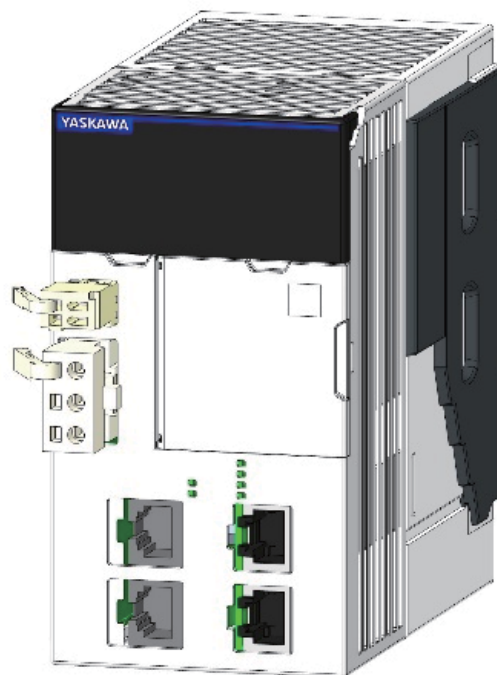


iC9000 Series iC9200 Product Manual

Model: JEYRM-MPX02210L32-2



Preface and General Precautions **1**

Overview **2**

Installation and Wiring **3**

Deployment **4**

Appearance and Parts **5**

Specifications **6**

External Dimensions **7**



Table of Contents

1. Preface and General Precautions.....	7
1.1 Copyright © YASKAWA Electric Corporation.....	8
1.1.1 All Rights Reserved.....	8
1.1.2 EC Conformity Declaration.....	8
1.1.3 Conformity Information.....	8
1.1.4 Trademarks.....	8
1.1.5 General Terms of Use.....	8
1.1.6 Document Support.....	9
1.1.7 Technical Support.....	9
1.2 About This Manual.....	10
1.3 Intended Audience.....	11
1.4 Using this Manual.....	12
1.4.1 Basic Terms Used in this Manual.....	12
1.4.2 Visual Aids.....	12
1.5 Safety Precautions.....	13
1.5.1 Safety Information.....	13
1.5.2 Safety Precautions That Must Always Be Observed.....	13
1.5.3 Intended Use.....	18
1.6 Warranty.....	19
1.6.1 Details of Warranty.....	19
1.6.2 Limitations of Liability.....	19
1.6.3 Suitability for Use.....	20
1.6.4 Specifications Change.....	20
1.7 Compliance with UL Standards and EU Directives.....	21
1.7.1 North American Safety Standards (UL).....	21
1.7.2 EU Directives.....	21

2. Overview	23
2.1 Introduction to the iC9200.....	24
2.2 Industrial Security and Installation Guidelines.....	25
2.2.1 Industrial security in information technology.....	25
2.2.2 Installation guidelines	27
2.3 Overview	30
2.3.1 iC9200	30
2.3.2 Components	30
2.3.3 Hardware Revision.....	35
2.4 System Configuration Example	37
2.5 Devices and Components That Can Be Used to Build a System	38
2.6 Specifications for Module Combinations	39
2.6.1 Specifications and Restrictions for iC9200 Module Combinations	39
2.6.2 Current Consumption and Rack Width Restrictions	39
3. Installation and Wiring	41
3.1 Properties.....	42
3.2 Installing the iC9200	43
3.2.1 Mounting CPU	43
3.2.2 Mounting Periphery Modules	45
3.3 Wiring the iC9200	47
3.3.1 Wiring the Power Supply	47
3.3.2 Wiring a Status Monitoring Device	48
3.3.3 Connecting EtherCAT Communications Devices.....	49
3.3.4 Connecting Ethernet Communications Devices.....	50
3.3.5 Wiring System SLIO Periphery.....	51
4. Deployment	61
4.1 Licensing information for open source software.....	62
4.2 Programming and file system.....	63
4.2.1 PLCnext Technology	63
4.2.2 Programming	63
4.2.3 Firewall.....	63
4.3 Commissioning.....	64
4.3.1 Install iCube Engineer.....	64
4.3.2 Online Access to the CPU	64

4.4	Memory Management	65
4.4.1	Internal Memory	65
4.4.2	Slot for Yaskawa SD Card	67
4.5	MRESET and Reset to Factory Settings.....	68
4.5.1	MRESET	68
4.5.2	Reset to Factory Settings Type 1.....	68
4.5.3	Reset to Factory Settings Type 2	69
4.6	Firmware Update	70
4.7	Safe Mode	71
4.7.1	Start-Up in Safe Mode	71
4.7.2	Start-up in Standard Mode	71
4.8	Web-Based Management - WBM.....	72
4.8.1	Overview and First Steps	72
4.8.2	Overview	74
4.8.3	Diagnostics.....	75
4.8.4	Configuration.....	85
4.8.5	Security	89
4.8.6	Administration	105
5.	Appearance and Parts.....	111
5.1	Appearance and Parts Description	112
5.1.1	Appearance and Part Names.....	112
5.1.2	Display and Indicators.....	113
5.1.3	Connectors	120
5.1.4	Switches	125
5.1.5	Memory.....	126
5.1.6	Buffering Mechanisms	127
6.	Specifications.....	129
6.1	iC9200 Installation and Operating Conditions	130
6.1.1	Installation and Operating Conditions.....	130
6.1.2	Control Panel Cooling Method.....	130
6.2	Power Supply Section.....	132
6.3	CPU Module Specifications	133
6.3.1	Hardware Specifications.....	133
6.3.2	Performance Specifications	134
6.3.3	Ethernet Communications Function Module Specifications	134

7. External Dimensions	135
7.1 iC9200	136
7.1.1 iC9226M-EC.....	136
Revision History	137

Preface and General Precautions

1.1	Copyright © YASKAWA Electric Corporation	8
1.1.1	All Rights Reserved	8
1.1.2	EC Conformity Declaration	8
1.1.3	Conformity Information.....	8
1.1.4	Trademarks.....	8
1.1.5	General Terms of Use.....	8
1.1.6	Document Support	9
1.1.7	Technical Support.....	9
1.2	About this Manual	10
1.3	Intended Audience	11
1.4	Using this Manual.....	12
1.4.1	Basic Terms Used in this Manual.....	12
1.4.2	Visual Aids.....	12
1.5	Safety Precautions	13
1.5.1	Safety Information.....	13
1.5.2	Safety Precautions That Must Always Be Observed	13
1.5.3	Intended Use	18
1.6	Warranty	19
1.6.1	Details of Warranty.....	19
1.6.2	Limitations of Liability.....	19
1.6.3	Suitability for Use	20
1.6.4	Specifications Change	20
1.7	Compliance with UL Standards and EU Directives	21
1.7.1	North American Safety Standards (UL).....	21
1.7.2	EU Directives	21

1.1 Copyright © YASKAWA Electric Corporation

1.1.1 All Rights Reserved

This document contains proprietary information of Yaskawa and is not to be disclosed or used except in accordance with applicable agreements.

This material is protected by copyright laws. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Yaskawa) except in accordance with applicable agreements, contracts or licensing, without the express written consent of Yaskawa and the business management owner of the material.

For permission to reproduce or distribute, please contact your nearest Yaskawa representative or one of the offices listed on the back of this manual.

1.1.2 EC Conformity Declaration

Hereby, YASKAWA Electric Corporation declares that the products and systems are in compliance with the essential requirements and other relevant provisions. Conformity is indicated by the CE marking affixed to the product.

1.1.3 Conformity Information

For more information regarding CE marking and Declaration of Conformity (DoC), please contact your local representative of YASKAWA Electric Corporation.

1.1.4 Trademarks

SLIO is a registered trademark of YASKAWA Europe GmbH.

All Microsoft Windows, Office and Server products mentioned are registered trademarks of Microsoft Inc., USA.

Linux is a registered trademark of Linus Torvalds.

PLCnext Technology is a registered trademark of Phoenix Contact.

EtherCAT® is a registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.

EtherCAT® 

PROFINET is a registered trademark of PROFIBUS and PROFINET International (PI).

QR code is a registered trademark of Denso Wave Inc.

Ethernet is a registered trademark of the Xerox Corporation.

All other trademarks, logos and service or product marks specified herein are owned by their respective companies.

1.1.5 General Terms of Use

Every effort has been made to ensure that the information contained in this document was complete and accurate at the time of publishing. We cannot guarantee that the information is free of errors, and we reserve the right to change the information at any time. There is no obligation to inform the customer about any changes. The customer is requested to actively keep his documents up to date. The customer is always responsible for the deployment of the products with the associated documentation, taking into account the applicable directives and standards.

This documentation describes all hardware units and functions known today. It is possible that units are described that do not exist at the customer. The exact scope of delivery is described in the respective purchase contract.

1.1.6 Document Support

If you have errors or questions regarding the content of this document, contact your nearest Yaskawa representative or one of the offices listed on the back of this manual.

1.1.7 Technical Support

If you encounter problems or have questions regarding the product, contact your nearest Yaskawa representative or one of the offices listed on the back of this manual.

1.2 About This Manual

Manual Name	Manual Number	Contents
iC9000 Series iC9200 Product Manual	SIEP C880901 00 (This manual)	Describes the basic operations and functions of the iC9226M-EC, as well as installation, wiring, communications settings for other devices, specifications, external dimensions, and usage methods.

This is the first manual you should read to build a system using the iC9200.

The contents of this manual are organized into the following chapters.

Chapter	Title	Contents
1	Preface and General Precautions	Provides a preface and general precautions.
2	Overview	Provides an overview of the iC9200.
3	Installation and Wiring	Describes the installation and wiring of the iC9200.
4	Deployment	Describes the basic operations of the iC9200.
5	Appearance and Parts	Describes detailed information on the appearance and parts of the iC9200.
6	Specifications	Describes installation and operating conditions of the iC9200 and provides details on the specifications.
7	External Dimensions	Provides the appearance and external dimensions of the iC9200.

Read this manual carefully to ensure the correct usage of the controller system and to apply the iC9200 to control your manufacturing system.

Keep this manual in a safe place so that it can be referred to whenever necessary.

1.3 Intended Audience

This manual is intended for the following people who are assumed to possess a basic knowledge of controllers and a basic knowledge of electric and electronic circuits.

- People who wish to deepen their understanding of controller products
- People who will select products to be used in equipment
- People who design controller systems
- People who maintain controller systems

1.4 Using this Manual

1.4.1 Basic Terms Used in this Manual

The following basic terms are used in this manual.

Basic Terms	Meaning
iC9000-Series	Series names of controllers including the iC9200.
iC9200	A generic name for the iC9226M and its function modules and I/O modules.
iC9226M	A specific name for an iC9200 controller equipped with a power supply section and CPU section.
I/O Module	A generic name for a SLIO I/O series module

1.4.2 Visual Aids

The following aids are used to indicate certain types of information for easier reference.



Important

Indicates precautions or restrictions that must be observed.

Indicates alarm displays and other precautions that will not result in machine damage.



Term

Indicates definitions of difficult terms or terms that have not been previously explained in this manual.

Information

Indicates supplemental information to deepen understanding or useful information.

1.5 Safety Precautions

1.5.1 Safety Information

To prevent personal injury and equipment damage in advance, the following signal words are used to indicate safety precautions in this document. The signal words are used to classify the hazards and the degree of damage or injury that may occur if a product is used incorrectly. Information marked as shown below is important for safety. Always read this information and heed the precautions that are provided.



DANGER

Indicates precautions that, if not heeded, are likely to result in loss of life, serious injury, or fire.



WARNING

Indicates precautions that, if not heeded, could result in loss of life, serious injury, or fire.



CAUTION

Indicates precautions that, if not heeded, could result in relatively serious or minor injury, or in fire.

NOTICE

Indicates precautions that, if not heeded, could result in property damage.

1.5.2 Safety Precautions That Must Always Be Observed

(1) General Precautions



WARNING

The installation must be suitable and it must be performed only by an experienced technician.

There is a risk of electrical shock or injury.

Before connecting the machine and starting operation, make sure that an emergency stop procedure has been provided and is working correctly.

There is a risk of injury.

Do not approach the machine after a momentary interruption to the power supply. When power is restored, the product and the device connected to it may start operation suddenly. Provide safety measures in advance to ensure human safety when operation restarts.

There is a risk of injury.

Do not touch anything inside the product.

There is a risk of electrical shock.

Do not attempt to modify the product in any way.

There is a risk of injury or device damage.


CAUTION

Do not remove the front cover, cables, connector, or options while power is being supplied.
There is a risk of electrical shock, malfunction, or damage.

Do not damage, pull on, apply excessive force to, place heavy objects on, or pinch the cables.

There is a risk of electrical shock, operational failure of the product, or burning.

NOTICE

Do not turn the power ON and OFF frequently.

This may cause the elements inside the base unit to deteriorate.

(2) Storage and Transportation Precautions

CAUTION

Hold onto the main body of the product when transporting it.

Holding the cables or connectors may damage them or result in injury.

Do not overload the product during transportation. (Follow all instructions.)

There is a risk of injury or malfunction.

NOTICE

Never subject the product to an atmosphere containing halogen (fluorine, chlorine, bromine, or iodine) during transportation.

There is a risk of malfunction or damage.

If disinfectants or insecticides must be used to treat packing materials such as wooden frames, plywood, or pallets, use a method other than fumigation.

For example, use heat sterilization (core temperature of 56°C or higher for 30 minutes or longer).

Treat the packing materials before the product is packaged instead of using a method that treats the entire packaged product.

If the electronic products, which include stand-alone products and products installed in machines, are packed with fumigated wooden materials, the electrical components may be greatly damaged by the gases or fumes resulting from the fumigation process. In particular, disinfectants containing halogen, which includes chlorine, fluorine, bromine, or iodine can contribute to the erosion of the capacitors.

Do not store the product in any of the following locations.

- **Locations that are subject to direct sunlight**
- **Locations that are subject to ambient storage temperatures that exceed product specifications**
- **Locations that are subject to relative humidities that exceed product specifications**
- **Locations that are subject to condensation as the result of extreme changes in temperature**
- **Locations that are subject to corrosive or flammable gases**
- **Locations that are near flammable objects**
- **Locations that are subject to dust, salts, or metal powder**
- **Locations that are subject to water, oil, or chemicals**
- **Locations that are subject to vibration or shock that exceeds product specifications**

If you store the product in any of the above locations, the product may fail or be damaged.

(3) Installation Precautions



CAUTION

Do not step on the product or place heavy objects on the product.

There is a risk of injury or malfunction.

Do not block the air ports on the product. Do not allow foreign objects to enter the product.

There is a risk of internal element deterioration, malfunction, or fire.

Leave the specified amount of space between the product, and the interior surface of the control panel and other devices.

There is a risk of fire or malfunction.

NOTICE

Never install the product in an atmosphere containing halogen (fluorine, chlorine, bromine, or iodine).

There is a risk of malfunction or damage.

Always mount the product in the specified orientation.

There is a risk of malfunction.

Do not subject the product to strong shock.

There is a risk of malfunction.

Do not touch the electrodes when installing the battery.

Static electricity may damage the internal electronic component.

Do not install the product in any of the following locations.

- **Locations that are subject to direct sunlight**
- **Locations that are subject to ambient operating temperatures that exceed product specifications**
- **Locations that are subject to relative humidities that exceed product specifications**
- **Locations that are subject to condensation as the result of extreme changes in temperature**
- **Locations that are subject to corrosive or flammable gases**
- **Locations that are near flammable objects**
- **Locations that are subject to dust, salts, or metal powder**
- **Locations that are subject to water, oil, or chemicals**
- **Locations that are subject to vibration or shock that exceeds product specifications**
- **Locations near devices that generate strong magnetic fields**
- **Locations that are subject to radioactivity**

If you install the product in any of the above locations, the product may fail or be damaged.

(4) Wiring Precautions



WARNING

Check the wiring to be sure it has been performed correctly.

There is a risk of motor run-away, injury, or malfunction.

⚠ CAUTION

Do not change any wiring while power is being supplied.

There is a risk of electrical shock or injury.

Always use a power supply of the specified voltage.

There is a risk of fire or malfunction.

Install breakers and other safety measures to provide protection against shorts in external wiring.

There is a risk of fire.

Configure the circuits to turn ON the 24-V I/O power supply after one second or longer has elapsed from when the power to the iC9200 was turned ON.

If the power to the iC9200 is turned ON after the external power supply, e.g., the 24-V I/O power supply, the outputs from the iC9200 may momentarily turn ON when the power to the iC9200 turns ON. This can result in unexpected operation that may cause injury or device damage.

Provide emergency stop circuits, interlock circuits, limit circuits, and any other required safety measures in control circuits outside of the product.

There is a risk of injury or device damage.

Connect the battery with the correct polarity.

There is a risk of battery damage or explosion.

NOTICE

In places with poor power supply conditions, ensure that the input power is supplied within the specified voltage range.

There is a risk of device damage.

Provide sufficient shielding when using the product in the following locations.

- Locations that are subject to noise, such as from static electricity
- Locations that are subject to strong electric or magnetic fields
- Locations that are subject to radioactivity
- Locations that are near power lines

There is a risk of device damage.

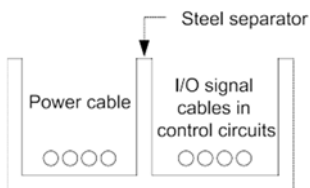
Select the I/O signal wires for external wiring to connect the product to external devices based on the following criteria:

- Mechanical strength
- Noise interference
- Wiring distance
- Signal voltage

Separate the I/O signal cables for control circuits from the power cables both inside and outside the control panel to reduce the influence of noise from the power cables.

If the I/O signal lines and power lines are not separated properly, malfunction may occur.

Example of Separated Cables



(5) Operation Precautions

WARNING

Follow the procedures and instructions in the manuals for the relevant products to perform normal operation and trial operation.

Operating mistakes while the servomotor and machine are connected may damage the machine or even cause accidents resulting in injury or death.

CAUTION

Implement interlock signals and other safety circuits external to the product to ensure safety in the overall system even if the following conditions occur.

- **Product failure or errors caused by external factors**
- **Shutdown of operation due to product detection of an error in self-diagnosis and the subsequent turning OFF or holding of output signals**
- **Holding of the ON or OFF status of outputs from the product due to fusing or burning of output relays or damage to output transistors**
- **Voltage drops from overloads or short-circuits in the 24-V output from the product and the subsequent inability to output signals**
- **Unexpected outputs due to errors in the power supply, I/O, or memory that cannot be detected by the product through self-diagnosis.**

There is a risk of injury, device damage, or burning.

(6) Maintenance and Inspection Precautions

CAUTION

Do not attempt to disassemble or repair the product.

There is a risk of electrical shock, injury, or device damage.

Do not forget to perform the following tasks when you replace the i9200:

- **Back up all programs and parameters from the i9200 that is being replaced.**
- **Transfer all saved programs and parameters to the new i9200.**

If you operate the i9200 without transferring this data, unexpected operation may occur. There is a risk of injury or device damage.

Do not change any wiring while power is being supplied.

There is a risk of electrical shock or injury.

(7) Disposal Precautions

Correctly discard the product and used batteries as stipulated by regional, local, and municipal laws and regulations. Be sure to include these contents in all labelling and warning notifications on the final product as necessary.



(8) Other General Precautions

- Figures provided in this manual are typical examples or conceptual representations. There may be differences between them and actual wiring, circuits, and products.
- The products shown in illustrations in this manual are sometimes shown with their covers or protective guards removed to illustrate detail. Always replace all covers and protective guards before you use the product.
- If you need a new copy of this manual because it has been lost or damaged, contact your nearest Yaskawa representative or one of the offices listed on the back of this manual.
- This manual is subject to change without notice for product improvements, specifications changes, and improvements to the manual itself. We will update the manual number of the manual and issue revisions when changes are made.
- Any and all quality guarantees provided by Yaskawa are null and void if the customer modifies the product in any way. Yaskawa disavows any responsibility for damages or losses that are caused by modified products

1.5.3 Intended Use

The CPU iC9226M-□ is constructed and produced for:

- industrial use.
- general control and automation tasks.
- industrial network communication, machine and process control.
- operation within the environmental conditions specified in the technical data.

1.6 Warranty

1.6.1 Details of Warranty

(1) Warranty Period

The warranty period for a product that was purchased (hereinafter called the “delivered product”) is one year from the time of delivery to the location specified by the customer or 18 months from the time of shipment from the Yaskawa factory, whichever is sooner.

(2) Warranty Scope

Yaskawa shall replace or repair a defective product free of charge if a defect attributable to Yaskawa occurs during the above warranty period. This warranty does not cover defects caused by the delivered product reaching the end of its service life and replacement of parts that require replacement or that have a limited service life.

This warranty does not cover failures that result from any of the following causes.

- Improper handling, abuse, or use in unsuitable conditions or in environments not described in product catalogs or manuals, or in any separately agreed-upon specifications
- Causes not attributable to the delivered product itself
- Modifications or repairs not performed by Yaskawa
- Use of the delivered product in a manner in which it was not originally intended
- Causes that were not foreseeable with the scientific and technological understanding at the time of shipment from Yaskawa
- Events for which Yaskawa is not responsible, such as natural or human-made disasters

1.6.2 Limitations of Liability

- Yaskawa shall in no event be responsible for any damage or loss of opportunity to the customer that arises due to failure of the delivered product.
- Yaskawa shall not be responsible for any programs (including parameter settings) or the results of program execution of the programs provided by the user or by a third party for use with programmable Yaskawa products.

1.6.3 Suitability for Use

- It is the customer's responsibility to confirm conformity with any standards, codes, or regulations that apply if the Yaskawa product is used in combination with any other products.
- The customer must confirm that the Yaskawa product is suitable for the systems, machines, and equipment used by the customer.
- Consult with Yaskawa to determine whether use in the following applications is acceptable. If use in the application is acceptable, use the product with extra allowance in ratings and specifications, and provide safety measures to minimize hazards in the event of failure.
 - Outdoor use, use involving potential chemical contamination or electrical interference, or use in conditions or environments not described in product catalogs or manuals
 - Nuclear energy control systems, combustion systems, railroad systems, aviation systems, vehicle systems, medical equipment, amusement machines, and installations subject to separate industry or government regulations
 - Systems, machines, and equipment that may present a risk to life or property
 - Systems that require a high degree of reliability, such as systems that supply gas, water, or electricity, or systems that operate continuously 24 hours a day
 - Other systems that require a similar high degree of safety
- Never use the product for an application involving serious risk to life or property without first ensuring that the system is designed to secure the required level of safety with risk warnings and redundancy, and that the Yaskawa product is properly rated and installed.
- The circuit examples and other application examples described in product catalogs and manuals are for reference. Check the functionality and safety of the actual devices and equipment to be used before using the product.
- Read and understand all use prohibitions and precautions, and operate the Yaskawa product correctly to prevent accidental harm to third parties.

1.6.4 Specifications Change

The names, specifications, appearance, and accessories of products in product catalogs and manuals may be changed at any time based on improvements and other reasons. The next editions of the revised catalogs or manuals will be published with updated code numbers. Consult with your Yaskawa representative to confirm the actual specifications before purchasing a product.

1.7 Compliance with UL Standards and EU Directives

Certification marks for the standards for which the product has been certified by certification bodies are shown on nameplate. Products that do not have the marks are not certified for the standards.

1.7.1 North American Safety Standards (UL)



Product	Model	North American Safety Standards (UL File No.)
iC9226M-EC	JEYRM-MPX02210L32-2	UL 61010-1, UL 61010-2-201 (E147823) CSA C22.2 No.61010-1, 61010-2-201

1.7.2 EU Directives



Product	Model	EU Directives	Harmonized Standards
iC9226M-EC	JEYRM-MPX02210L32-2	EMC Directive 2014/30/EU	EN 55011 group 1, class A EN 61000-6-2 EN 61000-6-4 EN 61131-2 (Zone B)
		RoHS Directive 2011/65/EU, (EU)2015/ 863	EN IEC 63000: 2018
		WEEE Directive 2012/19/EU	-

Overview

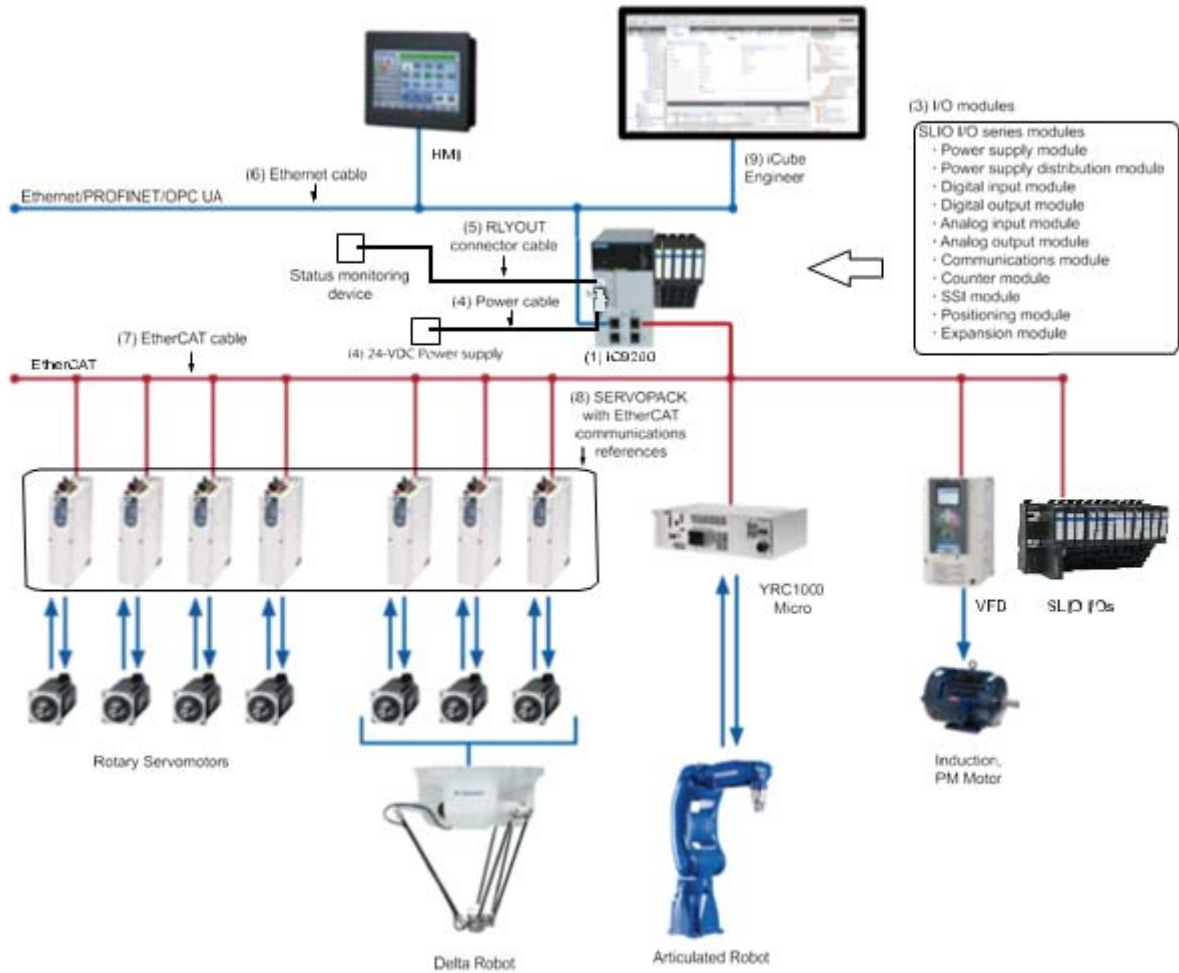
This chapter provides an overview of the iC9200.

2.1	Introduction to the iC9200	24
2.2	Industrial Security and Installation Guidelines	25
2.2.1	Industrial security in information technology	25
2.2.2	Installation guidelines	27
2.3	Overview	30
2.3.1	iC9200	30
2.3.2	Components	30
2.3.3	Hardware Revision	35
2.4	System Configuration Example	37
2.5	Devices and Components That Can Be Used to Build a System	38
2.6	Specifications for Module Combinations	39
2.6.1	Specifications and Restrictions for iC9200 Module Combinations	39
2.6.2	Current Consumption and Rack Width Restrictions	39

2.1 Introduction to the iC9200

The iC9200 supports the EtherCAT real-time network for motion and I/O, and Ethernet for general purpose communications.

The iC9200 is equipped with one connector for EtherCAT communications and two connectors for Ethernet communications. These connectors allow the iC9200 to communicate with a variety of peripheral devices. PROFINET (if configured) utilizes the Ethernet ports.



2.2 Industrial Security and Installation Guidelines

This chapter provides information on industrial security in information technology and installation guidelines.

