

SIEMENS

SIMATIC

Industrial PC SIMATIC IPC520A

Operating Instructions

Preface

Overview

1

Safety instructions

2

Installing and connecting the device

3

Installing OS and SDK components (Available for the device without pre- installed Industrial OS)

4

Secureboot

5

Expanding the device

6

Maintaining and repairing the device

7

Technical specifications

8

Technical support

A

Digital I/O terminal block

B

Reference files

C

Markings and symbols

D




List of abbreviations

E

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 AG. 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 IPC520A.

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

A solid background in personal computers and Microsoft operating systems is required to understand this manual. General knowledge in the field automation control engineering is recommended.

Validity of the operating instructions

These operating instructions are valid for all versions of the SIMATIC IPC520A.

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 IPC520A consists of:

- Product information "Important notes on your device"
- SIMATIC IPC520A Quick Install Guide
- SIMATIC IPC520A Operating Instructions
- SIMATIC IPC520A ReadMe OSS

Conventions

The term "device" is sometimes used to refer to the SIMATIC IPC520A 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
11/2021	First edition
05/2022	Add certification information and change the article number of lithium battery
07/2022	<ul style="list-style-type: none"><li data-bbox="539 476 1034 504">• Update the silk print on the interface panel.<li data-bbox="539 514 1230 551">• Update the procedures for installing OS and SDK components.
12/2022	Add Secureboot information
03/2023	Add information of installing SSD

Table of contents

	Preface	3
1	Overview	9
1.1	Product description	9
1.2	Structure of the devices	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	12
2	Safety instructions	15
2.1	General safety instructions.....	15
2.2	Security 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	29
3.3.1	Notes on connecting.....	29
3.3.2	Connecting the protective conductor	30
3.3.3	Connecting the power supply.....	32
4	Installing OS and SDK components (Available for the device without pre-installed Industrial OS)	33
4.1	Flashing the Ubuntu Operating System	33
4.2	Flashing the Jetson SDK components	37
4.3	Installing the "Siemens IPC520A support package"	41
4.4	Documentation for "Siemens IPC520A support package"	41
5	Secureboot	43
5.1	Overview of Secureboot.....	43

5.2	Enabling Secureboot with Nvidia Image	43
5.2.1	Installing the Secureboot Package	43
5.2.2	Preparing Key	44
5.2.2.1	Generating the RSA Key Pair	45
5.2.2.2	Generating the SBK Key	45
5.2.2.3	Generating the User Key	46
5.2.2.4	To access/read the fuse from the target board through force recovery mode	47
5.2.3	Burning PKC [SBK] Fuses	48
5.2.3.1	Non-Destructive Testing for Fuse Burning Operations	48
5.2.3.2	Burning PKC [SBK] Fuses to enable Secureboot	49
5.2.3.3	Flashing Boot Files	50
5.3	Signing files in the Siemens IPC520A support package	51
5.4	Installing the signed Siemens IPC520A support package	53
6	Expanding the device	55
6.1	Installing the M.2 module	55
6.2	Inserting the Micro SD card/Nano SIM card	57
6.3	Installing the SSD	57
7	Maintaining and repairing the device	61
7.1	Maintenance	61
7.2	Repair information	61
7.3	Replacing the backup battery	62
7.4	Recycling and disposal	64
8	Technical specifications	65
8.1	Certificates and approvals	65
8.2	Directives and declarations	69
8.2.1	Electromagnetic compatibility, Industrial and Residential Areas	69
8.2.2	RoHS directive	69
8.2.3	ESD guideline	69
8.3	Dimension drawings	72
8.4	General technical specifications	73
8.5	Ambient conditions	75
8.6	Power demand of the components	77
8.7	Direct current supply (DC)	77
8.8	Hardware descriptions	78
8.8.1	Motherboard	78
8.8.2	External Interfaces	79
8.8.2.1	Overview of external interfaces	79
8.8.2.2	Power supply	79
8.8.2.3	Digital I/O connector	79
8.8.2.4	USB	81
8.8.2.5	DisplayPort	82
8.8.2.6	Ethernet port	83

8.8.2.7	Serial port.....	84
8.8.3	Internal interfaces.....	85
8.8.3.1	Overview of internal interfaces	85
8.8.3.2	Micro SD interface	85
8.8.3.3	M.2 interface	85
A	Technical support	89
A.1	Service and support	89
A.2	Troubleshooting	90
B	Digital I/O terminal block.....	91
C	Reference files	93
C.1	prepare_Image.sh.....	93
C.2	command_history.sh	96
C.3	odmfuse.sh Option Examples.....	99
D	Markings and symbols.....	101
D.1	Overview	101
D.2	Safety.....	101
D.3	Operator controls.....	101
D.4	Certificates, approvals and markings	102
D.5	Interfaces	103
E	List of abbreviations	105
	Index.....	107

Overview

1.1 Product description



Features

SIMATIC IPC520A is powered by the NVIDIA® Jetson™ Xavier NX module. It provides high-level industrial functionality, accelerated AI performance to the Edge in a power-efficient and compact form factor.

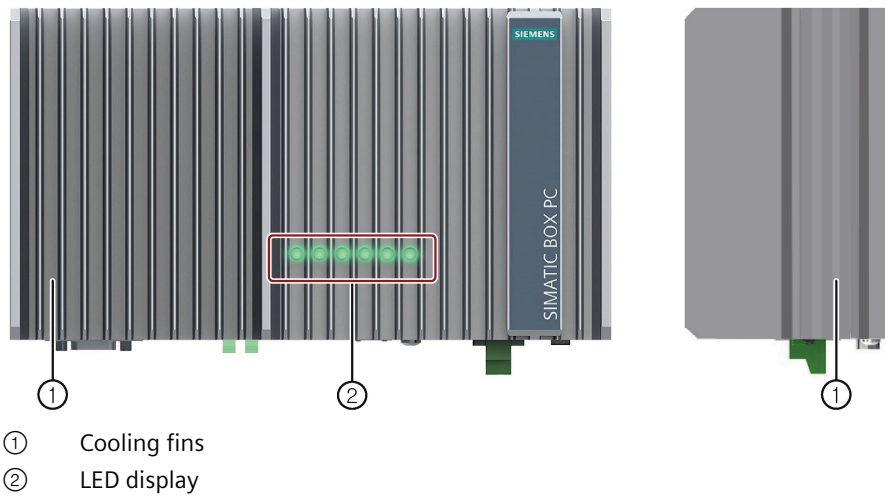
- Compact design
- Fanless
- Vibration control performance
- Various interfaces
- Support PoE power sourcing equipment (PSE) function
- Scalability of communications and storage, especially for 5G
- Support 4 DI and 2 DQ digital signals
- New functional safety capabilities
- Maintenance-free operation possibility

1.2 Structure of the devices

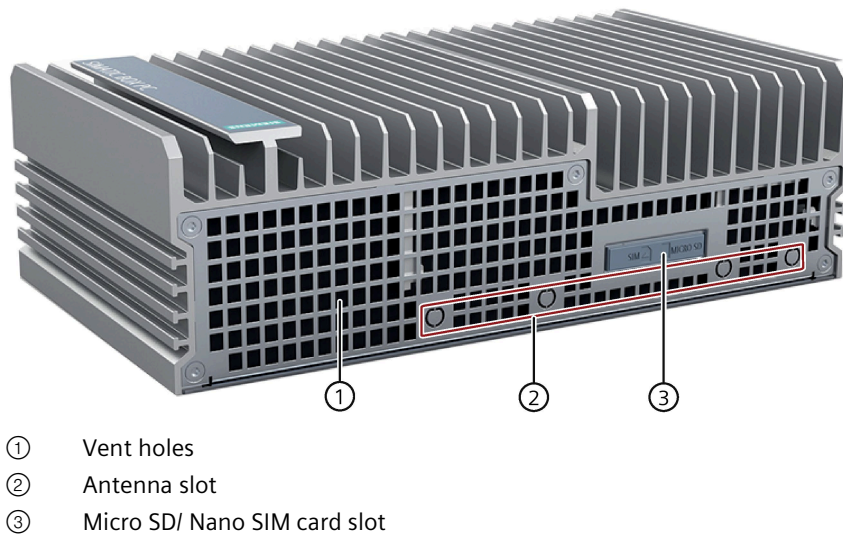
1.2.1 Views of the device

Front view and side view

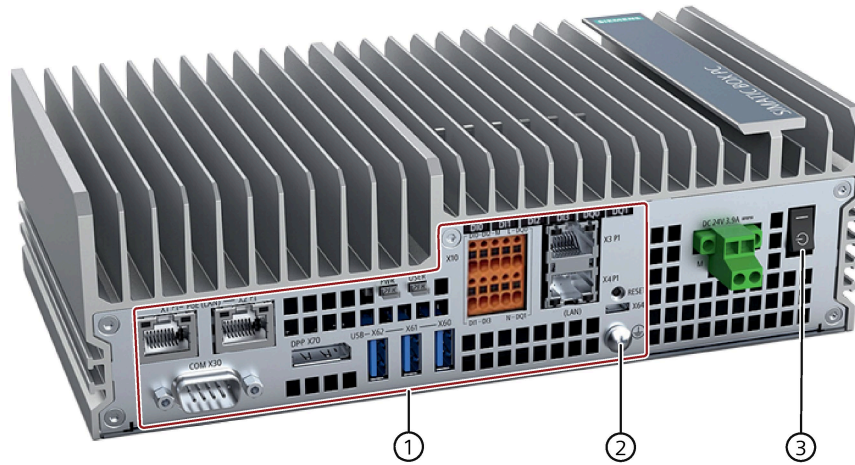
The front view on the left is the standard mounting position. The side view is on the right.



Top view

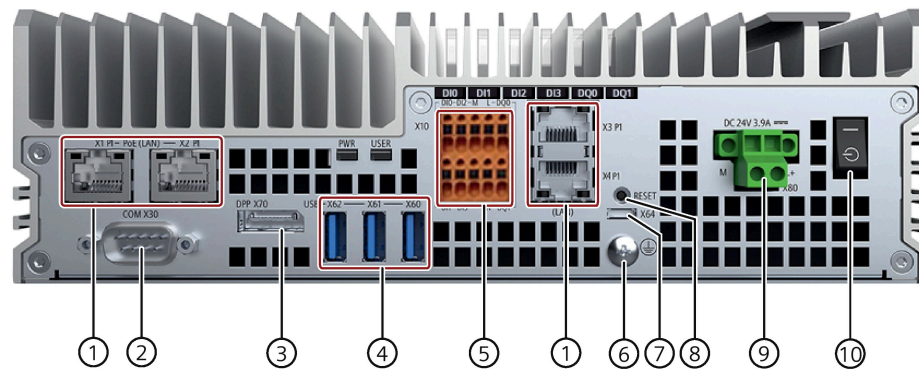


Bottom view



- ① Interfaces
- ② Protective conductor
- ③ On/Off switch

1.2.2 Interfaces of the device



- | | |
|---|---|
| <ul style="list-style-type: none"> ① LAN (X1P1/X2P1/X3P1/X4P1) ② COM (X30) ③ DPP (X70) ④ USB 3.0 port (X60/X61/X62) ⑤ Digital I/O Connector (X10) ⑥ Protective conductor ⑦ USB 2.0 port (X64) ⑧ RESET button ⑨ Power supply (X80) ⑩ On/Off button | <ul style="list-style-type: none"> 4 × RJ45 Ethernet connections for 10/100/1000 Mbps 1 × Serial interface, 9-pin RS232/RS422/RS485 D-sub connector 1 × DisplayPort connection 3 × USB 3.0 Type A, high current 4 × DI + 2 × DQ Connection for protective conductor 1 × USB 2.0 Micro B port Reset the device to factory settings Connection for a 24 V DC power supply Switch on (position "—"); Switch off (position "⏻") |
|---|---|

1.2.3 Status displays



LED	State	Description
DIO / DI1/DI2 /DI3	Off	No data transmission
	Green	Digital input data transmission
DQ0 /DQ1	Off	No data transmission
	Green	Digital output data transmission
PWR	Off	Power disconnected
	RED	Power connected, 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>)

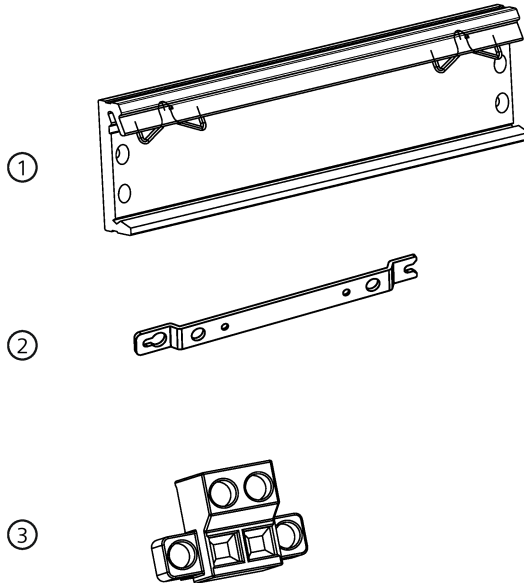
Accessories available for order

Accessories	Article number
Mounting accessory kit	A5E51286067
Lithium battery	A5E51740580
SSD heatsink accessory	A5E52560303

Mounting accessory kit


The mounting accessory kit contains:

- One standard rail bracket ①
- Two wall mounting brackets ②
- One DC connecting terminal block ③
- Eight M3 screws



Safety instructions

2.1 General safety instructions


 WARNING
<p>Life-threatening voltages are present with an open control cabinet</p> <p>When you install the device in a control cabinet, some areas or components in the open control cabinet might be carrying life-threatening voltages.</p> <p>If you touch these areas or components, you might be killed by electric shock.</p> <p>Switch off the power supply to the cabinet before opening it.</p>

System expansions

NOTICE
<p>Damage through system expansions</p> <p>Device and system expansions might be faulty and can affect the entire machine or plant.</p> <p>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.</p>

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 73).

 WARNING
<p>Risk of fire through expansion cards</p> <p>Expansion cards generate additional heat. The device may overheat and cause a fire.</p> <p>Note the following:</p> <ul style="list-style-type: none"> • Observe the safety and installation instructions for the expansion cards.

2.1 General safety instructions

NOTICE

Use in the scope of application for the UL61010-2-201

When the device is used in the area of Industrial Control Equipment in accordance with UL61010-2-201, note that the device is classified as "Open equipment".

Open equipment must be installed within an enclosure which protects you from hazards, including mechanical hazards, electrical shock and spread of fire.

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
<p>Risk of explosion and release of harmful substances</p> <p>Improper handling of lithium batteries can result in an explosion of the batteries.</p> <p>Explosion of the batteries and the released pollutants can cause severe physical injury. Worn batteries jeopardize the function of the device.</p> <p>Note the following when handling lithium batteries:</p> <ul style="list-style-type: none"> • 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: A5E51740580). • 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
<p>Observe immunity to RF radiation</p> <p>The device has an increased immunity to RF radiation according to the specifications on electromagnetic compatibility in the technical specifications.</p> <p>Radiation exposure in excess of the specified immunity limits can impair device functions, result in malfunctions and therefore injuries or damages.</p> <p>Read the information on immunity to RF radiation in the technical specifications.</p>

ESD Guideline



Electrostatic sensitive devices can be labeled with an appropriate symbol.

NOTICE
<p>Electrostatic sensitive devices (ESD)</p> <p>When you touch electrostatic sensitive components, you can destroy them through voltages that are far below the human perception threshold.</p> <p>If you work with components that can be destroyed by electrostatic discharge, observe the ESD Guideline (Page 69).</p>

2.2 Security information

Siemens provides products and solutions with industrial security 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 security 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 additional information on industrial security measures that may be implemented, please visit (<https://www.siemens.com/industrialsecurity>).

