

SIMATIC

Industrial PC SIMATIC IPC BX-35A

Operating Instructions

Preface

Overview

1

Safety instructions

2

Installing and connecting the device

3

Installing OS and SDK components

4

Security

5

Expanding the device

6

Maintaining and repairing the device

7

Technical specifications

8

Technical support

A

Digital I/O and CAN terminal block

B

Markings and symbols

C

List of abbreviations

D

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Preface

These operating instructions contain all the information you need for commissioning and operation of the SIMATIC IPC BX-35A.

It is intended both for programming and testing personnel who commission the device and connect it with other units (automation systems, programming devices), as well as for service and maintenance personnel who install add-ons or carry out fault/error analyses.

Basic knowledge requirements

Background knowledge listed below are required to understand this manual:

- Linux® system or Unix
- NVIDIA® Jetson™ and NVIDIA® tools or SDK components
- Python, docker containers and AI workflow to build the applications

General knowledge in the field of Machine Vision application and automation control engineering is recommended.

Validity of the operating instructions

These operating instructions are valid for all versions of the SIMATIC IPC BX-35A.

The updates of the document will be published on the Siemens Industry Online Support (<https://support.industry.siemens.com/cs/ww/en/view/109744171>).

Scope of this documentation

The documentation for the SIMATIC IPC BX-35A consists of:

- Product information "Important notes on your device"
- SIMATIC Box PC, SIMATIC Panel PC and SIMATIC Rack PC Original Operating Instructions
- SIMATIC IPC BX-35A Quick Install Guide
- SIMATIC IPC BX-35A Operating Instructions (this file)

Conventions

The term "device" is sometimes used to refer to the SIMATIC IPC BX-35A in this documentation.

Figures

This manual contains figures of the described devices. The supplied device may differ in some details from the figures. Within some of the figures, one device is used to represent all devices.

History

The following editions of these operating instructions have been published:

Edition	Comment
04/2024	First edition

Table of contents

	Preface	3
1	Overview.....	9
1.1	Product description.....	9
1.2	Structure of the device.....	10
1.2.1	Views of the device.....	10
1.2.2	Interfaces of the device.....	11
1.2.3	Status displays	12
1.3	Accessories	13
2	Safety instructions	15
2.1	General safety instructions.....	15
2.2	Cybersecurity information.....	18
2.3	Data protection.....	18
2.4	Disclaimer for third-party software updates	18
2.5	Notes on use	19
3	Installing and connecting the device	21
3.1	Preparing for installation.....	21
3.1.1	Checking the delivery.....	21
3.1.2	Identification data of the device	22
3.1.3	Permitted mounting positions and mounting types	23
3.2	Mounting the device.....	24
3.2.1	Mounting instructions.....	24
3.2.2	Mounting on DIN rails	26
3.2.3	Wall mounting	27
3.3	Connecting the device	28
3.3.1	Notes on connecting.....	28
3.3.2	Connecting the protective conductor	29
3.3.3	Connecting the power supply.....	30
4	Installing OS and SDK components	33
4.1	Installing Jetson™ Linux® with Support Package Manager.....	33
4.1.1	Support Package Manager introduction	33
4.1.2	Downloading Support Package Manager	34
4.1.3	Installing Support Package Manager	34
4.1.4	Installing JetPack Operating System	35
4.2	Installing the Jetson™ SDK components	35
4.3	Adjusting power and performance	35
5	Security.....	39

5.1	Security Features	39
5.1.1	Secure boot	39
5.1.2	Disk encryption	40
5.2	Enabling the Security Features	40
5.2.1	Preparing keys	42
5.2.2	Creating PKC hash by SPM.....	44
5.2.3	Creating the fuse configuration file	44
5.2.4	Verifying the fuse configuration file	46
5.2.5	Burning fuse by SPM	47
5.2.6	Installing secured images.....	48
5.2.6.1	Installing the OS image with UEFI Secureboot	48
5.2.6.2	Installing the OS image with UEFI Payload Encryption, Disk Encryption	50
5.3	Revoking the PKC key.....	53
6	Expanding the device	55
6.1	Installing the M.2 module	55
6.2	Inserting the Nano SIM card	57
6.3	Installing the SSD.....	58
6.4	Installing the SOM	60
7	Maintaining and repairing the device	63
7.1	Maintenance	63
7.2	Repair information.....	63
7.3	Replacing the backup battery	64
7.4	Recycling and disposal	66
8	Technical specifications.....	67
8.1	Certificates and approvals	67
8.2	Directives and declarations	71
8.2.1	Electromagnetic compatibility, Industrial and Residential Areas	71
8.2.2	RoHS directive	71
8.2.3	ESD guideline	71
8.3	Dimension drawings	74
8.4	General technical specifications	75
8.5	Ambient conditions	77
8.6	Power demand of the components.....	79
8.7	Direct current supply (DC).....	79
8.8	Hardware descriptions	80
8.8.1	Motherboard	80
8.8.2	External Interfaces.....	81
8.8.2.1	Overview of external interfaces.....	81
8.8.2.2	Power supply	81
8.8.2.3	Digital I/O connector	82
8.8.2.4	USB	84
8.8.2.5	DisplayPort	85

8.8.2.6	Ethernet port	86
8.8.2.7	Serial port.....	86
8.8.2.8	CAN port.....	88
8.8.3	Internal interfaces.....	88
8.8.3.1	Overview of internal interfaces	88
8.8.3.2	M.2 interface	88
A	Technical support	93
A.1	Service and support	93
A.2	Troubleshooting	94
B	Digital I/O and CAN terminal block	95
C	Markings and symbols.....	97
C.1	Overview	97
C.2	Safety.....	97
C.3	Operator controls.....	97
C.4	Certificates, approvals and markings	98
C.5	Interfaces	99
D	List of abbreviations	101
	Index.....	103

Overview

1.1 Product description



Features

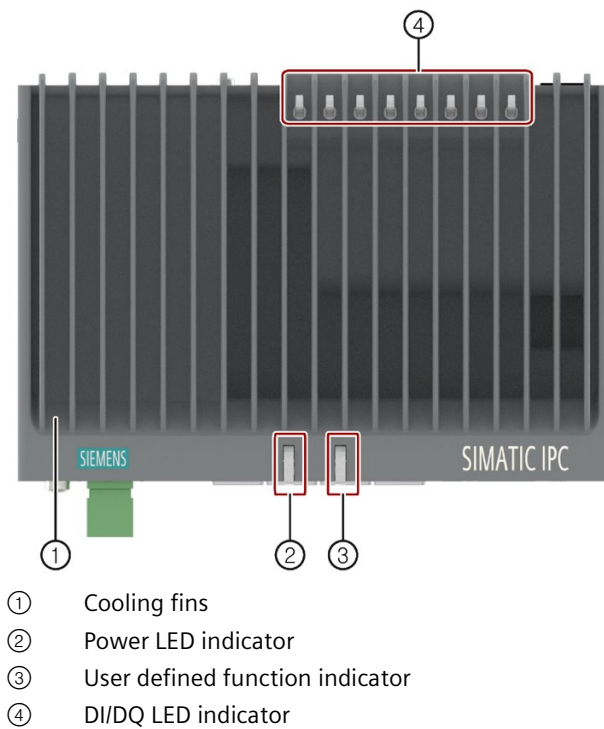
SIMATIC IPC BX-35A is powered by the NVIDIA® Jetson™ Orin NX module. It's a new generation of embedded edge computing products for high AI performance. It provides high-level industrial functionality, flexible expansion ability and a compact form factor for installation. It can be widely used in industrial artificial intelligence inference, machine vision, AGVs.

- Maintenance-free operation possibility
- High performance and compact design
- Fanless but wide temperature range for industrial use case
- Vibration resilience performance
- 4 LAN ports with up to 30W PoE
- Various interfaces: CAN, DI/DQ, COM, USB 3.0
- High expansibility: M.2 B key and M.2 E key
- Wide choice of connectors and storage: support up to 1TB M.2 SSD, M.2 B key support 4G/5G cellular network and flex module (optional)

1.2 Structure of the device

1.2.1 Views of the device

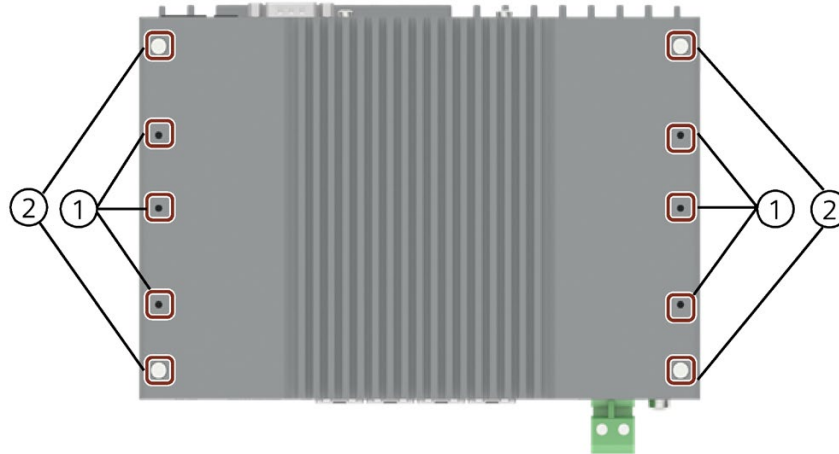
Front view



Side view

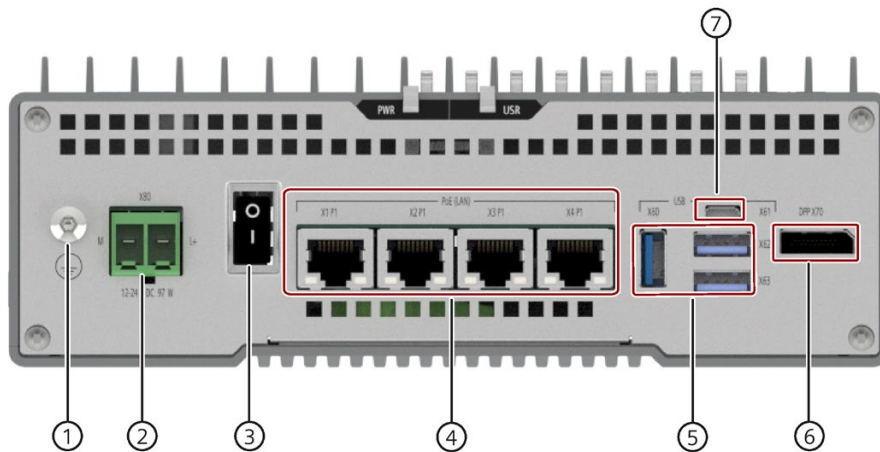


Rear view



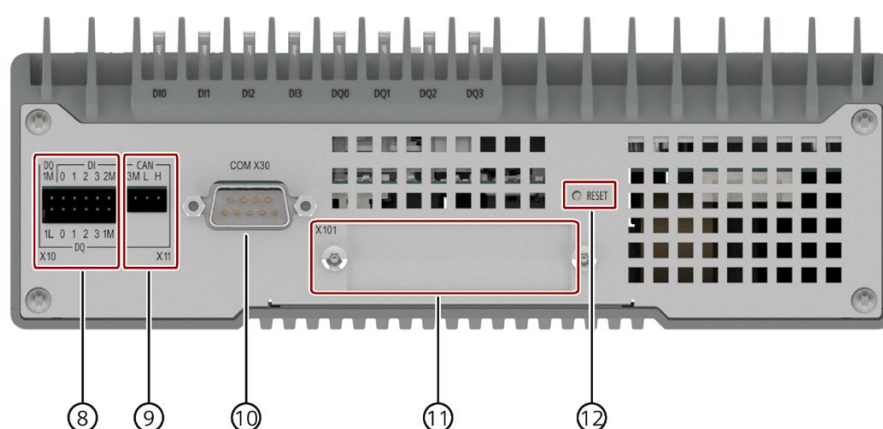
- ① Mounting screws
- ② Rear cover screws

1.2.2 Interfaces of the device



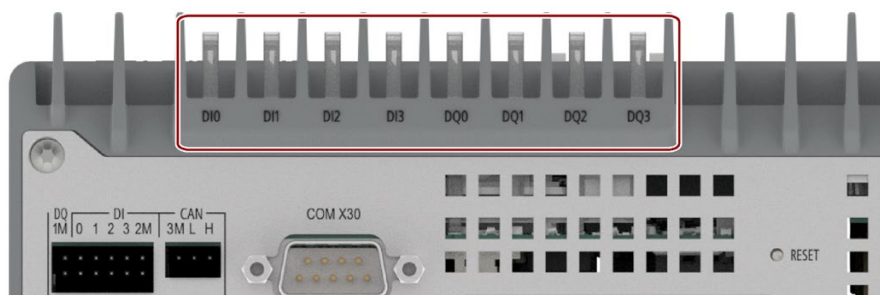
- | | |
|------------------------------|--|
| ① Protective conductor | Connection for protective conductor |
| ② Power supply (X80) | Connection for a DC 12-24 V (9-36 V) power supply |
| ③ On/Off switch | Switch position: " " for power on; " O " for power off. |
| ④ LAN (X1P1/X2P1/X3P1/X4P1) | 4 × RJ45 Ethernet connections for 10/100/1000 Mbps with PSE power supply |
| ⑤ USB 3.0 port (X60/X62/X63) | 3 × USB 3.0 Type A, high current |
| ⑥ DPP (X70) | 1 × DisplayPort connection |
| ⑦ USB 2.0 port (X61) | 1 × USB 2.0 Micro B port, device mode only |

1.2 Structure of the device

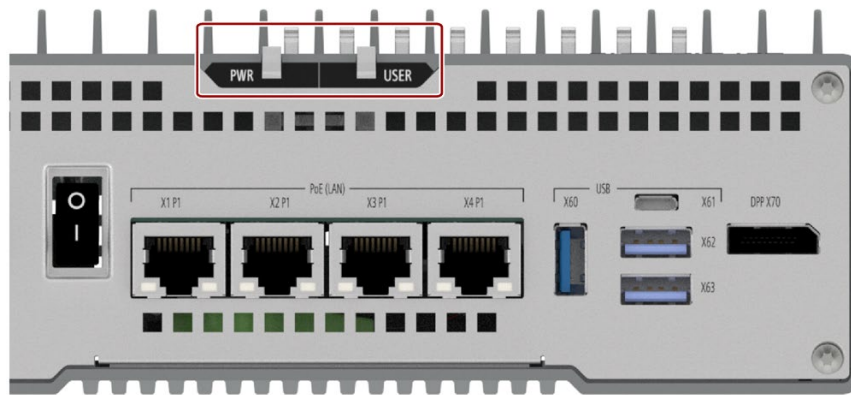


- ⑧ Digital I/O Connector (X10) 4 × DI + 4 × DQ
- ⑨ CAN Connector (X11) CAN BUS connector
- ⑩ COM (X30) 1 × Serial interface, 9-pin RS232/RS422/RS485 D-sub connector
- ⑪ Reserved (X101) Reserved for flex module
- ⑫ RESET button Reset the device or enter RCM (Recover Mode) when power on

1.2.3 Status displays



LED	State	Description
DI0 / DI1/DI2 /DI3	Off	Digital input no data transmission or data transmission low.
	Green	Digital input data transmission high.
DQ0 /DQ1/DQ2/DQ3	Off	Digital output data transmission low.
	Green	Digital output data transmission high.



LED	State	Description
PWR	Off	Power off
	RED	Power on, system off
	Green	System running
	Orange	System sleep
USER	Off/Red/Green/Orange	Customizable

1.3 Accessories

Accessories from Siemens are available for your device. These are not included in the scope of delivery.

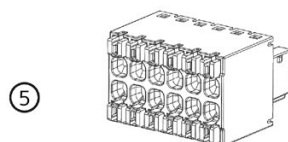
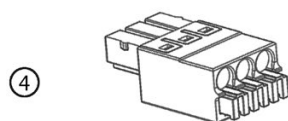
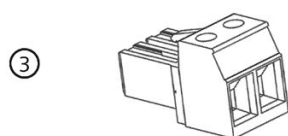
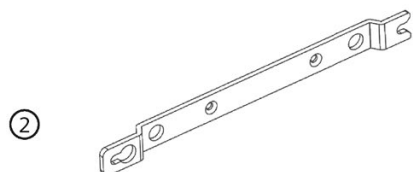
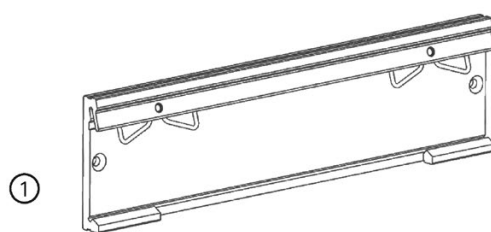
Additional accessories can be found on the Internet:

- Industry mall (<https://mall.industry.siemens.com>)
- Expansion components and accessories (<https://new.siemens.com/global/en/products/automation/pc-based.html>)

Mounting accessory kit

The mounting accessory kit contains:

- One standard rail bracket ①
- Two wall mounting brackets ②
- One DC connecting terminal block ③
- One CAN plug ④
- One DI/DQ plug ⑤
- Six M3 screws



Safety instructions

2.1 General safety instructions

WARNING

Life-threatening voltages are present with an open control cabinet

When you install the device in a control cabinet, some areas or components in the open control cabinet might be carrying life-threatening voltages.

If you touch these areas or components, you might be killed by electric shock.

Switch off the power supply to the cabinet before opening it.

System expansions

NOTICE

Damage through system expansions

Device and system expansions might be faulty and can affect the entire machine or plant.

The installation of expansions can damage the device, machine or plant. Device and system expansions might violate safety rules and regulations regarding radio interference suppression. If you install or exchange system expansions and damage your device, the warranty becomes void.

Note the following for system expansions:

- Only install system expansion devices designed for this device. Contact your technical support team or where you purchased your PC to find out which system expansion devices can safely be installed.
- Observe the information on electromagnetic compatibility (Page 75).

WARNING

Risk of fire through expansion cards

Expansion cards generate additional heat. The device may overheat and cause a fire.

Note the following:

- Observe the safety and installation instructions for the expansion cards.

NOTICE
Use in the scope of application for the IEC/UL/EN 61010-2-201
When the device is used in the area of Industrial Control Equipment in accordance with IEC/UL/EN 61010-2-201, note that the device is classified as "Enclosed equipment".
If the device is used in a manner not specified by the manufacturer, the approval is lost and the protection associated with it may be impaired.

Note

Limitation of liability

All technical specifications and approvals of the device only apply if you use expansion components that have a valid CE approval (CE mark). The installation conditions for expansion components in the associated documentation must be observed.

UL approval of the device only applies when the UL-approved components are used according to their "Conditions of Acceptability".

We are not liable for functional limitations caused by using of third-party devices or components.

NOTICE
The approvals are voided if certain modifications are made
The device approvals are voided if the following modifications are made:
• The enclosure was physically modified, for example, openings were created to make LEDs on a plug-in card in the device visible. • Cables are routed from the inside out of the device or from the outside into the device, for example, to connect sensors or displays.

