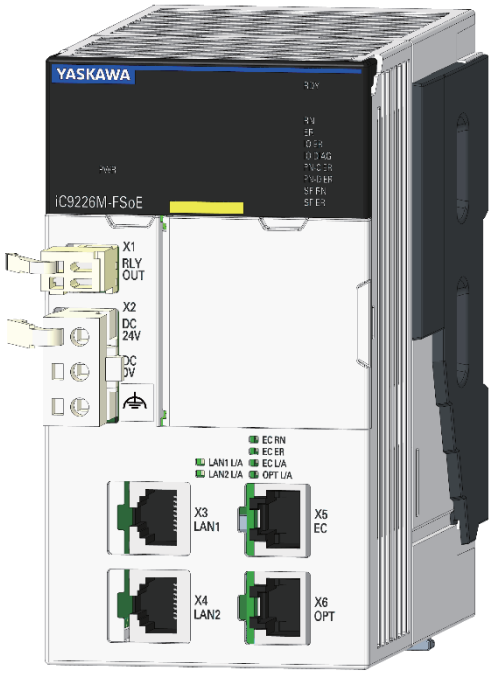
YASKAWA

iC9000 Series

iC9200

Safety Manual

Model: JEYRM-MPX022SE10L32-2



MANUAL NO. SIEP C880901 02A

Table of Contents

1

General

1.1 Copyright © YASKAWA Electric Corporation

1.1.1 All Rights Reserved

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® and Safety over EtherCAT® are registered trademarks and patented technologies,

licensed by Beckhoff Automation GmbH, Germany.

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

1.2.1 Objective and Contents

The manual describes the iC9226M-FSoE of the iC9200

Series.

- It describes the structure, configuration and application.
- The manual is targeted at users who have a background in automation technology.
- The manual consists of chapters. Each chapter describes a completed topic. For guidance, the manual provides:
  - An overall table of contents at the beginning of the manual.
  - References with pages numbers.
- When using the product, please refer to the latest manual and check that the product version is covered in the table below.

Table 1.1 Validity of the documentation

Product	Model Number	As of version:	
iC9226M-FSoE	JEYRM-MPX022SE10L32-2	HW: A03	FW: V2023.9 or higher

1.2.2 Icons Headings

Important passages in the text are highlighted by following icons and headings:

DANGER

Immediate danger to life and limb of personnel and others.
Non-compliance will cause death or serious injury.

WARNING

Hazardous situation to life and limb of personnel and others.
Non-compliance may cause death or serious injury.

CAUTION

Hazardous situation to life and limb of personnel and others. Non-compliance may cause slight injuries.
This symbol is also used as warning of damages to property.

NOTICE

Designates a possibly harmful situation. Non-compliance can damage the product or something in its environment.

Information Supplementary information and useful tips.

1.2.3 Liability Limitation

All data and notes in these instructions were prepared with consideration to the statutory standards and regulations, the present state of technology, as well as our many years of knowledge and experience.

The manufacturer accepts no liability for damage caused because:

- Non-compliance with the instructions
- Non-specified use
- Use of untrained personnel

The actual scope of delivery can, by special designs, deviate from the explanations and presentations given here, because of the utilization of additional order options, or because of the most recent technical changes.

The user is responsible for the execution of service and commissioning according to the safety instructions of the prevailing standards and other relevant national and local instructions concerning conductor dimensioning and protection, earthing, disconnector, overcurrent protection and so on.

For damages, which result from the mounting or from the connection, the one is liable, who has carried out the mounting or the installation.

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual are reviewed regularly. Necessary corrections are included in subsequent editions.

Suggestions for improvement are welcomed.

For damage, which results from missing or insufficient knowledge of the manual, any liability of the manufacturer is impossible.

Therefore, the operator is recommended to have the instruction of the persons concerned confirmed in writing.

Modifications or functional alternations on the product are not allowed due to safety reasons. Any modification on the product not explicitly authorized by the manufacturer will result in loss of any liability claims to the vendor. The same applies if non authorized parts or equipment are used.

1.2.4 Copyright

This manual is to be treated confidentially. It has been provided only for the personnel, which use the product. The transfer of this document to third parties without the authorization in writing of the vendor is prohibited.

Information

1.2.5 Use of This Manual

This safety manual contains information for the intended use of the iC9200 Series CPUs.

Knowledge of regulations and the proper technical implementation of the safety instructions detailed in this manual performed by qualified personnel are prerequisites for safely planning, engineering, programming, installing and starting up the iC9200 Series CPUs as well as for ensuring safety during their operation and maintenance.
1.8 Education of the Personnel on page 23

Yaskawa will not be held liable for severe personal injuries, damage to property or the surroundings caused by any of the following: unqualified personnel working on or with the devices, de-activation or bypassing of safety functions, or failure to comply with the instructions detailed in this manual.

The safety components and systems have been developed, manufactured and tested in compliance with the pertinent safety standards and regulations. They may only be used for the intended applications under the specified environmental conditions.

They must be used only as specified in environmental descriptions and be connected only to approved external devices.

The manual contains safety instructions, description of the modules and information about life cycle.

1.2.6 Applicable Documentation

In the safety CPUs components of other manufacturers are possibly integrated. For these purchased parts of the respective manufacturers risk evaluations were carried out. The conformity of the constructions to the valid European and national regulations was declared by the according manufacturer.

1.2.7 Warranty Conditions

The warranty conditions can be found in the "General terms and conditions" at www.yaskawa-global.com.

1.3 Safety Instructions

1.3.1 Intended Use

⚠ WARNING

Danger by non intended use!

Any other use beyond the intended use and/or other use of this product can lead to dangerous situations and is prohibited.

The CPU iC9226M-FSoE is constructed and produced for:

- industrial use.
- general control and automation tasks.
- industrial network communication, machine and process control.
- the connection to EtherCAT and PROFINET (optional).
- operation within the environmental conditions specified in the technical data.
- operation in a control cabinet with a degree of protection of IP 54 or better.

⚠ DANGER

This device is not certified for applications:

- **in explosive environments (EX-zone)**

1.3.2 Documentation

The manual must be available for:

- Project design department
- Installation department
- Commissioning
- Operation

⚠ CAUTION

The following conditions must be met before using or commissioning the components described in this manual:

- **Changes to the automation system may only be made when the power supply is disconnected!**
- **Installation and hardware modifications only by properly trained personnel.**
- **The national rules and regulations of the respective country must be satisfied (installation, safety, EMC ...)**

1.3.3 Maintenance

If you keep the prescribed environmental conditions the CPU is maintenance-free.

1.17 Approvals, Directives, Standards on page 34

1.3.4 Spare Parts

Please only use original spare parts of Yaskawa.

⚠ WARNING

Incorrect or faulty spare parts can cause damage, malfunction or failure as well as affect safety.

1.3.5 Shipping

For shipping always use the original packaging.

1.3.6 Disposal

National rules and regulations apply to the disposal of the device!

1.3.7 Residual Risks

⚠ WARNING

The CPU iC9226M-FSoE was developed as an assembly for functional safety in accordance with the procedure described in the relevant standards. The necessary risk reduction was implemented in the design and the corresponding warnings and requirements for the user are described in this manual. Please note that even with these measures, there is still a small residual risk to life and health of persons and take this into account as part of the risk evaluation for the plant/machine in which the CPU iC9226M-FSoE is used.

1.4 Safety Information for Users

1.4.1 Handling of Electrostatic Sensitive Modules

The modules make use of highly integrated components in MOS-Technology. These components are extremely sensitive to over-voltages that can occur during electrostatic discharges. The following symbol is attached to modules that can be destroyed by electrostatic discharges.

The Symbol is located on the module, the module rack or on packing material and it indicates the presence of electrostatic sensitive equipment. It is possible that electrostatic sensitive equipment is destroyed by energies and voltages that are far less than the human threshold of perception. These voltages can occur where persons do not discharge themselves before handling electrostatic sensitive modules and they can damage components thereby, causing the module to become inoperable or unusable. Modules that have been damaged by electrostatic discharges can fail after a temperature change, mechanical shock or changes in the electrical load. Only the consequent implementation of protection devices and meticulous attention to the applicable rules and regulations for handling the respective equipment can prevent failures of electrostatic sensitive modules.

1.4.2 Measurements and Alterations on Electrostatic Sensitive Modules

When you are conducting measurements on electrostatic sensitive modules you should take the following precautions:

- Floating instruments must be discharged before use.
- Instruments must be grounded.

⚠ CAUTION

Personnel and instruments should be grounded when working on electrostatic sensitive modules.

1.5 Intended Use

1.5.1 General

The product is exclusively designed and constructed for the intended use described in this manual. The product is intended used if all the notes and information of this manual are considered.

⚠ WARNING

Danger by not intended use!

Each use of the product, which differs to the intended use can lead to dangerous situations.

Therefore

- Use the product only intended.
- Use the product only together with the recommended components.
- Consider all the data in this manual.
- Ensure that only qualified personnel work with/at the product. *1.8 Education of the Personnel on page 23*
- Ensure during configuration that the product is operated within its specifications.
- Ensure that the power supply corresponds to the given specifications.
- Only use the product in a technically perfect condition.
- Only use the product in combination with approved components.
- Only use the product in an area of second type (industrial area). The product was developed such as this fulfils the requirements of the category C3. For operation an approved power supply (SELV/PELV) is necessary. Here With the usage of the product in an area of first type, category C2/C1 (living-, business and trade without an interstage transformer directly at a public low-voltage-system) the cabinet builder has to reduce the emission (conducted and radiated) by special measure steps, which are to be demonstrated, since it can come without any additional measures to EMC disturbances. Whether a product described here reaches category C2/C1 with additional measures, cannot be ensured.

1.5.2 Changes and Modifications at the Product

To avoid endangerments and to ensure the optimal power neither changes nor modifications may be made at the product, which are not specially approved by the manufacturer.

1.6 Responsibility of the User

1.6.1 General

The product is used in the commercial range. The user of the product is subject of the statutory duties to work safety. In addition to the safety instructions in this manual, for the usage environment of the product valid safety, accident prevention and environmental protection regulations must be adhered.

- The user must be informed about the valid industrial safety regulations and determine in an endangerment evaluation additionally dangers, which arise as a result of the special conditions for the product on the place of operation. This is to be transcribed with working instructions for the operation of the product.
- These working instructions must be kept in direct environment of the product and accessible at any time for people, which work with the product.
- The working instructions must fully be adhered.
- The product is only to be operated in a technically flawless condition.

1.7 Protective Devices

1.7.1 Degree of Protection

The place of installation of the CPU must comply for devices according to IP20.

⚠ WARNING

Serious dangers for the user and/or damage to property can result from improper or non-intended use and manipulation of the CPU.

Improper use may lead to serious danger.

NOTICE

The IP20 (IEC 60529/EN 60529) protection class of the CPU is intended for a clean and dry environment.

- **Do not subject the CPU to mechanical and/or thermal stress that exceeds the limits described.**
- **Please note that you must install the CPU in a lockable housing or a lockable control cabinet with at least protection class IP54 for proper operation.**

Incorrect use may lead to property damage.

1.7.2 Notes on Security

NOTICE

There is a risk of manipulation of the CPU through unauthorized physical access.

- **Protect your system from unauthorized physical access. Use a lockable control cabinet, for example.**

Unauthorized deletion/replacement of the safety-related project is possible.

- **Only provide the roles for user authentication “Admin”, “Commissioner”, and “Engineer” to those users who are authorized to program the safety-related control. Otherwise, the unauthorized exchange or deletion of the safety-related project by the user cannot be ruled out. You can set user roles in the web-based management. *5.5.5 User Authentication on page 214***
- **It is imperative that you install the CPU and the modules in a row in a lockable housing or a lockable control cabinet. The device housing is not protected against manipulation and access to the CPU cannot be validated. Access to the SD card is possible so that data can be read and manipulated. We recommend protecting the slot of the parametrization memory (SD card) on the CPU against manipulation with a seal.**

1.8 Education of the Personnel

⚠ WARNING

Risk of injury resulting from insufficient qualification!
Improper use can cause considerable personal injury and material damage.