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, subscribe to the Siemens Industrial Security RSS Feed visit (<https://www.siemens.com/cert>).

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 (<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 Secureboot feature to the first stage of boot/Cboot/kernel/DTB to prevent attack.
- Use SHA256 algorithm at least for public key hash collision.
- Use RSA 3072 algorithm and preserve it in a secured location for private key.
- Ensure that only the authorised 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.

2.5 Notes on use

- 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 cabinets, 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 DC connecting terminal block, one standard rail bracket, two wall mounting brackets and eight screws.

3.1 Preparing for installation

- If the contents of the packaging are incomplete, damaged, or do not match your order, inform the responsible delivery service immediately.

<p>⚠ WARNING</p> <p>Electric shock and fire hazard due to damaged device</p> <p>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.</p> <p>Death or serious injury could occur.</p> <ul style="list-style-type: none"> • 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.

<p>NOTICE</p> <p>Damage from condensation</p> <p>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.</p> <p>Moisture causes a short circuit in electrical circuits and damages the device.</p> <p>In order to prevent damage to the device, proceed as follows:</p> <ul style="list-style-type: none"> • 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.
--

- 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.
- Record the identification data of the device.

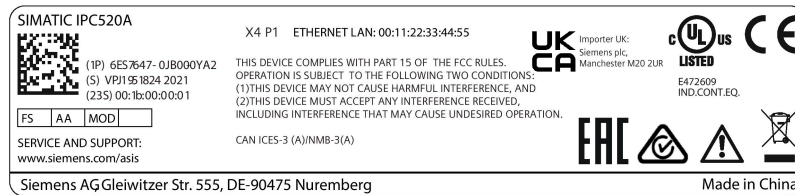
3.1.2 Identification data of the device

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	6ES7647-0JB00-0YA2
Serial number	S V
Production version	FS
All existing Ethernet addresses (MAC)	

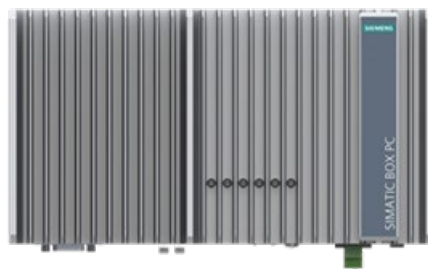
The following image shows the product label on the SIMATIC IPC520A as an example.



3.1.3 Permitted mounting positions and mounting types

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

Horizontal mounting position (preferred) Desk mounting position

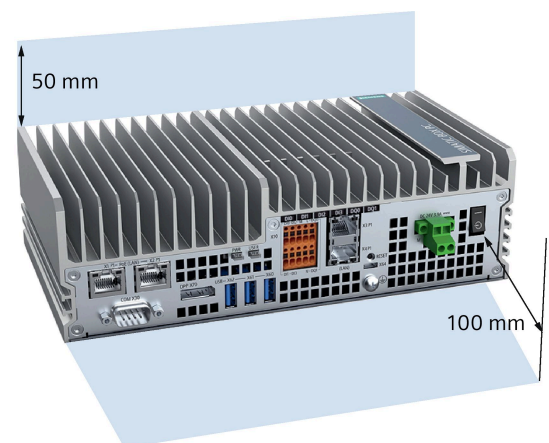
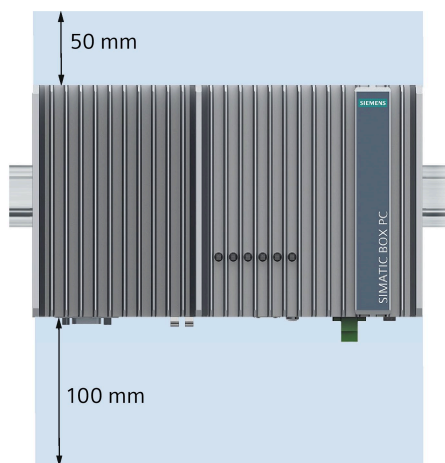


Consider the permitted temperature range for operation that depends on the mounting position in accordance with the "Technical specifications (Page 65)" section.

Clearances

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

- Underneath of the device at least 100 mm
- Side of the device at least 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 "Open equipment". Open equipment must be installed within an enclosure which protects you from hazards, including mechanical hazards, electrical shock, and spread of fire.
- 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	<ul style="list-style-type: none"> 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)		<ul style="list-style-type: none"> Screw M4 × 15 M4 nut

<p> WARNING</p> <p>Personal injuries or material damage in the case of insufficient load-bearing capacity of wall</p> <p>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.</p> <p>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 2 kg.</p>

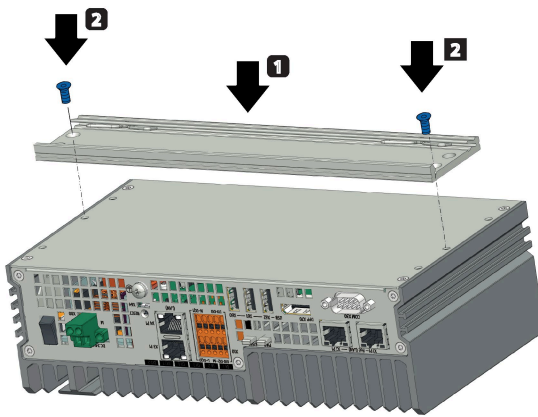
3.2.2 Mounting on DIN rails

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

Requirements

- A SIEMENS 35 mm standard rail TH35-15 conforming to EN 60715:200 is mounted.
- A standard rail bracket
 - The standard rail bracket and two screws are included in the order variant "Standard rail mounting".
- 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.
- 6** Applies to vertical standard rail mounting:
Fasten a standard rail ground terminal below the device.

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.

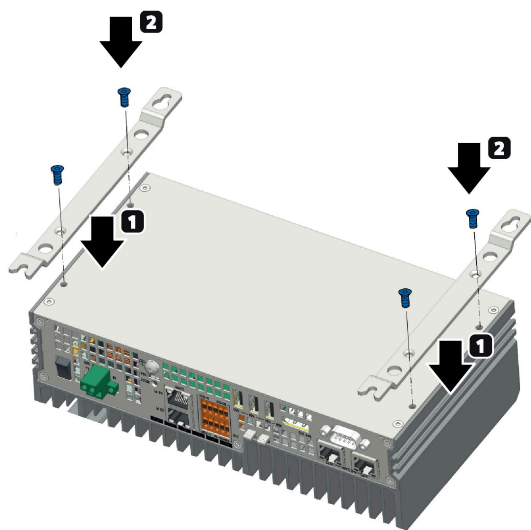
3.2.3 Wall mounting

Wall mounting is one of the horizontal mounting types.

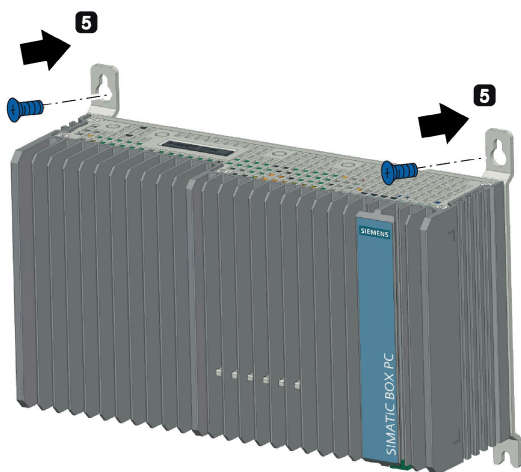
Requirements

- Two mounting brackets
The mounting brackets and four screws are included in the order variant "Wall mounting".
- 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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: <ul style="list-style-type: none">• 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.

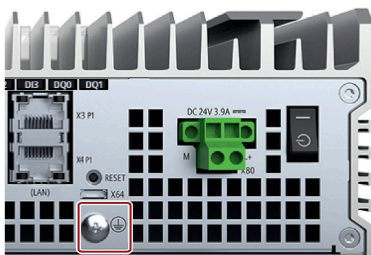
- Connect the device to the protective conductor before you put it into operation.
- The PE terminal on the device must be connected to the protective conductor of the control cabinet or system in which the device is installed.
- Never operate the device without a protective conductor.
- If a device 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).
- 3** 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

The device should only be connected to a 19.2 to 28.8 V DC power supply which meets the requirements of safe extra low voltage (SELV) according to IEC/EN/DIN EN/UL 61010-1.

Note

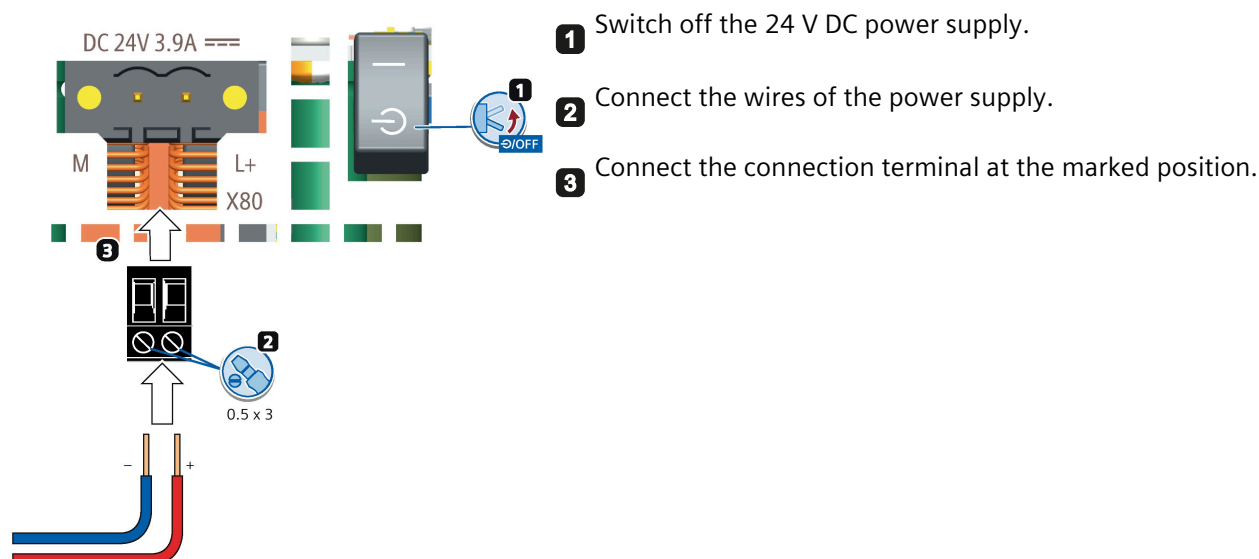
The power supply must be adapted to the input data of the device, see chapter "General technical specifications (Page 73)".

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 cross-section of 0.75 mm² to 2.5 mm²
 - rated temperature 70 °C
- Tightening torque: 0.56 Nm
- A slotted screwdriver with a 3 mm blade.

Procedure



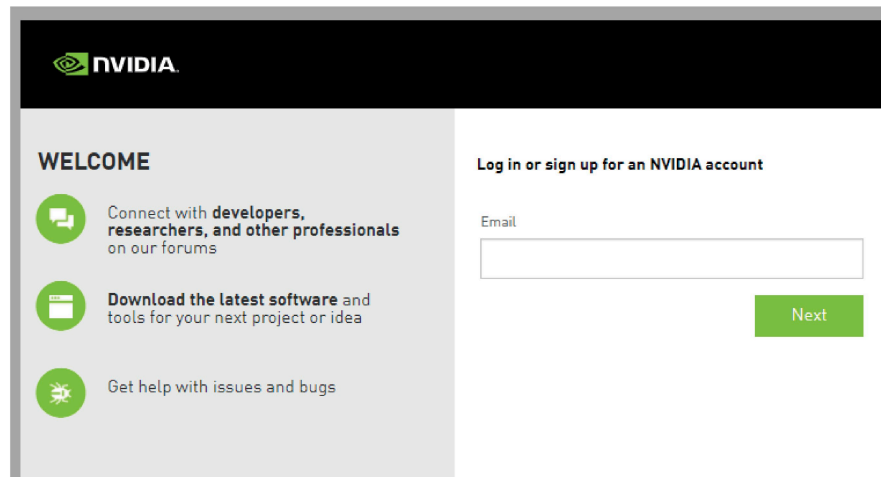
Installing OS and SDK components (Available for the device without pre-installed Industrial OS)

4

4.1 Flashing the Ubuntu Operating System

Follow these steps to flash the Ubuntu Operating System:

1. Install NVIDIA SDK Manager on a local PC. For detailed installation procedures, refer to the NVIDIA website (<https://docs.nvidia.com/jetson/jetpack/install-jetpack/index.html>).
2. Set the IPC520A to Force Recovery Mode (RCM).
 - 2.1 Switch off the IPC520A.
 - 2.2 Connect the IPC520A to local PC through a micro USB cable.
 - 2.3 Keep pressing the Reset button of IPC520A.
 - 2.4 Switch on the IPC520A and wait for more than 3 seconds, then release the Reset button.
 - 2.5 Check whether the IPC520A is entering the RCM: Enter the command `lsusb` on the local PC, then the output returns should be as below:
Bus <xxx> Device <xxx>: ID 0955: <7e19> Nvidia Corp
Otherwise, repeat step 2.
3. Start up NVIDIA SDK Manager, and register an NVIDIA account to log in to NVIDIA SDK Manager.

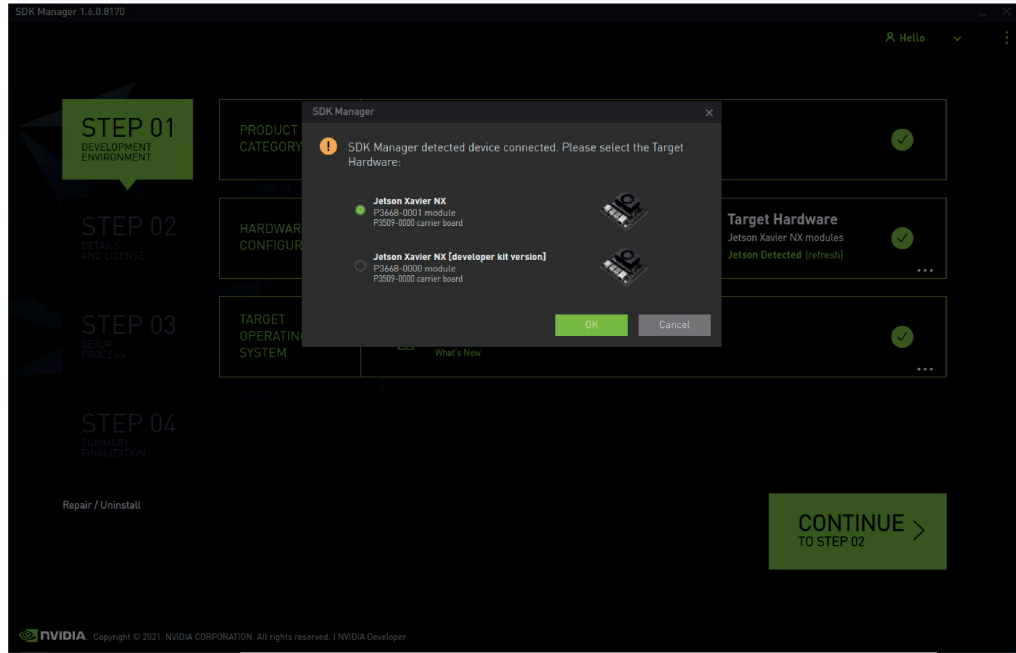


4.1 Flashing the Ubuntu Operating System

- Follow the steps below to flash the Ubuntu Operating System. For detailed configuration procedures, refer to the NVIDIA website. (<https://docs.nvidia.com/sdk-manager/install-with-sdkm-jetson/index.html>)