Battery and rechargeable battery

WARNING

Risk of explosion and release of harmful substances

Improper handling of lithium batteries can result in an explosion of the batteries.

Explosion of the batteries and the released pollutants can cause severe physical injury. Worn batteries jeopardize the function of the device.

Note the following when handling lithium batteries:

- Replace used batteries in good time; see the section "Replacing the backup battery" in the operating instructions.
- Replace the lithium battery only with an identical battery or types recommended by the manufacturer (article number: A5E34734290).
- Do not throw lithium batteries into fire, do not solder on the cell body, do not recharge, do not open, do not short-circuit, do not reverse polarity, do not heat above 100°C and protect from direct sunlight, moisture and condensation.

Strong high-frequency radiation

NOTICE

Observe immunity to RF radiation

The device has an increased immunity to RF radiation according to the specifications on electromagnetic compatibility in the technical specifications.

Radiation exposure in excess of the specified immunity limits can impair device functions, result in malfunctions and therefore injuries or damages.

Read the information on immunity to RF radiation in the technical specifications.

ESD Guideline



Electrostatic sensitive devices can be labeled with an appropriate symbol.

NOTICE

Electrostatic sensitive devices (ESD)

When you touch electrostatic sensitive components, you can destroy them through voltages that are far below the human perception threshold.

If you work with components that can be destroyed by electrostatic discharge, observe the ESD Guideline (Page 71).

2.2 Cybersecurity information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines, and networks.

In order to protect plants, systems, machines, and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For more information on protective industrial cybersecurity measures for implementation, please visit (<https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html>).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates at all times, subscribe to the Siemens Industrial Cybersecurity RSS Feed under (<https://new.siemens.com/global/en/products/services/cert.html>).

2.3 Data protection

Siemens observes the data protection guidelines, especially the requirements regarding data minimization (privacy by design). This means the following for this SIMATIC product: The product does not process / save any personal information, but only technical functional data (e.g. time stamps). If the user links this data to other data (e.g. shift plans) or if the user saves personal information on the same medium (e.g. hard disk) and therefore creates a personal reference in the process, the user has to ensure meeting the guidelines regarding data protection.

2.4 Disclaimer for third-party software updates

This product includes third-party software. Siemens AG only provides a warranty for updates/patches of the third-party software, if these have been distributed as part of a Siemens software update service contract or officially released by Siemens AG. Otherwise, updates/patches are undertaken at your own risk. You can find more information about our Software Update Service offer on the Internet at Software Update Service (<https://new.siemens.com/us/en.html>).

2.5 Notes on use

NOTICE

Possible functional restrictions in case of non-validated plant operation

The device is tested and certified based on the technical standards. In rare cases, functional restrictions can occur during plant operation.

Validate the correct functioning of the plant to avoid functional restrictions.

Note

Use in an industrial environment without additional protective measures

This device is designed for use in a normal industrial environment according to IEC 60721-3-3.

WARNING

為避免電磁干擾，本產品不應安裝或使用於住宅環境。

Disclaimer

Please note that the following list of recommended risk-minimizing security measures is not intended to be exhaustive. Thus, please consult your security expert for final assessment and configuration. Further, as already mentioned in Hotspot-Text (<https://www.siemens.com/industrialsecurity>).

Please note (i) that you are responsible for preventing unauthorized access to your plants, systems, machines, and networks, and (ii) that you should only connect such systems, machines, and components to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Since you are solely responsible for the conception, implementation, and maintenance of a holistic, state-of-the-art security concept to protect your enterprise, factories/plants, systems, machines, and networks (including the products) against cyberthreats, you are liable for any damage caused by implementing no or insufficient security measures.

Security notification

Siemens recommends that you observe the following security practices:

- Enable Secure boot feature to the first stage of boot/kernel/DTB to prevent attack.
- Use SHA512 algorithm for public key hash collision.
- Use RSA-3K/ECDSA P-256/ECDSA P-512 algorithm and preserve it in a secured location for private key.
- Ensure that only the authorized person can access the private key.
- Use access control practice for private key.

- Ensure the integrity during production.
- Follow the general security rules for networks.
- Install a hardware firewall before connecting to the internet. Install software firewall on the device and open necessary ports only.
- Deploy data leakage protection (DLP) across your system to protect sensitive data.
- Install the device in separated rooms or controlled areas. Restrict the access to the device with a lock, if possible.
- Only authorized personnel can access the device.
- Only access secured wireless networks using secured software/hardware components.
- Use separate accounts for admin tasks and user tasks.
- Only install software components from trusted sources.
- Change the system password regularly.
- The device can be identified by collecting MAC/UID information from the system.

Installing and connecting the device

3.1 Preparing for installation

3.1.1 Checking the delivery

Procedure

1. When accepting a delivery, please check the packaging for visible transport damage.
2. If any transport damage is present at the time of delivery, lodge a complaint at the shipping company in charge. Have the shipper confirm the transport damage immediately.
3. Unpack the device at its installation location.
4. Keep the original packaging, in case you have to transport the unit again.

Note

Damage to the device during transport and storage

If a device is transported or stored without packaging, shocks, vibrations, pressure and moisture may impact the unprotected unit. A damaged packaging indicates that ambient conditions have already had a massive impact on the device.

The device might be damaged.

Do not dispose of the original packaging. Pack the device during transportation and storage.

5. Check the contents of the packaging and any accessories you may have ordered for completeness and damage.
 - Device
 - One mounting accessory kit includes: one standard rail bracket, two wall mounting brackets, one DC connecting terminal block, one CAN plug, one DI/DQ plug and six M3 screws.
6. If the contents of the packaging are incomplete, damaged, or do not match your order, inform the responsible delivery service immediately.

 WARNING

Electric shock and fire hazard due to damaged device

A damaged device can be under hazardous voltage and trigger a fire in the machine or plant. A damaged device has unpredictable properties and states.

Death or serious injury could occur.

- Make sure that the damaged device is not installed or put into operation.
- Label the damaged device and keep it locked away.
- Send off the device for immediate repair.

3.1 Preparing for installation

NOTICE**Damage from condensation**

If the device is subjected to low temperatures or extreme fluctuations in temperature during transportation, for example in cold weather, moisture could build up on or inside the device.

Moisture causes a short circuit in electrical circuits and damages the device.

In order to prevent damage to the device, proceed as follows:

- Operate and store the device in a dry location.
- Bring the device to room temperature before starting it up.
- Do not expose the device to direct heat radiation from a heating device.
- If condensation develops, wait approximately 12 hours or until the device is completely dry before switching it on.

7. Keep the enclosed documentation in a safe place. You need the documentation when you commission the device for the first time or meet other problems.
8. Record the identification data of the device.

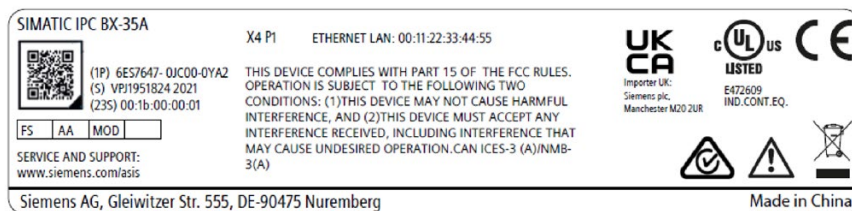
3.1.2 Identification data of the device

The device can be clearly identified with the help of this identification data in case of repairs or theft.

You can find this information on the rating plate. The following illustration shows an example.

Enter the identification data in the table below:	
Order number	6ES7647-OJC...-....
Serial number	S V
Production version	FS
All existing Ethernet addresses (MAC)	

The following image shows the product label on the SIMATIC IPC BX-35A as an example.

**ID link**

The ID link is a globally unique identifier according to IEC 61406, which you can find as a QR code on the product and product packaging. You can recognize the ID link by the frame with a black frame corner at the bottom left. After scanning the QR code on the product or on the packaging label with a smartphone camera, barcode scanner or reader app, the ID link takes

you to the digital nameplate of your products, where you can look through the following information:

Manuals: Quick Install Guide, Operating Instructions and Original Instructions

Certificates

Technical data

FAQ information

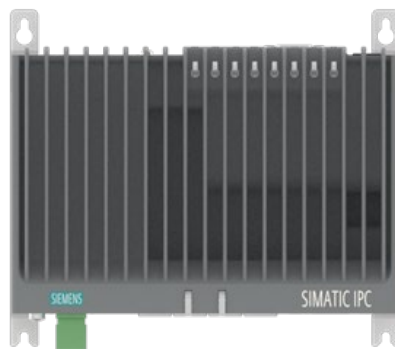
Product notes

3.1.3 Permitted mounting positions and mounting types

The device can be mounted horizontally on a DIN rail or to a wall.

For the permitted temperature range for operation on the mounting positions, refer to the "Technical specifications (Page 67)" section.

Wall mounting



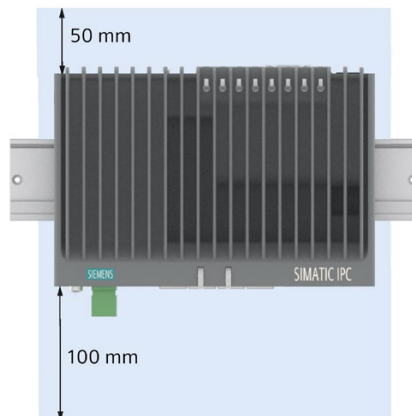
Mounting on DIN rails



Clearances

Ensure that the following clearances measurements to another component or to a wall of a housing are complied with:

- Below the device: ≥ 100 mm
- Above the device: ≥ 50 mm



3.2 Mounting the device

3.2.1 Mounting instructions

Note

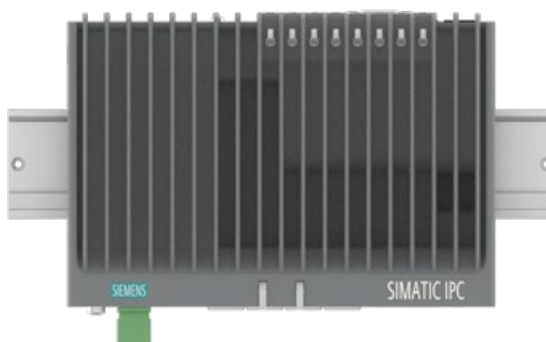
If the equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment might be impaired.

Note the following:

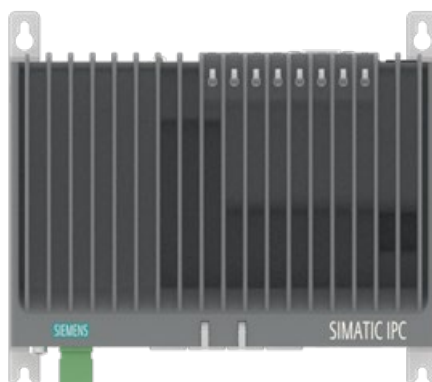
- The device is approved for indoor operation only.
- When the device is used in the area of Industrial Control Equipment in accordance with UL61010-2-201, the device is classified as "Enclosed equipment".
- Install the device only as one of the described permitted mounting positions.
- For installation of the control cabinet, observe the country-specific regulations.
- All external circuits of the device must be safe extra low voltage (SELV) circuits.
- All signal cables except DI/DQ are shielded.
- This device is designed for use in a normal industrial environment. Without additional protective measures (such as the provision of clean air), SIMATIC Box PCs may not be operated in harsh environments that are subject to caustic vapors or gases.

Possible mounting types of the device:

Mounting on DIN rails



Wall mounting



Fasten securely**NOTICE****Insufficient load carrying capacity**

If the mounting surface for wall mounting does not have enough load-bearing capacity, the device may fall and be damaged.

Ensure that the mounting surface on the wall can bear four times the total weight of the device, including fixing elements.

NOTICE**Incorrect fixing elements**

If you use anchors and screws other than those specified in the following table for wall mounting, safe mounting is not guaranteed. The device can fall and may be damaged.

Only use the anchors and screws specified in the following table.

Material	Bore diameter	Fixing element
Concrete	Select according to the specification of the mounting elements used	- Anchor, Ø 6 mm, 40 mm long - Screw, Ø 4 mm, 40 mm long
Plasterboard, (at least 13 mm thick)		Toggle plug, Ø 12 mm, 50 mm long
Metal, (at least 2 mm thick)		- Screw M4 × 15 - M4 nut

**WARNING****Personal injuries or material damage in the case of insufficient load-bearing capacity of wall**

The device could fall if the wall to which it is mounted has insufficient load-bearing capacity. This can result in personal injuries or material damage.

Ensure that the wall is capable of bearing four times the total weight of the device (including the brackets and expansion modules). The total weight of the device is approximately 1.76 kg.

3.2.2 Mounting on DIN rails

Mounting on a standard rail is suitable for horizontal mounting of the device.

Requirements

- A SIEMENS 35 mm standard rail TH35-15 conforming to EN 60715:2001
The standard rail is mounted.
- A standard rail bracket
The standard rail bracket and two screws are included.
- A T10 screwdriver

Procedure for mounting



- 1 Lay the standard rail bracket on the rear of the device.
- 2 Fasten the standard rail bracket with 2 screws.
- 3 Place the device with the standard rail bracket onto the mounting rail from above.
If the device is tilted when you place it down, the standard rail bracket does not grip.
- 4 Press the device down and toward the standard rail until the standard rail bracket engages.
- 5 Check whether the device is seated firmly on the standard rail.

Procedure for dismantling

1. Press the device down until the lower rail guide frees the device.
2. Swing the device out of the rails.
3. Remove the rail from the device.

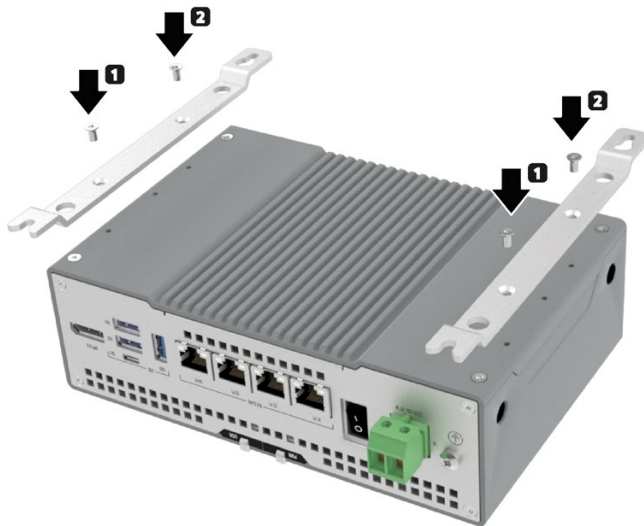
3.2.3 Wall mounting

Wall mounting is one of the horizontal mounting types.

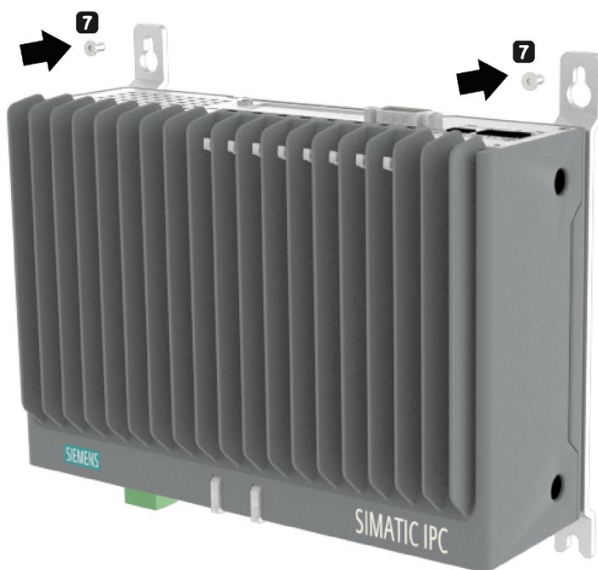
Requirements

- Two mounting brackets
The mounting brackets and four screws are included.
- A T10 screwdriver
- Four anchors and four screws

Procedure for mounting



- 1** Place the mounting bracket on the rear of the device.
- 2** Secure each of the mounting brackets with 2 screws.
- 3** Place the device with the mounting brackets onto the mounting surface.
- 4** Mark the fixing holes.



- 5** Drill the fixing holes.
- 6** Insert the anchors in the drilled holes.
- 7** Screw on the device.

3.3 Connecting the device

3.3.1 Notes on connecting

WARNING

Risk of fire and electric shock

The on/off switch does not isolate the device from the power supply. Risk of electric shock exists if the device is opened incorrectly or defective. There is also a risk of fire if the device or connecting lines are damaged. This can result in death or serious injury.

You should therefore protect the device as follows:

- Always pull out the power plug when you are not using the device, or if the device is defective. The power plug must be freely accessible.
- Use a central power isolating switch for cabinet installation.

WARNING

Risk of lightning strikes

A lightning surge may enter the power cables and data transmission cables and jump to a person.

Death, serious injury, and burns can be caused by lightning.

Take the following precautions:

- Disconnect the device from the power supply when a thunderstorm is approaching.
- Do not touch power cables and data transmission cables during a thunderstorm.
- Keep a sufficient distance from electric cables, distributors, and systems.

NOTICE

Fault caused by I/O devices

The connection of I/O devices can cause faults in the device.

The result might be personal injury and damage to the machine or plant.

Note the following when connecting I/O devices:

- Read the documentation of the I/O devices. Follow all instructions in the documentation.
- Only connect I/O devices which are approved for industrial applications in accordance with EN 61000-6-2 and IEC 61000-6-2.
- I/O devices that are not hot-pluggable may only be connected after the device has been disconnected from the power supply.

NOTICE**Damage through regenerative feedback**

Regenerative feedback of voltage to ground by a connected or installed component can damage the device.

Connected or built-in I/Os, for example, a USB drive, are not permitted to supply any voltage to the device. Regenerative feedback is generally not permitted.

**CAUTION****Use copper cables at connectors with terminal connections**

Use copper (Cu) cables for all supply lines that are connected to the device with terminals, e.g. 24 V DC power supply cables to the 24 V DC power supply connectors.

Utiliser des câbles en cuivre sur les connexions à bornes

Utilisez des câbles en cuivre (Cu) pour tous les câbles d'alimentation qui sont raccordés à l'appareil par des bornes, par exemple les câbles d'alimentation 24 V CC sur le connecteur d'alimentation 24 V CC.

NOTICE**Ferrite required at USB cables**

The interference immunity of the device according to the data in the technical specifications is only guaranteed when the cables at USB and micro USB ports are equipped with a ferrite magnet. Only use USB cables equipped with a ferrite magnet.

3.3.2 Connecting the protective conductor

A connected protective conductor discharges dangerous electrical charges from the metal enclosure. The current flowing through the protective conductor when such a fault occurs triggers an upstream protective device that disconnects the machine from the power supply.

The protective conductor also improves the discharge of interference generated by external power cables, signal cables or cables for I/O modules to ground.

The connection for the protective conductor is labeled with the following symbol:

**WARNING****Electric shock and risk of fire**

High voltage may be present in a defective device, which can cause fire or an electric shock if touched. This can result in death or serious injury.

