Hitachi Industrial Edge Computer

CE50-10 Instruction Manual

CC-65-0171

■ Product covered by this manual

CE50-10 (Operating system: Ubuntu 18.04 LTS (Linux kernel 4.15))

■ Export restrictions

If you export this product, please check all restrictions (for example, Japan's Foreign Exchange and Foreign Trade Law, and USA export control laws and regulations), and carry out all required procedures.

If you require more information or clarification, please contact your Hitachi sales representative.

■ Trademarks

HITACHI is a registered trademark of Hitachi, Ltd.

Intel and Intel ATOM are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

Linux(R) is the registered trademark of Linus Torvalds in the U.S. and other countries.

Ubuntu and Canonical are registered trademarks of Canonical Ltd.

Other company and product names mentioned in this document may be the trademarks of their respective owners.

■ Software

This product contains some open source software to perform its functions. The property rights, copyrights, and other intellectual property rights of the open source software belong to the author, and can be used under the conditions stated in the bundled license. For details, see the following file in this product:

/hitachi/licenses/copyright.txt

For open source software whose license specifies that the source code is to be provided, Hitachi will provide the source code of the open source software. Contact your Hitachi sales representative or distributor if you require such source code. Hitachi assumes no liability, including liability for damages, for open source software and its use.

This does not mean that Hitachi disclaims product liability for this unit.

■ Precautions

All contents of this manual are protected by copyright. No part of this manual may be reproduced in any form or by any means without permission in writing from the publisher. Information in this manual is subject to change without notice.

Read this manual carefully and keep it. Before using the unit, make sure that you thoroughly read and understand all the safety instructions. Keep this manual in a place where it can be readily accessed as necessary.

■ Issued

July 2020: CC-65-0171

December 2020: CC-65-0171

May 2021: CC-65-0171

■ Copyright

All Rights Reserved. Copyright (C) 2020, 2021, Hitachi, Ltd.

Preface

If the manual says *contact us*, please contact your Hitachi sales representative, distributor or customer support

■ Intended readers

This manual is intended for users involved in system planning, system design, installation, configuration, operation and maintenance of the Hitachi Industrial Edge Computer CE50-10 (referred to as *unit* or *this unit* hereinafter).

■ Organization of this manual

This manual is organized into the following chapters and appendixes:

1. Installing the CE50-10
> This chapter describes installation of the unit and connection with the power supply.

2. CE50-10 Names and Functions of Parts
> This chapter describes the name of each part.

3. Operating the Power Supply of the CE50-10
> This chapter describes operating the power supply and provides important information.

4. External Contact Functions
> This chapter describes the external contact function.

5. Configuring Software Environment
> This chapter describes OS settings, and development and registration of application programs.

6. Managing User Accounts
> This chapter describes management for user accounts.

7. Maintaining the CE50-10
> This chapter describes maintenance.

8. Troubleshooting
> This chapter describes troubleshooting.

A. Unit Specifications
> This appendix describes the unit specifications.

B. External Interface
> This appendix describes the external interface specifications.

C. Real-time Clock Specifications
> This appendix describes the clock specifications.

D. Connector Specifications
> This appendix describes the connector specifications.

E. Error Messages
> This appendix describes error messages output from programs.

F. Option Functions for Application Programs
> This appendix describes option functions relating to development and installation of application programs.

G. Library Interface Reference
> This appendix describes the library interfaces.

H. Security Specifications
> This appendix describes log capacities and the security functions.

I. Communication Sheet

This appendix describes the communication sheet.

■ Note on storage capacity calculations

Information such as memory capacities, memory requirements, file sizes, and storage requirements are calculated by using the formula 2^n. The following shows the results of such calculations by 2^n:

1 KB (kilobyte) is 1,024 bytes.

1 MB (megabyte) is 1,048,576 bytes.

1 GB (gigabyte) is 1,073,741,824 bytes.

1 TB (terabyte) is 1,099,511,627,776 bytes.

Information such as disk capacities and network transmission rate are calculated by using the formula 10^n as follows:

1 KB (kilobyte) is 1,000 bytes.

1 MB (megabyte) is $1,000^2$ bytes.

1 GB (gigabyte) is $1,000^3$ bytes.

1 TB (terabyte) is $1,000^4$ bytes.

⚠ Precautions for safe handling

Safety precautions are provided in the following headline, which consists of a safety warning symbol and the string *DANGER*, *WARNING*, *CAUTION*, or *Notice*.

⚠	This is a safety alert symbol used to notify the user of potential risk of personal injury. To avoid the risk, follow the messages indicated with this symbol.
⚠ **DANGER:**	Indicates a hazardous situation that, if not avoided, will result in death or serious injury. (This signal word is not used in this manual)
⚠ **WARNING:**	Indicates a hazardous situation that, if not avoided, could result in death or serious injury.
⚠ **CAUTION:**	Indicates a hazardous situation that, if not avoided, could result in minor or moderate injury.

NOTICE:	This signal word is used to indicate information considered important but not hazard-related (e.g. message related to property damage).

The headword Note is used to indicate precautions on handling and operating the unit.

- Pay special attention to and observe all precautions indicated on this product, in this manual and related documents. Failure to do so could result in physical injury, or damage to property including this product.

- Do not perform any operations or take any actions that are not described in this manual and related documents. If there is a problem with the unit not covered in this manual or related documents, please contact Hitachi or your distributor for assistance. The precautions indicated on the unit and in the manual have been carefully prepared considering your safety,

there is a possibility of unpredictable hazard. Use your own discretion at all times when using this product, in addition to following the instructions.

■ Safety guidelines

Before using the unit, carefully read the following safety guideline:

- Each operation you perform must comply with all applicable instructions or procedures in this manual.

■ ⚠ Warning: Electric shock hazard and fire hazard

- Insufficient grounding might cause electric shock during operation or maintenance inspection of the unit. Make sure that sufficient grounding is provided when installing the unit.

- Condensation might cause a short-circuit fire during operation of the unit. Make sure that no condensation is present.

- Subjecting the unit to physical impact during use might cause a short-circuit fire. Avoid impacting the unit in any way.

- If you see smoke or smell an unusual odor, stop the supply of power to the unit, unplug the power cable from the outlet, and then contact the sales branch or us. Using the damaged unit might cause a fire or electric shock.

- Do not modify the unit. Modification might cause a fire or electric shock. Hitachi shall not be responsible for any consequences resulting from modification of the unit.

- Do not use a multi-outlet extension cord. Use of such a cord might subject it to excessive current, which might cause overheating and fire.

- Do not insert or remove a power cable plug with wet or perspiring hands as doing so might cause electric shock.

- Firmly insert the power cable plug all the way to the base. A power cable plug that is inserted incompletely might cause heat generation due to poor contact. Dust accumulation and substances such as water droplets on the cable plug might cause overheating and fire.

Handling of power cables

   Do not use a power cable other than that supplied with the unit.

   If an insufficiently rated power cable is used, it might overheat due to excessive current, which might cause fire.

   Observe the following to prevent electric shock or fire due to damage to the power cable:

   - Do not pull the cable.

   - Dot not snag the cable in anything.

   - Do not bend the cable.

   - Do not expose the cable to chemical substances.

   - Do not twist the cable.

   - Do not place anything on the cable.

   - Do not bundle the cable with other cables.

   - Do not fix the cable with a stapler or the like.

   - Do not use a damaged cable.

- To remove a cable, hold the connector and then pull it out straight. Pulling the cable or applying excessive force on the connector might damage the cable and cause fire or electric shock.

- Use the I/O port only for interfaces of a suitable voltage and current rating. If overvoltage or overcurrent is applied, the part is damaged and might cause fire or failure.

■ ⚠ Other Warnings

- This unit is not intended for use in facilities or with equipment where human life or other extreme liability is involved or for the purpose of controlling such equipment. Examples of such facilities and equipment are medical equipment, nuclear power facility or equipment, aviation or space equipment, and transportation facilities and equipment. Hitachi shall not be liable for any accidents resulting in injury or death or property damage arising from the use of this unit in such facilities or with such equipment or control systems.

- Do not use the unit as a footstool or bookend, or for any purpose other than its original application. The unit might be damaged or might fall, causing injury or failure.

- Configure an emergency stop circuit or interlock circuit outside the product. Failure of this product might damage the devices connected to it or cause an accident.

■ ⚠ Caution against falls

- To avoid injury, be careful not to drop or topple the unit during transport or disposal.

■ ⚠ Caution against burn injury

- Note that the unit becomes hot during use. The unit with a failure might generate heat. Avoid direct contact with your skin. Parts within the unit are very hot immediately after the power supply to the unit is turned off. Before handling the unit, make sure that the parts have sufficiently cooled.

■ ⚠ Other cautions

- Be careful not to injure your fingers when unpacking or transporting the unit.

■ Notice

- When mounting or replacing hardware, wear a grounding band and take antistatic measures.

- When tightening or removing screws, use the tool appropriate for the size and type of screw head. Be careful not to damage the screw head. To prevent screw threads being damaged, tighten screws squarely into their holes. Do not apply excessive force during tightening.

- Avoid using this unit in a place that is dusty, humid, or exposed to corrosive gas. Use in such places might cause damage or fire.

- Do not subject the unit to impact during unpacking or transport. Doing so might cause damage.

- Allow sufficient space for ventilation in the front and rear of the unit. If ventilation is obstructed, overheating might cause failure or shorten the service life.

- This unit uses a lithium battery. To dispose of the unit, contact the Hitachi maintenance company. If you dispose of it by yourself, follow the rules or regulations of the local authority.

- When disposing of the unit, you are obliged to issue a manifest for industrial waste. For details, contact the industrial waste association of the relevant prefecture. The manifest form is available from the Japan Industrial Waste Information Center.

■ ⚠ WARNING indicated in this manual

- Insulation failure or electric leakage might cause an electric shock. When using the unit, make sure that the unit is grounded. (See pages VII and 3.)

- Do not modify or disassemble the unit. Failure to heed this warning might cause a fire or electric shock, or might damage the unit. (See page 2.)

- Use the power cable that comes with the unit. Using any other cable might cause equipment failure, fire, or electric shock. If this unit is to be used with a voltage over 125 V AC, prepare a suitable power cable and verify proper operation of the cable before use. (See page 2.)

- The outlet to which this unit is connected must have a ground terminal (ground pole). You must also install an electrical leakage breaker. Failure to take these measures might cause fire and electric shock. (See page 2.)

- Do not use a two-pole plug without a ground pole. Doing so might cause electric shock or equipment failure. (See page 2.)

- If you notice smoke or an unusual odor, turn off the main power switch (MAIN POWER). If you contracted maintenance services, contact the sales branch or maintenance personnel. Using the damaged unit might cause fire or electric shock. (See page 21).

- If you cannot immediately turn off the main power switch (MAIN POWER) because the unit is installed in a rack, stop the power at the power supply source. (See page 21).

- If there is smoke or an unusual odor, unplug the power cable plug from the outlet, and then contact us. Using the damaged unit might cause a fire or electric shock. (See page 144.)

■ ⚠ CAUTION indicated in this manual

- Storing the unit in a hot location might cause it to become excessively hot. In this case, do not touch the unit with bare hands. (See page 3.)

- For the LAN port IP address of the development unit, specify the same IP address as the network address of the LAN port connected to the unit that is to be set up. Make sure that the IP address of the development unit differs from that of the unit that is to be set up. If these units have the same IP address, the following error message appears. `KXDL010-W Ethernet adapter(`*interface-name*`) Duplicate IP address.` (See page 42.)

- Do not disassemble the unit during inspection or cleaning. The unit has a sealed structure and does not require internal inspection or cleaning. When the cover is removed, do not touch internal parts, as doing so might cause a burn injury, damage to internal parts, or unit failure. (See page 139.)

- This unit uses a lithium battery. When replacing the battery, you must use the one specified by Hitachi. Using any other battery might cause an explosion, fire, rupture, heat generation, leakage, or gas generation. (See page 140.)

## ■ Notice indicated in this manual

- Before moving the unit, shut down the OS, turn off the MAIN POWER switch (MAIN POWER), and then remove the power cable plug from the outlet. Not following this procedure might result in unit failure. (See pages 3 and 139.)

- When carrying or transporting the unit, use the packing materials in which the unit was packaged for delivery. (See pages 3 and 139.)

- When carrying or transporting the unit, it is recommended that you use the packing materials in which the unit was packaged for delivery. If such packing materials are not available or are damaged, carefully pack the unit in a way that protects it from shock, vibration, and electrostatic discharges. (See pages 3 and 139.)

- Moving or transporting a unit that is installed in a cubicle or rack with casters might subject it to excessive vibration or physical impact, resulting in failure of the unit. Select or design a cubicle or rack that meets the installation conditions. Similarly, make sure that the unit is not subject to vibration or physical impact when you move, carry, or transport it. (See pages 3 and 139.)

- Do not stack units or install a display on the units as excessive heat might radiate from the top of the unit. (See page 4.)

- Prevent heat accumulation around the unit to ensure that ambient temperature requirements are met. (See page 4.)

- Do not lay the power cable close to signal cables, as such a cable layout might cause equipment failure or malfunctions. (See page 8.)

- Application programs do not operate in maintenance mode. After maintenance work is finished, you must return the mode to normal mode. (See page 73.)

- Do not hot swap USB equipment or cables with the unit. Hot swapping might cause the unit to malfunction or stop. (See page 139.)

- Table 7–5: Periodic inspection items shows periodic inspection items. Hitachi is responsible for performing periodic inspections under a maintenance contract. Only Hitachi staff and officially-trained personnel are permitted to perform periodic inspections. (See page 139.)

- Do not use life-limited parts beyond their recommended replacement cycle. Deteriorated parts might cause damage. (See page 140.)

■ Warning indications on the product

The warning labels are attached in the following locations of the unit.
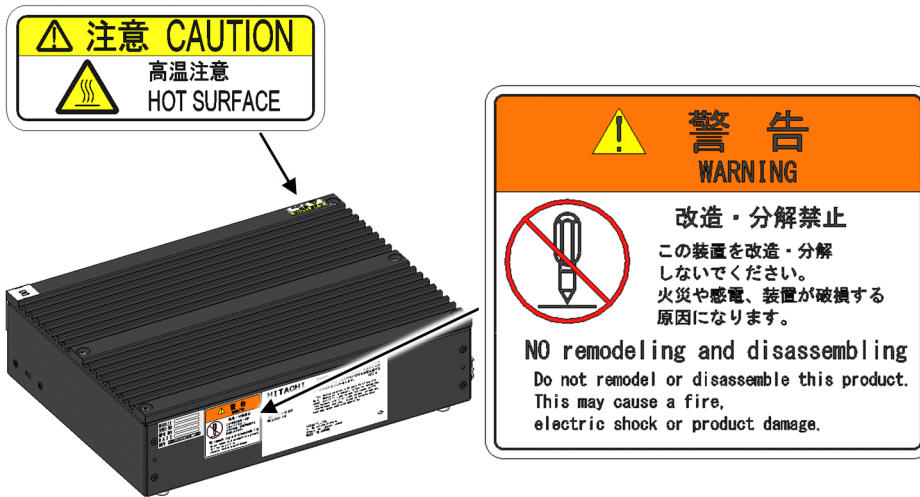
■ Indication based on EU Battery Directive (2006/66/EC)

EU
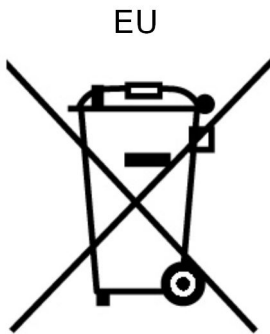
This symbol mark is valid in EU countries.

This symbol mark is defined in the EU Directive 2006/66/EC, Article 20 *Information for end-users* and Annex II.

The European Union has separate collection systems for used batteries and accumulators. Dispose of batteries and accumulators correctly at your local community waste collection/recycling center.

■ Before use

This manual describes basic operations and maintenance of the CE50-10.

For details about the specification of the unit, see A.1 Unit specifications

Descriptions of OS operation and software on systems without an OS are not provided in this manual.

Roles of operators

For a long and stable use of this unit, consider the following:

Considerations for characteristics of the unit
    Perform periodical cleaning, maintenance, and inspection of the unit.
    Periodically remove dust from around the unit (especially the bottom of the unit) and from grooves of the unit.
    The basic principle for handling is to follow the precautions in this manual. Do not turn on and off the power supply without due care.
    For details about handling and maintenance, see the relevant chapter.
Integrity of the unit
    Note the following to ensure integrity of the unit:
    Grounding

Type-D grounding (formerly type 3 grounding) is required to prevent electric shock, to maintain normal operation of electronic circuits containing LSI, and to protect the unit from abnormal voltage due to lightening surge.

Turning off the power supply

Turn off the main power switch on the front of this unit. (See 3.3 Turning off the power to the CE50-10.

⚠ WARNING: Insulation failure or electric leakage might cause an electric shock. When using the unit, make sure that the unit is grounded.

■ Regulations and countermeasures

Voluntary control of radio wave interference

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Countermeasures against instantaneous voltage drop in power supply

A defect might occur in this unit in the event of an instantaneous voltage drop in the power supply due to lightening. As the countermeasures against instantaneous voltage drop of power supply, we recommend that you use an uninterruptible AC power supply unit.

Contents

6

Managing User Accounts   127

7

Maintaining the CE50-10   133

8

Troubleshooting   141

Appendixes

1 Installing the CE50-10

This chapter describes installation of the CE50-10 and connection with the power supply.

1.1 Prerequisites

To ensure long service life of the unit without impairing its functions, appropriate environment and handling are required.

⚠ WARNING

> Do not modify or disassemble the unit. Failure to heed this warning might cause a fire or electric shock, or might damage the unit.

Do not install the unit in any of the following places. Doing so might damage the unit or shorten its service life:

- A place exposed to direct sunlight
  Example: Near a window
- A place subject to extreme changes of temperature or humidity
  Example: Near an air conditioner
- A place subject to electrical noise
  Example: Near a motor, generator, or air ionizer
- A place subject to strong magnetic fields
  Example: Near a magnet
- A place subject to excessive dust
- A place subject to frequent vibration
- A place subject to corrosive gas
- A place subject to sound-induced vibration
  Example: Near large buzzers or alarms
- A place subject to corrosive salt particles
  Example: Outdoors near the seashore

1.1.1 Rated power supply

Table 1–1: Input power supply voltage shows the input power supply voltage available for this unit.

Table 1–1: Input power supply voltage

Input power supply voltage
AC100V to AC240V +10%, -10%

1.1.2 Installation of the unit

⚠ WARNING

- Use the power cable that comes with the unit. Using any other cable might cause equipment failure, fire, or electric shock. If this unit is to be used with a voltage over 125 V AC, prepare a suitable power cable and verify proper operation of the cable before use.
- The outlet to which this unit is connected must have a ground terminal (ground pole). You must also install an earth leakage circuit breaker.
  Failure to take these measures might cause fire and electric shock.
- Do not use a two-pole plug without a ground pole. Doing so might cause electric shock or equipment failure.

⚠ CAUTION

- Storing the unit in a hot location might cause it to become very hot. In this case, do not touch the unit with bare hands.

NOTICE

- Before moving the unit, shut down the OS, turn off the MAIN POWER switch (MAIN POWER), and then remove the power cable plug from the outlet. Not following this procedure might result in unit failure.
- When carrying or transporting the unit, it is recommended that you use the packing materials in which the unit was packaged for delivery.
- If the packing materials in which the unit was packaged for delivery are missing or damaged, package the unit after taking antistatic measures. Also, make sure that the packaged unit is not subject to vibration or physical impact that exceed specified limits.
- Moving or transporting a unit that is installed in a cubicle or rack with casters might subject it to excessive vibration or physical impact, resulting in failure of the unit. Select or design a cubicle or rack that meets the installation conditions. Similarly, make sure that the unit is not subject to vibration or physical impact when you move, carry, or transport it.

Note

For notes on installation conditions, see 1.2 Installation conditions.

(1) Integrity of the unit

Note the following to ensure integrity of the unit:

(a) Grounding (earthing)

Secure and reliable earthing system is required to prevent electric shock, to maintain normal operation of electronic circuits containing LSI, and to protect the unit from abnormal voltage due to lightening surge.

(b) Turning off the power supply

Turn off the power switch on the front of this unit. (See 2.1 Indicators and controls on the unit.)

⚠ WARNING

Insulation failure or electric leakage might cause an electric shock. When using the unit, make sure that the unit is grounded.

1.2 Installation conditions

NOTICE

- As the heat is radiated from the top side of the unit, do not stack any other item on the top of the unit. For example, do not piggyback multiple units on each other, and do not place display devices on top of the unit.
- Install the unit in places where environmental conditions of the product are met, and in a way that heat will not accumulate around the unit.

1.2.1 Installation spacing

Secure spacing of at least 80 mm at the front of the unit, at least 50 mm at the rear, and at least 10 mm at the top.

Figure 1–1: Installation and operation space
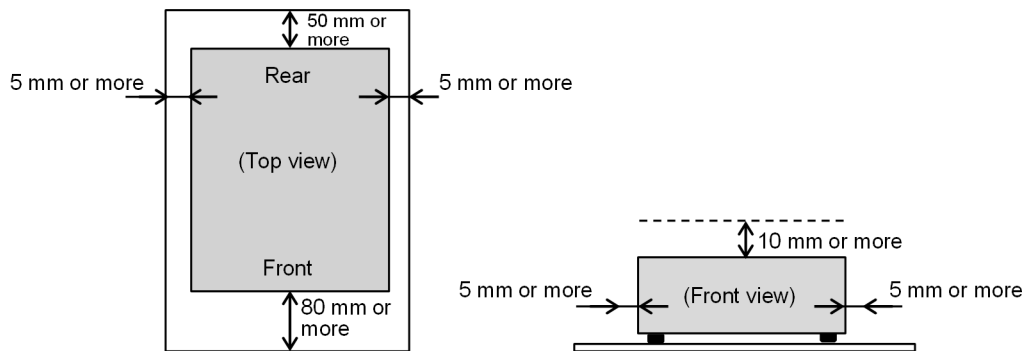
Multiple devices can be installed adjacent to each other, thereby sharing the side spacings, provided that you allow for sufficient spacing at the top, ensure that all other installation conditions and precautions are satisfied, and allocate sufficient operation space.

1.2.2 Installation position

You can install this unit on a desktop, in a 19-inch rack, or on the wall. The following describes the various installation positions.

(1) Desktop installation

Horizontally install the unit on a desktop. Do not install it on a floor.

(2) 19-rack installation

Install the unit in a rack by using the mounting brackets attached to the unit. For details about how to attachmounting brackets to the unit, see 1.2.3 Attaching the mounting brackets.

(3) Wall installation

You can install the unit in the following position on a suitably sturdy wall by using mounting brackets. For details about how to attach the mounting brackets to the unit, see 1.2.3 Attaching the mounting brackets.

Figure 1–2: Orientation when installing the unit on a wall
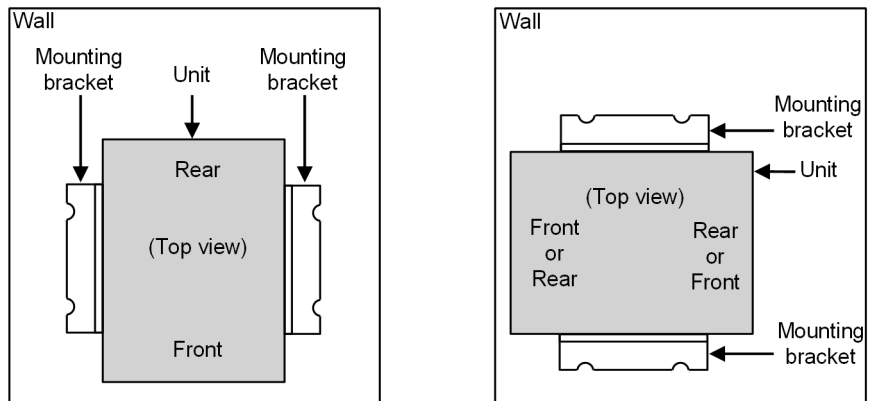
1.2.3 Attaching the mounting brackets

Remove the rubber feet from the bottom of the unit and attach the mounting brackets according to the following procedure.

1. Place the unit upside down.

   You can see the rubber feet on the top.

   Figure 1–3: Attaching mounting brackets (1)
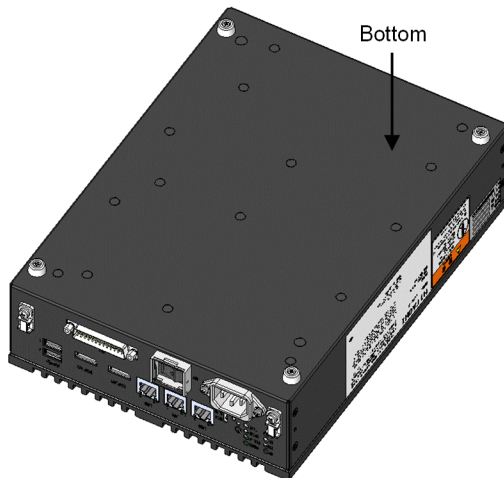
2. Remove the screws that secure the rubber feet.

   The rubber feet are removed.

Figure 1–4: Attaching mounting brackets (2)
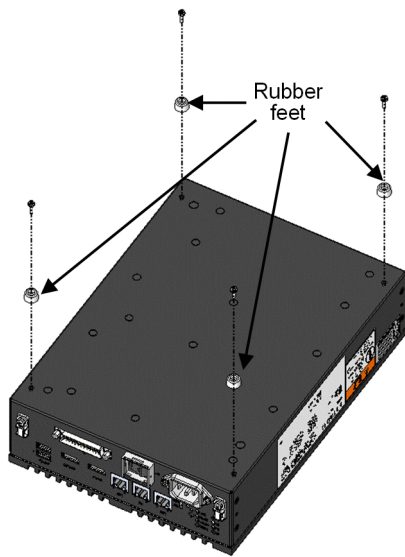
Rubber
feet

3. Attach the mounting brackets by using ISO metric M3 **x** 8 screws with washers to the screw holes to which the rubber feet were fixed.

Figure 1–5: Attaching mounting brackets (3)
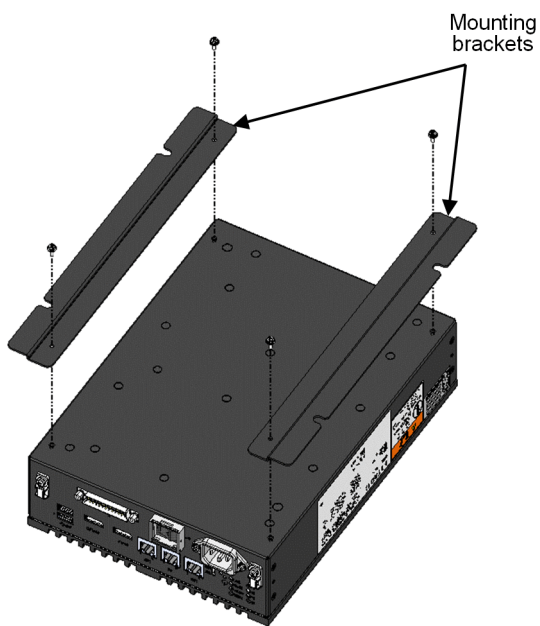
Mounting
brackets

4. Place the unit with its bottom facing down.

This completes attaching of the mounting brackets.

Figure 1–6: Attaching mounting brackets (4)

1.3 Connection to the power supply

NOTICE

Do not place the power cable adjacent to a signal cable, as such a cable layout might cause equipment failure or malfunctions.

Connect the power cable as shown in the following example.

Figure 1–7: Power supply connection
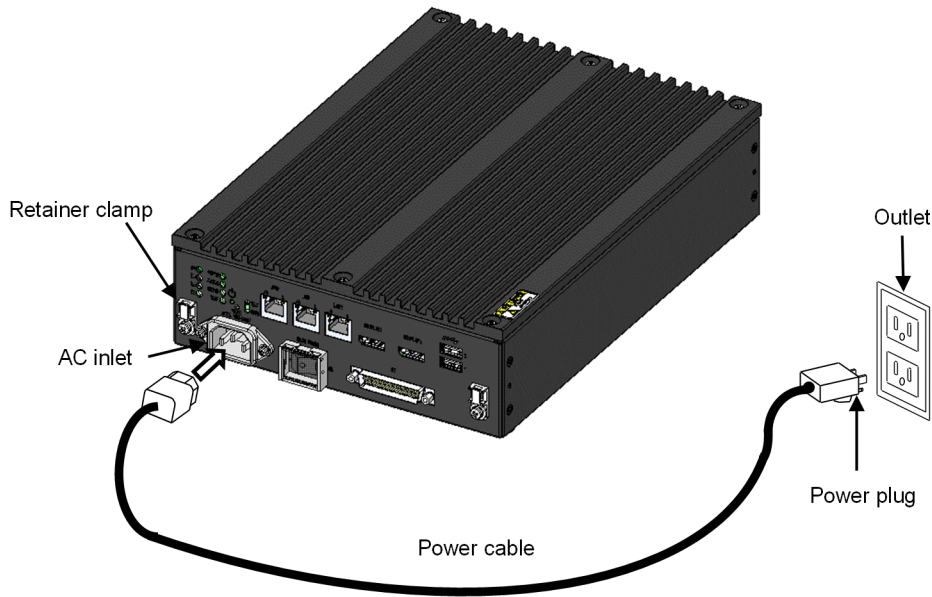
Connecting to a power supply outlet

Firmly insert the power cable plug into an outlet[#] that has a ground pole.

Figure 1–8: Connecting the power cable to an outlet

[#]
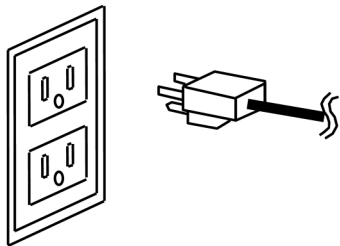
    If the only option is to use an outlet that does not have a ground pole, use a grounded to non-grounded conversion adapter and connect the green ground cable from the adapter to a secure and reliable ground of the building. Verify that the connections of grounded to non-grounded conversion are correct before use.

Preventing the power cable from being inadvertently disconnected

To prevent the power cable from being inadvertently disconnected, secure it by using a retainer clamp, as shown in the following figure.

When securing the power cable, make sure that the radius of the cable bundling is at least 40 mm.

Figure 1–9: Using a power cable retainer clamp
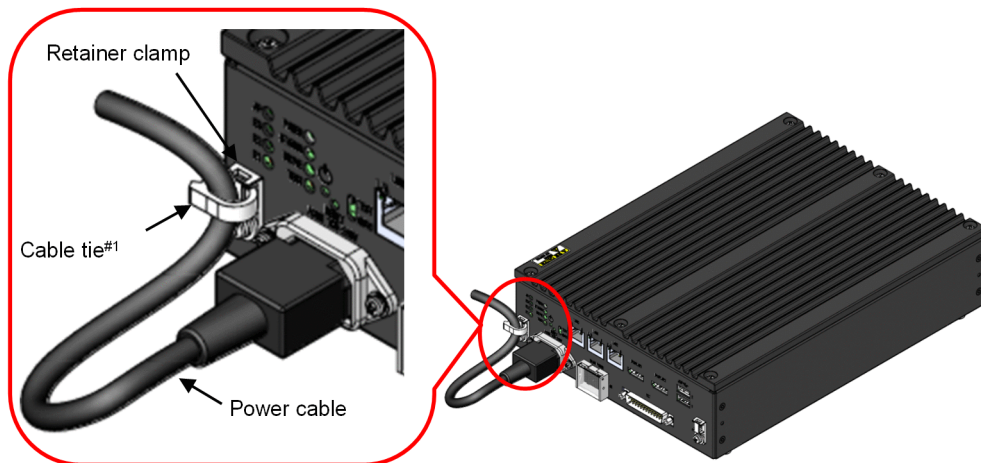
#1

    Cable ties are not provided with the product. To use cable ties, you need to purchase them yourself.

2

CE50-10 Names and Functions of Parts

This chapter describes the name and function of each part of the CE50-10.

2.1 Indicators and controls on the unit

Figure 2–1: CE50-10 front view
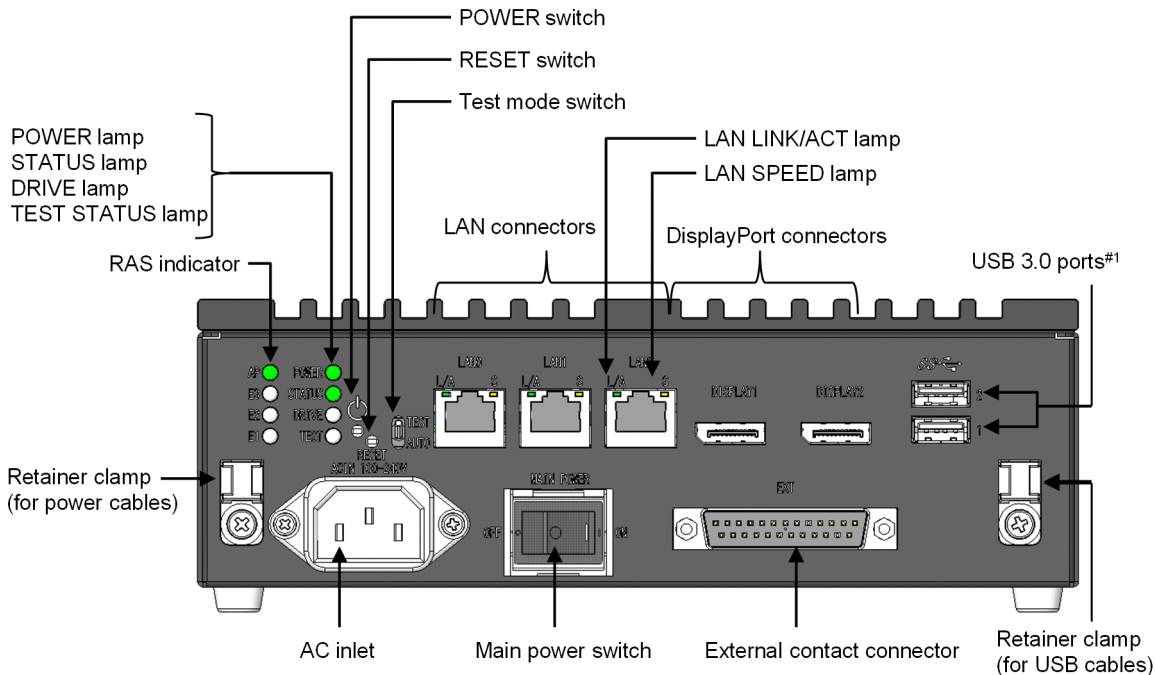
#1

USB ports do not support a locking mechanism. A USB cable might become disconnected if it is inadvertently knocked, for example. If necessary, fix the USB cable to the retainer clamp (for USB cables) on the front of the unit by using, for example, a cable tie.

2.1.1 POWER switch

This switch is used to shut down the OS in the case of an error.

Do not use this switch during normal operation. To completely turn off the power, use the main power switch.

If you forcibly turn off the power by pressing the POWER switch for 4 or more seconds, the unit is placed in the emergency shutdown state. In this state, the unit cannot be started by pressing the POWER switch. In such a case, turn off the main power switch, and then turn it on again to restore the unit.

2.1.2 Reset switch (RESET)

This switch is used to perform a hardware reset (restarting the unit).

Do not use this switch during normal operation. This switch is also used to collect a memory dump after an error occurs. To press the RESET switch, insert the eject pin and press the switch. The unit restarts after collecting a memory dump.

2.1.3 Test mode switch (AUTO, TEST)

Use this switch to set startup mode. Do not change the shipping configuration (AUTO). Set the mode before starting the unit.

AUTO: Start the unit in normal mode.

TEST: Start the unit in test mode, which is not used in normal operation.

Note

Do not operate the test mode switch.

If the shipping configuration (AUTO mode) is changed, the unit does not operate normally.

2.1.4 LAN connectors (LAN0, LAN1, LAN2)

Connect LAN cables to these ports.

2.1.5 Main power switch (MAIN POWER)

Power supply switch

○ : Power is turned off

| : Power is turned on

2.1.6 RAS indicator (AP, E3, E2, E1)

RAS functions are supplemental functions for improving the reliability, availability and serviceability (RAS) of this product.

These indicators show the cause of an error if an unexpected shutdown occurs. For the top indicator (AP), the meanings of the display can be defined by using a user program.

Table 2–1: RAS indicator (AP, E3, E2, and E1)

Position	Lamp	Description
Top (AP)	Off	Indicates that no error has occurred or the unit is not used.
	Green	The meaning of the lamp can be defined by the user program.[#]
	Red	The meaning of the lamp can be defined by the user program.[#]
3rd row (E3)	Off	Indicates that no error has occurred (normal status).[#]
	Red	Indicates that a kernel panic occurred.[#]
2nd row (E2)	Off	Indicates that no error has occurred (normal status).[#]
	Red	Indicates that a multi-bit error occurred in memory.[#]
Bottom (E1)	Off	Indicates that no error has occurred (normal status).
	Red	Indicates that a timeout of the watchdog timer occurred.

#: Cannot run without an OS.

2.1.7 Power lamp (POWER)

This lamp indicates the power status of the unit.

Table 2–2: Power lamp (POWER)

Lamp	Description
Green	Indicates that the unit is operating (power is turned on).
Red	Indicates that the unit is not operating (standby state).
Off	Indicates that the main power switch is turned off.

2.1.8 STATUS lamp (STATUS)

This lamp indicates the operating status of the unit.

Table 2–3: STATUS lamp (STATUS)

Lamp	Description
Green	Indicates that the OS is running.[#]
Red	Indicates that the BIOS is running, the OS is starting, or the unit stopped due to an error.
Off	Indicates that the OS has stopped.

#: Cannot run without an OS.

2.1.9 Drive lamp (DRIVE)

This lamp indicates the access status of the disk.

Table 2–4: DRIVE lamp (DRIVE)

Lamp	Description
Green	Indicates that the SSD is being accessed.
Red	Indicates that the disk is in abnormal status.[#1, #2]
Off	Indicates that no access is made to the SSD.

#1: Cannot run without an OS

#2: This lamp lights red if a failure occurs in a disk other than a built-in SSD, for example, in a USB HDD.

2.1.10 TEST STATUS lamp (TEST)

This lamp indicates the operating status of the test tool. This lamp is lit only when the test tool is used.

Table 2–5: TEST STATUS lamp (TEST)

Lamp	Description
Solid green	Indicates that the test tool terminated normally.
Blinking green	Indicates that the test tool is running.
Red	Indicates that the test tool terminated abnormally.
Off	Indicates that the test tool is not used.

2.1.11 LAN SPEED lamp (LAN0, LAN1, or LAN2)

This lamp indicates the link speed of the LAN.

Table 2–6: LAN SPEED lamp (LAN0, LAN1, or LAN2)

Lamp	Description
Green	Indicates that the network is operating at 1000 Mbps.
Yellow	Indicates that the network is operating at 100 Mbps.
Off	Indicates that the network is operating at 10 Mbps or a link has not been established.

2.1.12 LAN LINK/ACT lamp (LAN0, LAN1, or LAN2)

This lamp indicates the link status and communication status of the LAN.

Table 2–7: LAN LINK/ACT lamp (LAN0, LAN1, or LAN2)

Lamp	Description
Solid green	Indicates that a link has been established.
Blinking green	Indicates that network data is being sent or received. The blinking interval varies depending on the network traffic.
Off	Indicates that a link has not been established.

2.1.13 DisplayPort connectors (DISPLAY1 and DISPLAY2)

These connectors are for connecting cables from display devices.

2.1.14 External Contact connector (EXT)

This connector is used as a general-purpose contact I/O interface.

2.1.15 USB 3.0 ports (USB1 and USB2)

These connectors are for connecting USB devices.

2.2 Security slot

The security slot provided on the rear of the unit is used to secure the unit by using an anti-theft lock.