– **STEP 01 DEVELOPMENT ENVIRONMENT:**

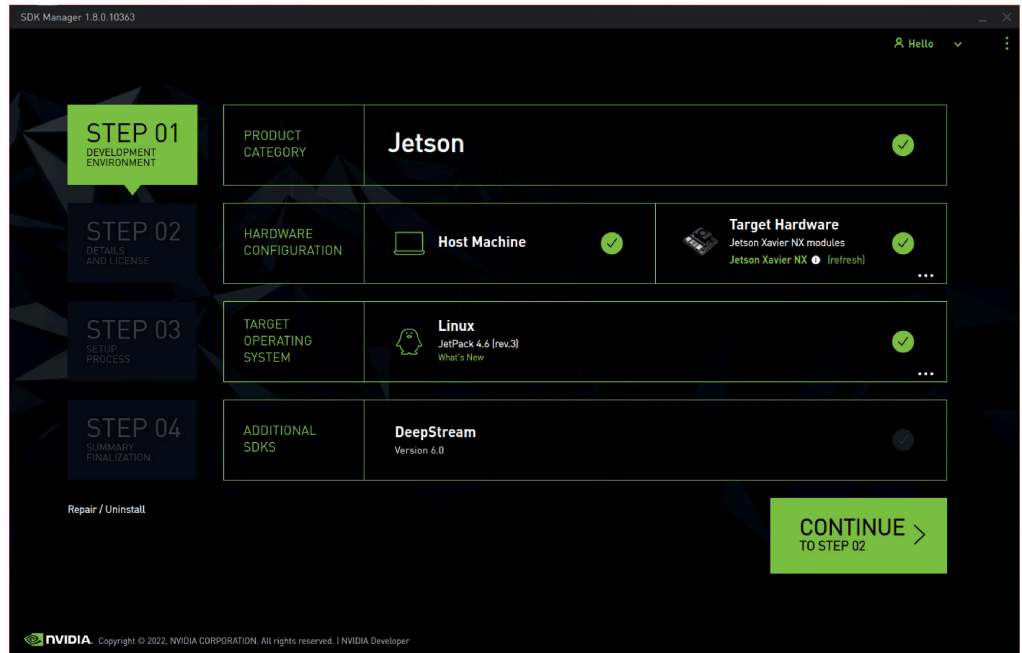
Select "Jetson Xavier NX (P3668-0001 module)" radio button as the **Target Hardware** and click the "OK" button in the pop-up window.



Select the jetpack version supported by IPC520A as the **Linux** version, and then click "CONTINUE TO STEP 02" button.

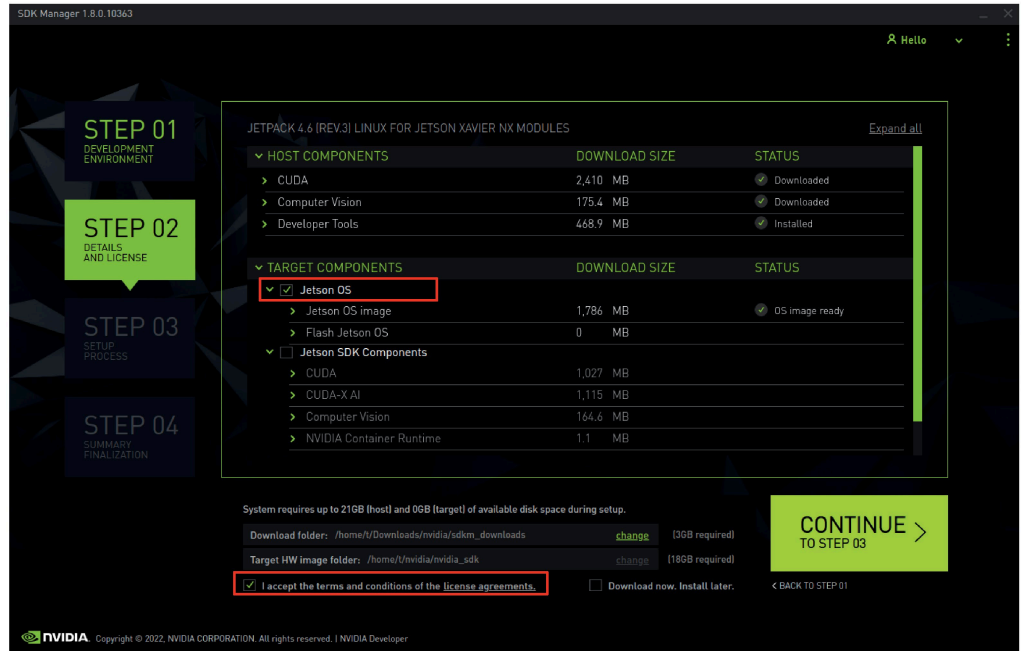
Note

You can get the version compatibility and supported jetpack version information from Siemens Industry Online Support website (<https://support.industry.siemens.com/cs/ww/en/view/109783704>).



– **STEP 02 DETAIL AND LICENSE:**

Click the checkbox before "Jetson OS" under the "TARGET COMPONENTS"; enable the checkbox to accept the terms and conditions of the license agreements, and then click the "CONTINUE TO STEP 03" button.



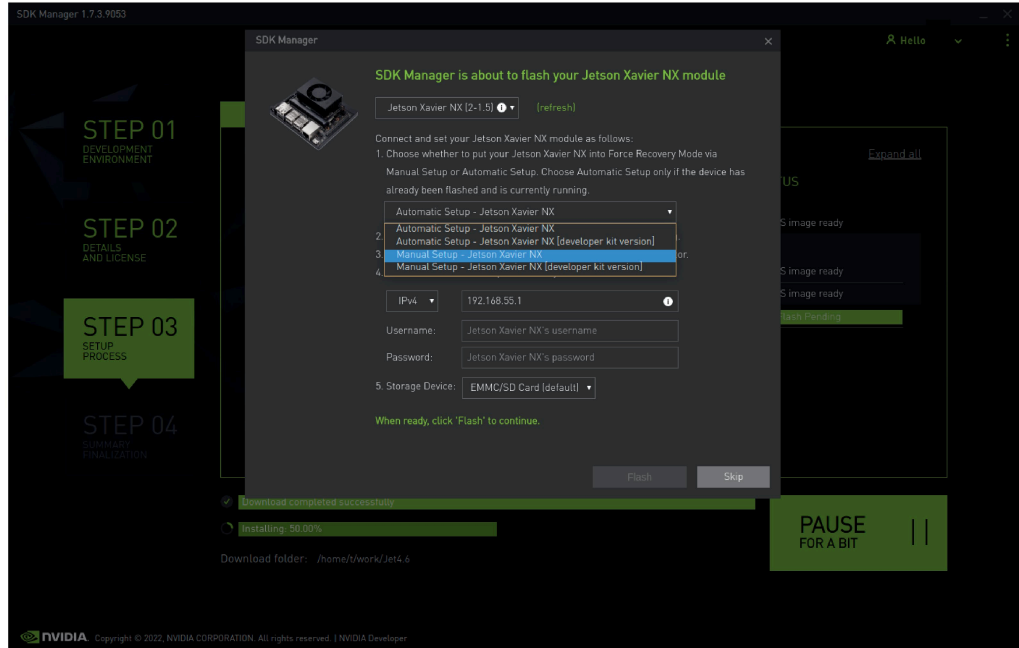
Note

Ignore the warnings such as "There is not enough space" or "There is not enough disk space to install the selected SDK", and click the "Continue" button in the prompt window to go to the next step.

4.1 Flashing the Ubuntu Operating System

– STEP 03 SETUP PROCESS:

Select "Manual Setup - Jetson Xavier NX" to put your device into Force Recovery Mode, and then click the "Flash" button to continue.



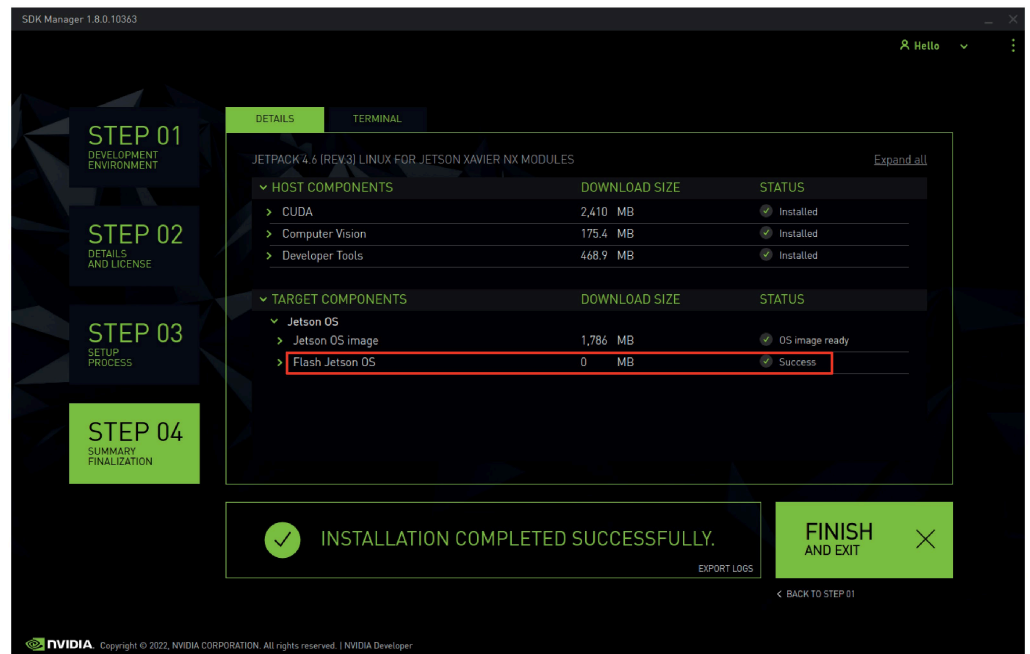
Note

SDK Manager supports two options to put your device into Force Recovery Mode:

- Manual setup: set the device to Force Recovery Mode through manual operations.
- Automatic setup: set the device to Force Recovery Mode through remote command. This requires the device to be flashed and currently running.

– STEP 04 SUMMARY FINALIZATION

Check the flash result. If the status of Flash Jetson OS is "Success", the flashing is finished.

**Note**

Only if the status of Flash Jetson OS is "Success", the flashing is successful, and you can ignore errors if there's any in the status.

- Reboot the IPC520A. When you boot the first time, the Jetson Xavier NX Developer Kit will take you through some initial setup, including:
 - Review and accept NVIDIA Jetson software EULA
 - Select system language, keyboard layout, and time zone
 - Connect to Wireless network
 - Create username, password and computer name
 - Log in

4.2 Flashing the Jetson SDK components

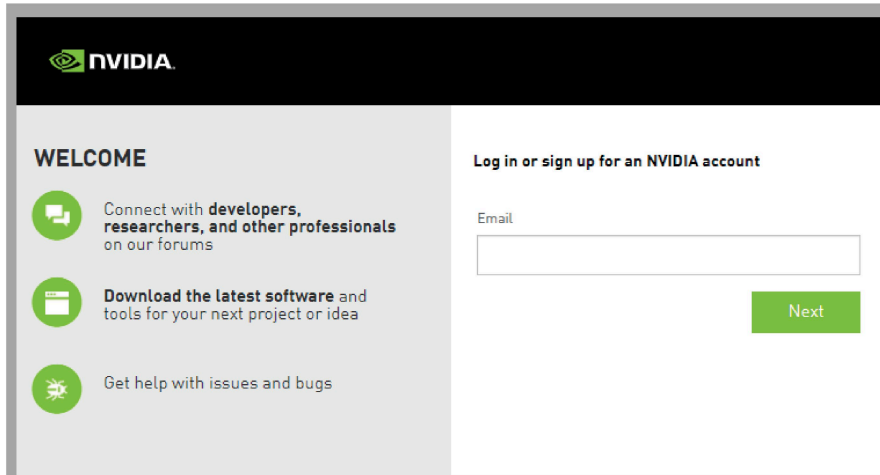
Follow these steps to flash the Jetson SDK components.

Note

Ubuntu Operating System is installed in IPC520A device.

4.2 Flashing the Jetson SDK components

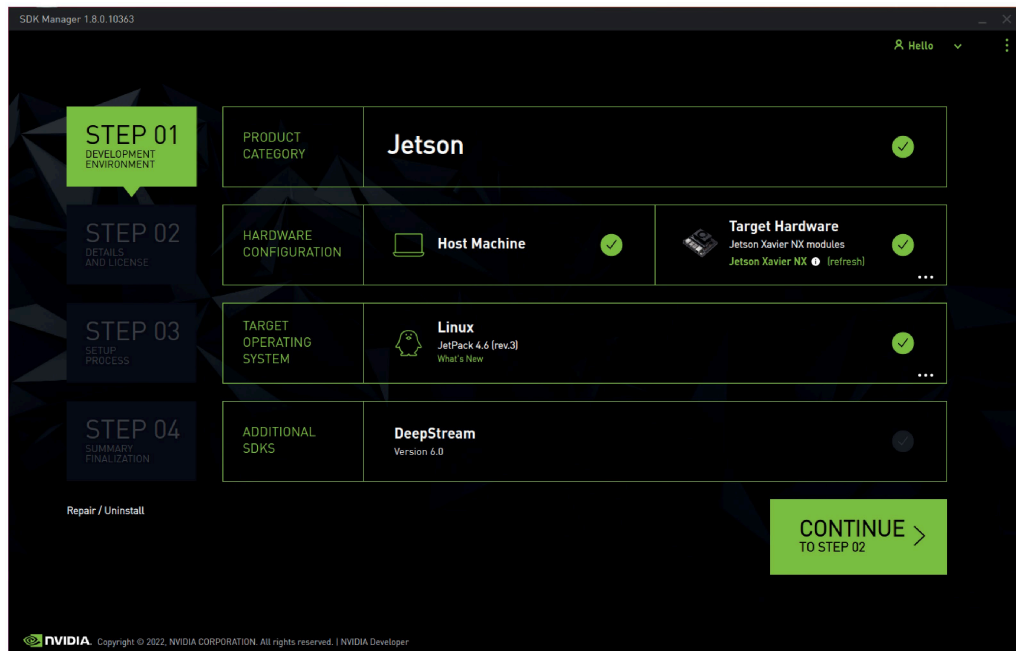
1. Start up NVIDIA SDK Manager, and log in to NVIDIA SDK Manager.



2. Follow the steps below to flash the Jetson SDK components. For detailed configuration procedures, refer to the NVIDIA website. (<https://docs.nvidia.com/sdk-manager/install-with-sdkm-jetson/index.html>)

– **STEP 01 DEVELOPMENT ENVIRONMENT:**

Make sure that Target Hardware is "Jetson Xavier NX (P3668-0001 module)" and that the Linux version is the same one you selected in Flashing the Ubuntu Operating System (Page 33), and then click "CONTINUE TO STEP 02".