2.2.1 Industrial security in information technology

Hazards	<p>The topic of data security and access protection has become increasingly important in the industrial environment. The increased networking of entire industrial systems to the network levels within the company together with the functions of remote maintenance have all served to increase vulnerability. Hazards can arise from:</p> <ul style="list-style-type: none"> • Internal manipulation such as technical errors, operating and program errors and deliberate program or data manipulation. • External manipulation such as software viruses, worms and Trojans. • Human carelessness such as password phishing.
Precautions	<p>The most important precautions to prevent manipulation and loss of data security in the industrial environment are:</p> <ul style="list-style-type: none"> • Encrypting the data traffic by means of certificates. • Filtering and inspection of the traffic by means of VPN - "Virtual Private Networks". • Identification of the user by "Authentication" via safe channels. • Segmenting in protected automation cells, so that only devices in the same group can exchange data. • Deactivation of unnecessary hardware and software.
Further information	<p>You can find more information about the measures on the following websites:</p> <ul style="list-style-type: none"> • Federal Office for Information Technology https://www.bsi.bund.de/EN/Home/home_node.html • Cybersecurity & Infrastructure Security Agency us-cert.cisa.gov • VDI / VDE Society for Measurement and Automation Technology www.vdi.de/en/home • IEC 62443 Security for industrial automation and control systems https://www.iec.ch/blog/understanding-iec-62443 •

(1) Protection of hardware and applications

(a) Precautions

- Do not integrate any components or systems into public networks.
 - Use VPN "Virtual Private Networks" for use in public networks. This allows you to control and filter the data traffic accordingly.
- Always keep your system up-to-date.
 - Always use the latest firmware version for all devices.
 - Update your user software regularly.
- Protect your systems with a firewall.
 - The firewall protects your infrastructure internally and externally.
 - This allows you to segment your network and isolate entire areas.
- Secure access to your plants via user accounts.
 - If possible, use a central user management system.
 - Create a user account for each user for whom authorization is essential.
 - Always keep user accounts up-to-date and deactivate unused user accounts.
- Secure access to your plants via secure passwords.
 - Change the password of a standard login after the first start.
 - Use strong passwords consisting of upper/lower case, numbers and special characters. The use of a password generator or manager is recommended.
 - Change the passwords according to the rules and guidelines that apply to your application.
- Deactivate inactive communication ports respectively protocols.
 - Only the communication ports that are used for communication should be activated.
 - Only the communication protocols that are used for communication should be activated.
- Consider possible defence strategies when planning and securing the system.
 - The isolation of components alone is not sufficient for comprehensive protection. An overall concept is to be drawn up here, which also provides defensive measures in the event of a cyber attack.
 - Periodically carry out threat assessments. Among others, a comparison is made here between the protective measures taken and those required.
- Limit the use of external storage media.
 - Via external storage media such as USB memory sticks or SD memory cards, malware can get directly into a system while bypassing a firewall.
 - External storage media or their slots must be protected against unauthorized physical access, e.g. by using a lockable control cabinet.
 - Make sure that only authorized persons have access.
 - When disposing of storage media, make sure that they are safely destroyed.
- Use secure access paths such as HTTPS or VPN for remote access to your plant.
- Enable security-related event logging in accordance with the applicable security policy and legal requirements for data protection.

(2) Protection of PC-based software

(a) Precautions

Since PC-based software is used for programming, configuration and monitoring, it can also be used to manipulate entire systems or individual components. Particular caution is required here!

- Use user accounts on your PC systems.
 - If possible, use a central user management system.
 - Create a user account for each user for whom authorization is essential.
 - Always keep user accounts up-to-date and deactivate unused user accounts.
- Protect your PC systems with secure passwords.
 - Change the password of a standard login after the first start.
 - Use strong passwords consisting of upper/lower case, numbers and special characters. The use of a password generator or manager is recommended.
 - Change the passwords according to the rules and guidelines that apply to your application.
- Enable security-related event logging in accordance with the applicable security policy and legal requirements for data protection.
- Protect your PC systems by security software.
 - Install virus scanners on your PC systems to identify viruses, trojans and other malware.
 - Install software that can detect phishing attacks and actively prevent them.
- Always keep your software up-to-date.
 - Update your operating system regularly.
 - Update your software regularly.
- Make regular backups and store the media at a safe place.
- Regularly restart your PC systems. Only boot from storage media that are protected against manipulation.
- Use encryption systems on your storage media.
- Perform security assessments regularly to reduce the risk of manipulation.
- Use only data and software from approved sources.
- Uninstall software which is not used.
- Disable unused services.
- Activate a password-protected screen lock on your PC systems.
- Always lock your PC systems as soon as you leave your PC workstation.
- Do not click any links that come from unknown sources. If necessary ask, e.g. on e-mails.
- Use secure access paths such as HTTPS or VPN for remote access to your PC system.

2.2.2 Installation guidelines

(1) General

The installation guidelines contain information about the interference free deployment of iC9200. There is the description of the ways, interference may occur in your PLC, how you can make sure the electromagnetic compatibility (EMC), and how you manage the isolation.

(2) What does EMC mean?

Electromagnetic compatibility (EMC) means the ability of an electrical device, to function error free in an electromagnetic environment without being interfered respectively without interfering the environment.

The components are developed for the deployment in industrial environments and meets high demands on the EMC. Nevertheless you should project an EMC planning before installing the components and take conceivable interference causes into account.

(3) Possible interference causes

Electromagnetic interferences may interfere your control via different ways:

- Electromagnetic fields (RF coupling)
- Magnetic fields with power frequency
- Bus system
- Power supply
- Protected earth conductor

Depending on the spreading medium (lead bound or lead free) and the distance to the interference cause, interferences to your control occur by means of different coupling mechanisms.

There are:

- galvanic coupling
- capacitive coupling
- inductive coupling
- radiant coupling

(4) Basic rules for EMC

In the most times it is enough to take care of some elementary rules to guarantee the EMC. Please regard the following basic rules when installing your PLC.

- Take care of a correct area-wide grounding of the inactive metal parts when installing your components.
 - Install a central connection between the ground and the protected earth conductor system.
 - Connect all inactive metal extensive and impedance-low.
 - Please try not to use aluminium parts. Aluminium is easily oxidizing and is therefore less suitable for grounding.
- When cabling, take care of the correct line routing.
 - Organize your cabling in line groups (high voltage, current supply, signal and data lines).
 - Always lay your high voltage lines and signal respectively data lines in separate channels or bundles.
 - Route the signal and data lines as near as possible beside ground areas (e.g. suspension bars, metal rails, tin cabinet).
- Proof the correct fixing of the lead isolation.
 - Data lines must be shielded.
 - Analog lines must be shielded. When transmitting signals with small amplitudes the one sided laying of the isolation may be favorable.
 - Cables for frequency inverters, servo and stepper motors must be shielded.
 - Lay the line isolation extensively on an isolation/protected earth conductor rail directly after the cabinet entry and fix the isolation with cable clamps.
 - Make sure that the isolation/protected earth conductor rail is connected impedance-low with the cabinet.
 - Use metallic or metallized plug cases for isolated data lines.
- In special use cases you should appoint special EMC actions.
 - Consider to wire all inductivities with erase links.
 - Please consider luminescent lamps can influence signal lines.
- Create a homogeneous reference potential and ground all electrical operating supplies when possible.
 - Please take care for the targeted employment of the grounding actions. The grounding of the PLC serves for protection and functionality activity.
 - Connect installation parts and cabinets with your PLC in star topology with the isolation/protected earth conductor system. So you avoid ground loops.
 - If there are potential differences between installation parts and cabinets, lay sufficiently dimensioned potential compensation lines.

(5) Isolation of conductors

Electrical, magnetically and electromagnetic interference fields are weakened by means of an isolation, one talks of absorption. Via the isolation rail, that is connected conductive with the rack, interference currents are shunt

via cable isolation to the ground. Here you have to make sure, that the connection to the protected earth conductor is impedance-low, because otherwise the interference currents may appear as interference cause.

When isolating cables you have to regard the following:

- If possible, use only cables with isolation tangle.
- The hiding power of the isolation should be higher than 80%.
- Normally you should always lay the isolation of cables on both sides. Only by means of the both-sided connection of the isolation you achieve high quality interference suppression in the higher frequency area. Only as exception you may also lay the isolation one-sided. Then you only achieve the absorption of the lower frequencies. A one-sided isolation connection may be convenient, if:
 - the conduction of a potential compensating line is not possible.
 - analog signals (some mV respectively μA) are transferred.
 - foil isolations (static isolations) are used.
- With data lines always use metallic or metallized plugs for serial couplings. Fix the isolation of the data line at the plug rack. Do not lay the isolation on the PIN 1 of the plug bar!
- At stationary operation it is convenient to strip the insulated cable interruption free and lay it on the isolation/protected earth conductor line.
- To fix the isolation tangles use cable clamps out of metal. The clamps must clasp the isolation extensively and have well contact.
- Lay the isolation on an isolation rail directly after the entry of the cable in the cabinet.



CAUTION

Please regard at installation!

At potential differences between the grounding points, there may be a compensation current via the isolation connected at both sides.

Remedy: Potential compensation line

2.3 Overview

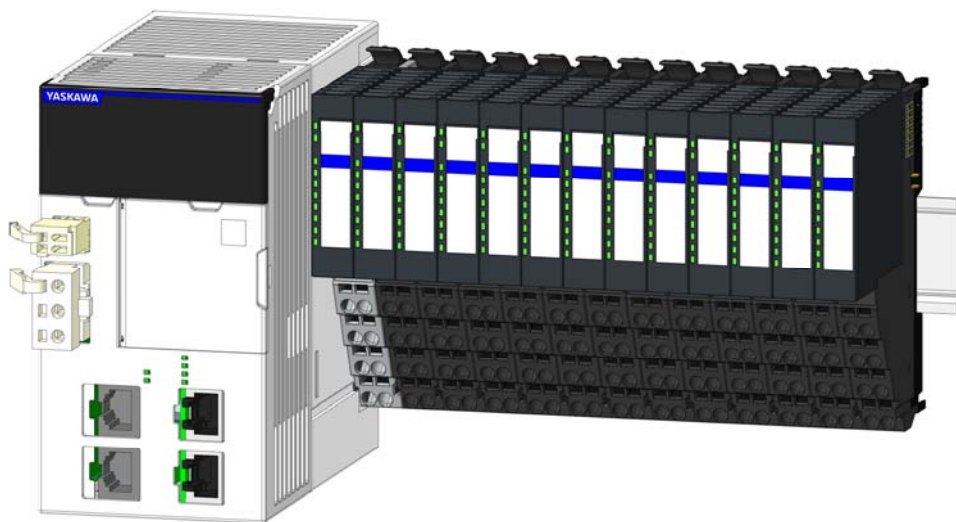
This chapter provides an overview of the iC9200.

2.3.1 iC9200

The iC9200 Series is a modular automation system for assembly on a 35×15 mm mounting rail. Due to the compatibility to the System SLIO from Yaskawa you can adapt this system exactly to your automation tasks by using the System SLIO periphery modules in 2-, 4-, 8- and 16-channel versions.

Information

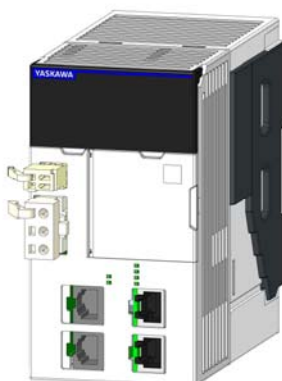
More detailed information about the usage of the System SLIO modules may be found in the according manual in the [Download Center] of www.yaskawa.eu.com under the corresponding order number.



2.3.2 Components

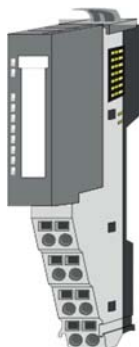
- CPU (head module)
- Power modules
- 8x periphery modules
- 16x periphery modules
- Accessories

(1) CPU iC9226M-EC



With the CPU iC9226M-EC electronics and power supply are integrated in one housing. The CPU is programmed and configured with iCube Engineer from Yaskawa in IEC 61131-3. On the right side via the SliceBus you can connect System SLIO periphery modules from Yaskawa. As head module via the integrated power module for power supply CPU electronic as well as the electronic of the periphery modules, which are connected via the SliceBus. For the connection of the power supply the CPU has a removable connector. To supply the power section of the connected periphery modules, you must always plug in the power module 007-1AB00 - DC 24V 10A directly after the CPU.

(2) Power Modules

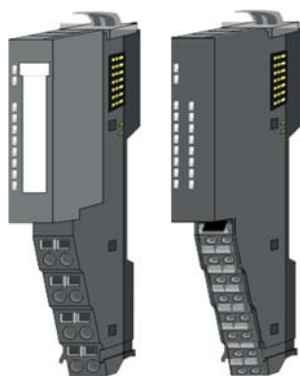


Information

When using System SLIO modules, you must always mount the power module 007-1AB00 - DC 24V 10A, because the CPU does not provide a power section supply due to the system.

The color-coded power modules are used when the CPU does not provide power section supply, like the CPU iC9226M-EC. These are also to be used if the power section supply of the I/O level or the electronic power supply is no longer sufficient. Depending on the power module used, you have the option of forming isolated groups. The power modules are to be supplied externally with DC 24V. Each power module has over voltage and reverse polarity protection.

(3) Periphery Modules

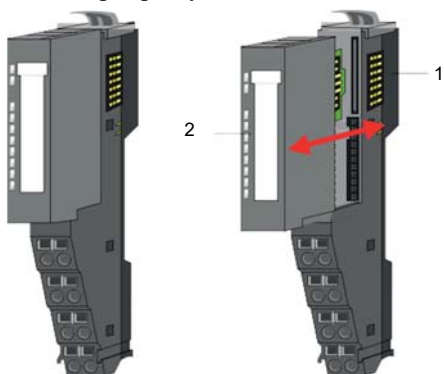


The periphery modules are available in the following versions, whereby of each the electronic part can be replaced with standing wiring:

- 8x periphery modules for a maximum of 8 channels.
 - Standard periphery modules
- 16x periphery module for a maximum of 16 channels.

(4) 8x Periphery Modules

Each 8x periphery module consists of a terminal and an electronic module.



- 1 Terminal module
- 2 Electronic module

(5) Terminal Module



The terminal module serves to carry the electronic module, contains the backplane bus with power supply for the electronic, the DC 24V power section supply and the staircase-shaped terminal for wiring. Additionally, the terminal module has a locking system for fixing it at a mounting rail. By means of this locking system your system may be assembled outside of your switchgear cabinet to be later mounted there as whole system.

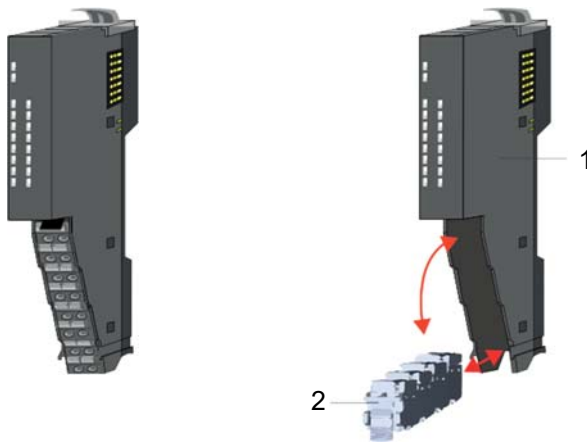
(6) Electronic Module



The functionality of a periphery module is defined by the electronic module, which is mounted to the terminal module by a sliding mechanism. With an error the defective electronic module may be exchanged for a functional module. Here the wiring persists. At the front side there are LEDs for status indication. For easy wiring, you will find the corresponding connection information for each electronic module on the front and on the side.

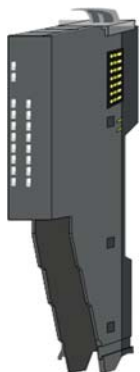
(7) 16x Periphery Modules

Each 16x periphery module consists of an electronic unit and a terminal block.



- 1 Electronic unit
- 2 Terminal block

(8) Electronic Unit



The functionality of a 16x periphery module is defined via the terminal block, which is connected to the electronic unit via a secure flap mechanism. In the case of an error you can exchange the defective electronic unit for a functional unit with standing wiring. At the front side there are LEDs for status indication. For easy wiring each electronic unit shows a corresponding connection diagram at the side. The electronic unit provides the slot for the terminal block for the wiring and contains the backplane bus with power supply for the electronic and the connection to the DC 24V power section supply. Additionally, the electronic unit has a locking system for fixing it at a mounting rail. By means of this locking system your system may be assembled outside of your switchgear cabinet to be later mounted there as whole system.

(9) Terminal Block



The terminal block provides the electrical interface for the signaling and supplies lines of the module. When mounting the terminal block, it is attached to the bottom of the electronic unit and turned towards the electronic unit until it clicks into place. With the wiring a "push-in" spring-clip technique is used. This allows a quick and easy connection of your signal and supply lines. The clamping off takes place by means of a screwdriver.

(10) Accessories

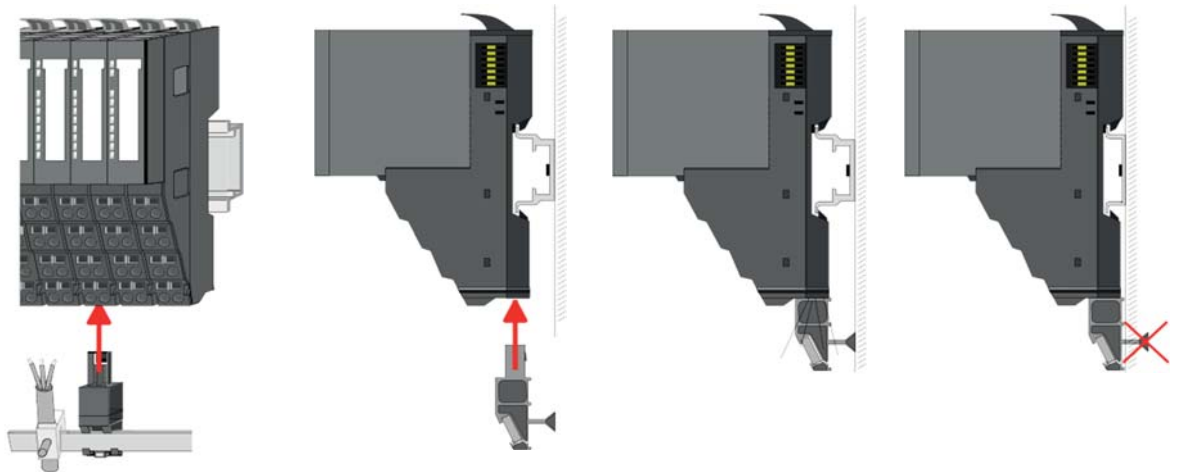
(a) Shield Bus Carrier

Information

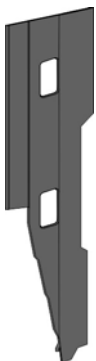
Please note that no shield bus carrier can be mounted on the CPU iC9226M-EC and a 16x periphery module!



The shield bus carrier (order no.: 000-0AB00) serves to carry the shield bus (10mm x 3mm) to connect cable shields. Shield bus carriers, shield bus and shield fixings are not in the scope of delivery. They are only available as accessories. The shield bus carrier is mounted underneath the terminal of the terminal module. With a flat mounting rail for adaptation to a flat mounting rail you may remove the spacer of the shield bus carrier.



(b) Bus Cover



With each head module, to protect the backplane bus connectors, there is a mounted bus cover in the scope of delivery. You have to remove the bus cover of the head module before mounting a System SLIO module. For the protection of the backplane bus connector, you always have to mount the bus cover at the last module of your system again. The bus cover has the order no. 000-0AA00.

(c) Coding Pins



Information Please note that a coding pin cannot be installed on a 16x periphery module! Here you have to make sure that the associated terminal block is plugged again when the electronics unit is replaced.

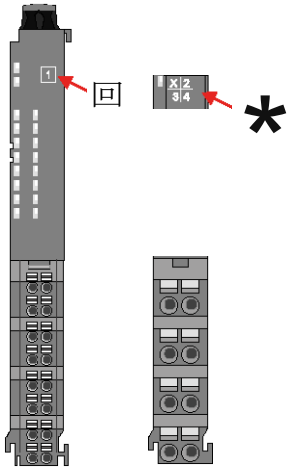
There is the possibility to fix the assignment of electronic and terminal module. Here coding pins (order number 000-0AC00) from Yaskawa can be used. The coding pin consists of a coding jack and a coding plug. By combining electronic and terminal module with coding pin, the coding jack remains in the electronic module and the coding plug in the terminal module. This ensures that after replacing the electronic module just another electronic module can be plugged with the same encoding.

2.3.3 Hardware Revision

- The hardware revision is printed on every module.
- Since a System SLIO 8x periphery module consists of a terminal and electronic module, you will find a hardware revision printed on each of them.
- The hardware revision of the iC9226M-EC is indicated on the left side nameplate.



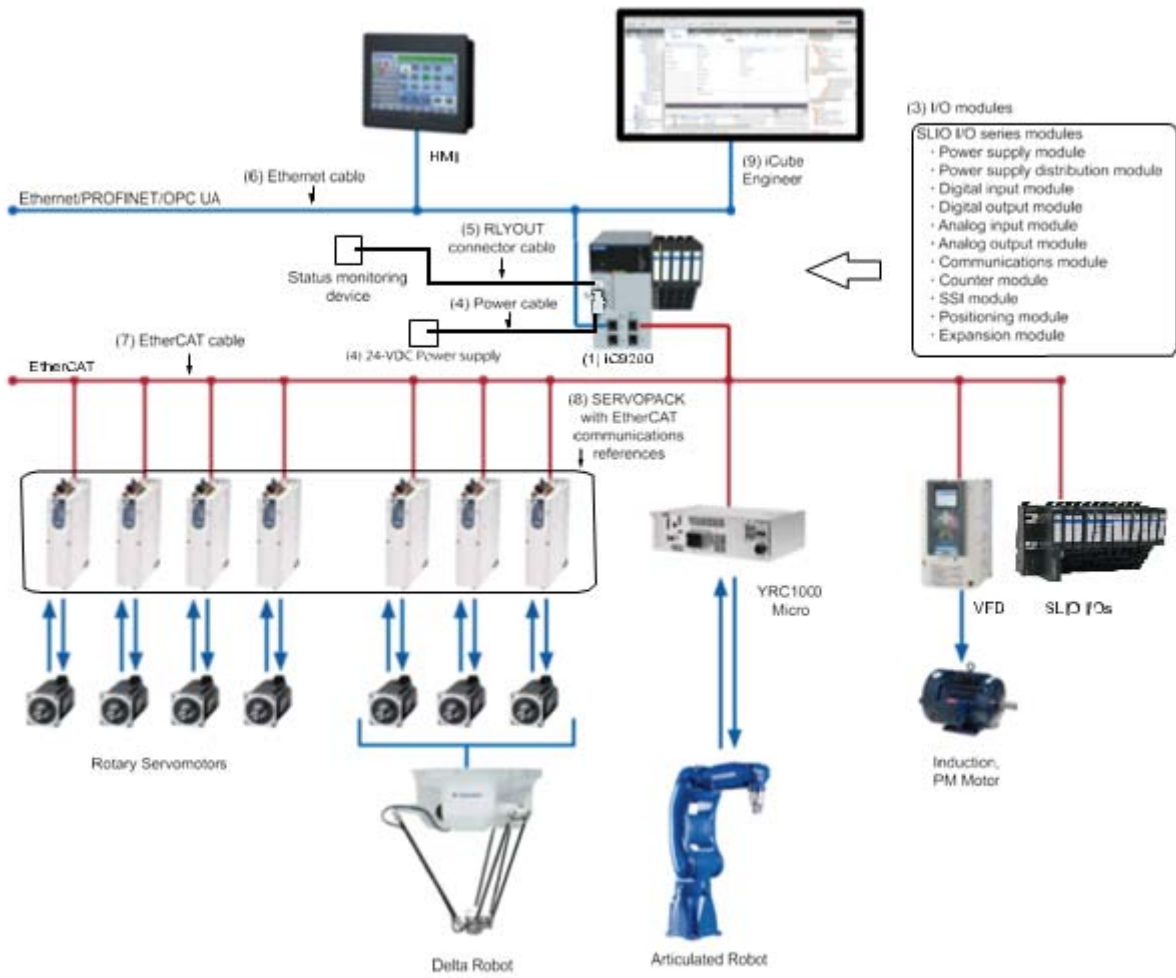
- Authoritative for the hardware revision of a System SLIO module is the hardware revision of the electronic module. This is always located under the labeling strip of the corresponding electronic module.
- Depending on the module type, there are the following 2 variants e.g. to indicate hardware revision 1:
 - With current labelling there is a **1** on the front.
 - With earlier labelling, the 1 is marked with [X] on a number grid.




2.4 System Configuration Example

The following figure shows a typical system configuration. Refer to the following section for details on (1) to (9) in the following figure.

☞ 2.5 Devices and Components That Can Be Used to Build a System on page 38







The iC9200 has four RJ-45 connectors.
 When wiring the product, be careful not to use the wrong connector.
Important

2.5 Devices and Components That Can Be Used to Build a System

The following table lists the devices and components that are required to build the system that is shown in the previous page. The numbers (1) to (9) correspond to the numbers in the figure that is shown in the previous page.

No.	Name	Use	Model	Remarks
(1)	iC9200	Programmable Machine Controller		Refer to the following section for details.  2.3 Overview on page 30
(2)	I/O Module	A module that is used to connect I/O signals to peripheral devices.		Refer to the following section for details.  2.6 Specifications for Module Combinations on page 39
(3)	Power Cable	Connects the iC9200 to a 24-VDC power supply.		Use a commercially available cable that meets the following conditions: <ul style="list-style-type: none"> • Wire size: AWG20 to AWG14 (0.5 mm² to 2.0 mm²) • Twisted-pair wire
(4)	24-VDC Power Supply	Supplies power to the power supply section of the iC9200.		Make sure to use a power supply with reinforced insulation or double insulation.
(5)	RLYOUT Connector Cable	Connects the iC9200 to a status monitoring device.		Use a commercially available cable that meets the following conditions: <ul style="list-style-type: none"> • Wire size: AWG28 to AWG14 (0.08 mm² to 2.0 mm²) • Sheath outer diameter: 3.3 mm max.
(6)	Ethernet Cable	Used to connect the iC9200 to Ethernet communications devices or to connect the iC9200 to a PC that has iCube Engineer installed on it.		Use a commercially available cable that meets the following conditions: <ul style="list-style-type: none"> • Ethernet specification: 10Base-T/100Base-TX <ul style="list-style-type: none"> – Category 5 or higher (with 8 conductors <i>*1</i>) – Twisted-pair cable with RJ-45 connectors • Ethernet specification: 1000Base-T <ul style="list-style-type: none"> – Category 5e or higher – Shielded twisted-pair cable with RJ-45 connectors
(7)	EtherCAT Cable (RJ-45 connector on both ends)	Connects the iC9200 to EtherCAT communications devices.	JZSP-xxxx-□□□□-E	Standard cable Length: 0.2 to 30 m
			JZSP-xxxx-□□□□-E	Cable with ferrite cores Length: 0.3 to 50 m
(8)	SERVOPACK with EtherCAT Communications	Used to control servomotors.	SGDXS-□□□□A0□□□□□□□□	Σ-X-series Σ-XS SERVOPACK with EtherCAT communications
			SGDXW-□□□□A0□□□□□□□□	Σ-X-series Σ-XW SERVOPACK with EtherCAT communications
			SGDXT-□□□□A0□□□□□□□□	Σ-X-series Σ-XT SERVOPACK with EtherCAT communications
			SGD7-□□□□A0□□□□□□□□	Σ-7-series Σ-7S SERVOPACK with EtherCAT communications
			SGD7W-□□□□A0□□□□□□□□	Σ-7-series Σ-7W SERVOPACK with EtherCAT communications
(9)	iCube Engineer	Used to adjust, maintain, and program the iC9226M.	JXPMC-ICE100	–

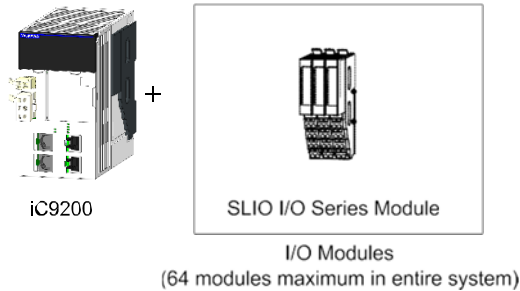
*1 A 4-conductor cable can also be connected if the network does not have devices that support 1000BASE-T.

2.6 Specifications for Module Combinations

The specifications when iC9200 modules are combined is given next.

2.6.1 Specifications and Restrictions for iC9200 Module Combinations

There are restrictions in the order in which you can connect the modules. Build the rack by connecting each module in the order that is shown below.



Item	Description
Maximum Configuration of iC9200 Controller	<ul style="list-style-type: none"> Maximum number of racks: 1 iC9200: One unit only in the controller system.
Maximum Configuration of I/O Modules	<ul style="list-style-type: none"> 64 modules maximum (Including SLIO expansion master module and SLIO expansion slave modules for expansion. The maximum number of units is 56 modules when using 4 racks, the maximum number of expansion I/O racks.) Note that the SLIO power supply module is not counted in the number of I/O modules. Maximum number of expansion racks: 4

2.6.2 Current Consumption and Rack Width Restrictions

When mounting multiple I/O modules, make sure the following conditions are met.

(1) Current Consumption

Output current of the power supply section $*1 \leq$ rated current of the power supply section (3 A)

*1 This is the total of the maximum internal current consumption of all I/O modules that are mounted to the iC9200.

Note:

The power supply section of the iC9200 has an overcurrent protection function to protect the equipment.

If the rated current of the power supply section is exceeded, the protection function will activate and the power supply to the system will be shut OFF.

Configure the I/O modules so that the power supply capacity is satisfied by adding power supply modules as necessary.

Ensure that the overcurrent protection function does not activate by referring to the manual for each connected module and checking the current consumption in advance.