Figure 2–2: CE50-10 diagonal view

Security slot
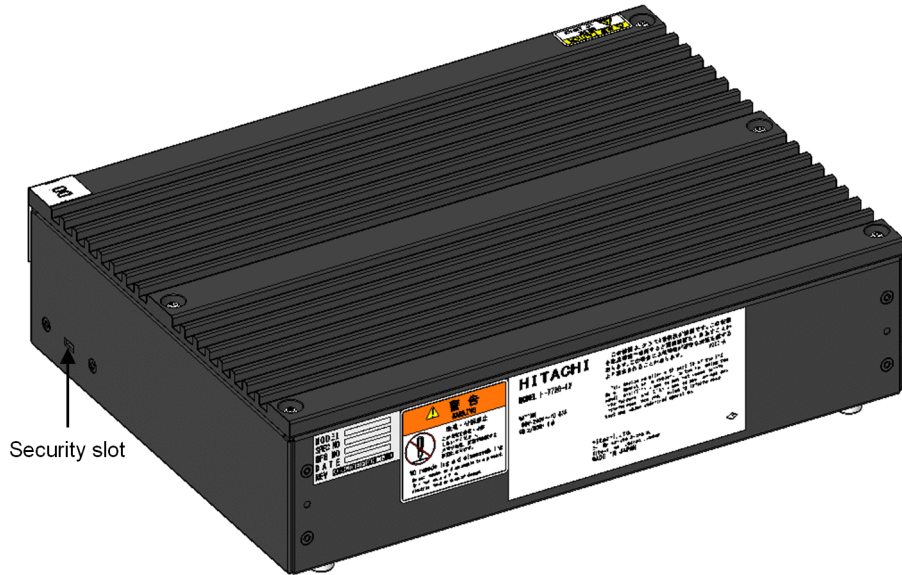
Note

The product does not include an anti-theft lock.

3

Operating the Power Supply of the CE50-10

This chapter describes operating the power supply of the CE50-10 and provides important information.

3.1 Precautions

3.1.1 Before turning on the power

Before turning off the power, see the precautions in the following:

- 1.1 Prerequisites
- 1.1.1 Rated power supply
- 1.1.2 Installation of the unit

3.2 Turning on the power to the CE50-10

Turning on the power to the unit starts the OS.

3.2.1 Starting the unit

To start the unit:

1. Make sure that the power cable and ground cable are correctly connected to the unit.

2. After connecting cables to the unit, insert the power cable plug into the outlet.

3. Turn on the main power switch (MAIN POWER).
   The POWER lamp (POWER) lights red, and then automatically changes to green and the unit is turned on.

4. When the BIOS starts, the STATUS lamp (STATUS) lights red. When the OS has started and the unit is running, the STATUS lamp (STATUS) changes to green.

Note

When you turn on the power to this unit for the first time, you need to log in by using the password described in 5.2 Logging in to the unit after powering it on for the first time. See 5.2 Logging in to the unit after powering it on for the first time and then log in to the unit.

3.3 Turning off the power to the CE50-10

Shut down the OS, and then turn off the power to the unit.

3.3.1 Stopping the unit

To stop the unit:

1. Log in (or remotely log in) to the unit.

   For the user name and password that are to be used for login, see 5.2 Logging in to the unit after powering it on for the first time.

2. Run the following command to shut down the OS.

   Before shutting down the unit, confirm that no other users are logged in.

```
$ shutdown -h 0
```

3. When the unit stops, the STATUS lamp is extinguished.

Note

To restart the unit after it is stopped, perform the steps in 3.3.2 Turning off the power to the CE50-10, and then perform the steps in 3.2 Turning on the power to the CE50-10. At this time, after turning off the power to the unit, wait at least 1 minute (3.3.2 Turning off the power to the CE50-10) before turning the power on again (3.2 Turning on the power to the CE50-10). If the interval is less than 1 minute, the unit might not start normally.

3.3.2 Turning off the power to the CE50-10

To turn off power to the CE50-10:

1. Make sure that the unit has stopped (for details, see 3.3.1 Stopping the unit).

2. Turn off the MAIN POWER switch (MAIN POWER).

3. When the power is turned off, the POWER lamp (POWER) is extinguished.

4. Remove the power cable from the outlet.

Note

After turning off the power, wait at least 1 minute before turning on the power again. If the interval is less than 1 minute, the unit might not start normally.

3.4 Stopping the CE50-10 in the case of an emergency

⚠ WARNING

If you notice any sign of serious damage in the unit (for example, smoke or an unusual odor), immediately turn off the main power switch (MAIN POWER) and contact us. If you contracted maintenance services, contact the maintenance personnel. Using the damaged unit might cause fire or electric shock.

If you cannot immediately turn off the main power switch (MAIN POWER) because the unit is installed in a rack, stop the power at the power supply source.

4

External Contact Functions

This chapter describes the external contact interfaces of the CE50-10. The external contact functions cannot run without an OS.

4.1 PSDOWN (EXT)

4.1.1 Signal name

PSDOWN, DO0_GND

4.1.2 Description

Power-off signals.

These signals indicate that power to the target unit is turned off.

4.1.3 Specifications

Table 4–1: PSDOWN contact specifications

I/O	Item	Specifications
Output specifications	Output method	Photo-MOS relay contact (Form B contact)
	Load voltage	Max. 40 V DC (external power supply required)
	Load current	Steady state: Max. 0.1 A/point
	Dielectric strength	250 V AC, 1 minute

4.1.4 Terminal number

Table 4–2: PSDOWN terminal number

Signal	Terminal number
PSDOWN	14
DO0_GND	2, 5, 15

4.1.5 Connection diagram

Figure 4–1: Connection diagram
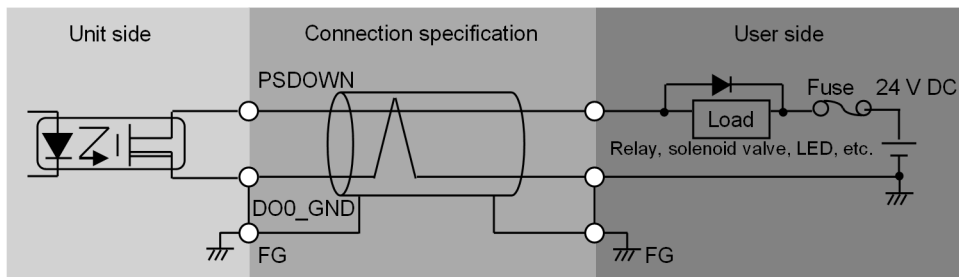
4.2 DO (EXT)

4.2.1 Signal name

- DO_01, DO_02, DO_03, DO_04, DO_05, DO0_GND
- DO_06, DO_07, DO_08, DO_09, DO_10, DO1_GND

4.2.2 Description

General-purpose contact output signals.

Meanings of the signals can be defined for each system by using a user program.

4.2.3 Specifications

Table 4–3: DO contact specifications

I/O	Item	Specifications
Output specifications	Output method	Photo-MOS relay contact (Form A contact)
	Rated output voltage	24 V DC (external power supply)
	Rated output current	0.1 A/point
	Response time	10 ms or less (per contact)
	Dielectric strength	250 V AC, 1 minute

4.2.4 Terminal number

Table 4–4: DO terminal number

Signal	terminal number		Signal	terminal number
DO_01	3		DO_06	19
DO_02	16		DO_07	7
DO_03	4		DO_08	20
DO_04	17		DO_09	9
DO_05	6		DO_10	22
DO0_GND*	2, 5, 15		DO1_GND*	8, 18, 21

*

DO0_GND is for PSDOWN and DO_01 to DO_05. DO1_GND is for DO_06 to DO_10.

4.2.5 Connection diagram

Figure 4–2: Connection diagram

- DO_01 to DO_05
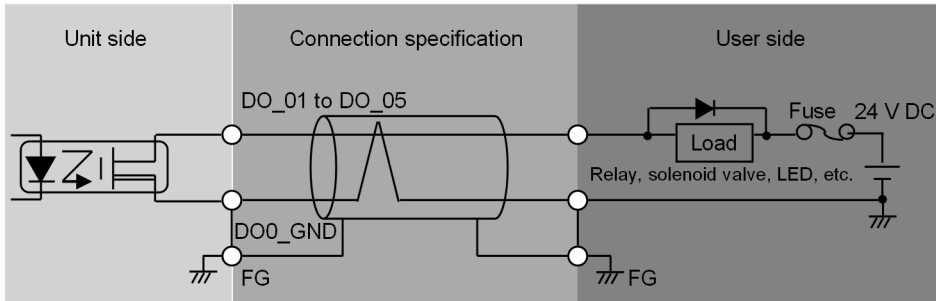
- DO_06 to DO_10
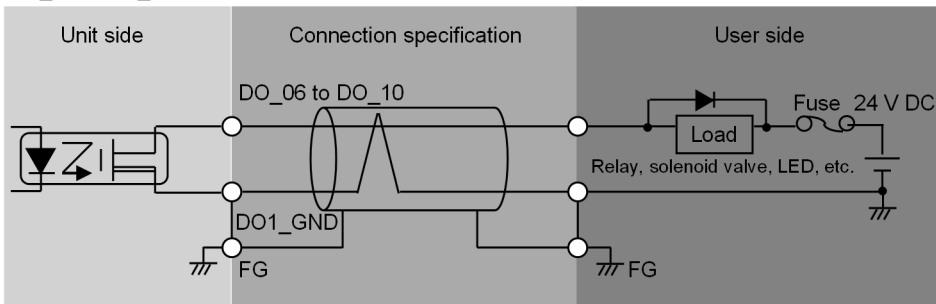
4.3 DI (EXT)

4.3.1 Signal name

DI_01, DI_02, DI_03, DI_04, DI_GND

4.3.2 Description

General-purpose contact input signals.

Meanings of the signals can be defined for each system by using a user program.

4.3.3 Specifications

Table 4–5: DI contact specifications

I/O	Item	Specifications
Input specifications	Input method	Photocoupler contact
	Rated input voltage	24 V DC (external power supply)
	Rated input current	5 mA/point
	Response time	10 ms or less (per contact)
	Dielectric strength	250 V AC, 1 minute

4.3.4 Terminal number

Table 4–6: DI terminal number

Signal	Terminal number
DI_01	11
DI_02	12
DI_03	24
DI_04	25
DI_GND	10, 13, 23

4.3.5 Connection diagram

Figure 4–3: Connection diagram
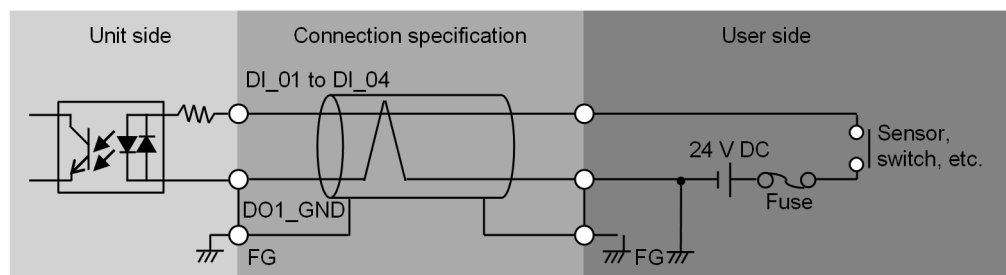
5 Configuring Software Environment

This chapter describes how to configure the OS settings of the CE50-10. This chapter also describes the procedures for the development and registration of application programs.

5.1 Constructing the setup environment

When you set up a unit or install application programs, you need to connect a unit containing a development environment (development unit) to the target unit (unit to be set up). The development environment and the target unit can also be consolidated into a single unit. In this case, there is no need to transfer the master files of application programs.

Figure 5–1: Configuration for constructing the environment
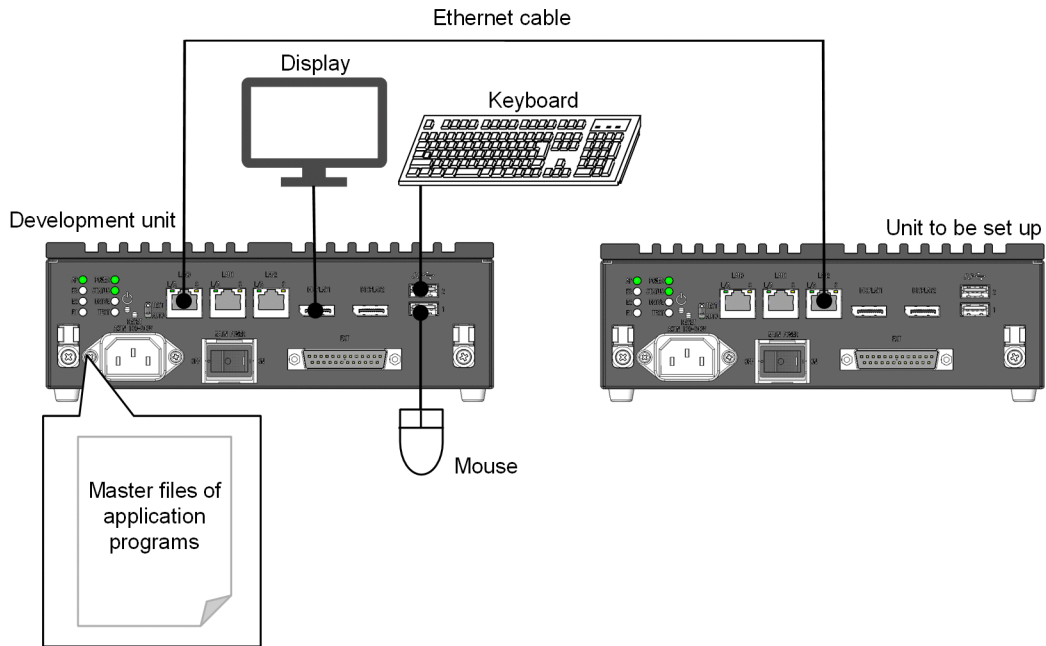
5.2 Logging in to the unit after powering it on for the first time

When you start the unit for the first time, you need to log in using the default user information shown in the table below and then change the password.

Table 5–1: Default user information

User name	Password	Description
edgeadm	Hitachi1 This password is only valid for the first login.	You must change the password at the first login.[#] Manage the new password so that you will not forget it.

#:

To ensure security, the password change function starts immediately after the first login.

Note that, when repair work is performed, the operating system might be reinstalled. In that case, the password and other settings will be initialized.

Set a new password for `edgeadm`. Use the new password for the subsequent login.

```
Login: edgeadm
Password: Hitachi1
You are required to change your password immediately (root enforced)
Changing password for edgeadm.
(current) UNIX password: <- Enter "Hitachi1" for the password.
New password: <- Enter the new password.
Retype new password: <- Enter the new password again for the confirmation
```

In addition, consider creating a user account for each person who operates the unit, such as for each maintenance worker, rather than allowing `edgeadm` to be shared by multiple users. Setting an account for each user makes it easier to identify the cause of a security incident.

For details about how to add or delete a user or change the password, see 6. Managing User Accounts.

After the password is set, the software license is displayed. Verify the displayed information, enter `yes`, and then press the **Enter** key.

Depending on the software installed on the product, multiple licenses might be displayed. If you verify all the licenses and then enter `yes`, you will be logged in to the unit.

5.3 Using the desktop

5.3.1 Starting the desktop

To start the desktop:

1. Start the unit in normal mode.

   You cannot use the desktop in maintenance mode. For details about how to change the OS operation mode, see 5.14 Changing OS operation mode.

2. Log in to the unit, and then run the following command.

```
$ sudo systemctl start gdm3.service
```

3. After the command is executed, the desktop login screen appears.

   Click the user ID to be used for login.
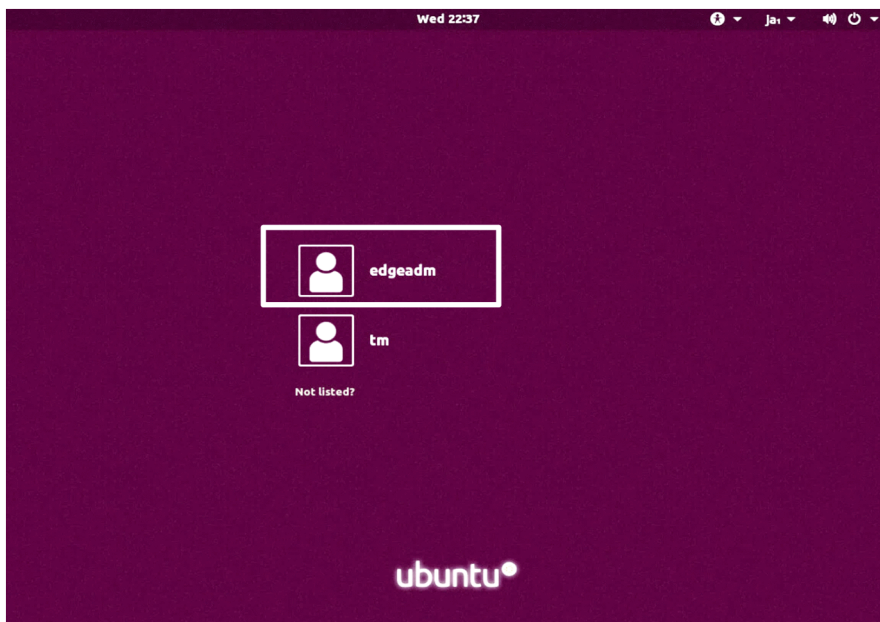
4. If the desired user is not displayed, click **Not listed?**.

   When the following screen appears, enter the user ID, and then click the **Next** button.
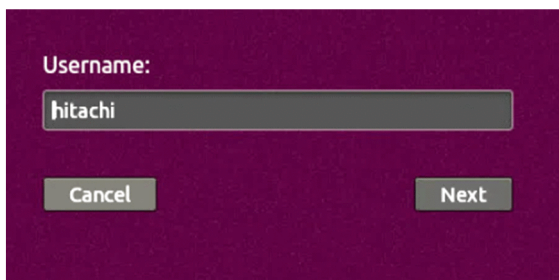
5. When the password entry screen appears, enter the password of the user who is logging in, and then click the **Sign In** button.
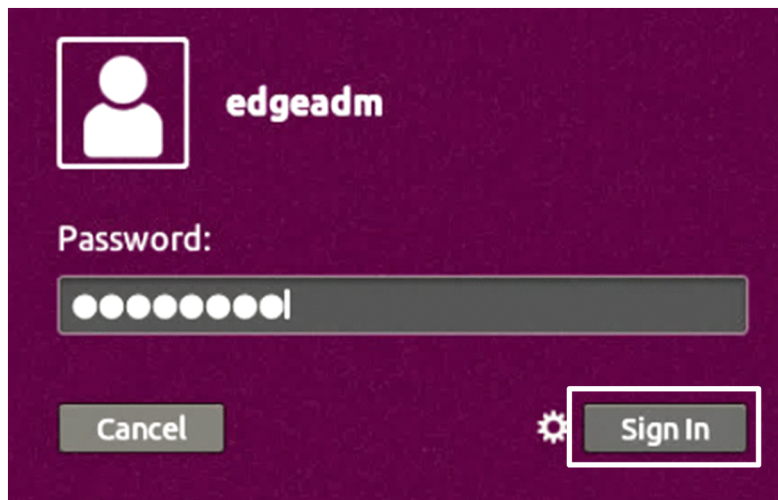
The desktop is now available.
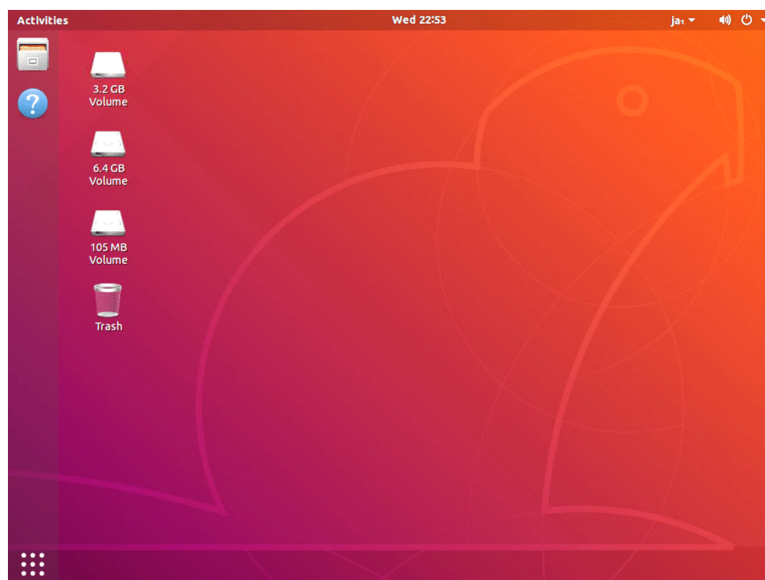
> ⚠ **Important note**
>
> In rare cases, desktop icons might overlap each other. In such cases, you can align the icons by right-clicking a desktop area where no icons exist, and then clicking **Organize Desktop by Name**.
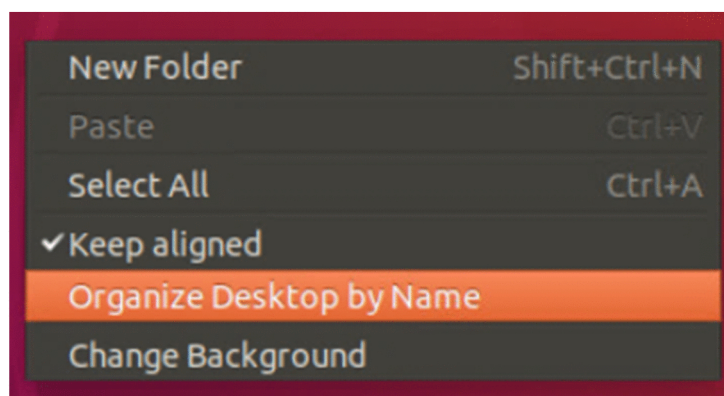
5.3.2 Stopping the desktop

You must restart the unit to stop the desktop. To do this:

1. Click the power icon in the upper right corner of the desktop. In the menu that appears, click the power icon.
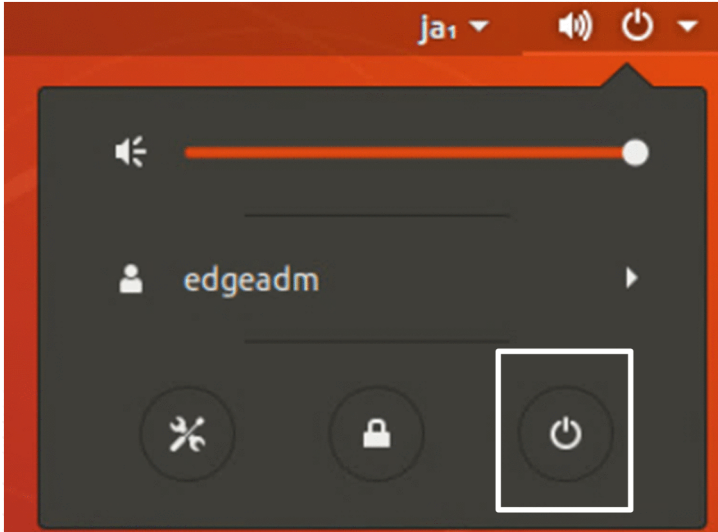
2. When the following dialog box appears, click **Restart**.
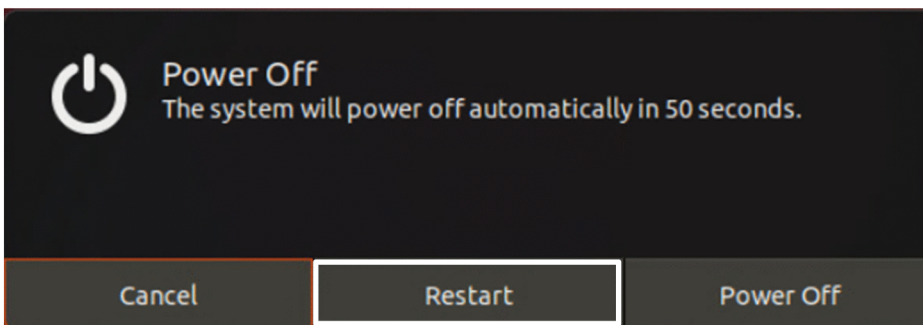
5.3.3 Hiding the desktop icons

To hide the desktop icons:

1. Click the nine-point dice icon in the lower left corner of the desktop.
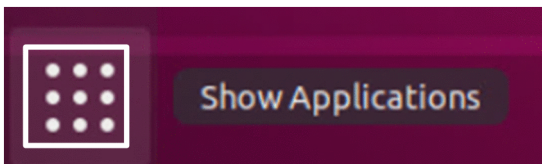
2. The application list appears. Click **Terminal**.
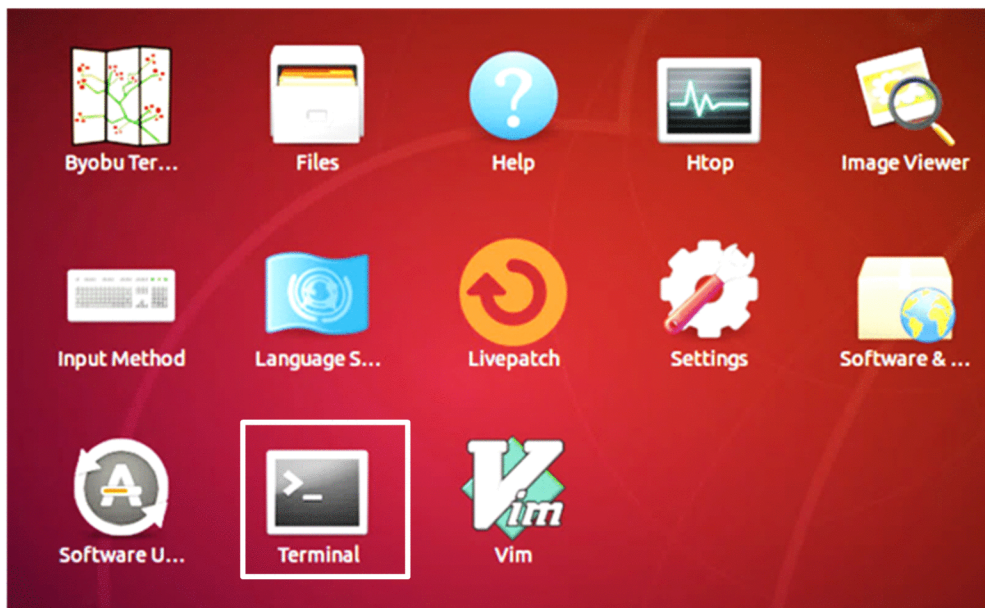
3. Enter the following command in the Terminal screen.

```
$ gsettings set org.gnome.desktop.background show-desktop-icons false
```
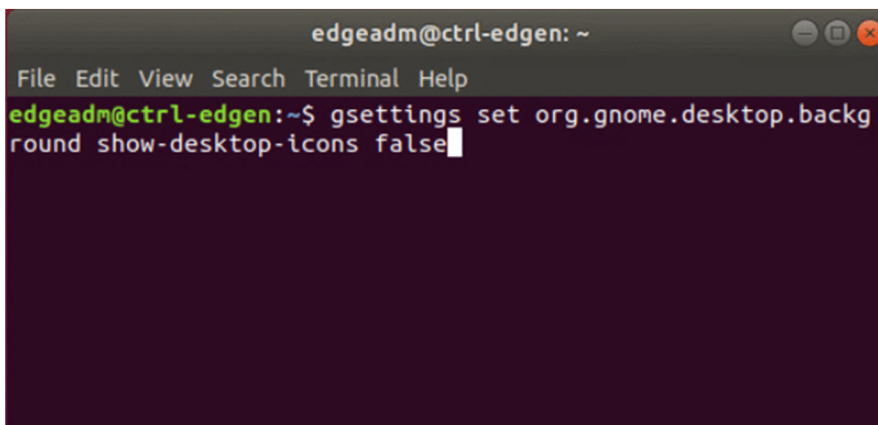

The icons are hidden in the desktop as shown below.
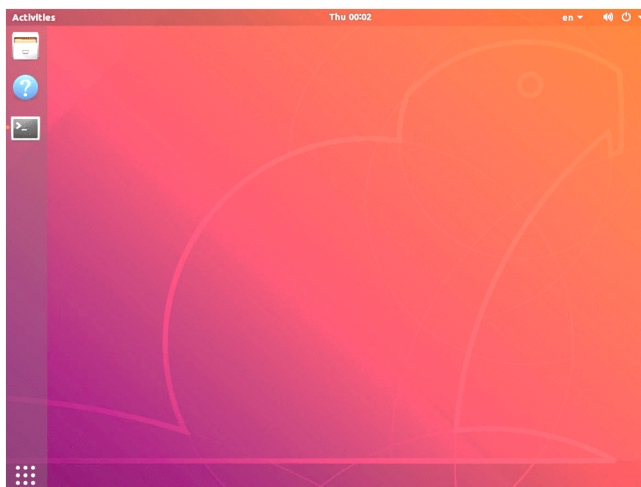
4. To re-display the icons on the desktop, run the following command on the Terminal screen.

```
$ gsettings set org.gnome.desktop.background show-desktop-icons true
```

5.4 Setting up the display

This section describes how to set the resolution for the display connected to the unit and how to set up dual displays. To set up the display, you need to start the desktop. For details about how to start the desktop, see 5.3.1 Starting the desktop.

5.4.1 Setting the display resolution

(1) Changing the resolution

To change the display resolution:

1. Click the power icon in the upper right corner of the screen.
   The system menu opens.

2. Click the Setting icon in the lower left corner of the system menu.
   The Setting screen opens.

3. Select **Devices**, and then **Displays**.
   The Displays screen appears.

4. Change the setting for **Resolution**.
   The **Apply** button appears in the upper right corner of the Displays screen.

   Figure 5–2: Displays screen
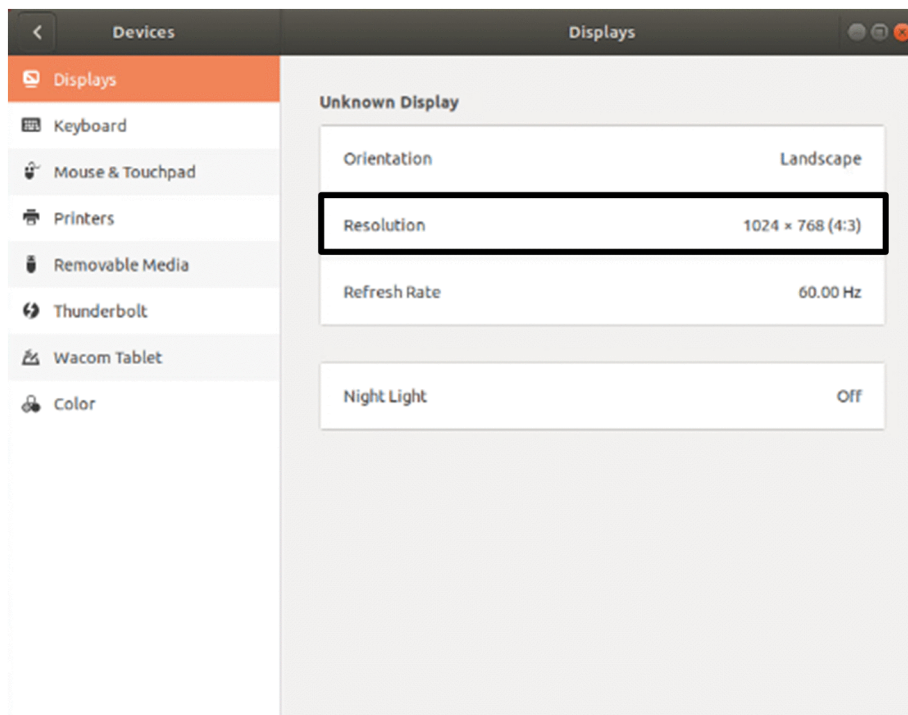
5. Click the **Apply** button in the upper right corner of the Displays screen.
   A popup screen appears.

Figure 5–3: Apply button in the Displays screen
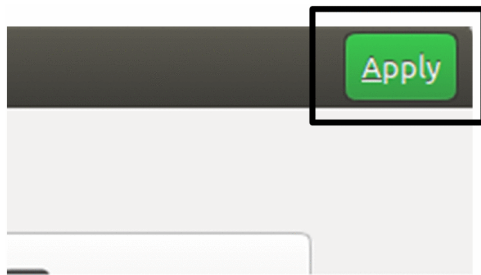
6. Click **Keep Changes** within 20 seconds.

The resolution is changed. If you do not click **Keep Changes** within 20 seconds, or if you click **Revert Settings**, the setting is not applied and the original setting is retained.

Note that any change made in the settings by clicking **Keep Changes** will be retained after the unit restarts.

Figure 5–4: Popup screen
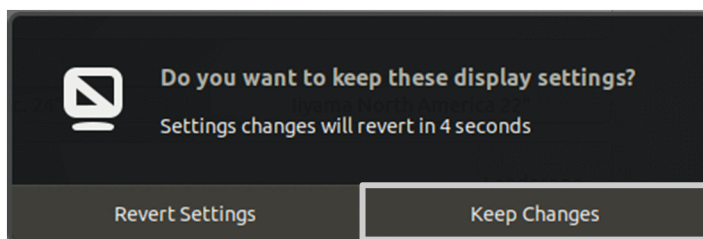
(2) Available resolutions

The following lists the display resolutions supported by the CE50-10. Display colors can be set in 24 bits (16,777,216 colors).

Table 5–2: Display resolution information

Resolution	Remarks
1,280 **x** 1,024 (SXGA)	Dual displays can be set.
1,920 **x** 1,080 (FHD)	Dual displays can be set.
1,920 **x** 1,200 (WUXGA)	Dual displays can be set.
3,840 **x** 2,160 (4K UHD)	Only a single display can be set.

5.4.2 Setting up dual displays

The CE50-10 has two ports for the DisplayPort interface. A dual display configuration can be created by connecting two displays to the unit. Dual displays support *Join Displays* (extended desktop) mode only.

(1) Changing the display mode from dual to single display

1. Click the power icon in the upper right corner of the screen.

The system menu opens.

2. Click the Setting icon.

The Setting screen opens.

3. Select **Devices**, and then **Displays**.

The Displays screen appears. This screen contains information about the currently connected displays, as shown below.

Figure 5–5: Current display mode (Join Displays)
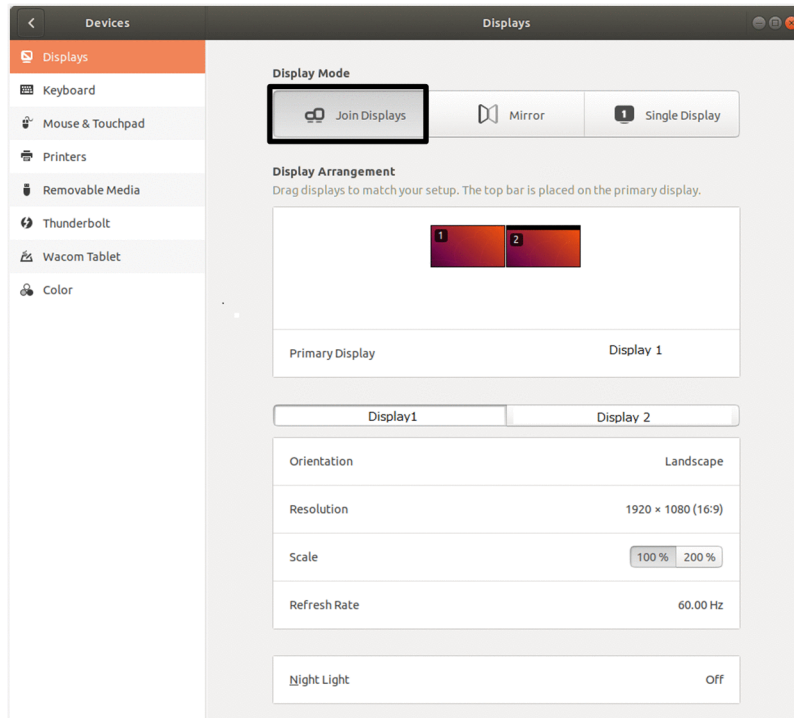
Note

In the product, the monitor model is displayed in place of **Display1** and **Display2**.

4. Select **Single Display**, and then select the display on which the screen is to be displayed.

Figure 5–6: Selecting Single Display
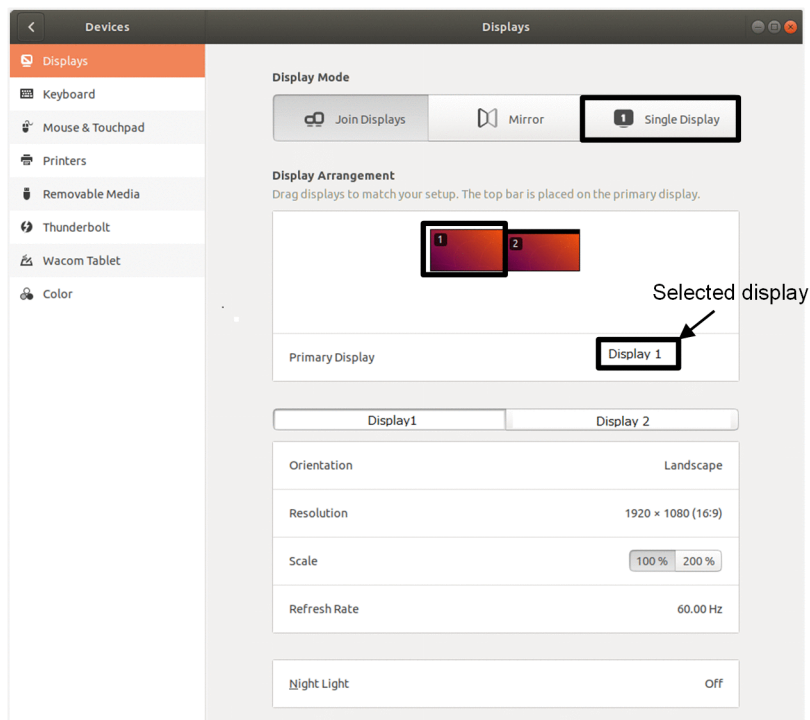
5. Click the **Apply** button in the upper right corner of the Displays screen.

A popup screen appears.

Figure 5–7: Apply button in the Displays screen
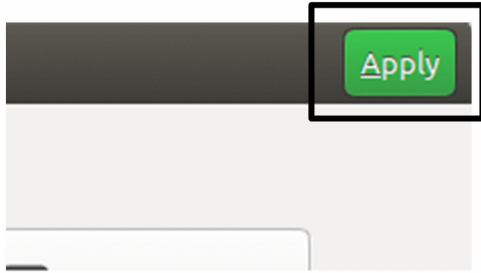
6. Click **Keep Changes** within 20 seconds.

The mode is changed to single display. If you do not click **Keep Changes** within 20 seconds or if you click **Revert Settings**, the change is not applied and the original setting is retained.

Note that any change made in the settings by clicking **Keep Changes** will be retained after the unit restarts.

Figure 5–8: Popup screen
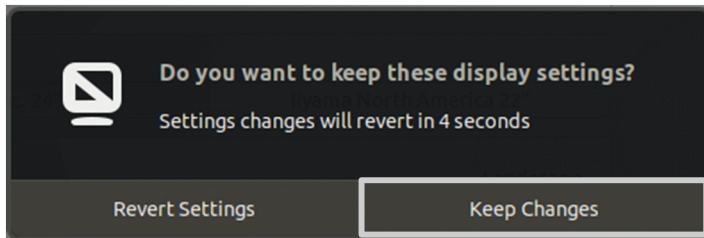
If you want to set the single display back to dual displays, select **Join Displays** in the Displays screen, click the **Apply** button, and then click **Keep Changes**.

5.5 Specifying IP address and IPv6 network

5.5.1 Configuring the network

(1) Network settings when the unit is provided

The following shows the default values of the IP address, network address, and communication mode for the LAN ports.

Network interface definition file: `/etc/netplan/50-cloud-init.yaml`

Table 5–3: Default values for LAN ports

Port (logical name)	IP address	Network address	Communication mode
LAN0 (`eth0`)	192.168.10.1	192.168.10.0	Auto negotiation
LAN1 (`eth1`)	192.168.11.1	192.168.11.0	Auto negotiation
LAN2 (`eth2`)	192.168.12.1	192.168.12.0	Auto negotiation

For example, when connecting to the LAN0 port of the unit that is to be set up, establish a connection to 192.168.10.1 from the development unit.