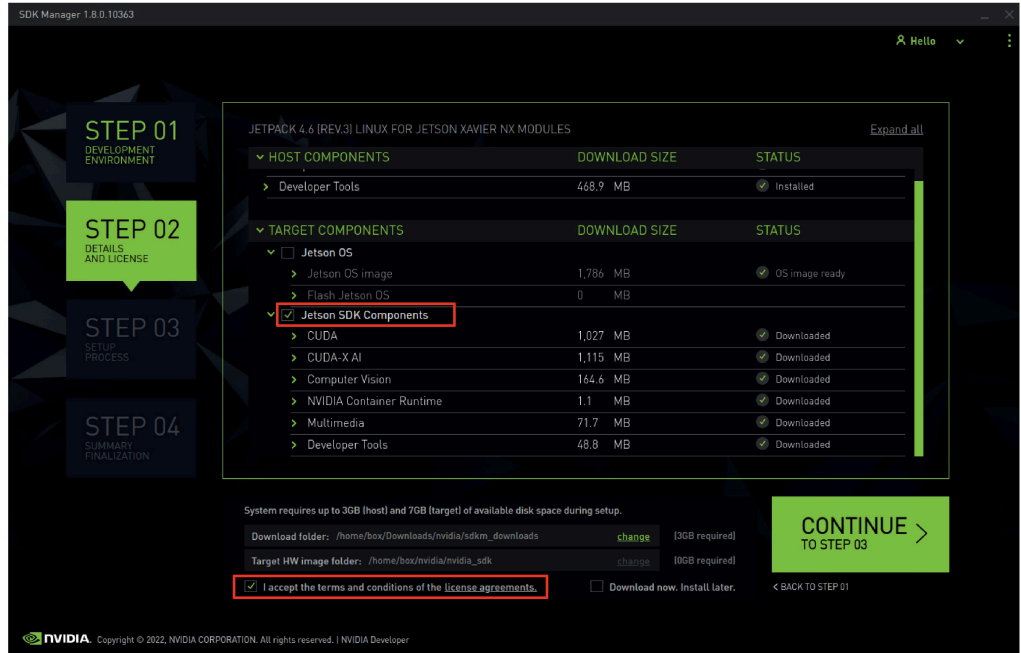


– **STEP 02 DETAIL AND LICENSE:**

Click the checkbox before "Jetson SDK components" under the "TARGET COMPONENTS"; enable the checkbox to accept the terms and conditions of the license agreements, and then click "CONTINUE TO STEP 03" button.

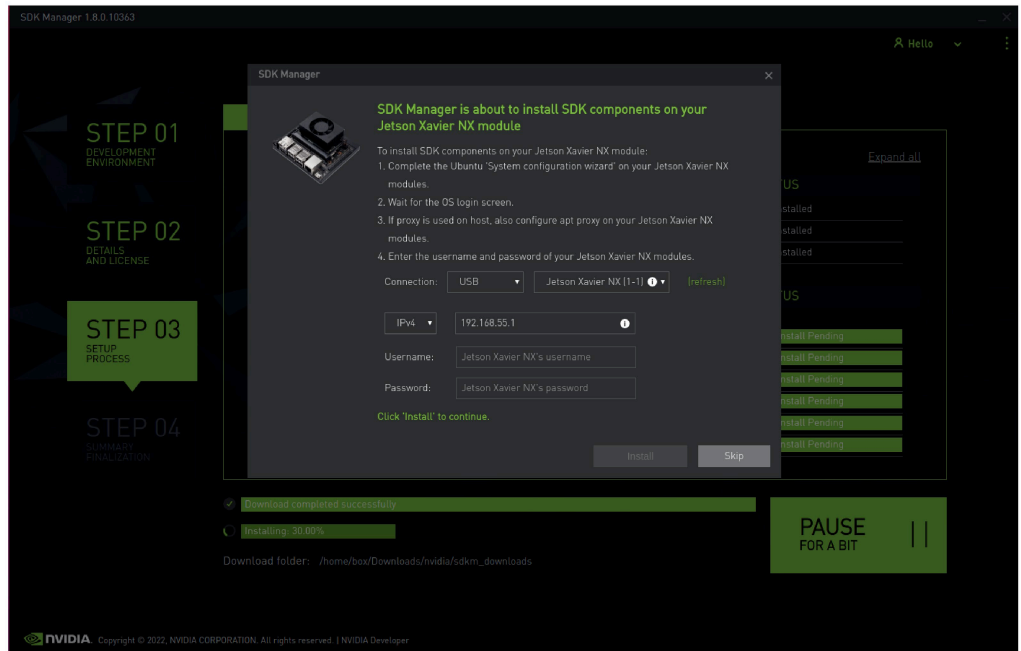
Note

Ignore the warnings such as "There is not enough space" or "There is not enough disk space to install the selected SDK", and click the "Continue" button in the prompt window to go to the next step.



– **STEP 03 SETUP PROCESS:**

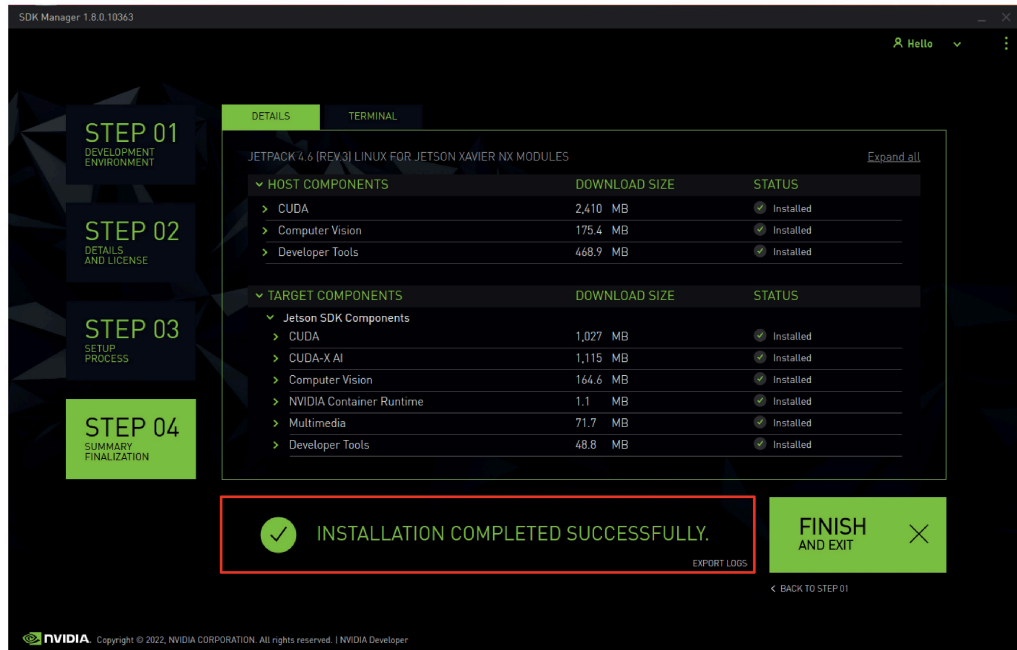
Enter the Username and Password for your Jetson Xavier NX module which is installed IPC520A and then click the "Install" button to continue.



4.2 Flashing the Jetson SDK components

– STEP 04 SUMMARY FINALIZATION:

Check the flash result. When you see the following marked installation result, the flashing is successful. Then click the "FINISH AND EXIT" button to exit.



4.3 Installing the "Siemens IPC520A support package"

Follow these steps to install the "Siemens IPC520A support package":

1. Search the "Siemens IPC520A support package" in the Siemens Industry Online Support website (<https://support.industry.siemens.com/cs/ww/en/view/109783704>) and download it to a FAT/FAT32 formatted USB stick.
2. Copy the "Siemens IPC520A support package" from the USB stick to the IPC520A and enter the following command:

```
$ sudo dpkg --force-overwrite -i ipc520a-jp${VERSION}-${DEB_VERSION}-
${CREATED_TIME}_arm64.deb
```

For example:

```
$ sudo dpkg --force-overwrite -i ipc520a-jp4.6-1.0-20220601122040_arm64.deb
```

Note

- `jp${VERSION}` is the version of supported JetPack;
 - `${DEB_VERSION}` is the version of "Siemens IPC520A support package" ;
 - `${CREATED_TIME}` is the time when support package is created.
-

3. Reboot IPC520A.

Note

- Do not press the On/Off button to switch off the device after the support package is installed.
- Run the following command to restart the device:

```
$ sudo reboot
```

4.4 Documentation for "Siemens IPC520A support package"

"Siemens IPC520A support package" is published on our Siemens Industry Online Support website. To use the "Siemens IPC520A support package", you need a login for online support.

Follow these steps to participate in the Siemens Industry Online Support website:

1. Open the "Siemens Industry Online Support website".
(<https://support.industry.siemens.com/cs/ww/en/view/75852684>)
2. If you do not yet have a login for online support, click "Register" at the top right of the window and follow the registration instructions.



> Register > Login [?]

During registration, you enter an alias for the forum. This alias is the pseudonym under which other users can see you and talk to you in the forum.

You will receive a confirmation e-mail after registering successfully.

Secureboot

5.1 Overview of Secureboot

Secureboot prevents execution of unauthorized boot codes through chain of trust. The root-of-trust is 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.

NVIDIA® Jetson™ Linux Driver Package (L4T) provides boot security using the Secureboot package. IPC520A Secureboot function is the same as the one on the NVIDIA Jetson Xavier NX.

To fulfill the Secureboot function on IPC520A, you need to perform the following steps:

1. Enabling Secureboot with Nvidia Image (Page 43)
2. Signing files in the Siemens IPC520A support package (Page 51)
3. Installing the signed Siemens IPC520A support package (Page 53)

5.2 Enabling Secureboot with Nvidia Image

This chapter shows an example on how to enable Secureboot with Nvidia Image.

You can get detailed information on how to enable Secureboot by searching "**Jetson Linux R32.6.1 Release Page | NVIDIA Developer**" to find "*Jetson Linux Developer Guide (online version) document*" from the Nvidia guideline (<https://docs.nvidia.com/>).

Note

Before enabling Secureboot, backup important user data to prevent data loss. When you enable Secureboot, all user data on the device will be wiped out.

5.2.1 Installing the Secureboot Package

Requirements

- The X86 host PC is running with Ubuntu 16.04 or 18.04 LTS.
- *libftdi-dev* for USB debug port support
- *openssh-server* package for OpenSSL

- Full installation of the latest L4T release on the host
Download "JETSON LINUX VERSION 32.6.1" release at: Jetson Linux Archive (<https://developer.nvidia.com/embedded/jetson-linux-archive>).
- The NVIDIA® Jetson™ platform is connected to the host with a Micro USB cable.

Procedures

1. Download Secureboot package "*Jetson Platform Fuse Burning and Secure Boot Documentation and Tools*" for Xavier NX module from the Jetson Download Center (<https://developer.nvidia.com/embedded/linux-tegra-r3261>).
2. Go to the directory that contains the *Linux_for_Tegra* directory.
3. Untar the Secureboot package to *Linux_for_Tegra* by entering the command:

```
tar xvjf secureboot_< release_version > .tbz2
```

This command overlays the contents of the file on the *Linux_for_Tegra* directory.
4. Check whether the file "*Linux_for_Tegra/bootloader/odmsign.func*" exists.
If it does, the Secureboot package is installed successfully.

5.2.2 Preparing Key

To enable Secureboot, you need to generate a Secureboot key first.

This chapter takes RSA Key Pair, SBK Key and User Key as examples.

 WARNING
--

Risk of losing key information

If you have lost your Secureboot key, the device cannot be flashed.

All the Secureboot keys are important, so you should save this information in a safe place.

Note

The key file is used to burn, fuse, and sign boot files for Jetson devices. The security of your device depends on how securely you keep the key file.

To ensure the security of the key file, restrict access permission to a minimum number of personnel.

5.2.2.1 Generating the RSA Key Pair

Secureboot requires an RSA key-pair whose length is 2048 bits (RSA 2K) or 3072-bits (RSA 3K). You can select either of these two key-pairs as the RSA Key Pair.

To generate a key-pair

1. Execute one of these commands on a local host PC:

- To generate an RSA 2K key:

```
$ openssl genrsa -out rsa_priv.pem 2048
```

- To generate an RSA 3K key:

```
$ openssl genrsa -out rsa_priv.pem 3072
```

Upon successful execution, OpenSSL generates the key file named *rsa_priv.pem*.

2. Rename and save the key file securely and safely.

Note

To generate a truly random number key, use the Hardware Security Module (HSM). Consult the Hardware Security Module User Guide for output format and private key conversion to PEM format.

5.2.2.2 Generating the SBK Key

If you want to encrypt Bootloader (and TOS), you must prepare the SBK fuse bits.

The SBK key consists of four 32-bit words stored in a file in big-endian hexadecimal format. Here is an example of a SBK key file:

```
0x12345678 0x9abcdef0 0xfedcba98 0x76543210
```

The representation in the fusing XML file is:

```
0x123456789abcdef0fedcba9876543210
```

Note

You can only use the SBK key with the PKC key. The encryption mode that uses these two keys together is called SBKPKC.

To generate an SBK key

1. Prepare a four 32-bit words in big-endian hexadecimal format. Take above SBK key file as an example.
2. Enter the following command:

```
echo "0x12345678 0x9abcdef0 0xfedcba98 0x76543210" > ./SBK
```

This command creates the SBK key. Copy and rename the resulting file, "SBK".

Note

For more information about fuse, refer to "Jetson Xavier NX Fuse Specification Application Note.pdf"

(<https://developer.nvidia.com/embedded/downloads#?search=Xavier%20NX%20Fuse%20Specification>).

5.2.2.3 Generating the User Key

If you want to encrypt a kernel image (including the *kernel*, *kernel-dtb* and *extlinux.conf* files), you must prepare the user key.

You need the user key, as well as the SBK key and the RSA Key Pair.

The user key is stored in the Encrypted keyblob (EKB) in encrypted form. The Secure Engine (SE) retrieves the user key from the EKB and uses it to decrypt the kernel image files.

The user key must be specified in two different formats for different purposes:

- For use in the `--user_key` command line option of the `flash.sh` command, it is a file containing four big-endian 32-bit words stored as four 8-digit hexadecimal numbers. (The `--user_key` option specifies the pathname of this file.)

Here is an example of a user key in this format:

```
0x12345678 0x9abcdef0 0xffeeddcc 0xbbaa9988
```

For more information, see the section To sign and flash in one step using the user, SBK, and PKC keys (https://docs.nvidia.com/jetson/archives/l4t-archived/l4t-3261/index.html#page/Tegra%20Linux%20Driver%20Package%20Development%20Guide/bootloader_secure_boot.html#wwpID0E02C0HA).

- For use in generating the EKB, it is a file containing 32 hexadecimal digits that represent the same key, interpreted as a single big-endian 128-bit value. Here is an example:

```
123456789abcdef0ffeeddccbbaa9988
```

For use in generating the EKB, it is a file containing 32 hexadecimal digits that represent the same key, interpreted as a single big-endian 128-bit value.

- 1 Download the file "`{l4t path}/public_sources/Linux_for_Tegra/source/public/trusty_src.tar.gz`" from the Nvidia website (https://developer.nvidia.com/embedded/l4t/r32_release_v7.2/sources/t186/public_sources.tbz2).

- 2 Untar the above file.

- 3 Go to the directory by entering the following command:

```
$ cd {l4t path}/public_sources/Linux_for_Tegra/source/public/trusty_src/trusty/app/nvidia-sample/hwkey-agent/CA_sample/tool/gen_ekb
```

- 4 Read *README* and modify *example.sh* in- the above directory to generate the EKB key.

Copy *eks.img* to `<linux_for_tegra>/bootloader/`.

Note

For information about how the EKB is generated, see EKB Generation (<https://docs.nvidia.com/jetson/archives/l4t-archived/l4t-3261/index.html#page/Tegra%20Linux%20Driver%20Package%20Development%20Guide/trusty.html#wwpID0E0QCOHA>) in the topic *Trusty, a Trusted Execution Environment*.

You must use the same user key in *flash.sh* to encrypt kernel images. That script flashes the EKB to the target along with the encrypted kernel images. The EKB is flashed to the EKS partition.

5.2.2.4 To access/read the fuse from the target board through force recovery mode

Perform the following steps to access/read the fuse from the target board through force recovery mode.