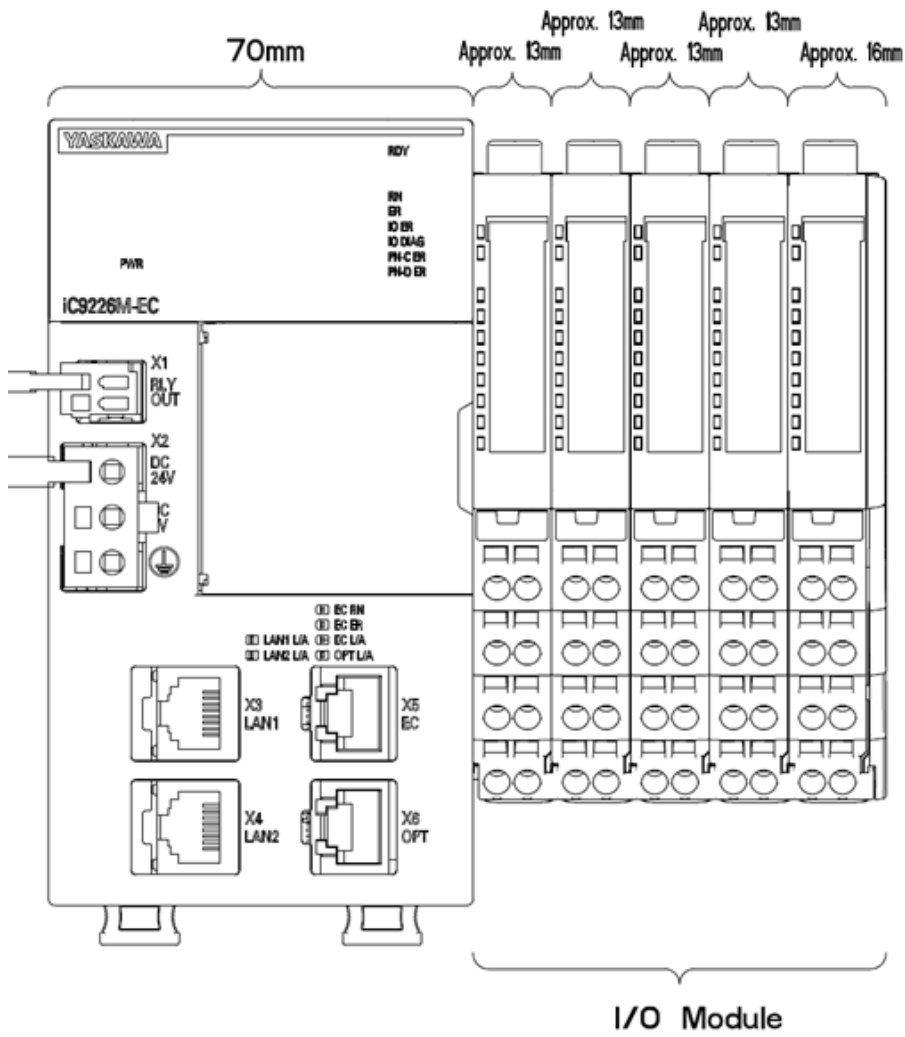
(2) Rack Width

The unit width of the iC9200 (model number: JEYRM-MPX022□□10L32-□) is 70 mm.

Also consider the width of the SLIO I/O series modules that you will use, and select a DIN rail with a length 25 mm or longer than the rack width.

<Example>

A rack with the configuration shown in the following diagram has a rack width of about 138 mm.



Installation and Wiring

This chapter describes the installation and wiring of the iC9200.

3.1	Properties	42
3.2	Installing the iC9200	43
3.2.1	Mounting CPU	43
3.2.2	Mounting Periphery Modules	45
3.3	Wiring the iC9200	47
3.3.1	Wiring the Power Supply	47
3.3.2	Wiring a Status Monitoring Device.....	48
3.3.3	Connecting EtherCAT Communications Devices.....	49
3.3.4	Connecting Ethernet Communications Devices	50
3.3.5	Wiring System SLIO Periphery.....	51

3.1 Properties

The following table describes the properties of the iC9200.

Hardware	Properties
CPU (iC9226M-EC)	<ul style="list-style-type: none">• Programmable in IEC 61131 via Yaskawa iCube Engineer.• Slot for external Yaskawa SD card.• Status LEDs for operating state and diagnostics.• X5: EtherCAT MDevice functionality.• X6: Ethernet interface for future extensions.• X3/X4: Ethernet (switch) - PROFINET optional.• Up to 64 System SLIO modules can be connected via <i>SliceBus</i>.
Memory	<ul style="list-style-type: none">• 2GB working memory (RAM).• 12MB program memory.• 32MB data memory.• 3072kB retentive data memory.

3.2 Installing the iC9200

Use a DIN rail to install the iC9200.

Refer to the following section for the installation and operating conditions.

☞ [5.1 iC9200 Installation and Operating Conditions on page 130](#)



Important

There are restrictions on the module configuration of iC9200 modules.

Refer to the following section for details.

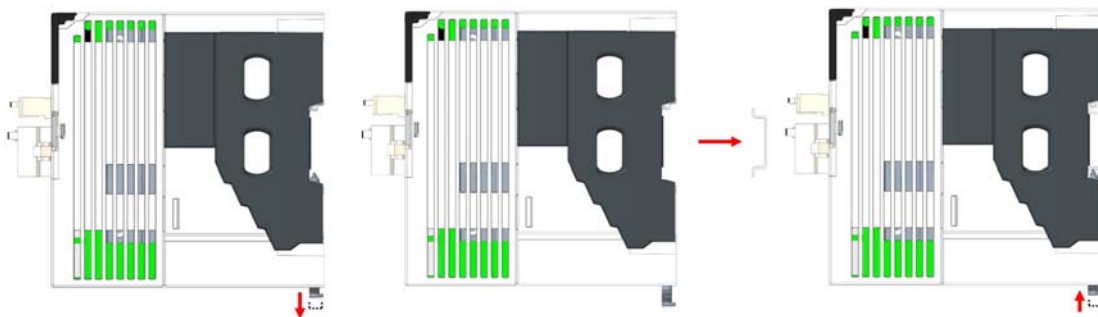
☞ [2.5 Devices and Components That Can Be Used to Build a System on page 38](#)

3.2.1 Mounting CPU

(1) Functional Principle

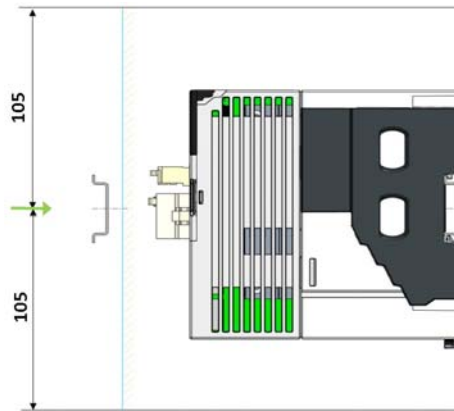
Move the DIN rail lock in under CPU to the open position. Hook the CPU to the top of the DIN rail and push it back to fix it to the mounting surface. Move the DIN rail lock to the locked position. The CPU is directly mounted at a mounting rail. Up to 64 System SLIO modules may be mounted.

The electronic power supply for the modules is connected via the connection to the backplane bus. The power module 007-1AB00 must always be installed at the right side of the CPU for the power section supply of the modules.

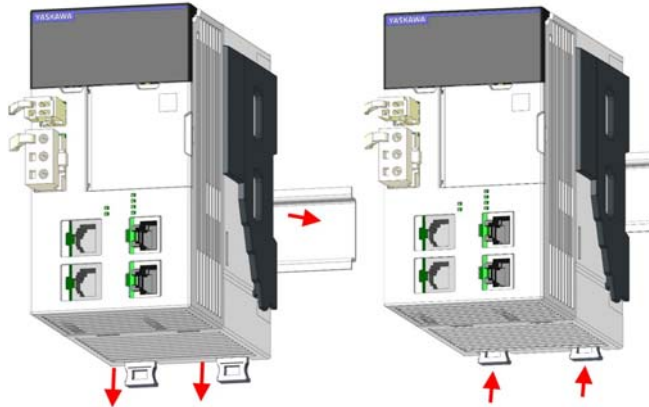


(a) Proceeding

1. **Mount the mounting rail!** Please consider that a clearance from the middle of the mounting rail of at least 105mm above and below exists.
And consider a clearance of at least 10 mm horizontally from the CPU (and SLIO) on either side.



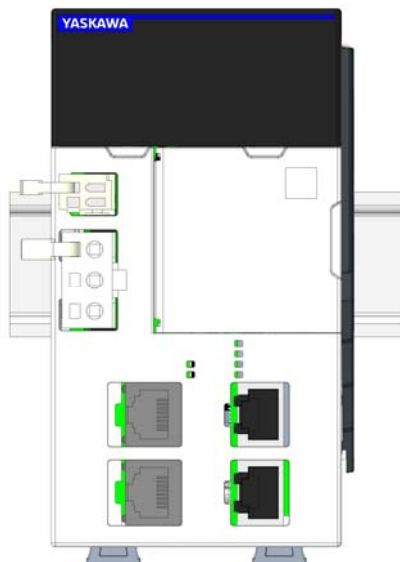
2. **Pull the locking brackets downward, place the CPU at the mounting rail and push the brackets upward.**



If you want to use the CPU without periphery modules, you can wire it now.

(2) Assembly Possibilities

Horizontal hanging:

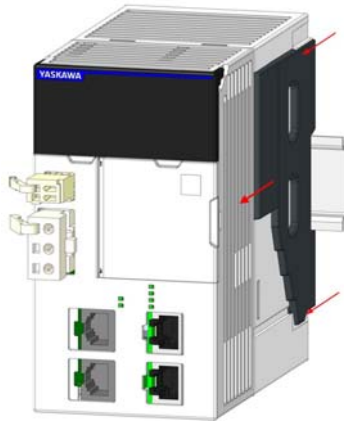


3.2.2 Mounting Peripheral Modules

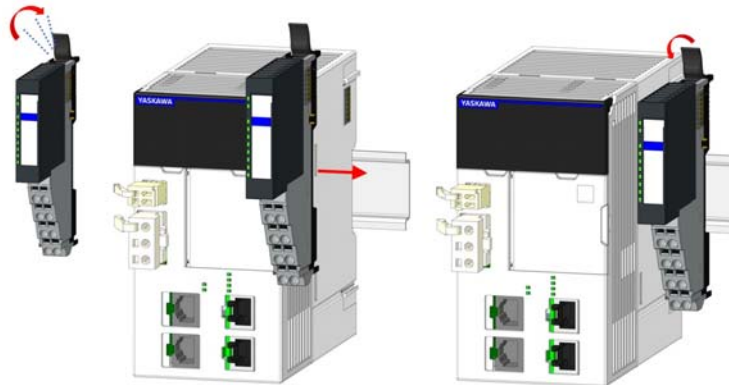
Information When using System SLIO modules, you must always mount the power module 007-1AB00 - DC 24V 10A, because the CPU does not provide a power section supply due to the system.

(1) Mounting Power Module 007-1AB00

1. Before mounting the peripheral modules, you have to remove the bus cover at the right side of the CPU by pulling it forward. Keep the cover for later mounting.



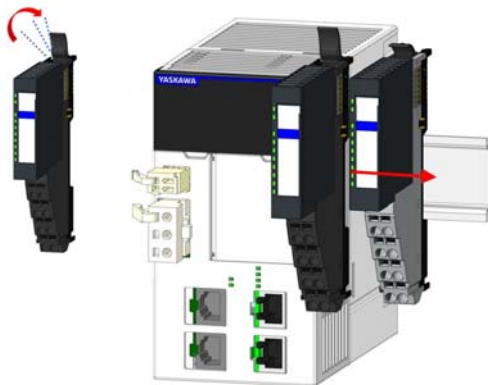
2. Mount the peripheral modules you want.



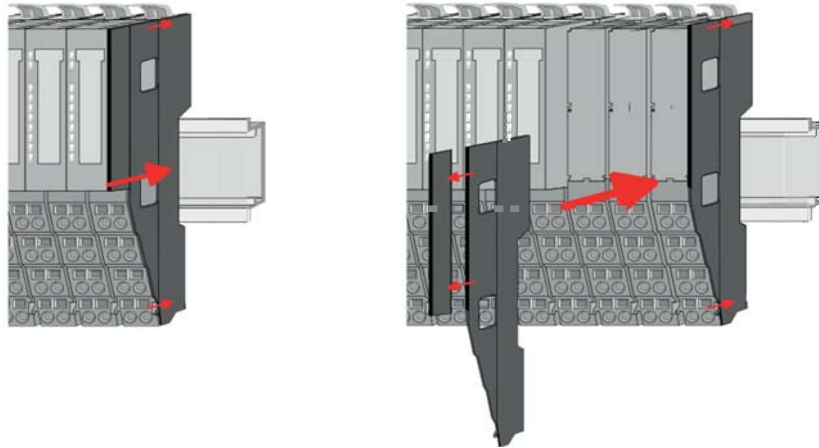
(2) Mounting Peripheral Modules

The procedure is identical for 8x and 16x periphery modules.

1. Mount the peripheral modules you want.



2. After mounting the whole system, to protect the backplane bus connectors at the last module you have to mount the bus cover, now. If the last module is a clamp module, for adaptation the upper part of the bus cover is to be removed.



The system can now be wired.

3.3 Wiring the iC9200

This chapter describes wiring the iC9200 to various devices.

3.3.1 Wiring the Power Supply



Input power within the rated voltage over the wiring to the iC9200.

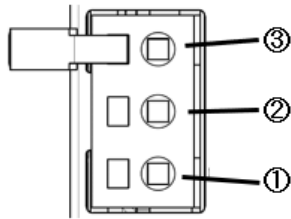
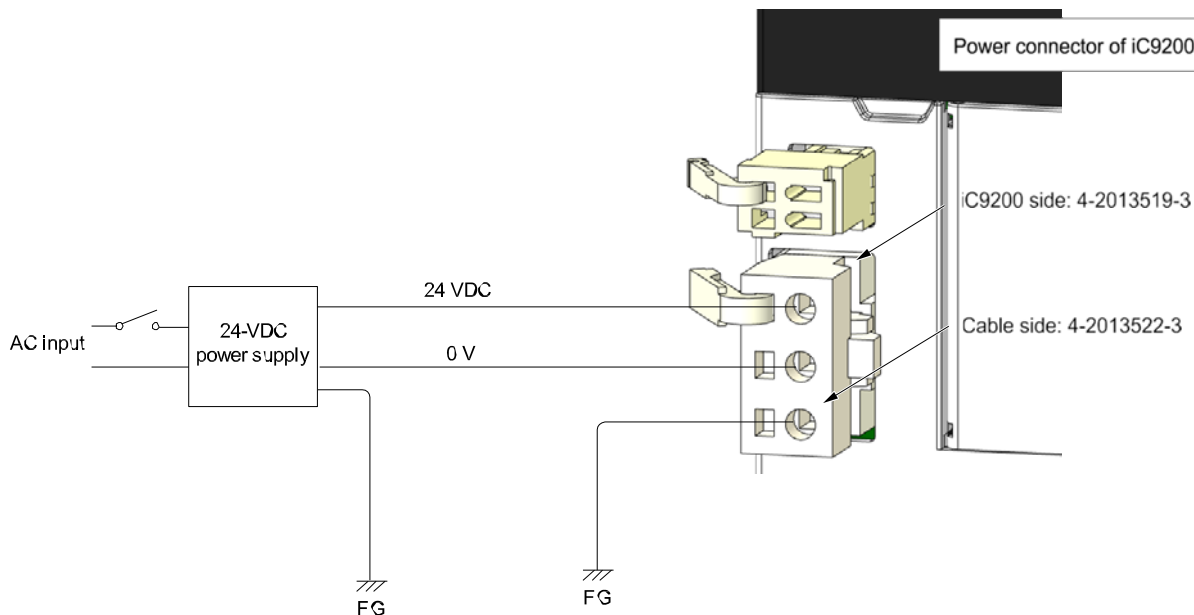
Important

Use a 24-VDC power supply to supply power to the power connector on the iC9200 (model number: JEYRM-MPX022□□10L32-□).

This section describes the specifications, pin assignments, and connection method for the power connector.

Name	Connectors	No. of Pins	Connector Model No.		
			Unit Side	Cable Side	Manufacturer
Power Connector	X2	3	4-2013519-3	4-2013522-3	TE Connectivity Ltd.

Pin No.	Signal Label	Description
3	DC24V	24-VDC input
2	DC0V	0-VDC input
1	FG	Connect to the frame ground.

Note:

Use an isolated 24-VDC power supply and install the power switch on the AC side.

If you install the power switch on the 24-VDC side, inrush current of approximately 40 A will flow when the power is turned ON.

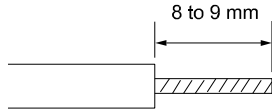
(1) Creating the 24-VDC Power Cable

The power terminal is a removable connector. Use the following procedure to wire the power connector. When connecting the power connector on the iC9200 to a 24-VDC power supply, use twisted-pair wires with a wire size between AWG20 and AWG14 (0.5 mm² and 2.0 mm²).

Use the following procedure to create the power cable.

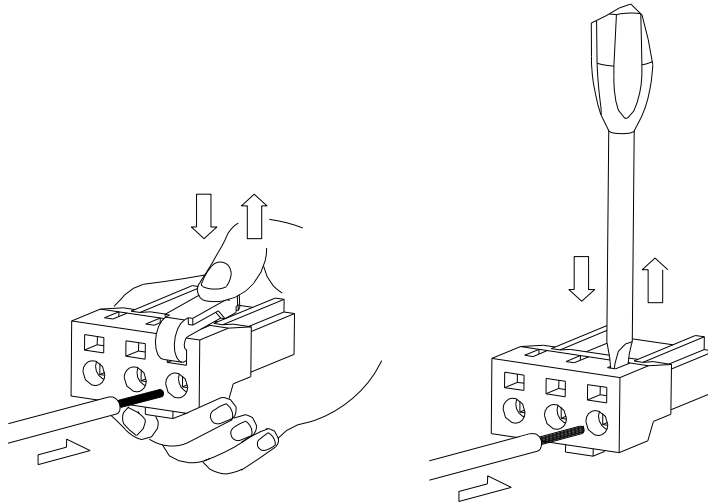
1. Strip the sheath covering the wires.

Expose the conductor by stripping the sheath about 8 to 9 mm from the tip.



2. Clamp the wire.

Push the conductor all the way into the plug and clamp it.



3.3.2 Wiring a Status Monitoring Device

Wire a status monitoring device to the RLY OUT connector on the iC9200. The RLY OUT connector is NO contact relay output in a status output terminal. The terminal works in conjunction with the RDY LED indicator. When the RDY LED indicator is lit, the terminal is short circuited, and when the RDY LED indicator is not lit, the terminal is open.

Information The lit status of the RDY LED indicator means that the iC9200 is operating normally. It does not mean that a user program is running.

(1) RLY OUT Connector Specifications

This connector works in conjunction with the RDY LED indicator on the iC9200.

RDY LED indicator is lit: Short circuited

RDY LED indicator is not lit: Open

(a) Contact Ratings

Input Voltage	Current Capacity
24 VDC	0.5 A (resistive load)
	0.25 A (inductive load)

(2) RLY OUT Connector Cable

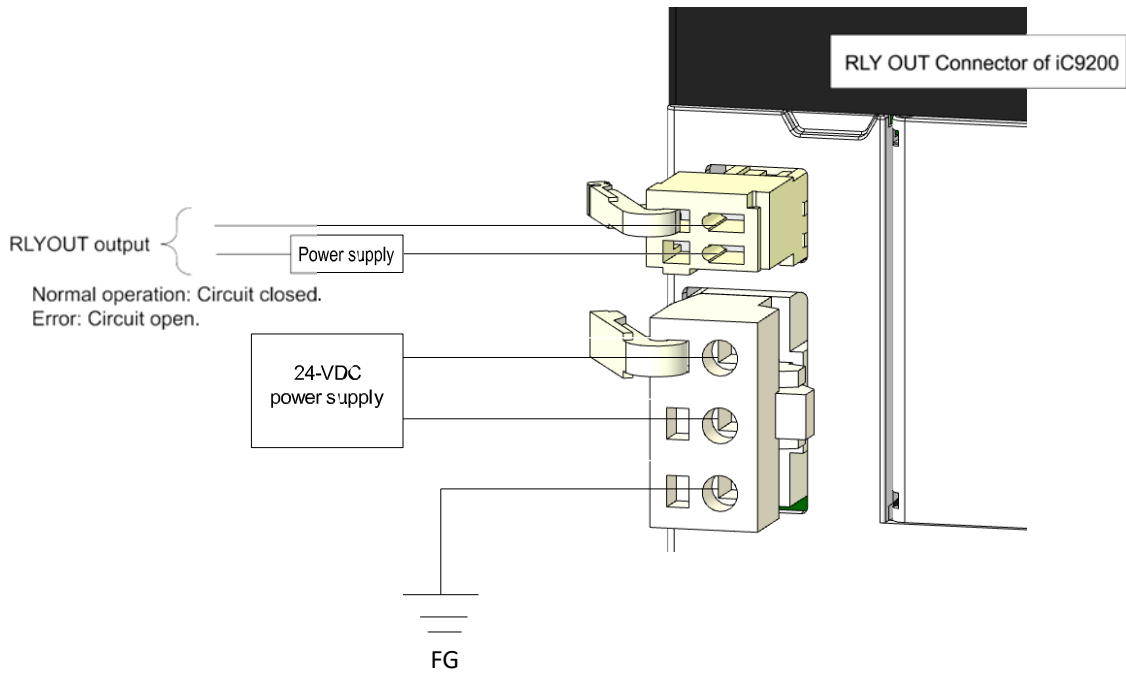
For the RLY OUT connector cable, use a cable with a wire size of AWG28 to AWG14 (0.08 mm² to 2.0 mm²) and a outer sheath diameter of 3.3 mm or less.

The procedure to create the RLY OUT connector cable is the same as that for the power cable.

(1) [Creating the 24-VDC Power Cable on page 47](#)

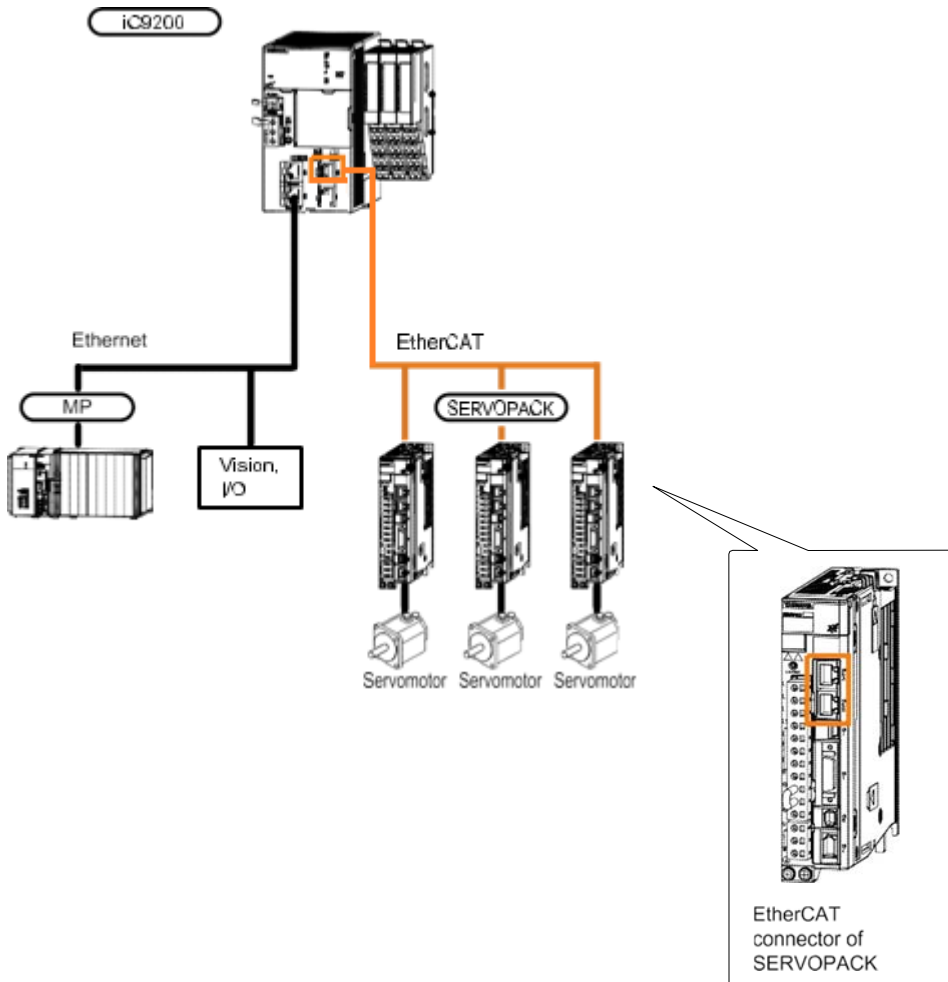
(3) Example RLY OUT Connector Connection

Refer to the following figure for the method to connect the RLY OUT connector.



3.3.3 Connecting EtherCAT Communications Devices

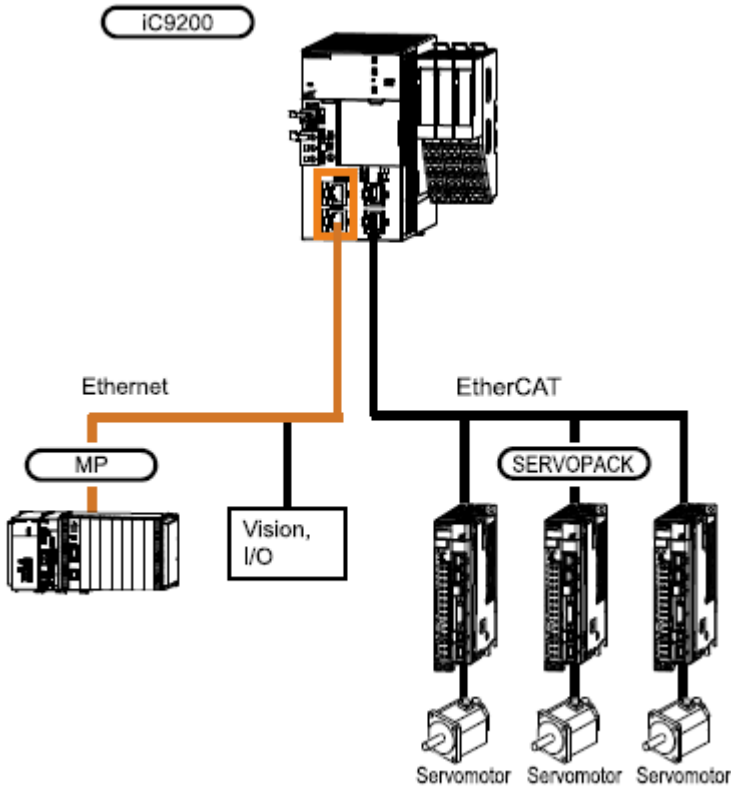
Connect the iC9200 and EtherCAT communications devices with an EtherCAT cable on X5.



3.3.4 Connecting Ethernet Communications Devices

Connect the iC9200 and an Ethernet communications device with an Ethernet cable.

Information The iC9200 has two Ethernet connectors. You can use port X3 or X4 for Ethernet or PROFINET.



3.3.5 Wiring System SLIO Periphery

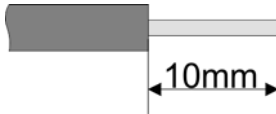
Information When using System SLIO modules, you must always mount the power module 007-1AB00 - DC 24V 10A, because the CPU does not provide a power section supply due to the system.

(1) Wiring Power Module

(a) Terminal Module Terminals

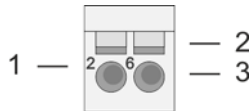
With the power module, terminals with spring clamp technology are used for wiring. The spring clamp technology allows quick and easy connection of your supply lines. In contrast to screw terminal connections this type of connection is vibration proof.

(b) Data



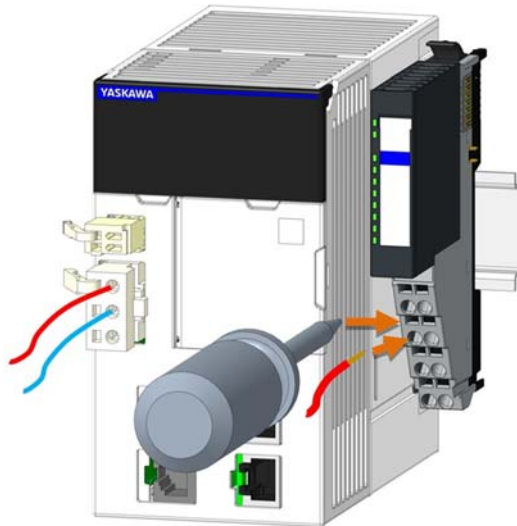
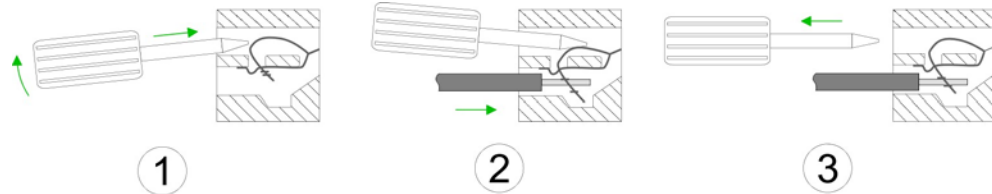
U_{\max}	30V DC
I_{\max}	10A
Cross section	0.08 ... 1.5mm ² (AWG 28 ... 16)
Stripping length	10mm

(c) Wiring Proceeding



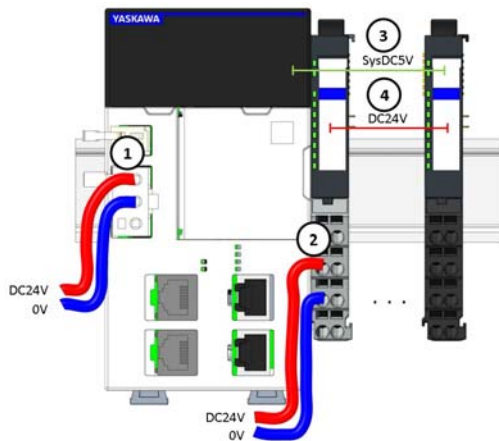
- 1 Pin no. at the connector
- 2 Opening for screwdriver
- 3 Connection hole for wire

1. Insert a suited screwdriver at an angle into the square opening as shown. Press and hold the screwdriver in the opposite direction to open the contact spring.