The following shows the contents of the network interface definition file.

```
network:
    version: 2
    renderer: networkd         -------- (A)
    ethernets:                 -------- (B)
        eth0:                  -------- (C)
            addresses:         -------- (D)
            - 192.168.10.1/24
        eth1:
            addresses:
            - 192.168.11.1/24
        eth2:
            addresses:
            - 192.168.12.1/24
```

(A)

Specify the service that runs at the back end.

(B)

Specify the type of LAN to be configured.

(C)

Specify the device name.

(D)

Specify the IP address and net mask.

(2) Changing IP addresses

To change the IP address or add an IPv6 address to the port:

1. Change the network interface definition file.

   The following shows an example.

```
ethX:
    addresses:
    - 192.168.1X.1/24                -------- (A)
    - 2001:db8::XXXX:YYYY/64         -------- (B)
```

(A)

To change the IP address or network class, change the value of the **<u>bold underlined part</u>**.

(B)

Add an IPv6 address. You can omit leading zeros in the string of numeric values separated by colons. To specify multiple IP addresses for one interface, add the IP address in the `addresses` key. Note that Netplan does not support interface aliases.

2. Apply the IP addresses.

Run the following command or restart the unit.

```
$ sudo ip_duplichk_start
```

⚠ CAUTION

For the LAN port IP address of the development unit, specify the same IP address as the network address of the LAN port connected to the unit that is to be set up.

Make sure that the IP address of the development unit differs from that of the unit that is to be set up. If these units have the same IP address, the following error message appears.

`KXDL010-W Ethernet adapter(`*interface-name*`) Duplicate IP address.`

5.5.2 IP multicast

Class D addresses in the range from 224.0.0.0 to 239.255.255.255 are available for IP multicast communication.

(1) Sending data by using IP multicast

To send data by using IP multicast, you must create communication sockets, and then specify the following settings by using a `setsockopt` system call.

1. Set the TTL (TimeToLive) value.

Specify the number of relays for multicast data for TTL. You can specify a value in the range from 0 to 255.

```
unsigned char  ipttl;

ipttl = 5;  /* Set the TTL value. */
setsockopt(sock, IPPROTO_IP, IP_MULTICAST_TTL, (char *)&ipttl, sizeof(ipttl));
```

2. Specify the IP multicast interface.

Before sending data by using IP multicast, specify the unit address.

```
unsigned int  ipmaddr;

ipmaddr = htonl(xxxxx);    /* Set the local unit address (binary format). */
setsockopt(sock, IPPROTO_IP, IP_MULTICAST_IF, (char *)&ipmaddr, sizeof(ipmaddr));
```

(2) Receiving data by using IP multicast

To receive data by using IP multicast, you must be a member of the IP multicast group. To join the IP multicast group, specify the addresses as follows by using the `setsockopt` system call.

```
struct ip_mreq  mreq;

memset((char *)&mreq, 0, sizeof(struct ip_mreq));
mreq.imr_multiaddr.s_addr = htonl(xxxxx); /* Specify the IP multicast address (binary
  format). */
mreq.imr_interface.s_addr = htonl(yyyyyy); /* Set the local unit address (binary forma
t). */
setsockopt(rcvsock, IPPROTO_IP, IP_ADD_MEMBERSHIP, (char *)&mreq, sizeof(mreq));
```

5.5.3 Using IPv6

IPv6 allows you to use the UDP and TCP communication functions.

(1) Overview of definition information files

The following shows the definition files that must be configured before you can use the IPv6 functions. For detailed contents, see the online manual in the development environment.

Table 5–4: List of IPv6 network definition information files

Definition information file name	Description
`50-cloud-init.yaml` (in `/etc/netplan`)	Network definition information file
`hostname` (in `/etc/hostname`)	Host name definition file

(2) Allocating IPv6 addresses

1. In the network definition information file, specify basic information for using IPv6 and the definition of IPv4.

```
network:
    version: 2
    renderer: networkd              --------  (A)
    ethernets:                      --------  (B)
        ethX:                       --------  (C)
            addresses:
            - 192.168.0.11/24       --------  (D)
            gateway4: 192.168.0.254 --------  (E)
            nameservers:            --------  (F)
                search: domain      --------  (G)
                addresses: 192.168.0.1 --------  (H)
        ethY:
            dhcp4: true             --------  (I)
```

(A)

Specify the service that runs at the back end.

(B)

Specify the type of LAN to be configured.

(C)

Specify the device name.

(D)

Specify the dot-separated IPv4 address and the netmask value. This definition is unnecessary if you do not use IPv4 or if you specify DHCP.

(E)

Specify the IP address of the default gateway (router). This setting is optional.

(F)

Specify the set item key for DNS information. (F, G, and H are optional.)

(G)

Specify the search domain. To specify multiple domains, enclose the domain names in square brackets ([ ]) and separate each name by a comma (,).

(H)

Specify the IP address of the DNS server. To specify multiple servers, enclose the server names in square brackets ([ ]) and separate each name by a comma (,).

(I)

Specify whether to enable DHCP. This definition is unnecessary if you specify a fixed IP.

`true`: Enabled, `false`: Disabled

2. (Optional) Specify the definition information for using the IPv6 address automatic allocation function.

To automatically allocate IPv6 addresses, specify the following definition information (in addition to basic information) in the setting fields for the device to be specified.

```
        dhcp6: true                 --------   (J)
        accept-ra: true             --------   (K)
```

(J)

Specify whether to enable DHCP. Specify `true`.

`true`: Enabled, `false`: Disabled

(K)

Specify whether to enable RA. Specify `true`.

`true`: Enabled, `false`: Disabled

3. (Optional) Specify the definition information for using the IPv6 address manual allocation function.

To manually allocate IPv6 addresses, specify the following definition information (in addition to basic information) in the setting fields for the device to be specified.

```
 addresses:
 - 2001:db8:1:1:20a:f7ff:fe15:d92b/64     --------   (L)
 gateway6: 2001:db8:1:1:21b:8bff:fe79:2e4 --------   (M)
```

(L)

Specify the IPv6 address to be individually assigned by using $aaaa:bbbb:cccc:dddd:eeee:ffff:1111:2222$ format. You can omit leading zeros in the string of numeric values separated by colons.

(M)

Specify the IPv6 default gateway (router) address in $aaaa:bbbb:cccc:dddd:eeee:ffff:1111:2222$ format. You can omit the setting if you do not use the gateway.

Specify manual allocation of IPv6 addresses if you want to generate a user-specific local address (unique local address) other than the link local address or global address used for communication beyond routers.

4. Apply the IP addresses.

Run the following command or restart the unit.

```
 $ sudo ip_duplichk_start
```

5.6 Configuring a tagged VLAN

You can configure tagged VLANs for NIC (Network Interface Card) of this unit. A maximum of 4,094 tagged VLANs can be configured for one NIC. Specify tagged VLAN IDs in the range from 1 to 4094.

5.6.1 Configuring the network definition file

To use the tagged VLAN function, add definition information to the network definition file. To define an interface by using the tagged VLAN, assign each segment a unique number called *VLAN ID*. For details, see the online manual in the development environment.

1. Edit the network definition file.

   Network definition file: `/etc/netplan/50-cloud-init.yaml`

   ```
   network:
       version: 2
       renderer: networkd
       ethernets:
           ethX:
               addresses:
               - 192.168.10.1/24
       vlans:
           ethX.128:                  --- (A)
               id: 128                --- (A)
               link: ethX             --- (A)
               addresses:
               - 192.168.128.1/24   --- (B)
   ```

   (A)

       For the ethX interface, define the tagged VLAN interface with ID 128.

   (B)

       Specify the IP address 192.168.128.1 for the tagged VLAN interface 128 (`ethX.128`).

2. Apply the IP addresses.

   Run the following command or restart the unit.

   ```
   $ sudo ip_duplichk_start
   ```

5.6.2 Starting or stopping the tagged VLAN

You can use the `ip` command to display the status of the tagged VLAN and start or stop the tagged VLAN.

(1) Displaying the status of the tagged VLAN

The following example shows how to run the command to display the status of the running tagged VLAN.

```
$ ip addr show  ethX.128
1: ethX.128@ethX:  BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
state UP group default qlen 1000
    link/ether 00:50:56:bf:45:1c brd ff:ff:ff:ff:ff:ff
    inet 192.168.128.1/24 brd 192.168.128.255 scope global ens160.128
       valid_lft forever preferred_lft forever
```

(2) Stopping the tagged VLAN

The following example shows how to run the command to stop the tagged VLAN.

```
$ sudo ip link set ethX.128 down
```

(3) Starting the tagged VLAN

The following example shows how to run the command to restart the stopped tagged VLAN.

```
$ sudo ip link set ethX.128 up
```

5.7 Configuring NIC bonding

Bonding of multiple NICs into a virtual NIC can increase availability of network communication and provide load distribution and redundancy. The CE50-10 supports bonding by using the standard function of Linux. This section describes how to configure bonding. For details, see the online manual.

5.7.1 Configuring the network definition file

To use the bonding function, add definition information to the network definition file.

1. Edit the network definition file.

   Network definition file: `/etc/netplan/50-cloud-init.yaml`

   ```
   network:
       version: 2
       renderer: networkd
       ethernets:
           ethX:
               addresses:
               - 192.168.10.X/24
           ethY:
               addresses:
               - 192.168.10.Y/24
       bonds:
           eth-bonds:
               interfaces: [ethX, ethY] --- (A)
               addresses:              --- (A)
               - 192.168.10.Z/24       --- (A)
               parameters:
                 mode: balance-rr      --- (B)
   ```

   (A)

       Define the virtual interface `eth-bond`, and then bond `ethX` and `ethY`, which are specified as slave interfaces.

   (B)

       Set the bonding operation mode.

2. Apply the IP addresses.

   Run the following command or restart the unit.

   ```
   $ sudo ip_duplichk_start
   ```

5.7.2 Bonding operation modes

Bonding has seven operation modes. Select the mode appropriate for your purpose. By default, `balance-rr` is selected. The following table lists the operation modes.

Table 5–5: Bonding operation modes

Operation mode	Description
balance-rr	Packets are sent by using all slave interfaces in turn (round-robin).
active-backup	Packets are sent by using only one slave interface as the active interface.
balance-xor	Packets are sent by using the send slave interface determined based on the MAC addresses of the sender and destination.
Broadcast	The same packet is sent from all slave interfaces.
802.3ad	Link aggregation conforming to IEEE 802.3ad (LACP) is performed.
balance-tlb	Packets are sent by using the send slave interface determined according to the loads on the slave interfaces.

Operation mode	Description
`balance-alb`	Load distribution is also applied to packet reception in addition to the function of `balance-tlb`.

5.8 Setting the time function

5.8.1 Setting the NTP client function

The unit supports the NTP client function. If the NTP server is running in the network environment connected to the unit, you can update the unit time based on the time distributed by the NTP server. Use the `systemd-timesyncd` service to synchronize the unit time with the time of the NTP server. When setting up `systemd-timesyncd`, you must first modify the definition file, and then set up the service.

The NTP client function is disabled by default. To enable this function, perform the following.

1. Modify the definition file.

   Definition file name: `/etc/systemd/timesyncd.conf`

   In the `timesyncd.conf` file, specify the NTP server to be referenced by the `systemd-timesyncd` service. The `timesyncd.conf` definition file does not contain any settings by default. Edit the file to specify required definitions, if any.

   ```
   [Time]
   #NTP=150.0.0.10                                          --- (A)
   #FallbackNTP=ntp.ubuntu.com                              --- (B)
   #RootDistanceMaxSec=5                                    --- (C)
   #PollIntervalMinSec=32                                   --- (D)
   #PollIntervalMaxSec=2048                                 --- (E)
   ```

   (A)

       Specify the host name or IP address of the NTP server that the `systemd-timesyncd` service will reference.

   (B)

       Specify the host name or IP address of the NTP server that is referenced if an attempt to synchronize with (A) fails.

   (C)

       Specify the maximum permitted communication delay time (communication between the NTP server and NTP client).

   (D)

       Specify at least 16 seconds as the minimum polling interval for NTP messages.

   (E)

       Specify the maximum polling interval for NTP messages. Specify a value greater than the value specified in (D).

2. If a firewall is enabled, permit transmission to port 123 with the UDP protocol.

   For details about how to set this up, see (3) Setting firewall rules.

   This setting is unnecessary if the firewall has been disabled as described in (2) Enabling or disabling the firewall.

3. Enable the service.

   Run the following command to enable the `systemd-timesyncd` service.

   ```
   $ sudo timedatectl set-ntp true
   ```

5.8.2 Setting the time zone for the OS time

The OS time of the CE50-10 is set to UTC (Coordinated Universal Time) at the time of product shipment.

If you want to display the OS time in your preferred local time zone, specify the following settings.

1. Obtains the time zone list.

   Run the following command to obtain a list of time zones that can be set.

   ```
   $ sudo timedatectl list-timezones
   ```

2. Set the time zone.
   Run the following command to set the time zone.

```
$ sudo timedatectl set-timezone TIMEZONE#
```

\#

Any time zone in the list

> ! Important note
>
> Even if you change the time zone, the RTC time displayed in the BIOS menu remains in UTC. If you change the time by using `timedatectl`, the time converted to UTC is written to RTC.

5.9 Changing the operation to be performed in the case of a disk fault

If a disk fault occurs during the operation of the unit or if a slowdown in the disk access time is detected, a kernel panic occurs by default. If you want to change this setting so that operation of the unit continues after a disk fault or a slowdown detection, you need to change the definition file settings.

Definition files

- Definition file for disk faults: `/hitachi/etc/dskptrl_stop.conf`
- Definition file for slowdown detection: `/hitachi/etc/slowdown_stop.conf`

Item specified in a definition file

```
stop definition-value --- (A)
```

(A)

Specify `0` or `1`. The default is `0`. To change the operation, change the setting to `1`.

Table 5–6: Definition values of the stop item

Definition value	Description
0	A kernel panic (default setting) occurs.
1	Unit operation continues.

5.10 Developing application programs

Application programming is performed by using this product. In addition to Linux standard development software, CE50-10 has an SDK to which various libraries for using unique functions are added.

5.10.1 Development environment hardware configurations

(1) Hardware configuration No. 1

A personal computer (PC) is connected to the unit as a human-machine interface device.

Table 5–7: Device connected to the unit in configuration No. 1

Device	Connection interface	Description
Personal computer (PC)	Ethernet	This device is used for the operation of data backup, data restore, and program update functions. Connect the PC to the development unit by using an Ethernet crossover cable.

Figure 5–9: Configuration for connecting the PC
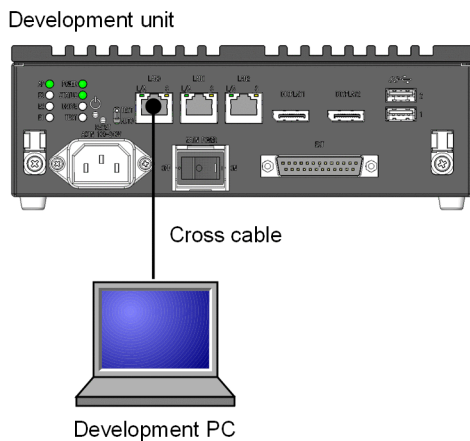
(2) Hardware configuration No. 2

A display, a keyboard, and a USB flash drive are connected to the unit as an HMI.

Table 5–8: Devices connected to the unit in configuration No. 2

Device	Connection interface	Description
Keyboard	USB	This device is used for the operation of data backup, data restore, and program update functions.
Display	DisplayPort	Console screen
USB flash drive	USB	External media that stores backup data

Figure 5–10: Configuration for connecting the keyboard, display, and USB flash drive to the unit
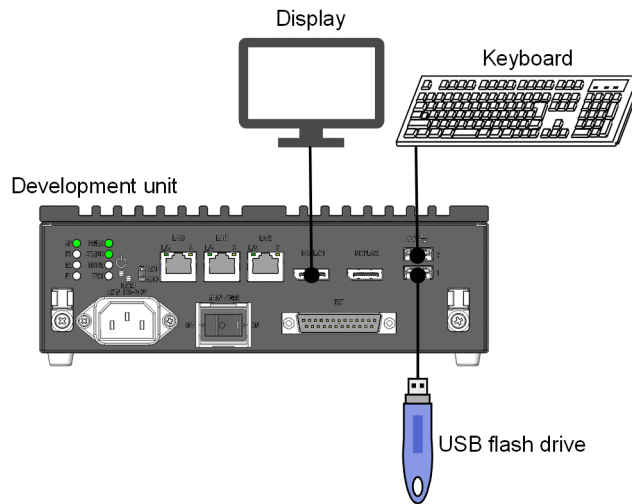
5.10.2 Supported functions

Table 5–9: Supported functions below shows the functions supported by the development environment. For information on how to use the commands shown in the *Details* columns, see the online manual.

Table 5–9: Supported functions

No.	Function	Details
1	Creating and compiling application programs	• Object creation by using the `gcc` command is supported. • Editing files by using the `vi` command is supported.
2	Extended RAS function	• Forced CPU restart function • USB port connection/disconnection function
3	Extended I/O device operation	I/O board I/O device operation
4	File transfer	The `scp` command is supported for file transfer.
5	Remote operation	The `ssh` command is supported for remote operations.

5.10.3 Provided files

Table 5–10: Files for application development by using the unique functions of CE50-10 below shows the files provided for using the unique functions of CE50-10.

Table 5–10: Files for application development by using the unique functions of CE50-10

No.	Application	File name	Description
1	Development of extended RAS function programs (forced CPU restart and USB port connection and disconnection)	`/hitachi/lib64/libras.so`	Library for extended RAS function programs
2		`/hitachi/usr/include/rasif.h`	Include file for extended RAS function programs
3	Development of extended I/O device operation programs	`/hitachi/lib64/libecextio.so`	Library for I/O board I/O devices

No.	Application	File name	Description
4	Development of extended I/O device operation programs	`/hitachi/usr/include/ecextioctl.h`	Include file for I/O board I/O devices
5	Path definition for additional libraries	`/etc/ld.so.conf.d/ctrl_edge_dev.conf`	Development environment definition file

5.10.4 Note about SSD life

The SSD installed in this unit is specified to operate for 10 years or more, based on a daily amount of write data of 50 GB or less.

Therefore, we recommend that you design the application so that the sum of the daily amount of data written by the application and the log data written by the system (50 MB/day) is no more than 50 GB.

5.11 Registering application programs

5.11.1 Environment for registering application programs

Figure 5–11: Environment for constructing applications below shows the environment used to construct assumed applications.

A single CE50-10 can be used as the development unit and as the construction unit .

In this case, there is no need to transfer the master file of the application program.

Figure 5–11: Environment for constructing applications
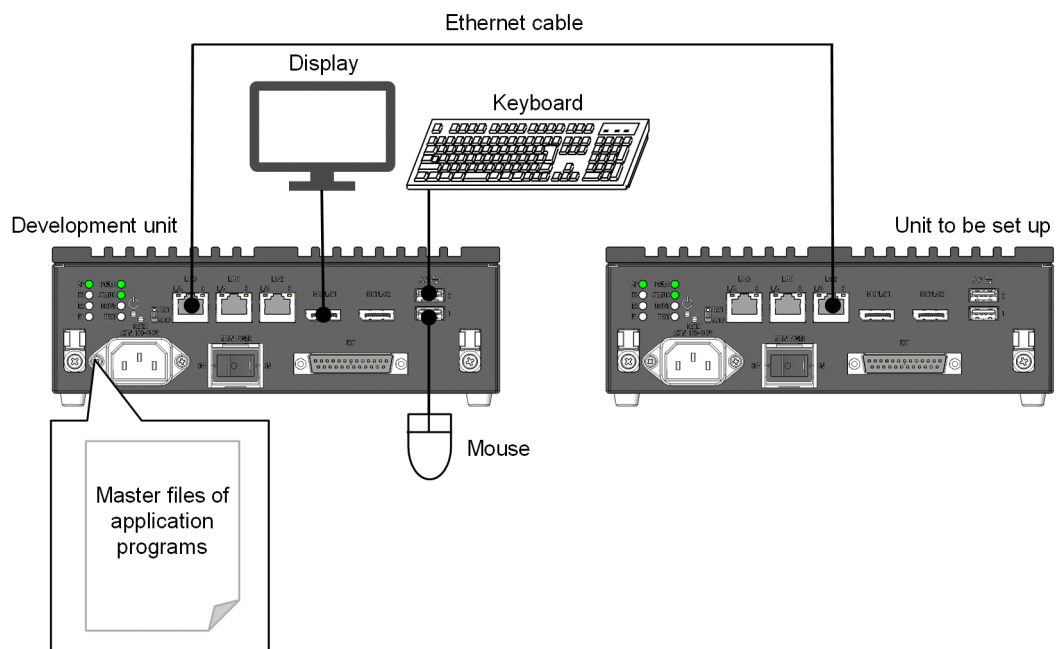
5.11.2 Application program registration procedure

Figure 5–12: Application installation procedure below shows the procedure for installing an application.

Figure 5–12: Application installation procedure

```
                    ▽
    ┌──────────────────────────┐      ┌ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┐
    │ (1) Setting up the user   │         Set up the user area in the setup target unit.
    │      area                 │─ ─ ─ 
    │      (See 5.11.3(1).)     │      └ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘
    └──────────────────────────┘

    ┌──────────────────────────┐      ┌ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┐
    │ (2) Installing the        │      │ Install the application program in the setup target unit by transferring
    │      application          │─ ─ ─   the application master file from the development unit.
    │      program              │      └ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘
    └──────────────────────────┘

    ┌──────────────────────────┐      ┌ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┐
    │ (3) Edit the setup file   │─ ─ ─   Modify OSS startup settings and ad-on function settings.
    └──────────────────────────┘      └ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘

                    △
```
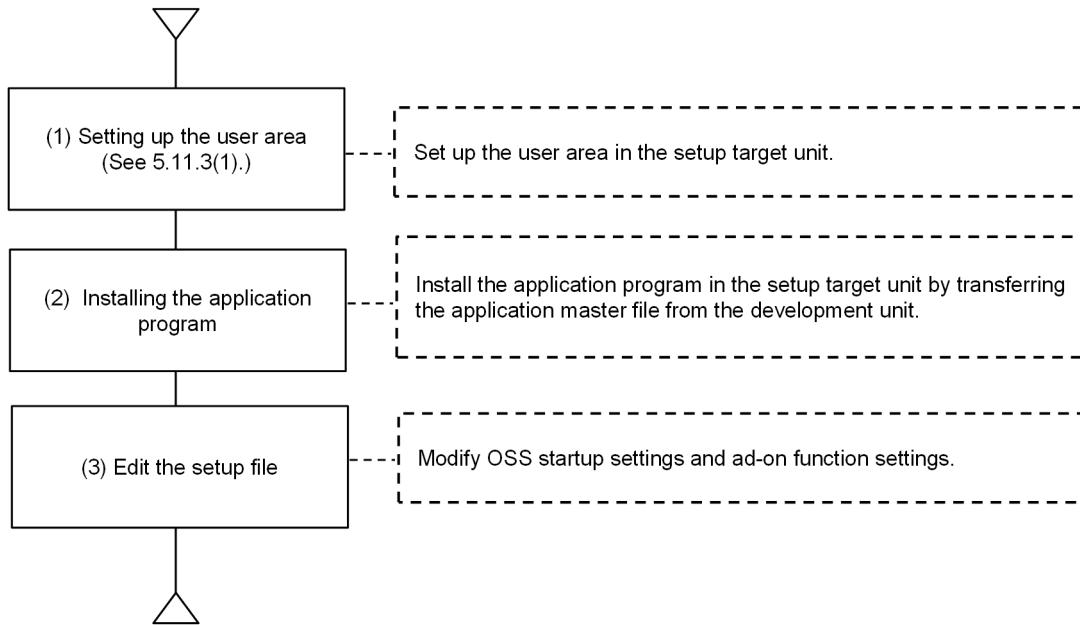
5.11.3 Setting up the user area

(1) Procedure for setting up the user area

In the SSD user area, create a desired partition and then mount it for use.

Figure 5–13: Overview of the user area setting procedure below shows the procedure for specifying settings to automatically mount the user area when the OS starts.

Figure 5–13: Overview of the user area setting procedure

```
                    ▽
    ┌──────────────────────────┐
    │ (a) Divide the user area. │
    └──────────────────────────┘

    ┌──────────────────────────┐
    │ (b) Create a file system. │
    └──────────────────────────┘

    ┌──────────────────────────┐
    │ (c) Change the operation  │
    │     parameter for file    │
    │     system check.         │
    └──────────────────────────┘

    ┌──────────────────────────┐
    │ (d) Specify user area     │
    │     mount settings.       │
    └──────────────────────────┘

                    △
```
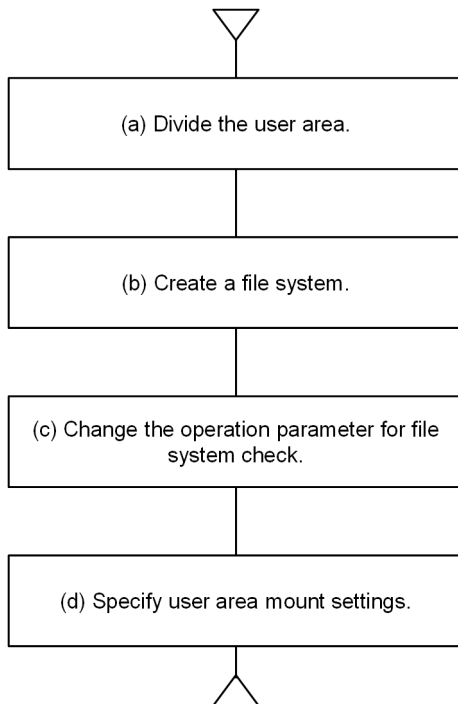
(a) Dividing the user area

Use the `gdisk` command to divide the user area (create partitions). For details about the procedure, see (2) Creating partitions, (3) Displaying partitions, and (4) Deleting partitions in 5.11.3 Setting up the user area.

(b) Creating a file system

Create a file system by using the `mkfs` command.

<Format>

```
mkfs -t ext4 device
```

<Options>

- `-t ext4`

  Specifies the file system type.

- *device*

  Specify the device name of the partition in which the file system is to be created.

<Display example>

The device name of the partition is `/dev/sda8` and the partition is formatted with ext4.

```
$ sudo mkfs -t ext4 /dev/sda8
```

(c) Changing the operation parameter for file system check

Even if the file system is not damaged, file system check is forcibly performed when a predefined period has passed since the last check date and time. Considering the influence of the check operation on the OS start time, disable the file system check that is triggered by the elapsed time in this unit.

<Format>

```
tune2fs -c 0 -i 0 device
```

<Options>

- `-c 0`

  Specifies the number of times the file system is to be checked. Specify `0` to disable the check.

- `-i 0`

  Specifies the interval for checking the file system. Specify `0` to disable the check.

- *device*

  Specify the device name of the partition in which the file system is to be created.

<Display example>

```
$ sudo tune2fs -c 0 -i 0 device
```

(d) Specifying user area mount settings

If you want to automatically mount the user area when the OS starts, use the application area mount function. For details, see (5) Specifying the definition to automatically mount the application area in 5.11.3 Setting up the user area.

(2) Creating partitions

To create partitions:

1. Start the `gdisk` command with `/dev/sda` specified for the argument.

```
$ sudo gdisk /dev/sda
GPT fdisk (gdisk) version 1.0.3

Partition table scan:
  MBR: not present
  BSD: not present
  APM: not present
```

```
   GPT: not present

Creating new GPT entries.

Command (? for help):
```

2. Enter `n` to run the command that creates a new partition.

```
Command (? for help):n
```

3. Enter the partition number you want to create.

If you press the **Enter** key without entering anything, the smallest unused number is allocated. The following example indicates that the ninth partition is created.

```
Partition number (1-128, default 9):9
```

4. Enter the start sector.

The start sector must be aligned at the 2048-sector boundary. If you specify a value less than 2048, the start sector is set to 2048. If you specify 2048 or greater, the start sector is automatically adjusted so that partitions are aligned at 2048 boundaries. You can specify the size rather than the sector. To do this, use +*xx* as the number of sectors from sector 2048, use −*xx* as the number of sectors from the end, and add K (kilobytes), M (megabytes), G (gigabytes), T (terabytes) or P (petabytes) at the end of the numeric value. If you press the **Enter** key without entering anything, the sector indicated by `default` = *xxxx* is allocated. In the following example, the default of sector 2048 is selected.

```
First sector (34-15728606, default = 2048) or {+-}size{KMGTP}:
```

5. Enter the end sector.

You can specify the size rather than the sector. To do this, use +*xx* as the number of sectors from the first sector, use −*xx* as the number of sectors from the end. If you press the **Enter** key without entering anything, the sector indicated by `default` = *xxxx* is allocated. In the following example, the default is selected.

```
Last sector (2048-15728606, default = 15728606) or {+-}size{KMGTP}:
```

6. Enter the partition type.

Entering L displays a list of partition types.

For the Linux file system, enter 8300. If you press the **Enter** key without entering anything, the default of 8300 is set. In the following example, the default of 8300 is selected.

```
Current type is 'Linux filesystem'
Hex code or GUID (L to show codes, Enter = 8300):
```

7. Repeat steps 2 to 6 for the partitions to be created.

8. Enter `w` to write the settings to the disk.

```
Command (? for help):w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!
```

When a confirmation message appears, enter Y to write the settings. If you enter N, the display returns to the state prior to step 8 without writing the settings.

```
Do you want to proceed? (Y/N):Y
```

9. When writing to the disk is complete, the following message appears and then the command ends:

```
OK; writing new GUID partition table (GPT) to /dev/sda.
The operation has completed successfully.
```

10. Run the `partprobe` command to report the change of partitions to the OS.

You do not have to restart the OS because this command makes the OS recognize the partitions.

```
$ sudo partprobe
```

(3) Displaying partitions

The following describes the procedure for displaying partitions.

Two methods are available. The following describes the procedure for each method.

(a) Display method 1

1. Start the `gdisk` command with `/dev/sda` specified for the argument.

```
$ sudo gdisk /dev/sda
GPT fdisk (gdisk) version 1.0.3

Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present

Found valid GPT with protective MBR; using GPT.
Command (? for help):
```

2. Enter `p` to run the command that displays partitions.

```
Command (? for help):p
Disk /dev/sda: 15728640 sectors, 7.5 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): 6A423A3C-EFD1-448C-AA4F-70DB2D2D757B
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 15728606
Partitions will be aligned on 2048-sector boundaries
Total free space is 2014 sectors (1007.0 KiB)
Number  Start (sector)    End (sector)  Size        Code  Name
   1          2048         15728606   7.5 GiB     8300   Linux filesystem
```

Note

The underlined part is partition information.

3. Enter `q` to terminate processing.

```
Command (? for help):q
```

(b) Display method 2

1. Start the `gdisk` command with `-l` option and with `/dev/sda` specified for the argument.

The `gdisk` command prompt does not appear, the partitions are displayed, and the command terminates.

```
$ sudo gdisk /dev/sda -l
Disk /dev/sda: 15728640 sectors, 7.5 GiB
Logical sector size: 512 bytes
Disk identifier (GUID): 6A423A3C-EFD1-448C-AA4F-70DB2D2D757B
Partition table holds up to 128 entries
First usable sector is 34, last usable sector is 15728606
Partitions will be aligned on 2048-sector boundaries
Total free space is 2014 sectors (1007.0 KiB)

Number  Start (sector)    End (sector)  Size        Code  Name
   1          2048         15728606   7.5 GiB     8300   Linux filesystem
```

Note

The underlined part is partition information.

(4) Deleting partitions

To delete partitions:

1. Start the `gdisk` command with `/dev/sda` specified for the argument.

```
$ sudo gdisk /dev/sda
GPT fdisk (gdisk) version 0.8.5

Partition table scan:
```

```
   MBR: protective
   BSD: not present
   APM: not present
   GPT: present

   Found valid GPT with protective MBR; using GPT.
   Command (? for help):
```

2. Enter `d` to run the command that deletes partitions.

```
   Command (? for help):d
```

3. Enter the partition number you want to delete. The following example shows how to select the ninth partition.

```
   Partition number (1-127):9
```

4. Enter `w` to run the command that writes the settings to the disk.

```
   Command (? for help):w

   Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
   PARTITIONS!!
```

When a confirmation message appears, enter `Y` to apply the settings. If you enter `N`, the display returns to the status in step 4 and the settings are not applied.

```
   Do you want to proceed? (Y/N):Y
```

5. When application to the disk is complete, the following message appears, and then the command ends:

```
   OK; writing new GUID partition table (GPT) to /dev/sda.
   The operation has completed successfully.
```

6. Run the `partprobe` command to report the change of partitions to the OS.

You do not have to restart the OS because this command makes the OS recognize the partitions.

```
   $ sudo partprobe
```

(5) Specifying the definition to automatically mount the application area

To automatically mount the user area when starting the unit, you need to add a definition in the mount definition file (`/hitachi/etc/fsconf`). By specifying the file definition items, you can automatically reconfigure the file system (by using `mkfs`) if an attempt to repair the file system fails or automatically mount the file system if its status is normal.

(a) Definition format

When user area generation is complete, the mount definition file contains no definitions. Therefore, add lines containing definitions as needed. To add a definition item to the mount definition file, enter data in the following format. A line that begins with a hash mark (#) is ignored during processing.

- Specification format of the mount definition file

```
   <device> _ <mount> _ <type> _ <mode> _ <initial> _ <fsckcnt>
```

Item enclosed in < >: Definition content

_: At least one space or tab

(b) Items to be added

To add a definition, you must specify all definition items. If any one of the definition items in a line of the definition file is missing, the definition file will be ignored during processing.

Table 5–11: Definition items in the mount definition file

Definition item	Description
<device>	Specify the name of the device (example: /dev/sda9) on which the file system is to be mounted.

Definition item	Description
`<mount>`	Specify the full path name of the mount destination directory. The specified directory is automatically created by the OS.
`<type>`	Specify the file system type. The applicable file system is EXT4 only.
`<mode>`	Specify either of the following as the write mode to be used when the file system is mounted: • `rw`: Read and write are possible. • `ro`: Read only (write prohibited)
`<initial>`	Specify whether to automatically reformat the file system if an attempt to repair the file system fails. To enable reformatting, you need to specify `1` or greater for the `fsckcnt` option. • `0`: Reformat. • `1`: Do not reformat.
`<fsckcnt>`	Specify how many times a file system check is to be performed, as a number in the range from `0` to `3`. Specify `0` if you do not want to have the file system checked.

(c) Applying the definition to the unit

After editing the definition file by a user, enable it by restarting the unit.

(d) Definition example

```
#<device>    <mount>       <type>   <mode> <initial> <fsckcnt>
/dev/sda11   /app/prog     ext4     ro     0         0
/dev/sda12   /app/log      ext4     rw     1         2
/dev/sda10   /app/contents ext4     rw     1         0
```

(e) Checking the definition file

After editing the definition file, run the `fsconfchk` command to check the contents. For details about the command, see 5.18.9 fsconfchk.

```
$ sudo fsconfchk
```

(f) Note

If the file system is not constructed yet, specifying a value from `1` to `3` for `fsckcnt` and `1` for `initial` causes the file system to be reformatted with the specified type. If `0` is specified for `initial` or `fsckcnt`, the file system is not reformatted and an attempt to mount the device fails.

5.11.4 Setting start and stop of application programs

(1) Creating a script file

To use `systemd` to start and stop application programs, you need to create a configuration file (`systemd` script file) and store it in the specified directory (`/lib/systemd/system/`). When the file is stored, an application program is registered as one of the services of the OS.

The following describes how to specify the `systemd` script.

Enter the following information in a file named *application-program-name*.`service` under the `/lib/systemd/system/` directory.

```
[Unit]
Description=<description>
Requires=<prerequisite-service>
After=fsmount.service<start-timing>
```

```
[Service]
ExecStart=<start-command>
ExecStop=<stop-command>
Type=<startup-check>
RemainAfterExit=<yes|no>

[Install]
WantedBy=<start-target>(edge-normal.target)
```

Table 5–12: Settings of the systemd script

Item	Description
description	Enter the description of the service.
prerequisite-service	Specify the service (*required-service*) to be started if it is not running when the application starts. If automatic startup of the application is enabled, the prerequisite service starts even if automatic startup of the prerequisite service is disabled. If the attempt to start the prerequisite service fails, startup of the application is canceled.
start-timing	If automatic startup is enabled, specify the service after which the application program is to be started.
	If, for example, there is a service (such as a database) which the application depends on, you can specify the order of starting the service. You must specify `fsmount.service`, which is the service for mounting the user area.
start-command	Specify the command that runs when the application program starts.
stop-command	Specify the command that runs when the application program stops.
	When you delete this line, the `kill` command stops all processes generated by the start command.
startup-check	Specify how to determine whether the application program has started.
	You can specify `oneshot`, `simple`, or `forking`. Their meanings are as follows:
	• `oneshot`: When the start command is run, the application is determined to have started. If `RemainAfterExit` is set to `no`, the application is determined to have terminated immediately. If `RemainAfterExit` is set to `yes`, the application is determined to be running irrespective of the application status. • `simple`: When the start command starts running, the application is determined to have started. A process of the start command is recognized as an application and monitored. • `forking`: When the start command terminates normally, the application is determined to have started. A child process of the start command is recognized as an application and monitored.
	When the OS shuts down, if the application program is recognized as running, run the stop command.
start-target	If automatic startup is enabled, specify the target on which the application program is to be started.
	Specify `edge-normal.target`.

(2) Enabling or disabling automatic startup

Run the following command to enable automatic startup of the application program.

```
$ sudo systemctl enable application-name
```

Run the following command to disable automatic startup of the application program.

```
$ sudo systemctl disable application-name
```

Run the following command to check whether automatic startup is enabled.

```
$ sudo systemctl is-enabled application-name
```

If automatic startup is enabled, `enabled` is displayed. If automatic startup is disabled, `disabled` is displayed.

5.12 Setting the security functions

You can use the following functions to safely operate the unit.

Table 5–13: Security functions

Function name	Description
Login policy	This function prevents unauthorized logins.
Password policy	This function defines the length, complexity, and update period of passwords.
Firewall	This function closes unused ports and blocks invalid packets.

5.12.1 Setting login policies

You can specify the following settings for users who log in to the unit:

- Root account login
- Account lock for a failed login
- Login timeout

(1) Setting root account login

This function permits (enables) or rejects (disables) login with the root account. This function is disabled by default.

(a) Enabling root login

1. Set a password for the root account.

   Use the `passwd` command to set the password.

   ```
   $ sudo passwd
   New password: <- Enter the password (the entered character string is not displayed)
   .
   Retype new password: <- Enter the password again (the entered character string is n
   ot displayed).
   passwd: password updated successfully
   ```

2. Enable login with the root account.

   The following example shows how to run the command.

   ```
   $ sudo passwd -u root
   passwd: password expiry information changed.
   ```

3. (Optional) To enable root login via ssh, edit the SSH configuration file.

   ```
   $ sudo vi /etc/ssh/sshd_config
   ```

4. (Optional) In the `sshd_config` file, change the setting of the `PermitRootLogin` option from `no` to `yes`.

   ```
   PermitRootLogin  no->yes
   ```

5. (Optional) After editing the SSH configuration file, you can enable the settings by running the following command.

   ```
   $ sudo systemctl restart ssh
   ```

(b) Disabling root login

Change the login with the root account from enabled to disabled.

The following shows an example of running the command.

```
$ sudo passwd -l root
passwd: password expiry information changed.
```

(2) Setting account lock for a failed login

This function prohibits login for a certain period after a certain number of login attempts fail due to password error. This function is enabled by default.

Default account lock settings

- Number of times an invalid password can be entered: 10

- Login prohibited time: 30 minutes

1. Edit the configuration file to disable or enable the function and change the settings.

```
$ sudo vi /etc/pam.d/common-auth
```

2. In the `common-auth` file, check the line succeeding to `# Account Lock` configuration.

```
# Account Lock configuration
auth    required          pam_tally2.so  deny=10  unlock_time=1800
```

How to disable the account lock

If you want to disable the function, add a hash mark (#) at the beginning of the line, as shown below.

```
# Account Lock configuration
#auth    required          pam_tally2.so  deny=10  unlock_time=1800
```

How to enable the account lock

If you want to enable the function again, delete the hash mark (#).

The following describes how to change the settings.

- Specify `deny=10` to lock the accounts if an invalid password is entered 10 times in succession.