Therefore: The special activities may only be executed by personnel nominated by the respective chapters.

1.8.1 Qualification

In the manual the following qualifications for different activities are defined:

(1) Operating Personnel

The automation system may only be operated by persons, which are trained, instructed and authorized. Troubleshooting, maintenance, cleaning, maintenance and replacement must be performed only by skilled or trained personnel. These persons have to know the instruction manual and have to act accordingly. Commissioning and training should only be performed by qualified personnel.

(2) Qualified Personnel

These are electrical engineers and electricians of the customer or third party, which are authorized by the manufacturer and which have learned installation and commissioning by the manufacturer and are allowed to ground, mark and install electrical circuits and devices in accordance to the standard safety technology. Qualified personnel is trained and instructed according to the corresponding valid standards in safety technology in the care and use of appropriate safety equipment.

1.9 Personal Protective Equipment

1.9.1 General

During work, the wearing of personal protective equipment is needed to minimize health hazards.

- Always wear the necessary protective equipment for the corresponding job.
- For your own safety regard the signs, which are in your work space.

1.9.2 Work Clothing

is close-fitting clothing with low tensile strength, with tight sleeves and without a protruding part. Depending on the application it should be prevented, that the carrier gets serious injured or is exposed to health risk during work. For reasons of injury no jewellery like rings and chains should be worn.

1.9.3 Protective Helmet

for protection against falling and flying objects.

1.9.4 Safety Shoes

for protection against falling heavy objects.

1.9.5 Protective Gloves

to protect hands from friction abrasions, punctures or injuries, as well as from contact with hot objects.

1.9.6 Wear at Special Works: Eye Protector

to protect eyes from flying parts and liquid splashes.

1.10 Special Hazards

1.10.1 General

In the following section the residual risks are listed. Regard the listed safety warnings here and the notes in the whole manual to reduce health hazards and to avoid dangerous situations.

1.10.2 Electric Current

⚠ DANGER

Risk of death by electric current!

Contact with live parts is immediate danger to life. Damage of the insulation or of components can be danger to life.

Therefore: Immediately turn off the power supply when the insulation is damaged. Work on the electrical system only by qualified personnel. Always power-off and secure the electrical system during the work on it.

1.10.3 Risk by Residual Energy

⚠ DANGER

Risk of death by electric current!

After disconnecting a device from main voltage, parts such as power connections should only be touched when the capacitors are discharged in the device.

Therefore: Regard discharge time of the capacitors, do not touch live parts before. Regard corresponding instructions on the device. If you have connected additional capacitors on the link, the discharge of the link can last considerably longer. In this case you have to determine the required waiting period or even to measure whether the device is free of voltage.

1.10.4 Moved Objects

⚠ WARNING

Risk of injury from moving parts!

Rotary respectively linear moved parts can cause serious injuries.

Therefore: Do not touch moving parts during operation. Do not open the cover during operation. The mechanical residual energy depends on the application. Driven components rotate respectively move for a certain time even after switching off the power supply. Here serve for suited safety devices.

1.11 Fire Fighting

⚠ DANGER

Risk of death by electric current!
Risk of an electrical shock when using a conducting fire fighting medium.

Therefore use the following fire fighting medium:
ABC powder / CO2

1.12 Electrical Safety

1.12.1 General

The safety CPU is designed according to IEC61131-2 for degree of pollution 2. This means only non-conductive pollution may occur during operation. Temporary conductivity by condensation is only allowed when the module is out of operation.

⚠ WARNING

Risk of injury from conductive pollution!

During the operation there is no conductive pollution allowed.

Therefore: Before the system is installed check and guarantee if necessary by additional measures that the degree of pollution 2 is not exceeded (e.g. installation in a cubicle with degree of protection IP54 or better).

1.12.2 Installation and Configuration

⚠ WARNING

Incorrect installation and retrofitting can pose serious risks

- **Devices and their installations in the system must be designed according to these requirements.**
- **Existing plants and systems that are retrofitted must also be checked in this regard.**

1.12.3 Note on Power Supply

⚠ WARNING

Risk of injury by electric current!

Only devices with safe insulation from the 230V mains may be connected to the CPU. The power supply for generating the 24V power must correspond to the requirements for PELV/ SELV according to EN 50178.

Hazardous shock currents and the loss of functional safety

Disregarding instructions for electrical safety may result in hazardous shock currents and the loss of functional safety.

In order to ensure electrical safety, please observe the following points:

- **Direct/indirect contact**
- **Safe isolation**

1.12.4 Direct/Indirect Contact

Ensure protection against direct and indirect contact in accordance with VDE 0100 Part 410 (IEC 60364-4-41) for all components connected to the system. In the event of a fault, parasitic voltages must not occur (single fault safety). This also applies to devices and components with dangerous touch voltages that are permanently connected to network and/or diagnostic interfaces of the devices used.

1.12.5 Safe Isolation

Only use units with safe isolation if dangerous contact voltages can occur at their connections during normal operation or as a result of an insulation error.

1.13 Safety Facilities

⚠ WARNING

Risk of death by non-functioning safety facilities!

Safety facilities serve for maximum safety during operation. Even if by safety facilities working process become complicated, its never allowed to circumvent them. The safety is guaranteed only when the safety facilities are intact.

Therefore: Before beginning the work check whether the safety facilities are installed properly and functional.

1.14 Behavior with Dangers and Accidents

1.14.1 Preventive Measures

- Always be prepared for accidents or fire!
- First-aid equipment (first aid kit, blankets etc.) and keep fire extinguisher handy.
- Make Personal with accident message, first-aid and rescue mechanisms familiar.

1.14.2 In Case of Emergency: Act Correctly

- Set immediately the device with emergency stop out of operation.
- Initiate first-aid measures.
- Rescue persons from the danger zone.
- Inform responsible on-site.
- Alarm medical and / or fire department.
- Make free the access routes for emergency vehicles.

1.15 Sign-Posting

⚠ WARNING

Danger of injury by illegible symbols

In course of time stickers and symbols on the devices can get dirty or otherwise become unrecognizable.

Therefore: Please hold all the safety warnings and operation instructions on the device in always well readable condition.

1.15.1 Signs

The following symbols and signs are in the work space. They refer to the direct environment in which they are attached.

(1) Electrical Voltage

In such marked workspace only qualified personnel may work. Unauthorized may not touch the marked equipment.

⚠ DANGER

Danger of life by electrical power!

Time for discharge > 1 Minute

Stored electrical charge

Therefore: Consider discharge time of capacitor and do not touch live parts before. Consider appropriate instructions on the device. If you have connected additional capacitors at DC, the discharge of the DC link can last longer. In this case you have to determine respectively to measure the required waiting time whether the device is free of voltage.

(2) Functional Earthing

To improve noise immunity, the terminals marked with this symbol should be functionally earthing.

(3) Refer to instruction manual/booklet

See the operating instructions/product manual before starting work on equipment marked with this symbol or operating the equipment.
Ensure that you refer in particular to the "Safety Precaution".

1.16 Safety Hints

The CPU represents the current state of the art and fulfill the valid safety regulations and the appropriate harmonized, European standards (EN)

For the user additionally is valid the:

- relevant rules for the prevention of accidents
- EC directives or other country-specific regulations
- generally accepted safety rules
- general ESD regulations

Disturbances of any kind or other damage must be reported to a responsible person. Protective and safety equipment must not be circumvented or bypassed. Dismounted protective equipment must be mounted and functionally tested before a restart. The modules are to be secured against misuse or accidental use. Original mounted signs, labels, stickers are to be always considered and be held in a readable condition.

1.17 Approvals, Directives, Standards

Conformity and approval		
Conformity		
CE	2014/30/EU	EMC Directive
	2006/42/EC	Machinery Directive
RoHS (EU)	2011/65/EU	Restriction of the use of certain hazardous substances
UKCA	2016 No. 1091	Electromagnetic Compatibility Regulations
	2008 No. 1597	Supply of Machinery (Safety) Regulation
RoHS (UK)	2012 No. 3032	Use of Certain Hazardous Substances

Protection of persons and device protection		
Type of protection	-	IP20
Electrical isolation		
to the field bus	-	electrically isolated
to the process level	-	electrically isolated
Insulation resistance	EN 61131-2	-
Insulation voltage to reference earth		
Inputs / outputs	-	DC 24V, test voltage AC 500V
Protective measures	-	against short circuit

Environmental conditions to EN 61131-2		
Climatic		
Storage / transport	EN 60068-2-14	-40…+70°C
Operation		
Horizontal installation hanging	EN 61131-2	0…+60°C
Air humidity	EN 60068-2-30	RH1 (without condensation, rel. humidity 10…95%)
Pollution	EN 61131-2	Degree of pollution 2
Installation altitude max.	-	2000m
Mechanical		
Oscillation	EN 60068-2-6	1g, 9Hz ... 150Hz
Shock	EN 60068-2-27	15g, 11ms

Mounting conditions		
Mounting place	-	In the control cabinet (IP54 or better)

EMC	Standard		Comment
Emitted interference	EN 61000-6-4		Class A (Industrial area)
Noise immunity zone B	EN 61000-6-2		Industrial area
		EN 61000-4-2	ESD 8kV at air discharge (degree of severity 3), 4kV at contact discharge (degree of severity 2),
		EN 61000-4-3	HF field immunity (casing) 80MHz … 1000MHz, 10V/m 1.4GHz ... 6.0GHz, 3V/m
		EN 61000-4-6	HF conducted 150kHz … 80MHz, 10V
		EN 61000-4-4	Burst, degree of severity 3
		EN 61000-4-5	Surge, degree of severity 2[1]

1) Due to the high-energetic single pulses with Surge an appropriate external protective circuit with lightning protection elements like conductors for lightning and over-voltage is necessary.

Example of lightning protection conductors			
Application	**Vendor**	**Article**	**Description**
Feed	Dehn	BLITZDUCTOR VT BVT AVD 24	External Lightning protection (DC24V/10A)
Digital inputs, test pulse outputs	Dehn	DEHNconnect RK DCO RK ME 24	External Lightning protection (DC24V/0.5A)
Digital outputs	Dehn	DEHNconnect RK DCO RK D 5 24	External Lightning protection (DC24V/10A)
EtherCAT interface	Dehn	DEHNpatch DPA M CLE RJ45B 48	External Lightning protection (RJ45/48V)

Norms and standards	
DIN EN 61508 part 1-7	Functional safety of electrical/electronic/programmable electronic safety-related systems
DIN EN ISO 13849-1	Safety of machinery: Safety-related parts of control systems
DIN EN 61784-3	Functional safety field buses - General rules and profile definitions
DIN EN 60204-1	Electrical equipment of machines
DIN EN 61131-2	Programmable logic controllers, part 2: Equipment requirements and tests
DIN EN 61000-4-11	Mains voltage variation
Row SN 29500	Failure rate, component, expected value, reliability
DIN EN 61496-1	Electro sensitive protective equipment

Requirements to clearance / creep-age current distances and system power supply	
DIN EN 61131-2	The definition of clearance and creep-age current distances takes place in accordance to EN 61131-2. For the safe field bus coupler over-voltage category 2 and degree of pollution 2 are basis.
DIN EN 13849	The acceptance of error exclusions for short-circuits between neighboring conductor or for short-circuits between neighboring components must be avoided as far as possible by suitable circuit and layout measures. If an error exclusion is inevitable, measures are to be used in accordance with EN 13849 part of 2.
DIN EN 50178	The device is developed for operation on 24V power supplies, which correspond to the PELV-/SELV regulations in accordance to EN 50178.
DIN EN 61508	The normative requirements of the 61508 (increased EMC requirements and requirements concerning isolation) are to be fulfilled also for the common voltage circuit of the SLIO system.

Continued on next page.

Continued from previous page.