2. Insert the stripped end of wire into the round opening. You can use wires with a cross section of 0.08mm² up to 1.5mm².
3. By removing the screwdriver, the wire is securely fixed via the spring contact to the terminal.

(d) Standard Wiring



- (1) DC 24V supply CPU:
DC 5V electronic section supply I/O area (max. 3A)
- (2) Power module 007-1AB00:
DC 24V power section supply (max. 10A)
- (3) DC 5V electronic section supply I/O area
- (4) DC 24V power section supply I/O area



CAUTION

Since the power section supply is not internally protected, it is to be externally protected with a fuse, which corresponds to the maximum current. This means max. 10A is to be protected by a 10A fuse (fast) respectively by a line circuit breaker 10A characteristics Z!

(e) Fusing


- The power section supply is to be externally protected with a fuse, which corresponds to the maximum current. This means max. 10A is to be protected with a 10A fuse (fast) respectively by a line circuit breaker 10A characteristics Z!
- It is recommended to externally protect the electronic power section supply for CPU an I/O area with a 2A fuse (fast) respectively by a line circuit breaker 2A characteristics Z.

(f) State of the Electronic Power Supply via LEDs

After PowerON the RUN respectively MF LED at every System SLIO module is on, so far as the sum current does not exceed the maximum value. With the CPU this is 3A. If the total current exceeds the maximum value, the LEDs are no longer triggered. Here the power module with the order number 007-1AB10 is to be placed between the periphery modules.

(2) Wiring 8x Periphery Modules

(a) Terminal Module Terminals

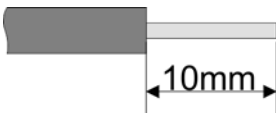

CAUTION

Do not connect hazardous voltages!
If this is not explicitly stated in the corresponding module description, hazardous voltages are not allowed to be connected to the corresponding terminal module!

Danger of injury from electrical shock and damage to the CPU respectively to the modules!
Put the iC9200 Series in a safe, powered down state before starting installation, disassembly or wiring of the iC9200 Series modules!

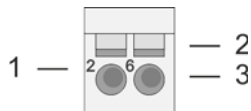
With wiring the terminal modules, terminals with spring clamp technology are used for wiring. The spring clamp technology allows quick and easy connection of your signal and supply lines. In contrast to screw terminal connections this type of connection is vibration proof.

(b) Data

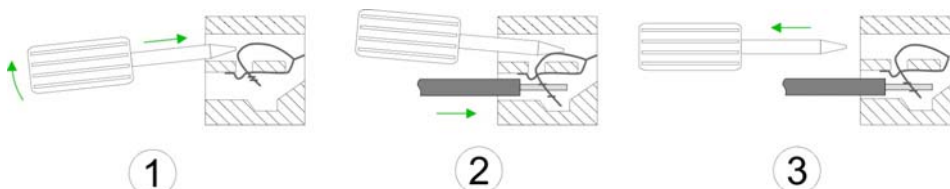


U _{max}	240VAC / 30V DC
I _{max}	10A
Cross section	0.08 ... 1.5mm ² (AWG 28 ... 16)
Stripping length	10mm

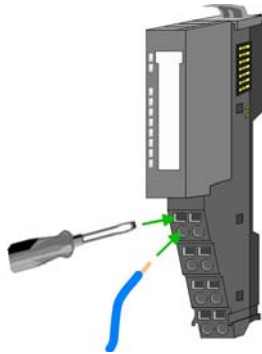
(c) Wiring Proceeding



- 1 Pin no. at the connector
- 2 Opening for screwdriver
- 3 Connection hole for wire



1. Insert a suited screwdriver at an angle into the square opening as shown. Press and hold the screwdriver in the opposite direction to open the contact spring.

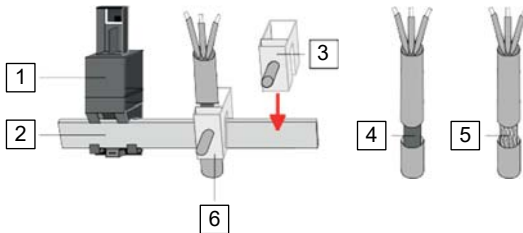


2. Insert the stripped end of wire into the round opening. You can use wires with a cross section of 0.08mm² up to 1.5mm².
3. By removing the screwdriver, the wire is securely fixed via the spring contact to the terminal.

(d) Shielding

◆ Overview

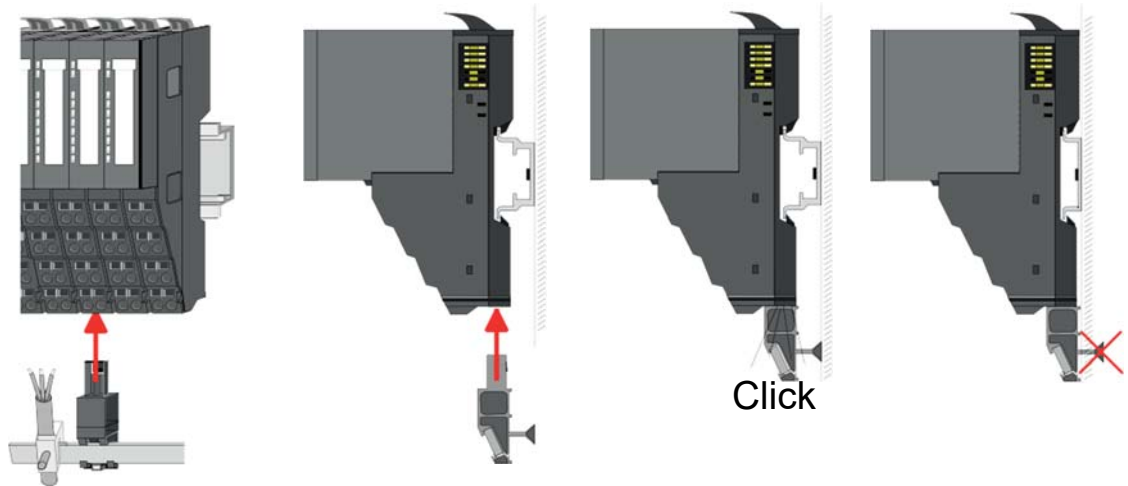
Shielding is required for interference-free signal transmission. This weakens electrical, magnetic or electromagnetic interference fields. To attach the shield the mounting of shield bus carriers are necessary. The shield bus carrier (available as accessory) serves to carry the shield bus to connect cable shields. [2.2.2 Installation Guidelines on page 27](#)



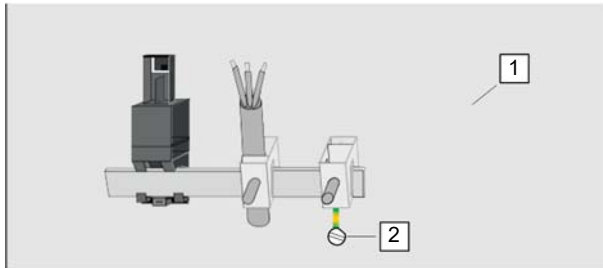
- | | |
|---|--------------------------------------------|
| 1 | Shield bus carrier |
| 2 | Shield bus (10mm x 3mm) |
| 3 | Shield clamp |
| 4 | Cable shield with metal foil |
| 5 | Cable shield with wire mesh (close-meshed) |
| 6 | Cable shield mounted with shield clamp |

◆ Shield Attachment

1. Each iC9200 Series 8x periphery module has a carrier hole for the shield bus carrier. Push the shield bus carrier, until they engage into the module. With a flat mounting rail for adaptation to a flat mounting rail you may remove the spacer of the shield bus carrier.
2. Put your shield bus into the shield bus carrier.



3. **Attach the cables with the accordingly stripped cable screen and fix it by the shield clamp with the shield bus.**
4. **The shield bus must always be earthed. Keep all cable connections as short as possible. To earth the shield bus, connect a PE conductor to the shield bus via a shield clamp and screw it to the base plate as close as possible and with low impedance.**



- 1** Base plate
- 2** PE conductor screwed to base plate

(3) Wiring 16x Periphery Modules

(a) Terminal Block Connectors



CAUTION

Do not connect hazardous voltages!

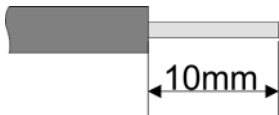
If this is not explicitly stated in the corresponding module description, hazardous voltages are not allowed to be connected to the corresponding terminal block!

Danger of injury from electrical shock and damage to the CPU respectively to the modules!

Put the iC9200 Series in a safe, powered down state before starting installation, disassembly or wiring of the iC9200 Series modules!

- The 16x periphery module has a removable terminal block for wiring.
- With the wiring of the terminal block a "push-in" spring-clip technique is used. This allows a quick and easy connection of your signal and supply lines.
- The clamping off takes place by means of a screwdriver.
- Please use copper wire only!

(b) Data



U _{max}	30V DC
I _{max}	10A
Cross section solid wire	0.25 ... 0.75mm ²
Cross section with ferrule	0.14 ... 0.75mm ²
Wire type	CU
AWG	24 ... 16
Stripping length	10mm

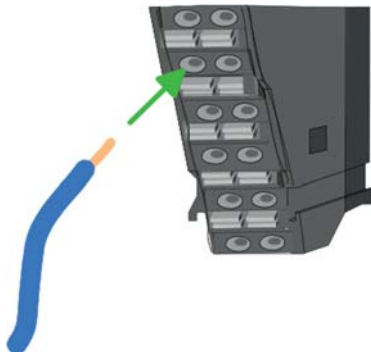
(c) Wiring Procedure



- 1 Release area
- 2 Connection hole for wire

◆ **Insert Wire**

The wiring happens without a tool.

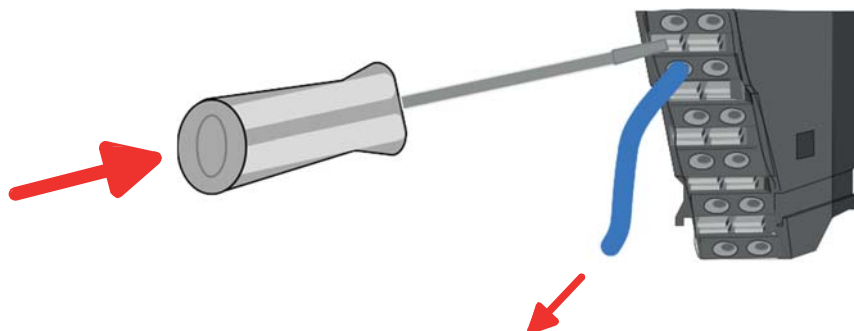


1. **Determine according to the casing labelling the connection position.**
2. **Insert through the round connection hole of the according contact your prepared wire until it stops, so that it is fixed.**
By pushing the contact spring opens, thus ensuring the necessary contact pressure.

◆ **Remove Wire**

The wire is to be removed by means of a screwdriver with 2.5mm blade width.

1. **Press with your screwdriver vertically at the release button.**



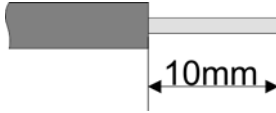
- The contact spring releases the wire.
2. **Pull the wire from the round hole.**

(4) Wiring Power Modules

(a) Terminal Module Terminals

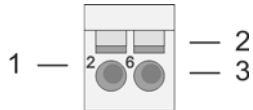
Power modules can be plugged between the periphery modules. With power modules, terminals with spring clamp technology are used for wiring. The spring clamp technology allows quick and easy connection of your signal and supply lines. In contrast to screw terminal connections this type of connection is vibration proof.

(b) Data

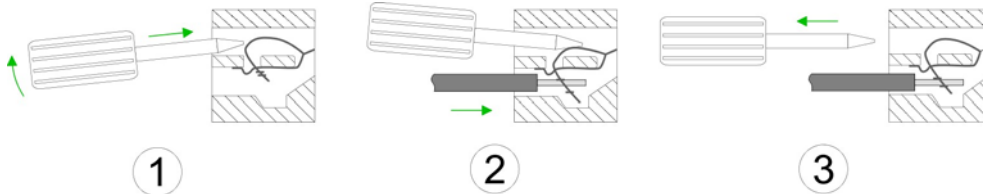


U_{\max}	30V DC
I_{\max}	10A
Cross section	0.08 ... 1.5mm ² (AWG 28 ... 16)
Stripping length	10mm

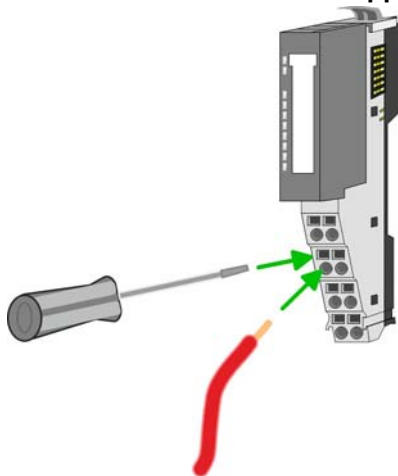
(c) Wiring Procedure



- 1 Pin number at the connector
- 2 Opening for screwdriver
- 3 Connection hole for wire



1. Insert a suited screwdriver at an angle into the square opening as shown. Press and hold the screwdriver in the opposite direction to open the contact spring.

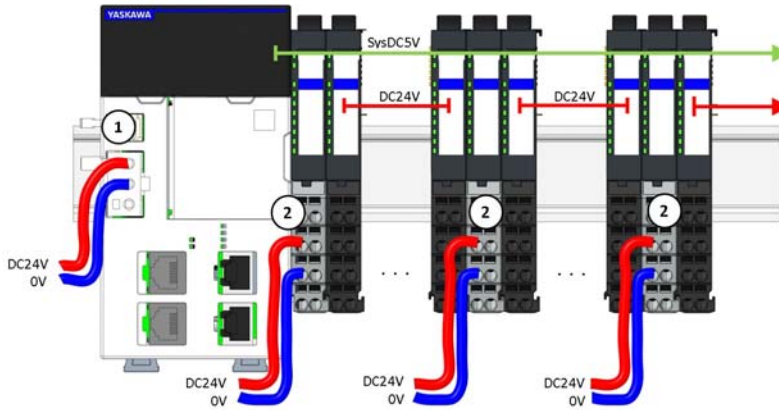


2. Insert the stripped end of wire into the round opening. You can use wires with a cross section of 0.08mm² up to 1.5mm²
3. By removing the screwdriver, the wire is securely fixed via the spring contact to the terminal.

(d) Deployment of the Power Modules

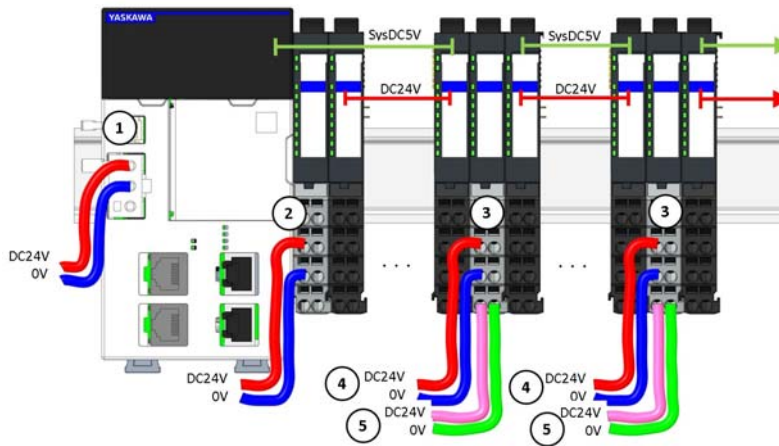
- The CPU does not provide a power section supply for the peripheral modules. By plugging the power module with the order no. 007-1AB00 the succeeding peripheral modules get a DC 24V power section supply with max. 10A. If the 10A are no longer sufficient, another power module must be plugged. So you have also the possibility to define isolated groups.
- The peripheral modules get their electronic power supply from the CPU with max. 3A. The power module with the order number 007-1AB10 is to be used if the 3A for the electronic power supply at the backplane bus is no longer sufficient. Additionally you get a new isolated group for the DC 24V power section supply with max. 4A.
- By plugging the power module 007-1AB10, modules with a maximum total current of the power section supply of 2A can be plugged at the succeeding backplane bus. Afterwards a power module is to be placed again. To secure the power supply, the power modules may be mixed used.

(e) Power Module 007-1AB00



- (1) DC 24V supply CPU:
DC 5V electronic section supply I/O area (max. 2A)
- (2) Power module 007-1AB00:
DC 24V power section supply (max. 10A)

(f) Power Module 007-1AB10



- (1) DC 24V supply CPU:
DC 5V electronic section supply I/O area (max. 2A)
- (2) Power module 007-1AB00:
DC 24V power section supply (max. 10A)
- (3) Additional power module 007-1AB10:
- (4) DC 24V power section supply (max. 4A)
- (5) DC 5V electronic section supply I/O area (max. 2A)



CAUTION

Since the power section supply is not internally protected, it is to be externally protected with a fuse, which corresponds to the maximum current. This means max. 10A is to be protected by a 10A fuse (fast) respectively by a line circuit breaker 10A characteristics Z!

Information The electronic power section supply is internally protected against higher voltage by fuse. The fuse is within the power module. If the fuse releases, its electronic module must be exchanged!

(g) Fusing

- The power section supply is to be externally protected with a fuse, which corresponds to the maximum current. This means max. 10A is to be protected with a 10A fuse (fast) respectively by a line circuit breaker 10A characteristics Z!
- It is recommended to externally protect the electronic power section supply for CPU an I/O area with a 2A fuse (fast) respectively by a line circuit breaker 2A characteristics Z.

(h) State of the Electronic Power Supply via LEDs

After PowerON the RUN respectively MF LED at every System SLIO module is on, so far as the sum current does not exceed the maximum value. With the CPU this is 3A. If the total current exceeds the maximum value, the LEDs are no longer triggered. Here the power module with the order number 007-1AB10 is to be placed between the periphery modules.

Deployment

This chapter describes the deployment of the iC9200.

4.1	Licensing information for Open Source software.....	62
4.2	Programming and file system	63
4.2.1	PLCnext Technology	63
4.2.2	Programming	63
4.2.3	Firewall	63
4.3	Commissioning.....	64
4.3.1	Install iCube Engineer	64
4.3.2	Online Access to the CPU	64
4.4	Memory Management.....	65
4.4.1	Internal Memory	65
4.4.2	Slot for Yaskawa SD Card.....	67
4.5	MRESET and Reset to Factory Settings	68
4.5.1	MRESET	68
4.5.2	Reset to Factory Settings Type 1	68
4.5.3	Reset to Factory Settings type 2.....	69
4.6	Firmware Update	70
4.7	Safe Mode	71
4.7.1	Start-Up in Safe Mode.....	71
4.7.2	Start-up in Standard Mode	71
4.8	Web-Based Management - WBM	72
4.8.1	Overview and First Steps.....	72
4.8.2	Overview	74
4.8.3	Diagnostics	75
4.8.4	Configuration.....	85
4.8.5	Security	89
4.8.6	Administration.....	105

4.1 Licensing information for Open Source software

- The CPU works with a Linux operating system.
- You can access license information for the individual Linux packages in Web-based management (WBM) via the [Legal Information] button. [4.8 Web-Based Management - WBM on page 72](#)
- Every open source software that is used in the product is subject to the respective license conditions, which are not affected by the Yaskawa software license conditions (**S**oftware **L**icense **T**erms - SLT) for the product.
- The licensee can change the respective open source software in accordance with the applicable license terms.

Information **Notes on OpenSSL**

- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>).
- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

4.2 Programming and file system

4.2.1 PLCnext Technology



- The CPU is based on PLCnext Technology® from Phoenix Contact.
- The CPU works with a Linux operating system.

4.2.2 Programming

- You can configure and program the CPU with iCube Engineer according to IEC 61131-3.

4.2.3 Firewall

Information

- On delivery the firewall in the CPU is disabled!
- Security recommendation: Enable the firewall!
- In the WBM, you can enable the firewall at [Security] - [Firewall].
- Please note that you only have access to the firewall settings as an administrator!

4.3 Commissioning

4.3.1 Install iCube Engineer

(1) Installation

The software iCube Engineer is required for commissioning the CPU.

1. **Download the software iCube Engineer to your PC. You can find this at <https://www.icubecontrol.com/icube-engineer.html>**

Unzip the file in your working directory and start the installation by double-clicking on the exe file.

2. **Follow the instructions of the installation wizard.**

The installation is started.

3. **When prompted, restart your system.**

The installation is finished. You can start iCube Engineer now. This will run for 30 days without a license.

4.3.2 Online Access to the CPU

(1) IP Address Parameters for Communication

On delivery the following IP address parameters for the communication are preset in the project template of the CPU:

- Ethernet-Port (X3/X4): 192.168.1.1
- Subnet mask: 255.255.255.0
- Gateway: -

If your CPU has different IP address parameters, you can adapt them for iCube Engineer.

4.4 Memory Management

4.4.1 Internal Memory

(1) Overview

Information Please note that, depending on the firmware and the components used, not the entire memory area is available.

CPU	Memory Details
iC9226M-EC	<ul style="list-style-type: none"> • 2GB working memory (RAM). • 12MB program memory. • 32MB data memory. • 3072kB retentive data memory.

(2) Working Memory

- During operation, the operating system stores temporary data and parts of the user program in the working memory.
- With MRESET you can set the CPU to the Ready state without a power cycle. This unloads the working memory, among others. [4.5.1 MRESET on page 68](#)

(3) Parametrization Memory

The parametrization memory as the sum of program and data memory provides memory for:

- Current firmware version
- Overlay file system for user program, configurations, user data and firmware adjustments.

Use of the overlay file system:

- As soon as you configure the CPU or make changes to the current firmware version, data are generated in the overlay file system.
- By [Resetting to the factory setting type 1], you can delete the overlay file system, among others. The current firmware version remains, but all changes to it are discarded. [4.5.2 Reset to Factory Settings Type 1 on page 68](#)
- By [Resetting to the factory setting type 2], you can delete the overlay file system and the current firmware version, among others. The current firmware version is overwritten by the original firmware version and the delivery state of the CPU is restored. [4.5.3 Reset to factory settings type 2 on page 69](#)

CAUTION

Damage to the internal parametrization memory due to high write activity!

- **Frequent write accesses by applications (for example: data logger applications to the overlay file system) may cause long term damage to the internal parametrization memory of the CPU and lead to a device defect.**

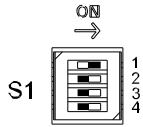
(4) Non-Volatile Memory for Retentive Data

- All data that were marked as retentive in iCube Engineer during configuration are permanently stored here.
- In the event of a power failure, retentive data are automatically backed up.
- By MRESET or resetting to factory setting type 1/2 you can, among others, delete the non-volatile memory for retentive data.

(5) Fix memory Overflow

If, during operation or when starting up the CPU, the error indication occurs that the memory of the overlay file system in the parametrization memory has overflowed, the CPU can be restarted via Safe Mode as follows:

1. **Switch off the power supply of the CPU.**
2. **Set the S1 DIP switches S1-1 and S1-2 under the front flap to the following position:**



Terminal	Setting	Action
S1-1	ON	After Power ON the CPU starts in Safe Mode.
S1-2	OFF	

3. **Switch on the power supply of the CPU again.**

The CPU starts in Safe Mode.

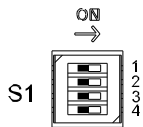
Refer to the section below for more details on Safe Mode.

4.7 Safe Mode on page 71

Here, a memory area reserved exclusively for Safe Mode is enabled, which allows the CPU to restart in the event of a memory overflow.

At Safe Mode the CPU starts with a default project, but your user program is still present in the file system.

4. **Check your user program for files on the file system that cause the system to overflow, such as log files, recipes, motion data.**
5. **Use an SSH client to access the file system and delete the causing files if necessary. Then start in Standard Mode again.**
6. **For this, switch off the power supply to the CPU.**
7. **Set the S1 DIP switches S1-1 and S1-2 to the default position:**



Terminal	Setting	Action
S1-1	OFF	After Power ON the CPU starts in Standard Mode - default setting.
S1-2	OFF	

8. **Switch on the power supply of the CPU again.**

The CPU starts in Standard Mode again. If a project was loaded in Safe Mode, it is executed in RUN operating mode.

4.4.2 Slot for Yaskawa SD Card

For future use

4.5 MRESET and Reset to Factory Settings

4.5.1 MRESET

- The CPU is set to the Ready state.
- The working memory is unloaded, but the user program remains in the overlay file system.
- The non-volatile memory for retentive data is deleted.
 1. **Switch your CPU to STOP state.**
 2. **Push the operating mode switch down to position MR.**
 3. **Release the operating mode switch after 3 seconds and press it back to the MR position within 3 seconds.**
 4. **Release the operating mode switch after 3 seconds.**
 - The CPU now executes a MRESET.
 - To confirm, you will receive a diagnostic message that a MRESET was executed. You can output e.g. in iCube Engineer via [Notifications] in the [Cockpit] editor.

4.5.2 Reset to Factory Settings Type 1

- The CPU is started in Standard Mode.
- The overlay file system with user program, configurations, user data and firmware adjustments is deleted.
- The non-volatile memory for retentive data is deleted.
- The current firmware version remains, but all changes to it are discarded.

(1) When Using Operating Mode Switch S3

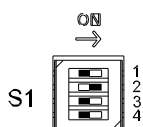
1. **Switch OFF the power supply of the CPU**
2. **Press and hold the operating mode switch in position MR and switch on the power supply of the CPU again.**
3. **As soon as the LEDs show the following behavior after start-up, release the operating mode switch again:**

LED Behavior										
RDY (green)	Resvd (yellow)	RN (green)	ER (red)	IO ER (red)	IO DIAG (red)	PN-C ER (red)	PN-D ER (red)	SD (yellow)	EC RN (green)	EC ER (red)
Not lit	Not lit	Flashing green 1 Hz interval	Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit

The CPU now executes a reset to factory setting type 1.

(2) When Using DIP Switch S1

1. **Switch OFF the power supply of the CPU.**
2. **Set the S1 DIP switches S1-1 and S-2 under the front flap to the following position:**



Terminal	Setting	Action
S1-1	OFF	After power is switched ON the CPU executes a reset to factory settings type 1.
S1-2	ON	

3. Switch ON the power supply of the CPU again.

After the start-up of the CPU it performs a reset to factory setting type 1 and shows the following LED behavior:

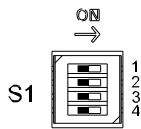
LED Behavior										
RDY (green)	Resvd (yellow)	RN (green)	ER (red)	IO ER (red)	IO DIAG (red)	PN-C ER (red)	PN-D ER (red)	SD (yellow)	EC RN (green)	EC ER (red)
Not lit	Not lit	Flashing green 1 Hz interval	Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit

The CPU requests a power cycle after a reset to factory settings type 1:

LED Behavior										
RDY (green)	Resvd (yellow)	RN (green)	ER (red)	IO ER (red)	IO DIAG (red)	PN-C ER (red)	PN-D ER (red)	SD (yellow)	EC RN (green)	EC ER (red)
Not lit	Not lit	Not lit	Flashing red 1 Hz interval	Flashing red 1 Hz interval	Flashing red 1 Hz interval	Flashing red 1 Hz interval	Flashing red 1 Hz interval	Not lit	Not lit	Not lit

4. Switch OFF the power supply of the CPU.

5. Set the DIP switch S1 to the default position:



Terminal	Setting	Action
S1-1	OFF	After switching power ON the CPU starts in Standard Mode - Default setting.
S1-2	OFF	

6. Switch ON the power supply of the CPU again.

The CPU starts in Standard Mode.

4.5.3 Reset to Factory Settings Type 2

- The overlay file system with user program, configurations, user data and firmware adjustments is deleted.
- The non-volatile memory for retentive data is deleted.
- The current firmware version is overwritten by the original firmware version and the delivery state of the CPU is restored.

1. Switch OFF the power supply of the CPU.
2. Press and hold the operating mode switch in position MR and switch on the power supply of the CPU again.
3. As soon as the LEDs show the following behavior after start-up, release the operating mode switch again (duration ca. 30s):

LED Behavior										
RDY (green)	Resvd (yellow)	RN (green)	ER (red)	IO ER (red)	IO DIAG (red)	PN-C ER (red)	PN-D ER (red)	SD (yellow)	EC RN (green)	EC ER (red)
Not lit	Not lit	Flashing green 2 Hz interval	Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit

The CPU now executes a reset to factory setting type 2 and is then in the delivery state.

4.6 Firmware Update

You can update the firmware via the Web-based management WBM.

Information Please note that you can only execute a firmware update with administrator rights!

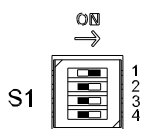
4.7 Safe Mode

4.7.1 Start-Up in Safe Mode

By means of the DIP switch [S1] beneath the front flap you can start your CPU in Safe Mode. Here the CPU starts with the following behavior:

- The CPU goes to RUN with the default project.
- A project can be loaded but not executed.
- The SliceBus is switched off.
- All field buses are disabled.
- The parametrization memory with the current firmware version and the overlay file system remains unchanged.
- During online access, you are informed that the CPU is in Safe Mode.
- The non-volatile memory for retentive data remains unchanged.
- The CPU can only be reached via the default IP address.
- Additionally, a memory area reserved exclusively for Safe Mode is enabled, which allows the CPU to restart in the event of a memory overflow.