- Specify `unlock_time=1800` to unlock the account after 1,800 seconds.

You can change the settings by changing the numeric values.

For set values, use 1 or greater half size integers.

(3) Setting the login timeout

This function allows the unit to automatically log out if no operation has been performed for a certain period. This function is disabled by default.

1. Edit the configuration file (`/etc/profile`) to enable the function.

```
$ sudo vi /etc/profile
```

2. For example, if you want the unit to automatically log out if no operation has been performed for 10 minutes (600 seconds), add the value to the end of the `/etc/profile` file as follows.

```
export TMOUT=600
```

Note

For set values, use 0 or greater half-size integers.

Set 0 to disable this function.

5.12.2 Setting password policies

You can specify the following settings for passwords of users who log in to the unit:

- Password conditions

- Password generation management

- Password expiration date

(1) Setting password conditions

This function ensures that only passwords that satisfy security conditions are used.

You can specify the following security conditions:

- Password length (minimum required number of characters)
- Combination of characters (uppercase letters, lowercase letters, numbers, and symbols)
- Check of whether the password was previously used

By default, nothing is specified. Specify conditions that meet your security requirements. Note that the Ubuntu's standard password policy always takes effect; the password must be at least 8 characters, must include at least 5 different types of characters, and must not be an easily guessable word such as password, qwerty, or hitachi.

1. To set this function, edit the configuration file.

```
$ sudo vi /etc/pam.d/common-password
```

2. In the `common-password` file, check the lines after `# password policy configuration`.

```
# password policy configuration
#Example: password        requisite     pam_pwquality.so retry=3 minlen=8 ucredit=-1 l
credit=-1 dcredit=-1 ocredit=-1 reject_username enforce_for_root
password    requisite    pam_pwquality.so retry=3
```

You can specify password conditions by adding options after `password requisite pam_pwquality.so retry=3`.

Table 5–14: List of password condition setting options below shows the options that can be set.

Table 5–14: List of password condition setting options

No.	Option	Description
1	`minlen`	Sets the password length (minimum required number of characters).
		If `minlen=8` is set, the password must contain at least eight characters.
2	`ucredit`	Sets the minimum number of uppercase alphabetic letters that a password must contain.
		If `ucredit=1` is set, the password must contain at least one uppercase alphabetic letter.[#]
3	`lcredit`	Sets the minimum number of lowercase alphabetic letters that a password must contain.
		If `lcredit=1` is set, the password must contain at least one lowercase alphabetic letter.[#]
4	`dcredit`	Sets the minimum number of numbers that a password must contain.
		If `dcredit=1` is set, the password must contain at least one number.[#]
5	`ocredit`	Sets the minimum number of symbols that a password must contain.
		If `ocredit=1` is set, the password must contain at least one symbol.
6	`reject_username`	Checks whether the password contains a user name.
		If you specify this option, the password cannot contain a user name.
7	`enforce_for_root`	Applies the same conditions to the root user.

#: If `minlen` is also specified, set a value multiplied by -1 (example: `ucredit=-1`).

3. The following shows a detailed example of password conditions.

```
# password policy configuration
password       requisite     pam_pwquality.so retry=3 minlen=8 ucredit=-1 lcredit=-1
dcredit=-1 ocredit=-1 reject_username enforce_for_root
```

In this case, the following conditions are set:

- The password must contain at least eight characters.
- The password must contain at least one uppercase alphabetic letter, one lowercase alphabetic letter, one number, and one symbol.
- A user name cannot be contained.
- The same conditions are applied to root.

(2) Setting password generation management

This function checks whether the entered password has been used in the past. If the same password is entered, the password change is not accepted. This setting is disabled by default.

1. To set this function, edit the configuration file.

```
$ sudo vi /etc/pam.d/common-password
```

2. In the `common-password` file, check the line following `# password policy configuration`.

```
# password policy configuration
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try
_first_pass sha512
```

3. Add the `remember` option to the succeeding line.

The `remember` option checks the password for the specified number of generations, and rejects the password change if the same password is used.

In the following example, the password change is not accepted if the same password is used within three generations.

```
# password policy configuration
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try
_first_pass sha512 remember=3
```

If the same password is entered, the following message appears.

```
$ passwd
Changing password for edgeadm.
(current) UNIX password:
New password:
Retype new password:
Password has been already used. Choose another.
passwd: Authentication token manipulation error
passwd: password unchanged
```

(3) Setting the password validity period

This function sets the validity period of a password. The validity period is not set by default, allowing a password to be used indefinitely.

1. Run the following command to set the password validity period.

```
$ sudo chage -M number-of-valid-days user-name-to-set-validity-period
```

number-of-valid-days: Specify the number of days in the validity period. Enter `99999` to use the password indefinitely.

When the password expires, the user of the password can no longer log in.

When the validity period is set, you must change the password within the validity period.

5.12.3 Setting up a firewall

Run the `iptables` or `ip6tables` command to set up a firewall.

Use `iptables` to set up a firewall for IPv4 communication, and use `ip6tables` to set up a firewall for IPv6 communication.

The following describes how to use the `iptables` command. When setting up a firewall for IPv6, replace *iptables* with *ip6tables* in the command execution examples.

(1) Firewall functions that can be specified

We provide firewall functions for managing attacks from malicious third parties and viruses.

Table 5–15: List of firewall functions below shows the firewall rules that can be specified and their defaults.

Table 5–15: List of firewall functions

No.	Rule name	Overview	Default
1	Port reception permission	Permits reception on only the specified ports and blocks all other ports. Security is improved by opening only the ports that need access from outside.	Disabled
2	Port transmission permission	Permits transmission to the specified ports and blocks all other transmission.	Communication to the following ports is possible: SSH (22/tcp) DNS (53/udp) HTTP (80/tcp) HTTPS (443/tcp)
3	Port reception permission (limited)	Permits reception on the specified ports while the number of connections within a certain period is limited. This setting provides effective protection against DoS (Denial of Service attacks), DDoS (Distributed Denial of Service attacks), and brute force attacks.	Data reception via SSH (22/tcp) is permitted a maximum of ten times per minute.

(2) Enabling or disabling the firewall

Firewall is enabled by default.

1. Run the following command to delete all settings and disable the firewall.

```
$ sudo iptables_allow_all
```

2. Run the following command to restore the default settings again and enable the firewall.

```
$ sudo default_iptables_configure
```

(3) Setting firewall rules

Use the following procedure to set firewall rules.

Figure 5–14: Procedure for setting the rules
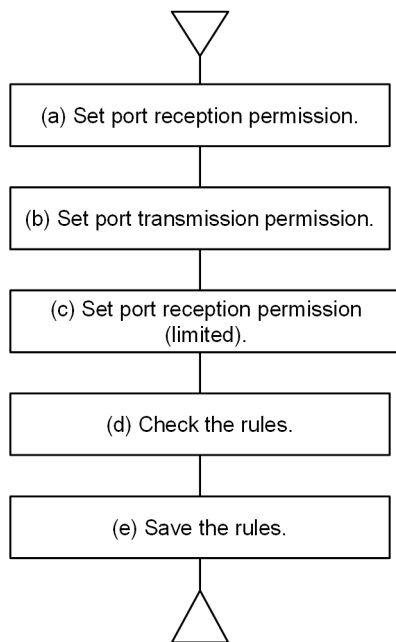
Note

The rule settings are applied when the command is run.

For example, if you perform an operation to cancel the reception permission of the SSH port while an SSH connection is being established, the ongoing communication may be disconnected and SSH login may be disabled.

(a) Setting the port permitted for reception

1. Run the following command to permit reception on a port with a given port number.

```
$ sudo iptables -A INPUT -p protocol: tcp|udp --dport port-number -j ACCEPT
```

Example: Specify as follows to permit reception on the HTTP server port (80/tcp):

```
$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

2. Run the following command to cancel the reception permission that has been set.

```
$ sudo iptables -D INPUT -p protocol:tcp|udp --dport port-number -j ACCEPT
```

Example: Specify as follows to cancel the reception permission for the HTTP server port (80/tcp).

```
$ sudo iptables -D INPUT -p tcp --dport 80 -j ACCEPT
```

(b) Setting the port permitted for transmission

1. Run the following command to connect to a port with a given number.

```
$ sudo iptables -A OUTPUT -p protocol:tcp|udp --dport port-number -j ACCEPT
```

Example: Specify as follows to permit transmission to the HTTP server port (80/tcp).

```
$ sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
```

2. Run the following command to cancel the transmission permission that has been set.

```
$ sudo iptables -D OUTPUT -p protocol:tcp|udp --dport port-number -j ACCEPT
```

Example: Specify as follows to cancel the transmission permission for the HTTP server port (80/tcp).

```
$ sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
```

(c) Setting the port permitted for reception with a limitation

1. Run the following command to permit reception on a port with a given port number while the number of connections that can be established per minute is limited.

Note

Before running the command, you must delete the existing reception permission, if any.

```
$ sudo iptables -A INPUT -m state --state NEW -m hashlimit --hashlimit-htable-ex
pire 60000 \
 --hashlimit-name hasht_port-number --hashlimit time/m --hashlimit-burst number-
of-connections \
 -p protocol:tcp|udp --dport port-number -j ACCEPT
```

Example: Specify as follows to permit a maximum of 10 times of data reception per minute on the SSH server port (22/tcp).

```
$ sudo iptables -A INPUT -m state --state NEW -m hashlimit --hashlimit-htable-expir
e 60000 \
 --hashlimit-name hasht_22 --hashlimit 1/m --hashlimit-burst 10 \
 -p tcp --dport 22 -j ACCEPT
```

2. Run the following command to cancel the reception permission that has been set.

```
$ sudo iptables -D INPUT -m state --state NEW -m hashlimit --hashlimit-htable-expir
e 60000 \
 --hashlimit-name hasht_port-number --hashlimit time/m --hashlimit-burst limitation
-count \
 -p protocol:tcp|udp --dport port-number -j ACCEPT
```

Example: Specify as follows to cancel the reception permission for the HTTP server port (22/tcp).

```
$ sudo iptables -D INPUT -m state --state NEW -m hashlimit --hashlimit-htable-expir
e 60000 \
 --hashlimit-name hasht_22 --hashlimit 1/m --hashlimit-burst 10 \
 -p tcp --dport 22 -j ACCEPT
```

(d) Confirming the set rules

1. Run the following command to confirm the firewall rules that have been set.

```
$ sudo iptables -L
```

The following shows a display example of the default rule settings.

```
Chain INPUT (policy DROP)
target     prot opt source              destination
ACCEPT     icmp --  anywhere            anywhere
ACCEPT     all  --  anywhere            anywhere
ACCEPT     all  --  anywhere            anywhere             state RELATED,ESTABLI
SHED
ACCEPT     tcp  --  anywhere            anywhere             state NEW limit: up t
o 1/min burst 10 tcp dpt:ssh

Chain FORWARD (policy DROP)
target     prot opt source              destination

Chain OUTPUT (policy DROP)
target     prot opt source              destination
ACCEPT     all  --  anywhere            anywhere             state RELATED,ESTABLI
SHED
ACCEPT     icmp --  anywhere            anywhere
ACCEPT     udp  --  anywhere            anywhere             udp dpt:domain
ACCEPT     tcp  --  anywhere            anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere            anywhere             tcp dpt:http
ACCEPT     tcp  --  anywhere            anywhere             tcp dpt:ntp
ACCEPT     tcp  --  anywhere            anywhere             tcp dpt:https
```

(e) Saving the rules

1. Save the firewall rules that have been set.

To apply the settings (even after the OS is restarted), run the following command.

```
$ sudo /etc/init.d/netfilter-persistent save
```

5.13 Setting host names

You can set the host name for the unit by editing the `/etc/hostname` file.

By default, `ctrl-edgen` is set.

```
$ sudo vi /etc/hostname
```

After editing the file, save it and then terminate processing. To exit the `vi` command, use `:wq` (write quit).

Then, use the `hostname` command to apply the host name you have set.

```
$ sudo hostname -F /etc/hostname
```

5.14 Changing OS operation mode

5.14.1 What is the OS operation mode?

You must change the OS operation mode depending on whether you perform normal operation or maintenance work.

(1) Normal mode

This mode allows you to start the OS and then operate user programs such as application programs. The factory default of the unit is normal mode.

To change maintenance mode to normal mode, specify *normal mode* for the next startup mode, and then restart the unit.

(2) Maintenance mode

This mode allows the OS to start without starting user programs such as application programs. To change normal mode to maintenance mode, specify *maintenance mode* for the next startup mode, and then restart the unit.

In all places marked with *maintenance mode* in this manual, you need to change the operation mode to maintenance mode before performing the relevant operation.

5.14.2 How to change the OS operation mode

Use the OS startup mode change command (`ecmodeset`) to change the OS operation mode. The following describes how to change the OS operation mode.

For details about the user name and password used to log in to the unit, see 5.2 Logging in to the unit after powering it on for the first time. For details about the commands used in each step, see 5.18 Command reference.

5.14.3 Changing normal mode to maintenance mode

NOTICE

Application programs do not operate in maintenance mode. After maintenance work is finished, you must return the mode to normal mode.

1. Log in to the unit.

```
login: edgeadm
Password: *******
```

2. Check the current OS operation mode.

Run the `showecmode` command to check the current OS operation mode. Confirm that `Normal mode` is displayed for both `Current` and `Next` (see the **bold underlined parts**).

```
$ sudo showecmode
Current  : Normal mode
Next     : Normal mode
$
```

3. Set the next OS operation mode to maintenance mode.

Run the `ecmodeset` command to set maintenance mode for the next startup mode of the OS (see the **bold underlined part**).

```
$ sudo ecmodeset -enable
Set next boot : Maintenance mode
$
```

4. Check the setting of the next OS operation mode.

Run the `showecmode` command to check the next OS operation mode. Confirm that the display for `Next` has changed to `Maintenance mode` (see the **<u>bold underlined part</u>**).

```
$ sudo showecmode
Current  : Normal mode
Next     : Maintenance mode
$
```

5. Stop the unit.

Run the `shutdown` command to stop the unit, and then turn off the power.

```
$ sudo shutdown -h 0
```

6. Unplug or connect the LAN cable.

Unplug the LAN cables to disconnect the unit from the remainder of the system. To connect the unit and the maintenance PC, use the LAN cable to directly connect them.

7. Start the unit.

Turn on the power to the unit.

8. Log in to the unit.

```
login: edgeadm
Password: *******
```

9. Check the current OS operation mode.

Run the `showecmode` command to check the current OS operation mode.

Confirm that `Maintenance mode` is displayed for both `Current` and `Next` (see the **<u>bold underlined parts</u>**).

```
$ sudo showecmode
Current  : Maintenance mode
Next     : Maintenance mode
$
```

5.14.4 Changing maintenance mode to normal mode

1. Log in to the unit.

```
login: edgeadm
Password: *******
```

2. Check the current OS operation mode.

Run the `showecmode` command to check the current OS operation mode. Confirm that `Maintenance mode` is displayed for both `Current` and `Next` (see the **<u>bold underlined parts</u>**).

```
$ sudo showecmode
Current  : Maintenance mode
Next     : Maintenance mode
$
```

3. Specify normal mode for the next OS operation mode.

Run the `ecmodeset` command to specify `Normal mode` for the next startup of the OS (see the **<u>bold underlined parts</u>**).

```
$ sudo ecmodeset -disable
Set next boot : Normal mode
$
```

4. Check the setting of the next OS operation mode.

Run the `showecmode` command to check the next OS operation mode. Confirm that the display for `Next` has changed to `Normal mode` (see the **<u>bold underlined parts</u>**).

```
$ sudo showecmode
Current  : Maintenance mode
Next     : Normal mode
$
```

5. Stop the unit.

Run the `shutdown` command to stop the unit, and then turn off the power.

```
$ shutdown -h 0
```

6. Unplug or connect the LAN cable.

Disconnect the cable connecting to the maintenance PC if it has been connected during maintenance work. Connect the LAN cables to the remainder of the system, which has been temporary disconnected during maintenance work.

7. Turn on the power to the unit.

Start the unit.

8. Log in to the unit.

```
login: edgeadm
Password: *******
```

9. Check the current OS operation mode.

Run the `showecmode` command to check the current OS operation mode. Confirm that `Normal mode` is displayed for both `Current` and `Next` (see the **bold underlined parts**).

```
$ sudo showecmode
Current  : Normal mode
Next     : Normal mode
$
```

5.15 Backup, restoration, and program updates

The following functions are available for managing software installed in the unit:

- Backup function
- Restore function
- Program update function

Figure 5–15: Flow of operations

```
              ▽
   ┌─────────────────────────────────────────────┐
   │ 1. Connect peripherals. (5.15.1)            │
   └─────────────────────────────────────────────┘
   ┌─────────────────────────────────────────────┐
   │ 2. (Optional) Create partitions in external media. (5.15.2) │
   └─────────────────────────────────────────────┘
   ┌─────────────────────────────────────────────┐
   │ 3. (Optional) Change the OS operation mode to │
   │    maintenance mode. (5.14)                  │
   └─────────────────────────────────────────────┘
   ┌─────────────────────────────────────────────┐
   │ 4. Perform an operation. (5.15.3, 5.15.4, or 5.15.5) │
   └─────────────────────────────────────────────┘
   ┌─────────────────────────────────────────────┐
   │ 5. (Optional) Change the OS operation mode to normal │
   │    mode. (5.14)                              │
   └─────────────────────────────────────────────┘
              △
```
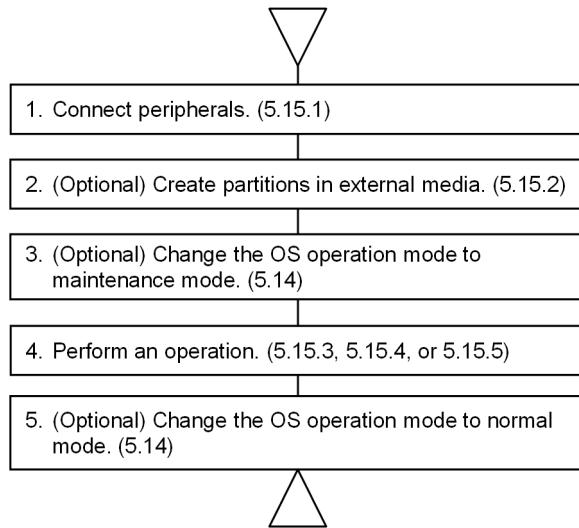
5.15.1 Device configuration when using each function

To back up or restore data or update programs, you need to connect the necessary peripherals to the unit. Select configuration No. 1, 2, or 3 according to the operating environment of the unit.

USB flash drive and CFast are available as "external media". In this section, USB flash drive is used as the example.

(1) Configuration No. 1

In this configuration, a USB flash drive and a maintenance PC are connected to the unit.

Table 5–16: Devices connected to the unit in configuration No. 1

Device	Connection method	Description
Maintenance PC	Ethernet	This device is used for the operation of data backup, data restore, and program update functions. To connect the maintenance PC to the unit, use an Ethernet crossover cable.
USB flash drive	USB	External media that stores backup data

Figure 5–16: Configuration for connecting a USB flash drive and maintenance PC to the unit
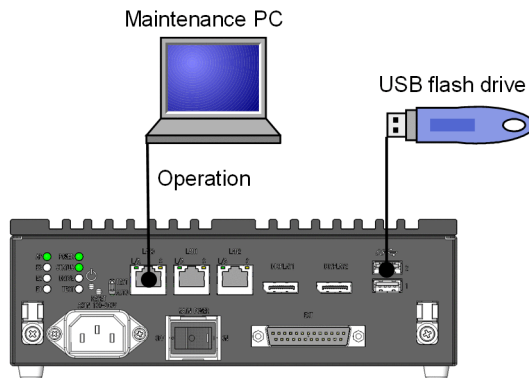
(2) Configuration No. 2

In this configuration, only the maintenance PC is connected to the unit.

Table 5–17: Device connected to the unit in configuration No. 2

Device	Connection method	Description
Maintenance PC	Ethernet	This device is used for the operation of data backup, data restore, and program update functions. To connect the maintenance PC to the unit, use an Ethernet crossover cable.

Figure 5–17: Configuration for connecting the maintenance PC
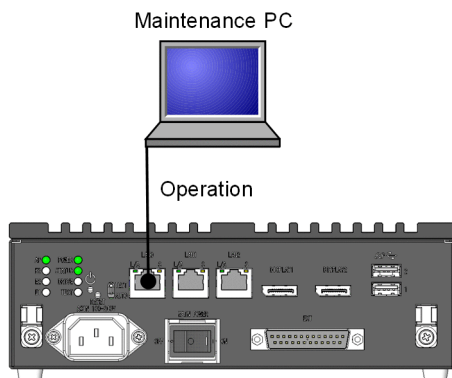
(3) Configuration No. 3

In this configuration, a monitor, keyboard, and USB flash drive are connected to the unit.

Table 5–18: Devices connected to the unit in configuration No. 3

Device	Connection method	Description
Keyboard	USB	This device is used for the operation of data backup, data restore and program update functions.
Display	DisplayPort	Console screen
USB flash drive	USB	External media that stores backup data

Figure 5–18: Configuration for connecting the keyboard, display, and USB flash drive to the unit
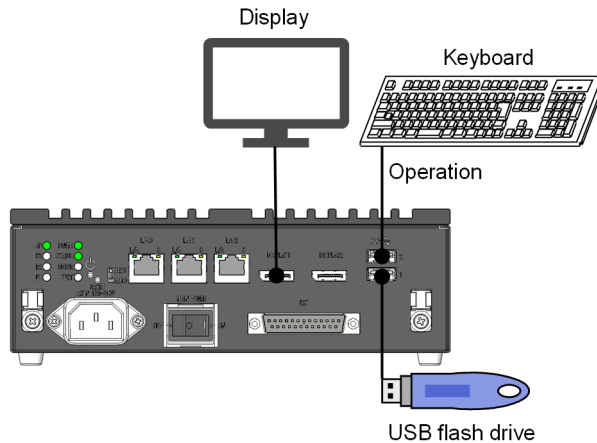
5.15.2 Creating and formatting partitions in the external media

In the external media to be used for the functions, create and format partitions in advance. The following describes how to create partitions in the external media and then create a file system.

1. Check the block device of the unit.

   Run the `lsblk` command to check the block device before the external media is connected. If the external media is not connected, only `sda` is displayed.

   ```
   $ lsblk -d
   NAME MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   sda    8:0    0   80G  0 disk
   $
   ```

2. Connect the external media to the unit.

3. Check the block device of the unit.

   Run the `lsblk` command to check the block device before the external media is connected. The part added to the information shown in step 1 indicates the device name assigned to the external media. In the following example, `sdb` is the device name assigned to the external media.

   ```
   $ lsblk -d
   NAME MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   sdb    9:0    0   16G  0 disk
   $
   ```

4. Create a partition in the external media.

   Run the `gdisk` command to create new partitions in the external media.

   Perform steps 2 to 10 in (2) Creating partitions.

   ```
   $ gdisk /dev/sdb
   ```

5. Create a file system in the partition.

   Use the `mkfs` command to create a file system in the partition you created. You can create a FAT32 or an EXT4 file system. FAT32 can be used in Linux and Windows, but individual files must not exceed 4 GB. EXT4 can be used in Linux only.

   • Example of running the command to create a FAT32 file system

   ```
   $ sudo mkfs -t vfat /dev/sdb1
   $
   ```

   • Example of running the command to create an EXT4 file system

   ```
   $ sudo mkfs -t ext4 /dev/sdb1
   $
   ```

5.15.3 Backing up storage data

(1) Overview of backup

When you perform backup, data in the storage of the unit is saved in the external media or maintenance PC. The following data can be backed up.

Table 5–19: Data that can be backed up

Data type	File or device name
Partition information	User area's partition configuration, file system, backup file list
Files in the configuration file area	Configuration files related to the configuration of the software environment (`/dev/sda7`)
Standard program product area	Files of program products added by enhancement of the unit and program products added by the user (`/dev/sda8`)
User area	Area constructed by the user (`/dev/sda9` to `/dev/sda128`)

If the data being saved in the backup destination exceeds 1 GB, the backup file is divided into blocks of 1 GB or smaller and saved. The backup procedure varies depending on the configuration. The following describes the procedure for each configuration.

(2) Backing up data in configuration No. 1

The following describes the procedure for backing up data in the external media connected to the unit.

(a) Preparation

- Create partitions in the external media and format them with EXT4.
  The backup data save area in the external media must be formatted with EXT4.

- Prepare external media that has free space greater than the capacity that is actually used in the directory partitions to be backed up.
  There is no need to consider the space for unused areas in partitions because the backup file is compressed before it is saved.

- The time required to back up data is approximately 30 seconds per GB. If files are to be verified, additional time (approximately 30 seconds) is required. More time might be required depending on the transfer rate of the external device.

- Stop the unit and then connect it with the maintenance PC by using an Ethernet cable.
  If necessary, disconnect other devices from the unit.

- Change the OS operation mode of the unit from normal mode to maintenance mode.

- Use terminal emulation software for remote connection to the unit from the maintenance PC, and then log in to the unit by using SSH.
  You must log in as a user who can run the `sudo` command.

(b) Operation procedure

Use the maintenance PC to remotely log in to the unit in which the information to be backed up is stored, and then run the backup command.

Figure 5–19: Flow of backup steps in configuration No. 1

1. Check the communication between the maintenance PC and the unit.

   Run the `ping` command to confirm that the maintenance PC can communicate with the unit.

   ```
   $ ping IP-address-of-the-target-unit
   ```

2. Remotely log in to the unit from the maintenance PC.

   Remotely log in to the unit as a user who can run the `sudo` command.

   Example user name: `edgeadm`

   ```
   login: edgeadm
   Password: *******
   ```

3. Confirm that the OS operation mode is set to maintenance mode.

   Run the `showecmode` command to confirm that the **bold underlined parts** are displayed as follows.

   ```
   $ sudo showecmode
   Current  : Maintenance mode
   Next     : Maintenance mode
   $
   ```

4. Connect the external media.

5. Mount the external media on `/mnt/ecbackup_data`.

   ```
   $ sudo mount external-media /mnt/ecbackup_data
   ```

6. Run the backup command.

   Run the `ecbackup` command to save the backup files in the external media. The following example shows how to run the `ecbackup` command.

   - When the backup menu appears, enter `1` (see the underlined part), and then press the **Enter** key to start backup.

- The backup destination, the range of target partitions, and a message indicating the processing status are displayed. Then, a message asking you whether you want to verify the saved backup files appears. Enter `y` to verify the files, or enter `N` to skip the verification.

- Finally, wait for the command to terminate, displaying the `Successfully complete` message.

```
$ sudo ecbackup
Please select a backup mode.
1. Back up to external media
2. Back up to maintenance PC
q. quit
> 1                               <- Back up to external media
Partition info backup started.
Partition info backup finished.
Backup directory: /mnt/ecbackup_data/ecbackup_20210525101010
Backup targets: /dev/sda8 /dev/sda9 /dev/sda10 /media/etc
Partition /dev/sda8 backup start.
(snip)
Will you verify backup files(y / N)? N  <- Whether to verify files
Finished:/mnt/ebackup_data/ecbackup_20210525101010/20210525101010_sda10_01.tgz:
xxx,xxx,xxx bytes
Successfully completed
$
```

If the command terminates displaying a message other than `Successfully completed`, the backup processing was interrupted due to an error. Take corrective action against the error, and then rerun the backup command.

7. Unmount and then remove the external media from the unit.

Run the following command to unmount the external media from the unit.

```
$ sudo umount /mnt/ecbackup_data
```

8. Log out from the unit.

```
$ exit
```

To change the OS operation mode to normal mode, see 5.14.4 Changing maintenance mode to normal mode.

(3) Backing up data in configuration No. 2

The following describes the procedure for backing up data in the maintenance PC connected to the unit.

(a) Preparation

- Format the backup data save area of the maintenance PC with ext4.

- On the maintenance PC, allocate free space greater than the capacity that is actually used in the directory partitions to be backed up.

  There is no need to consider the space for unused areas in partitions because the backup file is compressed before it is saved.

- The time required to back up data is approximately 30 seconds per GB. If files are to be verified, additional time (approximately 30 seconds) is required. In addition, the time for transferring backup files to the maintenance PC is required.

- Stop the unit, and then connect it to the maintenance PC by using an Ethernet cable.

  If necessary, disconnect other devices from the unit.

- Change the OS operation mode of the unit from normal mode to maintenance mode.

- Use terminal emulation software for remote connection to the unit from the maintenance PC, and then log in to the unit by using SSH.

  You must log in as a user who can run the `sudo` command.

- The maintenance PC shall have the capability of executing the `scp` command. (Tera Term has the scp capability.)

(b) Operation procedure

Use the remote operation terminal to remotely log in to the unit in which the information to be backed up is stored, and then run the backup command. Then, save the backup files in the maintenance PC by using the `scp` operation terminal.

Figure 5–20: Flow of backup steps in configuration No. 2

1. Check the communication between the maintenance PC and the unit by using the remote operation terminal.
   Run the `ping` command to confirm that the maintenance PC can communicate with the unit.

   ```
   $ ping IP-address-of-the-target-unit
   ```

2. Remotely log in to the unit from the maintenance PC by using the remote operation terminal.
   Remotely log in to the unit as a user who can run the `sudo` command.
   Example user name: `edgeadm`

   ```
   login: edgeadm
   Password: *******
   ```

3. Confirm that the OS operation mode is set to maintenance mode.
   Run the `showecmode` command to confirm that the **bold underlined parts** are displayed as follows.

   ```
   $ sudo showecmode
   Current  : Maintenance mode
   Next     : Maintenance mode
   $
   ```

4. Run the backup command.
   Run the `ecbackup` command to create backup files in the unit. The following example shows how to run the `ecbackup` command.

- When the backup menu appears, enter 2 (see the underlined part), and then press the **Enter** key to start backup.

- The backup destination, the range of target partitions, and a message indicating the processing status are displayed. Then, a message asking you whether you want to verify the saved backup files appears. Enter y to verify the files, or enter N to skip the verification. In addition, record the size of the tgz file.

- When the Please get *file-name*. Finished (y)? message appears, the file is created in the /mnt/ecbackup_data/ecbackup_*YYYYMMDDhhmmss* directory. Transfer the file to the maintenance PC by using the scp operation terminal.

- After transferring the file, enter y. Then delete the file and start saving the next backup file.

- Finally, wait for the command to terminate, displaying the Successfully complete message.

```
$ sudo ecbackup
Please select a backup mode.
1. Back up to external media
2. Back up to maintenance PC
q. quit
> 2                          <- Back up to maintenance PC.
Partition info backup started.
Partition info backup finished.
Backup directory: /mnt/ecbackup_data/ecbackup_20210525101010
Backup targets: /dev/sda8 /dev/sda9 /dev/sda10 /media/etc
Partition /dev/sda8 backup start.
31MiB 0:00:01 [16.1MiB/s] [====>                    ] 25% ETA 0:00:02
Will you verify backup files(y / N)? N   <-Whether to verify files
Finished:/mnt/ebackup_data/ecbackup_20210525101010/20210525101010_sda8_01.gz: xx
x,xxx,xxx bytes
Please get 20210525101010_sda8_01.gz. Finished (y)?> y <- Input it after transfe
rred the created files

(snip)

Successfully completed
$
```

If the command terminates displaying a message other than Successfully completed, the backup processing was interrupted due to an error. Take corrective action against the error, and then rerun the backup command.

5. When the Please get *file-name*. Finished (y)? message appears, save the backup file in the maintenance PC by using the scp operation terminal.

- When using Tera Term

    Click **File**, and then **SSH SCP** to display the Secure File Copy screen.

    In the bottom of the screen, enter the path to the backup file for **From**, and enter the path to the save destination for **To**.

    Click the **Receive** button.

- When using the scp command

    Run the following command.

```
$ scp edgeadm@IP-address:file-path save-destination-path
```

6. Enter y in response to the Please get *file-name*. Finished (y)?> message.

    The file indicated by *file-name* is deleted and creation of the next backup file starts. If you press the **Enter** key without entering anything or enter a character other than y, the same message appears again and the system waits for you to enter information again.

7. Compare the file sizes to confirm that the backup file is saved correctly.

    Compare the size of the backup file saved in the maintenance PC with the file size displayed when the backup command was run, and make sure that they are the same size.

8. When Successfully completed appears, save the partition information file in the maintenance PC by using the scp operation terminal. The partition information file named *YYYYMMDDhhmmss*_ecbackup.conf is placed in /mnt/ecbackup_data/ecbackup_*YYYYMMDDhhmmss*/.

    For details about how to obtain the file, see step 5.

9. Log out from the unit.

```
$ exit
```

To change the OS operation mode to normal mode, see 5.14.4 Changing maintenance mode to normal mode.

(4) Backing up data in configuration No. 3

The following describes the procedure for backing up data in the external media connected to the unit.
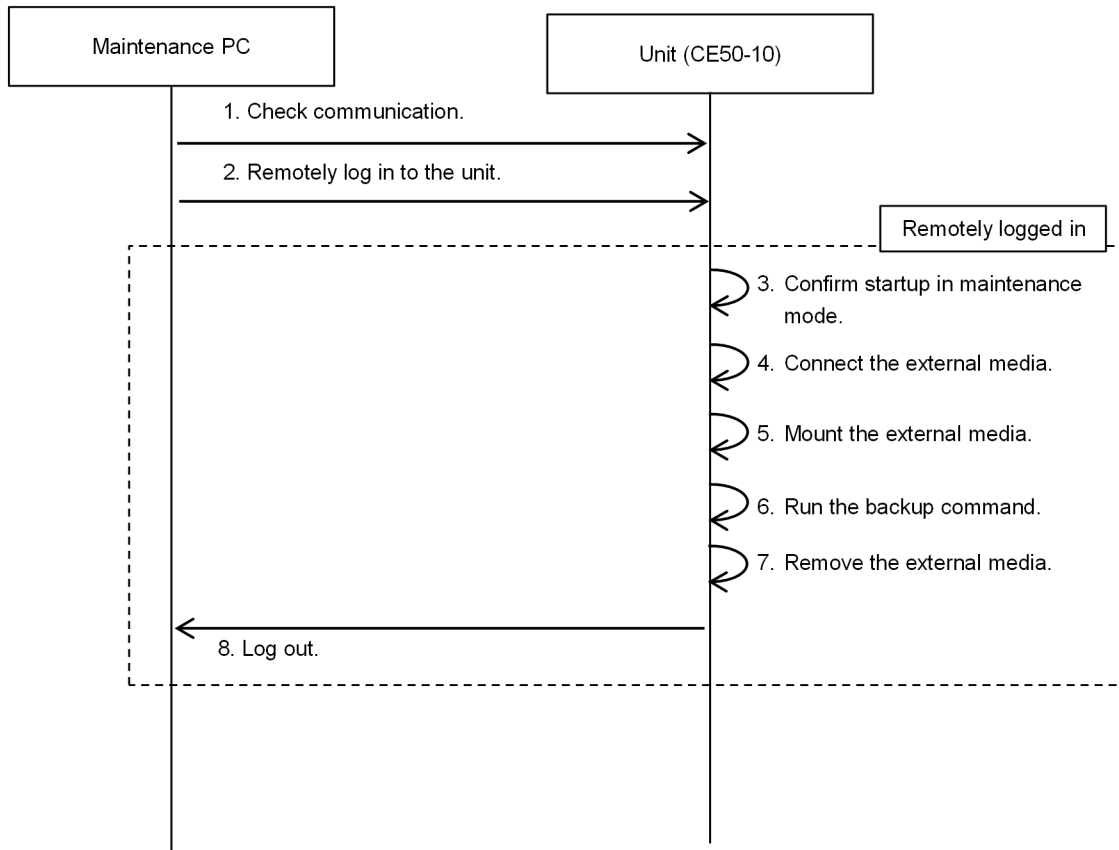
(a) Preparation

- Create partitions in the external media, and format them with EXT4.
  The backup data save area in the external media must be formatted with EXT4.

- Prepare external media that has free space greater than the capacity that is actually used in the directory partitions to be backed up.
  There is no need to consider the space for unused areas in partitions because the backup file is compressed before it is saved.

- The time required to back up data is approximately 30 seconds per GB. If files are to be verified, additional time (approximately 30 seconds) is required. More time might be required depending on the transfer rate of the external media.

- Change the OS operation mode of the unit from normal mode to maintenance mode.

(b) Operation procedure

Log in to the unit in which the information to be backed up is stored, and then run the backup command.

Figure 5–21: Flow of backup steps in configuration No. 3
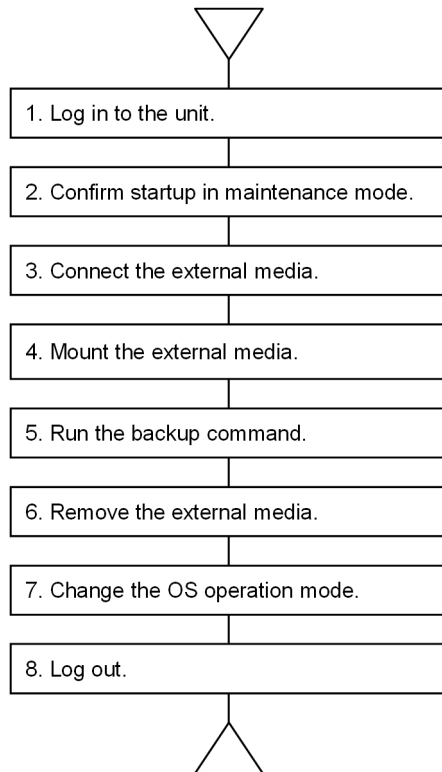
```
                    ▽
        ┌─────────────────────────────┐
        │ 1. Log in to the unit.      │
        └─────────────────────────────┘
        ┌─────────────────────────────┐
        │ 2. Confirm startup in maintenance mode. │
        └─────────────────────────────┘
        ┌─────────────────────────────┐
        │ 3. Connect the external media. │
        └─────────────────────────────┘
        ┌─────────────────────────────┐
        │ 4. Mount the external media. │
        └─────────────────────────────┘
        ┌─────────────────────────────┐
        │ 5. Run the backup command.  │
        └─────────────────────────────┘
        ┌─────────────────────────────┐
        │ 6. Remove the external media. │
        └─────────────────────────────┘
        ┌─────────────────────────────┐
        │ 7. Change the OS operation mode. │
        └─────────────────────────────┘
        ┌─────────────────────────────┐
        │ 8. Log out.                 │
        └─────────────────────────────┘
                    △
```

1. Log in to the unit.
   Remotely log in to the unit as a user who can run the sudo command.
   Example user name: edgeadm

```
login: edgeadm
Password: *******
```

2. Confirm that the OS operation mode is set to maintenance mode.

Run the `showecmode` command to confirm that the **<u>bold underlined parts</u>** are displayed as follows.

```
$ sudo showecmode
Current  : Maintenance mode
Next     : Maintenance mode
$
```

3. Connect the external media.

4. Mount the external media on `/mnt/ecbackup_data`.

```
$ sudo mount external-media /mnt/ecbackup_data
```

5. Run the backup command.

Run the `ecbackup` command to save the backup files in the external media. The following example shows how to run the `ecbackup` command.

- When the backup menu appears, enter `1` (see the underlined part), and then press the **Enter** key to start backup.

- The backup destination, the range of target partitions, and a message indicating the processing status are displayed. Then, a message asking you whether you want to verify the saved backup files appears. Enter `y` to verify the files or enter `N` to skip the verification.

- Finally, wait for the command to terminate, displaying the `Successfully complete` message.

```
$ sudo ecbackup
Please select a backup mode.
1. Back up to external media
2. Back up to maintenance PC
q. quit
> 1                              <- Back up to external media.
Partition info backup started.
Partition info backup finished.
Backup directory: /mnt/ecbackup_data/ecbackup_20210525101010 <- Backup destinati
on
Backup targets: /dev/sda8 /dev/sda9 /dev/sda10 /media/etc
Partition /dev/sda8 backup start.
(snip)
Will you verify backup files(y / N)? N <-Whether to verify files
Finished:/mnt/ebackup_data/ecbackup_20210525101010/20210525101010_sda10_01.tgz:
xxx,xxx,xxx bytes
Successfully completed
$
```

If the command terminates displaying a message other than `Successfully completed`, the backup processing was interrupted due to an error. Take corrective action against the error, and then rerun the backup command.

6. Unmount the external media from the unit.

Use the following command to unmount the external media from the unit.