Requirements to clearance / creep-age current distances and system power supply	
DIN EN 50178	So that the electrical values for extra-low voltage with safe separation cannot be exceeded on the safe field bus coupler, for the system 24V power supplies are exclusively used, which correspond to the PELV /SELV regulations in accordance with EN 50178.
	In order to protect the safe field bus couplers against over-voltage, a suitable over-voltage protection is provided.
DIN EN 60204-1	The 24V power supply must keep the voltage interrupt according to EN 60204-1.

Requirements for environmental and EMC testing	
DIN EN 61131-2	Programmable logic controllers, part 2: Equipment requirements and tests
DIN EN 61326-3-1:2017	For higher EMC immunity tests

1.18 Use in Difficult Operating Conditions

Information

Without additional protective measures, the products must not be used in locations with difficult operating conditions; e. g. due to:

- dust generation
- chemically active substances (corrosive vapors or gases)
- strong electric or magnetic fields

2

Basics and Mounting

2.1 Safety Notes for the User

⚠ DANGER

Safety instructions

Observe the following safety instructions! Disregarding these safety regulations may result in death, serious personal injury or damage to equipment.

- **Personal and property protection are only guaranteed if the CPU is used in accordance with its intended use.**
- **Observe the safety regulations of electrical engineering and the employer's liability insurance association!**
- **Only perform work on the CPU when the power is switched off!**
- **The CPU may only be installed by qualified personnel in accordance with the specifications in the corresponding documentation.**
- **Electrical work may only be performed by qualified electricians.**
- **The CPU may only be commissioned by a person responsible for the safety of the system. Only this person may connect the supply voltage.**
- **Observe the necessary precautions when handling electrostatically sensitive components (EN 61340-5-1, IEC 61340-5-1)!**
- **Repairs to the CPU, particularly the opening of the housing, must only be performed by the manufacturer.**
- **Keep the operating instructions!**
- **The operator of the CPU or plant is subject to the legal obligations regarding safety at work. The Machinery Directive must therefore be taken into account.**

Protection against dangerous voltages

- **When using the CPU, the user must be protected from touching hazardous voltage.**
- **You must therefore create an insulation concept for your system that includes safe separation of the potential areas of ELV and hazardous voltage.**
- **Here, observe the insulation voltages between the potential areas specified for the modules and take suitable measures, such as using PELV/SELV power supplies for the modules.**

Information **Safety instructions for starting applications**

When configuring the start conditions for your plant, take into account:

- The machine or plant may only be started when it has been ensured that no one is in the danger zone.
- Comply with the requirements of EN ISO 13849-1 with regard to the manual reset function. In this way, no machine movement may be initiated and or dangerous situations may be caused, caused by e.g.:
  - Switching on devices
  - Acknowledgement of device error messages
  - Acknowledgement of block error messages in the application
  - Removal of start-up barriers

Please also consider these instructions in order to exclude an unexpected machine start after acknowledgement with an "Operator Acknowledgement"!

2.1.1 Handling and Transport

(1) Handling of Electrostatic Sensitive Modules

NOTICE

The CPU contains components that can be damaged or destroyed by electrostatic discharge.

- **When handling the CPU, observe the necessary safety measures against electrostatic discharge (ESD) in accordance with EN 61340-5-1 and IEC 61340-5-1.**

The modules are equipped with highly integrated components in MOS technology. These components are highly sensitive to over-voltages that occur, e.g. with electrostatic discharge. The following symbol is used to identify these hazardous modules:

The symbol is located on modules, module racks or on packaging and thus indicates electrostatic sensitive modules. Electrostatic sensitive modules can be destroyed by energies and voltages that are far below the limits of human perception. If a person who is not electrically discharged handles electrostatic sensitive modules, voltages can occur and damage components and thus impair the functionality of the modules or render the modules unusable. Modules damaged in this way are in most cases not immediately recognized as faulty. The error can only appear after a long period of operation. Components damaged by static discharge can show temporary faults when exposed to temperature changes, vibrations or load changes. Only the consistent use of protective devices and responsible observance of the handling rules can effectively prevent malfunctions and failures on electrostatic sensitive modules.

(2) Shipping of Modules

Please always use the original packaging for shipping.

NOTICE

If you do not follow the ESD instructions when unpacking and packing, damage to the CPU may occur.

- **Please note the ESD instructions when unpacking and packing the CPU.**

(3) Measurement and Modification of Electrostatic Sensitive Modules

For measurements on electrostatic sensitive modules the following must be observed:

- Floating measuring instruments must be discharged before use.
- Measuring instruments used must be grounded.

When modifying electrostatic sensitive modules, ensure that a grounded soldering iron is used.

⚠ CAUTION

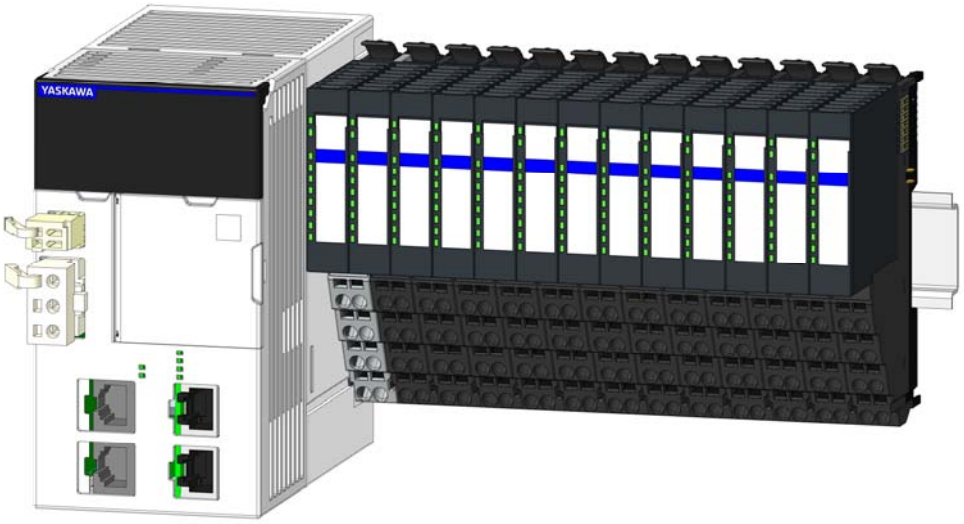
When working with and on electrostatic sensitive modules, make sure that personnel and equipment are adequately grounded.

2.2 System Conception

2.2.1 Overview

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.



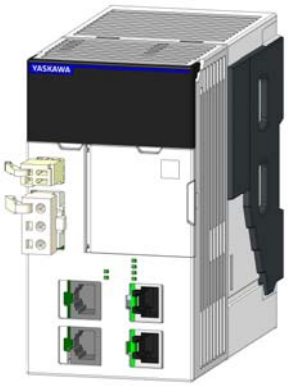
2.2.2 Components

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

⚠ CAUTION

Only modules of Yaskawa may be combined. A mixed operation with third-party modules is not allowed!

(1) CPU iC9226M-FSoE



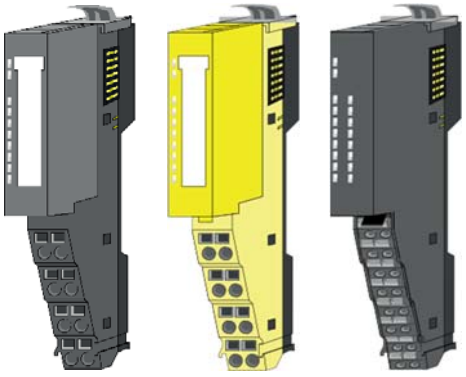
With the CPU iC9226M-FSoECPU electronics and power supply are integrated in one housing. The CPU is programmed and configured with iCube Engineer from Yaskawa in IEC 61131-3. On the right side via the SliceBus you can connect System SLIO periphery modules from Yaskawa. As head module via the integrated power mod- ule 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-FSoE. 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

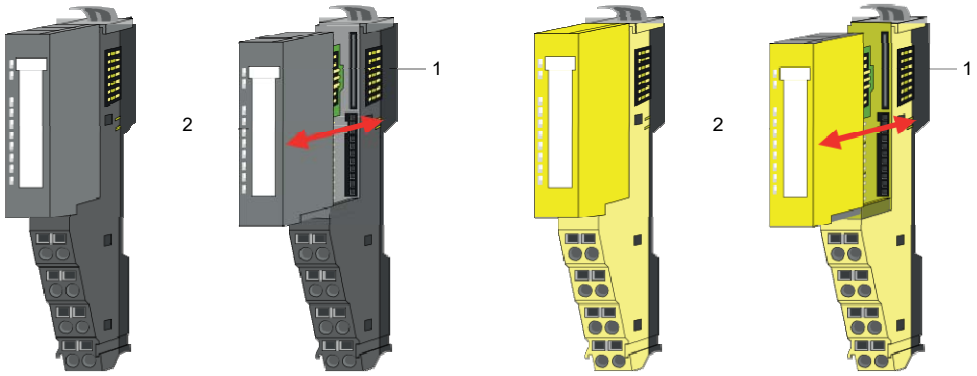


The periphery modules are available in the following versions, whereby of each the electronic part can be replaced with standing wiring:

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

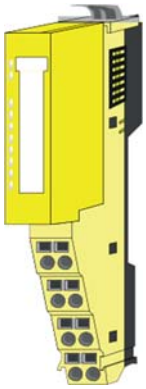
(4) 8x Periphery Modules

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



1 Terminal module

2 Electronic module

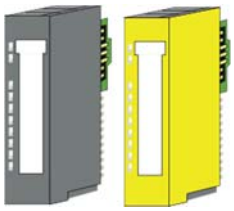


According to structure and dimensions the safety periphery modules correspond to the standard periphery modules of the System SLIO. For better recognition the color of the safety modules is yellow. Please consider that the safety electronic module may only be used at a yellow terminal module! The operation with mechanical compatible terminal modules is not allowed.

(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.

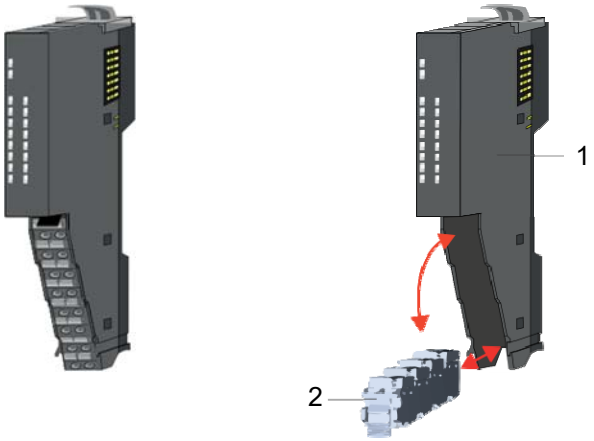
(6) Electronic Module



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

With the 16x periphery module the terminal block 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

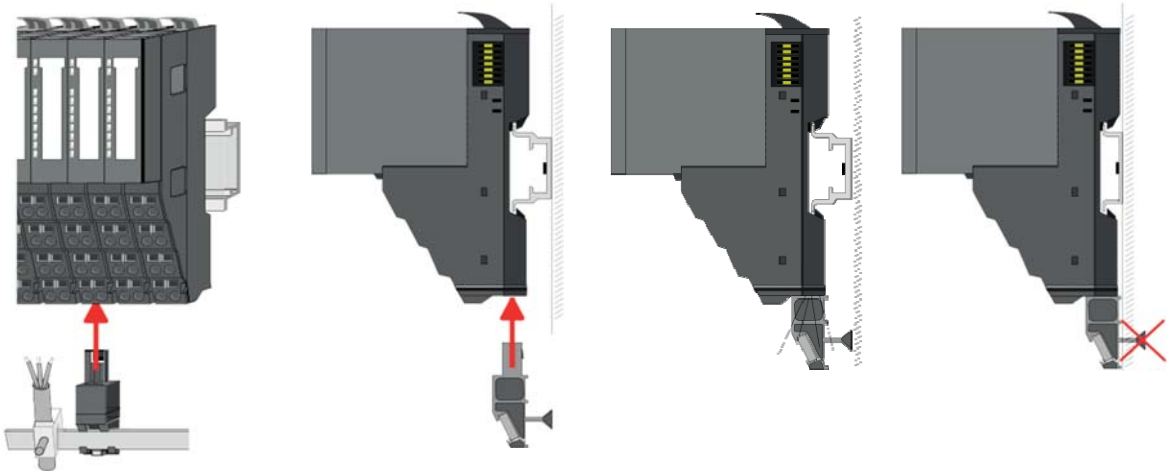
The terminal block provides the electrical interface for the signaling and supplies lines of the module. When mounting the terminal block, it is attached to the bottom of the electronic unit and turned towards the electronic unit until it clicks into place. With the wiring a "push-in" spring-clip technique 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

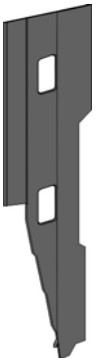
(a) Shield Bus Carrier

Information Please note that no shield bus carrier can be mounted on the CPU iC9226M-FSoE 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.