- Connect the device to the protective conductor before you put it into operation.
- The PE terminal on the device must be connected to the protective conductor of the control cabinet or system in which the device is installed.
- Never operate the device without a protective conductor.
- If a device is defective, remove it from operation without delay and label it accordingly.

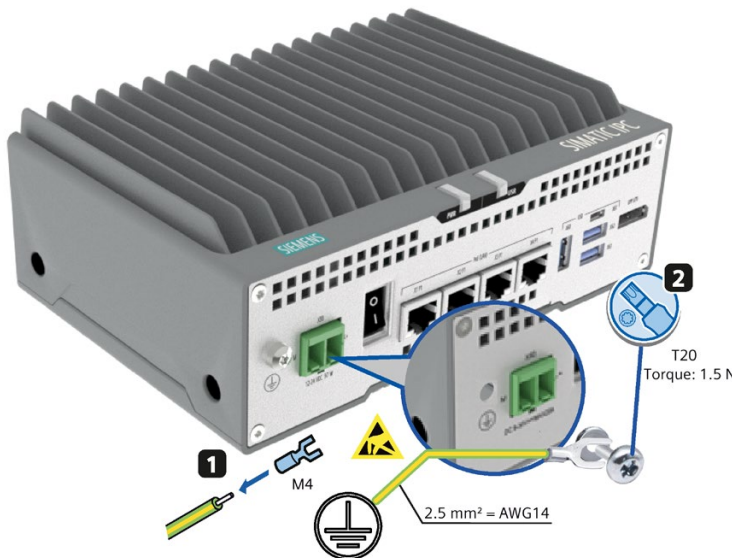
Note

The external bonding facility should provide effective connection of a conductor with a cross sectional area of at least 4 mm².

Requirements

- T20 screwdriver
- Cable lug for M4
- Protective conductor with minimum cross-section of 2.5 mm² copper cable (AWG14)

Procedure



- 1 Clamp the cable lug on the protective conductor.
- 2 Firmly attach the cable lug to the protective conductor connection on the device using the M4 thread with the torque of 1.5 Nm (see part labeled). Connect the protective conductor to the protective conductor connection of the cabinet or the plant in which the device is installed.

3.3.3 Connecting the power supply

Note

Approval in accordance with IEC/EN/UL61010:

- The device may only be connected to a DC 24 V power supply that meets the requirements of safe extra-low voltage (SELV/PELV) in accordance with the IEC/UL/EN/DIN-EN 61010-2-201 standard. The power supply must meet the Limited Energy requirement as specified in IEC/UL/EN/DIN-EN 61010-2-201.
 - If the device is installed in an enclosure that complies with section 9.3.2. c) of IEC/UL/EN/DIN-EN 61010-1 and IEC/UL/EN/DIN-EN 61010-2-201, the unit can be powered from a source "greater than NEC Class 2 / Limited Energy". The device is then classified as "OPEN EQUIPMENT".
-

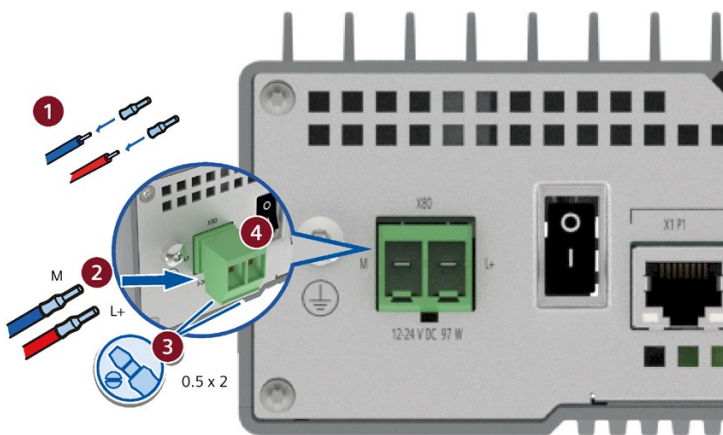
Note

The power supply must be adapted to the input data of the device, see chapter "General technical specifications (Page 75)".

If there are voltage peaks on power supply lines, use a protective device in the form of a varistor (MOV) UMOV = U-rated x 1.2 (BLITZDUCTOR BVT AVD 24 (918 422) or compatible).

Requirements

- The protective conductor is connected.
- You are using the supplied terminal.
- A two-core cable meet the following requirements:
 - a copper (Cu) cable with minimum cross-section of 2.1 mm² to 4.0 mm²
 - rated temperature 75 °C
- Tightening torque: 0.56 Nm
- A slotted screwdriver with a 3 mm blade.

Procedure

- 1** Connect the two-core cable to the cable head separately.
- 2** Connect the cable heads to the power supply terminal block.
- 3** Tighten the screws on the terminal block at shown.
- 4** Plug the terminal block into the power supply interface X80.

Installing OS and SDK components

4.1 Installing Jetson™ Linux® with Support Package Manager

4.1.1 Support Package Manager introduction

Support Package Manager (SPM) is designed to simplify firmware and OS installation for IPC BX-35A. You can use a host PC with Ubuntu® 20.04 or Ubuntu® 18.04 to install JetPack OS to IPC BX-35A NVME SSD.

Note

- The procedure described in this chapter is only available for the device without pre-installed industrial OS.
 - The latest supported JetPack version can be checked by command `sudo ./SPM -l`.
 - When installing JetPack OS image to NVME SSD on IPC BX-35A, SPM will erase all existing data on the BX-35A's storage devices, including the QSPI flash on the SOM and the NVME SSD. And the Siemens Support Package will be installed automatically.
 - Siemens recommends you use SPM to install Jetson™ Linux® on IPC BX-35A. If you use other tools for the installation, certain functions of IPC BX-35A might not work properly.
-

Available SPM command lines

```
sudo ./SPM [options] <product> <JetPack Version> <rootdev>
```

[options]:

- `-h, --help`: list all command lines
- `-c, --clean`: clean the old workshop
- `-l, --list`: list all supported JetPack version
- `--firmware-only`: only install firmware without OS image
- `--offline`: install to a USB storage device which is connected to the host without the IPC BX-35A connected

<product>:

Specify the target product to be burned. Optional value is *BX-35A* or *bx-35a*.

<JetPack Version>:

Specify JetPack version. For IPC BX-35A, optional value is:

- `jp5.1.2`: specify to use JetPack 5.1.2

4.1 Installing Jetson™ Linux® with Support Package Manager

<rootdev>:

Specify the storage media where OS will be installed. For IPC BX-35A, optional value is NVME.

For example: `sudo ./SPM BX-35A jp5.1.2 NVME`

4.1.2 Downloading Support Package Manager

Support Package Manager (SPM) is published on Siemens Industry Online Support website. To download SPM, log in to Siemens Industry Online Support website (<https://support.industry.siemens.com/cs/ww/en/view/109783704>). Find and click on the **SIMATIC IPC520A / IPC BX-35A** entry.

NOTICE

If you do not yet have an account to log in to the website, click "Register" at the top right of the window and follow the registration instructions.

[> Register](#) [> Login](#) [\[?\]](#)

4.1.3 Installing Support Package Manager

Requirements

- A host PC for installing the SPM:
 - with Ubuntu® 18.04 or Ubuntu® 20.04 installed
 - at least 60 GB free storage
 - stable network connection

Procedure - installing SPM to the host PC

1. Download SPM (Page 34) to the host PC.
2. Open the terminal (Ctrl + Alt + T) and switch to SPM file path.

For example, switch to SPM file path with command:

```
cd /usr/bin/<SPM_file_saved_directory>
```

3. Use command with SPM file name to extract SPM file.

For example, if the SPM file name is `SPM-Tool_V02.00.00.tar.xz`, run command:

```
tar -xpf SPM-Tool_V02.00.00.tar.xz
```

```
cd SPM-Tool_V02.00.00
```

4.1.4 Installing JetPack Operating System

Procedure

1. Connect IPC BX-35A and the host PC with a **USB-Type-A to USB-Micro-B cable**.
2. Connect IPC BX-35A and a monitor with a DP cable.
3. Ensure IPC BX-35A is shut down.
4. Press and hold `RESET` key, then power on IPC BX-35A. Release `RESET` after power LED has been on for 3s, then IPC BX-35A enters recovery mode (RCM).
5. Enter below command to start the installation:

```
$ sudo ./SPM bx-35a jp5.1.2 nvme
```

If the installation process is successful, IPC BX-35A will restart automatically.

4.2 Installing the Jetson™ SDK components

IPC BX-35A supports more features such as AI computing and big data processing. You need to install the Jetson™ SDK components to enable the features.

Requirements

- Ubuntu® Jetson™ Linux® is installed in the device (IPC BX-35A).

Procedure - installing the Jetson™ SDK components

1. Connect IPC BX-35A to a wireless or wired network.
2. Open the terminal (Ctrl + Alt + T) and enter below commands:

```
$ sudo apt update
```

```
$ sudo apt install -y nvidia-jetpack
```

4.3 Adjusting power and performance

The default power mode configuration for BX-35A is 15W mode. NVIDIA® offers the `powerestimator` tool to adjust the power and performance according to your specific needs. For detailed information, please refer to the official NVIDIA® documentation (<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/PlatformPowerAndPerformance/JetsonOrinNanoSeriesJetsonOrinNxSeriesAndJetsonAgxOrinSeries.html>).

The `powerestimator` tool is a web application. It can calculate the power consumption and generate the configuration file based on the given resource requirements. To access the tool, please visit NVIDIA® power estimator (<https://jetson-tools.nvidia.com/powerestimator/>).

Note

- The power calculated by the `powerestimator` should not exceed the maximum power budget claimed by the product.
- To access the `powerestimator`, you will need to log in to your NVIDIA® account. If you do not have an NVIDIA® account, please register for one before accessing and using this tool.

Procedure - Generating and applying the custom configuration

1. Log in to NVIDIA® power estimator (<https://jetson-tools.nvidia.com/powerestimator/>).
2. Select your device from the **Select Platform** dropdown menu:
 - for the BX-35A 16GB version, select **Jetson-Orin-NX-16G**
 - for the BX-35A 8GB version, select **Jetson-Orin-NX-8G**
3. Select **25W** from the **Power Modes** dropdown menu.
4. Adjust the CPU quantity, frequency, and load, the GPU frequency and load, and any other resources according to your needs.
5. Click **Estimate Power** to calculate the power consumption.
6. Click **Download** to download the `nvpmode1.conf` configuration file.
7. Login to your BX-35A device, and access the local `nvpmode1.conf` file on your device by inputting the following command:

```
$ cat /etc/nvpmode1.conf
```

8. Locate the `< POWER_MODEL >` line in the local `nvpmode1.conf` file, and locate the current max value of `POWER_MODEL ID=`. Add 1 to the current max value and record it.
 For example, in the local `nvpmode1.conf` file, if you locate 4 command lines starting with `< POWER_MODEL >` line, and the max value of ID value is `< POWER_MODEL ID=3 NAME=25W >`, you should record the value **4** (current max value 3 + 1).
9. Locate the `< POWER_MODEL >` section in the `nvpmode1.conf` file downloaded in step 6, and replace the value of `POWER_MODEL ID=` with the ID value recorded in step 8.

For example, in the downloaded `nvpmode1.conf` file, if you locate the below section, you should replace the ID value **0** with the value **4**:

```
< POWER_MODEL ID=0 NAME=MODE_22_9_W >
CPU_ONLINE CORE_0 1
CPU_ONLINE CORE_1 1
CPU_ONLINE CORE_2 1
CPU_ONLINE CORE_3 1
CPU_ONLINE CORE_4 1
CPU_ONLINE CORE_5 1
CPU_ONLINE CORE_6 0
CPU_ONLINE CORE_7 0
```

```
FBP_POWER_GATING FBP_PG_MASK 2
TPC_POWER_GATING TPC_PG_MASK 240
GPU_POWER_CONTROL_ENABLE GPU_PWR_CNTL_EN on
CPU_A78_0 MIN_FREQ 729600
CPU_A78_0 MAX_FREQ 1497600
CPU_A78_1 MIN_FREQ 729600
CPU_A78_1 MAX_FREQ 1497600
GPU MIN_FREQ 0
GPU MAX_FREQ 918000000
GPU_POWER_CONTROL_DISABLE GPU_PWR_CNTL_DIS auto
EMC MAX_FREQ 0
DLA0_CORE MAX_FREQ 614400000
DLA1_CORE MAX_FREQ 614400000
DLA0_FALCON MAX_FREQ 294400000
DLA1_FALCON MAX_FREQ 294400000
PVA0_VPS MAX_FREQ 512000000
PVA0_AXI MAX_FREQ 358400000
```

10. Locate the `< PM_CONFIG DEFAULT >` line in the local `nvpmodel.conf` file. Append the modified `< POWER_MODEL >` section in step 9 before the `< PM_CONFIG DEFAULT >` line, and save the file.

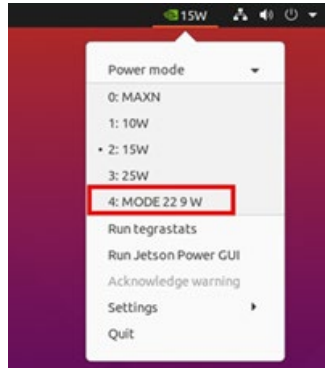
For example, append the modified `< POWER_MODEL >` section in step 9 to the local `nvpmodel.conf` file as below:

```
#The custom config
< POWER_MODEL ID=4 NAME=MODE_22_9_W >
CPU_ONLINE CORE_0 1
CPU_ONLINE CORE_1 1
CPU_ONLINE CORE_2 1
CPU_ONLINE CORE_3 1
CPU_ONLINE CORE_4 1
CPU_ONLINE CORE_5 1
CPU_ONLINE CORE_6 0
CPU_ONLINE CORE_7 0
FBP_POWER_GATING FBP_PG_MASK 2
TPC_POWER_GATING TPC_PG_MASK 240
GPU_POWER_CONTROL_ENABLE GPU_PWR_CNTL_EN on
CPU_A78_0 MIN_FREQ 729600
CPU_A78_0 MAX_FREQ 1497600
CPU_A78_1 MIN_FREQ 729600
CPU_A78_1 MAX_FREQ 1497600
GPU MIN_FREQ 0
GPU MAX_FREQ 918000000
GPU_POWER_CONTROL_DISABLE GPU_PWR_CNTL_DIS auto
EMC MAX_FREQ 0
DLA0_CORE MAX_FREQ 614400000
DLA1_CORE MAX_FREQ 614400000
DLA0_FALCON MAX_FREQ 294400000
DLA1_FALCON MAX_FREQ 294400000
PVA0_VPS MAX_FREQ 512000000
PVA0_AXI MAX_FREQ 358400000
```

4.3 Adjusting power and performance

```
# mandatory section to configure the default power mode  
< PM_CONFIG DEFAULT=2 >
```

11. Restart the device. You can switch to the custom power and performance configuration in the **Power mode** menu.



Note

The name of the custom configuration can be modified in step 10 command line `< POWER_MODEL ID=4 NAME=MODE_22_9_W >`.

Security

5.1 Security Features

IPC BX-35A supports the secure features consistent with the Jetson™ Orin NX Series SOM and NVIDIA® Jetson™ Linux®.

Before you enable the security features, please read the security-related information: security features of NVIDIA® Jetson™ Linux®

(<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security.html>).

5.1.1 Secure boot

Secure Boot features

IPC BX-35A (based on NVIDIA® Jetson™ Linux®) supports security features known as Secure Boot. Secure Boot prevents execution of unauthorized boot codes through the chain of trust. The root-of-trust is an on-die BootROM code that authenticates boot codes such as BCT, Bootloader, and warm boot vector using Public Key Cryptography (PKC) keys stored in write-once-read-multiple fuse devices. On Jetson™ platforms that support Secure Boot Key (SBK), you can use it to encrypt Bootloader images.

The root-of-trust that uses the NVIDIA® SoM fuses to authenticate boot codes ends at the Bootloader (known as Secure Boot). After this, the current Bootloader (UEFI) will use UEFI's Security Keys scheme (known as UEFI Secureboot) to authenticate its payloads.

- Secure Boot

Secure Boot authenticates boot codes ends at the Bootloader, it can be enabled by burning fuses.

- UEFI Secureboot

UEFI Secureboot uses digital signatures (RSA) to validate the authenticity and integrity of the codes that it loads. For detailed information: UEFI Secureboot

(<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#uefi-secureboot>).

- UEFI payload encryption

The UEFI Payload Encryption encrypts UEFI payloads with a user encryption key, and this key is stored in EKB, which is protected by OEM key from end user. When the system boots to OPTEE, the user key PTA extracts this key, and when the system boots to UEFI, the OS Loader (L4tLauncher) calls the TA to decrypt and loads the encrypted UEFI payloads. For detailed information: UEFI Payload Encryption

(<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#sd-security-secureboot-uefipayloadencryption>).

- Kernel Module Signing

The kernel module signing facility signs modules during installation and then checks the signature upon loading the module. This allows increased kernel security by disallowing the loading of unsigned modules or modules that were signed with an invalid key. For detailed information: Kernel Module Signing

(<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#kernel-module-signing>).

For IPC BX-35A, the certificate for authenticating driver modules is random generated by Linux® compile tools by default, however user can compile their own Linux® kernel image to use their own certificate to sign and authenticate driver modules.

- Revocation of the PKC Keys

IPC BX-35A (based on Jetson™ Orin NX serials SOM) supports three PKC public keys and provides a revoking mechanism if a key is compromised after the product is shipped. For detailed information: Revoking the PKC key (Page 53).

5.1.2 Disk encryption

Disk Encryption feature

Disk encryption encrypts the whole disk or a partition to protect the data it contains.

NVIDIA® Jetson™ Linux® offers disk encryption that is based on Linux® Unified Key Setup (LUKS) Data-at-rest encryption, which is the standard for Linux® disk encryption. It provides a standard disk format that stores all necessary setup information on the disk itself, in the partition header. The passphrase in the Jetson™ OP-TEE luks-srv Trusted Application (TA) supports disk encryption functionality with one-time passphrase generation during boot time to unlock the encrypted disk. For detailed information: Disk Encryption (<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/DiskEncryption.html#disk-encryption>)

For IPC BX-35A, only rootfs partition and UDA partition can be encrypted at flashing time. User defined partitions need to be encrypted at running time.

5.2 Enabling the Security Features

IPC BX-35A have fuses to protect the device from unknown access request. To enable the security features, the fuses have to be burned with a Fuse Configuration File.

Note

- The fuses are burned with the Fuse Configuration File.
 - **The fuses mentioned in this chapter can only be burned once. If the fuse keys are lost or compromised, the device is no longer safe.**
 - **If the device was burned with the wrong fuse value, it may become bricked.**
-

Keys for the security features

When you burn the fuses of IPC BX-35A, the hash value of the corresponding keys can be burned and used for security purpose.

Here are three kinds of keys to the fuses:

- **PKC Key:** an asymmetric key pair using the RSA-3K/ECDSA P-256/ECDSA P-512 algorithm for PKC key. This key pair is used to sign boot images and is **REQUIRED** for enabling the security features.
- **SBK key:** a symmetric key for SBK key is used to encrypt the boot images. This key is **OPTIONAL**. However, the boot component can never be encrypted without the SBK key.
- **OEMK1 and OEMK2:** a symmetric key for OemK1/OemK2 is used to encrypt the UEFI payloads and disk. This key is **OPTIONAL**. However, we highly recommend you set this key during burning fuse because the UEFI payload encryption and disk encryption can never be enabled without OEMK1/OEMK2.