```
$ sudo umount /mnt/ecbackup_data
```

7. Remove the external media from the unit.

8. Log out from the unit.

To change the OS operation mode to normal mode, see 5.14.4 Changing maintenance mode to normal mode.

5.15.4 Restoring backup data

(1) Overview of restoration

When you perform restoration, backup data saved in the external media or maintenance PC is copied to the unit. The restoration procedure varies depending on the configuration. The following describes the procedure for each configuration.

(2) Restoring data in configuration No. 1

The following describes the procedure for restoring backup data from the external media connected to the unit.

(a) Preparation

- Stop the unit, and then connect it with the maintenance PC by using an Ethernet cable.
  If necessary, disconnect other devices from the unit.

- Change the OS operation mode of the unit from normal mode to maintenance mode.

- Use terminal emulation software for remote connection to the unit from the maintenance PC, and then log in to the unit by using SSH.
  You must log in as a user who can run the `sudo` command.

- The time required to restore data from a backed up file is approximately 30 seconds per GB. If files are to be verified, additional time (approximately 30 seconds) is required. More time might be required depending on the transfer rate of the external device.

(b) Operation procedure

Use the maintenance PC to remotely log in to the unit in which the backup data is to be restored, and then run the restoration command.

Figure 5–22: Flow of restoration steps in configuration No. 1

1. Check the communication between the maintenance PC and the unit.
   Run the `ping` command to confirm that the maintenance PC can communicate with the unit.

   ```
   $ ping IP-address-of-the-target-unit
   ```

2. Remotely log in to the unit from the maintenance PC.
   Remotely log in to the unit as a user who can run the `sudo` command.

Example user name: `edgeadm`

```
login: edgeadm
Password: *******
```

3. Confirm that the OS operation mode is set to maintenance mode.

Run the `showecmode` command to confirm that the **<u>bold underlined parts</u>** are displayed as follows.

```
$ sudo showecmode
Current  : Maintenance mode
Next     : Maintenance mode
$
```

4. Connect the external media.

5. Mount the external media on `/mnt/ecbackup_data`.

```
$ sudo mount external-media /mnt/ecbackup_data
```

6. Run the restoration command.

Run the `ecrestore` command to save the backup files from the external media to the unit. The following example shows how to run the `ecrestore` command.

- When the restoration menu appears, enter `1` (see the underlined part), and then press the **Enter** key to start restoration.

```
$ sudo ecrestore
Please select a restore mode.
1. Restore from external media
2. Restore from maintenance PC
q. quit
> 1                             <-Restore from external media.
```

- When restoration starts, a list of directories containing backup files stored in the external media appears. Enter the number of the directory to be restored (see the underlined part), and then press the **Enter** key.

```
Backup directory list:
1. ecbackup_20210525101010
q. quit
> 1                             <- Directory to be restored
```

- The progress of processing, restored file name, and processing time are displayed. Then, a message asking you whether you want to verify the restored files appears. Enter `y` to verify the files or enter `N` to skip the verification.

```
Making partitions finished
Restoring from extra media.
Restoring: 20210525101010_sda8_01.gz
31MiB 0:00:01 [16.1MiB/s] [====>              ] 25% ETA 0:00:02
Will you verify restored area(y / N)?N <- Whether to verify files
Finished: 20210525101010_sda8_01.gz
(snip)
Successfully completed
```

- After running the command, wait for the command to terminate, displaying the `Successfully complete` message.

  If the command terminates displaying a message other than `Successfully completed`, the restoration processing was interrupted due to an error. Take corrective action against the error, and then rerun the restoration command.

7. Unmount the external media from the unit.

After restoration finishes, unmount the connected external media from the unit.

```
$ sudo umount /mnt/ecbackup_data
```

8. Remove the external media from the unit.

9. Reboot the unit.

```
$ sudo reboot
```

10. (No user operation required) Automatically log out from the unit.

To change the OS operation mode to normal mode, see 5.14.4 Changing maintenance mode to normal mode.

(3) Restoring data in configuration No. 2

The following describes the procedure for restoring backup data from the maintenance PC connected to the unit.

(a) Preparation

- The maintenance PC shall have the capability of executing the `scp` command. (Tera Term has the scp capability.)
- Stop the unit, and then connect it to the maintenance PC by using an Ethernet cable.
  If necessary, disconnect other devices from the unit.
- Change the OS operation mode of the unit from normal mode to maintenance mode.
- Use terminal emulation software for remote connection to the unit from the maintenance PC, and then log in to the unit by using SSH.
  You must log in as a user who can run the `sudo` command.
- The time required to restore data from a backed up file is approximately 30 seconds per GB. If files are to be verified, additional time (approximately 30 seconds) is required. More time might be required depending on the transfer rate of the external media. In addition, the time for transferring backup files to the unit is required.

(b) Operation procedure

Use the remote operation terminal to remotely log in to the unit in which the backup data is to be restored, and then run the restoration command. Then, send backup data from the maintenance PC to the unit by using the `scp` operation terminal.

Figure 5–23: Flow of restoration procedure in configuration No. 2

1. Check the communication between the maintenance PC and the unit by using the remote operation terminal.
   Run the `ping` command to confirm that the maintenance PC can communicate with the unit.

```
$ ping IP-address-of-the-target-unit
```

2. Remotely log in to the unit from the maintenance PC by using the remote operation terminal.

Remotely log in to the unit as a user who can run the `sudo` command.

Example user name: `edgeadm`

```
login: edgeadm
Password: *******
```

3. Confirm that the OS operation mode is set to maintenance mode.

Run the `showecmode` command to confirm that the **bold underlined parts** are displayed as follows.

```
$ sudo showecmode
Current  : Maintenance mode
Next     : Maintenance mode
$
```

4. Run the restoration command.

Run the `ecrestore` command to save the backup files from the maintenance PC to the unit. The following example shows how to run the `ecrestore` command.

When the restoration menu appears, enter 2 (see the underlined part), and then press the **Enter** key to start restoration.

```
$ sudo ecrestore
Please select a restore mode.
1. Restore from external media
2. Restore from maintenance PC
q. quit
> 2                              <- Restore from maintenance PC.
```

5. Send the backup file containing partition information to the unit.

When the following message appears, transfer the partition information file (*YYYYMMDDhhmmss*_ecbackup.conf) to /mnt/ecbackup_data/ by using the `scp` operation terminal. When transfer has finished, enter `y`, and then press the **Enter** key. The partition information is restored.

```
Please send YYYYMMDDhhmmss_ecbackup.conf to /mnt/ecbackup_data/   Finished? (y) y
        <- Enter this after scp transfer ends.
Making partitions finished
OK
```

6. Send the backup file to the unit.

Transfer the backup file to /mnt/ecbackup_data/ according to the message by using the `scp` operation terminal. When transfer has finished, enter `y`, and then press the **Enter** key. When you select whether to verify files, restoration is performed.

```
Restoring from maintenance PC.
Please send 20210525101010_sda8_01.gzto /mnt/ecbackup_data/.   Finished? (y)y
                <- Enter the response after scp transfer ends.
Restoring: 20210525101010_sda8_01.gz
31MiB 0:00:01 [16.1MiB/s] [====>                    ] 25% ETA 0:00:02
Will you verify restored area(y / N)? N <- Whether to verify files
Finished: 20210525101010_sda8_01.gz

(snip)

Successfully completed
$
```

Repeat these steps for all the backup files.

7. Reboot the unit.

```
$ sudo reboot
```

8. (No user operation required) Automatically log out from the unit.

To change the OS operation mode to normal mode, see 5.14.4 Changing maintenance mode to normal mode.

(4) Restoring data in configuration No. 3

The following describes the procedure for restoring backup data from the external media connected to the unit.
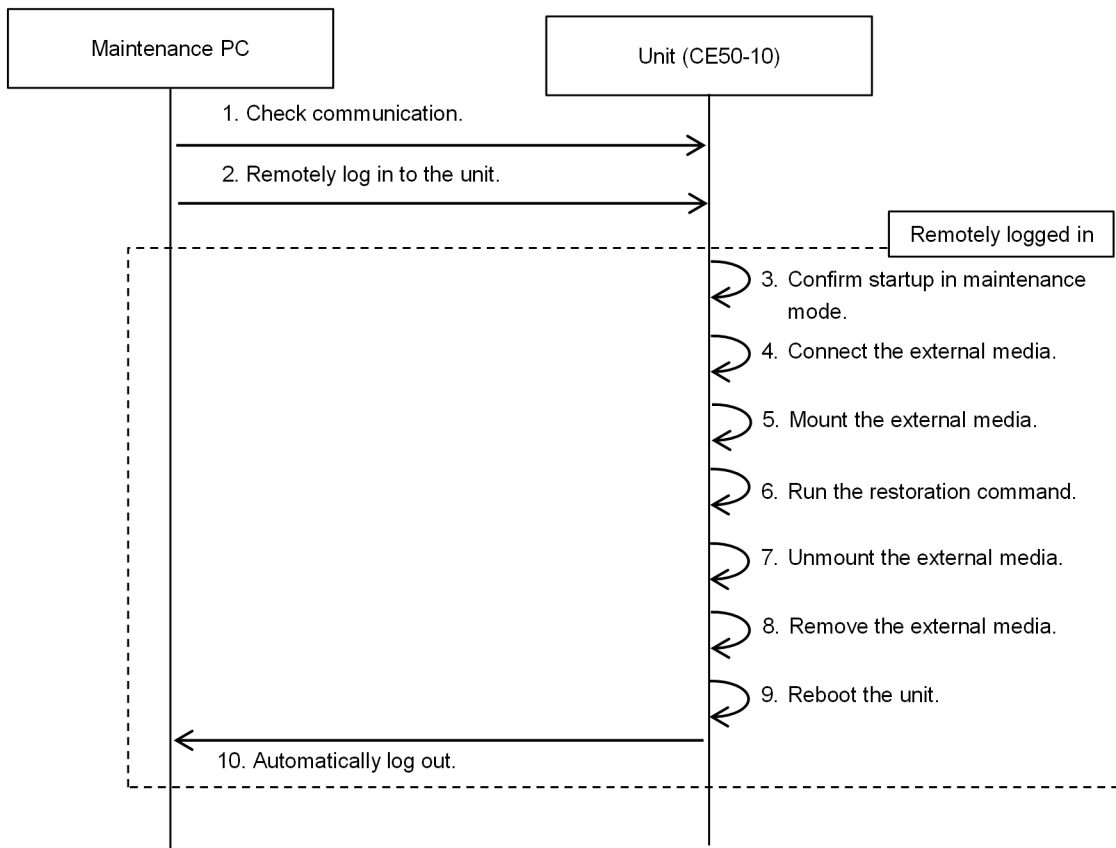
(a) Preparation

- Change the OS operation mode of the unit from normal mode to maintenance mode.
- The time required to restore data from a backed up file is approximately 30 seconds per GB. If files are to be verified, additional time (approximately 30 seconds) is required. More time might be required depending on the transfer rate of the external media.

(b) Operation procedure

Log in to the unit to be restored, and then run the restoration command.

Figure 5–24: Flow of restoration steps in configuration No. 3
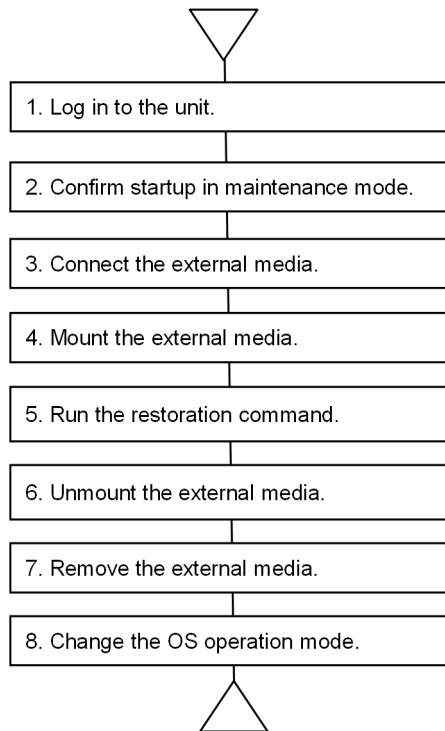
1. Log in to the unit.

   Remotely log in to the unit as a user who can run the `sudo` command.

   Example: When the user name is `edgeadm`

   ```
   login: edgeadm
   Password: *******
   ```

2. Confirm that the OS operation mode is set to maintenance mode.

   Run the `showecmode` command to confirm that the **bold underlined parts** are displayed as follows.

   ```
   $ sudo showecmode
   Current  : Maintenance mode
   Next     : Maintenance mode
   $
   ```

3. Connect the external media.

4. Mount the external media on `/mnt/ecbackup_data`.

   ```
   $ sudo mount < external-media> /mnt/ecbackup_data
   ```

5. Run the restoration command.

Run the `ecrestore` command to save the backup files from the external media to the unit. The following example shows how to run the `ecrestore` command.

- When the restoration menu appears, enter `1` (see the underlined part), and then press the **Enter** key to start restoration.

```
$ sudo ecrestore
Please select a restore mode.
1. Restore from external media
2. Restore from maintenance PC
q. quit
> 1                                    <- Restore from external media.
```

- When restoration starts, a list of directories containing backup files stored in the external media appears. Enter the number of the directory to be restored (see the underlined part), and then press the **Enter** key.

```
Backup directory list:
1. ecbackup_20210525101010
q. quit
> 1                                    <- Directory to be restored
```

- The restored file name and processing progress and time are displayed. Then, a message asking you whether you want to verify the restored files appears. Enter `y` to verify the files, or enter `N` to skip the verification.

```
Making partitions finished
Restoring: 20210525101010_sda8_01.gz
31MiB 0:00:01 [16.1MiB/s] [====>                    ] 25% ETA 0:00:02
Will you verify restored area(y / N)?N  <- Whether to verify files
Finished: 20210525101010_sda8_01.gz

(snip)
Successfully completed
```

- After running the command, wait for the command to terminate, displaying the `Successfully complete` message.

  If the command terminates displaying a message other than `Successfully completed`, the restoration processing has been interrupted due to an error. Take corrective action against the error, and then rerun the restoration command.

6. Unmount the external media from the unit

   After restoration finishes, unmount the connected external media from the unit.

```
$ sudo umount /mnt/ecbackup_data
```

7. Remove the external media from the unit.

8. Change the OS operation mode to normal mode.

   To change the OS operation mode to normal mode, see 5.14.4 Changing maintenance mode to normal mode.

5.15.5 Updating the OS

Use this function when you need to update the OS because, for example, measures must be taken for security threats or new functions are required. Only OSs supplied by Hitachi for CE50-10 can be used.

(1) Overview of the active area and inactive area

Two partitions in the unit are assigned to system area 1 and system area 2 (device file names: `/dev/sda2` and `/dev/sda3`). Each system area stores image data of the OS.

When the unit starts, either system area is activated to boot the unit. The system area that is active when the unit starts is called *active area*. The system area that is inactive when the unit starts is called *inactive area*.

When replacing the OS of the unit, update the OS in the inactive area, and then perform the operation to change the inactive area to the active area the next time the unit starts.

(2) Note

If an error is detected during the execution of the `ecosupdate` command, the active area is not changed. If an error is detected while the active area is being changed, the OSs in both areas might be placed in an inactive state. In this case, you need to eliminate the cause of the error by referring to the error message, and then rerun the command.

(3) Updating the OS in configuration No. 1

The following describes the procedure for updating the OS of the unit with the OS file in the external media connected to the unit. You can perform this operation in normal mode or maintenance mode. The following describes the operation procedure in normal mode.

(a) Preparation

- Save the following OS files currently stored in the unit, to the external media.

  OS file: `osprog_base.zip`

  OS version information file: `OSverinfo`

- Stop online application operations on the unit.

(b) Operation procedure

Use the maintenance PC to remotely log in to the target unit for updating the OS, and then run the OS update command.

Figure 5–25: Flow of OS update steps in configuration No. 1
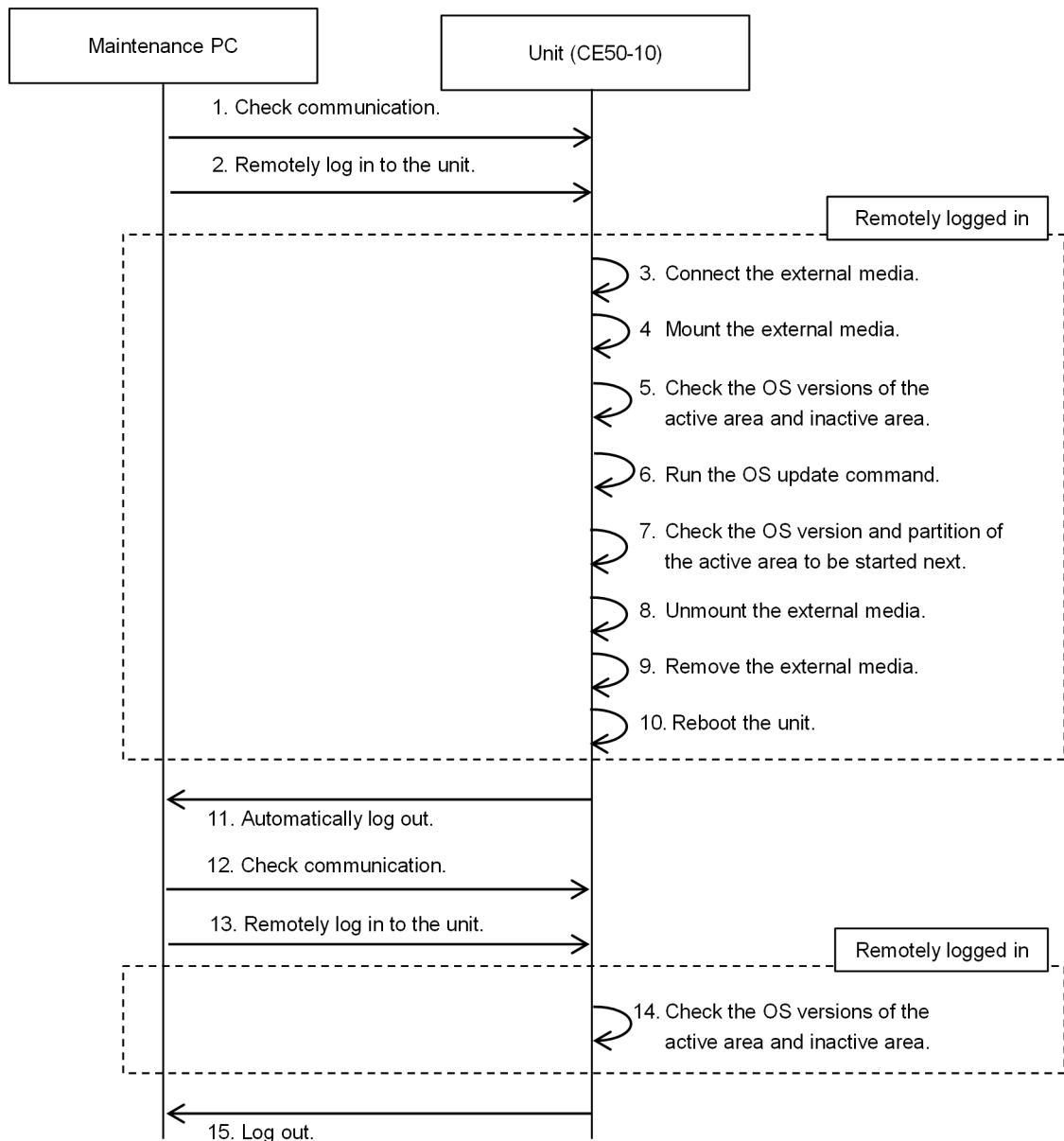
1. Check the communication between the maintenance PC and the unit.

   Run the `ping` command to confirm that the maintenance PC can communicate with the unit.

   ```
   $ ping IP-address-of-the-target-unit
   ```

2. Remotely log in to the unit from the maintenance PC.

   Remotely log in to the unit as a user who can run the `sudo` command.

   Example user name: `edgeadm`

   ```
   login: edgeadm
   Password: *******
   ```

3. Connect the external media.

4. Mount the external media on a path (for example, `/mnt/osupdate`).

   ```
   $ sudo mount external-media /mnt/osupdate
   ```

5. Run the version display command to check the OS versions of the active area and inactive area.

Run the `rxversion` command to check the device file names and OS versions for the active area and inactive area (see the **bold underlined parts**).

```
$ sudo rxversion
<Inactive>(/dev/sda2)
CTRL-EDGEN-IMG  model-name  version-information
<Active><Running>(/dev/sda3)
CTRL-EDGEN-IMG  model-name  version-information
<BIOS>
version-information
<RAS MCU F/W>
<version information>
<TPM>
<version information>
$
```

6. Run the OS update command.

Run the `ecosupdate` command to update the OS in the inactive area and switch the system area that will be the active area the next time the unit starts to the area containing the updated OS.

```
$ sudo ecosupdate /mnt/osupdate
```

7. Check the OS version and partition of the active area to be started next.

Run the `rxosenable` command with the `-p` (next startup area display) option specified. Then, confirm that the partition to be started next has changed to the current inactive area, and the OS version of that inactive area is updated (see the **bold underlined parts**).

```
$ sudo rxosenable -p
OS(version-number) is enabled. (/dev/sda2)
```

8. Unmount the external media from the unit.

After restoration finishes, unmount the connected external media from the unit.

```
$ sudo umount /mnt/osupdate
```

9. Remove the external media from the unit.

10. Reboot the unit.

```
$ sudo reboot
```

11. (No user operation required) Automatically log out from the unit.

Wait for the system to start.

12. Check the communication between the maintenance PC and the unit.

Run the `ping` command to confirm that the maintenance PC can communicate with the unit.

```
$ ping IP-address-of-the-target-unit
```

13. Remotely log in to the unit from the maintenance PC.

Remotely log in to the unit.

Example user name: `edgeadm`

```
login: edgeadm
Password: *******
```

14. Run the version display command to check the OS versions of the active area and inactive area.

Run the `showecmode` command to confirm that the OS operation mode is `Normal` mode (see the **bold underlined parts**).

```
$ sudo showecmode
Current  : Normal mode
Next     : Normal mode
$
```

Then, run the `rxversion` command to check the device file names and OS versions for the active area and inactive area (see the **underlined parts**). In this example, confirm that the device file name of the active area is `/dev/sda2`.

```
$ sudo rxversion
<Active><Running>(/dev/sda2)
CTRL-EDGEN-IMG  model-name  version-information
<Inactive>(/dev/sda3)
CTRL-EDGEN-IMG  model-name  version-information
<BIOS>
version-information
<RAS MCU F/W>
version-information
<TPM>
version-information
$
```

15. Log out from the unit.

```
$ exit
```

(4) Updating the OS in configuration No. 2

The following describes the procedure for updating the OS of the unit with the OS file in the maintenance PC connected to the unit. You can perform this operation in normal mode or maintenance mode. The following describes the operation procedure in normal mode.

(a) Preparation

- Save the OS file currently stored in the unit, to the maintenance PC.

- Stop online application operations on the unit.

- Stop the unit, and then connect it with the maintenance PC by using an Ethernet cable.
  If necessary, disconnect other devices from the unit.

(b) Operation procedure

Use the maintenance PC to remotely log in to the target unit for updating the OS, and then run the OS update command.

Figure 5–26: Flow of OS update steps in configuration No. 2
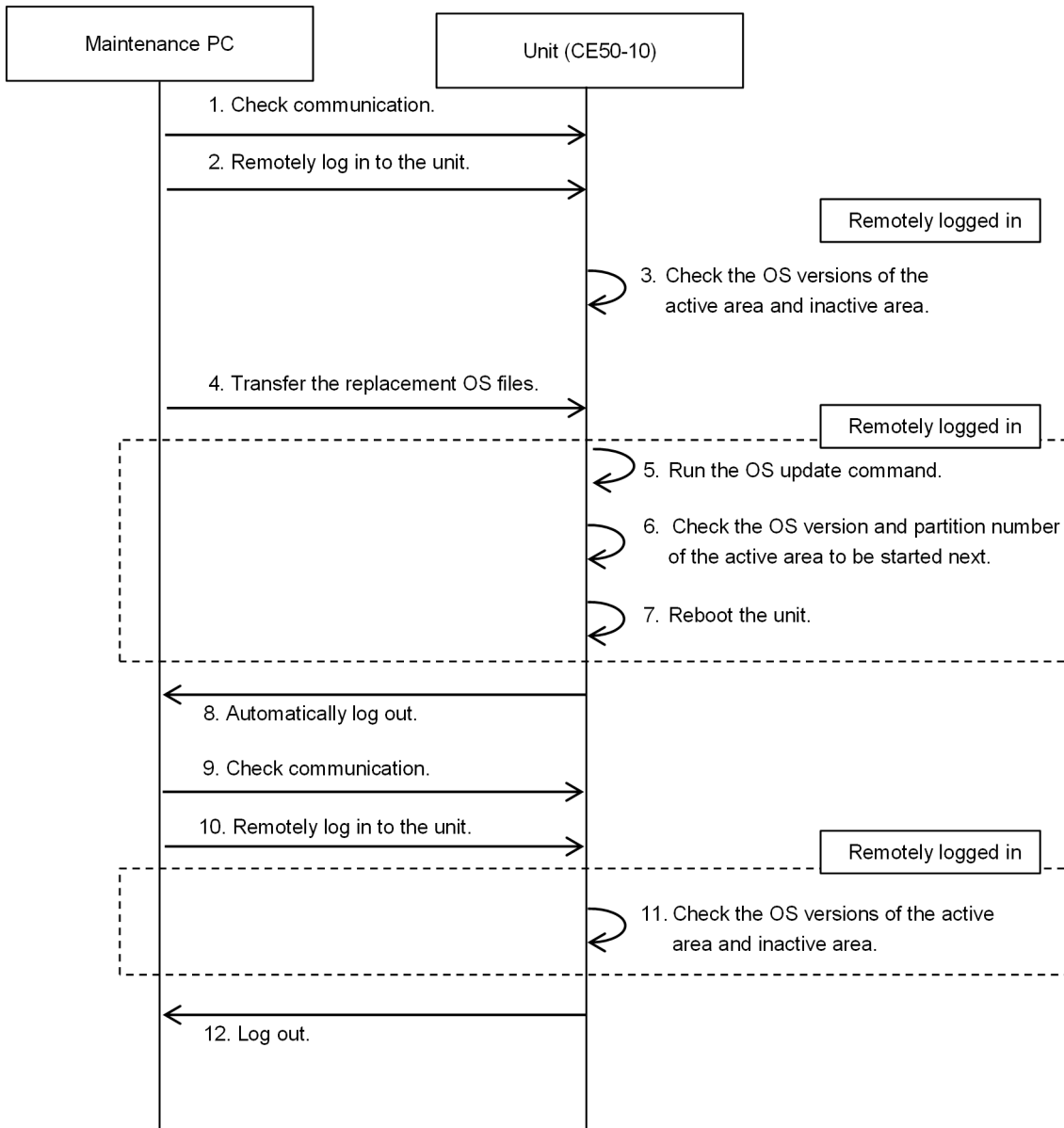
1. Check the communication between the maintenance PC and the unit.

   Run the `ping` command to confirm that the maintenance PC can communicate with the unit.

   ```
   $ ping IP-address-of-the-target-unit
   ```

2. Remotely log in to the unit from the maintenance PC.

   Remotely log in to the unit as a user who can run the `sudo` command.

   Example user name: `edgeadm`

   ```
   login: edgeadm
   Password: *******
   ```

3. Run the version display command to check the OS versions of the active area and inactive area.

   Run the `rxversion` command to check the device file names and OS versions for the active area and inactive area (see the **bold underlined parts**).

   ```
   $ sudo rxversion
   <Active><Running>(/dev/sda3)
   ```

```
CTRL-EDGEN-IMG   model-name   version-information
<Inactive>(/dev/sda2)
CTRL-EDGEN-IMG   model-name   version-information
<BIOS>
version-information
<RAS MCU F/W>
version-information
<TPM>
version-information
$
```

4. Send the update files from the maintenance PC to a path on the unit (for example, `/mnt/osupdate`).

  - Files to be sent
    OS file: `osprog_base.zip`
    OS version information file: `OSverinfo`

  - Destination directory: `/mnt/osupdate`

  - When using Tera Term
    Click **File**, and then **SSH SCP** to display the Secure File Copy screen.
    In the bottom of the screen, enter the path to the backup file for **From**, and enter the path to the save destination for **To**.
    Click the **Receive** button.

  - When using the `scp` command
    Run the following command.

    ```
    $ sudo scp user-name@IP-address:file-path /mnt/osupdate
    ```

5. Run the OS update command.
   Run the `ecosupdate` command to update the OS in the inactive area and switch the system area that will be the active area the next time the unit starts to the area containing the updated OS.

   ```
   $ sudo ecosupdate /mnt/osupdate
   ```

6. Check the OS version and partition of the active area to be started next.
   Run the `rxosenable` command with the `-p` (next startup area display) option specified. Then, confirm that the partition to be started next has changed to the current inactive area, and the OS version of that inactive area is updated (see the **bold underlined parts**).

   ```
   $ sudo rxosenable -p
   OS(version-number) is enabled. (/dev/sda2)
   ```

7. Reboot the unit.

   ```
   $ sudo reboot
   ```

8. (No user operation required) Automatically log out from the unit.
   Wait for the system to restart.

9. Check the communication between the maintenance PC and the unit.
   Run the `ping` command to confirm that the maintenance PC can communicate with the unit.

   ```
   $ ping IP-address-of-the-target-unit
   ```

10. Remotely log in to the unit from the maintenance PC.
    Remotely log in to the unit.
    Example user name: `edgeadm`

    ```
    login: edgeadm
    Password: *******
    ```

11. Run the version display command to check the OS versions of the active area and inactive area.
    Run the `showecmode` command to confirm that the OS operation mode is `Normal` mode (see the **bold underlined parts**).

```
$ sudo showecmode
Current  : Normal mode
Next     : Normal mode
$
```

Then, run the `rxversion` command to check the device file names and OS versions for the active area and inactive area (see the **bold underlined parts**). In this example, confirm that the device file name of the active area is `/dev/sda2`.

```
$ sudo rxversion
<Active><Running>(/dev/sda2)
CTRL-EDGEN-IMG  model-name  version-information
<Inactive>(/dev/sda3)
CTRL-EDGEN-IMG  model-name  version-information
<BIOS>
version-information
<RAS MCU F/W>
version-information
<TPM>
version-information
$
```

12. Log out from the unit.

```
$ exit
```

(5) Updating the OS in configuration No. 3

The following describes the procedure for updating the unit OS with the OS file in the external media connected to the unit. You can perform this operation in normal mode or maintenance mode. The following describes the operation procedure in normal mode.

(a) Preparation

- Save the following OS files currently stored in the unit, to the external media.

  OS file: `osprog_base.zip`

  OS version information file: `OSverinfo`

- Stop online application operations on the unit.

(b) Operation procedure

Log in to the target unit for updating the OS, and then run the OS update command.

Figure 5–27: Flow of OS update steps in configuration No. 3

```
                      ▽

  ┌─────────────────────────────────┐
  │ 1.  Log in to the unit.          │
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 2.  Connect the external media.  │
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 3.  Mount the external media.    │
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 4.  Check the OS versions of the │
  │     active area and inactive area.│
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 5.  Run the OS update command.   │
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 6.  Check the OS version and     │
  │     partition number of the active│
  │     area to be started next.     │
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 7.  Unmount the external media.  │
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 8.  Remove the external media.   │
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 9.  Reboot the unit.             │
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 10. Log out.                     │
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 11. Log in to the unit.          │
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 12. Check the OS versions of the │
  │     active area and inactive area.│
  └─────────────────────────────────┘
  ┌─────────────────────────────────┐
  │ 13. Log out.                     │
  └─────────────────────────────────┘

                      △
```

1. Log in to the unit.

   Log in to the unit as a user who can run the `sudo` command.

   Example user name: `edgeadm`

   ```
   login: edgeadm
   Password: *******
   ```

2. Connect the external media.

3. Mount the external media on a path (for example, `/mnt/osupdate`).

   ```
   $ sudo mount external-media /mnt/osupdate
   ```

4. Run the version display command to check the OS versions of the active area and inactive area.

   Run the `rxversion` command to check the device file names and OS versions for the active area and inactive area (see the **bold underlined parts**).

```
$ sudo rxversion
<Inactive>(/dev/sda2)
CTRL-EDGEN-IMG  model-name  version-information
<Active><Running>(/dev/sda3)
CTRL-EDGEN-IMG  model-name  version-information
<BIOS>
version-information
<RAS MCU F/W>
version-information
<TPM>
version-information
$
```

5. Run the OS update command.

Run the `ecosupdate` command to update the OS in the inactive area and switch the system area that will be the active area the next time the unit starts to the area containing the updated OS.

```
$ sudo ecosupdate /mnt/osupdate
```

6. Check the OS version and partition of the active area to be started next.

Run the `rxosenable` command with the `-p` (next startup area display) option specified. Then, confirm that the partition to be started next has been changed to the current inactive area, and the OS version of that inactive area is updated (see the **bold underlined parts**).

```
$ sudo rxosenable -p
OS(version-number) is enabled. (/dev/sda2)
```

7. Unmount the external media from the unit.

After restoration finishes, unmount the connected external media from the unit.

```
$ sudo umount /mnt/osupdate
```

8. Remove the external media from the unit.

9. Reboot the unit.

```
$ sudo reboot
```

10. (No user operation required) Automatically log out from the unit.

Wait for the system to restart.

11. Log in to the unit.

Log in to the unit.

Example user name: `edgeadm`

```
login: edgeadm
Password: *******
```

12. Run the version display command to check the OS versions of the active area and inactive area.

Run the `showecmode` command to confirm that the OS operation mode is `Normal mode` (see the **bold underlined parts**).

```
$ sudo showecmode
Current  : Normal mode
Next     : Normal mode
$
```

Then, run the `rxversion` command to check the device file names and OS versions for the active area and inactive area (see the **bold underlined parts**). In this example, confirm that the device file name of the active area is `/dev/sda2`.

```
$ sudo rxversion
<Active><Running>(/dev/sda2)
CTRL-EDGEN-IMG  model-name  version-information
<Inactive>(/dev/sda3)
CTRL-EDGEN-IMG  model-name  version-information
<BIOS>
version-information
<RAS MCU F/W>
version-information
<TPM>
```

```
version-information
$
```

13. Log out from the unit.

```
$ exit
```

5.16 Watchdog timer

Watchdog timer (*WDT*) is a function that monitors the execution times of the OS and processes. If one of the execution times exceeds its predefined time limit (timeout), WDT interprets it as a fault and restarts the unit. A function that monitors whether the OS is properly working is called a *hardware WDT*. A function that monitors whether the system daemon and application program processes are properly working is called a *software WDT*.

Figure 5–28: Operation states of the unit and when the hardware WDT and software WDT are active

Turn on the power to the CPU.

BIOS starts.

The boot loader starts.

Hardware WDT (active)

The OS starts.

A process starts.

Online operation   Software WDT (active)

Shutdown or Restart

Turn off the power to the CPU.
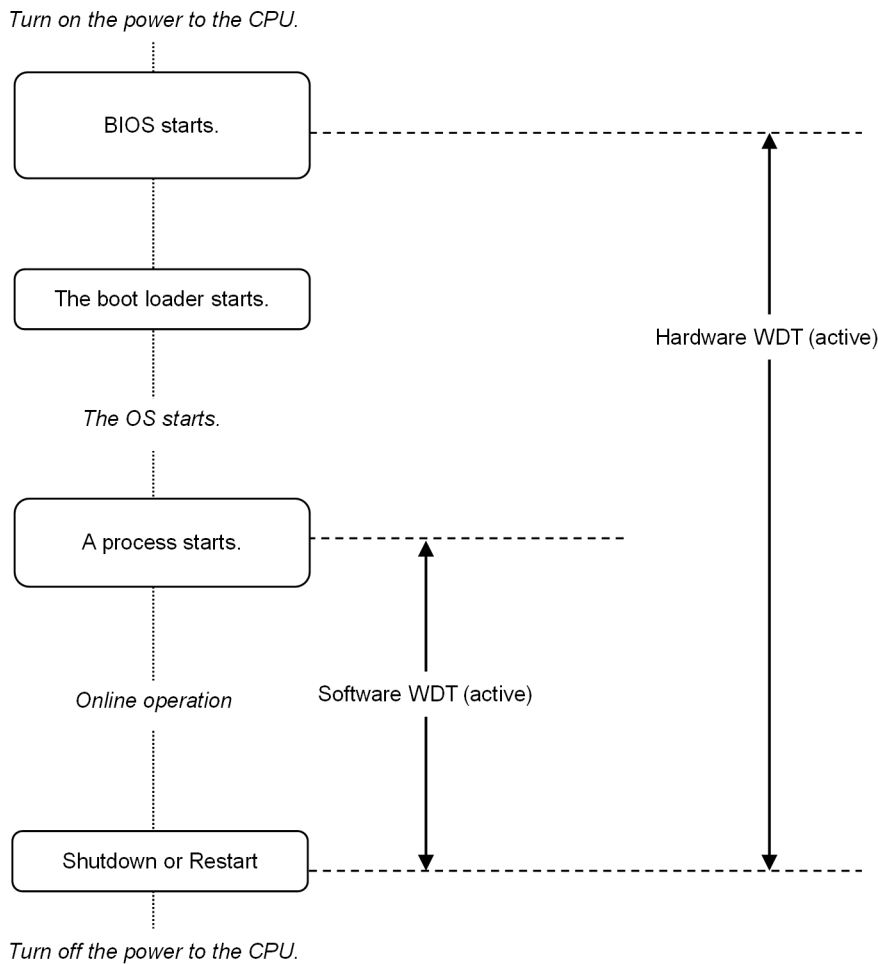
The following shows the interfaces used for operating the hardware WDT and software WDT.

Table 5–20: WDT operations and interfaces

Classification	Operation details	Interface name
Hardware WDT	Temporarily stop and restart operation.	`wdtctl` command
	Display the operation status.	`wdtstat` command
	Forcibly restart the unit.	`force_restart` command `force_restart` library
Software WDT	Start and stop.	`swdt.conf` definition file
	Temporarily stop the operation.	`swdt_stop` command
	Restart the temporarily stopped operation.	`swdt_start` command

Classification	Operation details	Interface name
Software WDT	Display the operation status.	`swdt_stat` command

5.16.1 swdt.conf definition file

Any changes made in this definition file are applied when the unit starts the next time.

If this file does not exist or a value outside the specifiable range is specified, monitoring with all default parameters is performed. If the same symbol is specified more than once, the last defined value takes effect.

(1) File

`/hitachi/etc/swdt.conf`

(2) Setting items

Table 5–21: Setting items

Symbol name	Default	Description of the definition name
`INLOOP`	`ON`	Specify whether to enable or disable the software WDT. You can specify `ON` (enable) or `OFF` (disable).
`TIMEOUT`	`15`	Specify the monitoring timeout value (seconds) in the range from 5 to 60.
`PANIC`	`ON`	Select `ON` or `OFF` to specify the operation to be performed if a fault is detected. `ON`: Collect a memory dump, and then restart the CPU. `OFF`: Restart the CPU without collecting a memory dump.
`CORE`	`4`	Specify the number of cores to be monitored in the range from 1 to 4. The default reboots the unit if processes stop after the software WDT time elapsed in four cores. Specify `1` to forcibly reboot the unit when an in-loop is detected in one core.

(3) Definition method

Enter the definitions according to the following format. If the symbol name or definition value is not correct, the default value is used for operation.

symbol-name_definition-value
　_: At least one space or tab. Any lines that begin with a hash mark (#) are ignored.

5.17 Checking the CPU usage ratio

Use the `vmstat` command to check the CPU usage ratio for the unit.

Run the command in the following format.

```
$ vmstat measurement-period(unit: second) measurement-count
```

Execution example:

```
$ vmstat 10 3
```

The following shows an example of output of the command.

The values in the first record (on the first line) indicate the average values from the time the OS starts to the time the command is run. The values in the second and subsequent records indicate the average values between measurement periods. In the execution example, the values in the second and subsequent records are the average values for the latest 10 seconds.

The sum of the values of `us` and `sy` indicates the CPU usage ratio. For example, the first record in the output example indicates that the CPU usage ratio from the time the OS started to the time the command was run is 17 + 3 = 20%.

For details about each item, see Table 5-22.