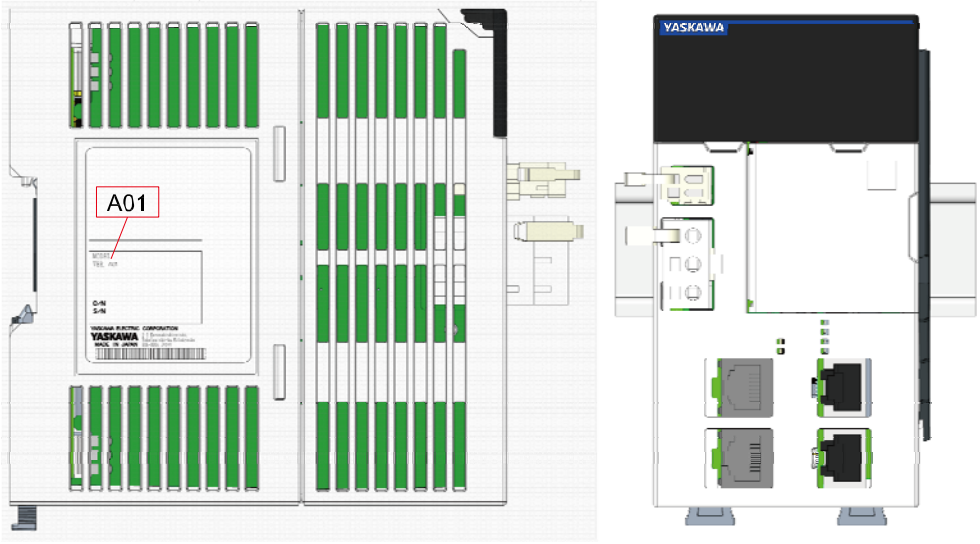
(c) Coding Pins

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.

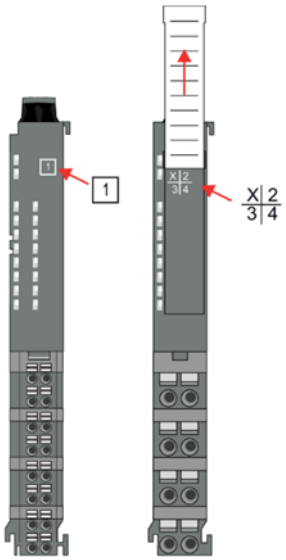
There is the possibility to fix the assignment of electronic and terminal module. Here coding pins (order number 000-0AC00) from Yaskawa can be used. The coding pin consists of a coding jack and a coding plug. By combining electronic and terminal module with coding pin, the coding jack remains in the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

2.2.3 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 iC9226 is indicated on the left side nameplate.



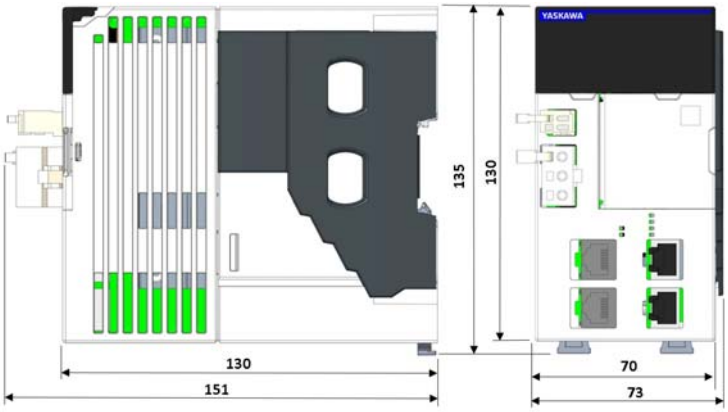
- Authoritative for the hardware revision of a System SLIO module is the hardware revision of the electronic module. This is always located under the labeling strip of the corresponding electronic module.
- Depending on the module type, there are the following 2 variants e.g. to indicate hardware revision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


1
X 2
3 4

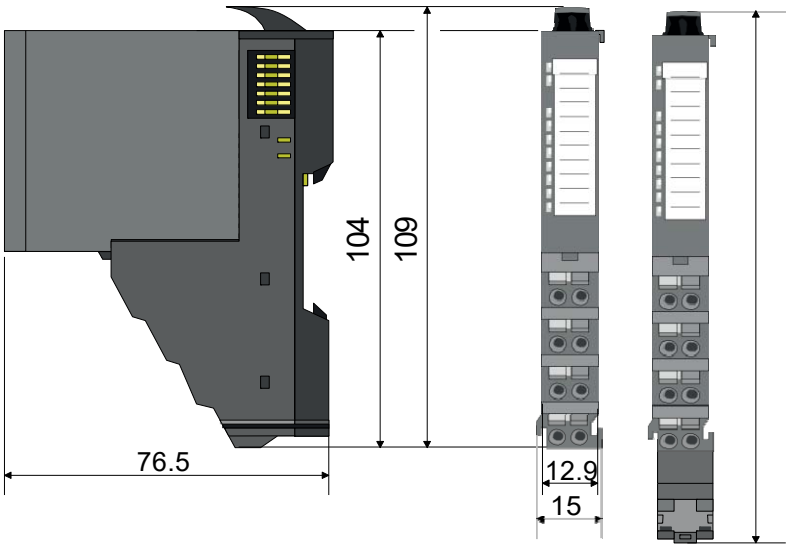
2.3 Dimensions

2.3.1 CPU iC9226M-FSoE

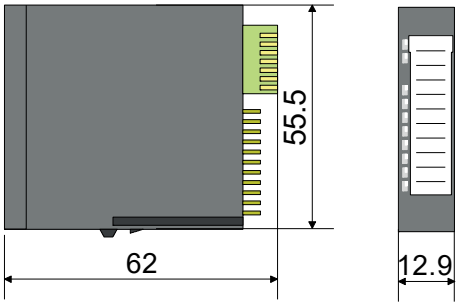
All dimensions are in mm.



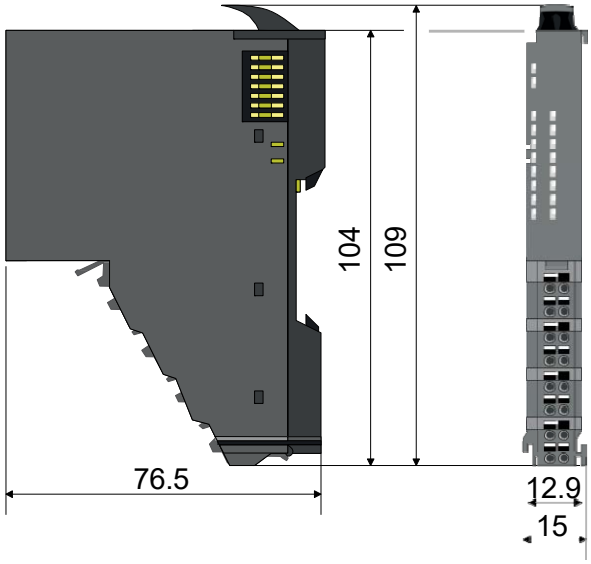
2.3.2 8x Periphery Module



2.3.3 Electronic Module



2.3.4 16x Periphery Module



2.4 Mounting

⚠ WARNING

Unintentional machine start-up

- **Do not mount or dismount when the power is on!**
- **Disconnect the CPU from the power supply before mounting or dismounting and secure the power supply against being switched on again!**
- **Do not switch on the power supply until the system has been completely mounted. Pay attention to the diagnostic indicators and any diagnostic messages.**
- **The machine/plant may only be started when no hazard can result from the machine/ plant.**

NOTICE

Insufficient external fusing will cause electronic damage to the CPU.

- **Fuse the supply voltage externally according to the connected load (number of System SLIO F participants/sum of current consumption of each participant).**
- **Ensure safe triggering of the external fuse.**
- **If you use a melting fuse, the power supply unit must be able to supply four times the rated current of the melting fuse. This ensures safe triggering in the event of an error.**

Improper handling may cause damage.

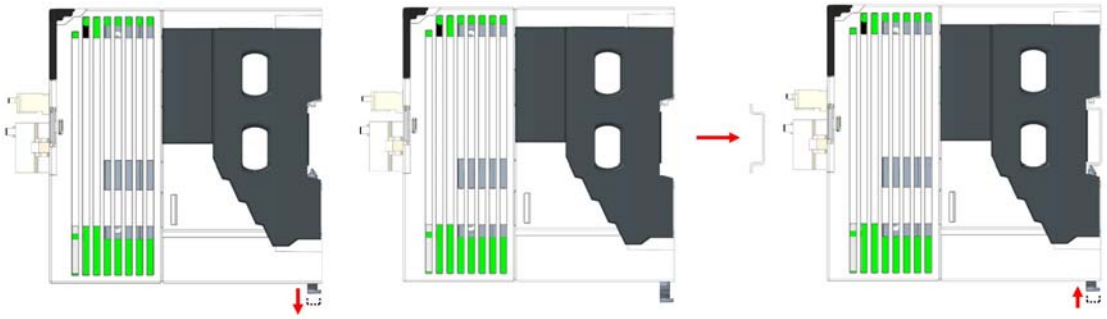
- **Handle the CPU and components with care!**
- **When installing the CPU and components, ensure that mechanical damage is avoided!**
- **Mount the CPU in a closed control cabinet or control box with degree of protection IP54 or higher on a 35×15mm standard mounting rail.**
- **Use a mounting rail according to EN 60715.**
- **Mount the mounting rail on a metal plate, which is connected to functional earth.**

2.4.1 Mounting CPU

(1) Functional Principle

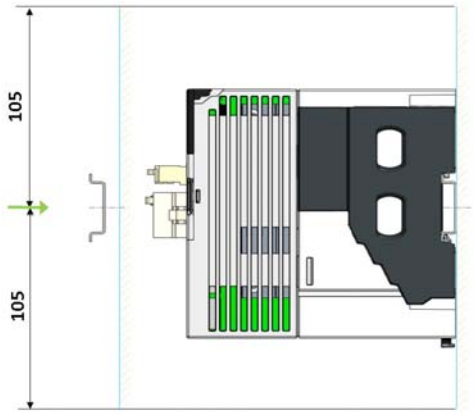
Move the DIN rail lock in under CPU to the open position. Hook the CPU to the top of the DIN rail and push it back to fix it to the mounting surface. Move the DIN rail lock to the locked position. The CPU is directly mounted at a mounting rail. Up to 64 System SLIO modules may be mounted.

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.

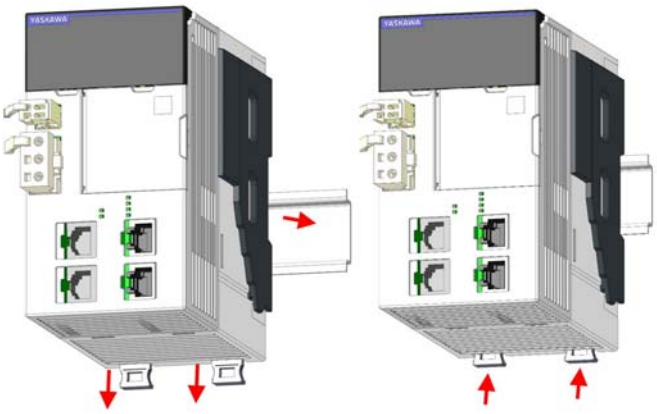


(a) Proceeding

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 on either side.