The PKC fuse, SBK fuse and OEMK1/OEMK2 fuse can only be burned all at once. You can choose the fuse to burn according to your need. Below table shows the fuse needed for each security feature:

Fuse	Signing boot images	Encrypting boot images	UEFI Secureboot	UEFI Payload Encryption	Disk Encryption	Revocation of the PKC Keys
PKC	REQUIRED	REQUIRED	OPTIONAL ¹	REQUIRED	REQUIRED	REQUIRED ²
SBK	OPTIONAL ³	REQUIRED	OPTIONAL ³	OPTIONAL ³	OPTIONAL ³	N/A
OEMK1	OPTIONAL	OPTIONAL	OPTIONAL	REQUIRED	REQUIRED	N/A
OEMK2	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	OPTIONAL	N/A

¹ : It is not safe to enable UEFI Secureboot without PKC fuse burned. Because the UEFI firmware can be easily modified without being verified by PKC fuse key. And this would result in UEFI Secureboot failure.

² : We strongly recommend that you burn three PKC fuses. To support PKC keys revocation, all three PKC keys must be fused at device provision.

³ : If SBK is not burned, boot images (including UEFI) cannot be encrypted.

Command options for enabling the security features

The basic usage of SPM is:

```
sudo ./SPM [options] <device> <JetPack Version> <rootdev>
```

- [options] is one or more command line options. All of the options are optional.
- <device> specifies the device name. For IPC BX-35A, the value of this parameter is *BX-35A* or *bx-35a*.
- <JetPack Version> specifies the JetPack version, you can get the supported JetPack version by command `sudo ./SPM -l`.
- <rootdev> specifies the root device to store the rootfs in device. You can get the supported root device by command `sudo ./SPM -l`.

SPM also provides the below command options for you to enable the security features on IPC BX-35A:

- `--create-pkchash`: to generate PublicKeyHash for the Fuse Configuration File
- `--burn-fuse`: to burn fuses those specified in the Fuse Configuration File to enable Secure Boot

You are required to enter the Fuse Configuration File path and burn fuse option. SPM uses the Fuse Configuration File and options to create a command line, which will call a script named "odmfuse.sh" to burn fuses on SoCs for IPC BX-35A. The `odmfuse.sh` script is from NVIDIA® Jetson™ Linux® package.

Note

When using `--burn-fuse` option, be sure that the values in the Fuse Configuration File are correct, otherwise you will face the risk that the device becomes bricked. Once the device is bricked, it is unable to be recovered.

- `--sign`: to sign secured images and flash the images to the device
- If Secure Boot is enabled (the fuses in IPC BX-35A have already been burned), the device needs secured images to boot up.
-

Note

When using `--sign` option, you must provide correct keys to sign/encrypt images. Otherwise, the device fails to boot up.

- `--enc`: to encrypt UEFI payloads and rootfs partition
- This option must be used together with `--sign` option. If `--sign` option is not input, this command option cannot work.
- `--revoke-pkc`: to revoke PKC key

5.2.1 Preparing keys

Requirement

- The needed keys are confirmed according to the security features, see Enabling the Security Features (Page 40).

Public Key Cryptography (PKC)

Generate an asymmetric key pair for PKC key. Refer to Generate A PKC Key Pair (<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#generate-a-pkc-key-pair>).

IPC BX-35A (Based on Jetson™ Orin NX) only support RSA-3K/ECDSA P-256/ECDSA P-521. For example:

```
#Generate an ECDSA P-256 key for PKC0, the key pair will be saved
into pkc0_ecp256.pem
$ openssl ecparam -name prime256v1 -genkey -noout -out
pkc0_ecp256.pem
#Generate an ECDSA P-256 key for PKC1, the key pair will be saved
into pkc1_ecp256.pem
$ openssl ecparam -name prime256v1 -genkey -noout -out
pkc1_ecp256.pem
#Generate an ECDSA P-256 key for PKC2, the key pair will be saved
into pkc2_ecp256.pem
$ openssl ecparam -name prime256v1 -genkey -noout -out
pkc2_ecp256.pem
```

! CAUTION

- We recommend that you generate 3 different key pairs with same algorithm for PKC0~PKC2.
- Please keep the key pair in a safe place, the security of your device depends on how securely you keep the key file.
- Do not save any key in SPM workshop or it's child path. SPM default workshop is: /home/{user}/.local/share/spm_workshop/

Secure Boot Key (SBK)

IPC BX-35A (Based on Jetson™ Orin SoC) requires an SBK key of eight 32-bit value (32 bytes).

For example, you can input the below command to generate the SBK key:

```
$ openssl rand -rand /dev/random -hex 32 > SBK.key #The key value
will be saved to SBK.key
```

! CAUTION

- We recommend that you use the Hardware Security Module (HSM) to generate a truly random number for an SBK key.
- Please keep the key in a safe place, the security of your device depends on how securely you keep the key file.
- Do not save any key in SPM workshop or it's child path. SPM default workshop is: /home/{user}/.local/share/spm_workshop/

Original Equipment Manufacturer (OEM) key

The two fuses, OEMK1 and OEMK2, are used to store the OEM key. For IPC BX-35A (based on Jetson™ Orin SoC), both OEMK1 and OEMK2 require a key with the length of 32 bytes.

For example, you can input the below command to generate the OEM key:

```
#Generate key for OemK1, the key value will be saved to OemK1.key
$ openssl rand -rand /dev/random -hex 32 > OemK1.key
```

```
#Generate key for OemK2, the key value will be saved to OemK2.key  
$ openssl rand -rand /dev/random -hex 32 > OemK2.key
```

**CAUTION**

- We recommend that you use the Hardware Security Module (HSM) to generate a truly random number for an OEM key.
- Please keep the key in a safe place, the security of your device depends on how securely you keep the key file.
- Do not save any key in SPM workshop or its child path. SPM default workshop is: `/home/{user}/.local/share/spm_workshop/`

5.2.2 Creating PKC hash by SPM

Requirement

- Support Package Manager (SPM) is installed on host PC, see Downloading Support Package Manager (Page 34).
- PKC fuse key is generated, see Preparing keys (Page 42).

Procedure - Generating hash for PKC fuse key

1. Run command `sudo ./SPM --create-pkchash bx-35a jp5.1.2` on host PC.
2. Input the absolute path of PKC0 key file in PEM format and press the Enter key to generate the hash value.
3. The hash value for PKC0 with the length of 512 bits will be displayed.

You must follow the above steps again to generate hash value for PKC1 and PKC2 key respectively.

5.2.3 Creating the fuse configuration file

Requirements

- Hash values for PKC0/PKC1/PKC2 are generated, see Creating PKC hash by SPM (Page 44).

1. Create a Fuse Configuration File, see Jetson™ Orin Fuse Configuration File (<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#jetson-orin-fuse-configuration-file>)
2. Fill the hash values of PKC0/PKC1/PKC2 in the Fuse Configuration File:
 - Hash value of PKC0 needs to be filled to the field named with `PublicKeyHash`.
 - Hash value of PKC1 needs to be filled to the field named with `PkcPubkeyHash1`.
 - Hash value of PKC2 needs to be filled to the field named with `PkcPubkeyHash2`.
3. Fill the SBK key value in the field named `SecureBootKey` in the Fuse Configuration File. See Prepare an SBK key (<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#prepare-an-sbk-key>).
4. Fill the OemK key values in the fields named `OemK1` and `OemK2` in the Fuse Configuration File. See Prepare K1/K2/KEK keys (<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#prepare-k1-k2-kek-keys>).
5. Fill in the `BootSecurityInfo`. This field is as known as `FUSE_BOOT_SECURITY_INFO_0`, which indicate the boot security info:

Bits [2:0] mapped to Secure Boot Authentication Scheme, where:

Bits not listed are reserved

For example:

- The generated PKC key pairs are ECDSA P-256 key pairs, so the value for *Bits[2:0]* should be 010b.
- The Fuse Configuration File contains SBK value, so the value for *Bit[3]* should be 1b.
- The ODM Key is valid, so the value for *Bit[9]* should be 1b.

[illegible]

 CAUTION

Please be sure that the `BootSecurityInfo` field you filled is correct, or the device may be bricked after burning fuses.

6. Fill in the field named `OptInEnable`.

This field is to prevent running an earlier version of the software, which compromises the revocation effect. Fill this field with `0x01`.

7. Fill in the field named `SecurityMode`.

This field indicate that whether the secure boot is to be enabled or not.

Fill this field with `0x01` or other non-zero values, then the secure boot will be enabled and the fuses specified in the `Fuse Configuration File` will be burned.

 CAUTION

The PKC fuse, SBK fuse and OEMK1/OEMK2 fuse can only be burned all at once. The fuses not specified in the `Fuse Configuration File` can never be burned again after the above steps are operated.

5.2.4 Verifying the fuse configuration file

Requirement

- The fuse configuration file is created, see Creating the fuse configuration file (Page 44).
- Enter recovery mode: press and hold the **RESET** key, then turn on IPC BX-35A, and release **RESET** after power LED has been on for 3s.
- IPC BX-35A is connected to the host PC by using a **Type-A to Micro-USB cable**.

Procedure

1. Run command `sudo ./SPM --burn-fuse bx-35a jp5.1.2` on host PC.
2. Read the disclaimer. Input **Agree** and press the Enter key if you want to proceed.
3. Input the absolute path of `Fuse Configuration File` and press the Enter key.
4. If the device has burned PKC fuse, you need to input the absolute path to the PKC key file.
5. Input **y** (or **Y**) and press the Enter key to start to test the `Fuse Configuration File`.
6. If no error was detected in the `Fuse Configuration File`, the message *Success to test burning fuse* will be displayed.

! CAUTION

- Do not burn any fuse if the error log is displayed. Check the `Fuse Configuration File` and verify until no errors were detected.
- The above steps cannot verify the value that will be/is being burned into device.
- Be sure that all the fuse value that you filled into Fuse configuration file are correct.

5.2.5 Burning fuse by SPM

Requirement

- The keys are created, see Preparing keys (Page 42).
- The PKC hash file is created, see Creating PKC hash by SPM (Page 44).
- The fuse configuration file is created and verified, see Verifying the fuse configuration file (Page 46).
- Enter recovery mode: press and hold the **RESET** key, then turn on IPC BX-35A, and release **RESET** after power LED has been on for 3s.
- IPC BX-35A is connected to the host PC by using a **Type-A to Micro-USB cable**.

! CAUTION

- **The fuses mentioned in this chapter can only be burned once. If the fuse keys are lost or compromised, the device is no longer safe.**
- **If the device was burned with the wrong fuse value, it may become bricked.**
- Before you burn the fuse, make sure that the fuse values in `fuse configuration file` are correct.

Procedure - example for burning fuse

1. Run command `sudo ./SPM --burn-fuse bx-35a jp5.1.2` on host PC, then the following the on-screen instructions to burn fuses.
2. Read the disclaimer. Input **Agree** and press the Enter key if you want to proceed.
3. Input the absolute path of `Fuse Configuration File` and press the Enter key.
4. If the device has burned PKC fuse, you need to input the absolute path to the PKC key file.
5. Press the Enter key to skip the test function and burn fuse directly.
6. Input **Yes** and press the Enter key to burn fuse.
7. If no error message is displayed after burning fuse process completed, the fuses are successfully burned.

5.2.6 Installing secured images

After the fuses are burned on IPC BX-35A, Secure Boot will be enabled and only secured and authorized images can be installed on this device. You have to enable the security features by installing the secured OS image to the device:

- to enable UEFI Secureboot, see Installing the OS image with UEFI Secureboot (Page 48).
- to enable UEFI Payload Encryption, Disk Encryption, or all the security features at once, see Installing the OS image with UEFI Payload Encryption, Disk Encryption (Page 50).

Note

After the secured OS image is installed on the device, restart the device and read the fuse status to check if Secure Boot is enabled. For detailed information: Read Fuses through the Linux® kernel

(<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#read-fuses-through-the-linux-kernel>).

5.2.6.1 Installing the OS image with UEFI Secureboot

Requirement

- The fuse is burned, see Burning fuse by SPM (Page 47).
- IPC BX-35A is connected to the host PC by using a **Type-A to Micro-USB cable**.
- The PKC key file in PEM format is generated. The SBK key file is generated. See Preparing keys (Page 42).

Note

If your device has burned PKC or SBK fuse, the key file is **Required**, otherwise the key file is not needed.

- If you want to enable the UEFI Secureboot feature, the **UEFI keys config file** is needed. You can refer to the following steps to generate the file:
 - Step 1. Generate UEFI keys (the PK, KEK, db RSA keypairs and certificates) by inputting the following commands:

```
#1. Create a work path for saving keys
$ mkdir uefi-keys
#2. Enter uefi-keys
$ cd uefi-keys
#3. Generate PK RSA keypair and certificate
$ openssl req -newkey rsa:2048 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -subj "/CN=my Platform Key/" -out PK.crt
#4. Generate KEK RSA keypair and certificate
$ openssl req -newkey rsa:2048 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -subj "/CN=my Key Exchange Key/" -out
```

```

KEK.crt
#5. Generate db_1 RSA keypair and certificate
$ openssl req -newkey rsa:2048 -nodes -keyout db_1.key -new -
x509 -sha256 -days 3650 -subj "/CN=my Signature Database key/"
-out db_1.crt
#6. Generate db_2 RSA keypair and certificate
$ openssl req -newkey rsa:2048 -nodes -keyout db_2.key -new -
x509 -sha256 -days 3650 -subj "/CN=my another Signature
Database key/" -out db_2.crt

```

– Step 2. Create a UEFI keys config file.

```

#1. Enter uefi-keys created in Step 1
$ cd uefi-keys
#2. Create "uefi_keys.conf" with vim and open it
$ vim uefi_keys.conf
#3. Insert the following lines to uefi_keys.conf file and then
save file:
UEFI_PK_KEY_FILE="PK.key";
UEFI_PK_CERT_FILE="PK.crt";
UEFI_KEK_KEY_FILE="KEK.key";
UEFI_KEK_CERT_FILE="KEK.crt";
UEFI_DB_1_KEY_FILE="db_1.key";
UEFI_DB_1_CERT_FILE="db_1.crt";
UEFI_DB_2_KEY_FILE="db_2.key";
UEFI_DB_2_CERT_FILE="db_2.crt";

```

Procedure

1. Run command `sudo ./SPM --sign bx-35a jp5.1.2 nvme` on the host PC, and follow the on-screen instructions.
2. If you have burned the PKC fuse, input the absolute path of **PKC key file** in PEM format. Press the Enter key.
3. If you have burned the SBK fuse, input the absolute path of **SBK key file**. Press the Enter key.
4. If you want to enable the UEFI Secureboot feature, input the absolute path to the **UEFI keys config file** and press the Enter key.

Note

After the installing process is finished successful, you can check if the UEFI Secureboot is enabled after the device startup. See Check if UEFI Secureboot is enabled (<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#check-if-uefi-secureboot-is-enabled>).

5. After the secured images are generated and marked as **Done**, press the Enter key to install the image to the device.
6. If the images is installed to the device successfully, the message **Flash is successful** will be displayed, otherwise an error message will be displayed.

Note

The device exits after finish cleaning the workshop. Do not terminate the dialog manually.

5.2.6.2 Installing the OS image with UEFI Payload Encryption, Disk Encryption

Requirement

- The fuse is burned, see Burning fuse by SPM (Page 47).
- IPC BX-35A is connected to the host PC by using a **Type-A to Micro-USB cable**.
- The PKC key file in PEM format is generated. The SBK, OEMK1, OEMK2 key files in KEY format are generated. See Preparing keys (Page 42).

Note

- If your device has previously burned PKC or SBK fuse, the key file is **Required**, otherwise the key file is not needed.
 - The OEMK1 and OEMK2 key files are **Required**.
-
- If you want to enable the UEFI Payload Encryption feature, the **user key for UEFI payload encryption** (a symmetric key with the length of 32 bytes) is needed for encrypting UEFI payloads. You can refer to the following steps to generate the key file:

```
$ openssl rand -rand /dev/random -hex 32 | tee user-uefi-enc.key
4574ef078b8ddccecf730959ed35744fdefedd04fbd095d46605215b18ef708d
#This is the key for UEFI payload encryption, and it has been
saved into user-uefi-enc.key
```

Note

- We recommend that you use the Hardware Security Module (HSM) to generate a truly random number for an UEFI payload encryption key.
 - Please keep the key in a safe place.
 - Do not save any key in SPM workshop or in its child path. SPM default workshop is:
/home/{user}/.local/share/spm_workshop/
-

- If you want to enable the Disk Encryption feature, the **user key for Disk encryption** (a symmetric key with the length of 16 bytes) is needed. You can refer to the following steps to generate the key file:

```
$ openssl rand -rand /dev/random -hex 16 | tee user-disk-enc.key
829ee118280a2e9e1d21183749a40fa8 #This is the key for disk
encryption, and it has been saved into user-disk-enc.key
```

Note

- We recommend that you use the Hardware Security Module (HSM) to generate a truly random number for a disk encryption key.
 - Please keep the key in a safe place.
 - Do not save any key in SPM workshop or in its child path. SPM default workshop is: `/home/{user}/.local/share/spm_workshop/`
-

- If you want to enable the UEFI Secureboot feature, the **UEFI keys config file** is needed. You can refer to the following steps to generate the file:

- Step 1. Generate UEFI keys (the PK, KEK, db RSA keypairs and certificates) by inputting the following commands:

```
#1. Create a work path for saving keys
$ mkdir uefi-keys
#2. Enter uefi-keys
$ cd uefi-keys
#3. Generate PK RSA keypair and certificate
$ openssl req -newkey rsa:2048 -nodes -keyout PK.key -new -x509
-sha256 -days 3650 -subj "/CN=my Platform Key/" -out PK.crt
#4. Generate KEK RSA keypair and certificate
$ openssl req -newkey rsa:2048 -nodes -keyout KEK.key -new -
x509 -sha256 -days 3650 -subj "/CN=my Key Exchange Key/" -out
KEK.crt
#5. Generate db_1 RSA keypair and certificate
$ openssl req -newkey rsa:2048 -nodes -keyout db_1.key -new -
x509 -sha256 -days 3650 -subj "/CN=my Signature Database key/"
-out db_1.crt
#6. Generate db_2 RSA keypair and certificate
$ openssl req -newkey rsa:2048 -nodes -keyout db_2.key -new -
x509 -sha256 -days 3650 -subj "/CN=my another Signature
Database key/" -out db_2.crt
```

- Step 2. Create a **UEFI keys config file**.

```
#1. Enter uefi-keys created in Step 1
$ cd uefi-keys
#2. Create "uefi_keys.conf" with vim and open it
$ vim uefi_keys.conf
#3. Insert the following lines to uefi_keys.conf file and then
save file:
UEFI_PK_KEY_FILE="PK.key";
UEFI_PK_CERT_FILE="PK.crt";
UEFI_KEK_KEY_FILE="KEK.key";
UEFI_KEK_CERT_FILE="KEK.crt";
UEFI_DB_1_KEY_FILE="db_1.key";
```

```
UEFI_DB_1_CERT_FILE="db_1.crt";  
UEFI_DB_2_KEY_FILE="db_2.key";  
UEFI_DB_2_CERT_FILE="db_2.crt";
```

Procedure

1. Run command `sudo ./SPM --sign --enc bx-35a jp5.1.2 nvme` on the host PC.
2. If you have burned the PKC fuse, input the absolute path of **PKC key file** in PEM format. Press the Enter key.
3. If you have burned the SBK fuse, input the absolute path of **SBK key file**. Press the Enter key.
4. Follow the on-screen instructions to input the absolute path of **OEMK1/OEMK2 key file** in KEY format and press the Enter key.
5. If you want to enable the UEFI Payload Encryption feature, input the absolute path to the **user key for UEFI payload encryption**. Press the Enter key.
6. If you want to enable the Disk Encryption feature, input the absolute path to the **user key for Disk encryption**. Press the Enter key.
7. If you want to enable the UEFI Secureboot feature, input the absolute path to the **UEFI keys config file**. Press the Enter key.