1. **Switch off the power supply of the CPU.**
2. **Set the S1 DIP switches S1-1 and S1-2 under the front flap to the following position:**

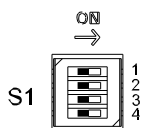


Terminal	Setting	Action
S1-1	ON	After power is switched ON the CPU starts in Safe Mode.
S1-2	OFF	

3. **Switch ON the power supply of the CPU again.**
The CPU starts in Safe Mode and shows this exclusively during online access.

4.7.2 Start-up in Standard Mode

1. **Switch OFF the power supply of the CPU.**
2. **Set the S1 DIP switches S1-1 and S1-2 to the default position:**



Terminal	Setting	Action
S1-1	OFF	After power is switched ON the CPU starts in Standard Mode - Default setting.
S1-2	OFF	

3. **Switch ON the power supply of the CPU again.**
The CPU starts in Standard Mode again. If a project was loaded in Safe Mode, it is executed in RUN.

4.8 Web-Based Management - WBM

4.8.1 Overview and First Steps

(1) Accessing WBM

- The CPU has a web-based management (WBM). In the WBM you can access static and dynamic information and change certain settings. You may access WBM via the Ethernet interfaces of the CPU.
- The communication between the PC and CPU takes place via a security certificate, which must be located on the CPU and PC.
- You may only access WBM if the CPU has a valid IP address.
- In the delivery state, the CPU has the IP address 192.168.1.1 via Ethernet port (X3/X4).

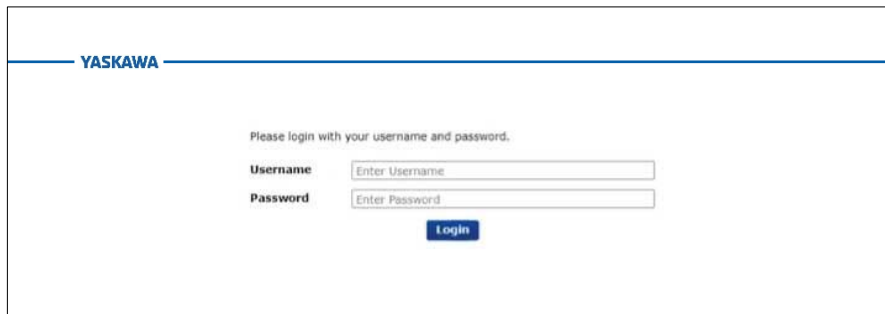
1. **For the initial commissioning, establish a secure connection between the PC and CPU, such as a point-to-point connection via Ethernet.**
2. **Open the web browser on your PC.**
3. **You can use the iCube Engineer search to determine the IP address of the corresponding Ethernet interface.**

Enter the URL in the address field such as `https://192.168.1.1`

For secure communication the CPU web server uses a self-signed TLS certificate that is automatically generated by the CPU during the commissioning. Due to the system, you will receive a security message regarding the certificate, as it has not yet been installed on the PC. After logging in, you can install the corresponding certificate from the CPU as a trusted certificate on your PC (see below). This authenticates the CPU to the web browser on the PC.

4. **Take note of the security message and only continue if there is a secure connection between the PC and CPU and no third parties can access it!**

The WBM login page opens.



5. **Enter your login details and click on [Login].**

Information On delivery, the following access data are preset with administrator rights:

- Username: admin
- The password is printed under the front flap on the front of the CPU.

You now have access to the WBM of the CPU with the access rights assigned to you.

(2) Install Certificate

Information **First access via TLS certificate**

- During commissioning, the CPU generates a TLS certificate during the start-up.
- The certificate is used for all Ethernet interfaces of the CPU and includes all IP addresses.
- When resetting to factory settings, a new certificate is automatically generated.

To secure communication, the same security certificate must be installed in the PC and CPU. You transfer the

1. After logging into the WBM, you can view or respectively adjust the contents of the automatically generated certificate via [Configuration] - [Web Services] and re-generate it with [Re-generate HTTPS certificate].


Information

As soon as you change one of the IP addresses of the CPU, you must regenerate the certificate via [Re-generate HTTPS certificate].

2. Navigate to the certificates via [Security] - [Certificate Authentication].
3. Switch to the tab Identity Store.

Here you have access to the generated certificate.



4. Load the requested HTTPS certificate onto your PC with . Here you can also transfer your own existing HTTPS certificate to the CPU.
5. Install the certificate according to your Windows system as a trusted root certification authority.

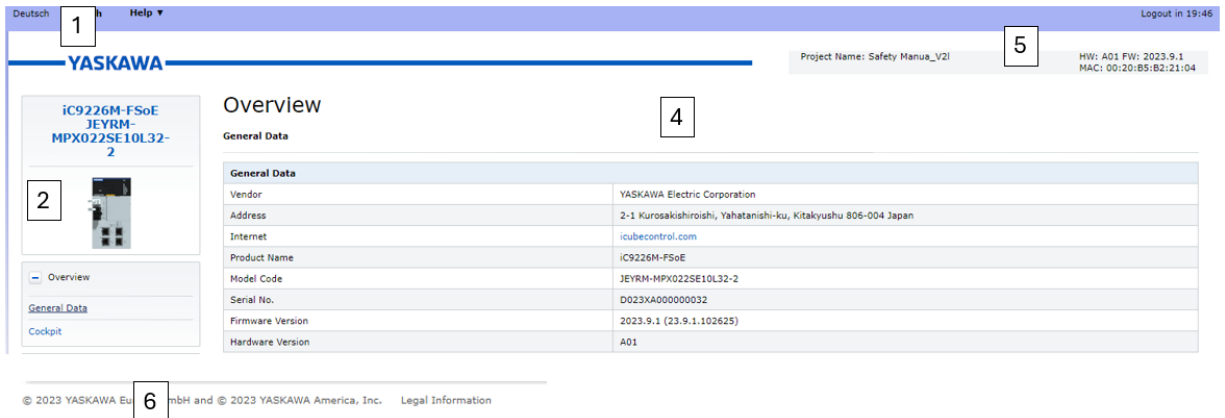
After installation, communication between the PC and CPU takes place as a [secure connection].

CAUTION

If the communication between PC and CPU is declared as an [insecure connection] during operation, either the certificate has changed, e.g. due to an IP address change, or your system has been compromised by third parties! Always make sure that either the current certificate of the CPU or, if available, an associated higher-level certificate is installed on the PC!

(3) Structural Design

The WBM is divided into the following areas:



The screenshot shows the YASKAWA WBM interface. At the top left, there is a language selector (1) set to 'Deutsch'. The main header displays the YASKAWA logo and a project name (5) 'Safety Manua_V2I'. On the right, it shows hardware and firmware information: 'HW: A01 FW: 2023.9.1 MAC: 00:20:B5:B2:21:04'. The main content area is titled 'Overview' (4) and contains a 'General Data' table. On the left, there is a menu column (3) with options for 'Overview', 'General Data', and 'Cockpit'. Below the menu, there is a front view of the CPU (2) with its model number 'iC9226M-FSoE JEYRM-MPX022SE10L32-2'. At the bottom, there is a footer (6) with copyright information: '© 2023 YASKAWA Europe GmbH and © 2023 YASKAWA America, Inc. Legal Information'.

General Data	
Vendor	YASKAWA Electric Corporation
Address	2-1 Kurosakishiroishi, Yahatanishi-ku, Kitakyushu 806-004 Japan
Internet	icubecontrol.com
Product Name	iC9226M-FSoE
Model Code	JEYRM-MPX022SE10L32-2
Serial No.	D023XA000000032
Firmware Version	2023.9.1 (23.9.1.102625)
Hardware Version	A01

- 1 Language switching between [German] and [English].
- 2 Front view of the CPU with type and order designation.
- 3 Menu column for navigation.
- 4 Area for information output and input dialogs
- 5 Shows the current hardware/firmware version and MAC address of the CPU.
- 6 Access to the Yaskawa software license conditions (**S**oftware **L**icense **T**erms - SLT) and the license information for the individual Linux packages.

4.8.2 Overview

(1) General Data

Here you will find general details about the CPU, e.g. hardware and firmware versions, order number as well as vendor information.

YASKAWA
Project Name: Safety Manua_V21

iC9226M-FSoE
JEYRM-
MPX022SE10L32-
2

- Overview
- General Data
- Cockpit

Overview

General Data

General Data	
Vendor	YASKAWA Electric Corporation
Address	2-1 Kurosakishiroishi, Yahatanishi-ku, Kitakyushu 806-004 Japan
Internet	icubecontrol.com
Product Name	iC9226M-FSoE
Model Code	JEYRM-MPX022SE10L32-2
Serial No.	D023XA000000032
Firmware Version	2023.9.1 (23.9.1.102625)
Hardware Version	A01

(2) Cockpit Cockpit

Here you will find the Cockpit toolbar and information about the time, status and utilization of the CPU.

YASKAWA
Project Name: Safety Manua_V21
PLC: A01 FW: 202
MAC: 00:20:B5:9

iC9226M-FSoE
JEYRM-
MPX022SE10L32-
2

- Overview
- General Data
- Cockpit
- Diagnostics
- Axis Grd
- EtherCAT
- Motion Alarms
- Notifications
- Profinet
- SliceBus
- SliceBus Modules
- Configuration
- Network
- Date and Time
- System Services
- Web Services
- Security

Overview

Cockpit

Date and Time

Current Timestamp (DD.MM.YYYY HH:mm:ss): 05.04.2024 13:48:18

System Uptime ([D:][H:]mm:ss): 22:57:16

Utilization

Memory: 15%

User Partition: 0% 80 MB/1 GB

CPU Load (total): 3%

CPU Load (Core 1): 4%

CPU Load (Core 2): 3%

CPU Load (Core 3): 1%

PLC Runtime

PLC State: Running

Program Memory: 0% 78 KB/12 MB

Data Memory: 0% 252 KB/32 MB







Retain Memory: 0% 0 Byte/3 MB

1. Cockpit Toolbar

The toolbar provides access to the following functions:

- : Stop - Stops program execution on the CPU.
- : Hot Start - Performs a hot start. The CPU is restarted and the program continues without initializing the variables.
- : Warm Boot - Performs a warm boot. The CPU is restarted and the program continues with initializing the variables. The values of the variables marked with "Retain" in iCube Engineer are retained.

74

-  Cold Start - Performs a cold start. CPU is restarted and the program continues with initializing all the variables.
-  : Memory download - Saves the retain data locally in a file.
-  : Memory upload - Restores the saved retain data.
-  : Reboot - Performs a reboot. The operation corresponds to a power off/on process. The loaded application (code and network configuration) is deleted from the RAM. The controller restarts with the last saved settings and, if available, loads the boot project from the flash memory.
-  : Reset - Resets the CPU to factory settings. Similar to the [Restart] command, the loaded application (code and network configuration) is deleted from the RAM but also from the flash memory (boot project). Additionally, all communication settings are reset to default settings.
-  : Change Password - This allows you to change the password of the current user account for online access to the CPU.

2.Date and Time

The current system time is shown via Current time stamp. System uptime shows the current runtime since PowerON. Date and time are set via [4. 8. 4\(2\) Date and Time on page 86](#).

3.Utilization

CPU memory utilization and the CPU load are shown here.

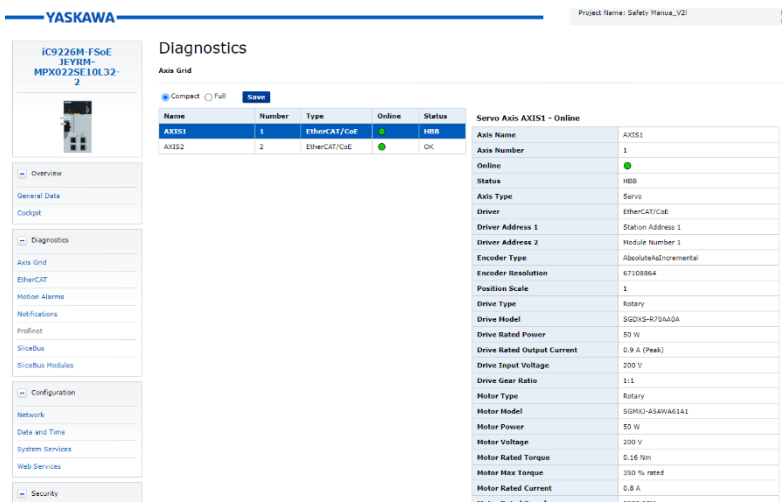
4.PLC Runtime

The CPU status and memory usage in the PLC runtime system are shown here.

4.8.3 Diagnostics

(1) Axis Grid

Here you will find basic information about configuring your axes such as servo drives.



The screenshot shows the YASKAWA diagnostics web interface. The main content area is titled "Diagnostics" and "Axis Grid". It features a table with columns for Name, Number, Type, Online, and Status. Below the table, there is a detailed configuration section for "Servo Axis AXIS1 - Online".

Name	Number	Type	Online	Status
AXIS1	1	EtherCAT/Cat	●	HB
AXIS2	2	EtherCAT/Cat	●	OK

Servo Axis AXIS1 - Online	
Axis Name	AXIS1
Axis Number	1
Online	●
Status	HB
Axis Type	Servo
Driver	EtherCAT/Cat
Driver Address 1	Station Address 1
Driver Address 2	Module Number 1
Encoder Type	Absolute/Incremental
Encoder Resolution	4710884
Position Scale	1
Drive Type	Rotary
Drive Model	SQDUP-R70A0A
Drive Rated Power	50 W
Drive Rated Output Current	0.9 A (Peak)
Drive Input Voltage	200 V
Drive Gear Ratio	1:1
Motor Type	Rotary
Motor Model	SGMH-45AW46141
Motor Power	50 W
Motor Voltage	200 V
Motor Rated Torque	0.16 Nm
Motor Max Torque	350 % rated
Motor Rated Current	0.8 A
Motor Rated Speed	3000 RPM

You have the following display options:

- Compact
 - All axes configured in the CPU and their states are listed here in a compact table.
 - By selecting an axis, you will receive all information about the corresponding axis in the table next to it.
- Full
 - All axes configured in the CPU are listed here with all information in a table.
 - By selecting EtherCAT/CoE or Virtual, you can limit the list to axes connected via FSoE or virtual axes.
- WithSave] you can save the axis information as a CSV file on your PC.

(2) EtherCAT

Here you will find basic information about the EtherCAT SubDevice stations that are connected via the EtherCAT network. Information is only shown here if the EtherCAT network is correctly configured and the EtherCAT SubDevice stations are in the OP, PreOP or SafeOP state. Otherwise you will receive the message [Invalid network configuration or network not ready for operation].

The screenshot shows the YASKAWA Diagnostics web interface. On the left, there is a sidebar with a navigation menu containing 'Overview', 'General Data', and 'Cockpit'. The main content area is titled 'Diagnostics' and 'EtherCAT'. It displays 'Slaves Found: 2' and 'Slaves in Config: 2'. Below this is a table with the following data:

Index	Station Address	Status	Device Name	Device Type	Vendor ID	Product Code	Revision Number	Serial Number
1	1	Online	SGDXS-R70AA0A	0x00020192	0x00000539	0x02200901	0x00010005	D02340269910005
2	2	Online	SGDXS-R70AA0A	0x00020192	0x00000539	0x02200901	0x00010005	D02340269910017

Below the table, there is a note: 'EtherCAT device information is available only when the following criteria are met: 1. Network is configured and operational 2. Device ESM state is OP, SAFEOP, or PREOP'.

The following information is shown in tabular form:

- Station address and Station alias
- Station name, type and vendor
- Product code, revision number and serial number
- [State]: ESM status of the corresponding EtherCAT SubDevice station:
 - OP
 - The EtherCAT SubDevice station is in the Operational state and exchanges process data cyclically.
 - PreOp
 - The EtherCAT SubDevice station is in the Pre-Operational state. Process data are not exchanged.
 - SafeOp
 - The EtherCAT SubDevice station is in the Safe-Operational state. In this case, the input process data are refreshed cyclically but the outputs are disabled.

(3) Motion Alarms

If you have connected a drive to your CPU, you will find the current motion alarms and their history here.

Timestamp	Error Code	Source	Description	More Info
2024-04-05 16:21:25	0x33030710	AXIS1	A.710: Overload: High Load	The motor was operating for several seconds to several tens of seconds under a torque largely exceeding ratings.
2024-04-05 16:21:24	0x43030910	AXIS1	A.910: Overload	This warning occurs before the overload alarms (A.710 or A.720) occur. If the warning is ignored and operation continues, an overload alarm may occur.
2024-04-05 16:21:00	0x33010022	AXIS2	Synchronous communication lost	The drive has lost synchronous communication with the controller. Reset the communication to continue.
2024-04-05 16:21:00	0x33010022	AXIS1	Synchronous communication lost	The drive has lost synchronous communication with the controller. Reset the communication to continue.
2024-04-05 16:02:44	0x11030102	SLDiEc	Motion kernel scan overrun	The motion kernel scan failed to complete before the next update period. The system update rate must be lowered.
2024-04-05 16:00:03	0x44080002	Alarm history	Alarm history stored in NVRAM was corrupted	The alarm history was configured to use NVRAM storage and the data was found to be corrupted. The alarm history has been lost. NOTE: this alarm also occurs if the configured size of the alarm history has been changed.

- [Active Alarms]
 - All currently pending motion alarms are listed here.
 - The table includes error code, source, description and more detailed information about the corresponding motion alarm.
- [Alarm History]
 - The last 100 motion alarms are listed here.
 - The table includes error code, source, description and more detailed information about the corresponding motion alarm.

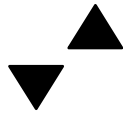
(4) Notifications

Every user with access rights can view and download message entries here. The page contains buttons for filter functions and for the CSV export of the messages, as well as an overview table of all messages and a full text area of a selected message. This information is refreshed once a second

Severity	Time	Sender	Name	Notification
✖	05.04.2024 16:21:25.046	FMK	Arp.Services.FMK.Alarm.Error	A.33030710 : A.710: Overload: High Load
ⓘ	05.04.2024 16:21:25.840	Arp.Io.Ecat	Arp.Io.Ecat.EcCoeEmergency	EtherCAT CoE Emergency from slave with station address ...
⚠	05.04.2024 16:21:24.819	FMK	Arp.Services.FMK.Alarm.Warn	A.43030910 : A.910: Overload
ⓘ	05.04.2024 16:21:24.812	Arp.Io.Ecat	Arp.Io.Ecat.EcCoeEmergency	EtherCAT CoE Emergency from slave with station address ...
ⓘ	05.04.2024 16:21:11.732	PLC Manager	Security.Arp.Plc.Domain.PlcManager.PlcStarted	PLC started. Start Kind: Warm, Used Memory: 18 %, CPUs...
ⓘ	05.04.2024 16:21:11.731	PLC Manager	Arp.Plc.Domain.PlcManager.StateChanged	Plc state changed: Stop (warm) ==> Running
ⓘ	05.04.2024 16:21:11.479	Arp.Io.Ecat	Arp.Io.Ecat.EcMasterStateChanged	EtherCAT master state changed from SafeOp to Op
ⓘ	05.04.2024 16:21:11.479	Arp.Io.Ecat	Arp.Io.Ecat.EcSlaveStateChanged	EtherCAT slave station address 1 changed to Op, ALStatus...
ⓘ	05.04.2024 16:21:11.479	Arp.Io.Ecat	Arp.Io.Ecat.EcSlaveStateChanged	EtherCAT slave station address 2 changed to Op, ALStatus...
ⓘ	05.04.2024 16:21:11.363	Arp.Io.SliceBus	Arp.Io.SliceBus.DiagnosisRemoved	Diagnosis status of slot 2 - slot OK
ⓘ	05.04.2024 16:21:11.362	Arp.Io.SliceBus	Arp.Io.SliceBus.DiagnosisRemoved	Diagnosis status of slot 1 - slot OK

1. Sort Criteria for the Message Entries

By default, the message entries in the table are sorted in descending order based on the time stamp. To sort the notifications, click on the header of the corresponding table column. The arrows at the column headings have the following meaning:



Double arrow

The table is not sorted by this column



Up arrow :

The table is sorted according to this column in ascending order.



Down arrow :

The table is sorted according to this column in descending order.

2. Full Text View

Below the table is the full text view of a selected message entry in the table. If no message is selected, the full text view remains empty.

Notifications					
Severity	Time	Sender	Name	Notification	
	02.08.2021 15:38:13.659	System Manager	Arp.System.Acf.SystemManager.StateChanged	SystemManager state changed: Running, error=fals...	
	02.08.2021 15:38:13.506	PLC Manager	Arp.Plc.Domain.PlcManager.StateChanged	Plc state changed: Stop (warm) ==> Running	
	02.08.2021 15:38:13.493	Device Interface	Arp.Device.Interface.EthernetLinkStateChanged	Link state changed: interface 1, port 1, status: Up	
	02.08.2021 15:38:13.483	System Manager	Arp.System.Acf.SystemManager.StateChanged	SystemManager state changed: Stop, error=false, warning...	
	02.08.2021 15:38:13.286	PLC Manager	Arp.Plc.Domain.PlcManager.StateChanged	Plc state changed: Ready ==> Stop (warm)	
	02.08.2021 15:38:13.072	System Manager	Arp.System.Acf.SystemManager.StateChanged	SystemManager state changed: Ready, error=false, warnin...	
	02.08.2021 15:38:07.857	System Manager	Arp.System.Acf.SystemManager.StateChanged	SystemManager state changed: Done, error=false, warnin...	

Notification
SystemManager state changed: Running, error=false, warning=false

3. Filter Functions

Specify the filter settings. By clicking on [Apply Filter], the previously made filter settings are activated and the table with the message entries is refreshed accordingly.

There are the following filter options:

- Archive name
 - Here you can filter the message entries by specifying an archive name.
- Severity
 - Here you can limit the message entries based on their severity.
 - The limitation is based on the following graduation for the minimum severity:
 - Internal Information Warning Error Critical Error Fatal Error
 - For example with Internal, all degrees of severity are listed. With the setting Error, all Error, Critical Error and Fatal Error are listed.
- Sender
 - Here you can limit the message entries by entering or selecting a sender in the selection field.
 - The currently list of message entries is always decisive for the names in the selection field.
 - When entering a name or part of the name, click on [Apply Filter] to list messages from senders that match or partially match the name you are looking for.

- Maximum number of notifications
 - Here you can limit the number of message entries to be listed.
 - 1024 is set by default, a maximum of 4000 is allowed.
- Time from, Time to
 - Here you can limit the period of the message entries by entering the date and time.
 - Time from: Lists all message entries that are not older than the specified time.
 - Time to: Lists all message entries that are older than the specified time.
 - When filtering by time specification, a date must always be entered and a time can be added.

(5) PROFINET – Optional

1. Tab: [Overview]

Here you will find information on the current PROFINET function of the controller and its IP settings.

Information

Please note that a separate licence is required for the use of PROFINET, which must be activated accordingly!

The screenshot shows the YASKAWA WBM interface for a device with model number iC9226M-FSoE. The left sidebar contains a navigation menu with options like Overview, Diagnostics, Axis Grid, EtherCAT, Motion Alarms, Notifications, Profinet, SliceBus, and SliceBus Modules. The main content area is titled 'Diagnostics' and 'PROFINET'. It has three tabs: Overview (selected), Device List, and Tree View. Under the Overview tab, there is a 'Profinet Controller' section with a 'Status' table and a 'Controller Details' section with input fields for Device Type, IP Address, Subnet Mask, Default Gateway, and Realtime Class. The status is 'Activated' and the IP address is '192.168.1.1'. At the bottom, it shows 'Diagnosis: Online' and 'Status: OK'.

Status	
Profinet Controller Function	Activated
Profinet Device Function	Deactivated

Controller Details	
Device Type	iC9226M-FSoE
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
Realtime Class	RT

2. Tab: [Device List]

The screenshot shows the YASKAWA WBM interface for the same device. The left sidebar is the same. The main content area is titled 'Diagnostics' and 'PROFINET'. It has three tabs: Overview, Device List (selected), and Tree View. Under the Device List tab, there is a 'Profinet Device List' section with a table listing the device. Below the table, there is a note: '* - Profinet participants with own Web based Management (Reachable via the link)'. At the bottom, it shows 'Diagnosis: Online' and 'Status: OK'.

No.	Name of Station	IP Address	Status	Details	Tree Node
1	vip4053-1ph01-001	192.168.1.10	OK (Outdoors)		

(a) Open the WBM of a PROFINET Device

To access the WBM of a PROFINET device, click on the corresponding PROFINET device in the Device Name column.

The WBM of the PROFINET device opens in a new tab in the web browser.

3. Device Information

For the corresponding PROFINET device, you will find information on IP settings and diagnostics at Device Information. This information is refreshed once a second.



To show the Device Information of a PROFINET device click in Details column on

The Device Information view with the current information on IP settings and diagnostics is opened.

Profinet Device	
Activation Status	TRUE
Device Number	1
Vendor ID	0x0111
Device ID	0x0300
Ethernet	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Station	0521...
CNS Hostname	0521...
Peripheral Errors	
Status	OK
Diagnostics Status Code	0x0000
Diagnostics Status Text	

Profinet Device	
Activation Status	TRUE
Device Number	1
Vendor ID	0x0111
Device ID	0x0300
Ethernet	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Station	0521...
CNS Hostname	0521...
Peripheral Errors	
Status	Warning
Diagnostics Status Code	0x0020
Diagnostics Status Text	0x 5: Neighbourhood information is not available

Profinet Device	
Activation Status	TRUE
Device Number	1
Vendor ID	0x0111
Device ID	0x0300
Ethernet	
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
Station	0521...
CNS Hostname	0521...
Peripheral Errors	
Status	Error
Diagnostics Status Code	0x0021
Diagnostics Status Text	0x 5: Lost connection to coupler 0x 5: Enable Data 0x 5: Neighbourhood information is not available

4. Tab: [Tree View]

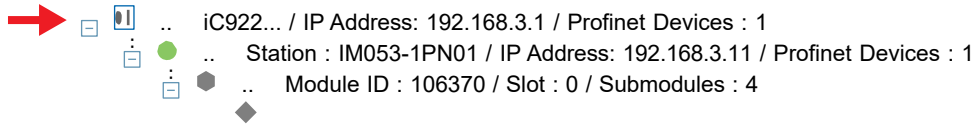
Here you have a tree view of all configured PROFINET devices. The overview contains the device names of the PROFINET devices, their current IP settings and the diagnostic status of the devices and modules. Via [+] and [-] you can open or close the next level of the Tree View.

The screenshot shows the YASKAWA diagnostics web interface. On the left, there is a navigation menu with options like Overview, Diagnostics, Axis Grid, EtherCAT, Hobon Alarms, Notifications, Profinet, SliceBus, SliceBus Modules, Configuration, Security, and Administration. The main area is titled 'Diagnostics' and 'PROFINET'. It features three tabs: Overview, Device List, and Tree View. The 'Tree View' tab is active, displaying a 'Profinet Tree View' with a hierarchical structure of devices and modules. The tree starts with 'IC9226M-FSoE / 192.168.1.1 [1]', followed by 'Vip0...01-001 / 192.168.1.10 / SLIO Coupler PROFINET (053-1PNO1) [3]'. Under this, there are several sub-items: '0x0 - DAP [4]', '0x1 - DAP', '0x8000 - Interface', '0x8001 - Port 1', '0x8002 - Port 2', '0x1 - DO 4xDC 24V 0.5A ETS (022-1B070) [1]', '0x1 - DO 4xDC 24V 0.5A ETS', '0x2 - DI 4xDC 24V ETS (021-1B070) [1]', and '0x1 - DI 4xDC 24V ETS'. A legend on the right side of the tree view defines the status icons: OK (green circle), Warning (yellow triangle), Urgent Warning (orange triangle), Error (red square), AD Deactivated (grey square), Module Difference (blue square), No Connection (red X), and No Information (grey circle). At the bottom of the interface, it shows 'Diagnostics: Online' and 'Status: OK'. The footer contains copyright information for YASKAWA Europe GmbH and YASKAWA America, Inc.

5. Controller Level

On the PROFINET controller level you will find the following information:

- Controller designation
- IP Address - IP address of the controller
- PROFINET Devices - Number of PROFINET devices



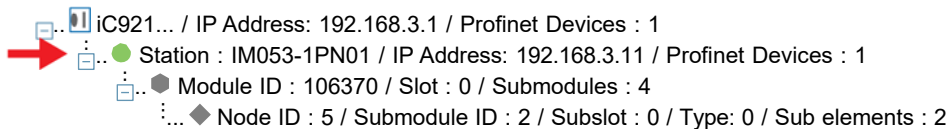
6. Station Level

On station level you will find the following information about the PROFINET devices:

- Station name
- IP Address - IP address of the station
- Vendor ID - the ID of the vendor
- Device ID - the ID of the device
- Modules - number of modules

Table 6.1 The following symbols inform about the current diagnostic state of the PROFINET device:

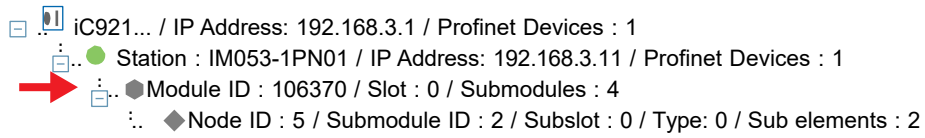
Symbol	Diagnostic status
	OK
	Warning
	Error



7. Module Level

On module level you will find the following information:

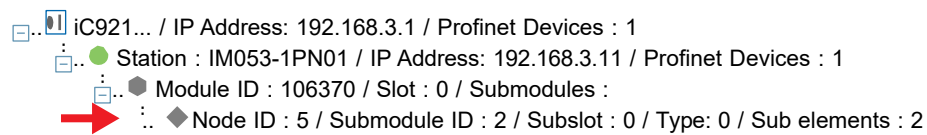
- Module ID - the ID of the module
- Slot - slot of the module
- Sub modules - the number of sub modules



8. Sub Module Level

On sub module level you will find the following information:

- Node ID - node ID of the sub module
- Sub module ID
- Sub slot
- Type
- Sub elements - number of sub module elements



9. PROFINET Diagnostics Code

Here you can get the status of a connection with an IO controller (Application Relation - AR) bit-coded.