```
procs ----------memory---------- ---swap--- ----io---- -system- -----cpu-----
 r  b  swpd free     buff  cache  si   so    bi   bo    in   cs  us sy id wa st
 0  0  0    7500852 21692 160028  0    0     12   0     69   34  17 3  80 0  0
 0  0  0    7500852 21692 160028  0    0     12   0     69   34  0  1  99 0  0
```

Table 5–22: List of items displayed by the vmstat command

Item	Meaning
r	Number of processes that are running or that are in the executable state
b	Number of processes that are in an uninterruptable sleep state
swpd	Virtual memory size being used
free	Available memory size
buff	Memory size being used as the buffer
cache	Memory size being used as the cache
si	Size of memory that is written back from a disk as a swap (per second)
so	Size of memory that is written to a disk as a swap (per second)
bi	Read size from a block device (per second)
bo	Write size to a block device (per second)
in	Number of interruptions (per second)
cs	Number of times context switching occurs (per second)
us	Ratio of the execution time of a user process (other than the kernel code)
sy	Ratio of the execution time of the system (kernel code)
id	Ratio of the idle time during which the CPU is not used (= 100% - `us` - `sy` - `wa` -`st`)
wa	Ratio of the I/O wait time
st	Ratio of the time for which usage is restricted by the virtual machine For the CE50-10, `0` is always displayed.

5.18 Command reference

This section describes the commands supported for this unit.

Table 5–23: List of commands

No.	Command name	Description	Reference
1	ecmodeset	Set the next OS startup mode.	5.18.1 ecmodeset
2	showecmode	Display the OS startup mode.	5.18.2 showecmode
3	ecbackup	Back up data.	5.18.3 ecbackup
4	ecrestore	Restore backup data.	5.18.4 ecrestore
5	ecosupdate	Update the OS in the inactive area.	5.18.5 ecosupdate
6	rxosenable	Change the active OS area.	5.18.6 rxosenable
7	rxversion	Display OS version information.	5.18.7 rxversion
8	disklchk	Diagnose the SSD life.	5.18.8 disklchk
9	fsconfchk	Check mount definitions.	5.18.9 fsconfchk
10	showkxmessage	Display extracted KX messages.	5.18.10 showkxmessage
11	eclogsave	Save overall maintenance information.	5.18.11 eclogsave
12	rasledctl	Control lighting of the RAS indicator AP lamp.	5.18.12 rasledctl
13	wdtctl	Enable and disable hardware WDT.	5.18.13 wdtctl
14	wdtstat	Check the monitoring status of hardware WDT.	5.18.14 wdtstat
15	force_restart	Forced restart function	5.18.15 force_restart
16	swdt_start	Restart the software WDT.	5.18.16 swdt_start
17	swdt_stop	Temporarily stop the software WDT.	5.18.17 swdt_stop
18	swdt_stat	Check the monitoring status of software WDT.	5.18.18 swdt_stat
19	usbctl	Connect or disconnect USB devices.	5.18.19 usbctl

5.18.1 ecmodeset

<Name>

 ecmodeset - Set the next OS startup mode.

<Format>

 ecmodeset [-enable | -disable]

<Description>

 This command changes the next OS startup mode.

<Options>

- -enable

 Sets maintenance mode as the next OS startup mode.

- -disable

 Sets normal mode as the next OS startup mode.

<Display examples>

 The following is displayed when maintenance mode is set as the next OS startup mode.

```
$ sudo ecmodeset -enable
Set next boot: Maintenance mode
$
```

The following is displayed when normal mode is set as the next OS start mode.

```
$ sudo ecmodeset -disable
Set next boot: Normal mode
$
```

<Diagnosis>

For the exit code, 0 is returned if the status is normal and 1 is returned if an error is detected. Table 5–24: List of ecmodeset command error messages below shows error messages that are output when an error is detected.

Table 5–24: List of ecmodeset command error messages

No.	Error message	Description
1	`Usage: ecmodeset [-enable	-disable]`	The specified argument is invalid.
2	`Failed to set next boot: Maintenance mode`	An attempt to set maintenance mode failed.
3	`Failed to set next boot: Normal mode`	An attempt to set normal mode failed.

5.18.2 showecmode

<Name>

showecmode - Display the OS operation mode.

<Format>

showecmode

<Description>

This command displays the current OS startup mode and the next OS startup mode.

<Display format>

```
Current  : OS-startup-mode
Next     : OS-startup-mode
```

Notes

- If normal mode is set, Normal mode is displayed.
- If maintenance mode is set, Maintenance mode is displayed.

If an attempt to collect information failed, Unknown is displayed. If Unknown is displayed, a fault is likely to exist in the SSD. In this case, replace the unit.

<Options>

No options need to be specified. Any specified options are ignored.

<Display example>

The command displays the current OS startup mode and the next OS startup mode.

The following shows an example of when the current mode is maintenance mode and the next startup mode is normal mode.

```
$ sudo showecmode
Current  : Normal mode
Next     : Maintenance mode
$
```

<Diagnosis>

For the exit code, 0 is returned if the status is normal and 1 is returned if an error is detected.

An error message is not output.

5.18.3 ecbackup

<Name>

    `ecbackup` - Back up data.

<Format>

    `ecbackup`

<Description>

    This command backs up data.

    When you run the command, the system waits for you to enter information. Perform backup according to the menu.

<Options>

    No options need to be specified. Any specified options are ignored.

<Execution example>

1. Run the `ecbackup` command.

   When you run the command, the menu appears. Then, the prompt character > appears and the system waits for you to enter information.

   ```
   $ sudo ecbackup
   Please select a backup mode.
   1. Back up to external media
   2. Back up to maintenance PC
   q. quit
   >
   ```

   The command processing proceeds according to the value you entered.

2. To back up data to the external media, enter `1`, and then press the **Enter** key.

   The screen is displayed as follows.

   ```
   Partition info backup started.                                    ...(a)
   Partition Info backup finished.                                   ...(a)
   Backup directory: /mnt/ecbackup_data/ecbackup_20210525101010      ...(b)
   Backup targets: /dev/sda8 /dev/sda9 /dev/sda10 /media/etc          ...(c)
   Partition /dev/sda8 backup start.                                 ...(d)
   31MiB 0:00:01 [16.1MiB/s] [====>              ] 25% ETA 0:00:02    ...(e)
   Will you verify backup files(y / N)? y                            ...(f)
   Verifying:20210525101010_sda8_01.gz                               ...(f)
   The file and the partition doesn't match. Retry?(y / N)y          ...(g)
   31MiB 0:00:01 [16.1MiB/s] [====>              ] 25% ETA 0:00:02    ...(e)
   Will you verify backup files(y / N)? y                            ...(f)
   Verifying: 20210525101010_sda8_01.gz                              ...(f)
   Finished:20210525101010_sda8_01.gz: xxx,xxx,xxx bytes             ...(h)

   (snip)

   Directory /media/etc backup start.                               ...(i)
   Will you verify backup files(y / N)? y                            ...(f)
   Verifying:20210525101010_etc_01.gz                                ...(f)
   Finished:20210525101010_sda8_01.gz: xxx,xxx,xxx bytes             ...(h)
   Successfully completed                                           ...(j)
   ```

Table 5–25: Description of the screen after backup to external media started

Item	Display	Description

(a)	`Partition info backup started.`
	
	`Partition Info backup finished.`
		This message indicates that backup of partition information started or terminated.

(b)	`Backup directory: /mnt/ ecbackup_data/ ecbackup_20210525101010`	The backup destination directory. The directory name is automatically created based on the date and time when the backup started. The example shows that the backup started at 10:10:10 on May 25, 2021.

Item	Display	Description
(c)	`Backup targets: /dev/ sda8 /dev/sda9 /dev/ sda10 /media/etc`	The partitions or directories to be backed up
(d)	`Partition /dev/sda8 backup start.`	The partition in which backup starts
(e)	`31MiB 0:00:01 [16.1MiB/s] [====> ] 25% ETA 0:00:02`	The storage status of the backup file being created in the external media. The following are displayed from left to right: • Capacity of the partition stored in the backup file • Elapsed time • Data transfer rate (amount of transferred data/second) • Progress bar • Progress rate (percentage display) • Estimated remaining time (required for processing) The displayed progress rate might slightly exceed 100%. The progress bar and the progress rate indicate the following values: Capacity of the partition stored in the current backup file ÷ (*partition size - capacity of partitions already backed up in the backup file*) **x** 100 (%) If the size of the backup file exceeds 1 GB, the saving of the backup file ends, and the progress bar and the progress rate indicate a value lower than 100%. The data that has not been backed up will be recorded in the next backup file.

(f)	`Will you verify backup files(y / N)? y`
	
	`Verifying:20210525101010_s da8_01.gz`
	
	`Will you verify backup files(y / N)? y`
	
	`Verifying: 20210525101010_sda8_01.gz`
		This message asks you whether you want to verify that the backup files are saved normally.
		
		If you enter `y`, the saved backup file is compared with the target partition or directory to confirm that they match.
		
		If you enter `N`, the message in (h) appears, and then creation of the next backup file starts.

(g)	`The file and the partition doesn't match. Retry?(y / N)y`	If the verification in (f) shows that the backup file was not saved normally, this message appears, asking you whether you want to rerun the backup. If you enter `y`, the message in (f) appears again.
(h)	`Finished:20210525101010_sd a8_01.gz: xxx,xxx,xxx bytes`	This message indicates that saving of the backup file finished. Information for (c) to (h) appears repeatedly for the partitions and directories that have not been backed up yet.
(i)	`Directory /media/etc backup start.`	The directory in which backup starts
(j)	`Successfully completed`	This message indicates that backup of all directories indicated in (c) finished.

3. To back up data to the maintenance PC, enter 2, and then press the **Enter** key.

The following screen appears.

```
Partition info backup started.                                    ...(a)
Partition Info backup finished.                                   ...(a)
Backup directory: /mnt/ecbackup_data/ecbackup_20210525101010      ...(b)
Backup targets: /dev/sda8 /dev/sda9 /dev/sda10 /media/etc          ...(c)
Partition /dev/sda8 backup start.                                 ...(d)
31MiB 0:00:01 [16.1MiB/s] [====>              ] 25% ETA 0:00:02    ...(e)
Will you verify backup files(y / N)? y                            ...(f)
```

```
Verifying:20210525101010_sda8_01.gz                              ...(f)
The file and the partition doesn't match. Retry?(y / N)y         ...(g)
31MiB 0:00:01 [16.1MiB/s] [====>              ] 25% ETA 0:00:02)  ...(e)
Will you verify backup files(y / N)? y                           ...(f)
Verifying: 20210525101010_sda8_01.gz                             ...(f)
Finished:/mnt/ebackup_data/ecbackup_20210525101010/
20210525101010_sda8_01.gz: xxx,xxx,xxx bytes                     ...(h)
Please get 20210525101010_sda8_01.gz. Finished? (y)              ...(k)

(snip)

Directory /media/etc backup start.                               ...(i)
Will you verify backup files(y / N)? y                           ...(f)
Verifying:20210525101010_etc_01.gz                               ...(f)
Finished:20210525101010_sda8_01.gz: xxx,xxx,xxx bytes            ...(h)
Please get 20210525101010_etc_01.gz. Finished? (y)               ...(k)
Successfully completed                                           ...(j)
```

Table 5–26: Description of the screen after backup to the maintenance PC started

Item	Display	Description
(a) to (j)	See Table 5–25: Description of the screen after backup to external media started.	See Table 5–25: Description of the screen after backup to external media started.

(k)	`Please get 20210525101010_sda8_01.gz. Finished? (y)`
	
	`Please get 20210525101010_etc_01.gz. Finished? (y)`
		If a message in `Please get` *file-name*`. Finished (y)?` format is output, a backup file with *file-name* is created under the directory indicated in (b). The example shows that `/mnt/ecbackup_data/ecbackup_20210525101010/20210525101010_sda8_01.gz` is created.
		
		If this message is output, transfer the `/mnt/ecbackup_data/`*file-name* file to the maintenance PC by using the `scp` command.
		
		After transferring the file, enter y, and then press the **Enter** key. Then, the file indicated by *file-name* is deleted and saving of the next backup file starts.
		
		If you press the **Enter** key without entering anything or enter a character other than y, the same message appears again and the system waits for you to enter information again.

4. Enter q, and then press the **Enter** key.

   The ecbackup command terminates.

   For details about running the command, see 5.15.3 Backing up storage data.

<Note>

1. If the command terminates abnormally while data is being backed up to the external media, temporary data in the process of being backed up might exist in the external media. If the command terminates abnormally, restart the unit, and then manually delete such data from the external media.

   The following describes how to delete the backup data from the external media after restarting the unit.

```
$ mount /dev/sdb1 /mnt/external
$ ls /mnt/external
ecbackup_YYYYMMDDHHMMSS   ecbackup_YYYYMMDDHHMMSS
```

   The backup work directory is displayed. For *YYYYMMDDHHMMSS*, a numeric value such as 20210525101010 is indicated as the date and time when the backup work was performed.

```
$ rm -rf /mnt/external/ecbackup_YYYYMMDDHHMMSS
$ umount /mnt/external
```

<Diagnosis>

   For the exit code, 0 is returned if the status is normal and 1 is returned if an error is detected. Table 5–27: List of ecbackup command error messages below shows error messages that are output when an error is detected.

Table 5–27: List of ecbackup command error messages

No.	Error message	Description	Action
1	`Backup failed.`	Backup was suspended due to an error.	Eliminate the cause of the error, and then rerun the command.
2	`ecbackup won't run on Normal mode.`	An attempt was made to run the `ecbackup` command in normal mode of the OS.	Change the mode to maintenance mode, and then run the command.
3	`/mnt/ecbackup_date doesn't have enough space.`	The `ecbackup_date` directory does not have the minimum required free space to save the backup file.	Use external media that has enough free space, or delete unnecessary files.
4	`ecbackup needs root privilege. Try 'sudo ecbackup'`	You need root privilege to run the `ecbackup` command.	Run the command by using the `sudo` command.
5	`Backup process haven't completed correctly.Retry? (y /N)`	An error occurred during the backup processing.	Press the **y** key to retry the backup processing. To stop the backup processing, press the **N** key.
6	`Backup aborted.`	Backup was canceled by a user operation.	None

5.18.4 ecrestore

<Name>

`ecrestore` - Restore backup data.

<Format>

`ecrestore`

<Description>

This command restores backup data.

When you run the command, the system waits for you to enter information. Perform restoration according to the menu.

<Options>

No options need to be specified. Any specified options are ignored.

<Display example>

1. Run the `ecrestore` command.

   When you run the `ecrestore` command, the menu appears. Then, the prompt character > appears and the system waits for you to enter information.

   ```
   $ sudo ecrestore
   Please select a restore mode.
   1. Restore from external media
   2. Restore from maintenance PC
   q. quit
   >
   ```

   The command processing proceeds according to the value you entered

2. To restore data from the external media, enter `1`, and then press the **Enter** key.

   This selects restoration from external media, and then the screen is displayed as follows.

   ```
   Backup directory list:
   1. ecbackup_20210525101010
   q. quit
   >
   ```

   The command processing proceeds according to the value you entered.

3. Enter `1`, and then press the **Enter** key.

Restoration starts from the selected data, and then the screen is displayed as follows.

```
Making partitions finished.                                        ...(a)
OK
Restoring from extra media.                                        ...(b)
Restoring: 20210525101010_sda8_01.gz  (start=0 size=123456)        ...(c)
31MiB 0:00:01 [16.1MiB/s] [====>            ] 25% ETA 0:00:02       ...(d)
Will you verify restored area(y / N)?y                             ...(e)
Verifying: 20210525101010_sda8_01.gz  (start=0 size=123456)        ...(e)
The file and the partition doesn't match. Retry?(y / N)            ...(f)
Restoring: 20210525101010_sda8_01.gz  (start=0 size=123456)        ...(c)
31MiB 0:00:01 [16.1MiB/s] [====>            ] 25% ETA 0:00:02       ...(d)
Finished: 20210525101010_sda8_01.gz                               ...(g)

(snip)

Will you verify restored directory(y / N)?                         ...(e)
Verifying: 20210525101010_etc_01.tgz                              ...(e)
The file and the directory doesn't match. Retry?(y / N)            ...(f)
Finished: 20210525101010_etc_01.tgz                               ...(g)
Successfully completed                                             ...(h)

$
```

Table 5–28: Description of the screen after restoration from external media started

Item	Display	Description
(a)	`Making partitions finished.OK`	This message appears when initialization of a partition finished.
(b)	`Restoring from extra media.`	This message appears when restoration from the external media starts.
(c)	`Restoring: 20210525101010_sda8_01.gz` `(start=0 size=123456)`	This message appears when restoration of the indicated backup file starts.
		If the restoration destination is a partition, the range to be restored is displayed. Specifically, the number of bytes from the beginning of the partition to the restoration start point is indicated for start=, and the size to be restored (unit: bytes) is indicated for size=.
(d)	`31MiB 0:00:01 [16.1MiB/s] [====>            ] 25% ETA 0:00:02`	The progress of restoration of the backup file.
		The following are displayed from the left to right:
		• Extended capacity
		• Elapsed time
		• Data transfer rate (amount of transferred data/second)
		• Progress bar
		• Progress rate (percentage display)
		• Estimated remaining time (required for processing)
		The displayed progress rate might slightly exceed 100%.
(e)	`Will you verify restored area(y / N)?y` `Verifying: 20210525101010_sda8_01.gz(start=0 size=123456)` `Will you verify restored directory(y / N)?` `Verifying: 20210525101010_etc_01.tgz`	This message asks you whether you want to verify that restoration to the partition has finished normally.
		If you enter y, the message in (f) appears. Then, the backup file is compared with the checksum of the target partition to confirm that they match.
		If you enter N, the message in (h) appears.
(f)	`The file and the partition doesn't match. Retry?(y / N)` `The file and the directory doesn't match. Retry?(y / N)`	This message appears if an error is detected as a result of the verification of restored data.
		If you enter y, the message in (c) appears and restoration of the same backup file starts.
		If you enter N, `Restore aborted.` is output to the standard output and the command terminates.

Item	Display	Description

(g)	`Finished: 20210525101010_sda8_0`
	`1.gz`
	`Finished: 20210525101010_etc_01`
	`.tgz`
		This message indicates that restoration of the relevant backup files finished normally.
		
		Messages (c) through (g) are displayed for all the files in the specified directory.

(h)	`Successfully completed`	This message indicates that restoration of all backup files finished normally.

4. To restore data from the maintenance PC, enter 2, and then press the **Enter** key.

This selects restoration from the maintenance PC, and then the following screen appears.

```
Making partitions finished.                                         ...(a)
OK
Restoring from maintenance PC.                                      ...(i)
Please send 20210525101010_sda8_01.gzto /mnt/ecbackup_data/. Finished? (y)...(j)
Restoring: 20210525101010_sda8_01.gz  (start=0 size=123456)        ...(c)
31MiB 0:00:01 [16.1MiB/s] [====>          ] 25% ETA 0:00:02        ...(d)
Will you verify restored area(y / N)?y                             ...(e)
Verifying: 20210525101010_sda8_01.gz  (start=0 size=123456)        ...(e)
The file and the partition doesn't match. Retry?(y / N)            ...(f)
Restoring: 20210525101010_sda8_01.gz  (start=0 size=123456)        ...(c)
31MiB 0:00:01 [16.1MiB/s] [====>          ] 25% ETA 0:00:02        ...(d)
Finished: 20210525101010_sda8_01.gz                               ...(g)

(snip)

Will you verify restored directory(y / N)?                        ...(e)
Verifying: 20210525101010_sda8_01.gz  (start=0 size=123456)        ...(e)
The file and the directory doesn't match. Retry?(y / N)           ...(f)
Finished: 20210525101010_etc_01.tgz                               ...(g)
Successfully completed                                            ...(h)
$
```

Table 5–29: Description of the screen after restoration from the maintenance PC started

Item	Display	Description
(a) to (h)	See Table 5–28: Description of the screen after restoration from external media started.	See Table 5–28: Description of the screen after restoration from external media started.
(i)	`Restoring from maintenance PC.`	This message indicates that restoration from the maintenance PC started.

(j)	`Please send 20210525101010_sda8_01`
	`.gzto /mnt/ecbackup_data/.  Finish`
	`ed? (y)`
		This message asks you to transfer the backup file.
		
		When this message appears, place the specified backup file in `/mnt/ecbackup_data`. After placing the file, enter `y`, and then press the **Enter** key to go to the next display.

5. Enter q, and then press the **Enter** key:

The `ecrestore` command terminates.

If you enter any other data, the prompt character (>) appears and the system waits for you to enter information again.

For details about running the command, see 5.15.4 Restoring backup data.

<Diagnosis>

For the exit code, 0 is returned if the status is normal and 1 is returned if an error is detected. Table 5–30: List of ecrestore command error messages below shows error messages that are output when an error is detected.

Table 5–30: List of ecrestore command error messages

No.	Error message	Description	Action
1	`Restore failed.`	Restoration failed due to an error.	Eliminate the cause of the error by referring to other error messages, and then rerun the command.

No.	Error message	Description	Action
2	`ecrestore won't run on Normal mode.`	An attempt was made to run the `ecrestore` command in normal mode of the OS.	Change the mode to maintenance mode, and then run the command.
3	`ecrestore needs root privilege. Try 'sudo ecbackup'`	You need root privilege to run the `ecrestore` command.	Run the command by using the `sudo` command.
4	*file-name* `is not found.`	The file necessary for restoration is not found.	Save the specified file in an appropriate location, and then rerun the command.
5	*file-name* `is broken.`	The specified file is corrupt.	Place the specified file again, and then rerun the command.
6	`Restore aborted.`	Restoration was canceled by the instruction of the user.	None
7	`Restore process haven't completed correctly. Retry? (y / N)`	The restore processing did not complete normally.	Press the **y** key to retry the restore processing. To stop the restore processing, press the **N** key.
8	`Backup directory is not found.`	The directory containing the backup file was not found in the external media used for restoration.	Connect the correct external media, and then rerun the command.

5.18.5 ecosupdate

<Name>

`ecosupdate` - Update the OS in the inactive area.

<Format>

`ecosupdate  [-h]  ` *directory-name*

<Description>

This command updates the OS in the inactive area of the unit with the OS update file in the specified directory. After the unit restarts, the inactive area with the updated OS is restarted as the active area. If you want to use an external media, mount it on the OS in advance. This command is run by using the `sudo` command.

Updating the OS in the inactive area is accomplished by overwriting the OS update file to the partition to which inactive area belongs.

After writing the file, the command verifies whether the data is correctly written by using the checksum of the partition. If the data is not correct, an error message is output.

<Options>

- `-h`

  Displays the help message.

- *directory-name*

  Name of the directory where the OS update file (`osprog_base.zip`) and the OS version information file (`OSverinfo`) are stored

<Display example>

`-h` option

```
$ sudo ecosupdate  -h
Usage:
 /hitachi/bin/ecosupdate -h
 /hitachi/bin/ecosupdate  <dir>

Options:
  -h  display this help message and exit
 <dir> directory name (ex. /tmp)
```

<Diagnosis>

For the exit code, 0 is returned if the status is normal and 1 is returned if an error is detected. Table 5–31: List of ecosupdate command error messages below shows error messages that are output when an error is detected.

Table 5–31: List of ecosupdate command error messages

No.	Error message	Description
1	Usage: /hitachi/bin/ecosupdate -h /hitachi/bin/ecosupdate <dir>	The specified argument is invalid. Revise the specified option, and then rerun the command.
2	ecosupdate: Directory not found.	The specified directory does not exist. Revise the specified directory path, and then rerun the command.
3	ecosupdate: Extracting root partition failed.	An attempt to extract the OS update file to the root partition failed. Rerun the command.
4	ecosupdate: OSverinfo is not found.	OSverinfo was not found. Store the file again, and then rerun the command.
5	ecosupdate: OSverinfo is broken.	OSverinfo is corrupted. Store the file again, and then rerun the command.
6	ecosupdate:OS update file is not found or broken.	osprog_base.tar was not found or is corrupted. Store the file again, and then rerun the command.
7	ecosupdate: Failed to save /hitachi/etc/ecosupdate/system<1|2>/boot.tgz	An attempt to save the boot partition file failed. Confirm that /hitachi/etc/ecosupdate/ is writable, and then rerun the command.
8	ecosupdate: Failed to save root partition to /dev/sda<2|3>.	An attempt to save the root partition failed. Rerun the command.
9	Backup for boot partition failed.	An attempt to back up the boot partition failed. Confirm that /hitachi/etc/ecosupdate/ is writable, and then rerun the command.
10	ecosupdate: ecosupdate needs root privilege. Try 'sudo ecosupdate'.	Running the command requires root privileges. Use sudo.
11	ecosupdate: OS update failed. Please re-try.	Processing of the ecosupdate command did not finish. The active area of the OS has not been changed. Eliminate the cause of the error, and then rerun the command.
12	ecosupdate: system,error. OS update failed.	Processing did not finish due to an unknown error. Restarting the OS might cause it to be unable to start. Eliminate the cause of the error, and then rerun the command.

5.18.6 rxosenable

<Name>

rxosenable - Change the active OS area.

<Format>

rxosenable [-h] [-p | -s | -e {2,3}]

<Description>

This command changes the system area to be started next.

\<Options\>

- `-h, --help`

  Displays the help message.

- `-p, --print`

  Displays the OS version and partition number of the system area to be started next (default).

- `-s, --switch`

  Changes the system area to be started next. This setting takes effect on and after the next startup.

- `-e {2,3}, --enable {2,3}`

  Starts the partition of the specified partition number (2 or 3) the next time and later.

\<Execution example\>

- `-s` option

```
$ sudo rxosenable
OS(01-01 [01]) is enabled. (/dev/sda2)
$ sudo rxosenable -s
switch done
$ sudo rxosenable
OS(01-02 [01]) is enabled. (/dev/sda3)
$
```

- `-e` option

```
$ sudo rxosenable
OS(01-01 [01]) is enabled. (/dev/sda2)
$ sudo rxosenable -e 3
enable done
$ sudo rxosenable
OS(01-02 [01]) is enabled. (/dev/sda3)
$
```

- `-h` option

```
$ sudo rxosenable -help
usage: rxosenable [-h] [-p | -s | -e {2,3}]

optional arguments:
  -h, --help            show this help message and exit
  -p, --print           Print enabled-OS version(default)
  -s, --switch          Switch the active-partition
  -e {2,3}, --enable {2,3}
                        Enable the partition 2/3
$
```

\<Diagnosis\>

For the exit code, 0 is returned if the status is normal and 1 is returned if an error is detected. Table 5–32: List of rxosenable command error messages below shows error messages that are output when an error is detected.

Table 5–32: List of rxosenable command error messages

No.	Error message	Description
1	`usage: rxosenable [-h] [-p	-s	-e {2,3}] rxosenable: error: unrecognized arguments: xxx`	The specified argument (*xxx*) is invalid.
2	`usage: rxosenable [-h] [-p	-s	-e {2,3}]rxosenable: error: argument -e/--enable: invalid choice: XX (choose from 2, 3)`	The specified partition number (*XX*) is invalid. Specify 2 or 3.

5.18.7 rxversion

<Name>

rxversion - Display OS version information.

<Format>

rxversion [--nodate]

<Description>

This command displays the OS versions (master CD versions) of the active and inactive areas, BIOS version, RAS MCU firmware version, and TPM version. These versions are specific to the product and differ from the Linux versions.

Run the command with the --nodate option to omit the display of the date parts ((8) and (11)) in the display format).

<Options>

- --nodate

  Omit the display of the date parts ((8) and (11) below).

<Display format>

Figure 5–29: rxversion display format

```
                  ⎧ <Active>(16) ((1))
Active area       ⎨ (3)    (4)    (5)-(6) [(7)]    (8)
                  ⎩ <Inactive>(17) ((2))
Inactive area     ⎨ (3)    (4)    (5)-(6) [(7)]    (8)
                  ⎧ <BIOS>
BIOS              ⎨ (9)-(10)
                    (11)
                    <RAS MCU F/W>
                    (12)-(13)
                    <TPM>
                    (14)-(15)
```

<Display items>
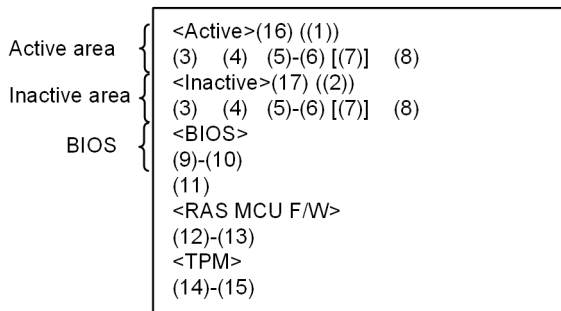
Table 5–33: List of items displayed by rxversion below shows the display items.

Table 5–33: List of items displayed by rxversion

No.	Display
(1)	Active area partition
(2)	Inactive area partition
(3)	Program product name
(4)	Program product model
(5)	OS version
(6)	OS revision
(7)	SI count of the OS
(8)	OS release (master CD created) date [*MM/DD/YYYY*]
(9)	BIOS version
(10)	BIOS revision
(11)	BIOS release date [*MM/DD/YYYY*]
(12)	RAS MCU firmware version
(13)	RAS MCU firmware revision

No.	Display
(14)	TPM major version
(15)	TPM minor version
(16)	A string `<Running>` is displayed for the currently running partition.

<Execution example>

```
$ sudo rxversion
<Active><Running>(/dev/sda2)
CTRL-EDGEN-IMG S-700C-M0U 01-00 [12] 05/18/2020
<Inactive>(/dev/sda3)
CTRL-EDGEN-IMG S-700C-M0U 01-00 [12] 05/18/2020
<bios>
47-18 X64
05/20/2020
<RAS MCU F/W>
01-02
<TPM>
47-18
```

<Diagnosis>

For the exit code, `0` is returned if the status is normal and `1` is returned if an error is detected. Table 5–34: List of rxversion command error messages below shows the error message that is output when an error is detected.

Table 5–34: List of rxversion command error messages

No.	Error message	Description
1	`usage: /hitachi/bin/rxversion` `[ --nodate ]`	The specified argument is invalid.

Note

- Error
  If an attempt to collect any of the information items (1) to (11) shown in the display format fails, `--` is output.

5.18.8 disklchk

<Name>

`disklchk` - Diagnose the SSD life.

<Format>

`disklchk`

<Description>

This command analyzes the write count information managed within the SATA-connected SSD, and displays the SSD life as a percentage (%) in the following format.

The value used to calculate the percentage is also displayed for each item.

<Display format>

```
referenced-item-name  = YY       (YY: Value used for calculation)
Disk write count rate = XX %  (XX: Calculation result displayed as a percentage)
```

<Execution example>

The following is an example when the command is executed for a Hagiwara Solutions SSD.

```
PROGRAM ERASE COUNT AVGAS = 30
Disk write count rate = 0 %
```

<Meanings of the items>

The following shows the meanings of items used for calculating percentages.

`PROGRAM ERACE COUNT AVG`: Average rewrite count for all blocks

Note that only the following type of SSD is applicable. If any other media is installed, an error message appears and the command terminates abnormally.

- Hagiwara Solutions product

<Options>

No options need to be specified. Any specified options are ignored.

<Diagnosis>

For the exit code, `0` is returned if the status is normal and `1` is returned if an error is detected. Table 5–35: List of disklchk command error messages below shows error messages that are output when an error is detected.

Table 5–35: List of disklchk command error messages

No.	Error message	Description
1	`disklchk: No supported disk.`	An unsupported SSD is installed.
2	`disklchk: Failed to get SMART.`	An attempt to acquire SMART information failed.

5.18.9 fsconfchk

<Name>

`fsconfchk` - Check mount definitions.

<Format>

`fsconfchk [confname]`

<Description>

`fsconfchk` is a check command for mount definition files in the user area. This command checks for syntax errors in mount definitions, but it does not check the consistency with partition information in the disk.

<Options>

If no option is specified, the command checks the contents of the `/hitachi/etc/fsconf` file.

- `[confname]`

  Specify the path of the file you want to check. If the file name is specified by the option, the command checks the contents of that file.

<Diagnosis>

For the exit code, `0` is returned if the status is normal and `1` is returned if an error is detected. Table 5–36: List of fsconfchk command error messages below shows error messages that are output when an error is detected.

Table 5–36: List of fsconfchk command error messages

No.	Error message	Description	Action
1	`Device not found. (line=X)`	The device file specified for `device` on line X is not found.	1. Check whether the device name is correct. 2. Check whether the partition specified for `device` has been created.
2	`Illegal paramater. (line=X, param=P)`	The parameter P on line X is invalid.	Check whether the parameter is correct.
3	`XXXX file not found.`	The file specified for *XXXX* is not found.	Check whether the file name is correct.
4	`Invalid definition. (line=X)`	The number of parameters on line X is invalid.	Check whether the parameters are correct.
5	`/dev/XXXX is redefined. (line=Y)`	Device *XXXX* is specified more than once. The second one is specified on line Y.	Delete the duplicated line.

5.18.10 showkxmessage

<Name>

showkxmessage - Display extracted KX messages.

<Format>

showkxmessage [-i | -w | -e]

<Description>

This command searches for KX messages recorded in log messages, and then displays the messages extracted according to the specified options. If no option is specified, the command displays all KX messages.

The search results are displayed in order of the search results of /var/log/syslog so that KX messages are displayed in the order they were generated.

<Options>

No option specified:

All KX messages are displayed.

- -i

  KX*xxxx*-I (Information) messages are only displayed.

- -w

  KX*xxxx*-W (Warning) messages are only displayed.

- -e

  KX*xxxx*-E (Error) messages are only displayed.

<Diagnosis>

For the exit code, 0 is returned if the status is normal and 1 is returned if an error is detected. Table 5–37: List of showkxmessage command error messages below shows error messages that are output when an error is detected.

Table 5–37: List of showkxmessage command error messages

No.	Error message	Description
1	Usage: showkxmessage [-i | -w | -e]	The specified argument is invalid.
2	showkxmessage: No matching message.	There is no relevant message.
3	showkxmessage: grep error.	An error occurred during message extraction.

<Display example>

The following shows an example of when all KX messages are displayed by the command with no option specified.

```
$ sudo showkxmessage
syslog.1:7:May 15 12:03:41 ec kernel: [   25.131888] KXDL001-E Ethernet adapter(eth
2) carrier lost.
syslog.1:615:May 15 12:04:47 ec kernel: [   25.686804] KXDL001-E Ethernet adapter(e
th1) carrier lost.
syslog.1:624:May 15 12:04:47 ec kernel: [   25.708623] KXDL001-E Ethernet adapter(e
th2) carrier lost.
syslog.1:1231:May 15 12:05:53 ec kernel: [   25.729182] KXDL001-E Ethernet adapter(
eth1) carrier lost.
syslog.1:1240:May 15 12:05:53 ec kernel: [   25.750993] KXDL001-E Ethernet adapter(
eth2) carrier lost.
syslog.1:1846:May 18 02:02:55 ec kernel: [   25.422017] KXDL001-E Ethernet adapter(
eth1) carrier lost.
syslog.1:1855:May 18 02:02:55 ec kernel: [   25.443826] KXDL001-E Ethernet adapter(
eth2) carrier lost.
syslog.1:2555:May 19 04:01:58 ec kernel: [   27.762318] KXDL001-E Ethernet adapter(
eth1) carrier lost.
syslog.1:2564:May 19 04:01:58 ec kernel: [   27.784119] KXDL001-E Ethernet adapter(
eth2) carrier lost.
syslog:2:May 19 04:24:36 ec kernel: [   24.696967] KXDL001-E Ethernet adapter(eth1)
 carrier lost.
syslog:9:May 19 04:24:36 ec kernel: [   24.718705] KXDL001-E Ethernet adapter(eth2)
 carrier lost.
$
```

Note

The messages are displayed in ascending order by date.

5.18.11 eclogsave

<Name>

`eclogsave` - Save overall maintenance information.

<Format>

`eclogsave [ -d logtype ] directory-name`

<Description>

Specify the full path name for *directory-name*.

This command stores collected log files, each of which is given a compressed file name *YYYYMMDDhhmmss-*`eclog.tgz`, under the directory specified by the argument. This command also creates and stores a file (*YYYYMMDDhhmmss*-`eclog.list`) that contains a list compressed files (*YYYYMMDDhhmmss*: Overall log collection start time).

Note

Under some conditions, the following message may be displayed when eclogsave failed to run some commands to correct log files.

```
eclogsave: command execution error. (XXXX)
eclogsave: Failed to create log files corretly.
```

eclogsave will correct available log files and export .tgz file. If you got .tgz file, eclogsave worked to the last. If you can't find correct .tgz file, please re-try to run eclogsave after stoppping your applications.

<Options>

No option specified:

All log data of the log type specified by the `-d` option are collected.

`-d logtype`

Log data of the log type specified for *logtype* is saved.

To specify multiple log types, separate each type by a comma (,). You can specify the following values for *logtype*.

- 1

    System log collection target files compressed to tgz format are collected.

- 2

    Memory dump data in the memory dump area to tgz format (maximum of 100 MB) is collected.

- 3

    Log data registered in the user definition file (`/hitachi/etc/save_applog.def`) is compressed to tgz format and collected.

- 4

    System information that exists when the batch collection command is run is compressed to tgz format and collected.

directory-name

Specify the directory in which the collected log files are to be stored. Specify a directory that has sufficient free space for storing the collected log files.

<Diagnosis>

For the exit code, `0` is returned if the status is normal and `1` is returned if an error is detected.

`2` is returned if eclogsave failed to run some command.

Table 5–38: List of eclogsave command error messages below shows error messages that are output when an error is detected.

Table 5–38: List of eclogsave command error messages

No.	Error message	Description
1	`Usage: eclogsave [ -d logtype ]`	The specified argument is invalid.
2	`eclogsave: Directory not found.`	The specified directory does not exist.
3	`eclogsave: Failed to create log files correctly.`	The log files haven't be saved correctly due to a system error.
4	`eclogsave: command execution error. (XXXX)`	eclogsave got error on running command. XXXX: the command.

List of log files stored in *YYYYMMDDhhmmss*-`eclog.tgz` when all log files are collected by the command without the `-d` option specified.

```
YYYYMMDDhhmmss-eclog/1_RAS_LOG/raslog.tgz
                    /2_MEM_DUMP/YYYYMMDDhhmmss.tgz
                    /3_SDA6_LOG/sda6.dump
                    /4_USER_LOG/userlog.tgz
                    /5_MAINT_INFO/maint_info.tgz
```

<Execution example>

The following example shows how to run the command when a formatted USB (external media) is connected to the unit and is recognized as `/dev/sdb1`.