Note

After the installing process is finished successful, you can check if the UEFI Secureboot is enabled after the device startup. See Check if UEFI Secureboot is enabled (<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#check-if-uefi-secureboot-is-enabled>).

8. Follow the on-screen instructions to enable the security features by entering `y` or `Y`. Press the Enter key.
9. After the secured images are generated and marked as **Done**, press the Enter key to install the image to the device.
10. If the images are installed to the device successfully, the message **Flash is successful** will be displayed, otherwise an error message will be displayed.

5.3 Revoking the PKC key

The BX-35A supports three PKC public keys and provides a revoking mechanism if a key is lost or compromised. For more information, see Revocation of the PKC Keys

(<https://docs.nvidia.com/jetson/archives/r35.4.1/DeveloperGuide/text/SD/Security/SecureBoot.html#revocation-of-the-pkc-keys>).

Note

- The SHA2-512 hash values of the PKC keys are burned into the fuses by the user with SPM (use the corresponding fuse name of PublicKeyHash, PkcPubkeyHash1, PkcPubkeyHash2 in the Fuse Configuration File).
 - The third PKC key (PKC2 or PkcPubkeyHash2) cannot be revoked. And the device can always boot with images signed with the private key of PKC2.
 - After a key is revoked, it is permanently unusable and cannot be restored.
 - To support PKC keys revocation, all three PKC keys must be fused at device provision.
-

Requirement

- IPC BX-35A is connected to the host PC by using a **Type-A to Micro-USB cable**.
- The key file in PEM format is generated. See Preparing keys (Page 42).
 - If you want to revoke the first PKC key (PKC0), the second PKC private key file (PKC1) or the third PKC private key file (PKC2) is needed.
 - If you want to revoke the second PKC key (PKC1), the third PKC private key file (PKC2) is needed.
- If the UEFI Payload Encryption feature is enabled, the **user key for UEFI payload encryption** is needed.
- If the Disk Encryption feature is enabled, the **user key for Disk encryption** is needed.
- If the UEFI Secureboot feature is enabled, the **UEFI keys config file** is needed.

Procedure - revoking the PKC key

1. Run command `sudo ./SPM --revoke-pkc bx-35a jp5.1.2 nvme` on the host PC.
2. Read the disclaimer and input `Agree`. Press the Enter key.
3. Follow the on-screen instructions to select the key that you want to revoke and input the key file path:
 - If you want to revoke the PKC0 key, input the absolute path to the PKC1 or PKC2 key file.
 - If you want to revoke the PKC1 key, input the absolute path to the PKC2 key file.
4. If the SBK fuse on this device has been burned, input the absolute path of **SBK key file**. Press the Enter key.
5. If the OEMK1 or OEMK2 fuse on this device has been burned, input the absolute path of **OEMK1/OEMK2 key file** in KEY format and press the Enter key.

5.3 Revoking the PKC key

6. If the UEFI Payload Encryption feature is enabled, enter the absolute path to the **user key for UEFI payload encryption**. Press the Enter key.
7. If the Disk Encryption feature is enabled, enter the absolute path to the **user key for Disk encryption**. Press the Enter key.
8. If the UEFI Secureboot feature is enabled, enter the absolute path to the **UEFI keys config file**. Press the Enter key.
9. After the boot components are signed and encrypted, and marked as **Done**, press the Enter key to revoke the PKC key.
10. If the PKC key is revoked successfully, the message **Success to flash images to BX-35A** will be displayed, otherwise the PKC key cannot be revoked.

Note

After the revoke procedure, SPM will clean the workshop and exit. Do not terminate the dialog manually.

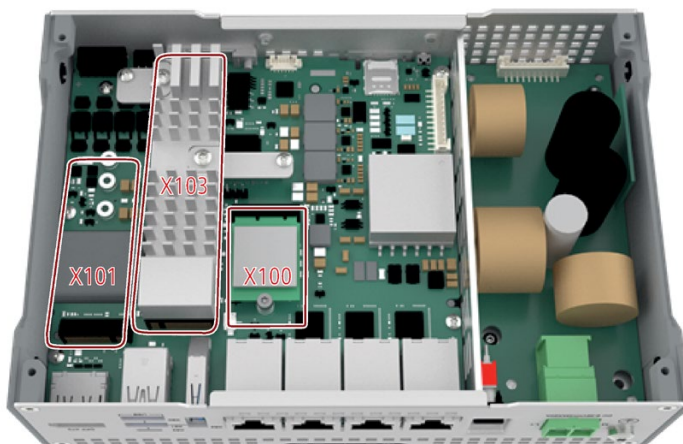
Expanding the device

6.1 Installing the M.2 module

Introduction to the M.2 module

Siemens uses the M.2 module to extend the Siemens IPC. You can use the M.2 module produced by Siemens or other third-party suppliers. The device provides three M.2 interfaces for M.2 B Key / E Key / M Key modules. The M.2 modules can be connected to the interface slot X100, X101, or X103 on the motherboard.

The position of each slot is marked as below:



Installation of the M.2 module in our device should not exceed the specified maximum outline or the maximum allowed power dissipation. The following table contains the detailed features and functions of the M.2 module:

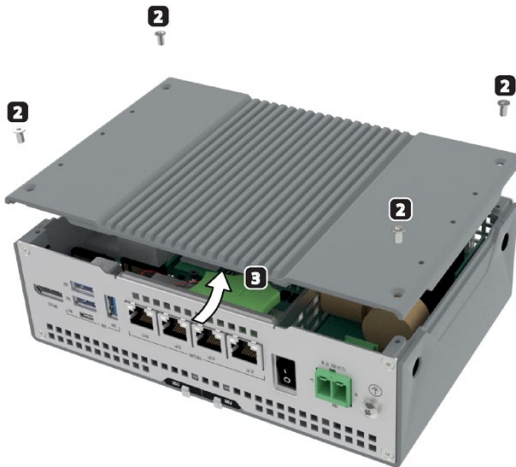
Module	M.2 module 1 (Slot X100)	M.2 module 2 (Slot X101)	M.2 module 3 (Slot X103)
Features and function			
Size	2230	2242, 2260, 3042, 3052, 3060	2242, 2280
Interface	E Key	B Key	M Key
Channel	1 × PCIe 3.0 (1 lane) + 1 × USB 2.0 + 1 × I2S + 1 × UART	1 × PCIe 3.0 (1 lane) + 1 × USB 3.0 + 1 × USB 2.0	1 × PCIe 3.0 (4 lane)
Support WLAN module, like Wi-Fi, Bluetooth	Yes	No	No
Support WWAN module ¹ , like 3G/4G/ 5G	No	Yes	No
Support NVMe SSD	No	No	Yes

¹ : You can insert a 4G/5G SIM card into the SIM card slot to connect to network. However, the SIM card function has not been certified by UL. Siemens recommends that you use SIM cards without PIN codes.

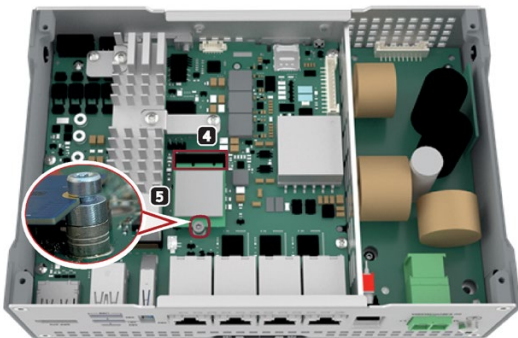
Requirements

- T10 screwdriver and T8 screwdriver

Procedure - Installing the M.2 module

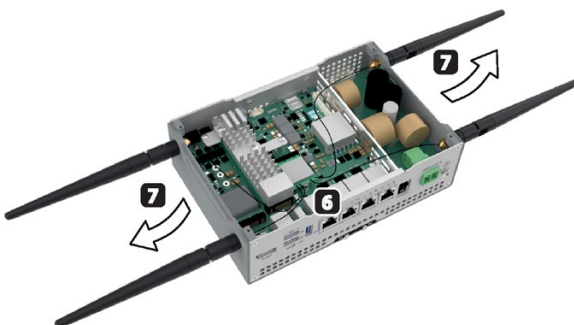


- 1** Disconnect the device from the power supply.
- 2** Remove the retaining screws on the rear cover of the device.
- 3** Lift up the device's rear cover.



- 4** Align the golden finger of the M.2 module on the motherboard, and then press firmly until it is completely seated on the slot.
- 5** Secure the M.2 module with a screw.
Note: Make sure the M.2 module board is located between head and spacer of assembly screw.

If the M.2 module has any installation accessories, such as an antenna, you can complete the following additional steps:



- 6** Connect the cables of the M.2 module installation accessory to the M.2 module.
- 7** Get the cable of the M.2 module installation accessory out of the housing through reserved antenna holes.
Note:
There are four caps on each reserved antenna holes. Remove the caps from inside.

Procedure - Removing the M.2 module

Follow the above steps in reverse order to remove the M.2 module.

6.2 Inserting the Nano SIM card

Requirements

- Nano SIM card that is suitable for industrial use.

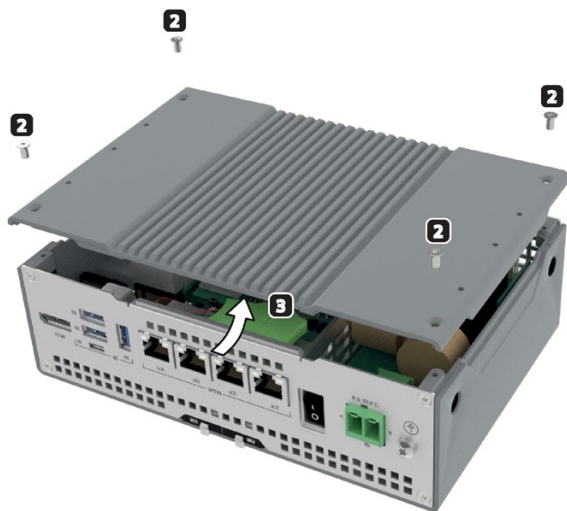
Installation

NOTICE

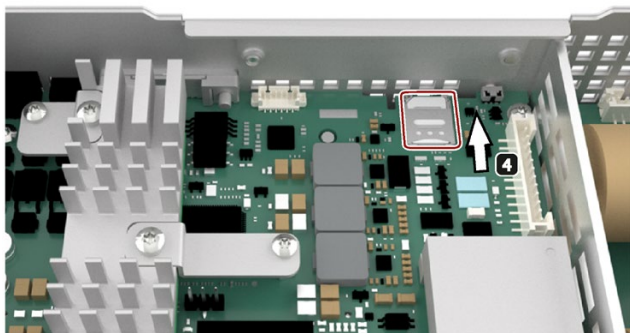
Inserting a SIM card

If you are using the Nano SIM card in a device installed in a system, you must observe the safety regulations for work on electrical systems.

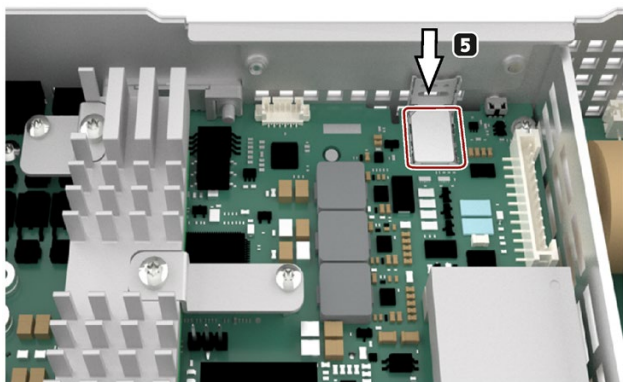
Carefully insert the Nano SIM card into the card holder without applying excess force.



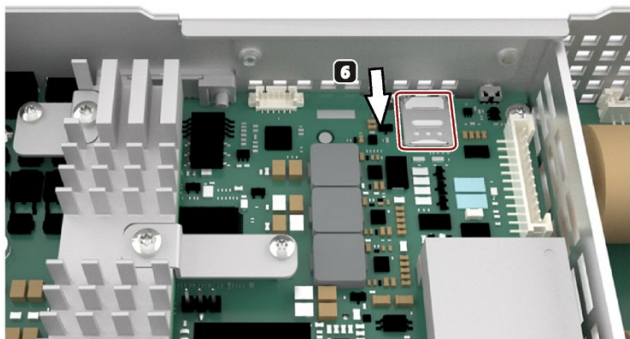
- 1** Disconnect the device from the power supply.
- 2** Remove the retaining four screws on the rear cover of the device.
- 3** Lift up the rear cover.



- 4** Push the card bracket cover in the marked direction to release the bracket.



- 5** Insert the Nano SIM card into the supporting frame. The contacts of the Nano SIM card must face to the motherboard.



- 6** Close the card bracket cover and push in the marked direction to tighten the bracket.

6.3 Installing the SSD

To ensure the heat dissipation and the performance of NVMe SSD, the BX-35A uses a heat sink to secure the SSD.

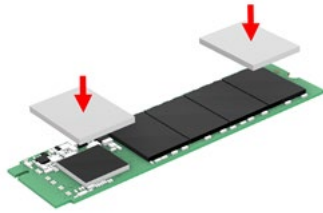
The heat sink accessory is designed for 2280 SSD, and it is also compatible for 2242 SSD.

Requirements

- The device is disconnected from the power supply.
- A NVMe SSD that is approved for industrial applications.
- T8 screwdriver and T10 screwdriver

Procedure - Installing the SSD

- 1** Place the SSD thermal interface material (TIM) on the chip of SSD.



- 2** Remove the 4 retaining screws on the rear cover of the device, and lift up the rear cover.

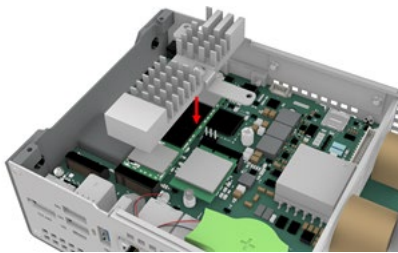


- 3** Align the golden finger of the SSD with custom slot on the motherboard, and then press firmly until it is completely seated on the slot.



- 4** Secure the SSD module with a screw.
Note: Ensure the SSD module board is located between head and spacer of assembly screw.





5 Cover the heat sink to the SSD module.



6 Secure the heatsink with two screws.

Procedure - Removing the SSD

Follow the above steps in reverse order to remove the SSD.

6.4 Installing the SOM

Requirements

- The device is disconnected from the power supply.
- A SoM (System on Module) that is approved for industrial applications.
- T8 screwdriver and T10 screwdriver

Procedure - installing the SoM



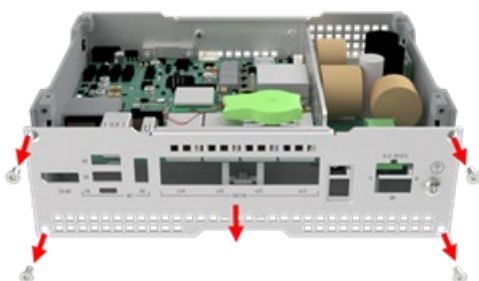
1 Remove the four retaining T10 screws on the rear cover of the device, and lift up the rear cover.



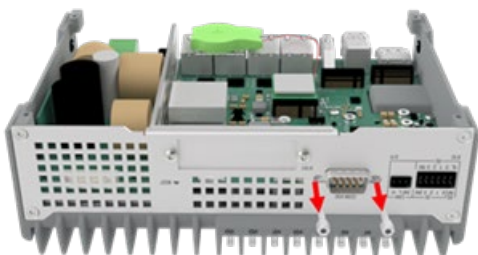
- 2** Remove the two T8 screws and release the SSD heatsink.



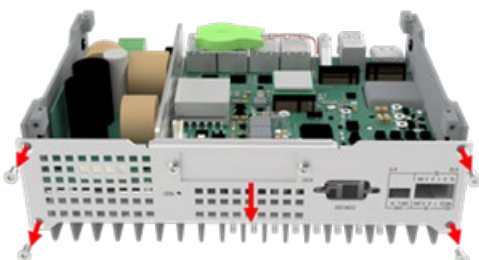
- 3** Remove the T8 screw and release the SSD.



- 4** Remove the four T10 screws and release the panel.

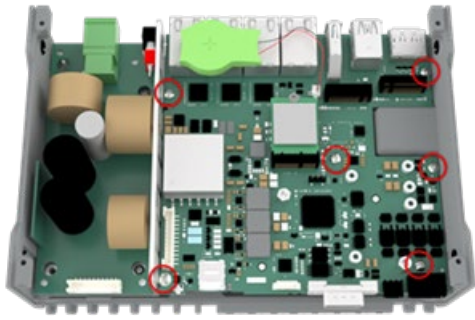


- 5** Turn to the back panel of the device and remove the two SW4.5 screw.



- 6** Remove the four T10 screws and release the panel.

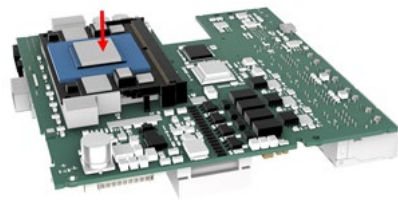
6.4 Installing the SOM



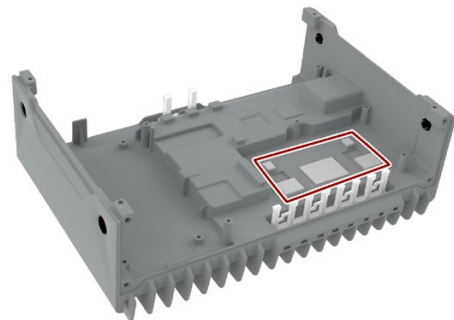
- 7** Remove the six T8 screws on the motherboard and release the motherboard.



- 8** Turn over the motherboard, and insert the SoM into the bracket.