Table 6.2 Status AR

Bit	Description and action recommendation
0	<p>Bit 0 is set when there is no connection.</p> <ul style="list-style-type: none"> The PROFINET controller could not establish a connection with the PROFINET device or the AR was deactivated. <ul style="list-style-type: none"> – Please check the Ethernet connection and the PROFINET device name with your iCube Engineer configuration tool. – Also check whether the AR was deactivated in the device settings of PROFINET.
1	<p>Bit 1 is set if the data is invalid.</p> <ul style="list-style-type: none"> The PROFINET device is connected to the PROFINET controller, but the process data were marked as invalid due to an error. The process data were not transferred to the process image. <ul style="list-style-type: none"> – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
2	<p>Bit 2 is set when a diagnostic message is pending.</p> <ul style="list-style-type: none"> The PROFINET device reports a diagnosis. <ul style="list-style-type: none"> – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
3	<p>Bit 3 is set if the module deviates from the configured module.</p> <ul style="list-style-type: none"> When the PROFINET connection was initialized, a discrepancy was found between the target and current configuration. <ul style="list-style-type: none"> – Please check the configuration of the PROFINET device. In the iCube Engineer default setting, the connection remains
4	<p>Bit 4 is set when the AR is disabled.</p> <ul style="list-style-type: none"> The PROFINET device is configured in the project, but the AR was disabled. <ul style="list-style-type: none"> – Check the PROFINET device settings and enable the AR.
5	<p>Bit 5 is set if no neighbor information is available.</p> <ul style="list-style-type: none"> No neighbor information are available in the network used. <ul style="list-style-type: none"> – This is usually due to the use of components that are not at least compatible with PROFINET Conformance Class-B (CC-
6	<p>Bit 6 is set if neighbor information are not uniform.</p> <ul style="list-style-type: none"> Neighbor information are available in the network used, but not clearly. This means that more than two PROFINET devices can be detected on a port by at least one switch. This is not permitted and may result in the automatic device change not working reliably.
7	<p>Bit 7 is set if the alias name of a device being searched for is already being used by an AR.</p> <ul style="list-style-type: none"> A DCP identification request (alias) was sent to the network. However, the alias of a device being searched for is already being used by an AR.
8	<p>Bit 8 is set when a maintenance request is pending.</p> <ul style="list-style-type: none"> The PROFINET device has transmitted a maintenance request (maintenance alarm). <ul style="list-style-type: none"> – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
9	<p>Bit 9 is set when a high-priority maintenance demand is pending.</p> <ul style="list-style-type: none"> The PROFINET device has transmitted a high-priority maintenance request (maintenance alarm). <ul style="list-style-type: none"> – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
10	<p>Bit 10 is set if a vendor- or channel-specific diagnosis is pending.</p> <ul style="list-style-type: none"> The PROFINET device has transmitted a vendor- or channel-specific diagnosis. <ul style="list-style-type: none"> – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.

4.8.4 Configuration

(1) Network

1. User with Read Permission

Here you can view the Ethernet settings of your CPU. You only have read access.

The screenshot shows the YASKAWA Configuration page for a user with Read Permission. The page displays the 'Configuration' section for the 'Network' tab. The 'LAN Interfaces' section is active, showing a table of LAN interface settings for Port X3 and Port X4. The 'Configuration' column contains input fields for IP Address, Subnet Mask, Default Gateway, DNS Server Addresses, and MAC Address. The 'Status' column shows the current status of each interface. The 'Configuration' column contains input fields for IP Address, Subnet Mask, Default Gateway, DNS Server Addresses, and MAC Address. The 'Status' column shows the current status of each interface.

LAN interface (LAN X3/X4)	Status	Configuration
IP Address	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	0.0.0.0	0.0.0.0
DNS Server Addresses	8.8.8.8	8.8.8.8
	8.8.4.4	8.8.4.4
MAC Address	00:20:B5:B2:21:04	
Port X3		
Data Rate	100 Mbit/s	
Duplex Mode	Full Duplex	
Link Status	LinkUp	
Port X4		
Data Rate		
Duplex Mode		
Link Status	LinkDown	

2. User with Write Permission

If you are logged in with administrator rights, you can view the Ethernet settings of your CPU here. You can also change the current network settings in the [Configuration] column.

The screenshot shows the YASKAWA Configuration page for a user with Write Permission. The page displays the 'Configuration' section for the 'Network' tab. The 'LAN Interfaces' section is active, showing a table of LAN interface settings for Port X3 and Port X4. The 'Configuration' column contains input fields for IP Address, Subnet Mask, Default Gateway, DNS Server Addresses, and MAC Address. The 'Status' column shows the current status of each interface. The 'Configuration' column contains input fields for IP Address, Subnet Mask, Default Gateway, DNS Server Addresses, and MAC Address. The 'Status' column shows the current status of each interface.

LAN interface (LAN X3/X4)	Status	Configuration
IP Address	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0
Default Gateway	0.0.0.0	0.0.0.0
DNS Server Addresses	8.8.8.8	8.8.8.8
	8.8.4.4	8.8.4.4
MAC Address	00:20:B5:B2:21:04	
Port X3		
Data Rate	100 Mbit/s	
Duplex Mode	Full Duplex	
Link Status	LinkUp	
Port X4		
Data Rate		
Duplex Mode		
Link Status	LinkDown	

To change the network settings, proceed as follows:

1. Enter your new settings in the [Configuration] column.
2. Click on [Apply and Reboot].

The settings are adopted, transferred to the CPU and the CPU is automatically restarted for activation.

Information You can also configure the network settings via iCube Engineer. For more details, please refer to the corresponding online help.

(2) Date and Time

The Date and Time page provides access to the NTP client configuration. NTP stands for **Network Time Protocol** and is a standard described in RFC 958 for time synchronisation in end devices connected via a network or the Internet. NTP is based on the connectionless UDP protocol (port 123). For synchronisation, NTP relies on Coordinated Universal Time (UTC), which is obtained from the individual clients and servers in a hierarchical system.

Information All iC9200 Series CPUs use UTC0 as the default setting, which corresponds to the coordinated world time UTC {00:00.

The Date and Time page provides access to the NTP client configuration. NTP stands for **Network Time Protocol** and is a standard described in RFC 958 for time synchronisation in end devices connected via a network or the Internet. NTP is based on the connectionless UDP protocol (port 123). For synchronisation, NTP relies on Coordinated Universal Time (UTC), which is obtained from the individual clients and servers in a hierarchical

Here you can configure the NTP client by adding new NTP server entries.



1. To do this, click below the table on

The dialog for adding an NTP server opens.

Add NTP server entry

Server Configuration	
Status	Active ▼
Server Hostname	<input type="text"/>
Min. polling time	1 min 4 sec ▼
Max. polling time	17 min 4 sec ▼
Comment	<input type="text"/>

2. Enter the according parameters.

- Server Host Name
 - Enter the address at which the NTP server can be reached in the network.
- Comment
 - Here you can assign an internal designation for the NTP server.
- The other parameters are for information and cannot be changed.

3. Click at [OK].

The dialog is closed and the NTP server is listed in the table.



You can remove entries with



and edit them with

4. Click on [Apply].

You will receive a message that applying the new NTP daemon configuration requires a restart of the NTP daemon and that this may lead to a real-time violation. With [OK], the NTP servers listed in the table are accepted for time-of-day synchronization and the NTP daemon is restarted.

(3) System Services


Here you can find status information about the enabled and disabled system services, as well as their factory default settings. You can increase the efficiency of your system by deactivating services that are not required.

Information

- Before disabling a service that is enabled by default, make sure that it is also not required for the entire system.
- Please also note that changing a setting always overwrites the entire system services settings.
- When PROFINET (optional) is disabled, the DCP protocol, which is used for identification and IP address assignment for participants in the PROFINET network, is also disabled.

YASKAWA Project Name: iCube_Demo_Case_03072024A HW: A01 FW: 2023-9-1 MAC: 00:20:85:B2:21:04

iC9226M-FSoE
JEYRM-
MPX022SE10L32-
2



Overview

General Data

Cockpit

Diagnostics

Axis Grid

EtherCAT

Motion Alarms

Notifications

Profinet

SliceBus

SliceBus Modules

Configuration

System Services

Service ID	Service Name	Factory Default	Activation
APP MANAGER	App Manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DATALOGGER	Data Logger	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ETHERCAT MASTER	EtherCAT Master	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FWM	Firewall Manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GRPC LOCAL SERVER	gRPC Remote Procedure Calls (Local)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IEC	IEC 61131-3 Runtime for iCube Engineer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
LINUX SYSLOG	PLCnext Syslog adapter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OPCUA	OPC UA Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
OPCUA CLIENT	OPC UA Client	<input type="checkbox"/>	<input type="checkbox"/>
PROFINET CONTROLLER	Profinet Controller	<input type="checkbox"/>	<input type="checkbox"/>
PROFINET DCP	Profinet DCP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
PROFINET DEVICE	Profinet Device	<input type="checkbox"/>	<input type="checkbox"/>
SLICEBUS	SliceBus	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
TRACING	Trace Controller	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1. Enable/Disable System Service

1. **By selecting or deselecting the corresponding check box, you enable respectively disable a system service in the list.**
2. **Use the [Apply and Reboot] button to apply the settings for the system services.**
After a security query, the settings for the system services are adopted and the CPU is restarted.

(4) Web Services

The page provides access to the configuration of web services, e.g. HTTPS certificate, which is used for the NGINX web server.

Information The HTTPS certificate and the associated private key are located as files in the file system of the CPU and are listed as symbolic links on the web page. During a firmware update, the existing certificate and key files are moved to a backup directory and symbolic links are created that refer to this backup.

1. NGINX Web Server

(a) Selected HTTPS Certificate

The HTTPS certificate is used to authenticate the CPU to the web server.

In the configuration table for the NGINX Web server you have the option of selecting the HTTPS certificate from one of the identity stores stored in the CPU.

1. **Select the corresponding Identity store.**

The corresponding HTTPS certificate is selected.

2. **Click on [Apply].**

The certificate is used for authentication in the configuration.

Information Please note that reconfiguring the web service can affect the real-time behavior of your system. Avoid this during productive operation.

(b) Self-signed HTTPS certificate


In addition to the HTTPS certificates stored in the CPU, you also have the option of selecting a self-signed certificate created by the firmware.

1. **To do this, select in the selection field [HTTPS-self-signed].**

The configuration of the self-signed HTTPS certificate is listed in a table. You can adapt these accordingly and generate new certificate files with [Apply].

2. **Enter the according parameters.**

- Distinguished name
 - Enter your company information here for identification.
- Validity
 - Enter the date in the format DD.MM.YYYY and the time in hh:mm:ss.
 - If at Valid not before the input field is empty, the current date is used.
 - If at Valid not after the input field is empty, the date 31.12.9999 and time 23:59:59 are used.
- Subject alternative names
 - The IP addresses from the network configuration of the CPU are suggested by default.

– You have the option of expanding or adapting this or specifying a DNS name. Use  to

add an entry. Use  to remove an entry.

Information If the web server is to be accessible via different IP addresses without an error message, you have to specify all IP addresses as Subject alternative names of the type IP address. If the CPU can be reached via DNS name, you have also to specify this!

3. **To apply the changes, click on [Re-generate HTTPS certificate].**

The certificate is regenerated. This overwrites an existing self-signed HTTPS certificate.

4. **Click on [Apply].**

The certificate is used for authentication in the NGINX configuration.

Information Please note that reconfiguring the web service can affect the real-time behavior of your system. Avoid this during productive operation.

4.8.5 Security

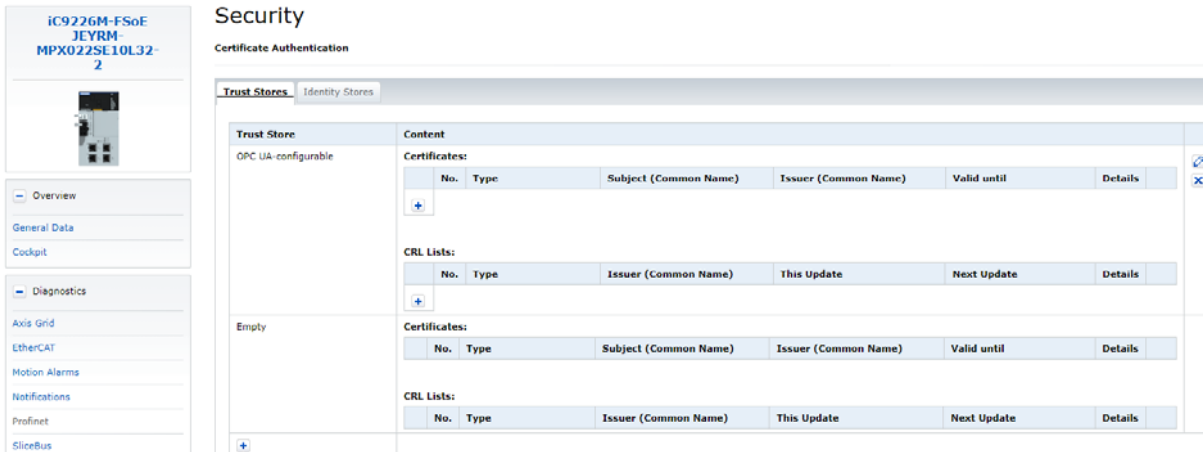
(1) Certificate Authentication

At [Certificate Authentication] you can manage your certificates for secure CPU communication. [Certificate Authentication] is divided into the following tabs:

- Trust Store
 - Trusted certificates and revocation lists of possible communication partners are stored here.
- Identity Store
 - The personally created certificates are stored here.

Information

- The name for each store can be used with the interfaces for TLS communication, e.g. TLS_SOCKET block in IEC 61131-3 or TlsSocket class in C++ or C#.
- The names of the stores are case-sensitive.



1. Tab: Trust Store

Each Trust Store is defined in the WBM by two tables:

- Table [Certificates]
 - In this table you can manage trusted Certificates and issuer certificates.
- Table [CRL lists]
 - In this table you can manage the revocation lists for the corresponding Trust Store. By storing untrusted certificates and issuer certificates here.

(a) Creating a Trust Store



1. To create a Trust Store, click the  button at the end of the table.

The input dialog opens for entering a name for the Trust Store.

2. Enter a name.
3. Click on [Add].

The dialog is closed and the new Trust Store is added.



You can remove it again with  and rename it with .

(b) Adding a Certificate



1. With  below the table [Certificates] you can add a certificate via the dialog.

Add Certificate

Trust Store

Certificate Type v

Certificate content in PEM Format:

Input Method

- Trust Store
 - Name of the Trust Store.
 - Certificate Type
 - Specify here whether the certificate is trusted or untrusted.
 - Certificate in PEM format
 - Certificate files can only be processed in PEM format.
 - Input Method
 - Here you can specify the format in which the certificate is to be added.
 - You can choose between text and file (PEM format).
2. **To add a certificate in text format, select at [Input Method] the [Text Content] parameter, enter the text in the input field and click on [Add].**
The input dialog is closed and the certificate is added in text format.
 3. **To add a certificate as file, select at [Input Method] the [File Upload] parameter, navigate to your certificate in PEM format via [Browse...] and click [Add].**
The input dialog is closed and the certificate is added as PEM file

(c) Adding a Revocation List



With  below the table [CRL lists] you can add a revocation list via the dialog.

Add CRL List

Trust Store

CRL Type

CRL content in PEM Format:

Input Method

- Trust Store
 - Name of the Trust Store.
- CRL Type
 - Specify here whether the revocation list is trusted or untrusted.
- Certificate in PEM format
 - Revocation list files can be processed in PEM format only.
- Input Method
 - Here you can specify the format in which the revocation list is to be added.
 - You can choose between text and file (PEM format).

(d) Deleting Certificates and Revocation Lists



1. To delete a certificate or a revocation list, click on the **certificate or revocation list**.
2. In the query dialog click on **[Remove]**.

(e) Detail View

The detail views provide detailed information on each certificate and each revocation list:



1. Click on **to open the detail view**.
The detail view is opened.
2. This is closed again with **[Close]**.

2. Tab: Identity Store

- You can create and manage multiple identity stores in the [Identity Store] tab.
- Each Identity Store usually contains an RSA key pair and the corresponding key certificate.
- Optionally, you can add further issuer certificates to an identity store.
- The IDevID and OPC UA-self-signed identity stores are part of the system and are supplied with the CPU.

Identity Store	Content				
	No.	Element	Type	Description	Details
IDeVID	1	Key Pair	RSA 2048 Hardware protected key	RSA Key Pair	[Details] [Download]
	2	Certificate	Key Certificate	Common Name: IC9226M-FSoE Valid not after: 9999-12-31T23:59:59 UTC	[Details] [Download]
	3	Certificate	Issuer Certificate	Common Name: IC9200 Series Device Signing RSA CA1 Valid not after: 9999-12-31T23:59:59 UTC	[Details]
	4	Certificate	Issuer Certificate	Common Name: IC9200 Series RSA CA1 Valid not after: 9999-12-31T23:59:59 UTC	[Details]
	5	Certificate	Issuer Certificate	Common Name: iCube Control Technology Root RSA CA1 Valid not after: 9999-12-31T23:59:59 UTC	[Details]
HTTPS-self-signed	1	Key Pair	RSA 2048	RSA Key Pair	[Details] [Download] [Close]
	2	Certificate	Key Certificate	Common Name: IC9200 Series HTTPS Valid not after: 9999-12-31T23:59:59 UTC	[Details] [Download] [Close]
OPC UA-configurable	1	Key Pair	RSA 2048	RSA Key Pair	[Details] [Download] [Close]
	2	Certificate	Key Certificate	Certificate not available. Please add a Key Certificate via the "Set" button on the right.	[Details]
OPC UA-self-signed	1	Key Pair	RSA 2048	RSA Key Pair	[Details] [Download] [Close]
	2	Certificate	Key Certificate	Common Name: eUAServer@IC9226M-FSoE Valid not after: 9999-12-31T23:59:59 UTC	[Details] [Download] [Close]

(a) Adding a Identity Store

1. With  below the table [Identity Store] you can add a Identity Store via the dialog.

Add Identity Store

Name

Key Pair ▼

Key Pair in PEM Format:

Input Method ▼

- Name
 - Name for the Identity Store.
 - Key Pairs
 - Specify here how the key pair is to be added.
 - You can enter the key pair or let it be generated.
 - Key Pair in PEM Format
 - Key files can be processed in PEM format only.
 - Input Method
 - Here you can specify the format in which the key pair is to be added.
 - You can choose between text and file (PEM format).
2. **To add a key pair in text format, select at [Key Pairs] the [Enter] parameter and at [Input Method] the [Text Content] parameter, enter the text in the input field and click on [Add].**
The input dialog is closed and the key pair is added in text format.
 3. **To add a key pair as file, select at [Key Pairs] the [Enter] parameter and at [Input Method] the [File Upload] parameter, navigate to your certificate in PEM format via [Browse...] and click [Add].**
The input dialog is closed and the key pair is added as PEM file.
 4. **To add a key pair generated by the CPU, select at [Key Pairs] the [Generate] parameter, select the encryption method in the dialog and click on [Add].**
The input dialog is closed and the key pair automatically generated by the CPU is added.

You can add, rename, define and remove key pairs or certificates by using the following buttons in the corresponding table entry:



- : New element - adds a new key pair or certificate.



- : Delete element - Deletes by clicking on [Remove] the selected key pair respectively certificate or, if selected, the Identity Store.



- : Details - Shows the detailed view of the corresponding element.



- : Download - You can download the public key content of a key pair as a PEM file.
 - If a key certificate is available, you can download it as a CRT file.
 - Save the file in a directory of your choice or open the file directly with a suitable tool.



- : Rename - depending on the position within a table, you can use this to rename the corresponding element.

(2) Firewall

The CPU is delivered with a preset firewall. The Linux[®] firewall [nftables] is used here. As described below, you can create rules from predefined basic rules or create your own new ones.

Information

- On delivery, the firewall is disabled!
- Please note that you only have access to the firewall settings as an administrator!

1. Accessing the Firewall

1. **Log in to the WBM as an administrator.**
2. **Navigate to [Security] - [Firewall].**

The configuration page for the firewall is opened.

The screenshot displays the WBM interface for the 'Security' section of an 'iC9226M-FSoE' device. The left sidebar contains navigation menus for Overview, Diagnostics, Configuration, and Security. The main content area is titled 'Security' and includes a 'Firewall' section. Under 'System Message', it shows 'Configuration status = OK'. The 'System Status' section indicates the firewall is 'Stopped' and provides a 'Show Rules' button. The 'General Configuration' section shows the status as 'Stop' and a checkbox for activation. Below this is the 'Basic Configuration' section, which includes 'ICMP Configuration' and a 'Basic Rules' table. The 'Basic Rules' table has columns for 'Seq.', 'Direction', 'Protocol', 'To Port', 'Comment', and 'Action'. It lists 8 rules, including NTP, Remoteing, SSH, HTTP, HTTPS, OPC UA, EtherCAT BAS server, and SNMP.

Seq.	Direction	Protocol	To Port	Comment	Action
1	Input	UDP	123	NTP (Network Time Protocol)	Accept
2	Input	TCP	41100	Remoteing (e.g. iCube Engineer)	Accept
3	Input	TCP	22	SSH	Accept
4	Input	TCP	80	HTTP	Accept
5	Input	TCP	443	HTTPS	Accept
6	Input	TCP	4840	OPC UA	Accept
7	Input	TCP	6000	EtherCAT BAS server	Accept
8	Input	UDP	161	SNMP (Simple Network Management Protocol)	Accept Discard Apply

2. [Apply] and [Discard]

- The changed firewall settings are transferred to the CPU with the [Apply] button.
- With the [Discard] button the settings made are discarded after a security query and the WBM page is reloaded.

3. [System Message]

Messages regarding the transfer of firewall settings to the CPU are shown at [System Message]. The following system messages can occur:

- Status = OK
 - The configured firewall settings were successfully transferred to the CPU.
- Warning
 - The CPU reports a warning, e.g. if one or more additional filter configurations in the system exist. The warn- ing contains the names of all additionally loaded filter tables.
- Error
 - At least one firewall configuration is incorrect.

4. [System Status]

- When the firewall is enabled, you can use the [Show Rules] button to show an overview of all enabled firewall rules as a txt file.
- With [Save to File] you can save the file locally on your PC as a txt file.

5. [General Configuration]

At [General Configuration] you can see the current firewall status and set it temporarily or permanently.

Temporary enabling

1. Select at [Status] the entry [Start] or [Restart].
2. Click on [Apply].

The firewall is enabled. After restarting the CPU, the firewall is disabled again.

Temporary disabling

1. Select at [Status] the entry [Stop].
2. Click on [Apply].

The firewall is disabled. After restarting the CPU, the firewall is enabled again.

Permanent enabling

1. **Activate the [Activation] selection field.**
2. **Click on [Apply].**

The firewall is enabled and remains enabled even after a restart.

Permanent disabling

1. **Disable the [Activation] selection field.**
2. **Click on [Apply].**

The firewall is disabled and remains disabled even after a restart.

Information By disabling the firewall you endanger the security of your system, especially if it can be reached via the Internet! The firewall should only temporarily be disabled for testing purposes such as troubleshooting.

6. Configuration

The configuration of the firewall rules is divided into the following tabs:

- Basic Configuration
 - Here you will find predefined firewall rules which you can enable or disable.
- User Configuration
 - Here you can create, enable or disable your own firewall rules according to defined specifications.

There is a [Action] column in both tabs. The firewall settings are applied with the [Apply] button. There are the following setting options for the [Action] column:

- Accept
 - The corresponding connection and connection request is accepted.
 - The corresponding connection can be established.
- Drop
 - The corresponding connection is interrupted.
 - There is no answer to the corresponding request.
 - The corresponding package is discarded.
- Reject
 - The corresponding connection is rejected.
 - The sender receives a response to the corresponding request.
- Continue
 - The rule is not executed.
 - This can be used e.g., to skip a rule in the [Basic Configuration] and instead create a rule in the [User Configuration] and enable it there.

7. Tab: Basic Configuration

[ICMP Configurations]

- [Incoming ICMP requests accepted]
 - enabled: Incoming ICMP echo requests are accepted. The CPU can be reached with a ping request.
 - disabled: Incoming ICMP echo requests are blocked. The CPU can not be reached with a ping request.
- [Outgoing ICMP requests accepted]
 - enabled: Outgoing ICMP echo requests are accepted. Ping requests from the CPU are transmitted.
 - disabled: Outgoing ICMP echo requests are blocked. Ping requests from the CPU are blocked. [Basic Rules]

- Here you will find predefined firewall rules for the corresponding incoming connections. You can control their use accordingly via [Action].
- The settings are valid for all Ethernet interfaces. For individual customization, you can instead create a rule in the [User Configuration] and enable it there.

Information **Blocking the WBM access**

- On the CPU the WBM is accessed via TCP port 443.
- By blocking this port with permanently enabled firewall, you have no more access to the WBM of the CPU even after a reboot.
- Resetting to the factory settings also resets the firewall to its default settings, among others. This way you get access to the WBM of the CPU again with the original access data.

Information **Deployment as PROFINET controller (optional)**

Connections to PROFINET devices can only be established if you select the rule [PROFINET unicast / multicast ports] (UDP ports 34962 - 34964) [Accept].

8. Tab: User Configuration

- In addition or as an alternative to the [Basic Rules], you can define and enable your own user-specific firewall rules for different filter categories.
- You create firewall rules for the output in the [Output Rules] tab.
- You create firewall rules for the input in the [Input Rules] tab.
- With the order of firewall rules in the table, you define the priority for applying them.
- You can create new rules, delete rules or change the order of the rules by using the following buttons at the end of the table:



– : New rule - adds a new firewall rule.



– : Delete rule - deletes the selected firewall rule.



– : Rule up - moves the rule up.





– : Rule down - moves the rule down.

- The firewall settings are applied and enabled with the [Apply] button. An existing configuration will be overwritten.

In addition to [Action], there are the following parameters for specifying a firewall rule:

- [Seq.]
 - Numbers the order for the priority according to which the firewall rules are applied.
 - The rules are applied in ascending order from 1.



– With  and  you can move the firewall rules accordingly.

- [Interface]
 - In the [Input Rules] tab you can select a single interface from a selection list for which the rule is to be applied.
 - You have no choice in the [Output Rules] tab. Here the rule applies to all interfaces.
- [From IP]
 - Enter the IP address for connections that are received from this address.

- [From Port]
 - Enter the port for connections that are received via this port.
 - You can specify all ports, selected ports, or a range of values.
- [To IP]
 - Enter the IP address for connections that are sent to this address.
- [To Port]
 - Enter the port for connections that are sent via this port.
 - You can specify all ports, selected ports, or a range of values.
- [Comment]
 - Here you can comment your filter rule accordingly.

(3) SD Card


The CPU has a slot for a Yaskawa SD card. *For future use.*

(4) Syslog Configuration

Here you can configure Syslog servers. Syslog respectively Syslog-ng is a standard for transmitting log messages in a network.

The screenshot shows the Yaskawa WBM interface for Syslog Configuration. The page title is 'Security' and the sub-section is 'Syslog Configuration'. Under 'General Options', there is a checkbox for 'Syslog Server Destinations Activation' which is currently unchecked. A warning message states: 'Warning: Applying the configuration can affect the real-time behavior of the system. Avoid reconfiguration during productive operation!'. Below this is a table for 'Syslog Server Destinations' with columns: Hostname, Port, Protocol, Facilities, and Severity Level. A plus sign (+) is located at the bottom of the Hostname column. At the bottom right of the configuration area, there are 'Discard' and 'Apply' buttons.

1. Create Syslog Server Destination

1. To create a Syslog server destination, click at  at the bottom of the table.

The dialog for configuring a Syslog server destination opens.

Add a new Syslog Server Destination

General Options	
Hostname	<input type="text"/> ! This field is required.
Protocol	TCP
Port	When empty or zero: Default value will be used
Filter Options	
Facilities	<input checked="" type="checkbox"/> auth <input type="checkbox"/> cron <input type="checkbox"/> daemon <input type="checkbox"/> kern <input type="checkbox"/> local <input type="checkbox"/> syslog <input type="checkbox"/> user
Severity Level	>= Warning (warning)

OK Cancel

2. **Under [General Options] enter the following parameters:**

- Host Name
 - Host name respectively IP address of the Syslog server to which the log data is to be sent.
- Protocol
 - Transmission protocol to the server. TLS is recommended for secure transmission; for this purpose, a trust store must be defined for verification. This can be done via [4.8.5 \(1\) Certificate Authentication on page 89](#).
You can specify the corresponding Trust Store at [Trust Store].
- Port
 - Port over which the communication with the Syslog server is to take place. Ensure that the port is enabled in the firewall settings for outgoing requests. [4.8.5 \(2\) Firewall on page 94](#)

3. **Specify the following parameters at Filter Options:**

- Facilities
 - Here you specify the system type of the log data.
- Severity Level
 - Determine here the severity level from which the log data is sent to the Syslog server. Level 1: >= Internal (debug): All messages are sent. Level 2: >= Information (info): Messages >= level 2 are sent. Level 3: >= Warning (warning): Messages >= level 3 are sent. Level 4: >= Error (err): Messages >= level 4 are sent. Level 5: >= Critical Error (crit): Messages >= level 5 are sent. Level 6: >= Fatal Error (alert): Messages >= level 6 are sent. Level 7: Emergency (emerg) Only emergency messages are sent.