1. Navigate to the directory where you installed Secureboot.

For example: `cd ~/Linux_for_Tegra`

2. Place the Jetson device into Force Recovery mode with Micro USB connection.
3. Enter the command: `$ sudo ./odmfuserread.sh -i 0x19 [-k <pkc_keyfile>] [-S <sbk_keyfile>] <device_name>`

For example:

```
$ sudo ./odmfuserread.sh -i 0x19 \  
-k /secure_boot_save/01_rsa_pri_key/rsa_priv.pem \  
-S /secure_boot_save/02_sbks/SBK \  
--KEK2 /secure_boot_save/03_userkey/kek2_key \  
jetson-xavier-nx-devkit-emmc
```

Note

Path of `/secure_boot_save` depends on where you have saved the previous key.

Upon successful execution, fuse information will be saved in `bootloader/fuse_info.txt`.

5.2.3 Burning PKC [SBK] Fuses

This chapter describes how to burn PKC and SBK fuses using a private key file in PEM format.

Perform the following procedures to burn the PKC fuse:

1. Navigate to the directory where you installed Secureboot tool.
2. Put the Jetson device into Forced Recovery Mode with USB connection.
3. Burn the fuse using the *odmfuse.sh* script. See *odmfuse.sh* Command Line Option Examples (https://docs.nvidia.com/jetson/archives/l4t-archived/l4t-3261/index.html#page/Tegra%20Linux%20Driver%20Package%20Development%20Guide/bootloader_secure_boot.html#wwplD0E06E0HA) for examples of common operations.

Note

- *odmfuse.sh* uses OpenSSL to burn PKC fuses.
 - For examples of common operations, refer to *odmfuse.sh* Option Examples (Page 99).
-

5.2.3.1 Non-Destructive Testing for Fuse Burning Operations

Fuse burning operations are high-risk because they can't be reversed. Siemens strongly recommends that you use the *--test* option to verify fuse burning operations before you perform them.

When you add *--test* to an *odmfuse.sh* command, the command performs pre-burn processing and verification, but does not actually burn the fuse. If the command reports the results you want, you can re-enter the command without *--test* and burn the fuse with greater confidence that you are doing it correctly.

5.2.3.2 Burning PKC [SBK] Fuses to enable Secureboot

Burning PKC Fuse will enable Secureboot. Follow the steps to enable Secureboot and use the user key to encrypt kernel (*user-kek2*), fuse with PKC (Public hash), and SBK(Secureboot key).

1. Enter the command on the *Linux_for_Tegra*:

```
# close production mode fuse test
sudo ./odmfuse.sh -i 0x19 --test -p \
-k /secure_boot_save/01_rsa_pri_key/rsa_priv.pem \
-S /secure_boot_save/02_sbk/SBK \
--KEK2 /secure_boot_save/03_userkey/kek2_key \
jetson-xavier-nx-devkit-emmc
```

2. If there is no error return, execute the following command.

This command will start the fuse burning operation.

```
# close production mode fuse without `--test`
sudo ./odmfuse.sh -i 0x19 -p \
-k /secure_boot_save/01_rsa_pri_key/rsa_priv.pem \
-S /secure_boot_save/02_sbk/SBK \
--KEK2 /secure_boot_save/03_userkey/kek2_key \
jetson-xavier-nx-devkit-emmc
```

3. If there is no error return, the device has fused with your key.

Check if Secureboot is enabled or not, and follow To access/read the fuse from the target board through force recovery mode (Page 47).

The return log contains the values of SBK and PKC, if the values of SBK and PKC are full of "f", like "fff...ffff", the value indicates the key has burning successfully.

Note

--test: prevents the script from actually burning fuses. Pre-burn processing and tests are performed as usual. *--test* option is normally used for fuse burning tests, since fuse values cannot be changed once they are burned.

For using more keys, refer to Jetson Xavier NX Fuse Specification Application Note.pdf (<https://developer.nvidia.com/embedded/downloads/#?search=Xavier%20NX%20Fuse%20Specification>) .

5.2.3.3 Flashing Boot Files

When you reflash a previously flashed device, you must determine the type of signing that has been used on the device and reflash with the same type. This is because the type of signing is specified by fuses which can be written only once.

For example, if a device is first flashed with PKC signing, that type of signing is burned into its fuses, and it cannot be reflashed with SBKPKC signing later.

1. Navigate to the directory where you installed Secureboot.
2. Place the Jetson device into Force Recovery mode.
3. Flash with key:

```
$ sudo ./flash.sh -u <pkc_keyfile> -v <sbk_keyfile> --user_key <user_keyfile>  
<device_name> mmcblk0p1
```

- <pkc_keyfile>: an RSA 2K or 3K key file
- <sbk_keyfile>: an SBK key file
- <user_keyfile>: a user key file

Note

Use the same key in Preparing Key (Page 44).

For example:

```
$ sudo ./flash.sh -u /secure_boot_save/01_rsa_pri_key/rsa_priv.pem -v  
/secure_boot_save/02_sbk/SBK --user_key /secure_boot_save/03_useykey/kek2_key jetson-  
xavier-nx-devkit-emmc mmcblk0p1
```

Results:

- If flashing boot files succeeds, the device will restart automatically, and you can boot up to OS, Secureboot on the Nvidia Image is successful.
- If flashing boot files succeeds, but the device cannot boot up to OS, check whether the same key in "Preparing the key (Page 44)" is used.
- If flashing boot files fails, check whether the keys or commands are correct.

You can find all above operations in Nvidia guideline

(<https://docs.nvidia.com/jetson/archives/l4t-archived/l4t-3261/index.html#page/Tegra%20Linux%20Driver%20Package%20Development%20Guide/flashing.html#wwpID0E0400HA>).

Note


- This command will also wipe out all the user data on the device.
 - You need to use the signed Image.
-

5.3 Signing files in the Siemens IPC520A support package

When you enable Secureboot, three files *kernel-Image*, *kernel-dtb* and *extlinux.conf* are signed on IPC520A.

The Siemens IPC520A support package also contains these three files, but they are not signed.

When you install the Siemens IPC520A support package, all files from Siemens IPC520A support package replaces the ones in IPC520A. If the status of these three files becomes unsigned, the kernel load has failed.

 WARNING
Install the Siemens IPC520A support package directly after enabling the Secureboot, device will halt on loading kernel.
<ul style="list-style-type: none">• Because the Siemens IPC520A support package contains kernel image and kernel-dtb.• You should sign kernel image and kernel-dtb in Siemens IPC520A support package first, and then install the signed Siemens IPC520A support package.

This chapter describes how to sign *kernel-Image*, *kernel-dtb* and *extlinux.conf* files. For other use case, refer to Nvidia Guideline (https://docs.nvidia.com/jetson/archives/l4t-archived/l4t-3261/index.html#page/Tegra%20Linux%20Driver%20Package%20Development%20Guide/bootloader_secure_boot.html#wwpID0ESHA).

Procedures

Perform the following steps to sign *kernel-Image*, *kernel-dtb* and *extlinux.conf* files.

1. Untar the Siemens IPC520A support package, you can use the `prepare_Image.sh` (Page 93) as a reference.

- Copy the Siemens IPC520A support package and `prepare_Image.sh` to the local host.
- Execute the command:

```
$ chmod a+x prepare_image.sh
$ ./prepare_image.sh get_image <Siemens IPC520A support package name>
```

The output folder is named `deb_temp/not_signed/`.

2. Sign *kernel-Image*, *kernel-dtb* and *extlinux.conf* files.

- Navigate to the `Linux_for_Tegra/` directory on the host PC.
- Enter the command:

```
$./l4t_sign_image.sh --file <Path and file name> --chip 0x19 --key <keyfile>] --
encrypt_key <encrypt_keyfile>
```

Sign the following three files which are untared from Siemens IPC520A support package. For more information, refer to Nvidia guideline

(https://docs.nvidia.com/jetson/archives/l4t-archived/l4t-3261/index.html#page/Tegra%20Linux%20Driver%20Package%20Development%20Guide/bootloader_secure_boot.html#wwpID0E0ZD0HA).

File	Path and file name
kernel Image	<code>deb_temp/not_signed/boot/Image.ipc520a</code>
kernel-dtb	<code>deb_temp/not_signed/boot/dtb/ipc520a-tegra194-p3668-all-p3509-0000.dtb</code>
extlinux.conf	<code>deb_temp/not_signed/boot/extlinux/extlinux.conf</code>

For example:

```
$./l4t_sign_image.sh --file
/home/t/work/to_sign_deb/deb_temp/not_signed/boot/Image.ipc520a --chip 0x19 --key
/secure_boot_save/01_rsa_pri_key/rsa_priv.pem --encrypt_key
secure_boot_save/03_userkey/kek2_key
```

```
$./l4t_sign_image.sh --file
/home/t/work/to_sign_deb/deb_temp/not_signed/boot/dtb/ipc520a-tegra194-p3668-
all-p3509-0000.dtb --chip 0x19 --key /secure_boot_save/01_rsa_pri_key/rsa_priv.pem -
-encrypt_key secure_boot_save/03_userkey/kek2_key
```

```
$./l4t_sign_image.sh --file
/home/t/work/to_sign_deb/deb_temp/not_signed/boot/extlinux/extlinux.conf --chip
0x19 --key /secure_boot_save/01_rsa_pri_key/rsa_priv.pem --encrypt_key
secure_boot_save/03_userkey/kek2_key
```

If there is no error return, go to next step.

3. Make a new support package and name it "signed Siemens IPC520A support package".

- Execute the command:

```
$./prepare_image.sh get_deb
```

The signed Siemens IPC520A support package is saved in folder *encrypt_signed_support_package*.

Note

Once the Siemens IPC520A support package is signed, do not sign it again.

5.4 Installing the signed Siemens IPC520A support package

After you get the "signed Siemens IPC520A support package", perform the following steps to install it on the IPC520A:

1. Copy the "signed Siemens IPC520A support package" from the USB stick to the IPC520A and enter the following command:

```
$ sudo dpkg --force-overwrite -i ipc520a-jp${VERSION}-${DEB_VERSION}-
${CREATED_TIME}_arm64.deb
```

For example:

```
$ sudo dpkg --force-overwrite -i ipc520a-jp4.6-1.0-20220601122040_arm64.deb
```

Note

- *jp\${VERSION}* is the version of supported JetPack;
 - *\${DEB_VERSION}* is version of "signed Siemens IPC520A support package";
 - *\${CREATED_TIME}* is the time when signed Siemens IPC520A support package is created.
-

2. Reboot IPC520A.

Note

- Do not press the On/Off button to switch off the device after the "signed Siemens IPC520A support package" is installed.
- Run the following command to restart the device:

```
$ sudo reboot
```

3. Check the status of the signed Siemens IPC520A support package by entering:

```
$ sudo cat /sys/kernel/debug/gpio | grep D
```

If the return value contains "DI_0", "DI_1" or "DI_2", the signed Siemens IPC520A support package is installed successfully.

Example:

```
gpio-236 (DISABLE_WIFI_N |wifi-disable ) out hi
gpio-237 (DISABLE_BT_N |bt-disable ) out hi
gpio-240 (WWAN_DISABLE_N |wwan-disable ) out hi
gpio-242 (COM1_MODE0 |sysfs ) out hi
```

5.4 Installing the signed Siemens IPC520A support package

```
gpio-243 (COM1_MODE1 |sysfs) out lo
gpio-246 (LED_UDF_RD |?) out lo
gpio-247 (LED_UDF_GN |?) out lo
gpio-264 ( |DI_2) in hi
gpio-265 ( |DI_3) in hi
gpio-266 ( |DO_0) out lo
gpio-267 ( |DO_1) out lo
gpio-419 ( |DI_1) in hi
gpio-421 (GPIO01 |DI_0) in hi
gpio-446 (I2S0_DOUT)
gpio-447 (I2S0_DIN)
```

Note

If the following errors occur, the signing of Siemens IPC520A support package failed.

- After installing the signed Siemens IPC520A support package, the device cannot be booted to desktop.
 - The device can be booted to desktop, but above command return log value does not contain "DI_0", "DI_1" or "DI_2".
-

For more information, refer to:

- Command log for security boot (Page 96)
- Jetson Xavier NX Fuse Specification Application Note (<https://developer.nvidia.com/embedded/downloads#?search=Xavier%20NX%20Fuse%20Specification>)
- NVIDIA Jetson Linux Driver Package Software Features (<https://docs.nvidia.com/jetson/archives/l4t-archived/l4t-3261/index.html>)

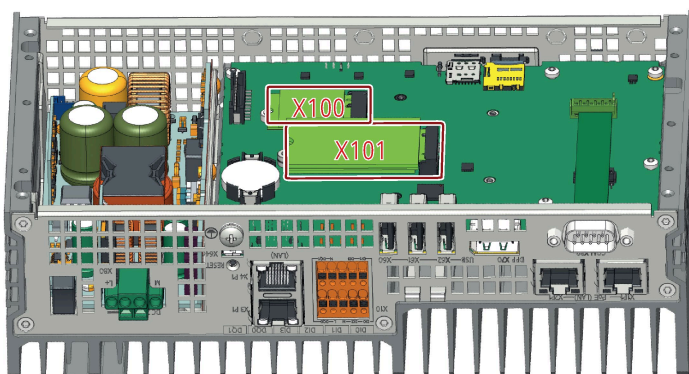
Expanding the device

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. Our device provides two M.2 Key B/ Key E interfaces and mounting positions. M.2 key B module or Key E module can be connected to the interface slot X100 or X101 on the motherboard.

The position of each slot is marked in the following image.



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:

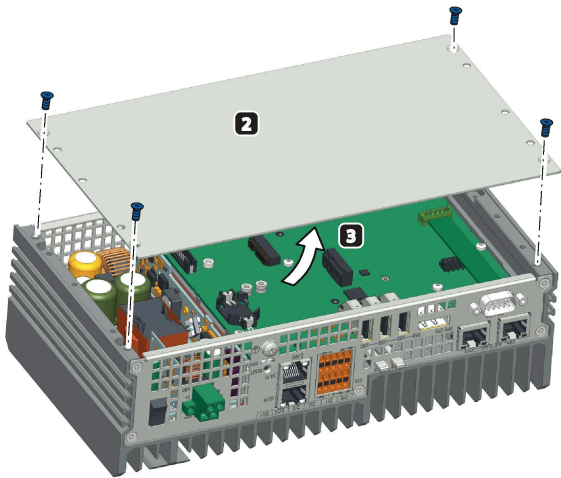
Module	M.2 module 1 (Slot X100)	M.2 module 2 (Slot X101)
Features and function		
Size	2230	2242, 3042, 2250
Interface	Key E	Key B
Channel	1 × PCIe 3.0 (1 lane) + 1 × USB 2.0	1 × PCIe 3.0 (1 lane) + 1 × USB 3.0
Support WLAN module, like Wi-Fi, Bluetooth	Yes	No
Support WWAN module ¹ , like 3G/4G/5G	No	Yes
Support NVMe SSD	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 you to use SIM cards without PIN codes.

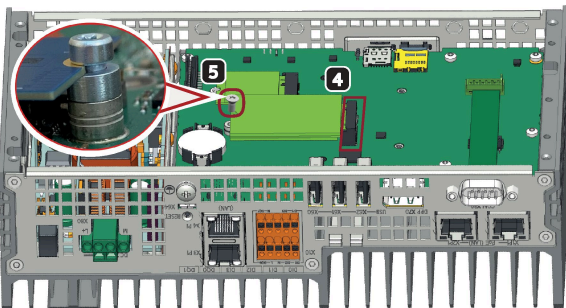
Requirements

- A T10 screwdriver

Procedure - Installing the M.2 module

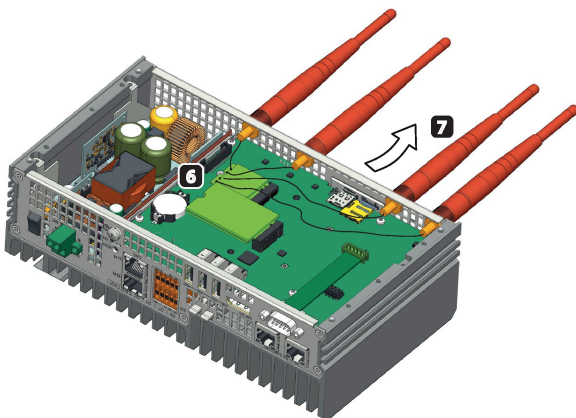


- 1 Disconnect the device from the power supply.
- 2 Remove the retaining screws on the back cover of the device.
- 3 Lift up the device's rear panel.