- 9** Push the SoM in the direction as shown.
Note: Make sure the side buckles of the bracket are secured.



- 10** Remove the tapes on the TIMs attached on the top housing.

- 11** Follow the above steps in reverse order to install the SOM.

Maintaining and repairing the device

7.1 Maintenance

To maintain high system availability, Siemens recommends preventative replacement of the back-up battery at replacement intervals of 3 years.

7.2 Repair information

Carrying out repairs

Only qualified personnel are permitted to repair the device. Contact your local representative, see section "Service and support (Page 93)".

WARNING

Unauthorized opening and improper repairs on the device may result in substantial damage to equipment or endanger the user.

- Always disconnect the power plug before you open the device.
- Only install system expansion devices designed for this device. If you install other expansion devices, you may damage the device or violate the safety requirements and regulations on RF suppression. Contact your technical support team or where you purchased your PC to find out which system expansion devices may safely be installed.

If you install or exchange system expansions and damage your device, the warranty becomes void.

CAUTION

Electrostatic sensitive devices (ESD)

The device contains electronic components which are destroyed by electrostatic charges. This can result in malfunctions and damage to the machine or plant.

Make sure you take precautionary measures even when you open the device, for example, when opening device doors, device covers or the housing cover. For more information, refer to the chapter "ESD Guideline (Page 71)"

Limitation of liability

All technical specifications and approvals of the device only apply if you use expansion components that have a valid CE approval (CE mark). The installation instructions for expansion components in the associated documentation must be observed.

7.3 Replacing the backup battery

UL approval of the device only applies when the UL-approved components are used according to their "Conditions of Acceptability".

We are not liable for functional limitations caused by using third-party devices or components.

7.3 Replacing the backup battery

Prior to replacement



WARNING

Risk of explosion and release of harmful substances

An explosion or fire HAZARD could occur through fitting a battery of the wrong type.

Improper handling of lithium batteries also can result in an explosion of the batteries.

Explosion of the batteries and the released pollutants can cause severe physical injury. Aged batteries jeopardize the function of the device.

Note the following when handling lithium batteries:

- Replace the battery every 3 years.
- Replace the lithium battery only with the type recommended by the manufacturer. The new lithium battery must be certificated by UL and meet the following requirements:
 - Type: BR2450A
 - Rated voltage: 3 V DC
 - Max abnormal charging current: 5 mA
- For any requirements on product maintenance, contact Siemens Technical support (Page 93).
- Do not throw lithium batteries into fire, do not solder on the cell body, do not recharge, do not open, do not short-circuit, do not reverse polarity, do not heat above 100°C and protect from direct sunlight, moisture and condensation.

! WARNING**Risque d'explosion et d'émission de substances nocives**

l'installation d'une pile ou d'un accumulateur de type inadéquat peut provoquer un DANGER d'explosion ou d'incendie.

Une manipulation non conforme des piles au lithium peut conduire à leur explosion.

L'explosion des piles et l'émission de polluants qui en résulte peuvent entraîner de graves lésions corporelles. Des piles usagées constituent un danger pour le fonctionnement de l'appareil.

Observez les remarques suivantes lorsque vous manipulez des piles au lithium:

- Remplacez la pile tous les 3 ans.
- Remplacez la pile au lithium uniquement par une pile du type recommandé par le constructeur. La nouvelle pile au lithium doit avoir une certification UL et satisfaire aux exigences suivantes :
 - Type: BR2450A
 - Tension nominale: 3 V CC
 - Courant de charge anormal max.: 5 mA
- Pour toute demande concernant la maintenance du produit, contactez le support technique (Page 93) Siemens.
- Ne jetez pas au feu des piles au lithium, n'effectuez pas de soudage sur la pile, ne la rechargez pas, ne l'ouvrez pas, ne la court-circuitez pas, n'intervertissez pas les pôles, ne la chauffez pas à plus de 100 °C et protégez-la de l'ensoleillement direct, de l'humidité et de la condensation.

! WARNING**電池和蓄電池**

- 置換可能影響安全防護的錯誤型式的電池（例：在某些鋰電池類型的情形下）：
- 電池丟入火焰或烤箱中，或將電池作可能導致爆炸的機械擠壓或切割；
- 電池置於可能導致爆炸或可燃性液體或氣體洩露的高溫環境中；且
- 電池承受可能導致爆炸或可燃性液體或氣體洩露的極度低氣壓。

NOTICE**Disposal of batteries**

Batteries do not belong in domestic garbage. Users are legally obliged to return used batteries.

Used batteries pollute the environment as special waste. You as a user are liable to prosecution if you do not properly dispose of batteries.

Observe the following when disposing of batteries:

- Dispose of used batteries as hazardous waste in accordance with local regulations.
- You can return used batteries to public collection points and wherever batteries of the type in question are sold.
- Label the battery container "Used batteries".

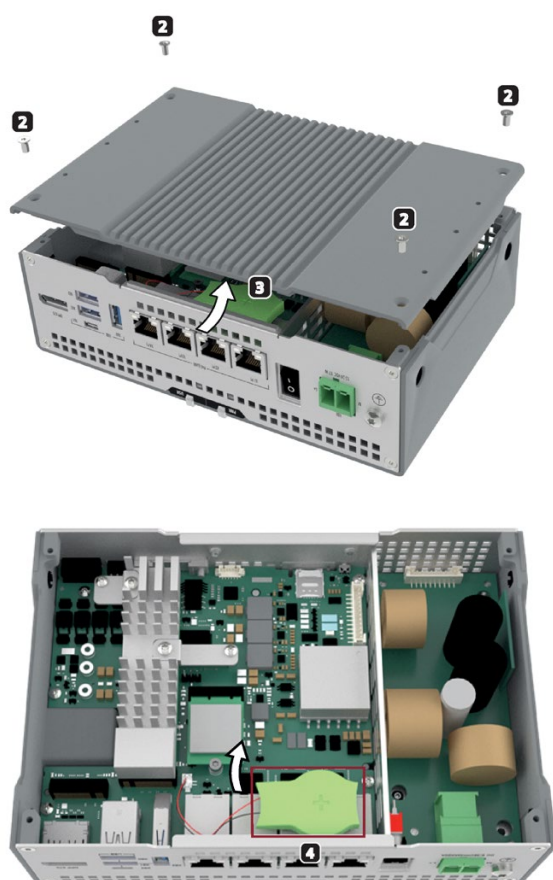
Note

Replace batteries only in non-hazardous areas.

Requirements

- A T10 screwdriver

Procedure



- 1 Disconnect the device from the power supply.
- 2 Remove the retaining screws on the rear cover of the device.
- 3 Lift up the rear cover.

- 4 Slide the battery out 45 degrees from the upper left. Pull the battery out gently and insert a new battery.
Note: The positive electrode (+) of the battery should be positioned toward the outside of the device.

7.4 Recycling and disposal

Due to the low levels of pollutants in the devices described in these operating instructions, they can be recycled.

Contact a certified disposal service company for electronic scrap for environmentally sound recycling and disposal of your old devices, and dispose of the device according to the relevant regulations in your country.

Technical specifications

8.1 Certificates and approvals

Note

Applicability

The following shows the approvals that may be available. For the device itself, it is certificated as shown on the product label and package label.

ISO 9001 certificate

The Siemens quality management system for all production processes (Development, Production, Sales and Service of Automation Products, -Systems and -Solutions) meets the requirements of ISO 9001:2015

Certificate registration no. 01 100 1430201.

Software license agreements



If the device is supplied with preinstalled software, you must observe the corresponding license agreements.

EMC Directive:

2014/30/EU Directive of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility; Official Journal of the EU L96, 29/03/2014, p. 79–106

RoHS Directive:

2011/65/EU Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment; Official Journal of the EU L174, 1/07/2011, p.88–110

EMC EN 61000-6-2, EN 61000-6-4;

RoHS EN IEC 63000:2018

FCC and Canada

USA	
Federal Communications Commission Radio Frequency Interference Statement	This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
Shielded Cables	Shielded cables must be used with this equipment to maintain compliance with FCC regulations.
Modifications	Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.
Conditions of Operations	This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CANADA	
Canadian Notice	This Class A digital apparatus complies with Canadian ICES-003 (A).
Avis Canadien	Cet appareil numérique de la classe A est conforme à la norme NMB-003 (A) du Canada.

Responsible party for Supplier's Declaration of Conformity

Siemens Industry, Inc.

Digital Factory - Factory Automation

5300 Triangle Parkway, Suite 100

Norcross, GA 30092

USA

Mail to: (amps.automation@siemens.com)

UL approval



The following approvals are available for the device:

- Underwriters Laboratories (UL) in accordance with Standard UL61010-1 and UL61010-2-201, File E472609
- Canadian National Standard CAN/CSA No.61010-1-12 and CAN/CSA C22.2 No.61010-2-201

Identification for Eurasian Customs Union



- EAC (Eurasian Conformity)
- Customs union of Russia, Belarus and Kazakhstan
- Declaration of conformity according to Technical Regulations of the Customs Union (TR CU)

RCM (Australia / New Zealand)



This product meets the requirements of EN 61000-6-3 Generic standards - Emission standard for residential, commercial and light-industrial environments.

This product meets the requirements of the standard EN 61000-6-3 Generic standards - Emission standard for residential, commercial and light-industrial environments.

Korea Certificate



This product meets the requirements of Korean certification.

This product satisfies the requirement of the Korean Certification (KC Mark).



The device complies with the designated British standards (BS) for IPC published in the official consolidated list of the British Government. The device meets the requirements and protection targets of the following regulations and related amendments:

- Electrical Equipment (Safety) Regulations 2016 (Low-Voltage)
- Electromagnetic Compatibility Regulations 2016 (EMC)
- Regulations on the restriction of the use of certain hazardous substances in electrical and electronic equipment 2012 (RoHS).

UK Declarations of Conformity for the respective authorities are available from:

Siemens AG
Digital Industries
Factory Automation
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg

The UK Declaration of Conformity is also available for download from the Siemens Industry Online Support website under the keyword "Declaration of Conformity".

BIS



This product meets the requirements of India certification.



This product meets the requirements of CNS14336-1(099/09/30), CNS15936(105) generic standard.

Table 8- 1 限用物質含有情況標示聲明

設備名稱：Industrial PC, 型號（型式）：BX-35A Equipment name Type designation (Type)						
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr ⁺⁶)	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
外殼	○	○	○	○	○	○
電路板	○	○	○	○	○	○
固態硬碟	-	○	○	○	○	○
線材	○	○	○	○	○	○
備考 1. "超出 0.1 wt %"及"超出 0.01 wt %" 係指限用物質之百分比含量超出百分比含量基準值。 Note 1: "Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition. 備考 2. "○" 係指該項限用物質之百分比含量未超出百分比含量基準值。 Note 2: "○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence. 備考 3. "-" 係指該項限用物質為排除項目。 Note 3: The "-" indicates that the restricted substance corresponds to the exemption.						

Responsible party for Supplier's Declaration of Conformity

西門子股份有限公司

臺北市 11503 南港區園區街 3 號 8 樓

電子郵件信箱: (Adscs.taiwan@siemens.com)

WEEE label (European Union)



Disposal instructions, observe the local regulations and the section "Recycling and disposal (Page 66)".

8.2 Directives and declarations

8.2.1 Electromagnetic compatibility, Industrial and Residential Areas

Electromagnetic compatibility

This product meets the requirements of EU Directive 2014/30/EU "Electromagnetic Compatibility".

The device is designed for the following areas of application corresponding to the CE marking:

Scope of application	Requirements for	
	Interference emission	Immunity to interference
Industrial area	EN 61000-6-4 +A1, CAN/CSA-CISPR 32	EN 61000-6-2

8.2.2 RoHS directive

This product meets the requirements stated in the RoHS directive (Restriction of Hazardous Materials): 2011/65/EU

Compliance with the directive has been reviewed according to the following standard: EN IEC63000

8.2.3 ESD guideline

What does ESD mean?

An electronic module is equipped with highly integrated components. Due to their design, electronic components are highly sensitive to overvoltage and thus to the discharge of static electricity. Such electronic components or modules are labeled as electrostatic sensitive devices.

The following abbreviations are commonly used for electrostatic sensitive devices:

- ESD – Electrostatic sensitive device
- ESD – Electrostatic Sensitive Device as a common international designation

Electrostatic sensitive devices can be labeled with an appropriate symbol.



NOTICE

Damage to ESD from touch

Electrostatic sensitive devices, ESD, can be destroyed by voltages which are far below the human perception limit. If you touch a component or electrical connection of a module without discharging any electrostatic energy, these voltages may arise.

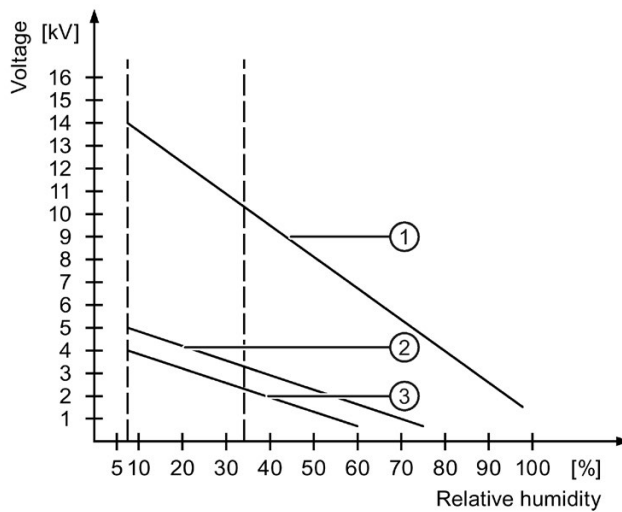
The damage to a module by an overvoltage can often not be immediately detected and only becomes evident after an extended period of operation. The consequences are incalculable and range from unforeseeable malfunctions to a total failure of the machine or system.

Avoid touching components directly. Make sure that persons, the workstation and the packaging are properly grounded.

Charge

Every person without a conductive connection to the electrical potential of his/her surroundings can be electrostatically charged.

The material with which this person comes into contact is of particular significance. The figure shows the maximum electrostatic voltages with which a person is charged, depending on humidity and material. These values conform to the specifications of IEC 61000-4-2.



- ① Synthetic materials
- ② Wool
- ③ Antistatic materials such as wood or concrete

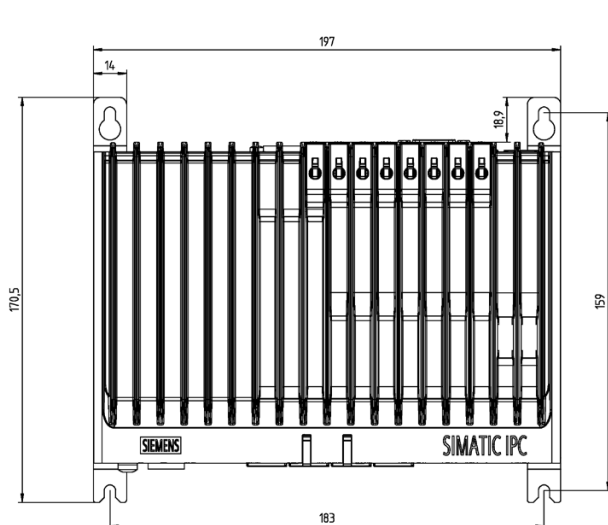
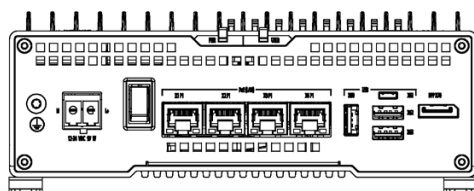
NOTICE
Grounding measures
There is no equipotential bonding without grounding. An electrostatic charge is not discharged and may damage the ESD.
Protect yourself against discharge of static electricity. When working with electrostatic sensitive devices, make sure that the person and the workplace are properly grounded.

Protective measures against discharge of static electricity

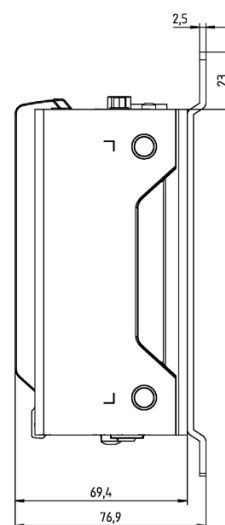
- Disconnect the power supply before you install or remove modules which are sensitive to ESD.
- Pay attention to good grounding:
 - When handling electrostatic sensitive devices, make sure that persons, the workstation and devices, tools and packaging used are properly grounded. This way you avoid static discharge.
- Avoid direct contact:
 - As a general rule, do not touch electrostatic sensitive devices, except in the case of unavoidable maintenance work.
 - Hold the modules at their edge so that you do not touch the connector pins or conductor paths. This way, the discharge energy does not reach and damage the sensitive components.
 - Discharge your body electrostatically before you take a measurement at a module. Do so by touching grounded metallic parts. Always use grounded measuring instruments.

8.3 Dimension drawings

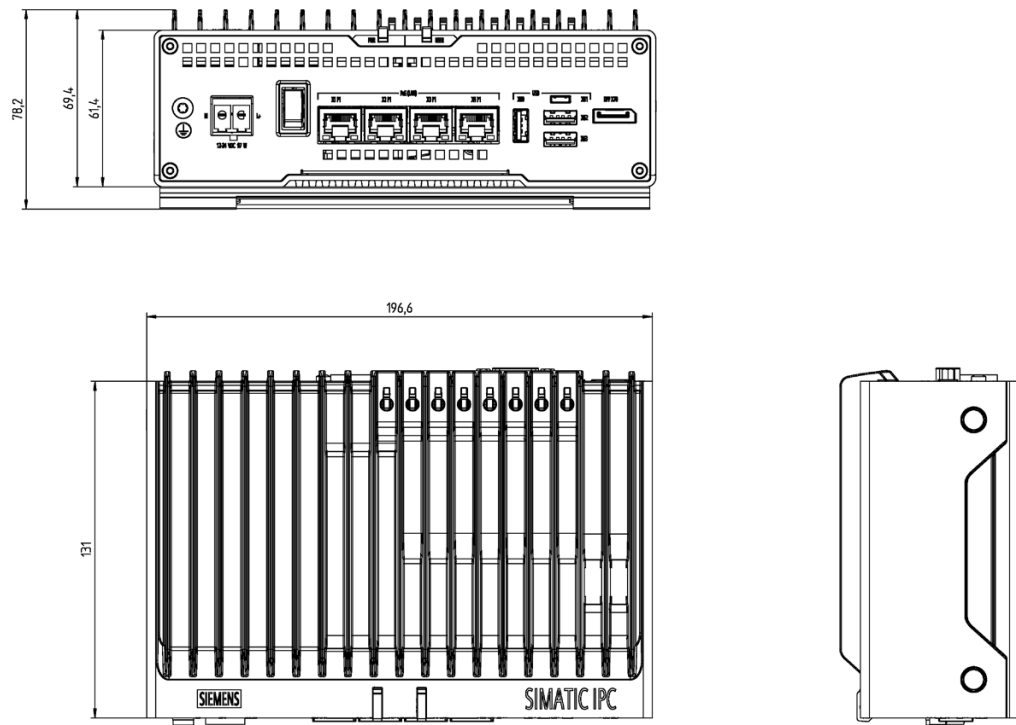
Wall mounting



All dimensions in mm.