4. **Click at [OK].**

The dialog is closed and the Syslog server is listed in the table.

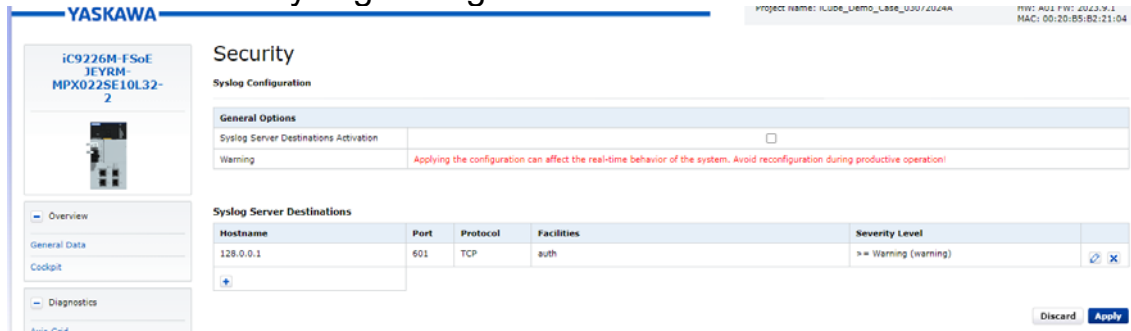


You can remove entries with



and edit them with

2. Enable or Disable Syslog Configuration

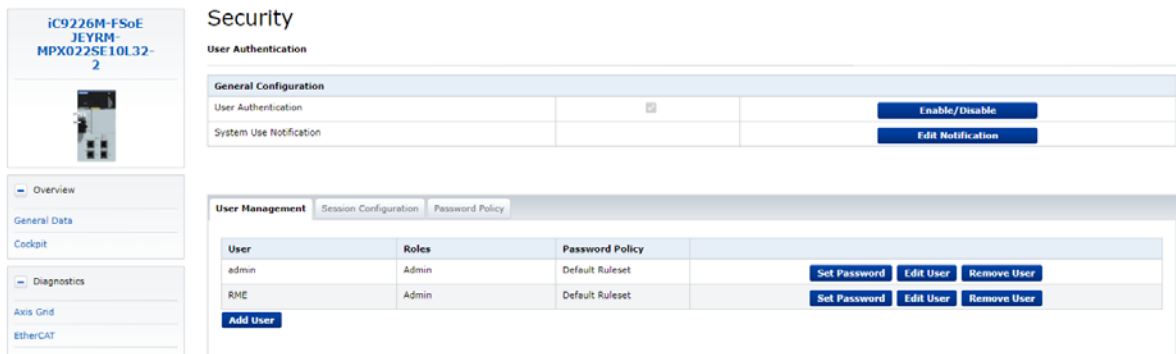


1. By selecting or deselecting the control field of [Syslog Server Destination Activation] at [Syslog Configuration] you can enable respectively disable the Syslog server targets specified in the table.
2. Click on [Apply].
The settings are accepted.

(5) User Authentication

- At [User Authentication] you can enable or disable user authentication.
- If user authentication is enabled, you have access to definable components of the CPU and functions in iCube Engineer exclusively by specifying user name and password.
- If user authentication is disabled, access takes place without a user query. The areas for the administrator remain password-protected.

- Information**
- By default user authentication is enabled. On delivery, the "admin" user is already created with administrator rights.
 - Please note that by disabling the user authentication you endanger the security of your system against unauthorized access!
 - Use the administrator password printed on the CPU only for the initial login to the WBM.
 - After you have successfully logged in, you should change the administrator password for security reasons.



1. Enable/Disable User Authentication

1. **Click the [Enable/Disable] button next to User Authentication.**
The user authentication dialog is opened.
2. **Here you can enable respectively disable the user authentication by selecting or dese- lecting the checkbox.**
3. **With [Save] the changes are applied and the dialog is closed.**

2. Changing System Use Notification

Every time you log on to the CPU via WBM or iCube Engineer, System Use Notification is shown. You can edit this text for customization. The displayed information is independent of the language used for the user interface. You should therefore take into account all required languages when editing.

1. **To edit, click [Edit Notification] next to System Use Notification.**
The dialog window for editing the text is opened.
2. **Adjust your text accordingly.**
3. **With [Save] the changes are applied and the dialog is closed.**

3. User Management

User authentication is used to manage the access data of all users who are authorized to access the CPU and to assign the required access authorizations to each user. The user data of the newly created users are stored internally in the CPU.

(a) Adding a User

1. **Click the [Add User] button.**
The dialog window for creating a new user is opened.
2. **Enter user name and password.**

Information When assigning user names and passwords, note the length restriction of 127 bytes for passwords and 63 bytes for user names. The characters are encoded with UTF-8 and the number of bytes used depends on which characters are entered. For normal characters (letters a-z or digits 0-9) 1 byte per character is used. Up to 4 bytes per character are used for special characters and umlauts. The length limit therefore limits the number of bytes and not the number of characters.

3. **With [Add] the new user is added to the list and the dialog is closed.**

(b) Removing a User

1. **In the table behind the user entry that you want to remove, click on the [Remove User] button.**
A security query follows to remove the user entry.
2. **With [Remove] the user entry is removed from the table and the dialog is closed.**

(c) Change Password

1. **Click the [Set Password] button in the table behind the user entry whose password you want to change.**
The dialog window for entering the password for the corresponding user entry is opened.
2. **Enter your new password in the 2 input fields.**
3. **With [Save] the new password for the user entry is applied and the dialog is closed.**

4. Modifying User Roles

You can select one or more user roles with different permissions for each user entry. These permissions control access to:

- SD card / parametrization memory (param. memory) of the CPU
- Operating system
- iCube Engineer
- Web-based management - WBM
- OPC UA server of the CPU

4. **Click the [Modify Roles] button in the table behind the user entry whose role you want to change.**

The dialog window for assigning roles for the corresponding user entry opens.

5. **Assign the corresponding roles to the user entry by selecting them.**

6. **With [Save] the selected roles for the user entry are applied and the dialog is closed.**

Table 6.3 User roles and their access rights

Access to SD card / param. memory	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
SFTP access to the file system with an FTP client Please note: Authentication with user name and password is always required for SFTP access, even if user authentication is disabled.	✓												
Accessing the operating system	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
SSH access to the operating system Please note: Authentication with user name and password is always required for SSH access, even if user authentication is disabled.	✓												
iCube Engineer	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
Show values in the cockpit (e.g. utilization).													
Transfer the project to the CPU.													
CPU stop / CPU cold/warm/restart													
CPU restart (reboot).	✓												

Continued on next page

Continued from previous page

iCube Engineer	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Write
CPU reset (default type 1).	✓												
Read online variables.	✓	✓	✓			✓		✓	✓	✓	✓		
Overwrite variables.	✓					✓		✓		✓			
Set and delete breakpoints.	✓					✓		✓					
Read CPU status.	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Read device information.	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Accessing WBM	Admin	Security Admin	Security Auditor	Cert. Manager	User manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Write
Information - General Data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - EtherCAT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - Motion Alarms	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - Notifications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - PROFINET (optional)													
Diagnostics - SliceBus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - SliceBus Modules													
Configuration - Network													
Configuration - Date and Time													
Configuration - System Services	✓	✓											
Configuration - Web Services	✓	✓											
Security - Certificate Authentication													

4.8 Web-Based Management - WBM

Accessing WBM	Admin	Security Admin	Security Auditor	Cert. Manager	User manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
Security - Firewall	✓	✓											
Security - SD Card	✓	✓											
Security - Syslog Configuration	✓	✓											
Security - User Authentication	✓	✓			✓								
Administration - iCube Apps	✓	✓				✓							
Administration - Firmware Update													
Administration - License Management													
Accessing OPC UA server	Admin	Security Admin	Security Auditor	Cert. Manager	User Manager	Engineer	Commissioner	Service	Data Viewer	Data Changer	Viewer	File Reader	File Writer
Read online variables.	✓	✓				✓		✓	✓	✓	✓		
Write online variables.	✓					✓		✓		✓			
Read files.												2	
Write files.													3

1) Read access only.

2) FileReader can only read files via an OPC UA client if the OPC UA file transfer is activated in iCube Engineer. Information on this can be found in the iCube Engineer online help.

3) FileWriter can only write files via an OPC UA client if the OPC UA file transfer is activated in iCube Engineer. Information on this can be found in the iCube Engineer online help.

4.8.6 Administration

(1) iCube Apps

1. Enable/Disable User Authentication

Here you can install and uninstall apps. After successful installation, you can also start and stop the apps from here. iCube Apps are software applications ranging from libraries to complete programmes provided to you by Yaskawa.

The screenshot shows the 'Administration' page for iCube Apps. On the left, there is a sidebar with 'Overview' selected, showing 'General Data' and 'Credits'. The main content area is titled 'Administration' and 'iCube Apps'. It features a 'System Message' section with an 'Information' message and a 'Warning' message. Below this is a table titled 'Installed iCube Apps' with columns for App Name, App ID, Version, Min FW Version, Manufacturer, License Status, and App Status. The table contains one entry: 'iCube-Web/Visu Daemon' with App ID '80015910091101', Version '0.1', Min FW Version '23.3.0', Manufacturer 'exor', License Status 'License invalid', and App Status 'STOP'. There are 'Start' and 'Uninstall' buttons for this app. An 'Install App' button is also visible at the bottom left of the table.

App Name	App ID	Version	Min FW Version	Manufacturer	License Status	App Status
iCube-Web/Visu Daemon	80015910091101	0.1	23.3.0	exor	License invalid	STOP

All installed apps are listed in the table with additional app-specific information.

- App Name
 - Name of the App.
- App ID
 - Unique identifier of the app.
- Version
 - Version of the app
- Min FW Version
 - Firmware version of the CPU from which the app can be used.
- Manufacturer
 - Manufacturer of the App.
- License Status
 - License status of the app.

Information and warning messages are listed under [System Message].

- Information
 - Additional apps can have a negative impact on real-time behavior.
 - Please note that a licence may be required for installation or use.

2. Installing an App

To install an app, proceed as follows:

1. **Click at [Install App].**
2. **In the file explorer that opens, select the app (*.app) to be installed.**
3. **Click at [Open].**

The selected app container is now sent to the controller and installed. After successful installation, the app is listed in the Installed iCube Apps table.

3. Starting an App

To start an app, click in the table [Installed iCube Apps] at [Start] behind the corresponding app.

The app is started and the app status [RUN] in the column [App Status] is shown.

Information Please note that starting multiple apps may require a CPU restart. You will be informed of the impending restart by a dialog that opens.

4. Quit an App

To quit an app, click in the table [Installed iCube Apps] at [Stop] behind the corresponding app.

The app is quit and the app status [Stop] in the column [App Status] is shown.

5. Uninstalling an App

1. To uninstall an app, you must quit it first. To do this, click in the table [Installed iCube Apps] at [Stop] behind the corresponding app.
2. To uninstall, click the following in the table [Installed iCube Apps] at [Uninstall] behind the corresponding app.

After a security prompt, the corresponding app is uninstalled.

(2) Firmware Update

Here you can execute a firmware update on your CPU.

Information Please note that you can only execute a firmware update with administrator rights!

The screenshot shows the YASKAWA Administration web interface. On the left is a sidebar with the YASKAWA logo and navigation links: Overview, General Data, Cockpit, Diagnostics, Axis Grid, EtherCAT, Motion Alarms, and Notifications. The main content area is titled 'Administration' and 'Firmware Update'. It contains a section 'Select the update container file' with a 'Browse...' button. Below this, the status is shown as 'Status: OK'. The top right corner of the interface displays 'Project Name: iCube_Demo_Case_03072024A'.

1. Proceeding



When installing a new firmware you have to be extremely careful. Under certain circumstances you may destroy the CPU, for example if the voltage supply is interrupted during transfer or if the firmware file is defective. In this case, contact our support!

You can find the currently installed firmware version of your CPU in the WBM at [Information] - [General Data]. Here you can also check whether the firmware update was successful. [4.8.2\(1\) General Data on page 74](#)

1. The latest firmware can be found at <https://www.icubecontrol.com/downloads.html>

Load the current firmware file into your working directory.

2. **Unzip the zip file.**
3. **Go back to the WBM to [Firmware Update] and click on [Browse...].**

A file selection window is opened.

4. **Navigate to the unzipped raucb file and click on [Open].**

The firmware file to be installed is loaded and shown in the WBM.

5. **Click on [Start Update].**

The firmware file is transferred to the CPU and the firmware update is started. The status of the file transfer and the status of the update process are shown in the WBM as a progress bar.

6. **The connection to the CPU is interrupted during the firmware update. After the start-up of the CPU you have to log on to the WBM of the CPU again. This will refresh the WBM pages.**
7. **To check the firmware update, in WBM, go to [Information] - [General Data] page.**
[4.8.2\(1\) General Data on page 74](#)

The new firmware version should be shown here. Otherwise start the update again. If the update does not work, please contact our support.

(3) License Management

1. Tab: [View Containers]

Here you can view and manage the licenses that are installed on the CPU. Several licenses can be combined in one [container].

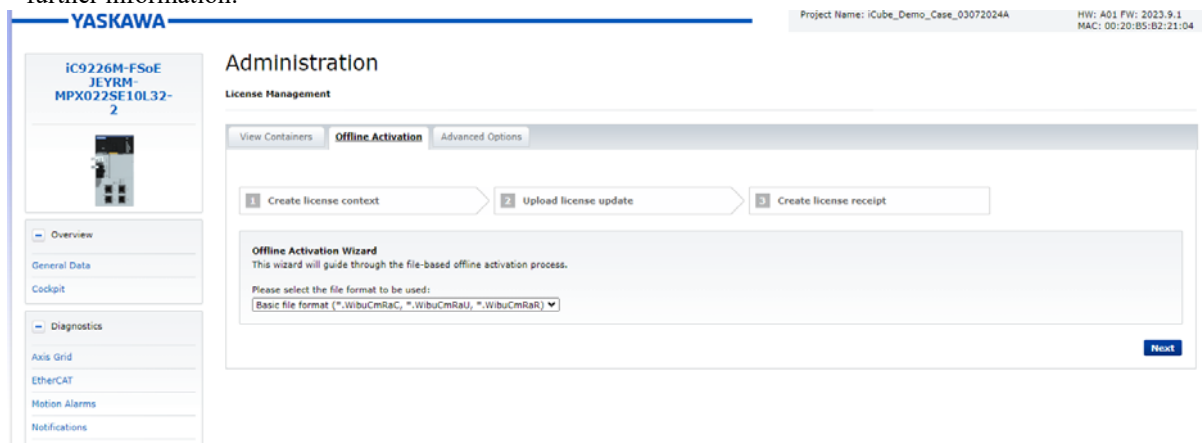
Container	Storage Location	Firm Code	Firm Text	Product Code	Feature Map	Product Text
130-3854516288	Device	6001591				

In the table all containers with the licenses are listed. The [Refresh] button reloads the list.

- Container
 - Serial number of the container in which the licenses are managed.
- Storage Location
 - Storage location where the container is stored.
- Firm Code
 - Identification number of the licensor.
- Firm Text
 - Description of the licensor.
- Product Code
 - Unique identification code of the licensed software.
- Feature Map
 - Information on the functional scope of the software.
- Product Text
 - Description of the license.

2. Tab: [Offline Activation]

Here you can activate a previously purchased license offline by means of a license file. The term "offline" in this context means that the CPU on which the licensed software is running does not have to be connected to the Internet. The offline activation wizard guides you through the activation process and provides further information.



3. Tab: [Advanced Options]

With the button [Create Container] you can create a new license container for your licence files. To delete the corresponding container, click on the corresponding button [Delete].

Information Please note that you cannot undo the deletion of a license container! You should only carry out this action on the instructions of Yaskawa support!

YASKAWA Administration

Project Name: iCube_Demo_Case_03072024A HW: A01 FW: 2023.9.1
MAG: 00:20:85:B2:21:04

ic9226M-FSoE
JEVRM-
MPX022SE10L32-
2

Overview
General Data
Cockpit

Diagnostics
Axis Cmd
EtherCAT
Motion Alarms
Notifications
Profinet
Sicebus

License Management

View Containers Offline Activation **Advanced Options**

Storage Location	Container
Device UUID: 0ae71409-b0e1-4b9d-9b5f-9bceff8dc3c	Active <input type="button" value="Delete"/> 130-3854516288

4. Steps of Activation

You have received a license key from Yaskawa. The activation of the license in your CPU takes place according to the following procedure:

Please follow the "Get Help" button in the controller feature license section of <https://icubecontrol.com/licensing.html>.

Information Please note that if you have purchased a PROFINET license, you must activate the PROFINET functionality in WBM in the configuration after activation. [4.8.4\(3\) System Services on page 87](#)

Appearance and Parts

This chapter describes detailed information on the appearance and parts of the iC9200.

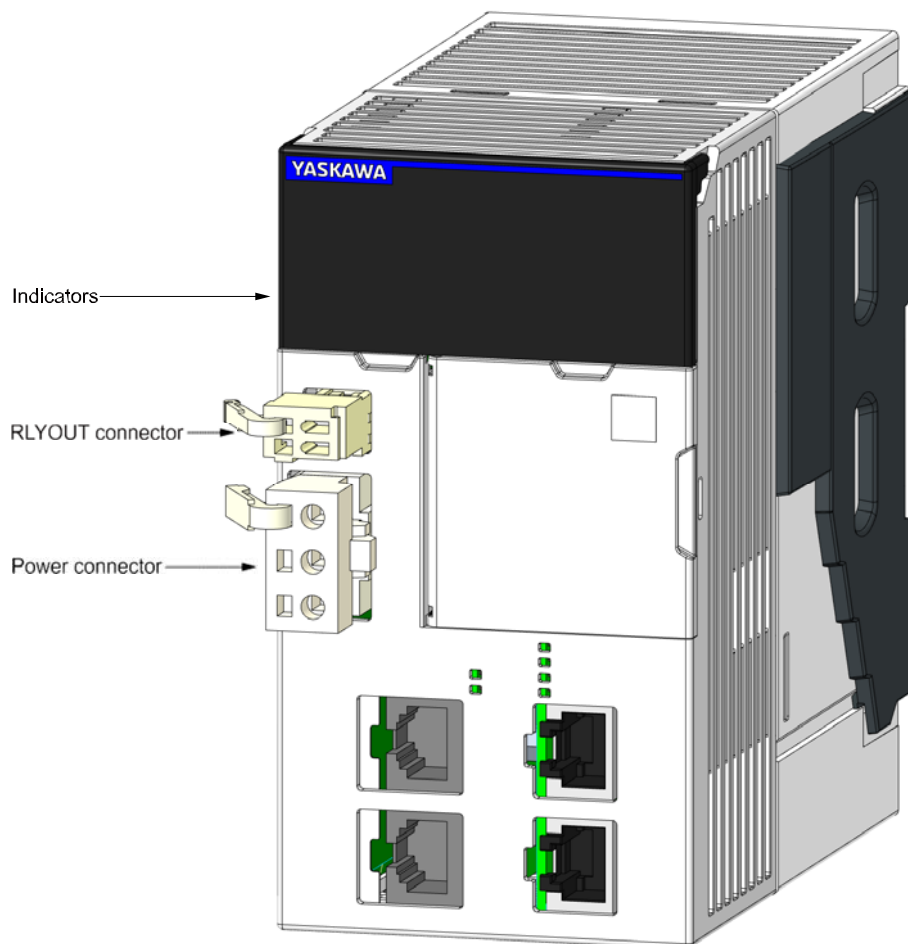
5.1	Appearance and Parts Description	112
5.1.1	Appearance and Part Names	112
5.1.2	Display and Indicators.....	113
5.1.3	Connectors.....	120
5.1.4	Switches.....	125
5.1.5	Memory.....	126
5.1.6	Buffering Mechanisms	127

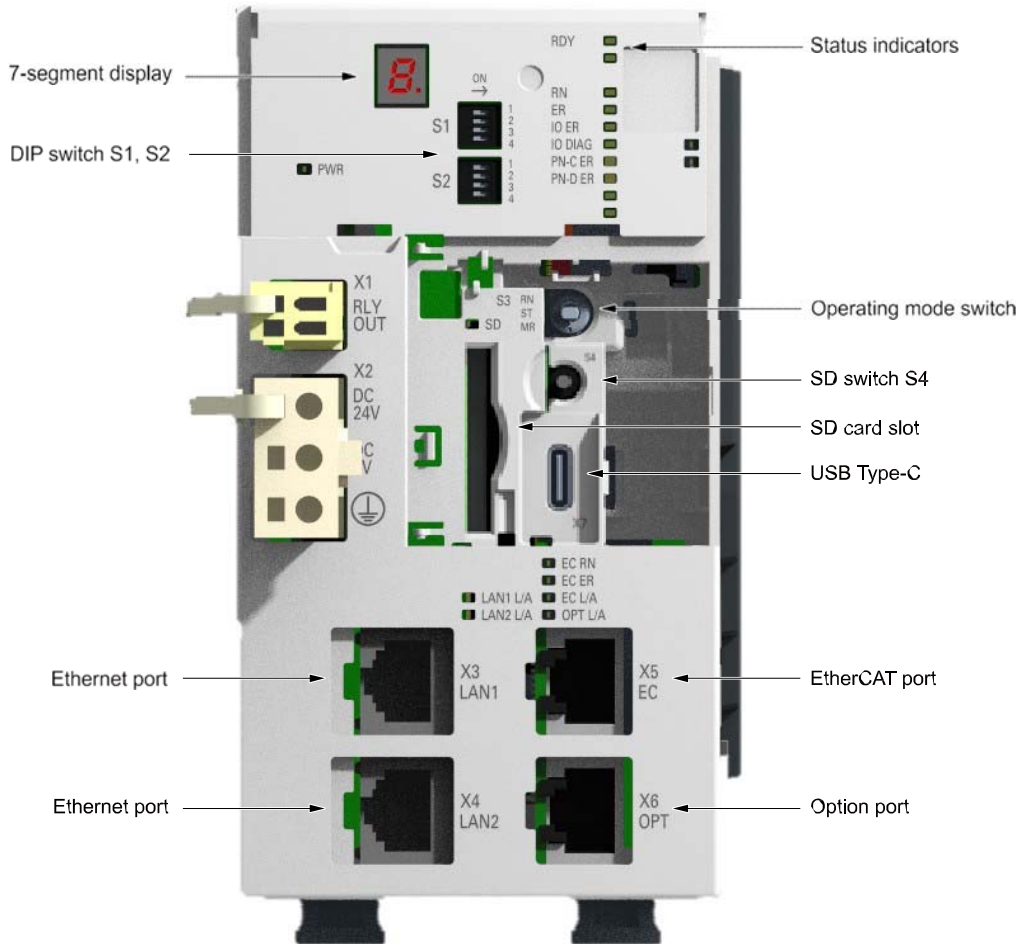
5.1 Appearance and Parts Description

This section shows the appearance and part names and describes the indicators and connectors.

5.1.1 Appearance and Part Names

The following figure shows the appearance of the power supply section and the part names.

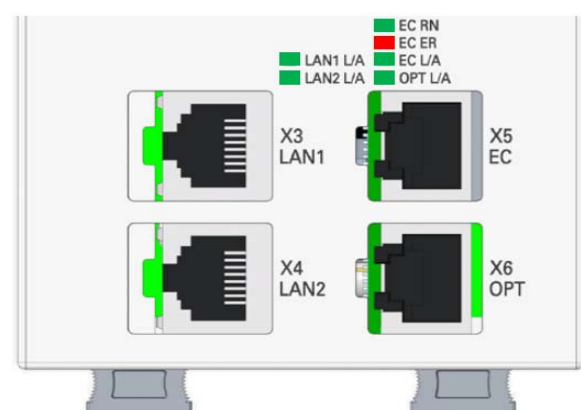
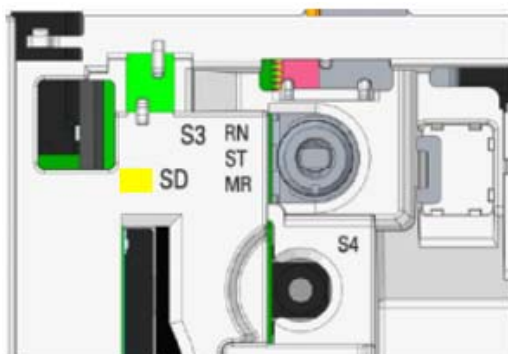
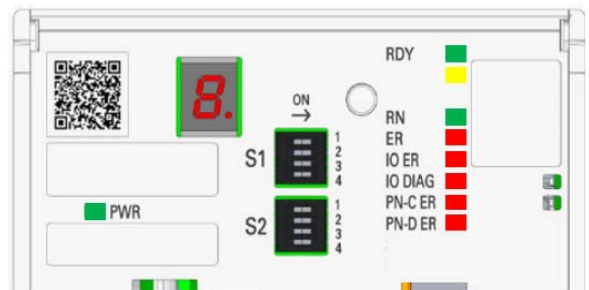









5.1.2 Display and Indicators

(1) Status Indicators

The indicators on the front of the product indicate the status of the functions listed below.



Function	Reference
POWER LED	 (a) <i>POWER LED on page 115</i>
Uboot	 (b) <i>Uboot on page 115</i>
Linux and Overlay File System	 (c) <i>Linux and Overlay File System on page 116</i>
Firmware Update	 (d) <i>Firmware Update on page 117</i>
Factory Reset	 (e) <i>Factory Reset on page 117</i>

Continued on next page.

Continued from previous page.

Function	Reference
SliceBus	(f) <i>SliceBus on page 117</i>
PROFINET Controller	(g) <i>PROFINET Controller on page 117</i>
PROFINET Device	(h) <i>PROFINET Device on page 118</i>
PROFINET System	(i) <i>PROFINET System on page 118</i>
SD Card	(j) <i>SD Card on page 119</i>
EtherCAT Operation	(k) <i>EtherCAT Operation on page 119</i>
Ethernet Link	(l) <i>Ethernet Link on page 119</i>
EtherCAT Link	(m) <i>EtherCAT Link on page 119</i>

(a) POWER LED

The following LED indicator shows the operation status of the iC9226M.

Indicator	Indicator Name	Color	Meaning When Lit
PWR	PWR	Green	The iC9226M is operating normally.

(b) Uboot

LED Behavior											Controller State
RDY (green)	Resvd (yellow)	RN (green)	ER (red)	IO ER (red)	IO DIAG (red)	PN-C ER (red)	PN-D ER (red)	SD (yellow)	EC RN (green)	EC ER (red)	
Not lit	Not lit	Not lit	Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Uboot bootloader is starting.
Flashing green 2 Hz interval	Not lit	Not lit	Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Uboot bootloader has copied the kernel successfully.
Not lit	Not lit	Not lit	Flashing red 2 Hz interval	Lit	Lit	Lit	Lit	Not lit	Not lit	Not lit	An error occurred when loading kernel and/or device tree.
Not lit	Not lit	Not lit	Flashing red 2 Hz interval	Flashing red 2 Hz interval	Flashing red 2 Hz interval	Flashing red 2 Hz interval	Flashing red 2 Hz interval	Not lit	Not lit	Not lit	An error occurred due to illegal DIP switch combination.

(c) Linux and Overlay File System

LED Behavior											Controller State
RDY (green)	Resvd (yellow)	RN (green)	ER (red)	IO ER (red)	IO DIAG (red)	PN-C ER (red)	PN-D ER (red)	SD (yellow)	EC RN (green)	EC ER (red)	
Not lit	Not lit	Not lit	Flashing red 0.5 Hz	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	PLCnext runtime isn't loaded or it has shut down.
Not lit	Not lit	Not lit	Flashing red 2 Hz interval	Not lit	Not lit	Not lit	Not lit	Flashing yellow 2 Hz interval	Not lit	Not lit	Error mounting SD-card
Not lit	Not lit	Not lit	Flashing red 2 Hz interval	Not lit	Not lit	Not lit	Not lit	Flashing yellow 1 Hz interval	Not lit	Not lit	Error SD-card certificate
Not lit	Not lit	Not lit	Flashing red 2 Hz	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Error out of flash memory
Flashing green 2 Hz interval	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	PLC is loading FW
Not lit	Not lit	Not lit	Flashing red 1 Hz	Flashing red 1 Hz	Flashing red 1 Hz interval	Flashing red 1 Hz interval	Flashing red 1 Hz interval	Not lit	Not lit	Not lit	Power cycle of the PLC required
Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	PLCnext runtime system successfully initialized. The controller is in the READY/STOP/HALT state; user application program is not being processed.
Lit	Not lit	Flashing green 0.2s ON/1s	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	The controller is in the HALT state; user application program is not being processed.
Lit	Not lit	Not lit	Flashing red 1 Hz	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	System watchdog was triggered and the controller has rebooted.
Lit	Not lit	Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	The controller is in the RUN state. No error has occurred.
Lit	Not lit	Not lit	Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	The controller is in the PLC state READY/STOP with error.