- 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: Use a screwdriver to pry open the reserved antenna holes. Make sure that there are no iron scraps left on the motherboard.

Procedure - Removing the M.2 module

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

6.2 Inserting the Micro SD card/Nano SIM card

Requirements

- The device is disconnected from the power supply.
- Micro SD card or Nano SIM card that is suitable for industrial use.

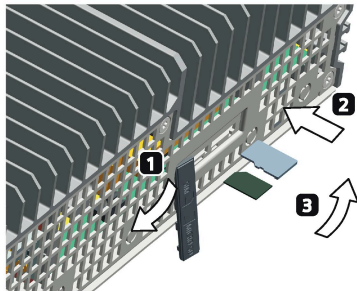
Installation

NOTICE

Inserting a memory card

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

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



- 1** Open the card cover on the bottom.
- 2** Push the Micro SD card/Nano SIM card correctly into the supporting frame. The contacts of the Micro SD card/Nano SIM card must face to the motherboard.
- 3** Push the card cover back.

6.3 Installing the SSD

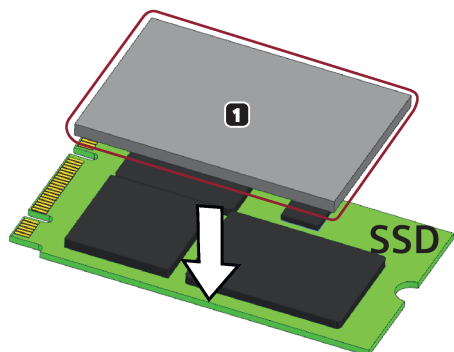
To ensure the heat dissipation performance of SSD, the IPC520A uses a heat sink to secure the SSD.

The heatsink accessory only support 2242 SSD.

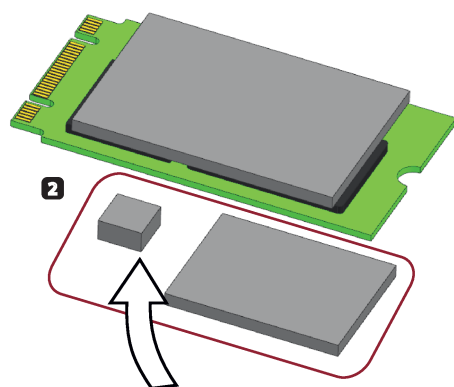
Requirements

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

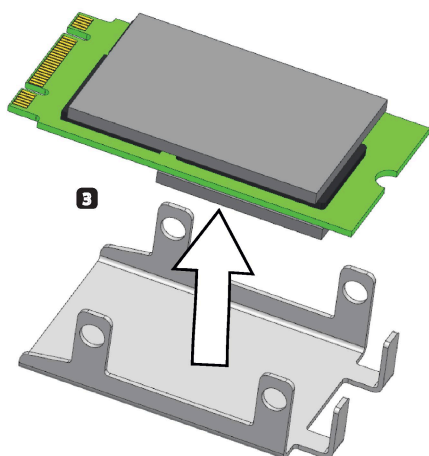
Procedure - Installing the SSD



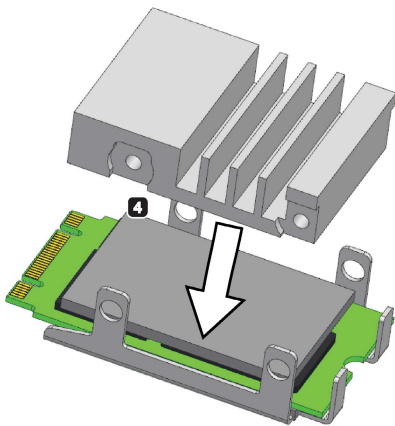
- 1 Place the SSD Thermal Interface Material (TIM) on the chip of SSD.



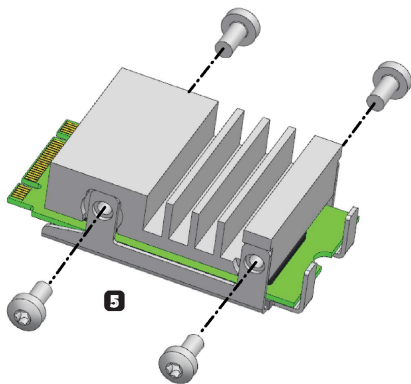
- 2 Place another two SSD TIMs on the other side of SSD.



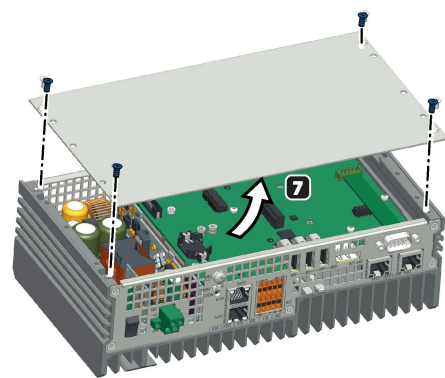
- 3 Place the SSD with TIMs into the sheet metal.



- 4** Cover the heat sink to the sheet metal.

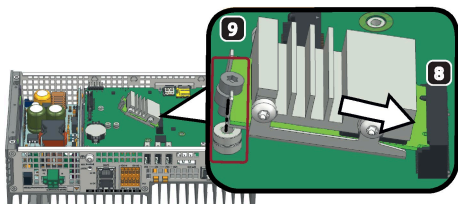


- 5** Fasten the heat sink with 4 screws.



- 6** Disconnect the device from the power supply.

- 7** Remove the retaining screws on the back cover of the device, and lift up the device rear panel.



- 8** 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.

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

Procedure - Removing the SSD

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

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 89)".

 WARNING
<p>Unauthorized opening and improper repairs on the device may result in substantial damage to equipment or endanger the user.</p> <ul style="list-style-type: none"> • 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
<p>Electrostatic sensitive devices (ESD)</p> <p>The device contains electronic components which are destroyed by electrostatic charges. This can result in malfunctions and damage to the machine or plant.</p> <p>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 69)"</p>

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: CR2032W
 - Rated voltage: 3 V DC
 - Max abnormal charging current: 10 mA
- For any requirements on product maintenance, contact Siemens Technical support (Page 89).
- 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 : CR2032W
 - Tension nominale : 3 V CC
 - Courant de charge anormal max. : 10 mA
- Pour toute demande concernant la maintenance du produit, contactez le support technique (Page 89) 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".

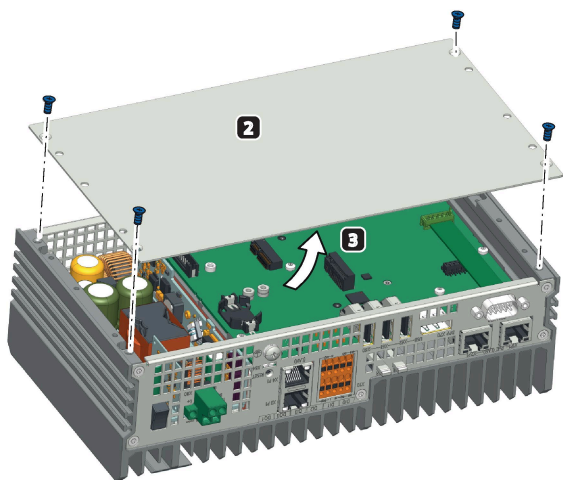
Note

Replace batteries only in non-hazardous areas.

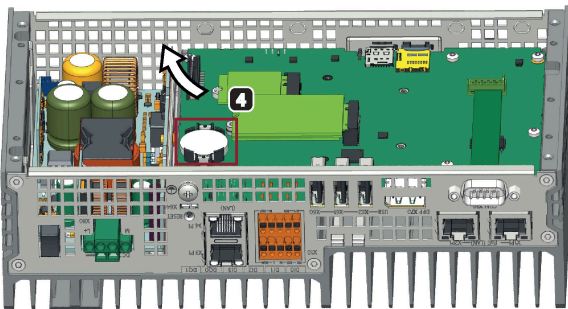
Requirements

- A T10 screwdriver

Procedure



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



- 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）：IPC520A 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 64)".

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.

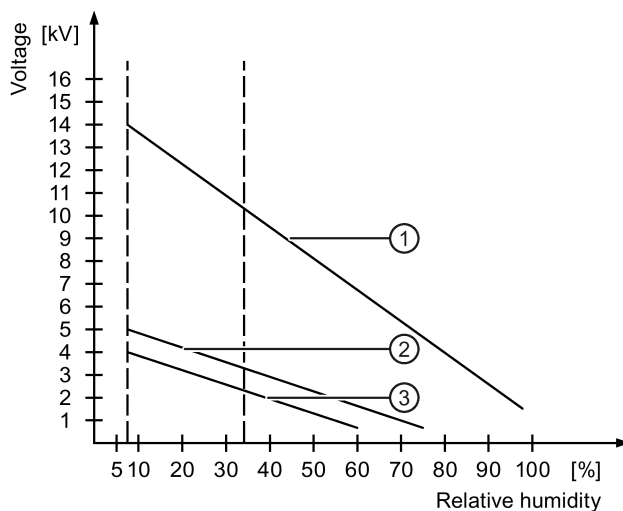
The damage to a module by an overvoltage can often not be immediately detected and only becomes evident after an extended period of operation. The consequences are incalculable and range from unforeseeable malfunctions to a total failure of the machine or system.

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.

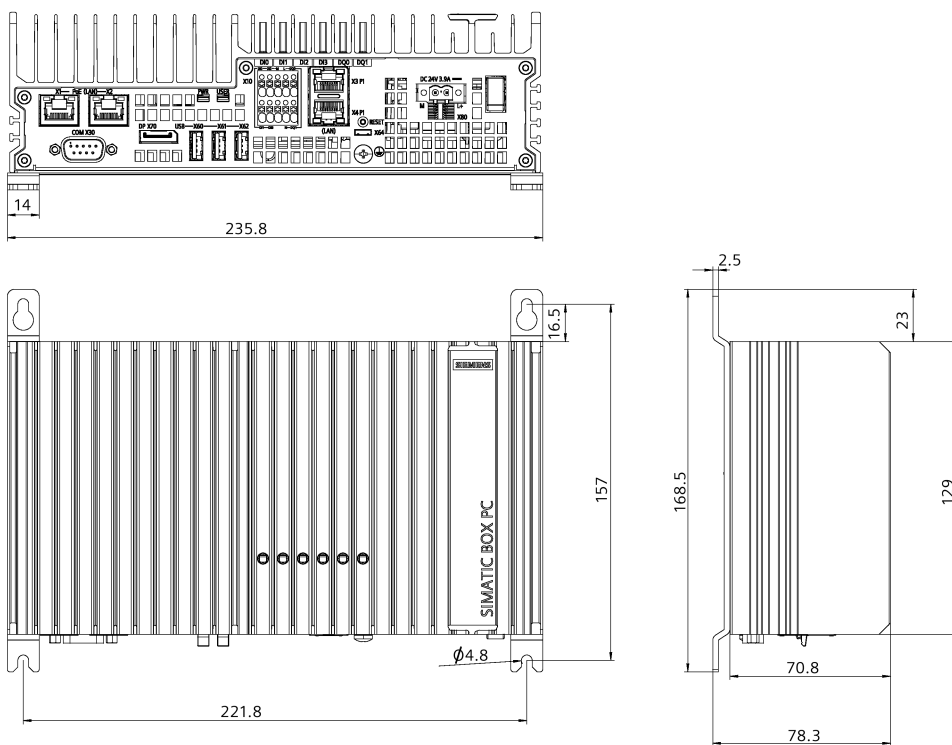
Protect yourself against discharge of static electricity. When working with electrostatic sensitive devices, make sure that the person and the workplace are properly grounded.

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.

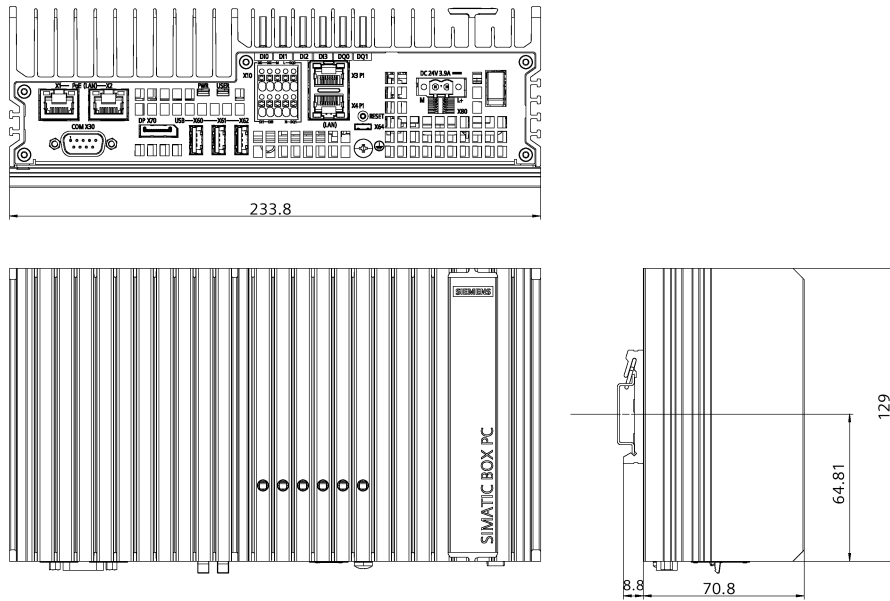
8.3 Dimension drawings

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. 1927.0 g
Power supply ¹	DC 24 V (19.2 to 28.8 V DC)
Brief voltage interruption in accordance with Namur	Up to 5 ms buffer time at 24 V DC and full load ² Max. 10 events per hour; recovery time at least 10 s
Current consumption	Max. 3.9 A
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 : The device may only be connected to a 24 V DC power supply which meets the requirements of a safe extra-low voltage (SELV) or protective extra-low voltage (PELV) in accordance with IEC/EN/DIN EN/UL 61010-2-201.

² : In the event of low supply voltage, the buffer time is reduced.