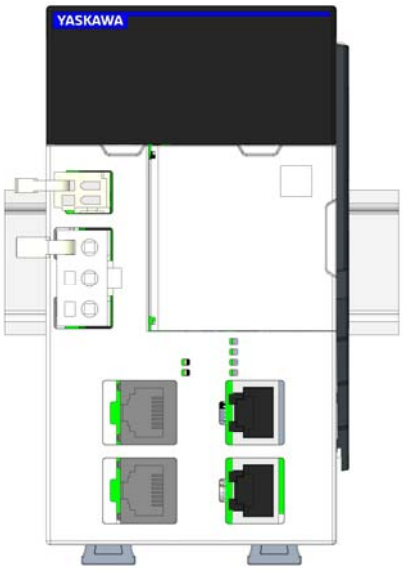
2. **Pull the locking brackets downward, place the CPU at the mounting rail and push the brackets upward.**



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

(2) Assembly Possibilities

Horizontal hanging:

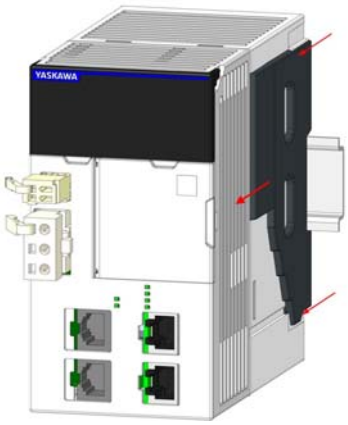


2.4.2 Mounting Periphery Modules

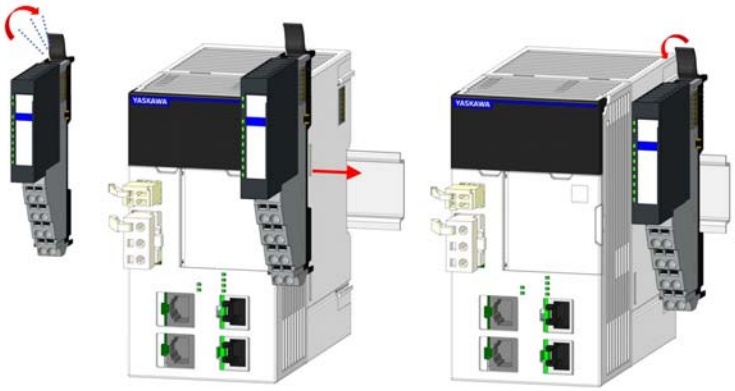
Information When using System SLIO modules, you must always mount the power module 007-1AB00 - DC 24V 10A, because the CPU does not provide a power section supply due to the system.

(1) Mounting Power Module 007-1AB00

1. **Before mounting the periphery 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.**



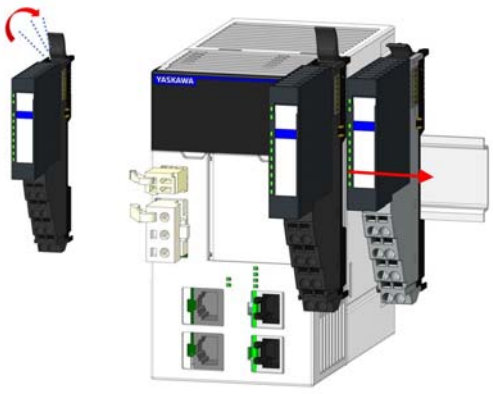
2. **Mount the periphery modules you want.**



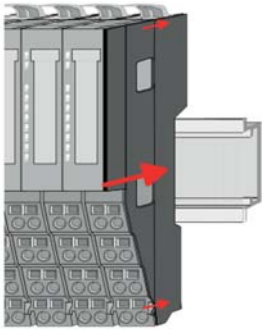
(2) Mounting Periphery Modules

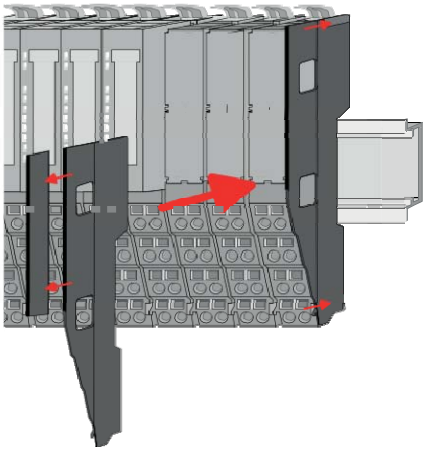
The procedure is identical for 8x and 16x periphery modules.

1. **Mount the periphery 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.

2.5 Wiring

⚠ CAUTION

Consider temperature for external cables!

Cables may experience temperature increase due to system heat dissipation. Thus the cabling specification must be chosen 25°C above ambient temperature!

Electrical safety - loss of safety function when using unsuitable power supplies

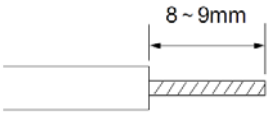
- **Only devices with safe insulation from the 230V mains may be connected to the CPU.**
- **The power supply for generating the DC 24V power must correspond to the requirements for PELV/SELV according to EN 50178. In these, a short circuit between the primary and secondary sides is excluded.**

2.5.1 Wiring CPU

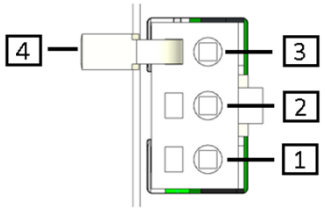
(1) CPU Connector

The CPU has a removable connector for the power supply. With the wiring of the connector spring clamp technique is used. This enables a rapid and straightforward connection of the supply lines by means of an attached locking lever.

(2) Data



V_{max}	30 V DC
I_{max}	10A
Cross section	0.5 ... 2.0mm² (AWG 20 ... 14)
Stripping length	8~9mm



1 Ground

2 0-VDC input

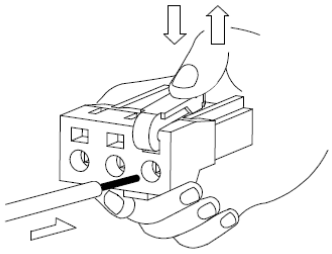
3 24-VDC input

4 Locking lever

(3) Plug Wire

The wiring happens with an attached tool.

1. **Attach the accessory opener tool to the pin to be wired and, while pushing the opener tool in, insert the prepared wire until it stops in the connection hole.**



By pushing the contact spring opens, thus ensuring the necessary contact pressure.

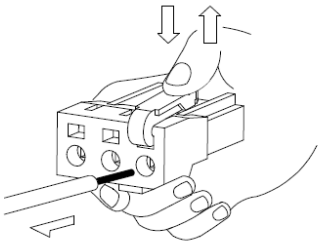
2. **Determine the pin position according to the pin assignment.**
3. **Connect the ground pole (Gnd) of your functional earthing to pin 1.**
4. **Connect the positive pole (+) of your external DC 24V power supply to pin 3**
5. **Connect the minus pole (0V) of your external DC 24V power supply to pin 2.**

   As soon as the CPU is power supplied, the associated LED lights up.

(4) Remove Wire

The removal of wiring happens with an attached tool.

1. **Attach the accessory opener tool to the pin where the wire should be removed and push**



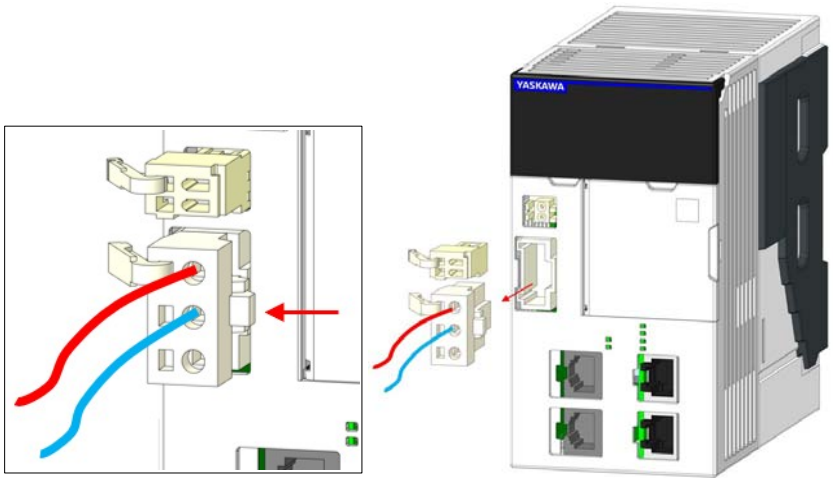
The contact spring releases the wire.

2. **Pull the wire from the connection hole.**

(5) Remove Connector

You have the option to remove the connector of the power supply, e.g. for a module change with fixed wiring. For this the connector has a locking lever. The connector is removed as follows:

1. **Remove connector:**



By pressing the release button as shown, the connector is released and can be removed.

2. **Plug connector:**

The connector is plugged by plugging it directly into the release lever. Here, the release button return to its original position.

2.5.2 Wiring System SLIO Periphery

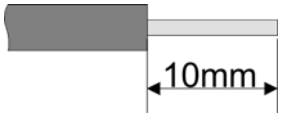
Information When using System SLIO modules, you must always mount the power module 007-1AB00 - DC 24V 10A, because the CPU does not provide a power section supply due to the system.

(1) Wiring Power Module

(a) Terminal Module Terminals

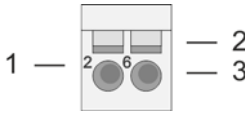
With the power module, terminals with spring clamp technology are used for wiring. The spring clamp technology allows quick and easy connection of your supply lines. In contrast to screw terminal connections this type of connection is vibration proof.

(b) Data



U_{max}	30V DC
I_{max}	10A
Cross section	0.08 ... 1.5mm² (AWG 28 ... 16)
Stripping length	10mm

(c) Wiring Proceeding

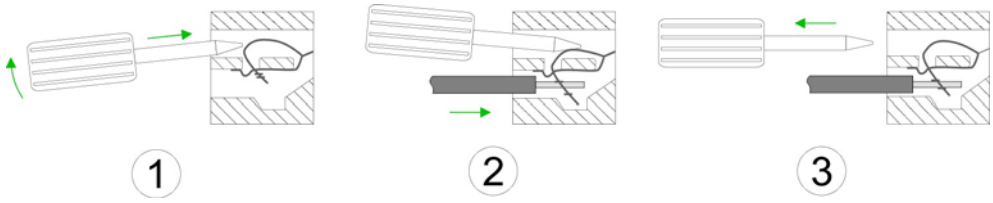


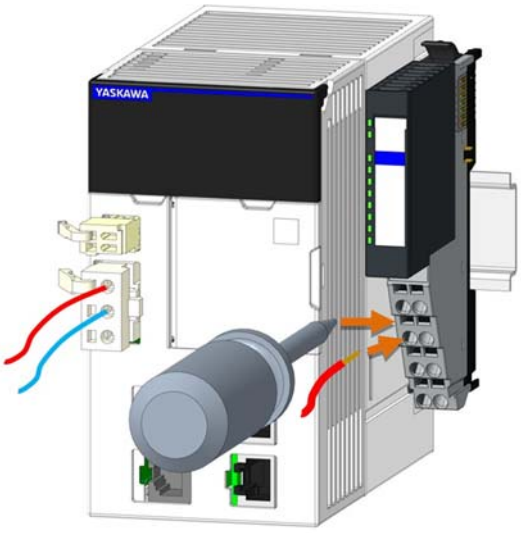
1 Pin no. at the connector

2 Opening for screwdriver

3 Connection hole for wire

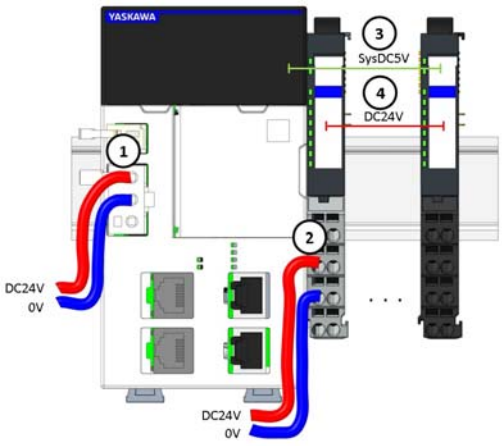
1. **Insert a suited screwdriver at an angel into the square opening as shown. Press and hold the screwdriver in the opposite direction to open the contact spring.**





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 SliceBus 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 and I/O area with a 4A fuse (fast) respectively by a line circuit breaker 4A 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!