Mounting on a standard rail



All dimensions in mm.

8.4 General technical specifications

General technical specifications

Weight without mounting brackets	Approx. 1760.0 g
Power supply	DC 12-24 V (9 to 36 V)
Brief voltage interruption in accordance with Namur	Up to 10 ms buffer time at 9 V DC and full load ¹ Up to 20 ms buffer time at 12 V DC and full load ¹
Power consumption	Max. 10.9 A (at 9 V)
Noise emission	< 55 dB(A) in accordance with DIN 45635-1
Degree of protection	IP20 in accordance with IEC 60529
Protection class	Protection class III in accordance with IEC 61140
Degree of pollution	Device is designed for environments with pollution degree 2
Quality assurance	In accordance with ISO 9001

¹ : In the event of low supply voltage, the buffer time is reduced.

8.4 General technical specifications

Electromagnetic compatibility

Radiation Emission (Enclosure port) in accordance with IEC 61000-6-4 + A1/ CAN/CSA-CISPR 32	30 to 230 MHz: 50 dB(μV/m) Quasi-peak (3 m distance) 230 to 1000 MHz: 57 dB (μV/m) Quasi-peak (3 m distance) 1 to 3 GHz: 76 dB (μV/m) Peak; 56 dB (μV/m) Average (3 m distance) 3 to 6 GHz: 80 dB (μV/m) Peak; 60 dB (μV/m) Average (3 m distance)
Immunity with regard to conducted interference on supply lines	± 2 kV (5 kHz /100 kHz) in accordance with IEC 61000-4-4; Burst ± 1 kV line to line, ±2 kV line to earth in accordance with IEC 61000-4-5; Surge
Immunity on the signal lines	Burst: ± 1 kV (5 kHz /100 kHz) in accordance with IEC 61000-4-4; Length of signal port extension cable < 30 m ± 2 kV (5 kHz /100 kHz) in accordance with IEC 61000-4-4; Length of signal port extension cable ≥ 30 m Surge: ± 1 kV line-to-line; ± 2 kV line-to-earth in accordance with IEC 61000-4-5
Immunity to discharges of static electricity	± 6 kV contact discharge in accordance with IEC 61000-4-2 ± 8 kV air discharge in accordance with IEC 61000-4-2
Immunity to RF interference	Radiation Immunity (according to IEC 61000-4-3) 80 MHz to 2.7GHz 10 V/m, 80 % AM (1 kHz) 2.7 GHz to 6.0 GHz 3 V/m, 80 % AM (1 kHz) Conducted Immunity (according to IEC 61000-4-6) 10 kHz to 80MHz: 10 V, 80% AM (1kHz)
Conducted Emission (Low voltage DC mains port), in accordance with IEC 61000-6-4 + A1	0.15 to 0.5 MHz / 89 dB (μV) Q, 76 dB (μV) M 0.5 to 30 MHz / 83 dB (μV) Q, 70 dB (μV) M
Conducted Emission (Telecommunications/Network Port), in accordance with IEC 61000-6-4 + A1	0.15 to 0.5 MHz: 97 dB(μV) to 87 dB(μV) Q 84 dB(μV) to 74 dB(μV) M
	0.5 MHz to 30 MHz: 87 dB(μV) Q / 74 dB(μV) M

Motherboard

SOM (System on Module)	Processor and RAM	6-Core NVIDIA ARM v8.2 (64bit) Processor, 8GB LPDDR5 8-Core NVIDIA ARM v8.2 (64bit) Processor, 16GB LPDDR5
	QSPI Flash	64 Mb on board QSPI flash

Carrier board	Nano SIM card	Slot for one Nano SIM card
	Storage	• Without SSD • 256GB NVMe SSD • 512GB NVMe SSD • 1TB NVMe SSD
	Expansion slots	Slot X100: 1 × M.2 E Key WiFi/BT 2230 with E Key Slot X101: 1 × M.2 B Key WWAN 2242, 2260, 3042, 3052, 3060 with B key

Interfaces

USB	• 1 × USB 2.0 Micro USB (X61) • 3 × USB 3.0 Gen 1 Type A (X60, X62, X63)
DisplayPort (X70)	• 1 × DisplayPort interface (DP)
Ethernet port	4 × Gbe RJ45 (X1, X2, X3, X4) with Addition PoE Function ¹
COM (X30)	• RS232, max. 115 Kbps, D-sub connector, 9-pin • RS422, max. 115 Kbps, D-sub connector, 9-pin • RS485, max. 115 Kbps, D-sub connector, 9-pin
Digital I/O Connector (X10)	• 4 × DI + 4 × DQ
CAN BUS (X11)	1× isolated CAN FD port

¹ : Siemens recommends that PoE Ethernet port only connect to the PD device and non-PoE ethernet device.

8.5 Ambient conditions

Climatic ambient conditions

For permitted mounting positions, see section "Permitted mounting positions and mounting types (Page 23)".

Ambient temperature tested in accordance with IEC 60068-2-1, IEC 60068-2-2 and IEC 60068-2-14	
Operation	15W CPU, 30W PoE, 3W M.2 B key and E key module: 0°C to 50°C 25W CPU, 15W PoE: 0°C to 40°C *
Storage/transport	-20 to 70 °C
Gradient	
Operation	Max. 10 °C/h
Storage	20 °C/h, no condensation
Relative humidity , tested in accordance with IEC 60068-2-78, IEC 60068-2-30	
Operation	up to 85% at 30°C, no condensation
Storage/transport	up to 95 % at 25/55 °C, no condensation

Atmospheric pressure, Altitude	
Operation	1140 to 795 hPa, corresponds to an elevation of -1000 m to 2000 m
Storage/transport	1140 to 660 hPa, corresponds to an elevation of -1000 to 3500 m

Multiplication factors for equipment ambient temperature of operation at altitudes up to 3000 m, tested in accordance with IEC 61131-2:2017	
Altitude	Derating ratio for temperature ¹
0 to 2000 m ²	1.0
3000 m	0.9

* : 15W CPU, 30W POE, 7W M.2 B key and E key module: 0°C to 45°C

¹ : Equipment ambient temperature rating at 2000 m.

² : Atmospheric pressure and air density increases with decreasing altitude. Therefore, utilization of the derating factor for 0 m to 2000 m for altitudes below sea level is considered conservative.

Mechanical ambient conditions

Vibration resistance, tested in accordance with IEC 60068-2-6	
Operation	Except DIN-Rail: • 5 to 8.4 Hz: 3.5 mm • 8.4 to 200 Hz: 9.8 m/s² DIN-Rail: • 10 to 58 Hz: 0.0375 mm • 58 to 200 Hz: 4.9 m/s²
Storage/transport	• 5 to 8.4 Hz: 3.5 mm • 8.4 to 500 Hz: 9.8 m/s²
Shock resistance, tested in accordance with IEC 60068-2-27	
Operation	• 150 m/s², 11 ms
Storage/transport	• 250 m/s², 6 ms

8.6 Power demand of the components

Maximum power consumption of the auxiliary components

For the ambient temperature for permitted mounting position, refer to Ambient conditions (Page 77).

Auxiliary components		Maximum permitted power consumption		Maximum total power	
		+5 V	+3.3 V		
USB device 3.0	High current	900 mA	--	6.5 W (for all USB devices)	
M.2 B Key module	Per slot	--	1.5 A	M.2 B Key connector: max. 7W	Permitted power distribution: Total: 10W
M.2 E Key module	Per slot	--	0.6 A	M.2 E Key connector: max. 2.5W	
M.2 M Key module	Per slot	--	1.5 A	M.2 M Key connector: max. 3W	

8.7 Direct current supply (DC)

Technical specifications

Input voltage	Rated voltage range: 12-24 V DC Normal operation voltage range: 9-36V
Power consumption	Max. 97 W

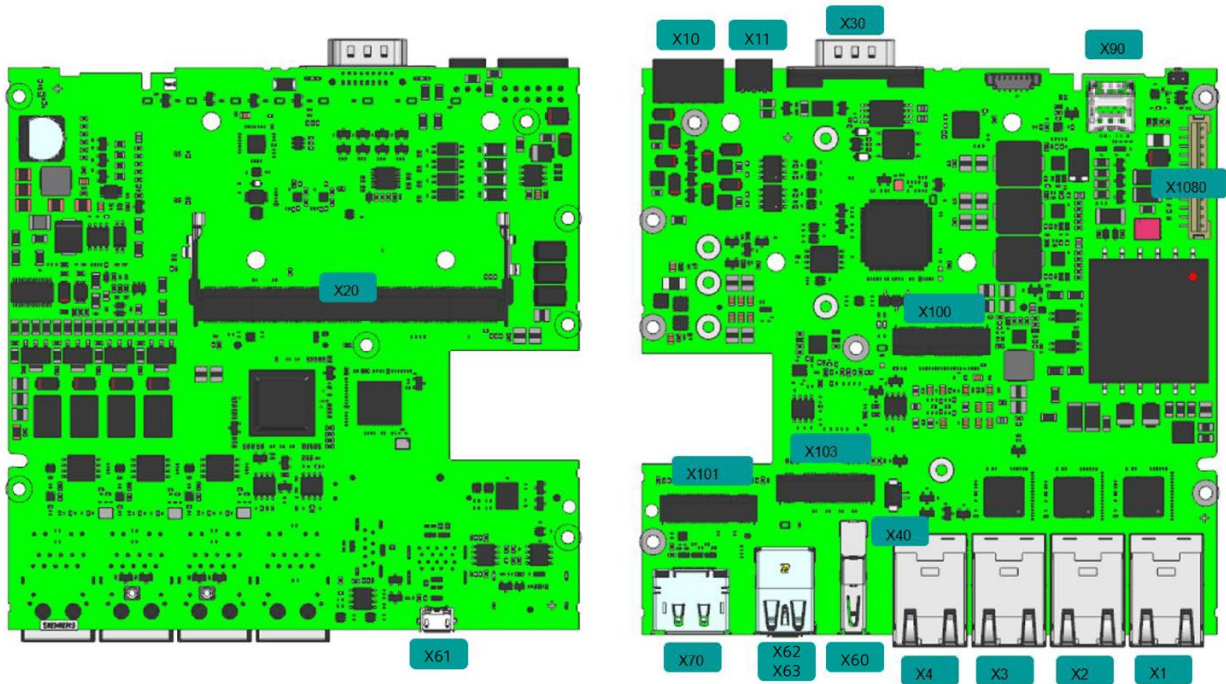
Typical power consumption

	Power consumption (at a rated voltage of 12-24 V)
Basic device	12 W
POE max. load	1 × 30 W or 2 × 15 W or 4 × 7.5 W
USB port max. load	6.5 W
Orin NX modules	20 W for 8GB 25 W for 16GB

8.8 Hardware descriptions

8.8.1 Motherboard

The following figures show the motherboard of the SIMATIC IPC BX-35A.



Component/interface	Description	Meaning
X1	Ethernet 1	RJ45 POE optional
X2	Ethernet 2	RJ45 POE optional
X3	Ethernet 3	RJ45 POE optional
X4	Ethernet 4	RJ45 POE optional
X10	Digital interface	4 × DI + 4 × DQ
X11	CAN BUS	
X30	COM D-Sub9	RS232/RS422/RS485
X60, X62, X63	USB A Host	3 × USB3.0
X61	Micro B	1 × USB2.0
X70	DisplayPort	
X90	SIM card slot	
X1080	Power supply	
X103	M.2 M Key	Support NVMe SSD x1
X101	M.2 B Key	Support WWAN card through PCIe x1/USB3.0
X100	M.2 E Key	Support WiFi/BT card through PCIe x1/USB2.0/I2S/UART
X40	Coin battery connector	
X20	SoM (System-on-Module) slot	support NVIDIA® Jetson™ Orin NX 8GB/16GB

8.8.2 External Interfaces

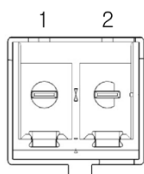
8.8.2.1 Overview of external interfaces

Interface	Position	Description
USB	External	1 × USB 2.0 Micro B (X61) 3 × USB 3.0 Type A (X60, X62, X63)
Ethernet port	External	4 × Gbe RJ45 (X1P1, X2P1, X3P1, X4P1) with POE function
DisplayPort (X70)	External	1 × DP
COM (X30)	External	- RS232, max. 115 Kbps, D-sub connector, 9-pin - RS422, max. 115 Kbps, D-sub connector, 9-pin - RS485, max. 115 Kbps, D-sub connector, 9-pin
Digital I/O Connector (X10)	External	4 × DI + 4 × DQ
CAN connector (X11)	External	1 × CAN BUS connector

8.8.2.2 Power supply

Plug connector, 2-pin

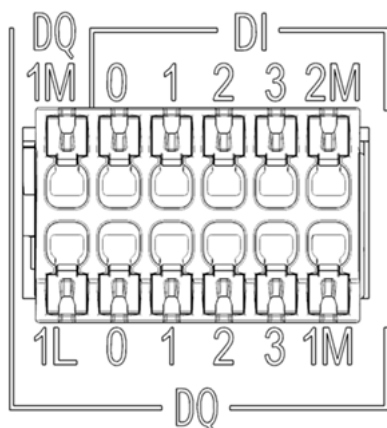
Name of interface on the device: X80



Pin	Assignment
1	GND (M)
2	DC 12-24 V (9 to 36 V DC) (L+)

8.8.2.3 Digital I/O connector

Name of interface on the device: X10



Short description	Meaning	GPIO number
DI0	Digital signal input 0	453
DI1	Digital signal input 1	446
DI2	Digital signal input 2	328
DI3	Digital signal input 3	329
DI_2M	Digital signal reference M	
DQ_1M	Digital signal output reference M	
DQ_1L	Digital signal output reference L	
DQ_1M	Digital signal output reference M	
DQ0	Digital signal output 0	330
DQ1	Digital signal output 1	331
DQ2	Digital signal output 2	465
DQ3	Digital signal output 3	450

Note

The GPIO number may be changed after the Jetpack update.

Enter the following command in the console to get the real GPIO number.

- `sudo cat /sys/kernel/debug/gpio | grep "DI_n/DQ_n"`
- `sudo dmesg | grep DQ_n/DI_n` (If GPIO is exported after startup)

n refers to the number (0~3) for DI or DQ.

General specifications and DI features

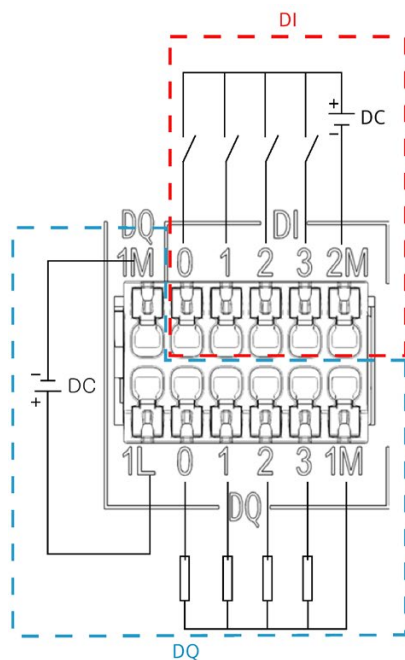
Technical data	Digital inputs
Number of inputs	4
Type	Sink

Technical data	Digital inputs
Rated voltage	24 V DC at 4 mA, nominal
Continuous permissible voltage	30 V DC, max.
Surge voltage	35 V DC for 0.5 sec.
Logic 1 signal (min.)	12 V DC at 2.5 mA
Logic 0 signal (max.)	5 V DC at 1 mA
Isolation (field side to logic)	500 V AC for 1 minute
Input frequency	• Normal input • High speed input
	• Max. 20 Hz • --

General specifications and DQ features

Technical data	Digital Outputs
Number of outputs	4
Type	Solid state - MOSFET (sourcing)
Voltage range	20.4 to 28.8 V DC
Continuous permissible voltage	30 V DC, max.
Surge voltage	35 V DC for 0.5 sec.
Logic 1 signal at max. current	20 V DC min.
Logic 0 signal with 10 K Ω load	0.1 V DC max.
Rated current per point (max.) (Resistive load)	0.5 A
Rated current per point (max.) (pilot duty)	0.5 A
Rated current per common (max.)	2 A
Lamp load (Tungsten)	5 W
ON state resistance	0.034 Ω max.
Leakage current per point	10 μ A max.
Surge current	8 A for 100 ms max.
Overload protection	No
Isolation (field side to logic)	500 V AC for 1 minute
Switching rate	
Mechanical	--
Electrical	10 Hz
Resistive load/lamp load (Tungsten)	10 Hz
Inductive load (pilot duty)	0.5 Hz

Wiring diagrams

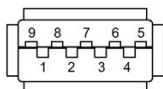


Digital I/O connector uses a double-level terminal block for connection. For more information, refer to Digital I/O and CAN terminal block (Page 95).