Electromagnetic compatibility

Radiation Emission (Enclosure port) in accordance with IEC 61000-6-4 + A1/ CAN/CSA-CISPR 32	<ul style="list-style-type: none"> • 30 to 230 MHz: 40 dB(μV/m) Quasi-peak (10 m distance) • 230 to 1000 MHz: 47 dB (μV/m) Quasi-peak (10 m distance) • 1 to 3 GHz: 70 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	<ul style="list-style-type: none"> • ± 2 kV (5 kHz /100 kHz) in accordance with IEC 61000-4-4; Burst • ± 1kV line to line, ±2 kV line to earth in accordance with IEC 61000-4-5; Surge
Immunity on the signal lines	<p>Burst:</p> <ul style="list-style-type: none"> • ± 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 <p>Surge:</p> <ul style="list-style-type: none"> • ± 1 kV line-to-line; ± 2 kV line-to-earth in accordance with IEC 61000-4-5; Length of signal port extension cable ≥ 30 m
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	<p>Radiation Immunity (according to IEC 61000-6-2)</p> <ul style="list-style-type: none"> • 80 MHz to 1GHz 10 V/m, 80 % AM (1 kHz) • 1.4 GHz to 2 GHz 3 V/m, 80 % AM (1 kHz) • 2 GHz to 6 GHz 3 V/m, 80 % AM (1 kHz) <p>Conducted Immunity (according to IEC 61000-4-6)</p> <ul style="list-style-type: none"> • 10 kHz to 80MHz: 10 V, 80% AM (1kHz)
Conducted Emission (Low voltage DC mains port), in accordance with IEC 61000-6-4 + A1	<ul style="list-style-type: none"> • 0.15 to 0.5 MHz / 79 dB (μV) Q, 66 dB (μV) M • 0.5 to 30 MHz / 73 dB (μV) Q, 60 dB (μV) M
Conducted Emission (Telecommunications/Network Port), in accordance with IEC 61000-6-4 + A1	<p>0.15 to 0.5 MHz:</p> <p>97 dB(μV) to 87 dB(μV) Q 74 dB(μV) to 74 dB(μV) M</p> <p>0.5 MHz to 30 MHz:</p> <p>87 dB(μV) Q / 74 dB(μV) M</p>

Motherboard

Processor	ARMv8.2(64bit) heterogeneous multi-processing (HMP) CPU NVIDIA Carmel (Dual-Core) Processor
RAM	8GB LPDDR4x

BIOS SPI Flash	16 MB
Micro SD	Slot for one Micro SD card
Nano SIM card	Slot for one Nano SIM card
EMMC	16 GB EMMc 5.1
Expansion slots	Slot X100: 1 × M.2 Key E WiFi/BT 2230 with Key E
	Slot X101: 1 × M.2 Key B WWAN 2242, 3042, 2250 with key B

Interfaces

USB	<ul style="list-style-type: none"> 1 × USB 2.0 Micro B (X64) 3 × USB 3.0 Type A (X60, X61, X62)
DisplayPort (X70)	<ul style="list-style-type: none"> 1 × DisplayPort interface (DP)
Ethernet port	<ul style="list-style-type: none"> 2 × Gbe RJ45 (X3) Dual channel 2 × Gbe RJ45 (X1) and RJ45 (X2) (with Addition POE Function ¹)
COM (X30)	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> 4 × DI + 2 × DQ

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	Horizontal mounting: 0 to 45 °C
	Desk mounting: <ul style="list-style-type: none"> without SSD: 0 to 45 °C with SSD (max.load 3W): 0 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

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: <ul style="list-style-type: none"> • 5 to 8.4 Hz: 3.5 mm • 8.4 to 500 Hz: 9.8 m/s² DIN-Rail: <ul style="list-style-type: none"> • 10 to 58 Hz: 0.0375 mm • 58 to 200 Hz: 4.9 m/s²
Storage/transport	<ul style="list-style-type: none"> • 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	With SSD: <ul style="list-style-type: none"> • 150 m/s², 11 ms • 50 m/s², 30 ms
Storage/transport	<ul style="list-style-type: none"> • 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 75).

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)
USB Device 2.0	High current	500 mA	--	
M.2 Key B module	Per slot	--	0.8 A	Permitted power distribution: • M.2 module : Total 5 W
M.2 Key E module	Per slot	--	0.8 A	

8.7 Direct current supply (DC)

Technical specifications

Input voltage	DC 24 V (19.2 to 28.8 V DC)
Power consumption	Max. 80 W

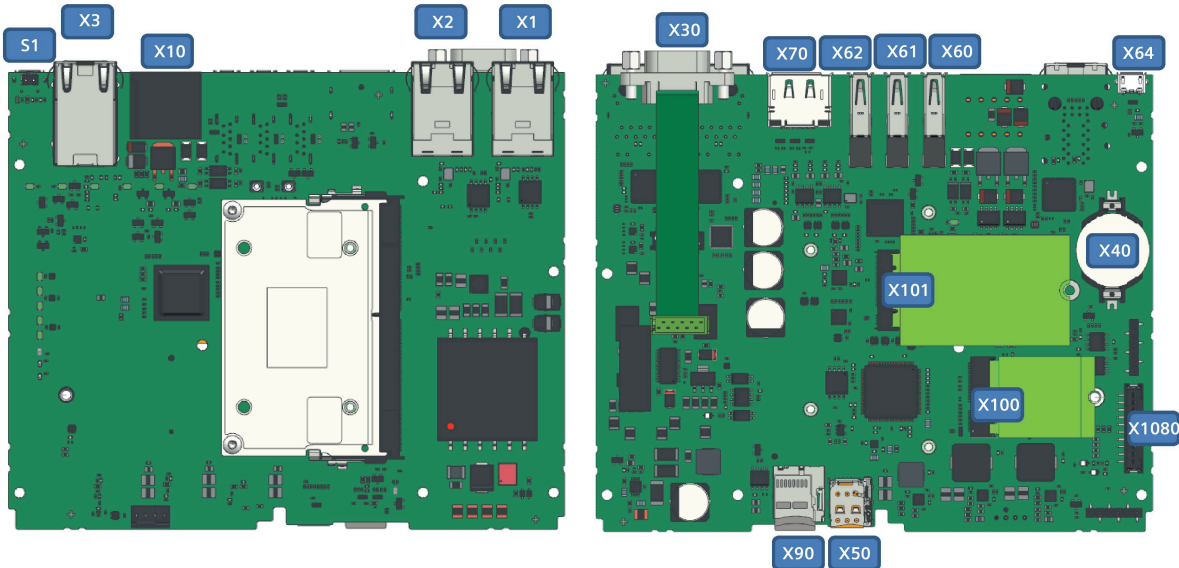
Typical power consumption

	Power consumption (at a rated voltage of 24 V)
Basic device	20 W
POE max. load	2 × 15 W or 1 × 30 W
USB port max. load	6.5 W
Xavier NX modules	15 W

8.8 Hardware descriptions

8.8.1 Motherboard

The following figures show the motherboard of the SIMATIC IPC520A.



Component/interface	Description		Meaning
H1100	LED	PWR	Power (green)
H1101	LED	User	User LED (green/red/orange), programmable
H1200, H1201, H1202, H1203	LEDs	DI0, DI1, DI2, DI3	Input insert (Green)
H1300, H1301	LEDs	DQ0, DQ1	Output Enable (Green)
S1	RESET		For a reset of the CPU
X1	Ethernet 1		RJ45 POE optional
X2	Ethernet 2		RJ45 POE optional
X3	Ethernet 3 and Ethernet 4		Dual Channel RJ45
X30	COM D-Sub9		RS232/RS422/RS485
X60, X61, X62	USB A Host		3 × USB3.0
X64	Micro B		1 × USB2.0
X70	DisplayPort		
X40	Battery-Con		
X50	Micro SD slot		
X90	SIM card slot		
X1080	Power supply		
X100	M.2 Key E		Support WiFi/BT card through PCIe ×1/USB2.0
X101	M.2 Key B		Support WWAN card through PCIe ×1/USB3.0
X10	Digital interface		4 × DI + 2 × DQ

8.8.2 External Interfaces

8.8.2.1 Overview of external interfaces

Interface	Position	Description
USB	External	<ul style="list-style-type: none"> 1 × USB 2.0 Micro B (X64) 3 × USB 3.0 Type A (X60, X61, X62)
Ethernet port	External	<ul style="list-style-type: none"> 2 × Gbe RJ45 (X3) Dual channel 2 × Gbe RJ45 (X1) and RJ45 (X2) (with Addition POE Function)
DisplayPort (X70)	External	<ul style="list-style-type: none"> 1 × DP
COM (X30)	External	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 4 × DI + 2 × DQ

8.8.2.2 Power supply

Plug connector, 2-pin

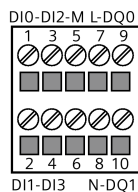
Name of interface on the device: X1080



Pin	Assignment
1	GND (M)
2	DC 24 V (19.2 to 28.8 V DC) (L+)

8.8.2.3 Digital I/O connector

Name of interface on the device: X10



Pin	Short description	Meaning	GPIO number
1	DI0	Digital signal input 0	421
2	DI1	Digital signal input 1	419
3	DI2	Digital signal input 2	264
4	DI3	Digital signal input 3	265
5	DI_M	Digital signal reference M	
6	NC		
7	DQ_L	Digital signal output reference L	
8	DQ_N	Digital signal output reference N	
9	DQ0	Digital signal output 0	266
10	DQ1	Digital signal output 1	267

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
```

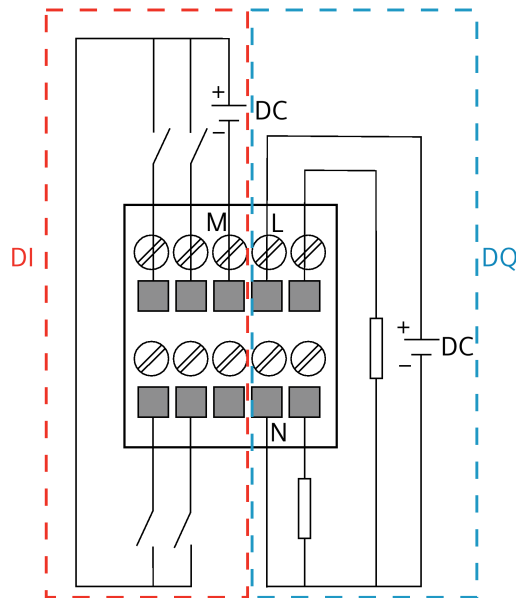
General specifications and features

Technical data	Digital inputs
Number of inputs	4
Type	Sink
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.)	12V±2V DC at 2.5 mA
Logic 0 signal (max.)	5 V±2V DC at 1 mA
Isolation (field side to logic)	500 V AC for 1 minute
Input frequency	<ul style="list-style-type: none"> • Normal input • High speed input
	<ul style="list-style-type: none"> • Max. 20 Hz • --

Technical data	Digital Outputs
Number of inputs	2
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 KΩ load	0.1 V DC max.
Rated current per point (max.) (Resistive load)	0.5 A

Technical data	Digital Outputs
Rated current per point (max.) (pilot duty)	0.5 A
Rated current per common (max.)	1 A
Lamp load (Tungsten)	5 W
ON state resistance	0.6 Ω max.
Leakage current per point	10 μA 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

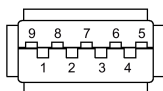


Digital I/O connector uses a double-level terminal block for connection. For more information, refer to Digital I/O terminal block (Page 91).

8.8.2.4 USB

USB 3.0 Type A

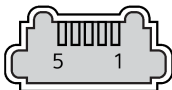
Name of interface on the device: USB-- X60 --- X61--- X62



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

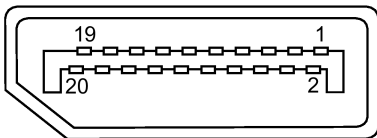
Name of interface on the device: X64



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

8.8.2.5 DisplayPort

Name of interface on the device: X70



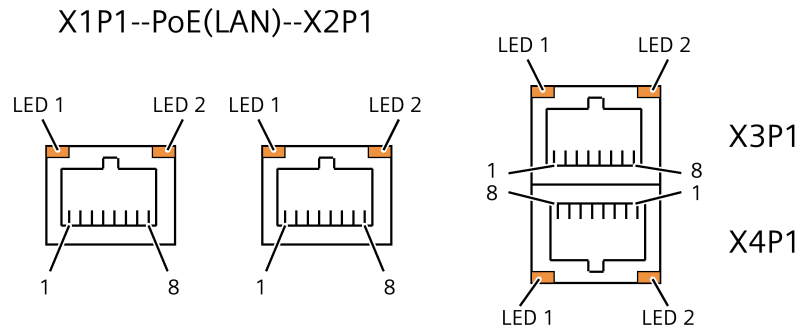
DisplayPort interface			
Pin no.	Abbreviation	Meaning	Input/output
1	ML_Lane 0+	DP data 0+	Output
2	GND	Ground	-
3	ML_Lane 0-	DP data 0-	Output
4	ML_Lane 1+	DP data 1+	Output
5	GND	Ground	-
6	ML_Lane 1-	DP data 1-	Output
7	ML_Lane 2+	DP data 2+	Output
8	GND	Ground	-
9	ML_Lane 2-	DP data 2-	Output

DisplayPort interface			
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--PoE(LAN)--X2P1; X3P1; X4P1

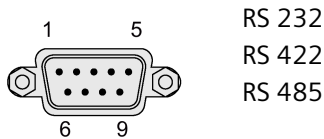


Pin no.	Short description	Meaning	Input / output
1	BI_DA+	Bi-directional data A+	Input/output
2	BI_DA-	Bi-directional data A-	Input/output
3	BI_DB+	Bi-directional data B+	Input/output
4	BI_DC+	Bi-directional data C+	Input/output
5	BI_DC-	Bi-directional data C-	Input/output
6	BI_DB-	Bi-directional data 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	Orange light:1000 Mbps Off: Else	-
	LED 2	Green light: Link Green 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



Assignment RS 232

Pin	Short description	Meaning
1	DCD	Data carrier detect (I)
2	RxD	Received data (I)
3	TxD	Transmitted data (O)
4	nc	
5	M	Ground
6	DSR	Data set ready (I)
7	RTS	Request to send (O)
8	CTS	Clear to send (I)
9	RI	Incoming call (I)

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	

Pin	Short description	Meaning
5	M	Signal ground
6	nc	
7	nc	
8	nc	
9	nc	

8.8.3 Internal interfaces

8.8.3.1 Overview of internal interfaces

Interface	Position	Description
Micro SD slot (X50)	Internal	1 × Micro SD slot
Nano SIM card slot (X90)	Internal	1 × SIM card slot
M.2 Key E (X100)	Internal	Support WiFi/BT card through PCIe x1/USB2.0
M.2 Key B (X101)	Internal	Support WWAN card through PCIe x1/USB3.0

8.8.3.2 Micro SD interface

Name of interface on the device: **X50**

Pin	Abbreviation	Function
1	Dat2	Data line bit 2
2	Dat3	Card Detect / data line bit 3
3	CMD	Command Line
4	Vdd	Voltage supply 2.7–3.6 V
5	Clk	Clock input
6	GND	Signal Ground
7	Dat0	Data line bit 0
8	Dat1	Data line bit 1

8.8.3.3 M.2 interface

M.2 Key E module

Name of interface on the device: X100

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

68	SUSCLK	RESET#	67
66	SIM DETECT	ANTCTL3	65
64	COEX_RXD(I)	ANTCTL2	63
62	COEX_TXD(O)	ANTCTL1	61
60	COEX3(I/O)	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	ALERT#	PERp0	43
42	SMB_DATA	PERn0	41
40	SMB_CLK	GND	39
38	DEVSLP	PETp1	37
36	UIM-PWR	PETn1	35
34	UIM-DATA	GND	33
32	UIM-CLK	PERp1	31
30	UIM-RESET	PERn1	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 Key B 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	NC	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	COEX_TXD(O)	PETn0	47
46	COEX_RXD(I)	GND	45
44	COEX3(I/O)	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	NC	GND	5
4	3.3V	GND	3
2	3.3V	NC	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>)

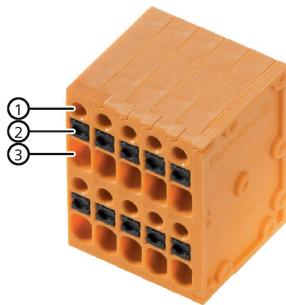
A.2 Troubleshooting

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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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.
The USB3.0 hub can not work on the device.	The support package is not installed on the device.	After installing the support package and rebooting the device, the USB3.0 hub works correctly.

Digital I/O terminal block

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

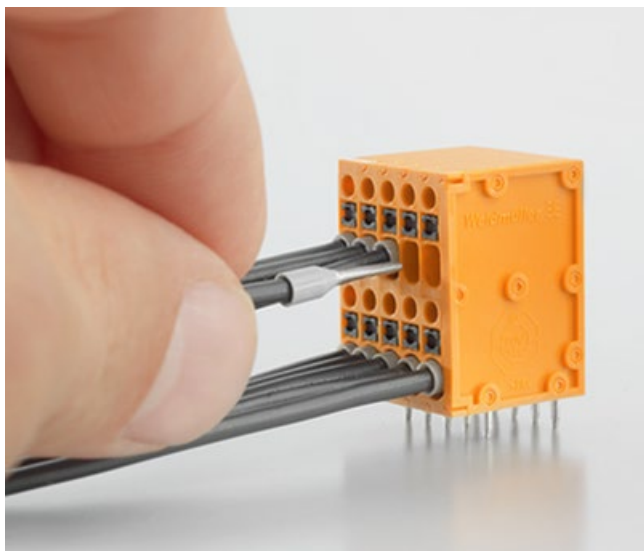


- ① Test point
- ② Button
- ③ Wire entry

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



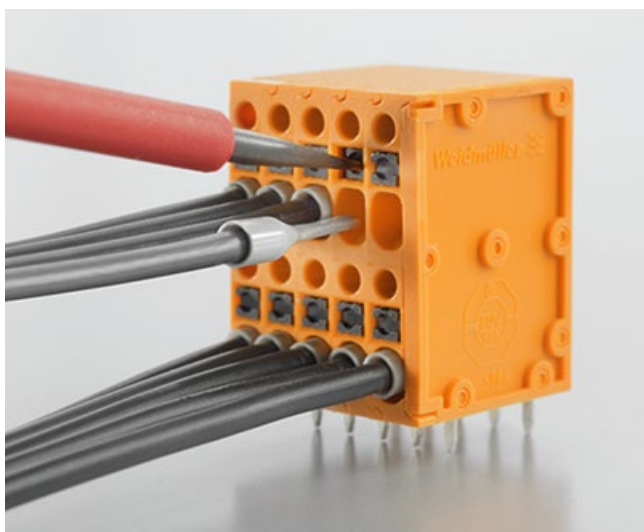
Flexible wire without ferrule:

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

Flexible wire with ferrule and solid:

1. Push the wire directly into wire entry.

Procedure for wiring release



1. Push button with screwdriver and keep pressing button with screwdriver.
2. Pull the wire out of wire entry.
3. Release the button.

Reference files

C.1 prepare_Image.sh