(d) Firmware Update

LED Behavior											Controller State
RDY (green)	Resvd (yellow)	RN (green)	ER (red)	IO ER (red)	IO DIAG (red)	PN-C ER (red)	PN-D ER (red)	SD (yellow)	EC RN (green)	EC ER (red)	
Not lit	Not lit	Flash - ing green 2 Hz interval	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Firmware update in progress

(e) Factory Reset

LED Behavior											Controller State
RDY (green)	Resvd (yellow)	RN (green)	ER (red)	IO ER (red)	IO DIAG (red)	PN-C ER (red)	PN-D ER (red)	SD (yellow)	EC RN (green)	EC ER (red)	
Not lit	Not lit	Not lit	Flash - ing green 1 Hz interval	Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit
Not lit	Not lit	Not lit	Flash - ing green 2 Hz interval	Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit
Not lit	Not lit	Not lit	Flash - ing green 2 Hz interval	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit

(f) SliceBus

LED Behavior		Controller State
IO ER (red)	IO DIAG (red)	
Not lit	Not lit	No errors on local bus
Lit	Not lit	Configuration/bus failure
Not lit	Lit	Diagnostic information available

(g) PROFINET Controller

LED Behavior	Controller State
PN-C ER (red)	
Not lit	Active communication to each configured PN device, or PN controller not configured in user project
Lit	No link status or no 100MBit/s or full duplex link available while PN Controller is configured
Flashing red 1 Hz interval	Link status available but no active communication to all configured PN devices available while PN controller is configured

(h) PROFINET Device

LED Behavior	Controller State
PN-D ER (red)	
Not lit	Active communication to a PN controller
Lit	No active PN communication established and no link available
Flashing red 1 Hz interval	Link status available but no active PN communication to PN controller

(i) PROFINET System

LED Behavior	Controller State
RDY (green)	
Flashing green 1 Hz interval	Device identification blinking (DCP protocol)

(j) SD Card

LED Behavior											Controller State
RDY (green)	Resvd (yellow)	RN (green)	ER (red)	IO ER (red)	IO DIAG (red)	PN-C ER (red)	PN-D ER (red)	SD (yellow)	EC RN (green)	EC ER (red)	
Not lit	Not lit	Not lit	Flashing red 1 Hz interval	Flashing red 1 Hz interval	Flashing red 1 Hz interval	Flashing red 1 Hz interval	Flashing red 1 Hz interval	Flashing yellow 1 Hz interval	Not lit	Not lit	Unauthorized removal of SD card during operation
Not lit	Not lit	Not lit	Lit	Not lit	Not lit	Not lit	Not lit	Lit	Not lit	Not lit	SD card used for overlay file system

(k) EtherCAT Operation

LED Behavior		Controller State
EC RUN (green)	EC ERR (red)	
Flashing green 2.5 Hz interval	–	Pre operation
Flashing green 0.2s ON/1s interval	–	Safe operation
Lit	–	Operating
Not lit	–	INIT/Unknown (default)
–	Not lit	No error state (default)
–	Flashing red 2.5 Hz interval	SubDevices configured, link available but topology not ok
–	Lit	SubDevices configured, link not available

(l) Ethernet Link

LED Behavior		Controller State
LAN1 L/A (green)	LAN2 L/A (green)	
Not lit	Not lit	Ethernet link is down
Lit	Lit	Ethernet link is up 100MBit/s, no activity detected
Flashing green	Flashing green	Ethernet link is up 100MBit/s, activity detected
Lit	Lit	Ethernet link is up 1GBit/s, no activity detected
Flashing green	Flashing green	Ethernet link is up 1GBit/s, activity detected

(m) EtherCAT Link

LED Behavior		Controller State
EC L/A (green)	OPT L/A (green)	
Not lit	Not lit	Ethernet link is down
Lit	Not lit	Ethernet link is up, no activity detected
Flashing green	Not lit	Ethernet link is up, activity detected

(2) 7-Segment Display

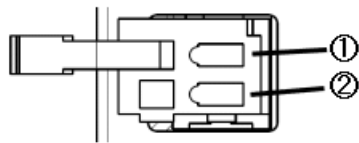
For future use

5.1.3 Connectors

The iC9226M has the RLYOUT ,power supply, EtherCAT, Ethernet, USB connector, and the SD card slot.

(1) RLYOUT Connector

This connector outputs the operating status of the iC9226M.



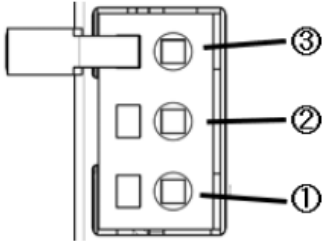
Model: 734-302

(a) Pin Assignments

No.	Signal Label	Contents
1	OUT	Normal operation: Circuit closed. Error: Circuit open.
2	OUT	

(2) Power Connector

Connect the DC power supply to the power connector on the power supply section.



Name	Model	Color
Power Connector	4-2013522-3	White

(a) Pin Assignments

Pin No.	Signal Label	Contents
3	DC 24 V	24-VDC input
2	DC 0 V	0-VDC input
1	FG	Connects to the frame ground.

(3) EtherCAT port X5

This connector is used to connect EtherCAT communications devices.
 This product is equipped with one EtherCAT communications circuit using one port.

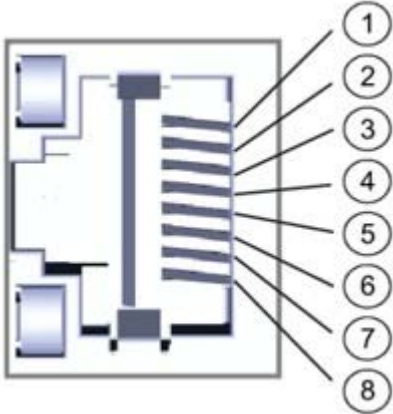


Table 4.1 8pin RJ45 jack:

Pin	Signal	Description
1	TD+	Send data +
2	TD-	Send data -
3	RD+	Receive data +
4	n.c.	reserved
5	n.c.	reserved
6	RD-	Receive data -
7	n.c.	reserved
8	n.c.	reserved

- The CPU has an integrated Ethernet communication processor with EtherCAT controller.
- You can use the EtherCAT controller in an EtherCAT system as an EtherCAT MDevice .
- It is connected via the integrated EtherCAT port X5.
- Connect this interface with the RJ45 jack "IN" of your EtherCAT SubDevice station.
- EtherCAT uses Ethernet as transfer medium. Standard CAT5 cables are used. Here distances of about 100m between two stations are possible.
- An EtherCAT network always consists of an EtherCAT MDevice and a various number of EtherCAT SubDevice.
- Each EtherCAT SubDevice has an "IN" and "OUT" RJ45 jack. The arriving EtherCAT cable from the direction of the MDevice is to be connected to the "IN" jack. The "OUT" jack is to be connected to the next station. With the respective last station the "OUT" jack remains free.

(4) Ethernet port X3/X4

These connectors are used to connect devices compatible with Ethernet communications. Connectors X3 and X4 by default are switched together.

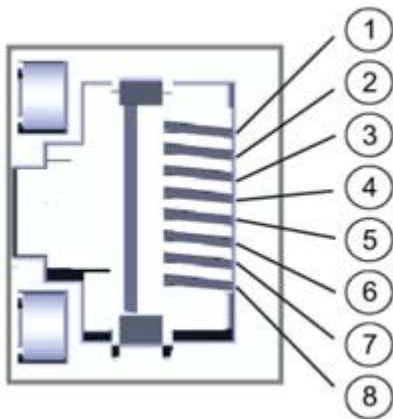


Table 4.2 8pin RJ45 jack:

Pin	Signal	Description
1	DA+	Bidirectional pair A + (send data +)
2	DA-	Bidirectional pair A - (send data -)
3	DB+	Bidirectional pair B + (receive data +)
4	DC+	Bidirectional pair C +
5	DC-	Bidirectional pair C -
6	DB-	Bidirectional pair B - (receive data -)
7	DD+	Bidirectional pair D +
8	DD-	Bidirectional pair D -

- The CPU has an integrated Ethernet communication processor.
- The connection happens via an integrated 2-port switch (X3/X4).
- Via Ethernet (default: 192.168.1.1, [MAC1]) you have access to:
 - Programming / remote maintenance of the CPU.
 - Web-based management WBM of the CPU.
 - OPC UA communication of the CPU.
- In the optionally available [PROFINET IO controller] operating mode, you can connect your PROFINET devices here.
- In the optionally available [PROFINET I-Device] operating mode, you can connect your CPU as I-Device to a PROFINET IO controller here.

(5) SD Card Slot

This SD card slot is used to connect an SD card.

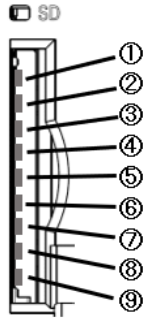


Table 4.3 SD Card Slot Pin Assignments

Pin	Signal	Description
1	DAT3/CS	Data line 3, chip select
2	CMD/DI	Command line, data In
3	VSS1	Ground
4	VDD	Power
5	CLK	Clock
6	VSS2	Ground
7	DAT0/DO	Data line 0, data Out
8	DAT1/IRQ	Data line 1, interrupt request line
9	DAT2/NC	Data line 2, unused



Important

Before removing the SD card, press the SD/STOP switch and wait until the SD card status indicator goes out. If the SD card is removed while the SD card status indicator is lit or flashing, the data may become corrupted.

(6) USB Type-C Connector

This connector is used to connect devices compatible with USB Type-C.

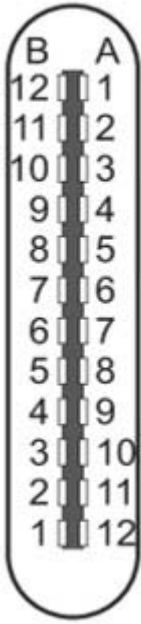


Table 4.4 24pin USB-C jack

Pin No.	Signal	Contents	Pin No.	Signal	Contents
1	GND	Ground	1	GND	Ground
2	TX1+	High speed data path 1 +	2	TX2+	High speed data path 2 +
3	TX1-	High speed data path 1 -	3	TX2-	High speed data path 2 -
4	VBUS	Voltage + 5V	4	VBUS	Voltage + 5V
5	CC1	Control channel 1 for connector orientation	5	CC2	Control channel 1 for connector orientation
6	D+	USB 2.0 data +	6	D+	USB 2.0 data +
7	D-	USB 2.0 data -	7	D-	USB 2.0 data -
8	n.c.	Reserved	8	n.c.	Reserved
9	VBUS	Voltage + 5V	9	VBUS	Voltage + 5V
10	RX2-	High speed data path 2 -	10	RX1-	High speed data path 1 -
11	RX2+	High speed data path 2 +	11	RX1+	High speed data path 1 +
12	GND	Ground	12	GND	Ground

The interface is located under the front flap.

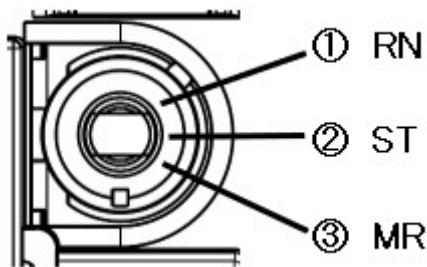
5.1.4 Switches

The iC9226M has the following three switches.

- Operating mode switch: S3
- DIP switch: S1, S2
- Pushbutton switch: S4

(1) Operating Mode Switch: S3

This switch primarily sets the operating mode of the iC9226M.



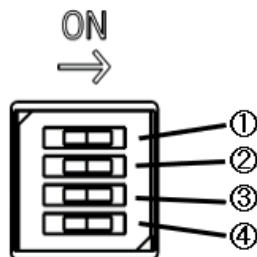
- With the operating mode switch, you can select between the operating modes ST (STOP) and RN (RUN) on the CPU.
- With the button position MR (Memory Reset) you can request a reset of the CPU in different levels. [INSERT LINK]Chap. 4.6 'MRESET and reset to factory settings' page 71

Switch Position: Name	Operating Mode	Default	Description
Top: RN	CPU RUN	RN (RUN)	
Middle: ST	CPU STOP		
Bottom: MR	Clear Memory (Clear normal memory and reset to factory default condition)		

(2) DIP Switch: S1, S2

This switch primarily sets the operating mode of the iC9226M.

The operating mode is judged from the status of the switches when the power is turned ON.



(a) S1 (Top DIP Switch)

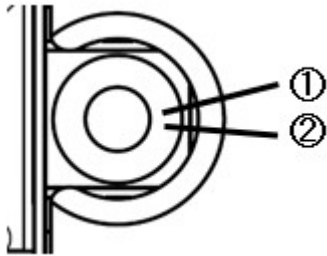
Name	Status	Operating Mode	Default	Remarks
1	OFF	Normal startup	OFF	Software control
	ON	Safe mode startup		
2	OFF	Normal startup	OFF	Software control
	ON	Type 1 reset		
3	OFF	Normal startup	OFF	OFF
	ON	Reserved		
4	OFF	Normal startup	OFF	OFF
	ON	Reserved		

(b) S2 (Bottom DIP Switch)

Name	Status	Operating Mode	Default	Remarks
1	OFF	Normal startup	OFF	Software control
	ON	Enable DHCP, Disable DCP		
2	OFF	Normal startup	OFF	OFF
	ON	Reserved		
3	OFF	Normal startup	OFF	OFF
	ON	Reserved		
4	OFF	Normal startup	OFF	OFF
	ON	Reserved		

(3) Pushbutton switch: S4

For future use.

**5.1.5 Memory****(1) Internal Memory**

The CPU has an integrated memory. You will find information on the memory sizes in the technical data.

The memory is divided into the following parts:

- Working memory for temporary data and parts of the user program.
- Parametrization memory for current firmware and overlay file system with firmware adjustments, user program and data.
- Non-volatile memory for retentive data.

[4.4 Memory Management on page 65](#)

(2) Slot for Yaskawa SD Card

For future use

5.1.6 Buffering Mechanisms

- The iC9200 Series CPU has a capacitor-based mechanism to buffer the internal clock in case of power failure for max. 14 days.
- The retentive data defined during configuration are automatically saved in the non-volatile memory in the event of a power failure.

Specifications


This section provides the installation and operating conditions of the iC9226M-EC. It also provides detailed specifications of the iC9226M-EC .

6.1	iC9226M-EC Installation and Operating Conditions	130
6.1.1	Installation and Operating Conditions	130
6.1.2	Control Panel Cooling Method	130
6.2	Power Supply Section	132
6.3	CPU Module Specifications	133
6.3.1	Hardware Specifications.....	133
6.3.2	Performance Specifications	134
6.3.3	Ethernet Communications Specifications	134

6.1 iC9226M-EC Installation and Operating Conditions

6.1.1 Installation and Operating Conditions

The installation and operating conditions for the iC9226M-EC are given in the following table.

	Item	Specifications
Environmental Conditions	Ambient Operating Temperature	0°C to +60°C (forced-air cooling is required when the temperature exceeds 55°C)
	Ambient Storage Temperature	-25°C to +85°C
	Ambient Operating Humidity	10% to 95% RH (with no condensation)
	Ambient Storage Humidity	10% to 95% RH (with no condensation)
	Pollution Level	Conforms to JIS B 3502 Pollution Degree 2.
	Corrosive Gas	There must be no combustible or corrosive gas.
	Operating Altitude	2000 m max.
Mechanical Operating Conditions	Vibration Resistance	Conforms to JIS B 3502. • Continuous vibration: 5 Hz to 9 Hz with single-amplitude of 1.75 mm 9 Hz to 150 Hz with fixed acceleration of 4.9 m/s ² • Intermittent vibration: 5 Hz to 9 Hz with single-amplitude of 3.5 mm 9 Hz to 150 Hz with fixed acceleration of 9.8 m/s ² 10 sweeps each in X, Y, and Z directions for both intermittent and continuous vibration
	Shock Resistance	Size of shock: Peak acceleration of 147 m/s ² (15 G) Duration: 11 ms 3 times each in X, Y, and Z directions
Electrical Operating Conditions	Noise Resistance	Planned to conform to EN 61000-6-2, EN 61000-6-4, EN 55011 (group 1, class A)
Installation Conditions	Ground	Ground to 100 Ω max.
	Cooling Method	Natural cooling or forced-air cooling Refer to the following section for details.  6.1.2 Control Panel Cooling Method on page 130
	Air Space around Module	10 mm or more space on the left and right sides. 40 mm or more space at the top and bottom.

6.1.2 Control Panel Cooling Method

The components that are used in the iC9226M-EC require the ambient operating temperature to be between 0°C and 60°C. Use one of the methods described below to ensure adequate cooling in the control panel.

(1) Control Panels with Natural Cooling

- Do not mount the iC9226M-EC in a location where air that is heated by devices in the panel (including self-generated heat) stagnates.
- Leave sufficient space above and below the iC9226M-EC, and maintain adequate distances from other devices, cable ducts, and other objects to ensure suitable air circulation.
- Do not mount the controller in any direction other than the specified direction.
- Do not mount the controller on top of any device that generates a significant amount of heat.
- Do not subject the controller to direct sunlight.

(2) Control Panels with Forced-air Cooling

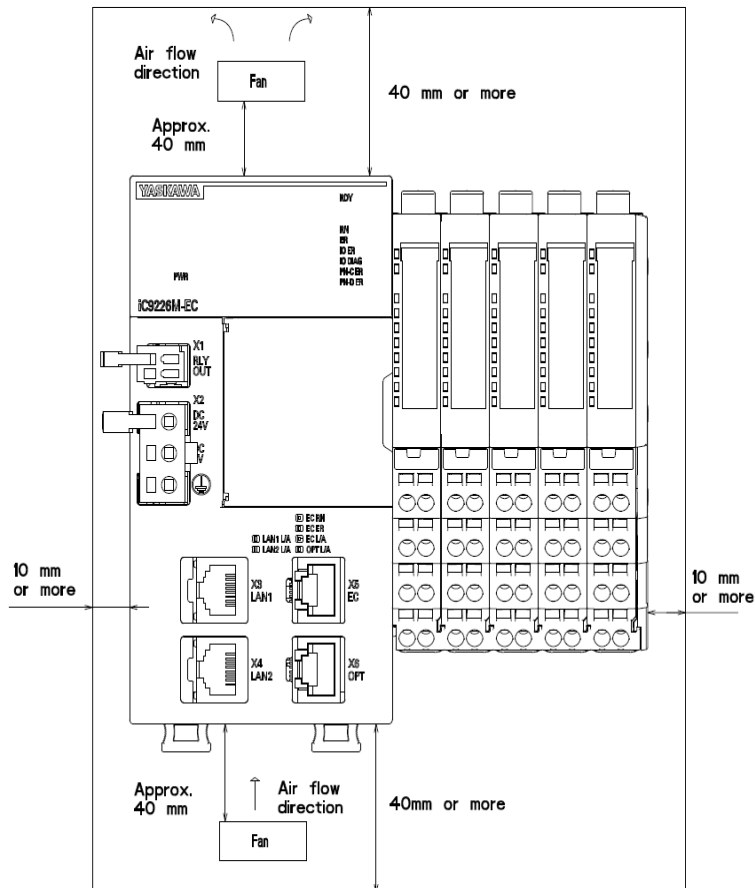
Use one of the following methods to install a fan at the center of the top or bottom of the iC9226M-EC.

- Forced draft method (A fan or a similar device is used to circulate the air in the interior and the exterior of the panel.)
- Forced circulation method (A fan or a similar device is mounted to the airtight panel to circulate the air inside.)





Important

1. Use the following guideline when selecting the fan.
80 mm × 80 mm or larger, maximum air flow 0.9 m³/min, maximum static pressure 26.5 Pa or higher
2. The installation locations and air flow directions for the fan are shown in the following figure.



6.2 Power Supply Section

The specifications of the power supply unit are given in the following table.

Item	Specifications	
Input Voltage	24 VDC	
Allowable Input Voltage Range	20.4 VDC to 28.8 VDC	
Allowable Frequency Range	–	
Allowable Distortion in Input Waveform	–	
Input Current	5.0 A max. (at rated input/output)	
Inrush Current ^{*1}	10 A, 0.1 ms max.	
Overvoltage category	II	
Allowable Power Loss Time	10 ms max.	
Rated Voltage ^{*2}	5 V	
Rated Current ^{*2}	3 A	
Withstand Voltage ^{*3}	500 VAC between group of power supply input terminals and FG terminal for 1 min	
Insulation Resistance ^{*3}	100 MΩ or higher between group of power supply input terminals and FG terminal (with 500-VDC insulation resistance tester)	
Status Output	NO contact relay output synchronized with the status of the CPU module	
	<ul style="list-style-type: none"> • Normal operation: Circuit closed. • Error: Circuit open. 	
	Contact Ratings	
	Input Voltage	Current Capacity
	24 VDC	0.5 A (resistive load)
		0.25 A (inductive load)
Indicators	POWER Refer to the following section for details.  (a) POWER LED on page 115	
Connectors	<ul style="list-style-type: none"> • POWER: Power supply connector • RLY OUT: Relay contact connector • Unit connector Refer to the following section for details.  5.1.3 Connectors on page 120	

*1 These numeric values are for a cold start at room temperature.

*2 Output characteristics of the power supplied from the SLIO I/O series module. Refer to the product manual of each SLIO I/O series module for its power consumption.




*3 The iC9226M-EC (model number: JEYRM-MPX02210L32-□) is not isolated between the primary DC power supply and the secondary DC power supply. Therefore, there are no specifications for withstand voltage and insulation resistance between the primary power supply and the secondary power supply.

6.3 CPU Module Specifications

This section provides the hardware, performance, and functionality specifications of the CPU section.

6.3.1 Hardware Specifications

The hardware specifications of the CPU module are given in the following table.

Item	Specifications
Calendar	Timer for seconds to years and days of the week (data is retained for about 14 days after the power is turned OFF)
Ethernet	10Base-T, 100Base-TX, or 1000BASE-T 2 ports
SD Card	<ul style="list-style-type: none"> For future use
Indicators	<ul style="list-style-type: none"> Seven-segment display Status Indicators SD Card Status Indicators Ethernet Status Indicators Refer to the following section for details.  5.1.2 Display and Indicators on page 113
Switches	<ul style="list-style-type: none"> Mode Switch: S3 DIP switch: S1, S2 Pushbutton switch: S4 Refer to the following section for details.  5.1.4 Switches on page 125
Connectors	<ul style="list-style-type: none"> EtherCAT Connector Ethernet Connectors SD Card Slot Refer to the following section for details.  5.1.3 Connectors on page 120

6.3.2 Performance Specifications

The performance specifications of the CPU module are given in the following table.

Item		Specifications	Remarks
System Configuration	Maximum Number of Racks	1	–
	Maximum Number of Local SliceBus Modules Controllable by the CPU Module	64	–

6.3.3 Ethernet Communications Specifications

The specifications of the Ethernet communications that is built into the CPU module are given in the following table.

Item		Specifications	Remarks
Common Items	Communications Interface	10Base-T/100Base-TX	–
	Number of Communications Ports (Connectors)	2	–
	Communications Protocols	TCP/UDP/IP/ARP/ICMP/GMP	–
Ethernet Communications	Maximum Number of Communications Connections	20	–
	Maximum Number of Communications Channels	20	–
	Automatic Reception	Supported.	–
	Automatic Transmission	Supported.	–

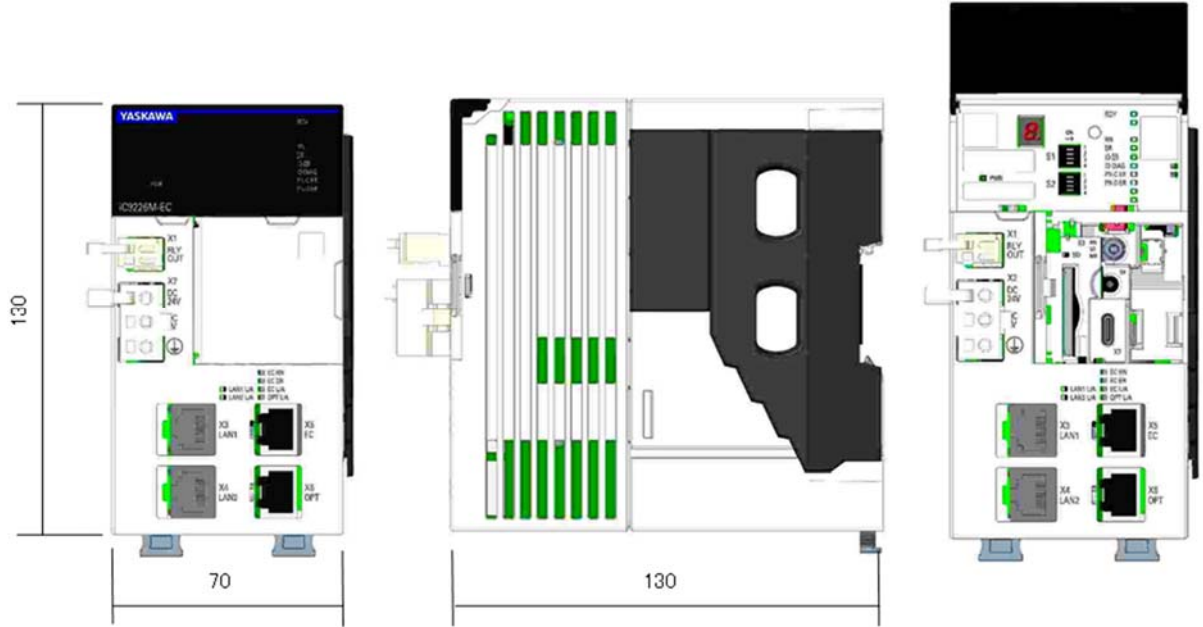
External Dimensions

This chapter gives the appearance and external dimensions of the iC9226M-EC.
Refer to the relevant user's manuals for the appearance and external dimensions of option modules.

7.1	iC9200	136
	7.1.1 iC9226M-EC	136

7.1 iC9200

7.1.1 iC9226M-EC



Revision History

The date of publication, revision code, revision number, and web revision number are given at the bottom right of the back cover. Refer to the following example.

MANUAL NO. SIEP C880901 00A <0>-0
Published in Japan March 2024

Revision number
Revision code Web revision number
Date of publication

Date of Publication	Rev. Code	Rev. No.	Web Rev. No.	Section	Revised Contents
September 2024	A	<0>	0	–	First edition

iC9000 Series iC9200 Product Manual

IRUMA BUSINESS CENTER (SOLUTION CENTER)

480, Kamifujisawa, Iruma, Saitama, 358-8555, Japan
Phone: +81-4-2962-5151 Fax: +81-4-2962-6138
www.yaskawa.co.jp

YASKAWA AMERICA, INC.

2121, Norman Drive South, Waukegan, IL 60085, U.S.A.
Phone: +1-800-YASKAWA (927-5292) or +1-847-887-7000 Fax: +1-847-887-7310
www.yaskawa.com

YASKAWA ELÉTRICO DO BRASIL LTDA.

777, Avenida Piraporinha, Diadema, São Paulo, 09950-000, Brasil
Phone: +55-11-3585-1100 Fax: +55-11-3585-1187
www.yaskawa.com.br

YASKAWA EUROPE GmbH

Philipp-Reis-Str. 6, 65795 Hattersheim am Main, Germany
Phone: +49-6196-569-300 Fax: +49-6196-569-398
www.yaskawa.eu.com E-mail: info@yaskawa.eu.com

YASKAWA ELECTRIC UK LTD.

1 Hunt Hill Cumbernauld G68 9LF, UK
Phone: +44-1236-806000 Fax: +44-1236-458182

YASKAWA ELECTRIC KOREA CORPORATION

6F, 112, LS-ro, Dongan-gu, Anyang-si, Gyeonggi-do, Korea
Phone: +82-31-8015-4224 Fax: +82-31-8015-5034
www.yaskawa.co.kr

YASKAWA ASIA PACIFIC PTE. LTD.

30A, Kallang Place, #06-01, 339213, Singapore
Phone: +65-6282-3003 Fax: +65-6289-3003
www.yaskawa.com.sg

YASKAWA ELECTRIC (THAILAND) CO., LTD.

59, 1F-5F, Flourish Building, Soi Ratchadapisek 18, Ratchadapisek Road, Huaykwang, Bangkok, 10310, Thailand
Phone: +66-2-017-0099 Fax: +66-2-017-0799
www.yaskawa.co.th

YASKAWA ELECTRIC (CHINA) CO., LTD.

22F, Link Square 1, No.222, Hubin Road, Shanghai, 200021, China
Phone: +86-21-5385-2200 Fax: +86-21-5385-3299
www.yaskawa.com.cn

YASKAWA ELECTRIC (CHINA) CO., LTD. BEIJING OFFICE

Room 1011, Tower W3 Oriental Plaza, No.1, East Chang An Avenue,
Dong Cheng District, Beijing, 100738, China
Phone: +86-10-8518-4086 Fax: +86-10-8518-4082

YASKAWA ELECTRIC TAIWAN CORPORATION

12F, No. 207, Section 3, Beishin Road, Shindian District, New Taipei City 23143, Taiwan
Phone: +886-2-8913-1333 Fax: +886-2-8913-1513 or +886-2-8913-1519
www.yaskawa.com.tw

YASKAWA

YASKAWA ELECTRIC CORPORATION

In the event that the end user of this product is to be the military and said product is to be employed in any weapons systems or the manufacture thereof, the export will fall under the relevant regulations as stipulated in the Foreign Exchange and Foreign Trade Regulations. Therefore, be sure to follow all procedures and submit all relevant documentation according to any and all rules, regulations and laws that may apply. Specifications are subject to change without notice for ongoing product modifications and improvements.

© 2024 YASKAWA ELECTRIC CORPORATION

MANUAL NO. SIEP C880901 00A <0>-0

Published in Japan September 2024

24-5

Original instructions