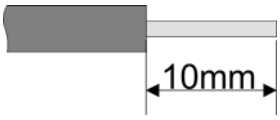
If this is not explicitly stated in the corresponding module description, hazardous voltages are not allowed to be connected to the corresponding terminal module!

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!

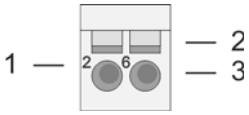
With wiring the terminal modules, terminals with spring clamp technology are used for wiring. The spring clamp technology allows quick and easy connection of your signal and supply lines. In contrast to screw terminal connections this type of connection is vibration proof.

(b) Data



U_{max}	240VAC / 30V DC
I_{max}	10A
Cross section	0.08 ... 1.5mm² (AWG 28 ... 16)
Stripping length	10mm

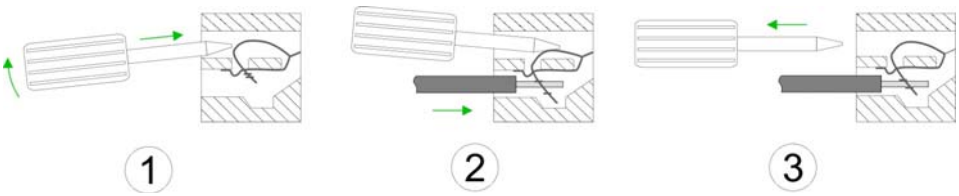
(c) Wiring Proceeding



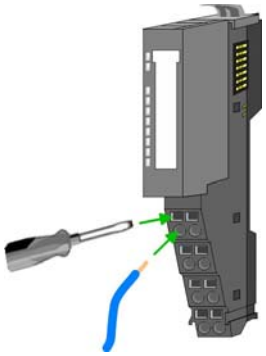
1 Pin no. at the connector

2 Opening for screwdriver

3 Connection hole for wire



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

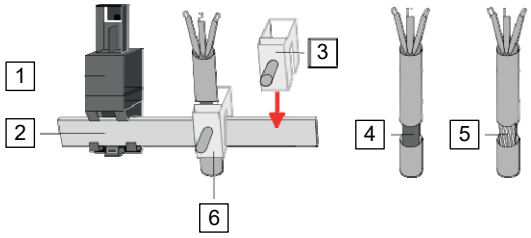


2. **Insert the stripped end of wire into the round opening. You can use wires with a cross section of 0.08mm² up to 1.5mm².**
3. **By removing the screwdriver, the wire is securely fixed via the spring contact to the terminal.**

(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. *2.8.2 Installation Guidelines on page 81*



1 Shield bus carrier

2 Shield bus (10mm x 3mm)

3 Shield clamp

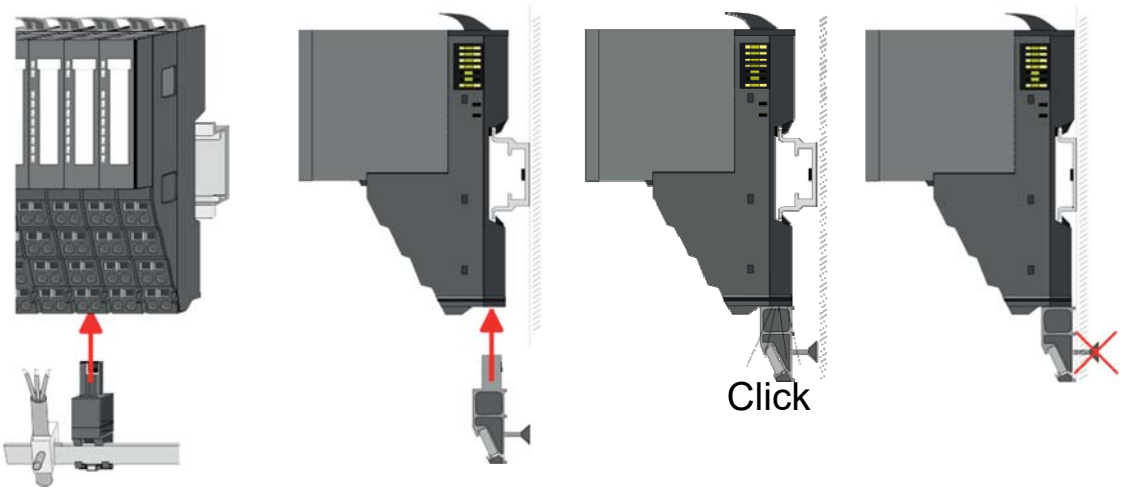
4 Cable shield with metal foil

5 Cable shield with wire mesh (close-meshed)

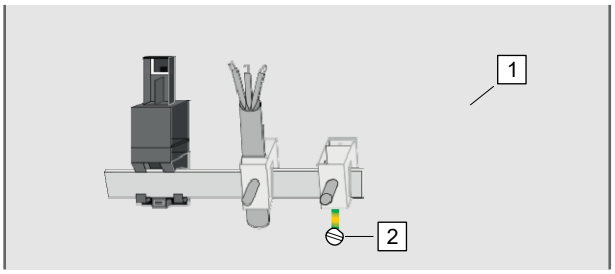
6 Cable shield mounted with shield clamp

◆ 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!

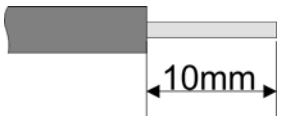
If this is not explicitly stated in the corresponding module description, hazardous voltages are not allowed to be connected to the corresponding terminal block!

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 ... 0.75mm²
Cross section with ferrule	0.14 ... 0.75mm²
Wire type	CU
AWG	24 ... 16
Stripping length	10mm

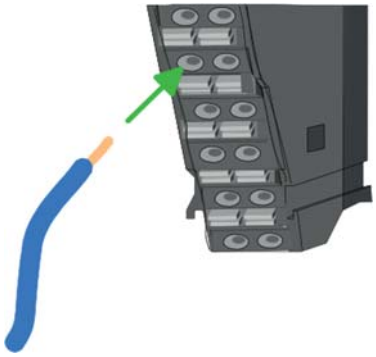
(c) Wiring Procedure

1 Release area

2 Connection hole for wire

◆ Insert Wire

The wiring happens without a tool.



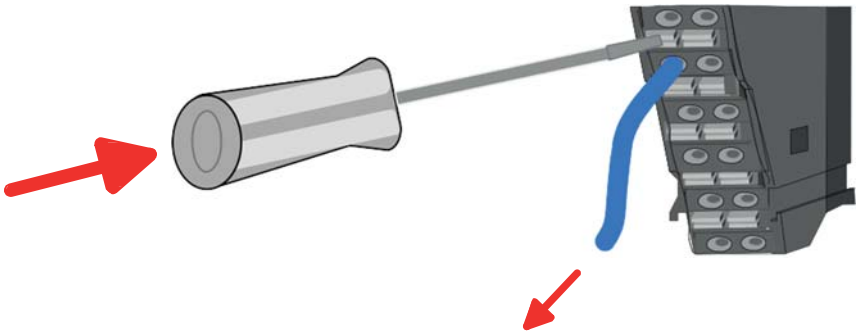
1. **Determine according to the casing labelling the connection position.**
2. **Insert through the round connection hole of the according contact your prepared wire until it stops, so that it is fixed.**

   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.**



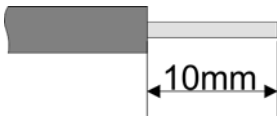
   The contact spring releases the wire.
2. **Pull the wire from the round hole.**

(4) Wiring Power Modules

(a) Terminal Module Terminals

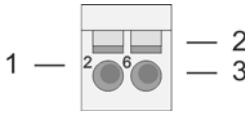
Power modules can be plugged between the periphery modules. With power modules, terminals with spring clamp technology are used for wiring. The spring clamp technology allows quick and easy connection of your signal and supply lines. In contrast to screw terminal connections this type of connection is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

(b) Data



U_{max}	30V DC
I_{max}	10A
Cross section	0.08 ... 1.5mm² (AWG 28 ... 16)
Stripping length	10mm

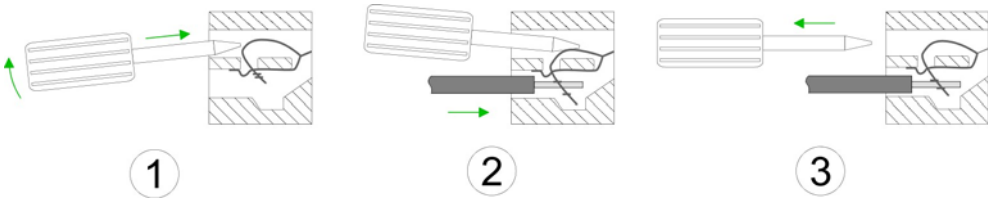
(c) Wiring Procedure



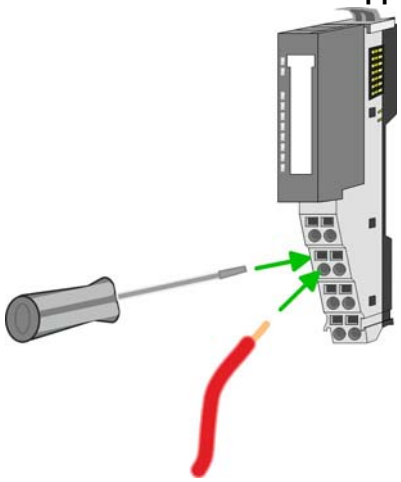
1 Pin number at the connector

2 Opening for screwdriver

3 Connection hole for wire



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

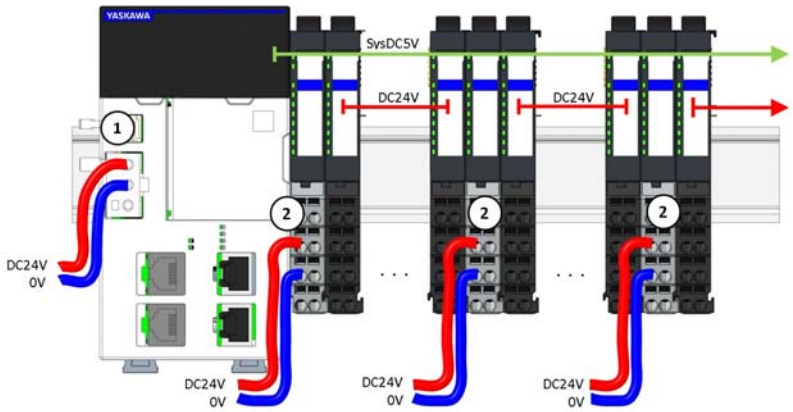


2. **Insert the stripped end of wire into the round opening. You can use wires with a cross section of 0.08mm² up to 1.5mm²**
3. **By removing the screwdriver, the wire is securely fixed via the spring contact to the terminal.**

(d) Deployment of the Power Modules

- The CPU does not provide a power section supply for the periphery modules. By plugging the power module with the order no. 007-1AB00 the succeeding periphery 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 periphery 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



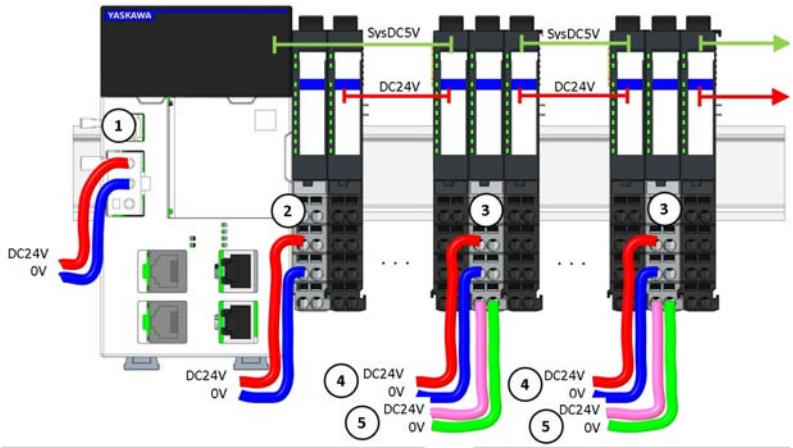
(1) DC 24V supply CPU:

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 and 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.