```
#!/bin/bash

#####

# This script can untar deb package and recreate deb package
# This script will not sign them.
# there are three file need be signed and encrypt if fused with user key.
# kernel Image : boot/Image.ipc520a
# kernel-dtb : boot/dtb/ipc520a-tegra194-p3668-all-p3509-0000.dtb
# extlinux.conf : boot/extlinux/extlinux.conf

# if re-create deb, deb was in encrypt_signed
#####

set -e

do_get_signed_encrypt_image()
{
  if [ -e $1 ];then
    echo "extracting Image from $1"
  else
    echo "error: $1 not exist, check it"
  fi
  exit
fi

#clean work dir
echo cleaning dir
rm -rf deb_temp
rm -rf encrypt_signed

mkdir -p deb_temp/not_signed
mkdir -p deb_temp/encrypt_signed

touch deb_temp/this_is_temporary_folder
mkdir -p encrypt_signed_deb

# untar the siemens deb
dpkg -e $1 deb_temp/not_signed/DEBIAN
dpkg -x $1 deb_temp/not_signed

echo "now use sign tool to sign and encrypt Image"
}
```

```

modify_deb_discription()
{

# echo "modify control"
# echo "old info"
# echo
# cat deb_temp/encrypt_signed/DEBIAN/control
OLD_DISCRIPTION=`cat deb_temp/encrypt_signed/DEBIAN/control | grep Description`
NEW_DISCRIPTION=${OLD_DISCRIPTION}"only for security boot"
sed -i "s/${OLD_DISCRIPTION}/${NEW_DISCRIPTION}/g"
deb_temp/encrypt_signed/DEBIAN/control
# echo
# echo "new info"
# echo
# cat deb_temp/encrypt_signed/DEBIAN/control
}

do_create_deb()
{
echo "creating deb, need sure had sign and encrypt
kernel Image kernel-dtb and extlinux.conf with same key with fused"

cp -r deb_temp/not_signed/* deb_temp/encrypt_signed

mkdir -p encrypt_signed_deb

modify_deb_discription

# To prepare deb name

Package=`cat deb_temp/encrypt_signed/DEBIAN/control | grep Package`
# echo ${Package#*: }
Version=`cat deb_temp/encrypt_signed/DEBIAN/control | grep Version`
# echo ${Version#*: }
TimeStamp=`date "+%Y%m%d%H%M%S"`
# echo $TimeStamp
Architecture=`cat deb_temp/encrypt_signed/DEBIAN/control | grep Architecture`
# echo ${Architecture#*: }

# Create deb with signed file
dpkg -b deb_temp/encrypt_signed/ encrypt_signed_deb/${Package#*:}-${Version#*:}-${TimeStamp}_${Architecture#*:}.deb

if [ "$?" == "0" ]; then
echo ${Package#*:}-${Version#*:}-${TimeStamp}_${Architecture#*:}.deb was re-created
success at encrypt_signed_deb/
else
echo meet some error during build deb
fi
}

```

```
if [ "$1" == "get_image" ]; then
if [ "$2" == "" ]; then
echo "Usage $0 $1 xxx.deb"
exit
fi
do_get_signed_encrypt_image $2
elif [ "$1" == "get_deb" ]; then

do_create_deb
else
echo "wrong args $1, Usage
$0 get_image xxx.deb to get image
or
$0 get_deb to recreate signed deb"
exit
fi
```

C.2 command_history.sh

Command log for security boot.

```
# open terminal
```

```
sudo mkdir -p /security_boot_key/01_rsa_pri_key
sudo mkdir -p /security_boot_key/02_sbk
sudo mkdir -p /security_boot_key/03_userkey
# 0777 was just a example
sudo chmod 0777 /security_boot_key -R
cd /security_boot_key/01_rsa_pri_key
openssl genrsa -out rsa_priv.pem 2048
ls rsa_priv.pem
cd /security_boot_key/02_sbk
```

```
echo "0x11111111 0x11111111 0x11111111 0x11111111" > ./SBK
```

```
cd /home/t/work/public_sources/Linux_for_Tegra/source/public/trusty_src/trusty/app/nvidia-
sample/hwkey-agent/CA_sample/tool/gen_ekb/
```

```
/*
```

```
file example.sh:
```

```
echo "22222222222222222222222222222222" > kek2_key
```

```
# This is the default initial vector for EKB.
```

```
echo "bad66eb4484983684b992fe54a648bb8" > fv_ekb
```

```
echo "22222222222222222222222222222222" > sym.key
```

```
echo "00000000000000000000000000000000" > sym2.key
```

```
*/
```

```
./example.sh
```

```
-----
fuse: test
```

```
# cd <Linux_for_Tegra/>
```

```
sudo ./odmfuse.sh -i 0x19 --test \
-k /security_boot_key/01_rsa_pri_key/rsa_priv.pem \
-S /security_boot_key/02_sbk/SBK \
--KEK2 /security_boot_key/03_userkey/kek2_key \
jetson-xavier-nx-devkit-emmc
```

```
fuse :
```

```
sudo ./odmfuse.sh -i 0x19 \
-k /security_boot_key/01_rsa_pri_key/rsa_priv.pem \
-S /security_boot_key/02_sbk/SBK \
--KEK2 /security_boot_key/03_userkey/kek2_key \
jetson-xavier-nx-devkit-emmc
```

```

sudo ./odmfuseread.sh -i 0x19 \
-k /security_boot_key/01_rsa_pri_key/rsa_priv.pem \
-S /security_boot_key/02_sbk/SBK \
jetson-xavier-nx-devkit-emmc

check key and copy backup now .

# clsoe -p
# need add --auth PKCSBK, "SBKPKC" was depend on your key configuration
# to make sure value of SecurityMode was not 0, for example: "SecurityMode: 00000001"

sudo FAB=100 BOARDID=3668 BOARDSKU=0001 BOARDREV=A.0 ./odmfuse.sh -i 0x19 -p --
auth SBKPKC --force \
-k /security_boot_key/01_rsa_pri_key/rsa_priv.pem \
-S /security_boot_key/02_sbk/SBK \
--KEK2 /security_boot_key/03_userkey/kek2_key \
jetson-xavier-nx-devkit-emmc

# to check if -p options was success (value be become fffffff because of it was hide after '-p')
sudo ./odmfuseread.sh -i 0x19 \
-k /security_boot_key/01_rsa_pri_key/rsa_priv.pem \
-S /security_boot_key/02_sbk/SBK \
jetson-xavier-nx-devkit-emmc

-----
#flash OS with security boot key
sudo ./flash.sh \
-u /security_boot_key/01_rsa_pri_key/rsa_priv.pem \
-v /security_boot_key/02_sbk/SBK \
--user_key /security_boot_key/03_userkey/kek2_key \
jetson-xavier-nx-devkit-emmc mmcblk0p1

#####
###
# all above was totally same with guideline from Nvidia
# now need sign siemens-deb
#####
###

-----

mkdir -p /home/t/work/to_sign_deb; cd /home/t/work/to_sign_deb

# sign deb, need copy script prepare_Image.sh and deb to this folder
chmod a+x prepare_Image.sh
# 1 untar deb

```

```
./prepare_Image.sh get_image ipc520a-1.0-20211121181901_arm64.deb

# 2 sign file
# cd <Linux_for_Tegra/>

./l4t_sign_image.sh --file
/home/t/work/to_sign_deb/deb_temp/not_signed/boot/Image.ipc520a --chip 0x19 --key
/security_boot_save/01_rsa_pri_key/rsa_priv.pem --encrypt_key
security_boot_save/03_userkey/kek2_key

./l4t_sign_image.sh --file /home/t/work/to_sign_deb/deb_temp/not_signed/boot/dtb/ipc520a-
tegra194-p3668-all-p3509-0000.dtb --chip 0x19 --key
/security_boot_save/01_rsa_pri_key/rsa_priv.pem --encrypt_key
security_boot_save/03_userkey/kek2_key

./l4t_sign_image.sh --file
/home/t/work/to_sign_deb/deb_temp/not_signed/boot/extlinux/extlinux.conf --chip 0x19 --key
/security_boot_save/01_rsa_pri_key/rsa_priv.pem --encrypt_key
security_boot_save/03_userkey/kek2_key

./prepare_Image get_deb

# cd <Linux_for_Tegra/>

sudo ./flash.sh \
-u /security_boot_key/01_rsa_pri_key/rsa_priv.pem \
-v /security_boot_key/02_sbk/SBK \
--user_key /security_boot_key/03_userkey/kek2_key \
jetson-xavier-nx-devkit-emmc mmcblk0p1

# cd deb folder
./prepare_Image.sh get_image ipc520a-1.0-20211121181901_arm64.deb

# 2 sign file
# cd <Linux_for_Tegra/>

./l4t_sign_image.sh --file
/home/t/work/to_sign_deb/deb_temp/not_signed/boot/Image.ipc520a --chip 0x19 --key
/security_boot_save/01_rsa_pri_key/rsa_priv.pem --encrypt_key
security_boot_save/03_userkey/kek2_key

./l4t_sign_image.sh --file /home/t/work/to_sign_deb/deb_temp/not_signed/boot/dtb/ipc520a-
tegra194-p3668-all-p3509-0000.dtb --chip 0x19 --key
/security_boot_save/01_rsa_pri_key/rsa_priv.pem --encrypt_key
security_boot_save/03_userkey/kek2_key

./l4t_sign_image.sh --file
/home/t/work/to_sign_deb/deb_temp/not_signed/boot/extlinux/extlinux.conf --chip 0x19 --key
/security_boot_save/01_rsa_pri_key/rsa_priv.pem --encrypt_key
security_boot_save/03_userkey/kek2_key

./prepare_Image get_deb
```

C.3 odmfuse.sh Option Examples

For Jetson Xavier NX:

- To fuse PKC HASH from the .pem file with JTAG enabled:

```
$ sudo ./odmfuse.sh -i <chip_id> -p -k <key.pem> --KEK[0-2] <KEK file> -S <SBK_file> >  
<device_name>
```

- To fuse PKC HASH from the .pem file with JTAG disabled:

```
$ sudo ./odmfuse.sh -i <chip_id> -p -k <key.pem> --KEK[0-2] <KEK file> -S <SBK_file> --  
disable-jtag <device_name>
```

- To burn a secure fuse with PKC, SBK, and KEK2:

```
$ sudo ./odmfuse.sh -i <chip_id> -k <PKC file> -S <SBK file> --KEK2 <KEK2 file>  
<device_name>
```

- To burn a secure fuse with PKC and KEK2:

```
$ sudo ./odmfuse.sh -i <chip_id> -k <PKC file> --KEK2 <KEK2 file> <device_name>
```

Where:

- <chip_id> is:
 - For Jetson Xavier NX: 0x19
- <device_name> is the device name of the Jetson platform you are using, as shown in the table of device names in the topic Quick Start.
 - For Jetson Xavier NX: jetson-xavier-nx-devkit-emmc









Markings and symbols

D.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.

D.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

D.3 Operator controls





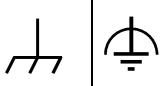













Symbol	Meaning	Symbol	Meaning
	On/off switch, without electrical isolation		Eject CD/DVD
	On/off switch, without electrical isolation		

D.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.

D.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 Electronical 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, 64
Bottom view, 11
BSMI, 68

C

Certificates
 Certifications and approvals, 65
Clearance, 23
COM, 79
Components sensitive to electrostatic charge, 69
Condensation, 22
Connecting
 Peripherals, 29
 Power supply, 32
 protective conductor, 30
Connecting the protective conductor, 31
Current consumption, 73

D

DC power supply, 77
Degree of pollution, 73
Degree of protection, 73
Digital I/O Connector, 79
Directive
 ESD Directive, 69
DisplayPort, 79
DisplayPort interface, 82

E

EAC, 67
ESD, 69
ESD Directive, 69
Ethernet port, 79
Expansion slot, 75

F

FCC, 66
Features, 9
Flash, 75
Front view, 10

G

General technical specifications, 73

I

Identification data, 22
Installation on a DIN rail, 23
Interface
 DisplayPort, 82
Interfaces, 75
 USB 3.0, 82

K

Korea Certificate, 67

L

Limitation of liability, 16, 61
Lithium battery, 62

M

M.2 module
 Installing, 56
 Removing, 57
Micro SD card or Nano SIM card, 57
Motherboard
 Technical features, 78
Mounting
 Wall, 27
Mounting on a standard rail, 73
Mounting position, 23
Mounting type, 23, 25

N

New Zealand
RCM, 67
Noise emission, 73

P

Package contents, 21
 Checking, 21
Packaging, 21
 Checking, 21
 Removing, 21
Pile au lithium, 63
Power supply
 Connecting, 32
 DC power supply, 77
Processor, 74
PROFINET, 77
Protection class, 73
Protective measure
 Static electricity, 71

R

Radiation, 17
 High frequency radiation, 17
RAM, 74
Rating plate, 22
RCM, 67
RCM Australia/New Zealand, 67
Repairs, 61

S

Safety information
 Storage, 22
 Transportation, 22
Side view, 10
SSD
 Installing, 58
 Removing, 59
Static electricity
 Protective measures, 71
Supply voltage, 73

T

Top view, 10

U

UKCAI, 67
USB, 79
USB 3.0
 Interface, 82

W

Wall mounting, 23, 27, 72
Warranty, 15
Weight, 73