8.8.2.4 USB

USB 3.0 Type A

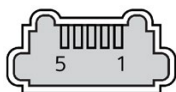
Name of interface on the device: USB-- X60 --- X62--- X63



Pin	Short name	Meaning	Input / output
1	VBUS	+ 5 V (Power switch)	Power out
2	D-	Data channel USB2	Input / output
3	D+	Data channel USB2	Input / output
4	GND	Ground	–
5	RX-	Data channel USB3	Input
6	RX+	Data channel USB3	Input
7	GND	Ground	–
8	TX-	Data channel USB3	Output
9	TX+	Data channel USB3	Output

USB 2.0 Micro B

Name of interface on the device: X61

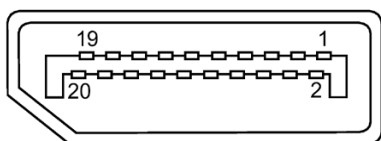


Pin	Assignment
1	+5 V DC, in (max. 500 mA)
2	USB-DN
3	USB-DP
4	NC
5	GND

8.8.2.5

DisplayPort

Name of interface on the device: X70

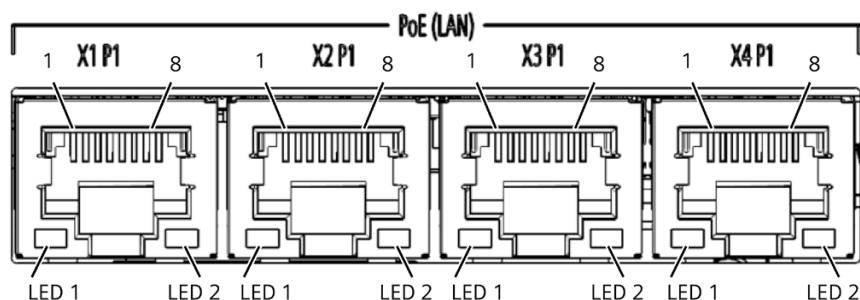


DisplayPort interface			
Pin no.	Abbreviation	Meaning	Input/output
1	ML_Lane 0+	DP data 0+	Output
2	GND	Ground	-
3	ML_Lane 0-	DP data 0-	Output
4	ML_Lane 1+	DP data 1+	Output
5	GND	Ground	-
6	ML_Lane 1-	DP data 1-	Output
7	ML_Lane 2+	DP data 2+	Output
8	GND	Ground	-
9	ML_Lane 2-	DP data 2-	Output
10	ML_Lane 3+	DP data 3+	Output
11	GND	Ground	-
12	ML_Lane 3-	DP data 3-	Output
13	CONFIG1	CONFIG1	-
14	CONFIG2	CONFIG2	-
15	AUX_CH+	Auxiliary channel+	Bidirectional
16	GND	Ground	-
17	AUX_CH-	Auxiliary channel-	Bidirectional
18	HPD	Hot Plug Detect	Input
19	GND	Ground	-
20	DP_PWR	+3.3 V (Power switch)	power out

8.8.2.6 Ethernet port

RJ45 socket

Name of interface on the device: X1P1; X2P1; X3P1; X4P1

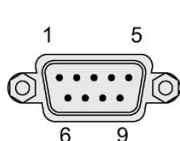


Pin no.	Short description	Meaning	Input / output
1	BI_DA+	Bi-directional data A+	Input/output
2	BI_DA-	Bi-directional data A-	Input/output
3	BI_DB+	Bi-directional data B+	Input/output
4	BI_DC+	Bi-directional data C+	Input/output
5	BI_DC-	Bi-directional data C-	Input/output
6	BI_DB-	Bi-directional data B-	Input/output
7	BI_DD+	Bi-directional data D+	Input/output
8	BI_DD-	Bi-directional data D-	Input/output
S		Shield	—
	LED 1	Green light: 1000 Mbps Off: Else	—
	LED 2	Orange light: Link Orange Blink: Activity Off: No Link	—

8.8.2.7 Serial port

D-sub socket, 9-pin, with screw lock

Name of interface on the device: X30 COM



RS 232

RS 422

RS 485

Assignment RS 232

Pin	Short description	Meaning
1	nc	
2	RxD	Received data (I)
3	TxD	Transmitted data (O)
4	nc	
5	M	Ground
6	nc	
7	RTS	Request to send (O)
8	CTS	Clear to send (I)
9	nc	

Assignment RS 422

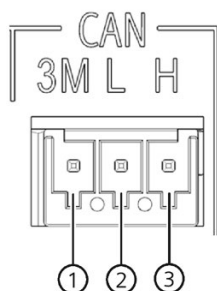
Pin	Short description	Meaning
1	TX-	Transmitted data - (O) for full-duplex mode
2	TX+	Transmitted data + (O) for full-duplex mode
3	RX+	Receive data + (I) for full-duplex mode
4	RX-	Receive data - (I) for full-duplex mode
5	M	Signal ground
6	nc	
7	nc	
8	nc	
9	nc	

Assignment RS 485

Pin	Short description	Meaning
1	Data-	Transmit / receive data - (I/O) for half-duplex mode
2	Data+	Transmit / receive data+ (I/O) for half-duplex mode
3	nc	
4	nc	
5	M	Signal ground
6	nc	
7	nc	
8	nc	
9	nc	

8.8.2.8 CAN port

Name of interface on the device: **X11**



CAN BUS interface		
Pinno.	Abbreviation	Meaning
1	3M	CAN ground, isolated
2	CAN_L	CAN BUS low signal
3	CAN_H	CAN BUS high signal

8.8.3 Internal interfaces

8.8.3.1 Overview of internal interfaces

Interface	Position	Description
Nano SIM card slot (X90)	Internal	1 × SIM card slot
M.2 E Key (X100)	Internal	Support WiFi/BT card through PCIe ×1/USB2.0/I2S/UART
M.2 B Key (X101)	Internal	Support WWAN card through PCIe ×1/USB2.0/USB3.0 and flex module
M.2 M Key (X103)	Internal	Support NVME SSD card through PCIe GEN4 ×4

8.8.3.2 M.2 interface

M.2 E Key module

Name of interface on the device: X100

Pin no.	Signal	Signal	Pin no.
		GND	75
74	3.3V	NC	73
72	3.3V	NC	71
70	NC	GND	69
68	NC	NC	67

66	NC	NC	65
64	NC	GND	63
62	M2E_ALERT_N	NC	61
60	I2C2_SCL	NC	59
58	I2C2_SDA	GND	57
56	DISABLE_WIFI_N	PCIE_WAKE_N	55
54	DISABLE_BT_N	PCIE1_CLKREQ_N	53
52	PCIE1_RST_N	GND	51
50	SUSCLK_M2_EKEY	PCIE1_CLK_N	49
48	COEX_TXD_M2E	PCIE1_CLK_P	47
46	COEX_RXD_M2E	GND	45
44	COEX3_M2E	PCIE1_RX0_N	43
42	NC	PCIE1_RX0_P	41
40	NC	GND	39
38	NC	PCIE1_TX0_N	37
36	UART0_RTS_N	PCIE1_TX0_P	35
34	UART0_CTS_N	GND	33
32	UART0_TXD	CONNECTOR KEY E	31
30	CONNECTOR KEY E	CONNECTOR KEY E	29
28	CONNECTOR KEY E	CONNECTOR KEY E	27
26	CONNECTOR KEY E	CONNECTOR KEY E	25
24	CONNECTOR KEY E	NC	23
22	UART0_RXD	NC	21
20	NC	NC	19
18	GND	NC	17
16	NC	NC	15
14	I2S1_DOUT	NC	13
12	I2S1_DIN	NC	11
10	I2S1_FS	NC	9
8	I2S1_SCLK	GND	7
6	NC	USB2_D_N_CONN	5
4	3.3V	USB2_D_P_CONN	3
2	3.3V	GND	1

M.2 B Key module

Name of interface on the device: X101

Pin no.	Signal	Signal	Pin no.
		NC	75
74	3.3V	GND	73
72	3.3V	GND	71
70	3.3V	CFG1	69
68	SUSCLK	RESET#	67
66	SIM_DETECT (optional)	ANTCTL3	65
64	COEX_RXD	ANTCTL2	63
62	COEX_TXD	ANTCTL1	61

60	COEX_NC	ANTCTL0	59
58	NC	GND	57
56	NC	REFCLKp	55
54	PEWAKE#	REFCLKn	53
52	CLKREQ#	GND	51
50	PERST#	PETp0	49
48	NC	PETn0	47
46	NC	GND	45
44	NC	PERp0	43
42	SMB_DATA	PERn0	41
40	SMB_CLK	GND	39
38	DEVSLP	USB3_TP	37
36	NC	USB3_TN	35
34	NC	GND	33
32	NC	USB3_RP	31
30	NC	USB3_RN	29
28	NC	GND	27
26	NC	NC	25
24	NC	NC	23
22	NC	NC	21
20	NC	CONNECTOR KEY B	19
18	CONNECTOR KEY B	CONNECTOR KEY B	17
16	CONNECTOR KEY B	CONNECTOR KEY B	15
14	CONNECTOR KEY B	CONNECTOR KEY B	13
12	CONNECTOR KEY B	GND	11
10	NC	USB_D-	9
8	W_DISABLE#	USB_D+	7
6	WWAN_PWR_OFF_N	GND	5
4	3.3V	GND	3
2	3.3V	NC	1

M.2 M Key module

Name of interface on the device: X100

Pin no.	Signal	Signal	Pin no.
		GND	75
74	3.3V	GND	73
72	3.3V	GND	71
70	3.3V	NC	69
68	SUSCLK_M2_MKEY	NC	67
58	NC	GND	57
56	NC	PCIE0_CLK_P	55
54	NC	PCIE0_CLK_N	53
52	PCIE0_CLKREQ_N	GND	51
50	PCIE0_RST_N	PCIE0_TX0_P_C	49
48	NC	PCIE0_TX0_N_C	47

46	NC	GND	45
44	M2M_ALERT_N	PCIE0_RX0_P	43
42	NC	PCIE0_RX0_N	41
40	NC	GND	39
38	NC	PCIE0_TX1_P_C	37
36	NC	PCIE0_TX1_N_C	35
34	NC	GND	33
32	NC	PCIE0_RX1_P	31
30	NC	PCIE0_RX1_N	29
28	NC	GND	27
26	NC	PCIE0_TX2_P_C	25
24	NC	PCIE0_TX2_N_C	23
22	NC	GND	21
20	NC	PCIE0_RX2_P	19
18	3.3V	PCIE0_RX2_N	17
16	3.3V	GND	15
14	3.3V	PCIE0_TX3_P_C	13
12	3.3V	PCIE0_TX3_N_C	11
10	SSD_ACTIVE_LED	GND	9
8	PLN#	PCIE0_RX3_P	7
6	NC	PCIE0_RX3_N	5
4	3.3V	GND	3
2	3.3V	GND	1

Technical support

A.1 Service and support

You can find additional information and support for the products described on the Internet at the following addresses:

- Technical support (<https://support.industry.siemens.com>)
- Support request form (<https://support.industry.siemens.com/cs/my/src>)
- After Sales Information System SIMATIC IPC/PG (<http://www.siemens.com/asis>)
- Documentation for SIMATIC Industrial PCs (<https://support.industry.siemens.com/cs/us/en/view/109744171>)
- Your local representative (https://www.automation.siemens.com/aspa_app)
- Training center (<https://www.sitrain-learning.siemens.com/PLG/?AppLang=en>)
- Industry Mall (<https://mall.industry.siemens.com/>)

When contacting your local representative or Technical Support, please have the following information at hand:

- MLFB of the device
- Other installed hardware
- Other installed software

Tools & downloads

Please check regularly if updates and hotfixes are available for download to your device. The download area is available on the Internet at the following link:

After Sales Information System SIMATIC IPC/PG (<http://www.siemens.com/asis>)

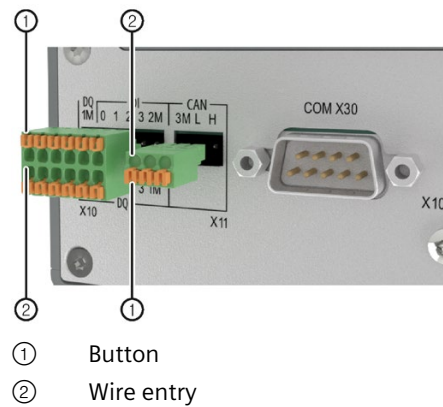
A.2 Troubleshooting

This chapter provides you with tips on how to locate and/or troubleshoot problems.

Problem	Possible cause	Possible remedy
The device is not operational	No power supply	- Check the power supply, the power cord and the power plug. - Check if the On/Off switch is in the correct position.
	Device is being operated outside the specified ambient conditions	- Check the ambient conditions. - After transport in cold weather, wait approximately 12 hours before switching on the device.
The mouse pointer does not appear on the screen	The mouse driver is not loaded	Check whether the mouse driver is properly installed and available when you start the user program. Detailed information about the mouse driver is available in the corresponding documentation.
	Mouse not connected	- Check whether the mouse cord is properly connected to the system unit. - If you use an adapter or extension for the mouse cable, also check these connectors.
		If the mouse pointer still does not appear on the screen after you have performed these checks and actions, contact your technical support team.
USB device does not respond	The USB ports are not correctly supported.	You need to install the USB device drivers for the required operating system.

Digital I/O and CAN terminal block

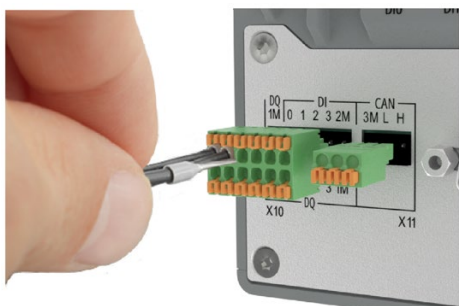
Digital I/O connector uses a double-level terminal block with simple and reliable connection.



Requirements

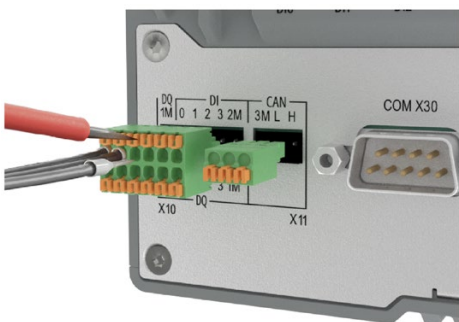
- The device is disconnected from the power supply.
- Type of wire:
 - Solid
 - Flexible
 - Stranded
- Clamping range:
 - without plastic collar ferrule: 0.2 mm² to 1.5m²
 - with plastic collar ferrule: 0.2 mm² to 0.75m²
- A screwdriver

Procedure for wiring connection



Flexible wire with ferrule and solid:

1. Push the wire directly into wire entry.



Flexible wire without ferrule:

1. Push button with a screwdriver and keep pressing the button with the screwdriver.
2. Put the wire into the wire entry.
3. Release the button.

Procedure for wiring release

Follow the above steps in reverse direction to release the wire.

Markings and symbols

C.1 Overview

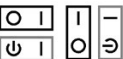
The following tables show all the symbols which may be found on your SIMATIC industrial PC, SIMATIC industrial monitor or SIMATIC Field PG in addition to the symbols which are explained in the operating instructions.

The symbols on your device may vary in some details from the symbols shown in the following tables.

C.2 Safety

Symbol	Meaning		Symbol	Meaning
	Warning, observe the supplied documentation.			Lock is closed
	Attention, radio equipment			Lock is open
	Disconnect the power plug before opening			Opening for Kensington lock
	Attention ESD (Electrostatic sensitive device)			Warning of hot surface

C.3 Operator controls

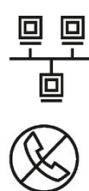
Symbol	Meaning		Symbol	Meaning
	On/off switch, without electrical isolation			Eject CD/DVD
	On/off switch, without electrical isolation			

C.4 Certificates, approvals and markings

The following table shows symbols relating to certificates, approvals and markings which may be on the device. You can find more information in the operating instructions for your device:

Symbol	Meaning	Symbol	Meaning
 	Approved for Australia and New Zealand		Marking for the Eurasian Customs Union
	Approved for China		Test mark of Factory Mutual Research
	CE markings for European countries		Marking of Federal Communications Commission for the USA
	EFUP (Environment Friendly Use Period) marking for China		Approved for Korea
	Test mark of the Underwriters Laboratories		Disposal information, observe the local regulations.

C.5 Interfaces

Symbol	Meaning	Symbol	Meaning
	Connection to the power supply		PS/2 mouse interface
	Protective conductor terminal		PS/2 keyboard-interface
	Connection for functional earthing (equipotential bonding line)		Multimedia Card Reader
DPP	DisplayPort interface		Smart Card Reader
	DVI-D interface		Line In
LAN 	LAN interface, not approved for connecting WAN or telephone		Line Out
	Serial port		Microphone input
	USB port		Universal Audio Jack
	USB 2.0 high-speed port		Headphone output
	USB 3.0 super-speed port		

List of abbreviations

ACPI	Advanced Configuration and Power Interface	
BIOS	Basic Input Output System	
CE	Communauté Européenne	
COM	Communications Port	Term for the serial interface
CPU	Central Processing Unit	CPU
CSA	Canadian Standards Association	Canadian organization for tests and certifications according to national or binational standards
CTS	Clear To Send	Clear to send
DC	Direct Current	DC current
DCD	Data Carrier Detect	Data carrier signal detection
DLP	Data Leakage Protection	
DQS	Deutsche Gesellschaft zur Zertifizierung von Qualitätsmanagement mbH	
DSR	Data Set Ready	Ready for operation
DTB	Device Tree Binary file	
DTR	Data Terminal Ready	Data terminal is ready
ESD	Components sensitive to electrostatic charge	
EN	European standard	
ESD	Electrostatic Sensitive Device	Electrostatic Sensitive Devices
	Electrostatic discharge	Electrostatic discharge
GND	Ground	Chassis ground
IDE	Integrated Device Electronics	
IEC	International Electrotechnical Commission	
LAN	Local Area Network	Computer network that is limited to a local area.
LED	Light Emitting Diode	Light emitting diode
LPS	Limited Power Source	
MAC	Media access control	Media access control
MLFB	Machine-readable product designation	
PC	Personal computer	
PCB	Printed circuit board	
PCIe	Peripheral Component Interconnect express	High-speed serial, differential full-duplex PtP interface with high data rate.
PELV	Protective extra-low voltage	
PG	Programming device	
PoE	Power over Ethernet	
PSE	Power Sourcing Equipment	

RI	Ring Input	Incoming call
RSA	Rivest Shamir Adleman	
RTS	Request to send	Request to send
RxD	Receive Data	Data transfer signal
SELV	Safety Extra Low Voltage	Safety extra low voltage
SHA	Secure Hash Algorithm	
UEFI	Unified Extensible Firmware Interface	
UID	Unique ID	
UL	Underwriters Laboratories Inc.	US organization for testing and certification according to national or binational standards.
USB	Universal Serial Bus	

Index

A

Approval, (EAC)

B

Backup battery, 66
BSMI, 70

C

Certificates
 Certifications and approvals, 67
Clearance, 23
COM, 81
Components sensitive to electrostatic charge, 71
Condensation, 22
Connecting
 Peripherals, 28
 Power supply, 30
 protective conductor, 29
Connecting the protective conductor, 30

D

DC power supply, 79
Degree of pollution, 75
Degree of protection, 75
Digital I/O Connector, 81
Directive
 ESD Directive, 71
DisplayPort, 81
DisplayPort interface, 85, 88

E

EAC, 69
ESD, 71
ESD Directive, 71
Ethernet port, 81
Expansion slot, 77

F

FCC, 68
Features, 9
Flash, 76
Front view, 10

G

General technical specifications, 75

I

Identification data, 22
Installation on a DIN rail, 23
Interface
 DisplayPort, 85, 88
Interfaces, 77
 USB 3.0, 84

K

Korea Certificate, 69

L

Limitation of liability, 16, 63
Lithium battery, 64

M

M.2 module
 Installing, 56
 Removing, 57
Micro SD card or Nano SIM card, 57
Motherboard
 Technical features, 80
Mounting
 Wall, 27
Mounting on a standard rail, 75
Mounting position, 23
Mounting type, 23, 24

N

New Zealand
RCM, 69
Noise emission, 75

P

Package contents, 21
 Checking, 21
Packaging, 21
 Checking, 21
 Removing, 21
Pile au lithium, 65
Power consumption, 75
Power supply
 Connecting, 30
 DC power supply, 79
Processor, 76
PROFINET, 79
Protection class, 75
Protective measure
 Static electricity, 73

R

Radiation, 17
 High frequency radiation, 17
RAM, 76
Rating plate, 22
RCM, 69
RCM Australia/New Zealand, 69
Repairs, 63

S

Safety information
 Storage, 22
 Transportation, 22
Siemens Support Package, 33
SPM, 33, 33
 Downloading SPM, 34
 Installing SPM, 34
SSD
 Installing, 59
 Removing, 60
Static electricity
 Protective measures, 73
Supply voltage, 75
Support Package Manager, 33

U

UKCAI, 69
USB, 81
USB 3.0
 Interface, 84

W

Wall mounting, 23, 27, 74
Warranty, 15
Weight, 75