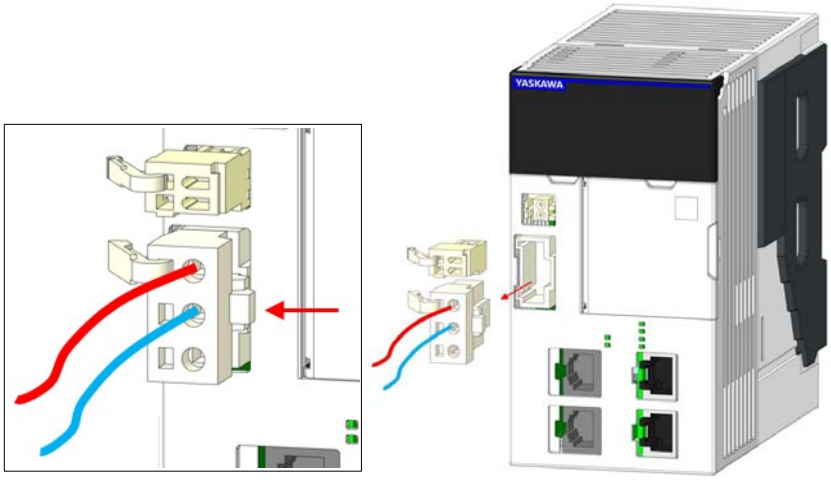
2.6 Demounting

2.6.1 Demounting CPU

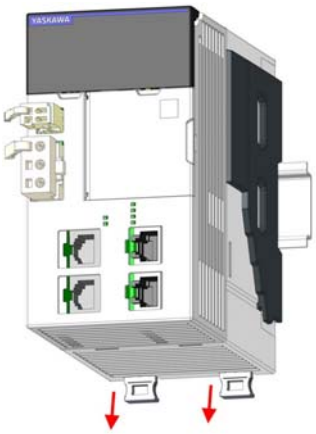
(1) Demounting in Standalone Operation

1. **Power-off your system.**

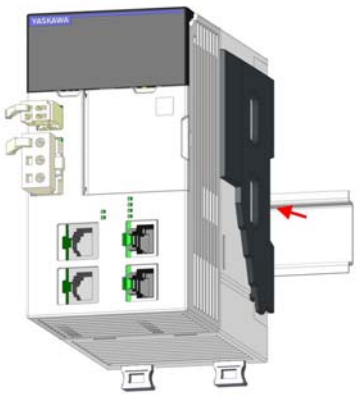
2. **Remove the connector of the power supply of the CPU. By pressing the release button as shown, the connector is released and can be removed.**



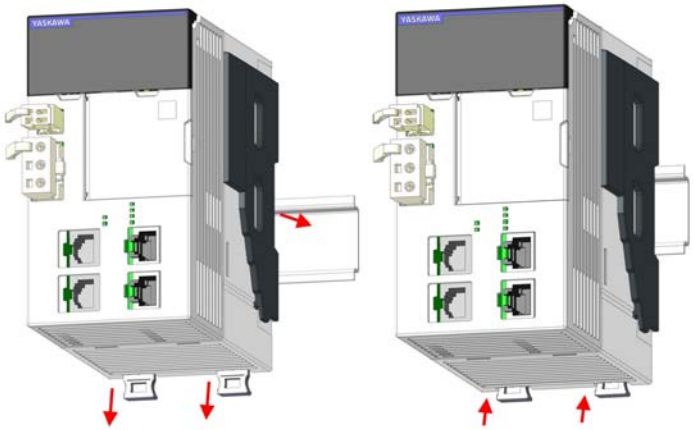
3. **Pull the locking brackets of the CPU downwards.**



4. **Pull the CPU forward.**



5. **Pull the locking brackets of the CPU to be mounted downwards, place the CPU at the mounting rail and push the brackets upward.**

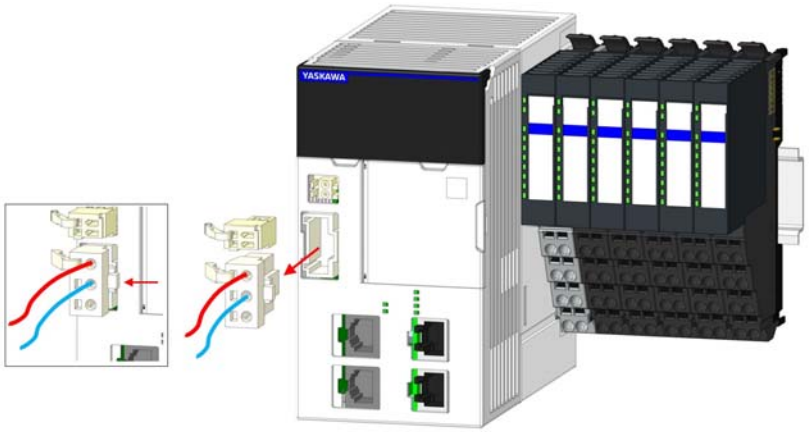


6. **Reconnect the connector of the power supply.**
7. **Now you can bring your system back into operation.**

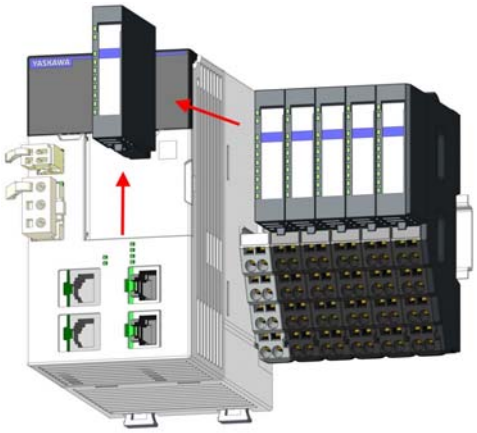
(2) Demounting on System SLIO

1. **Power-off your system.**

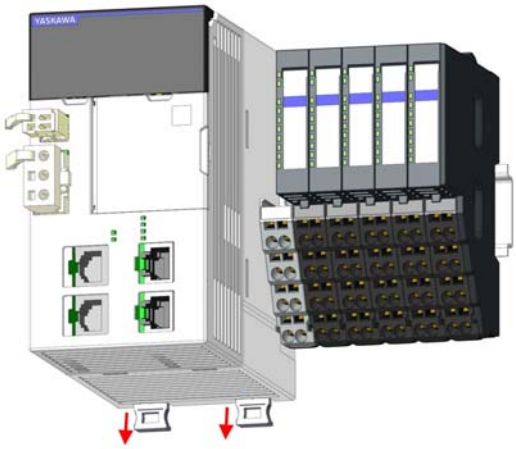
2. **Remove the connector of the power supply of the CPU. By pressing the release button as shown, the connector is released and can be removed.**



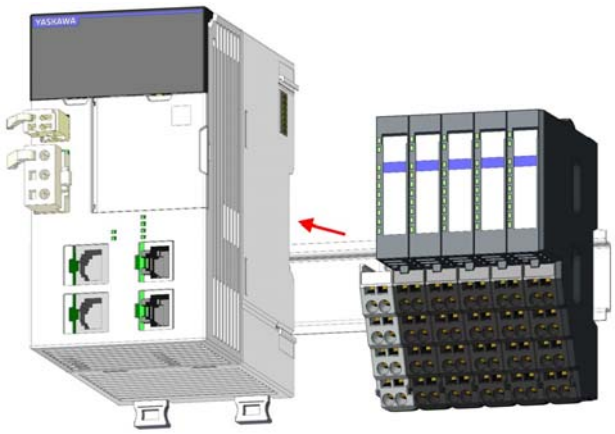
3. **For mounting reasons you have to remove the electronic module of the power module located right beside the CPU. Press the unlocking lever at the lower side of the power module and pull it forward.**



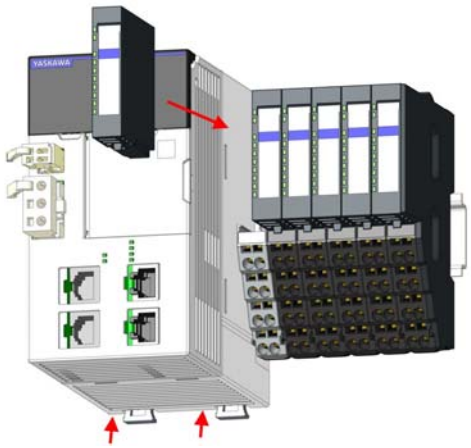
4. **Pull the locking brackets of the CPU to be exchanged downwards.**



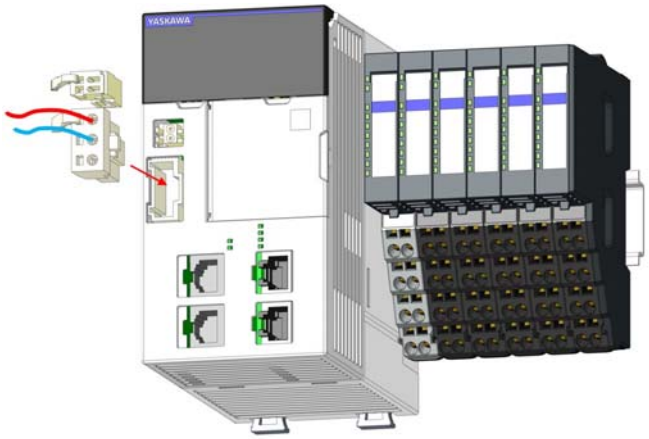
5. **Pull the CPU forward.**



6. **For mounting pull all the locking brackets of the CPU to be mounted downwards.**
7. **To mount the CPU put it to the left periphery module and push it, guided by the stripes, to the mounting rail.**
8. **Push all the locking brackets upward, again.**
9. **Plug again the electronic module, which you have removed before. For installation plug the electronic module guided by the strips at the lower side until this engages to the terminal module.**



10. **Reconnect the connector of the power supply.**



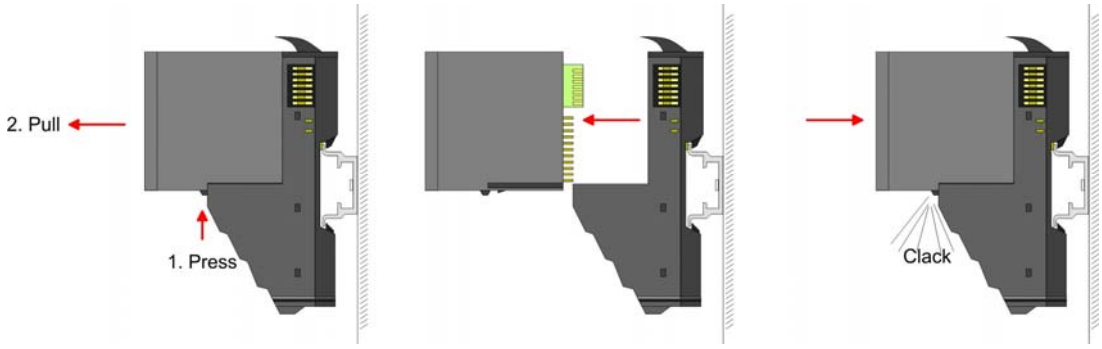
11. **Now you can bring your system back into operation.**

2.6.2 Demounting 8x Periphery Modules

(1) Proceeding

(a) Exchange of an Electronic Module

1. **Power-off your system.**
2. **For the exchange of an electronic module, the electronic module may be pulled forward after pressing the unlocking lever at the lower side of the module.**

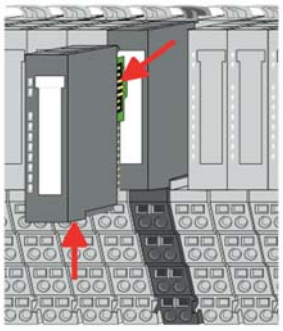


3. **For installation plug the new electronic module guided by the strips at the lower side until this engages to the terminal module.**

   Now you can bring your system back into operation.