```
$ sudo mkdir /tmp/logdir
$ sudo mount /dev/sdb1 /tmp/logdir
$ sudo eclogsave -d 4 /tmp/logdir
```

5.18.12 rasledctl

<Name>

`rasledctl` - Control lighting of the RAS indicator AP lamp.

<Format>

`rasledctl`

<Description>

This command controls lighting of the RAS indicator (AP).

<Options>

- `-green`

  Turn on the green RAS indicator (AP) light.

- `-red`

  Turn on the red RAS indicator (AP) light.

- `-off`

  Turn off the RAS indicator (AP).

- `-info`

  Indicate the current state of the RAS indicator (AP).

1. Display example when the indicator is lit green

   `RAS-LED(AP): Green`

2. Display example when the indicator is lit red

   `RAS-LED(AP): Red`

3. Display example when the indicator is off

   `RAS-LED(AP): Off`

<Diagnosis>

For the exit code, `0` is returned if the status is normal and `1` is returned if an error is detected.

5.18.13 wdtctl

<Name>

`wdtctl` - Enable and disable hardware WDT.

<Format>

`wdtctl`

<Description>

Running this command with root privileges enables or disables hardware WDT (OS in-loop monitoring). Even after hardware WDT (OS in-loop monitoring) is disabled, restarting the unit enables hardware WDT (OS in-loop monitoring) again.

<Options>

- `-s`

  Disables (temporarily stops) hardware WDT (OS in-loop monitoring).

- `-r`

  Enables (restarts) hardware WDT (OS in-loop monitoring).

<Diagnosis>

For the exit code, `0` is returned if the status is normal and `1` is returned if an error is detected. Table 5–39: List of wdtctl command error messages below shows error messages that are output when an error is detected.

Table 5–39: List of wdtctl command error messages

No.	Error message	Description
1	`usage: wdtctl -s | -r`	No option is specified, or the specified option is invalid.
2	`wdtctl: device is not found.`	The driver for hardware WDT has not started or the device file for accessing the driver cannot be opened.
3	`wdtctl: not a super-user.`	The command is not run with root privileges.
4	`wdtctl: wdtctl library error. (errno=XX)`	An error other than above occurred in the `wdtctl` library. *XX*: Relevant error number

5.18.14 wdtstat

<Name>

`wdtstat` - Check the current monitoring state of the hardware WDT.

<Format>

`wdtstat`

<Description>

This command displays the current operation state of hardware WDT (OS in-loop monitoring).

<Display example>

- If monitoring is running

  ```
  Hard-WDT is running.
  ```

- If monitoring has stopped

  ```
  Hard-WDT is stopping.
  ```

<Diagnosis>

For the exit code, `0` is returned if the status is normal and `1` is returned if an error is detected. Table 5–40: List of wdtstat command error messages below shows error messages that are output when an error is detected.

Table 5–40: List of wdtstat command error messages

No.	Error message	Description
1	`wdtstat: device is not found.`	The driver for hardware WDT has not started or the device file for accessing the driver cannot be opened.
2	`wdtstat: wdtstat library error.(errno=XX)`	An error other than above occurred in the `wdtstat` library. *XX*: Relevant error number

5.18.15 force_restart

<Name>

`force_restart` - Forced restart function

<Format>

`force_restart`

<Description>

Running this command with root privileges forcibly resets and restarts the CPU within approximately 15 to 30 seconds.

<Diagnosis>

For the exit code, `0` is returned if the status is normal and `1` is returned if an error is detected. Table 5–41: List of force_restart command error messages below shows error messages that are output when an error is detected.

Table 5–41: List of force_restart command error messages

No.	Error message	Description
1	`force_restart: device is not found.`	The driver for the hardware WDT has not started or the device file for accessing the driver cannot be opened.
2	`force_restart: not a super-user.`	The command is not run with root privileges.

5.18.16 swdt_start

<Name>

`swdt_start` - Restart the software WDT.

<Format>

`swdt_start`

<Description>

Running this command with root privileges restarts software WDT (fixed priority process in-loop monitoring) that is temporarily stopped. However, because the definition of fixed priority process in-loop monitoring has a higher priority, if the command is issued when monitoring has stopped by `/hitachi/etc/swdt.conf` (`OFF` is defined for the `INLOOP` symbol), the command terminates abnormally without restarting monitoring. If the command is issued when monitoring has already started, the command terminates normally without doing anything.

<Diagnosis>

For the exit code, `0` is returned if the status is normal and `1` is returned if an error is detected. Table 5–42: List of swdt_start command error messages below shows error messages that are output when an error is detected.

Table 5–42: List of swdt_start command error messages

No.	Error message	Description
1	`swdt_start: device is not found.`	The driver for the software WDT has not started or the device file for accessing the driver cannot be opened.
2	`swdt_start: not a super-user.`	The command is not run with root privileges.
3	`swdt_start: can not execute.`	The command cannot run because the monitoring definition (INLOOP) in the `swdt.conf` definition file is set to `OFF`.
4	`swdt_start: swdt_start library error.(errno=XX)`	An attempt to issue the library for restarting the software WDT failed. *XX*: Relevant error number

5.18.17 swdt_stop

<Name>

`swdt_stop` - Temporarily stop the software WDT.

<Format>

`swdt_stop`

<Description>

Running this command with root privileges temporarily stops software WDT (fixed priority process in-loop monitoring).

Note that this command temporarily stops the running software WDT. After the unit is restarted, the operation of the software WDT follows the definition of the `INLOOP` symbol in the `/hitachi/etc/swdt.conf` file.

<Diagnosis>

For the exit code, `0` is returned if the status is normal and `1` is returned if an error is detected. Table 5–43: List of swdt_stop command error messages below shows error messages that are output when an error is detected.

Table 5–43: List of swdt_stop command error messages

No.	Error message	Description
1	`swdt_stop: device is not found.`	The driver for the software WDT has not started or the device file for accessing the driver cannot be opened.
2	`swdt_stop: not a super-user.`	The command is not run with root privileges.
3	`swdt_stop: swdt_stop library error.(errno=XX)`	An attempt to issue the library for pausing the software WDT failed. *XX*: Relevant error number

5.18.18 swdt_stat

<Name>

`swdt_stat` - Check the current monitoring status of the software WDT.

<Format>

`swdt_stat`

<Description>

This command displays the current operating status of software WDT (fixed-priority process in-loop monitoring).

<Display example>

- If monitoring is running

```
Soft-WDT is running.
```

• If monitoring has stopped

```
Soft-WDT is stopping.
```

<Diagnosis>

For the exit code, 0 is returned if the status is normal and 1 is returned if an error is detected. Table 5–44: List of swdt_stat command error messages below shows error messages that are output when an error is detected.

Table 5–44: List of swdt_stat command error messages

No.	Error message	Description
1	swdt_stat: device is not found.	The driver for the software WDT has not started or the device file for accessing the driver cannot be opened.
2	swdt_stat: swdt_stat library error.(errno=*XX*)	An error other than above occurred in the library for getting the software WDT status. *XX*: Relevant error number

5.18.19 usbctl

<Name>

usbctl - Connect or disconnect USB devices.

<Format>

usbctl -p port [-c | -d]

<Description>

This command connects a device to a USB port, disconnects a device from a USB port, or checks the connection state.

<Options>

--p port

Displays the connection state (connected or disconnected) of the USB device for the specified USB port. If the device is connected, Connect appears. If the device is disconnected, Disconnect appears.

For port, specify the USB port number (1 or 2) on which you want to perform operations. To perform operations for all ports or check their states at the same time, specify all.

• 1

Perform operations on USB port number 1.

• 2

Perform operations on USB port number 2.

• all

Perform operations on USB port number 1 and USB port number 2.

--c

Connect the device to the USB port specified for port.

--d

Disconnect the device from the USB port specified for port.

<Diagnosis>

For the exit code, 0 is returned if the status is normal and 1 is returned if an error is detected. Table 5–45: List of usbctl command error messages below shows error messages that are output when an error is detected.

Table 5–45: List of usbctl command error messages

No.	Error message	Description
1	usage: usbctl -p port [-d	-c]	No option is specified, or the specified option is invalid.

No.	Error message	Description
2	`usbctl: device is not found.`	The GPIO driver has not started or the device file for accessing the driver cannot be opened.
3	`usbctl: I/O error.`	A hardware access error is detected.
4	`usbctl: usbctl library error. (errno=`*XX*`)`	An error other than above is detected in the `usbctl` library. *XX*: Relevant error number
5	`Illegal port number.`	The `port` argument is specified incorrectly.

<Examples>

- `-p` option

  The following example shows how to run the command to check the state of USB port number 2. This example shows that the device is disconnected from port 2.

  ```
  $ sudo usbctl -p 2
   Port#2 : Disconnect
  ```

  The following example shows how to run the command to check the states of all USB ports. This example shows that devices are connected to all ports.

  ```
  $ sudo usbctl -p all
   Port#1 : Connect
   Port#2 : Connect
  ```

- `-c` option

  The following example shows how to run the command to connect a device to USB port number 1.

  ```
  $ sudo usbctl -p 1 -c
  ```

  The following example shows how to run the command to connect devices to all USB ports (USB port number 1 and USB port number 2).

  ```
  $ sudo usbctl -p all -c
  ```

- `-d` option

  The following example shows how to run the command to disconnect the device from USB port number 2.

  ```
  $ sudo usbctl -p 2 -d
  ```

6 Managing User Accounts

This chapter describes how to add and delete user accounts for the CE50-10.

6.1 Adding a user account

This operation uses a `sudo` command.

1. Enter a user name, and then run the `adduser` command.

   Enter as follows.

   ```
   $ sudo adduser user-name --gecos ""
   ```

2. Enter a password.

   Enter a password that conforms to the policies. For details about the password policies, see 5.12.2 Setting password policies.

   ```
   New password:<Enter the password.>
   Retype new password:<Enter the password again for confirmation.>
   ```

3. Check the output message.

   When the user account has been added successfully, the following message appears.

   ```
   passwd: password updated successfully
   ```

6.2 Deleting a user account

This operation uses the `sudo` command. To delete a user account, specify the user name and then run the `userdel` command.

```
$ sudo userdel -r user-name
```

6.3 Changing the password of a user

To change the password of a user who is logged in:

1. Log in to the OS as the user whose password is to be changed.

2. Run the `passwd` command.

   Enter as follows.

   ```
   $ passwd
   ```

3. Change the password according to the output messages.

   ```
   $ passwd
   Changing password for current-login-user-name.
   (current) UNIX password:<Enter the current password.>
   New password:<Enter the new password.>
   Retype new password:<Enter the new password again for confirmation.>
   ```

4. Check the output message.

   When the password has changed successfully, the following message appears.

   ```
   passwd: password updated successfully
   ```

6.4 Managing privileges for sudo command execution

6.4.1 Checking the existence of the privilege for sudo command execution

1. Run the `id` command with the user name specified.

   Enter as follows.

   ```
   $ id user-name
   ```

2. Check the execution result.

   If `27(sudo)` appears after `groups=`, the user has the privilege for `sudo` command execution. The following example shows that the privilege for `sudo` command execution has been granted to the user named `myuser`.

   ```
   uid=1002(myuser) gid=1002(myuser) groups=1002(myuser),27(sudo)
   ```

6.4.2 Adding the privilege for sudo command execution

This operation uses the `sudo` command. Run the `gpasswd` command with the user name specified.

```
$ sudo gpasswd -a user-name sudo
```

6.4.3 Deleting the privilege for sudo command execution

This operation uses a `sudo` command. Run the `gpasswd` command with the user name specified.

```
$ sudo gpasswd -d user-name sudo
```

7 Maintaining the CE50-10

This chapter describes maintenance of the CE50-10.

7.1 BIOS settings

BIOS containing system configuration information is stored in battery-backed-up SRAM (CMOS) and ROM. If you change the system configuration, BIOS settings might need to be changed.

Note:

At the time of product shipment, the BIOS settings are optimized for the system configuration.

Changing the BIOS settings might cause unstable operation or might prevent the system from starting normally. Do not change the settings of the items for which change is prohibited in *Table 7-2 BIOS setup menu list*.

Note that the BIOS might be updated during repair work. In that case, the BIOS password and other settings will be initialized.

(1) Starting the setup menu

You need to start the setup menu to set up the BIOS.

When the unit starts, the system initialization message appears. Press the **F2** key to start the setup menu.

(2) Operating the setup menu

The following keys are mainly used to operate the setup menu.

Table 7–1: BIOS setup menu operation keys

Key name	Description
Esc	Used to end the setup, or to return to the high order menu from the low order menu.
← and →	Used to select a menu or a menu group displayed at the top of the screen.
↑ and ↓	Used to select an item in a menu or menu group.
+ and -	Used to select a value to be set. Values that can be set vary depending on the items selected by the key operation. Use the + and - keys on the numeric keypad because Japanese characters cannot be entered in the system BIOS screen.
Space	Used to select a value to be set. If only two choices exist, this key works like a toggle switch to change the displayed value.
Tab	Used to set the date or time or to move a cursor between items such as from month to day or from hour to minute.
Enter	Used to move from a higher-level menu to a lower-level menu, or to end the setup (by saving data to ROM).

(3) Setup menu configuration

The setup menu contains the following large-category items.

Main:

The Main screen appears when the setup menu starts. The basic settings of the system, such as date and time, are specified on this screen.

Advanced:

Used to specify settings, including operation mode, according to the system's configuration.

Security:

Used to specify security settings for the unit.

Boot:

Used to specify the priority of devices for starting the OS.

Exit:
Used to save the changed configuration information to ROM, or to resume the defaults.

(4) Setup menu details

The following shows details of items that can be specified in each menu.

Table 7–2: BIOS setup menu list

High order menu	Set item		Default	Notes
Main	**System Date**		--	#1
	System Time		--	
	Boot Options	**NumLock**	**On**	Do not change the settings.
		Quick Boot	**Disabled**	
		Network Boot	**Enabled**	
		OS Selection	**Linux**	
	BIOS Version		Automatically recognized	
	System Memory		Automatically recognized	
	System Information	**Microcode Revision**	Automatically recognized	
		GOP Version	Automatically recognized	
		FRC Version	Automatically recognized	
		TXE Version	Automatically recognized	
Advanced	**EIST**		**Disabled**	Do not change the settings.
	Turbo Boost		**Disabled**	
	USB Legacy		**Enabled**	
	After AC Power On		**Power On**	Specify the processing to be performed when the power to the unit is turned on. **Power On**: The OS automatically starts when the power is turned on. **Stay Off**: The OS enters software power-off mode when the power is turned on. **Auto**: If the OS was running when the power was turned off the last time, the OS starts the same way when **Power On** is specified. If the OS was not running when the power was turned off the last time, the OS enters software power-off mode the same way when **Stay Off** is specified.
	CPU Frequency		**Normal Frequency**	Change the CPU frequency and TDP.#2

High order menu	Set item	Default	Notes
Security	Secure Boot Configuration	--	Do not change the settings.
	Supervisor Password is:	Cleared	
	User Password is:	Cleared	
	Set Supervisor Password	Enter	
	Supervisor Hint String	Blank	
	Set User Password	Enter	
	User Hint String	Blank	
	Min. password length	8	
Boot	Boot Priority Order	1. **ubuntu** 2. **PCI LAN** 3. **USB CD** 4. **USB HDD** 5. **ATA HDD0** 6. **Internal Shell**	Specify the priority of devices for starting the OS and whether the OS starts from each device. Do not change the settings. Note that the defaults (shown on the left) were specified at the time of product shipment, and are different from the settings specified by clicking **Load Setup Defaults**. If you click **Load Setup Defaults**, change the setting of **Boot Priority Order** to the defaults.
Exit	Exit Saving Changes	--	Click this item to save the setup changes to ROM, and then reboot the system.
	Exit Discarding Changes		Click this item to discard the setup changes, and then reboot the system with the information that was saved in ROM the last time.
	Load Setup Defaults		Click this item to read the BIO default settings. This only reads the defaults, without saving them to ROM. To save the settings to ROM, use **Exit Saving Changes**.

#1
> The date and time are applied to the RTC (real time clock) as soon as they are changed.

#2
> The CPU frequency and TDP are changed depending on the CPU operation mode (**CPU Frequency**) as shown below.

Table 7–3: List of CPU operation modes

CPU Frequency	CPU frequency	TDP
Normal Frequency	1.6 GHz	12 W
Low Frequency	1.3 GHz	7 W

Change the setting of CPU operation mode (CPU Frequency) according to the operating environment (average ambient temperature and operation conditions of the unit). For details about the average ambient temperature and operation conditions of the unit, see A. Unit Specifications.

(5) How to resume the default settings

To resume the default settings of the setup menu items:

1. Start the setup menu (see *(1) Starting the setup menu*).

2. Open **Exit** in the high order menu. Position the cursor to **Load Setup Defaults**, and then press the **Enter** key.
   The following message appears: `Load default configuration now?`

3. Select `Yes`, and then press the **Enter** key.

4. Open **Boot** in the high order menu. In **Boot Priority Order**, change the value to the default value.

5. Open **Exit** in the high order menu again. Position the cursor to **Exit Saving Changes**, and then press the **Enter** key.

   The following message appears: `Save configuration changes and exit now?`

6. Select `Yes`, and then press the **Enter** key.

This is the end of the operation.

7.2 Daily user maintenance items

Table 7–4: Daily inspection items*s* shows the items that we recommend the user to perform on a daily basis.

Table 7–4: Daily inspection items

Item	Frequency	Description
Cleaning	Once a day	Before starting operation, clean around the unit (the unit especially attracts dust due to static electricity). Use a dry cloth to wipe the display. Also, remove any dust or dirt adhering to the heat sink of the unit.
Checking for abnormal temperature or humidity, and abnormal noise	Once a day	Make sure that the ambient temperature and humidity around the unit are within the range of ambient temperature and humidity shown in A.2 Operating environmental conditions. Also, make sure that no abnormal noise is generated from the unit.
Checking whether lamps are lit	Once a day	Check whether any lamp indicating abnormality (such as the alarm lamp) is lit.

7.3 Periodic inspection items

⚠ CAUTION

Do not disassemble the unit during inspection or cleaning. The unit has a sealed structure and does not require internal inspection or cleaning. When the cover is removed, do not touch internal parts, as doing so might cause a burn injury, damage to internal parts, or unit failure.

NOTICE

- Do not hot swap USB equipment or cables with the unit. Hot swapping might cause the unit to malfunction or stop.

- Before moving the unit, shut down the OS, turn off the MAIN POWER switch, and then remove the power cable plug from the outlet. Not following this procedure might result in unit failure.

- When carrying or transporting the unit, it is recommended that you use the packing materials in which the unit was packaged for delivery. If such packing materials are not available or are damaged, carefully pack the unit in a way that protects it from shock, vibration, and electrostatic discharges.

- Moving or transporting a unit that is installed in a cubicle or rack with casters might subject it to excessive vibration or physical impact, resulting in failure of the unit. Select or design a cubicle or rack that meets the installation conditions. Similarly, make sure that the unit is not subject to vibration or physical impact when you move, carry, or transport it.

- Table 7–5: Periodic inspection items shows periodic inspection items. Hitachi is responsible for performing periodic inspection under maintenance contract. Only Hitachi staff and officially-trained personnel are permitted to perform periodic inspection.

Include the inspection in the system operation schedule.

Table 7–5: Periodic inspection items

Item	Frequency	Time required
Collecting and checking logging information	Once a year	10 minutes
Checking and cleaning the parts • Checking and cleaning inside and outside of the cubicle (each unit) • Checking connectors and screws for looseness • Checking operation of lamps • Checking operation of switches and buzzers	Once a year	30 minutes
Checking operations and functions • Checking the set time • Checking operation by using a test program • Checking operation of application programs	Once a year	60 minutes
Periodically replacing life-limited parts	See Table 7–6: Life-limited parts.	

7.4 Life-limited parts

Parts are subject to wear and tear during their use. Table 7–6: Life-limited parts shows the parts that need to be replaced at predefined cycles.

These parts are replaced for profit.

Table 7–6: Life-limited parts

No.	Name	Life	Q'ty (standard)	Remarks
1	SSD	10 years (When the amount of write data per day is 50 GB or less)	1	If the amount of write data per day exceeds 50 GB, its useful life will be shorter.

- Environmental conditions relating to corrosion of this unit are defined in JEITA IT-1004B Class B (temperature of 35 degrees Celsius and humidity of 50% RH). The recommended replacement cycles shown in the preceding table are specified under the condition that the average ambient temperature is 35 degrees Celsius. If the average ambient temperature exceeds 35 degrees Celsius or if the environmental conditions are not met, the replacement cycle shall be shortened.

- Maintenance parts (life-limited parts) are replaced at a fee. We ask you to factor maintenance fees into your budget.

- This unit uses a lithium battery. To dispose of the battery, contact us.

  If you want to dispose of the battery by yourself, follow the rules or regulations of the local authority.

- When the unit or part is replaced in the event of failure or repair, or for any other reason, the new unit or part might be of a different model with compatible functions.

- For peripheral devices, refer to the user's guide that comes with each device for the necessary information about maintenance.

- We have confirmed that zinc oxide whiskers could negatively affect devices. Do not use electrogalvanized materials in the place where this unit and peripheral devices are installed.

  Information from *JEITA Technical Report, Guideline of Facilities and Equipment for Information Systems* (JEITA ITR-1001D):

  Places where zinc whiskers are generated: Electrogalvanized floor panels, stringers, poles, and aseismic flat steel

  Phenomenon: A problem occurs when whisker-like zinc crystals (conductive whiskers) on the floor float in the air and enter devices, causing short-circuits on PCBs or terminals. Because the phenomenon that appears varies depending on the location of the short-circuits, identifying the cause of the problem is difficult. Typically, such problems are handled as transitory errors. Therefore, it takes time to find the cause of the problem.

⚠ CAUTION

This unit uses a lithium battery. When replacing the battery, you must use the one specified by Hitachi. Using any other battery might cause an explosion, fire, rupture, heat generation, leakage, or gas generation.

NOTICE

Do not use life-limited parts beyond their recommended replacement cycle. Deteriorated parts might cause damage.
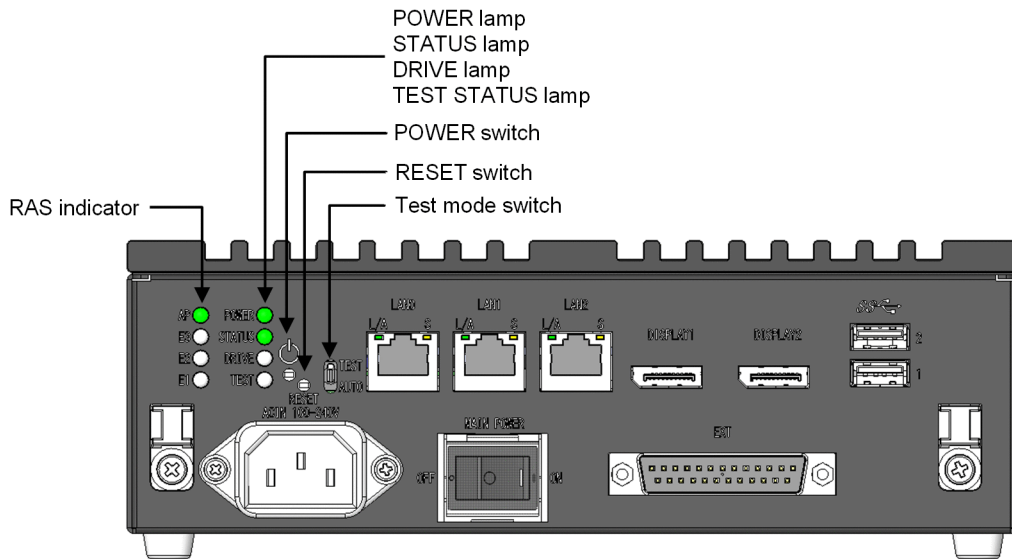
8 Troubleshooting

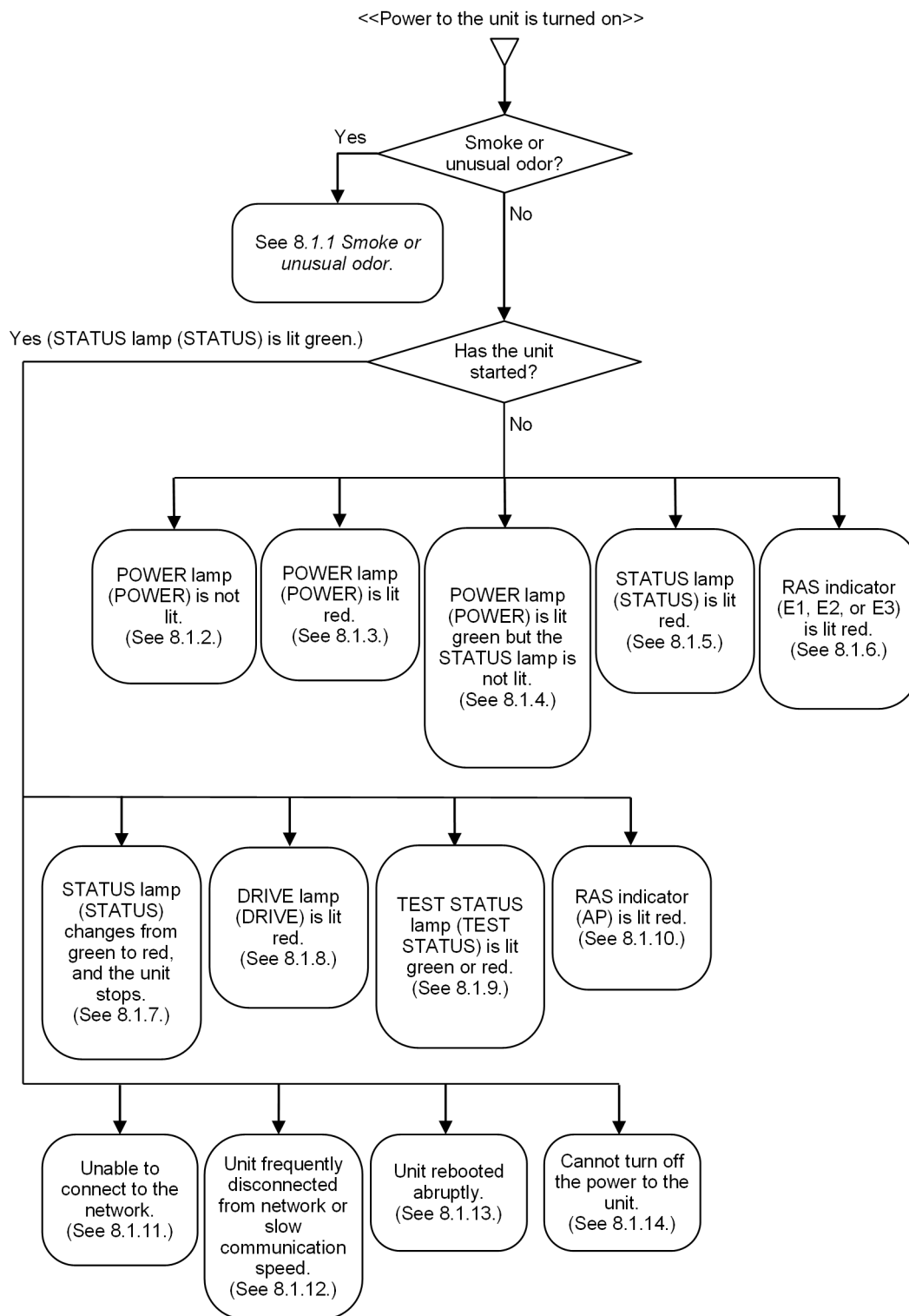This chapter describes troubleshooting of the CE50-10.

8.1 Troubleshooting flow chart

Figure 8–1: Front view of the unit

The following shows the troubleshooting flow chart.

Figure 8–2: Troubleshooting flow chart

8.1.1 Smoke or unusual odor

⚠ WARNING

If there is smoke or an unusual odor, unplug the power cable plug from the outlet, and then contact us. Using the damaged unit might cause a fire or electric shock.

8.1.2 POWER lamp (POWER) does not light by turning on the power

The unit might not be supplied with power. Take the following actions:

1. Confirm that the power cable is correctly connected to the AC inlet and the user-provided power source.

2. Confirm that the voltage output of the power source is correct.

3. If the power cable is connected correctly and the user-provided power source is functioning properly, the power cable might be faulty. In this case, replace the power cable.

4. If the power cable is not faulty, a unit failure might have occurred. In this case, contact us.

8.1.3 POWER lamp (POWER) is lit red after the power is turned on

A unit failure might have occurred. Please contact us.

8.1.4 POWER lamp (POWER) is lit green but the STATUS lamp (STATUS) is off after the power is turned on

A unit failure might have occurred. Please contact us.

8.1.5 STATUS lamp (STATUS) is lit red after the power is turned on

A fault might have occurred during BIOS initialization or OS startup. Please contact us.

8.1.6 RAS indicator (E1, E2, or E3) is lit red after the power is turned on

A fault has been detected in the unit. Please contact us. The following shows the lamp indications and their respective error descriptions.

Table 8–1: Lamps that light up in the event of fault detection

Lamp	Error
E3	A kernel panic occurred.
E2	A multi-bit error in memory is detected.
E1	A watchdog timer detected a timeout.

8.1.7 STATUS lamp (STATUS) changes from lit green to lit red, and the unit stops

The unit might have stopped due to detection of an OS error during unit operation. Please contact us.

8.1.8 DRIVE lamp (DRIVE) is lit red

A disk error occurred, and it is possible that information, such as log information, cannot be saved. If a USB HDD is connected, disconnect it, restart the OS, and check that the DRIVE lamp is no longer red.

If the problem persists, or if the problem occurred while the USB HDD is not connected, the built-in SSD might be abnormal. Please contact us.

8.1.9 TEST STATUS lamp (TEST) is lit green or red

The test mode switch (AUTO, TEST) might be set to TEST. Check the setting of the test mode switch (AUTO, TEST), and then take the following actions.

If the test mode switch (AUTO, TEST) is set to TEST:

1. Stop the unit (see 3.3.1 Stopping the unit).

2. Turn off the power supply connected to the unit (see 3.3.2 Turning off the power to the CE50-10).

3. Set the test mode switch (AUTO, TEST) to AUTO (see 2.1 Indicators and controls on the unit).

4. Turn on the power supply, and then turn on the power to the unit.

If the test mode switch (AUTO, TEST) is set to AUTO:

A unit failure might have occurred. Please contact us.

8.1.10 RAS indicator (AP) is lit red after the power is turned on

An application program detected an error. Refer to the documentation of the application program, or contact the developer of the program.

8.1.11 Unable to connect to the network

A probable cause of the problem is a mistake in the LAN settings or an incomplete connection with network equipment (such as a hub) or a LAN cable. Take the following actions.

1. Check the network settings (see 5. Configuring Software Environment).

2. Unplug the LAN cable, and then insert it firmly.

3. Confirm that the LAN cable is connected to the correct port.

4. Replace the LAN cable.

5. If you are using network equipment, take the following actions.

  • Confirm that the power to the network equipment is turned on.

  • Turn on the power to the network equipment, and then turn on the power to the unit.

  • Replace the network equipment, and then check the operation.

8.1.12 Unit frequently disconnected from network or slow communication speed

A probable cause of the problem is a mistake in the LAN settings or an incomplete connection with network equipment (such as a hub) or the LAN cable. Take the following actions.

1. Check the network settings (see 5. Configuring Software Environment).

2. Unplug the LAN cable, and then insert it firmly.

3. Confirm that the LAN cable is connected to the correct port.

4. Replace the LAN cable.

5. If you are using network equipment, take the following actions.

  • Turn on the power to the network equipment, and then turn on the power to the unit.

  • Replace the network equipment, and then check the operation.

8.1.13 Unit rebooted abruptly

An error might have been detected in the unit and caused it to reboot. Please contact us.

8.1.14 Cannot turn off the power to the unit

Please contact us.

8.2 Collecting maintenance information

The procedure for collecting maintenance information for the unit varies depending on the device configuration. This section describes how to collect maintenance information for each device configuration. For details about device configurations, see 5.15 Backup, restoration, and program updates.

- To collect maintenance information in configuration No. 1, see 8.2.1 Collecting maintenance information in configuration No. 1.
- To collect maintenance information in configuration No. 2, see8.2.2 Collecting maintenance information in configuration No. 2.
- To collect maintenance information in configuration No. 3, see 8.2.3 Collecting maintenance information in configuration No. 3.

8.2.1 Collecting maintenance information in configuration No. 1

Use a maintenance PC to save maintenance information in external media connected to the unit. Before you start this operation, perform the following:

- Disconnect the unit from the external system.
- Stop the unit, and then connect it to the maintenance PC by using an Ethernet cable.
- Create partitions in the external media, and then format them with EXT4.
  The backup data save area in the external media must be formatted with EXT4.
- Change the OS operation mode to maintenance mode.

  Figure 8–3: Flow of maintenance information collection in configuration No. 1

The following describes the operation procedure and command input examples. When entering a command, check the underlined parts.

1. Check the communication between the maintenance PC and the unit.

Run the `ping` command to confirm that communication is possible between the maintenance PC and the unit.

```
$ ping  IP-address-of-the-target-unit
```

2. Log in to the unit from the maintenance PC via ssh.

Log in to the unit via ssh as a user who can run the `sudo` command.

Example user name: `edgeadm`

```
$ ssh  IP-address-of-the-target-unit
login: edgeadm
Password: *******
```

3. Confirm that the OS operation mode is set to maintenance mode.

Run the `showecmode` command to confirm that the **<u>bold underlined parts</u>** are displayed as follows.

```
$ sudo showecmode
Current  : Maintenance mode
Next     : Maintenance mode
$
```

4. Connect the external media.

Connect the external media, and then run the `usbctl` command. The following example shows how to run the command to connect the external media to USB port number 1.

```
$ sudo usbctl -p 1 -c
```

5. Run the batch collection command.

Run the `eclogsave` command to save maintenance information in external media. The following shows an example in which the external media is recognized as `/dev/sdb` and batch collected information is stored in `/dev/sdb1`.

```
$ sudo eclogsave /dev/sdb1
### Started a save of system information. ###
20150801181021-eclog/1_RAS_LOG/raslog.tgz completed.
20150801181021-eclog/2_MEM_DUMP/20150718212439.tgz completed.
20150801181021-eclog/3_SDA6_LOG/sda6.tgz completed.
20150801181021-eclog/4_USER_LOG/userlog.tgz completed.
20150801181021-eclog/5_MAINT_INFO/maint_info.tgz completed.
20150801181021-eclog/6_EXTPP_LOG/extpplog.tgz completed.
### Started a compression of system information. ###
### Successfully completed.(20150801181021-eclog.tgz) ##
$
```

6. Remove the external media from the unit.

Run the `usbctl` command, and then remove the external media. The following example shows how to run the command to disconnect the external media from USB port number 1.

```
$ sudo usbctl -p 1 -d
```

7. Log out from the unit.

```
$ exit
```

To change the OS operation mode to normal mode, see 5.14.4 Changing maintenance mode to normal mode.

8.2.2 Collecting maintenance information in configuration No. 2

Save maintenance information in a maintenance PC connected to the unit. Before you start this operation, perform the following:

• Disconnect the unit from the external system.

• Stop the unit, and then connect it to the maintenance PC by using an Ethernet cable.

• Create partitions in the maintenance PC, and then format them with EXT4 or FAT32.
  The backup data save area must be formatted with EXT4 or FAT32.

• Change the OS operation mode to OS operation mode

Figure 8–4: Flow of maintenance information collection in configuration No. 2

The following describes the operation procedure and command input examples. When entering a command, check the underlined parts.

1. Check the communication between the maintenance PC and the unit.

   Run the `ping` command to confirm that communication is possible between the maintenance PC and the unit.

   ```
   $ ping   IP-address-of-the-target-unit
   ```

2. Log in to the unit from the maintenance PC via ssh.

   Log in to the unit via ssh as a user who can run the `sudo` command.

   Example user name: `edgeadm`

   ```
   $ ssh IP-address-of-the-target-unit
   Login: edgeadm
   Password: *******
   ```

3. Confirm that the OS operation mode is set to maintenance mode.

   Run the `showecmode` command to confirm that the **bold underlined parts** are displayed as follows.

   ```
   $ sudo showecmode
   Current  : Maintenance mode
   Next     : Maintenance mode
   $
   ```

4. Run the batch collection command.

   Run the `eclogsave` command to save maintenance information in external media. The following shows an example in which maintenance information is saved in the `/tmp` directory.

   ```
   $ sudo eclogsave /tmp
   ### Started a save of system information. ###
   20150801181021-eclog/1_RAS_LOG/raslog.tgz completed.
   20150801181021-eclog/2_MEM_DUMP/20150718212439.tgz completed.
   20150801181021-eclog/3_SDA6_LOG/sda6.tgz completed.
   20150801181021-eclog/4_USER_LOG/userlog.tgz completed.
   20150801181021-eclog/5_MAINT_INFO/maint_info.tgz completed.
   20150801181021-eclog/6_EXTPP_LOG/extpplog.tgz completed.
   ```

```
### Started a compression of system information. ###
### Successfully completed.(20150801181021-eclog.tgz) ##
$
```

5. Use the `ls` command to check the size of the maintenance information file.

```
$ ls /tmp
-rw-r--r-- 1 0        0            873 Aug  1 18:10 20150801181021-eclog.list
-rw-r--r-- 1 0        0      115753706 Aug  1 18:10 20150801181021-eclog.tgz
```

6. Log out.

   Log out from the target unit.

```
$ exit
```

7. Use the `scp` command to transfer the file to the maintenance PC.

   Log in by using any user ID.

   The following shows an example of when the target unit is `192.168.11.1`. For the file name, enter the file name displayed in step 4 (enter the **bold underlined parts**).

```
$ scp user-name@192.168.11.1:/tmp/20150801181021-eclog.* .
Password:password
```

8. Check the size of the transferred file.

   Confirm that the size of the file saved in the maintenance PC is the same as the file at the acquisition source (check the **bold underlined parts**).

   If the maintenance PC is Linux:

```
$ ls -l 20150801181021-eclog.list
-rw-r--r-- 1 root root        873 Aug  1 18:10 20150801181021-eclog.list
$ ls -l 20150801181021-eclog.tgz
-rw-r--r-- 1 root root 115753706 Aug  1 18:10 20150801181021-eclog.tgz
```

   If the maintenance PC is Windows:

```
> dir
directory-under-W:\Users\hoge\eclogsave_dir
2015/08/01  18:10            873       20150801181021-eclog.list
2015/08/01  18:10  115,753,706       20150801181021-eclog.tgz
```

8.2.3 Collecting maintenance information in configuration No. 3

Save maintenance information in external media connected to the unit. Before you start this operation, perform the following:

- Disconnect the unit from the external system.

- Create partitions in the external media, and then format them with EXT4.
  The backup data save area in the external media must be formatted with EXT4.

- Change the OS operation mode to maintenance mode.

Figure 8–5: Flow of maintenance information collection in configuration No. 3
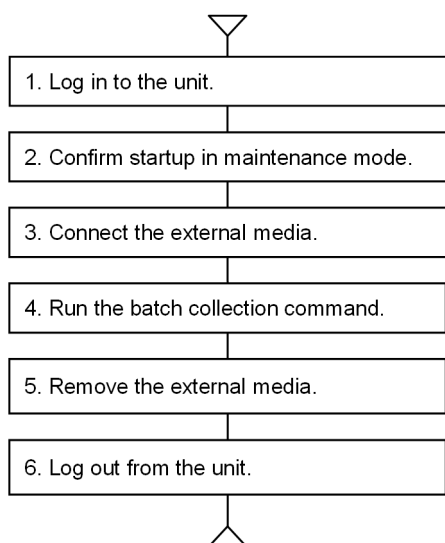
```
            ▽
┌─────────────────────────────────┐
│ 1. Log in to the unit.          │
└─────────────────────────────────┘
┌─────────────────────────────────┐
│ 2. Confirm startup in maintenance mode. │
└─────────────────────────────────┘
┌─────────────────────────────────┐
│ 3. Connect the external media.  │
└─────────────────────────────────┘
┌─────────────────────────────────┐
│ 4. Run the batch collection command. │
└─────────────────────────────────┘
┌─────────────────────────────────┐
│ 5. Remove the external media.   │
└─────────────────────────────────┘
┌─────────────────────────────────┐
│ 6. Log out from the unit.       │
└─────────────────────────────────┘
            △
```

The following describes the operation procedure and command input examples. When entering a command, check the underlined parts.

1. Log in to the unit.

```
Login: edgeadm
Password: *******
```

2. Confirm that the OS operation mode is set to maintenance mode.

   Run the `showecmode` command and confirm that the following is displayed (**check the underlined parts**).

```
$ sudo showecmode
Current  : Maintenance mode
Next     : Maintenance mode
$
```

3. Connect the external media.

   Connect the external media, and then run the `usbctl` command. The following example shows how to run the command to connect the external media to USB port number 1.

```
$ sudo usbctl -p 1 -c
```

4. Run the batch collection command.

   Run the `eclogsave` command to save maintenance information in the external media. The following shows an example in which the external media is recognized as `/dev/sdb` and batch collected information is stored in `/dev/sdb1`.

```
$ sudo eclogsave /dev/sdb1
### Started a save of system information. ###
20150801181021-eclog/1_RAS_LOG/raslog.tgz completed.
20150801181021-eclog/2_MEM_DUMP/20150718212439.tgz completed.
20150801181021-eclog/3_SDA6_LOG/sda6.dump completed.
20150801181021-eclog/4_USER_LOG/userlog.tgz completed.
20150801181021-eclog/5_MAINT_INFO/maint_info.tgz completed.
20150801181021-eclog/6_EXTPP_LOG/extpplog.tgz completed.
### Started a compression of system information. ###
### Successfully completed.(20150801181021-eclog.tgz) ##
$
```

5. Remove the external media.

   Run the `usbctl` command, and then remove the external media. The following example shows how to run the command to disconnect the external media from USB port number 1.

