.08 to value 1.

Locking the parameters with a custom passphrase

When a custom passphrase is set, lock the parameters as follows:

1. Enter the correct passphrase into parameter 96.02.
2. Set parameter 96.02 to value 358 to lock the parameters.
3. Set bit 1 of parameter 96.102 to value 1. This prevents a change in the parameter lock state (setting parameter 96.02 to value 358 has no effect).
4. Start the control unit again.
5. Set parameter 96.08 to value 1.

Unlocking the parameters with a custom passphrase

When the parameters are locked with a custom passphrase, unlock the parameters as follows:

1. Enter the correct passphrase into parameter 96.02.
2. Set bit 1 of parameter 96.102 to value 0. This lets you change the state of the parameter lock.
3. Set parameter 96.02 to value 358 to unlock the parameters.

Preventing file downloads with a custom passphrase

When a custom passphrase is set, you can prevent file downloads to the drive control unit. This prevents firmware upgrades and other actions. For more information, refer to the drive firmware manual:

- To disable file downloads, set bit 2 of parameter 96.102 to value 1.
- To enable file downloads, set bit 2 of parameter 96.102 to value 0.

Documentation review (SG-7)

ABB has a user documentation review process, and a process to get feedback on user documentation, including cyber security issues.

If you find a cyber security-related or other issue in the user documentation, send an e-mail to the ABB cyber security mailbox: cybersecurity@ch.abb.com or contact an ABB representative. Give information on the document number and the revision.

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.

a368 (working)
PDF-A4
Created: 2025-05-14, 09:20:07

www.abb.com/drives

3AXD50001145798A