```
$ sudo usbctl -p 1 -d
```

6. Log out from the unit.

Start the target unit by turning on the power.

For details about how to change the OS operation mode to normal mode, see 5.14.4 Changing maintenance mode to normal mode.

Appendixes

These appendixes describe the unit specifications, external interface, real-time clock specifications, connector specifications, error messages, option functions for application programs, library interface reference, security specifications, and communication sheet.

A. Unit Specifications

This appendix describes the CE50-10 unit specifications.

A.1 Unit specifications

Table A–1: Unit specifications (1/2)

Item		Specification
Model		CE50-10
OS		Ubuntu 18.04 LTS (Linux kernel 4.15)
Processor (SoC)		Intel Atom$^{(R)}$x7-E3950
Built-in drive unit	SSD	mSATA SSD (64GB) x1, SATA 6.0 Gbps
Interface	Display	• DisplayPort x 2 • Video controller: On-boarded • Colors: 24-bit colors (16,777,216 colors) • Resolution: 1,280 x 1,024 (SXGA) 1,920 x 1,080 (FHD) 1,920 x 1,200 (WUXGA) 3,840 x 2,160 (4K UHD. It is recommended that the main memory capacity be 8 GB. (See A.3 Optional parts.)[1] • Refresh rate: 60Hz
	USB	USB 3.0 x 2
	LAN	RJ45 x 3ch (1000BASE-T, adopted to Wake on LAN)
	Serial	Not supported
	External contact (EXT)	D-Sub25-pin (when an EXT board is mounted)
		DI — General-purpose input signals / Photocoupler contact x 4
		DO — General-purpose output signals / Photo MOS relay contact (form A) x 10
		PSDOWN — Power supply down signals / Photo MOS relay contact (form B) x 1
External dimension (width x depth x height)		210 x 285 x 69mm (excluding the height of the rubber feet)

[1]
The resolution of 3,840 x 2,160 (4K UHD) is supported only for a single monitor (multiple monitors cannot be used).

Table A–2: Unit specifications (2/2)

Item	Specification
RAS function	• Hardware state monitoring (such as a temperature error) • Watchdog timer • Status Display: RAS indicators (AP, E3, E2, E1), Power lamp (POWER), Status lamp (STATUS), Drive lamp (DRIVE), Test status lamp (TEST), LAN board (ACT/LINK lamp (LAN0, LAN1, LAN2), Speed lamp (LAN0, LAN1, LAN2))

Item	Specification
RAS function	• Memory dump collection • PSDOWN contacts
Weight	4kg or less
Rated power	40W or less
RTC time accuracy	Plus-minus 9 seconds per day (when the ambient temperature is 25 degree Celsius)
System time accuracy[#2]	Plus-minus 6 seconds per day (when the ambient temperature is 25 degree Celsius)
Lifetime[#3]	10 years[#4] (Depending on the operating conditions, the replacement of life-limited parts might be necessary.)

#2

    Not applicable when operating without an OS.

#3

    The lifetime is defined based on the following operating conditions.

#4

    For details, see 7.4 Life-limited parts.

Table A–3: Operating conditions for lifetime definitions

	Condition 1	Condition 2
Average ambient temperature	35 degrees Celsius or less	40 degrees Celsius or less
Operation mode[#5]	Normal Frequency mode	Low Frequency mode
CPU frequency[#5]	1.6 GHz	1.3 GHz
TDP[#5]	12 W	7 W
External equipment connection	Unmentioned	USB equipment is not used (excluding a mouse and keyboard), or USB self-power equipment is used.
Load ratio	Unmentioned	CPU usage ratio: Average 70% or less[#6]

#5

    The CPU frequency and TDP (CPU's allowable thermal design power) change depending on the operation mode, which is set to *Normal Frequency mode* at the time the product is shipped. For details about how to change the operation mode, see 7.1 BIOS settings.

#6

    For details about the CPU usage ratio, see 5.17 Checking the CPU usage ratio.

A.2 Operating environmental conditions

Table A–4: Operating environmental conditions

Item	Specification
Ambient temperature	Operation: 0 to 50 degrees Celsius Storage: -10 to 70 degrees Celsius[#1]
Temperature gradient	Plus-minus 10 K/h or less
Humidity	Operation: 20 to 80 %RH (No condensation must be present.) Non-operation: 10 to 90 %RH (No condensation must be present.)

Item	Specification
Humidity gradient	Plus-minus 10%/h or less
Dust[#2]	General office level (0.3 mg/m^3: JEITA IT-1004B Class B) Complies with IP40.
Corrosive gas	Must not be present. (JEITA IT-1004B Class B (35 degree Celsius per 50%RH))
Vibration resistance	5.9 m/s^2 (10 Hz, and 5s)
Shock resistance	19.6 m/s^2 when power is applied, 49.0 m/s^2 when no power applied
Power supply voltage	AC 100 V to AC 240 V (Tolerance: plus-minus 10 %)
Power supply frequency	50/60 Hz (Tolerance: plus-minus 3Hz)
Rush current	AC100V: 20A or less AC240V: 48A or less
Electrostatic noise	Contact Discharge: 4 kV, Aerial discharge: 8 kV
Insulation resistance	DC 500 V, 5 MΩ
isolation voltage	AC 1.5 kV, 1 minute
Leak current	3.5 mA or less
Grounding wiring	The ground pole of the power outlet to which the power cable of this unit is connected shall be connected to a secure and reliable earthing system (equivalent to D class[#3] or better).
Altitude	1,000 m or below

Note #1

Even if the power to the unit is turned off, some components such as the clock operates by battery backup. If the unit is stored in an environment outside the temperature range of guaranteed operation, you might have to reset the BIOS settings such as the time when re-using the unit. If you need to reset the BIOS settings, contact us.

Note #2

The unit cannot be used in an environment where conductive dust is present in the air.

The dustproof specification of this product is not a guarantee against damage or failure.

The tests specified in JIS C 0920:2003 are implemented for IP40.

Areas containing conductive dust are outside the scope of application of the unit.

There is no drip-proof performance.

A.3 Optional parts

Table A–5: Optional parts

Item	Specification
Main memory [#1, #2]	H-7719-10: DDR3L-1600, with ECC, 4GB H-7719-11: DDR3L-1600, with ECC, 8GB

#1

Selecting a memory option is mandatory. When purchasing memory, select either of the preceding types.
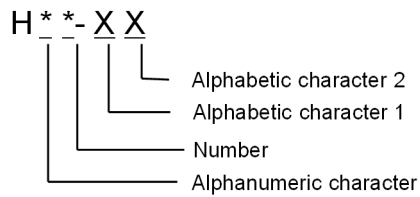
#2

You cannot change your selected option after the product is assembled.

A.4 List of spec numbers

The following explains the naming conventions for spec numbers (spec No.), and provides a list of the spec numbers.

Figure A–1: Spec No. naming conventions

Alphanumeric characters (Hard specification 1)

0: Without an external connection

E: With an external connection

Number (hard specification 2)

1: Memory 4 GB

2: Memory 8 GB

Alphabetic character 1 (OS specification)

S: Standard specification (Ubuntu)

U: Without an OS (Hardware only)

Alphabetic character 2 (software specification)

A: With OpenVINO installed

Table A–6: Spec No. List

No.	Spec No.	Description	Individual specification
1	H01-S	Standard specification (Memory: 4 GB, without an external connection)	Without frame fixing brackets
2	HE2-S	Standard specification (Memory: 8 GB, with an external connection)	--
3	H02-SA	Standard specification (Memory: 8 GB, without an external connection)	--
4	HE2-SA	Standard specification (Memory: 8 GB, with an external connection)	--
5	H01-U	Model without an OS (Memory: 4 GB, without an external connection)	• Without an OS • Secure boot is disabled. The default hardware WDT is disabled.
6	HE2-U	Model without an OS (Memory: 8 GB, with an external connection)	• Without an OS • Secure boot is disabled. The default hardware WDT is disabled.

B. External Interface

External interface information are described as follows:

- Cable length specification for an external interface
- Current specification for the USB 3.0 port and Display port

B.1 Cable length specification for external interface

Table B–1: External interface cable length specification

Interface name	Cable length	Remarks
USB 3.0 port	2 m	Use a USB 3.0-compliant shielded cable. Note that using an extension cable might cause malfunction of the unit.
LAN interface	100 m	Use a cable of UTP category 5e or higher.
External contact input/output interface	30 m	Use a shielded cable.
DisplayPort interface	For details on usable cables, see Remarks.	Recommended to use a cable attached with a display.

B.2 Current specifications for the USB 3.0 port and DisplayPort

The maximum current for each port of the unit is as follows:

Table B–2: Maximum current for port

Interface name	Voltage	Maximum current
USB 3.0 port	5 V	900 mA per port
DisplayPort	3.3 V	500 mA per port

Make sure that the inrush current does not exceed the maximum current limit. If the inrush current exceeds the maximum current limit, the overcurrent protection circuit might be activated, causing the device to become invalid.

C. Real-time Clock Specifications

This unit employs an RTC (real-time clock) IC for its internal clock. The RTC incorporates the calendar and continues to run on a backup battery while the power is off.

Table C–1: Real-time clock specifications

Item	Specification
Clock function	Hour, minute, second (24 hour system)
Date function	Year, month, day
Time accuracy	Plus-minus 9 seconds per day or less[#]
Battery backup	Lithium battery

\#

Reference value when the ambient temperature is 25 degrees Celsius.

D. Connector Specifications

Connector specifications are described as follows:

- USB 3.0 connector (USB3.0-1, USB3.0-2 ports)
- LAN (RJ-45 8-pin) connector
- DisplayPort connector (20-pin, male connector)
- External contact (EXT) connector (D-sub25-pin, inch screw thread, male connector)

D.1 USB 3.0 connector (USB3.0-1, USB3.0-2 ports)
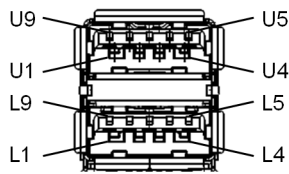
Figure D–1: USB 3.0 pin assignment

Table D–1: USB 3.0 signal names

Pin number	Signal name	Pin number	Signal name
U1	+5V	L1	+5V
U2	USBD0-	L2	USBD0-
U3	USBD0+	L3	USBD0+
U4	GND	L4	GND
U5	SSRX0-	L5	SSRX0-
U6	SSRX0+	L6	SSRX0+
U7	GND	L7	GND
U8	SSTX-	L8	SSTX-
U9	SSTX+	L9	SSTX+

D.2 LAN (RJ-45 8-pin) connector

Figure D–2: LAN (RJ-45) pin assignment
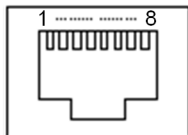
Table D–2: LAN (RJ-45) signal names

Pin number	Signal name	Pin number	Signal name
1	TRD0+	5	TRD2-
2	TRD0-	6	TRD1-
3	TRD1+	7	TRD3+

Pin number	Signal name	Pin number	Signal name
4	TRD2+	8	TRD3-

D.3 DisplayPort connector (20-pin, male connector)

Figure D–3: DisplayPort pin assignment
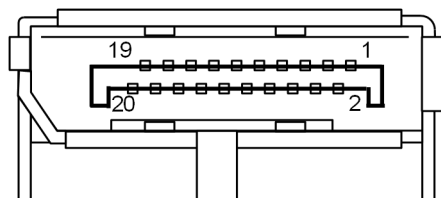
Table D–3: DisplayPort signal names

Pin number	Signal name	Pin number	Signal name
1	Lane0+	11	GND
2	GND	12	Lane3-
3	Lane0-	13	Config1
4	Lane1+	14	Config2
5	GND	15	AUX+
6	Lane1-	16	GND
7	Lane2+	17	AUX-
8	GND	18	HPD
9	Lane2-	19	GND
10	Lane3+	20	POW

D.4 External contact (EXT) connector (D-sub25-pin, inch screw thread, male connector)
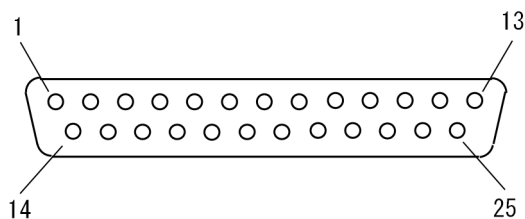
Figure D–4: External contact (EXT) pin assignment

Table D–4: External contact (EXT) signal names

Pin number	Signal name	Pin number	Signal name
1	(Reserved)	14	PSDOWN
2	DO0_GND[#1]	15	DO0_GND[#1]

Pin number	Signal name	Pin number	Signal name
3	DO_01	16	DO_02
4	DO_03	17	DO_04
5	DO0_GND[#1]	18	DO1_GND[#2]
6	DO_05	19	DO_06
7	DO_07	20	DO_08
8	DO1_GND[#2]	21	DO1_GND[#2]
9	DO_09	22	DO_10
10	DI_GND	23	DI_GND
11	DI_01	24	DI_03
12	DI_02	25	DI_04
13	DI_GND	-	-

Note #1

DO0_GND is the return signal for PSDOWN and for DO_01 through DO_05.

Note #2

DO1_GND is the return signal for DO_06 through DO_10.

E. Error Messages

This appendix describes error messages of the CE50-10.

- Error messages at unit startup
- LAN error messages
- SoC (System-on-a-chip) temperature error messages
- Resource shortage error messages
- I/O board error messages

E.1 Error messages at unit startup

Table E–1: Error messages at unit startup

Message ID	Message	Cause (meaning)	Action
KXBT001-W	FScheck failed.(dev=*XXXX*) *XXXX*: Device file name	File system error	None
KXBT002-W	SMART RETURN STATUS is *XXX*. *XXX*: SMART RETURN STATUS value	SMART STATUS error	A unit failure has occurred or a sign of potential failure has been detected. Replace the unit.
KXBT010-E	Ethernet device check failed. (Bus=*X* Device=*Y* Func=*Z*) *X*: Bus number, *Y*: Device number, *Z*: Function number	LAN controller error	
KXBT011-W	PCI device check failed.(Bus=*X* Device=*Y* Func=*Z*) *X*: Bus number, *Y*: Device number, *Z*: Function number	PCI device error other than LAN	
KXBT030-E	Core check failed. (core=*N*) *N*: Number of detected cores	Abnormal number of cores	
KXBT040-E	Physical memory check failed (DRAM= X) X: Installed memory capacity (KB)	Main memory capacity error	
KXBT020-I	GPIO data is as follows. *xx xx xx xx* (GPIO data is dumped in hexadecimal.)	GPIO log acquired	There is no information, or there is no action to be taken.
No ID	Max GPU frequency error.(freq= X MHz) X: Detected maximum GPU frequency	Maximum GPU frequency error	None

E.2 LAN error messages

Table E–2: LAN error messages

Message ID	Message	Cause (meaning)	Action
KXDL001-W	Ethernet adapter(*ethX*) Link is down. *ethX*: Interface name	Link disconnected	1. Check the power supply state at the connection destination.

Message ID	Message	Cause (meaning)	Action
KXDL001-W	Ethernet adapter(*ethX*) Link is down. *ethX*: Interface name	Link disconnected	2. Check the LAN cable for a fault (such as disconnection or loose connection). 3. Confirm that the type of the LAN cable (straight or cross) is correct. If it is not correct, replace the LAN cable. 4. Confirm that the communication speed is correct. If it is not, match the communication speed at the connection destination. 5. If there are no problems in the preceding items, a unit failure might have occurred. Replace the unit.
KXDL002-W	Ethernet adapter(*ethX*) collision retry error. *ethX*: Interface name	Collision retry error	Traffic (communication load) is too high. 1. Reduce the traffic because processing delays might be caused by a large amount of discarded data due to collisions. 2. If this error frequently occurs when traffic is low, confirm that the communication speed is correct. If it is not, match the communication speed at the connection destination. 3. If there is no problem in the preceding items, a unit failure might have occurred. Replace the unit.
KXDL003-E	Ethernet adapter(*ethX*) PCIe Bus Error: severity=Uncorrected (Fatal). *ethX*: Interface name	Bus error	A PCI bus error was detected in the unit. A unit failure might have occurred. Replace the unit.
KXDL005-E	Ethernet adapter(*ethX*) initial error. *ethX*: Interface name	Initialization error	An attempt to initialize the LAN controller failed. Replace the unit because the LAN controller is faulty.
KXDL006-E	Ethernet adapter(*ethX*) transmit timeout error. *ethX*: Interface name	Transmission completion timeout (transmission TI monitoring timeout)	A data transmission timeout was detected. Replace the unit because the LAN controller is faulty.
KXDL009-E	Ethernet adapter(*ethX*) Duplicate IP address. *ethX*: Interface name	Duplicate IP address (during initialization)	1. An invalid IP address might be defined on the local host. Correct the IP address definition file, and then restart the unit.
KXDL010-W	Ethernet adapter(*ethX*) Duplicate IP address. *ethX*: Interface name	Duplicate IP address (during online)	2. A loop configuration network is not supported. If the unit is connected to the network that uses a loop configuration, change the network configuration.
KXDL020-E	Ethernet adapter (*ethX*) transmit queue *Y* timed out. *ethX*: Interface name *Y*: Queue number	Transmission queue timeout	A transmission queue timeout was detected. Replace the unit because the LAN controller is faulty.

Message ID	Message	Cause (meaning)	Action
KXDL200-I	Ethernet adapter (*ethX*) Link is up at *XXX* Mbps, *YYY* duplex. *ethX*: Interface name *XXX*: 10, 100, or 1000 (Mbps) *YYY*: half or full (transmission method)	Link established	None

E.3 SoC (System-on-a-chip) temperature error messages

Table E–3: SoC temperature error messages

Message ID	Message	Cause (meaning)	Action
KXTM001-W	TCC ON	TCC[#] started.	None. Although unit operation continues, a processor error might have occurred or the ambient temperature might be too high.
KXTM002-I	TCC OFF	Temperature is recovered after TCC[#] started.	

#

Abbreviation for Thermal Control Circuitry. This function starts when the internal temperature of SoC reaches approximately 110 degree Celsius to suppress heat generation by adjusting the SoC clock or voltage.

E.4 Resource shortage error messages

Table E–4: Resource shortage error messages

Message ID	Message	Cause (meaning)	Action
KXKL101-W	There is not enough free memory ($X^{#1}$ KB limit, $Y^{#2}$ KB free)	The memory capacity is insufficient (free space is less than 20%).	Use the showmem command to identify which process uses a lot of memory.
KXKL102-E	Insufficient memory (free size = $Y^{#2}$ KB)	The memory capacity is insufficient (free space is less than 10%).	
KXKL301-E	Insufficient disk (device = $Z^{#3}$ free size = $Y^{#2}$ KB)	The partition capacity is insufficient (free space is less than 10%).	Delete unnecessary files to allocate sufficient free space.
KXKL111-I	System free memory recovered ($X^{#1}$ KB limit, $Y^{#2}$ KB free)	Free space in memory is recovered to 20% or more.	None
KXKL112-I	System free memory recovered ($X^{#1}$ KB limit, $Y^{#2}$ KB free)	Free space in memory is recovered to 10% or more.	
KXKL311-I	Disk capacity recovered (device = $Z^{#3}$ free size = $Y^{#2}$ KB)	Free space in the partition is recovered to 10% or more.	

#1

X: Upper limit of available space

#2

Y: Remaining free space

#3

Z: Device name of the partition

E.5 I/O board error messages

Table E–5: I/O board error messages

Message ID	Message	Cause (meaning)	Action
KXDI001-W	`DI read timeout`	DI software timeout[4]	Processing contention might have occurred due to concurrent issuance of I/O library functions. Revise the user program.
KXDO001-W	`DO write timeout`	DO software timeout[1, 4]	
KXSI001-W	**`Super I/O initialization failed`**	Super I/O initialization failed.	An I/O board failure might have occurred. Replace the unit.
KXDO002-W	`DO write failed`	An attempt to write DO output data failed. [2, 4]	
KXDO003-W	`DO through mode change failed`	An attempt to change DO output through mode failed. [2, 4]	
KXDO004-W	`DO hold mode change failed`	An attempt to change DO hold mode failed. [3, 4]	
KXIO001-E	`IO board cable disconnected`	The I/O board cable is disconnected (during online).	

#1

Whether the previous output value is retained or the current value is output depends on the timing at which an error occurred.

#2

An attempt to write output data failed for all DO channels (that is, the previous value is retained).

#3

Data of the current value is output for all DO channels.

#4

In the case of a fixed error that is not transient, the message is output each time the user accesses the device. A library function immediately returns without waiting for I/O of the device. Therefore, make sure that continuous operation without waiting time does not result in sequential output of error messages or a high load on the CPU.

F. Option Functions for Application Programs

This appendix describes the following functions:

- Container function (Docker)
- OPC-UA client function

F.1 Container function (Docker)

By using Docker, you can deploy application programs, libraries, and prerequisite programs as containers in the operation environment (CE50-10). A container is provided as a single image file. By transferring an image file from the development environment to the operation environment, you can run the application program in the same environment as the development environment. This simplifies the work required to put new or updated application programs into use.

Figure F–1: Deploying image files from the development environment
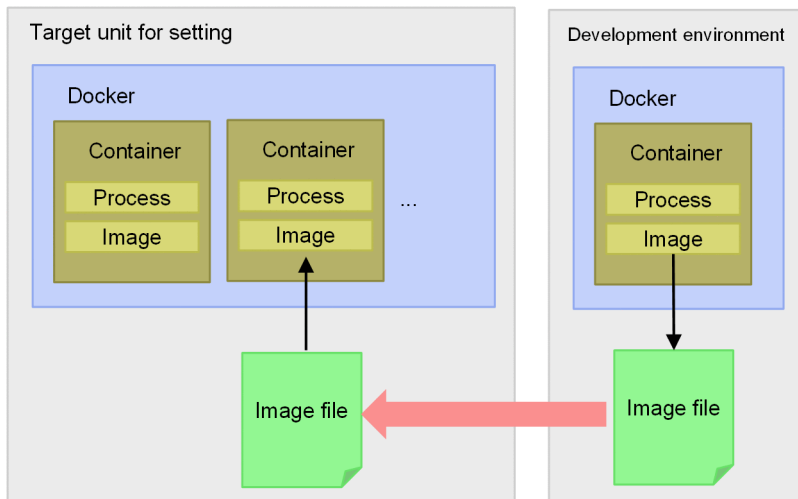
To use the container function, you need to create a partition in the operation environment, mount the partition as the area for use by Docker, and then load the image file for the container.

(1) Initializing Docker

To use Docker, you need to mount the Docker partition in the operation environment.

For details about how to create partitions, see (2) Creating partitions. To start an Ubuntu 18.04.3 image, at least 150 MB free space is required for a partition. More free space is required according to the types of applications and containers to be deployed on Docker.

Set up the created partition so that it will be mounted in `/var/lib/docker` when the OS starts.

To temporarily use Docker, run the following command to mount the created partition before starting Docker.

```
$ sudo mount /dev/sda9 /var/lib/docker
```

(2) Starting and stopping Docker

By default, Docker is stopped when the OS starts. The following describes how to start and stop Docker and how to start Docker when the OS starts.

(a) Starting Docker

Run the following command to start Docker.

```
$ sudo systemctl start docker
```

(b) Stopping Docker

Run the following command to stop Docker.

```
$ sudo systemctl stop docker
```

(c) Starting Docker when the OS starts

Run the following command to start Docker when the OS starts.

```
$ sudo systemctl enable docker
```

(3) Loading image files on Docker

The following describes how to transfer an image file to Docker and load it as a Docker image. The following example describes how a Docker image is loaded by using an image called Ubuntu 18.04.3 distributed by the Docker official repository.

1. Transfer the image file from the development environment to the container directory in the operation environment.

2. Remotely or locally log in to the operation environment.

3. Move to the directory in which the image file is placed, and then run the following command.
   The image file is loaded.

```
$ sudo docker load < ubuntu-18.04.3.tar
```

4. Run the following command to confirm that the image file has been successfully loaded as a Docker image.

```
$ sudo docker images
```

If loading has been performed normally, the following should be displayed.

```
REPOSITORY        TAG        IMAGE ID        CREATED        SIZE
ubuntu            18.04      a2a15febcdf3    5 days ago     64.2MB
```

This concludes the loading of Docker images to the operation environment.

(4) Confirming that the container has started

The following describes how to start a container from a Docker image and then terminate that container. The following example describe how to start the container for the Docker image Ubuntu 18.04.3.

1. Run the following command to start the container.

```
$ sudo docker run --rm -it repository-name:tag-name bash
```

For *repository-name*:*tag-name*, enter the values acquired from the information displayed by running the `docker images` command.

- *repository-name*: Character string displayed in the `REPOSITORY` column (example: `ubuntu`)

- *tag-name*: Character string displayed in the `TAG` column (example: `18.04`)

For example, enter as follows:

```
$ sudo docker run --rm -it ubuntu:18.04 bash
```

When the container operates normally, the `bash` command is run on the container.

2. When you confirm the normal operation, terminate the container.

```
root@a647f8520afd:/$ exit
```

This concludes operation verification of the container.

F.2 OPC-UA client function

We provide the following programs to use the CE50-10 as an OPC-UA client.

- Library: OSS Open62541
- Sample programs for operation verification: `tutorial_server_variable.c` (server program) and `client.c` (client program)

(1) Compiling a program that uses the OPC-UA library

To compile a C program that uses Open62541, run the following command.

```
$ gcc C-program-file-name -lopen62541 -o program-name
```

(2) Verifying operation of the OPC-UA sample program

You can run the sample program to check communication between the client and the server via the OPCUA protocol. The following describes how to run the sample program. `[Enter]` in command examples indicates pressing of the **Enter** key on the keyboard.

1. Copy the sample program to any directory.

```
$ cp /usr/share/open62541/examples/{tutorial_server_variable.c,client.c} .
```

2. Compile the sample program.

```
$ gcc client.c -lopen62541 -o client
$ gcc tutorial_server_variable.c -lopen62541 -o server
```

3. Run the sample program.

```
$ ./server &
$ ./client
```

When OPC-UA communication is successful, the following appears.

```
Connection 5 | SecureChannel 2 | Session ab3211ff-db96-588f-bc5b-358373d79d49 | Act
ivateSession: Session activated
```

4. Terminate the client, and then terminate the server.

To terminate the client, Press the **Ctrl** and **C** keys at the same time.

To terminate the server, run the following command.

```
$ kill %1
```

This concludes operation verification of the OPC-UA sample program.

G. Library Interface Reference

This appendix describes the following library interfaces:

- Lighting control of the RAS indicator AP lamp
- DIDO input/output operation
- Forced CPU restart
- USB device connection/disconnection operation

G.1 rasledctl (lighting control of the RAS indicator AP lamp)

This interface allows the user to control lighting of the RAS indicator AP lamp.

(1) Compiling

To compile the program in the development environment, enter as follows:

```
$ sudo cc -I/hitachi/usr/include -o xxx xxx.c -L/hitachi/lib64 -lras
```

- *xxx*: Specify the object file name.
- *xxx.c*: Specify the source file name.

For details about include files and libraries that are to be specified when compiling the program, see Table 5–10: Files for application development by using the unique functions of CE50-10.

(2) Reference

(a) Format

```
#include <rasif.h>
int    rasledctl(int cmd);
```

(b) Description

You can control lighting of the RAS indicator AP lamp by issuing this library interface with an argument added.

(c) Arguments

USER_GREEN

Turn on the green RAS indicator AP lamp.

USER_RED

Turn on the red RAS indicator AP lamp.

USER_OFF

Turn off the RAS indicator AP lamp.

USER_INFO

Return the status of the RAS indicator AP lamp.

(d) Return values

-1

Returned when an error occurs. The error number is set for errno.

0

If an argument other than USER_INFO is specified, the return value is 0 if the status is normal.

USER_GREEN, USER_RED, or USER_OFF

> If the USER_INFO argument is specified, one of these values is returned according to the the current status of the AP lamp.

G.2 didoctl (DIDO input/output operation)

This interface allows the user to operate DI input and DO output.

(1) Compiling

To compile the program in the development environment, enter as follows:

```
$ sudo cc -I/hitachi/usr/include -o xxx xxx.c -L/hitachi/lib64 -lecextio
```

- *xxx*: Specify the object file name.
- *xxx.c*: Specify the source file name.

For details about include files and libraries that are to be specified when compiling the program, see Table 5–10: Files for application development by using the unique functions of CE50-10.

(2) Reference

(a) Format

```
#include <stdio.h>
#include <ecextioctl.h>
int   didoctl(int board, int cmd, int *buf)
```

(b) Description

DI inputs data to the unit and DO outputs data from the unit. The value specified for the cmd argument determines whether access is made to DI or DO. This interface accesses all DI or DO channels by a single call. Four DI channels or ten DO channels can be accessed.

The standard access time for DI or DO is approximately 5 milliseconds or less in a normal state. If DI or DO does not return a response for 10 milliseconds, a timeout is detected and the processing terminates abnormally. At this time, the error code ETIMEDOUT is returned.

(c) Arguments

board

> Specify the access target I/O board number. For the CE50-10, specify BOARD_NO1, which is defined in ecextioctl.h.
>
> If a value other than BOARD_NO1 is specified, processing terminates abnormally, the return value is -1, and EINVAL is returned for the error number (errno).

cmd

> Specify the processing details.
>
> - DIO_READ: Access DI and input data to the unit.
> - DIO_WRITE: Access DO and output data from the unit.
>
> Note that DIO_READ and DIO_WRITE are defined in ecextioctl.h.

buf

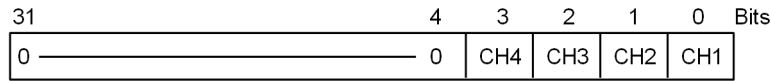> When you specify DIO_READ for cmd, specify the address of the area in which input data is to be stored.
>
> When you specify DIO_WRITE for cmd, specify the address of the area in which output data is to be stored.
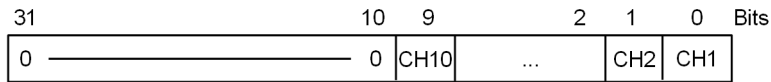>
> The following shows the format of the area specified for buf.

Figure G–1: Format of the area specified for buf

cmd=DIO_READ specified:

```
 31                                          4   3     2     1     0   Bits
┌──────────────────────────────────────────┬────┬─────┬─────┬─────┐
│0 ──────────────────────────────────── 0  │CH4 │ CH3 │ CH2 │ CH1 │
└──────────────────────────────────────────┴────┴─────┴─────┴─────┘
```

cmd=DIO_WRITE specified:

```
 31                              10   9               2    1     0   Bits
┌────────────────────────────────┬──────┬──────────┬─────┬─────┐
│0 ────────────────────────── 0  │CH10  │   ...    │ CH2 │ CH1 │
└────────────────────────────────┴──────┴──────────┴─────┴─────┘
```

(d) Return values

`0`

Normal termination

`-1`

Abnormal termination. One of the following codes is returned for the error number (`errno`).

Table G–1: Codes for the error number (errno)

Code	Description
EINVAL	The value specified for `cmd` is neither `DIO_READ` nor `DIO_WRITE`. Alternatively, the value specified for `board` is not `BOARD_NO1`. When `DIO_WRITE` is specified, the data for bit 10 to bit 31 in the area specified for `buf` is not output to `DO`. Therefore, the specification content is not checked.
EFAULT	NULL is specified for the area specified for `buf`.
ENXIO	An attempt to open the device to be used within the library failed. Alternatively, an error occurred in the IPC (shared memory) in the library. Restart the unit.
EIO	When DO was accessed, a hardware error was detected by writing and reading back the register. Message KXDO002-W, KXDO003-W, or KXDO004-W is output.
ETIMEDOUT	A timeout was detected during access to DI or DO. A message KXDI001-W or KXDO001-W is output.

(e) Notes

- For the value specified for the `buf` argument, whether NULL is specified is checked but whether the specified area is accessible is not checked. Therefore, you must allocate the data storage area and specify the address of that area. If the specified area is not accessible or is too small, a program error might occur. If a program error occurs, the application program (process) that called the library terminates abnormally.

- If the external power supply of DO is lost due to a power failure or any other failure, DO data is not output but `didoctl` terminates normally. CE50-10 is unable to detect incorrect DO data output caused by a failure in an external power supply.

(f) Coding example

```
#include <stdio.h>
#include <stdlib.h>
#include <errno.h>
#include <ecextioctl.h>

int main()
{
    int    ret, board, cmd, bufdata;

        board = BOARD_NO1;
        cmd = DIO_READ;     /* Read DI data. */
    bufdata = 0;
```

```
    ret = didoctl(board, cmd, &bufdata);
    if (ret == -1) {
        perror("didoctl");
        exit(1);
    }
    printf("DI data = 0x%x\n", bufdata);

        cmd = DIO_WRITE;      /* Write DO data. */
    bufdata |= 0x00000001;    /* Output 1 for CH1.*/
    ret = didoctl(board, cmd, &bufdata);
    if (ret == -1) {
        perror("didoctl");
        exit(1);
    }
        exit(0);
}
```

G.3 force_restart (forced CPU restart)

This interface allows the user to forcibly reset and restart the CPU.

(1) Compiling

To compile the program in the development environment, enter as follows.

```
$ sudo cc -I/hitachi/usr/include -o xxx xxx.c -L/hitachi/lib64 -lras
```

- *xxx*: Specify the object file name.
- *xxx.c*: Specify the source file name.

For details about include files and libraries that are to be specified when compiling the program, see Table 5–10: Files for application development by using the unique functions of CE50-10.

(2) Reference

(a) Format

```
#include <rasif.h>
int    force_restart(void);
```

(b) Description

Issuing this function without an argument forcibly resets and restarts the CPU within approximately 20 to 60 seconds.

(c) Return values

0

    Normal termination

-1

    Abnormal termination. The following code is returned for the error number (`errno`).

    ENXIO

        The driver for monitoring the hardware watchdog timer has not started or the device file for accessing the driver cannot be opened.

G.4 usbctl (USB device connection/disconnection operation)

This interface allows the user to connect, disconnect, or obtain the status of the device connected to the USB port.

(1) Compiling

To compile the program in the development environment, enter as follows:

```
$ sudo cc -I/hitachi/usr/include -o xxx xxx.c -L/hitachi/lib64 -lras
```

- *xxx*: Specify the object file name.
- *xxx.c*: Specify the source file name.

For details about include files and libraries that are to be specified when compiling the program, see Table 5–10: Files for application development by using the unique functions of CE50-10.

(2) Reference

(a) Format

```
#include <rasif.h>
int    usbctl(int req, int port);
```

(b) Description

This interface connects, disconnects, or obtains the status of the device, according to the request specified for the `req` argument. For the `port` argument, specify the USB port number (`1` or `2`) of the device to be connected or disconnected. The following describes details about the arguments.

(c) Arguments

`req`

Specify one of the following requests:

`USB_DISABLE`

Disconnect the device for the USB port number specified for the `port` argument.

`USB_ENABLE`

Connect the device for the USB port number specified for the `port` argument.

`USB_STAT`

Obtain the connection and disconnection states for all USB port numbers, ignoring the value of the `port` argument.

`port`

Specify the USB port number 1 or 2. To perform operation for all ports at the same time, specify a negative value.

Note: Macro that determines the connection state

Specifying the return value of `USB_STAT` and the target USB port number for the arguments of the `USB_PORT_CHECK` macro allows you to determine whether the device is disconnected (= 1) or connected (= 0).

`USB_PORT_CHECK` (*return-value*, *port-number*)

(d) Return values

■ For normal termination

If `USB_DISABLE` or `USB_ENABLE` is specified

For normal termination, `0` is returned. Note that an attempt to connect a device that is already connected or disconnect a device that is already disconnected also causes normal termination.

If `USB_STAT` is specified

The value indicating a connection or disconnection state is stored in the bit string for each USB port, and then the value is returned.

Figure G–2: Return value when USB_STAT is specified

USB_STAT specified:
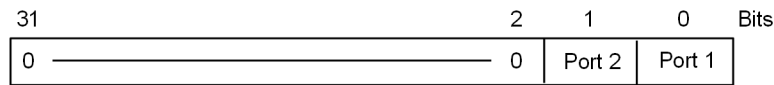
Values that can be stored in the bit string for port 1 or port 2
0: Connected
1: Disconnected

■ For abnormal termination

For abnormal termination, -1 is returned and one of the following codes is returned for the error number (`errno`).

`EINVAL`

The argument has an error.

`ENXIO`

The driver for monitoring the hardware watchdog timer has not started, or the device file for accessing the driver cannot be opened.

`ENOENT`

A device file for the GPIO driver does not exist.

`EIO`

A hardware access error occurred.

H. Security Specifications

This appendix describes the following items related to the security specifications:

- List of log capacities
- Security function list

H.1 List of log capacities

Log files, which are stored in `/var/log`, are important for finding signs of security attacks or for investigating security accidents. There is a limit on the amount of log data that can be stored in CE50-10. Due to these specifications, log files are automatically deleted after a certain period has passed after the log data is generated.

Table H–1: Log file retention period list shows the standard retention period of log files generated by the OS and RAS function of the CE50-10. If necessary, consider copying log files to external media before they are deleted. For some log files, the retention period might change depending on how they are used. For such log files, the prerequisite specification conditions for the retention period are also described.

Table H–1: Log file retention period list

No.	Log file name	Description	Retention period (standard)	Prerequisite
1	syslog	System message	Approx. 3 days	The unit is restarted once a day.
2	wtmp	Login history	Approx. 160 days	A login to the unit is performed once a day.
3	auth.log	Authentication history	Approx. 13 days	Operation with root privileges is performed approximately 20 times per day.
4	sar.log	Operation management information	Approx. 3 days	--
5	netlog	Network statistics	Approx. 21 days	--
6	errlog	KX message	Approx. 5,000 days	One KX message is generated per day.
7	temp.log	Temperature information	Approx. 7 days	--
8	memlog.log	Memory error information	Approx. 213 days	--
9	ras_mcu.log	RAS MCU monitoring error information	Approx. 1,280 days	One error occurs per day.
10	volt.log	Voltage value information	Approx. 71 days	--
11	uptime.log	Cumulative power-on time per manufacturing number	--[#1]	--
12	reg.log	Internal register information	Approx. 71 days	--
13	flog.log	RAS MCU Flash log	--[#1]	--

#1
Only the latest information is always saved. Past information is not saved.

H.2 Updating the encryption algorithm

If a vulnerability is found in the algorithm used for encryption, you need to stop using that algorithm and use another.

To update the algorithm used to perform encryption in the CE50-10:

1. Hitachi provides the new algorithm as package files (extension `.deb`) containing OpenSSL binary data that implements encryption.

2. Start the unit in normal mode.

3. Copy the package files.
   Use the following command to create the directory where the package files are to be placed.

   ```
   $ mkdir /tmp/opessl_update
   ```

   Copy all the package files from the external media or maintenance PC to the directory you created.

4. Run the following command.

   ```
   $ sudo apt -y install /tmp/openssl_update/*.deb
   ```

This ends the procedure for updating the encryption algorithm.

I. Communication Sheet

If you need technical assistance from Hitachi during the troubleshooting of this product as described in 8. Troubleshooting, it is recommended that you first fill in the form shown in Table I–1: Data sheet. Then share the data sheet with Hitachi's technical assistance personnel so as to expedite the process.

Inquiries about the product: https://www.hitachi.co.jp/products/it/control_sys/platform/cs_edge/

Enter your inquiries about this product on our website. You will then be contacted by the appropriate department.

Contact:

Table I–1: Data sheet

No.	Item	Status

1	Lamp status	• POWER lamp (POWER): Green, red, off
		• STATUS lamp (STATUS): Green, red, off
		• DRIVE lamp (DRIVE): Green, green (blinking), red, off
		• TEST STATUS lamp (TEST): Green, red, off
		• RAS indicator
		  - AP: Green, red, off
		  - E3: Red, off
		  - E2: Red, off
		  - E1: Red, off

2	Indication on the display	

Note:

The operating system or the BIOS might be updated during repair work. In that case, the OS or BIOS password and other settings will be initialized.