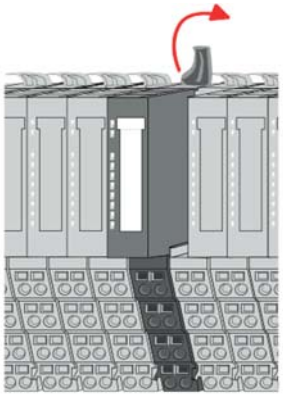
(2) Exchange of a Periphery Module

1. **Power-off your system.**
2. **Remove if exists the wiring of the module.**
3. **Press the unlocking lever at the lower side of the just mounted right module and pull it forward.**

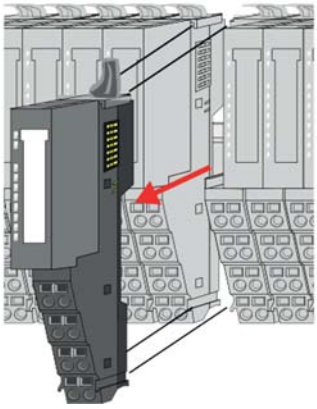


Information For demounting and exchange of a (head) module or a group of modules, due to mounting reasons you always have to remove the electronic module right beside. After mounting it may be plugged again.

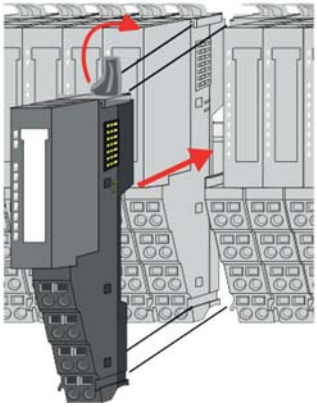
4. **Turn the locking lever of the module to be exchanged upwards.**



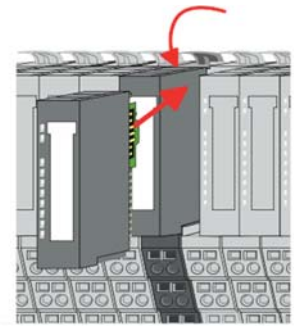
5. **Pull the module.**



6. **For mounting turn the locking lever of the module to be mounted upwards.**
7. **To mount the module put it to the gap between the both modules and push it, guided by the stripes at both sides, to the mounting rail.**



8. **Turn the locking lever downward, again.**
9. **Plug again the electronic module, which you have removed before.**



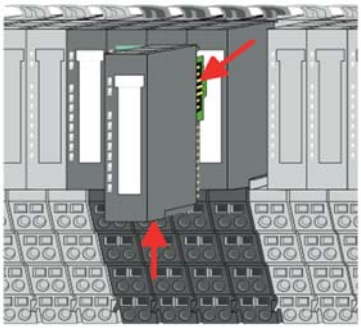
10. **Wire your module.**

    Now you can bring your system back into operation.

(3) Exchange of a Module Group

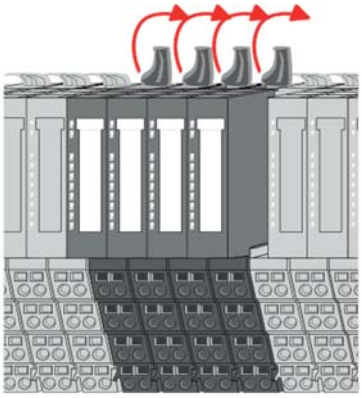
1. **Power-off your system.**
2. **Remove if exists the wiring of the module group.**

3. **Press the unlocking lever at the lower side of the just mounted right module near the module group and pull it forward.**

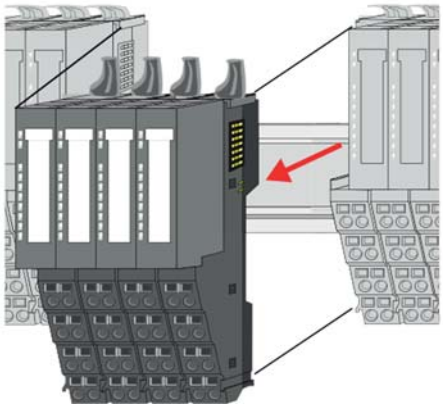


Information For demounting and exchange of a (head) module or a group of modules, due to mounting reasons you always have to remove the electronic module right beside. After mounting it may be plugged again.

4. **Turn all the locking lever of the module group to be exchanged upwards.**

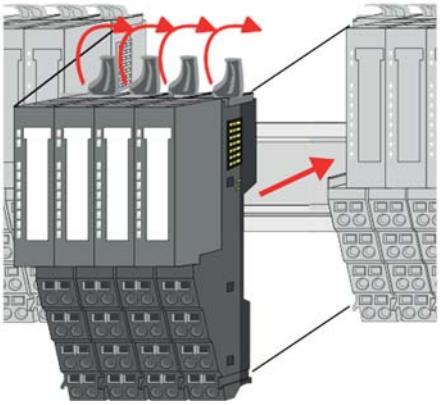


5. **Pull the module group forward.**

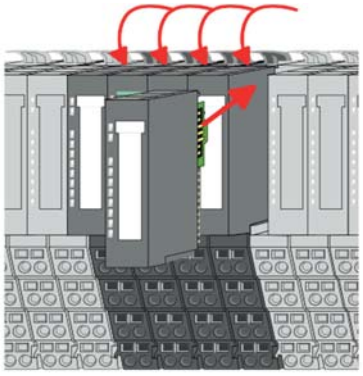


6. **For mounting turn all the locking lever of the module group to be mounted upwards.**

7. **To mount the module group put it to the gap between the both modules and push it, guided by the stripes at both sides, to the mounting rail.**



8. **Turn all the locking lever downward, again.**
9. **Plug again the electronic module, which you have removed before.**



10. **Wire your module group.**

    Now you can bring your system back into operation.

2.6.3 Demounting 16x Periphery Modules

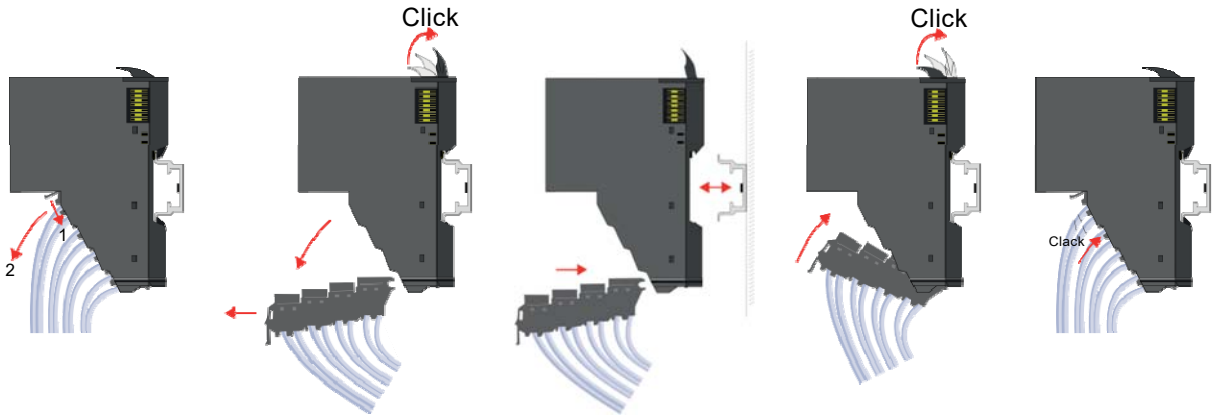
(1) Proceeding

(a) Exchange of an Electronic Unit

1. **Power-off your system.**
2. **To replace an electronic unit, you can push down and pull off the terminal block after releasing the lock.**

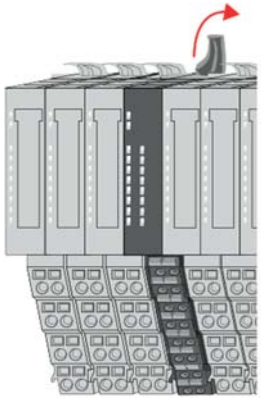
   To mount the terminal block, place it horizontally on the lower side of the electronic unit and push it towards the electronic unit until it clicks into place.

   Now you can bring your system back into operation.



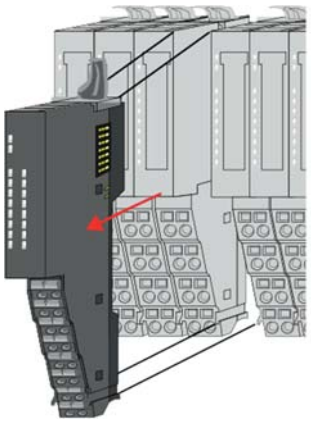
(2) Exchange of a 16x Periphery Module

1. **Power-off your system.**
2. **Remove if exists the wiring of the module respectively the wired terminal block.**
3. **Turn the locking lever of the module to be exchanged upwards.**



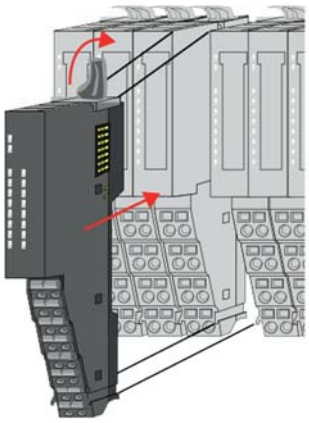
Information In contrast to 8x periphery modules, you can directly demount and mount 16x periphery modules.

4. **Pull the module.**

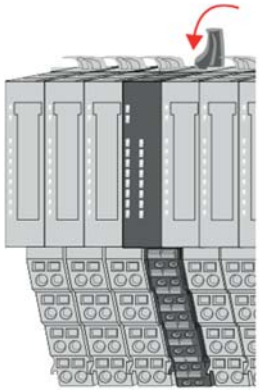


5. **For mounting turn the locking lever of the module to be mounted upwards.**

6. **To mount the module put it to the gap between both modules and push it, guided by the stripes at both sides, to the mounting rail.**



7. **Turn the locking lever downward, again.**

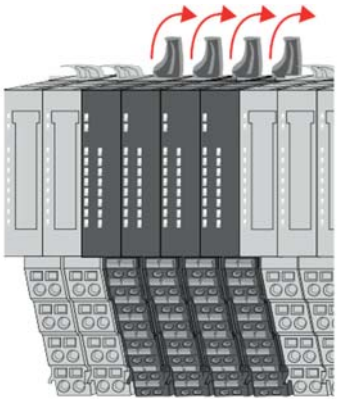


8. **Wire your module respectively plug the wired terminal block again.**

   Now you can bring your system back into operation.

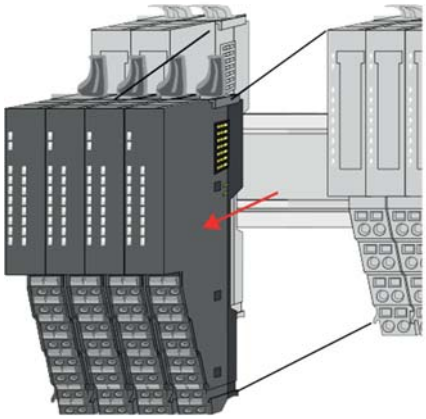
(3) Exchange of a Module Group

1. **Power-off your system.**
2. **Remove if exists the wiring of the module group respectively the wired terminal blocks.**
3. **Turn all the locking lever of the module group to be exchanged upwards.**

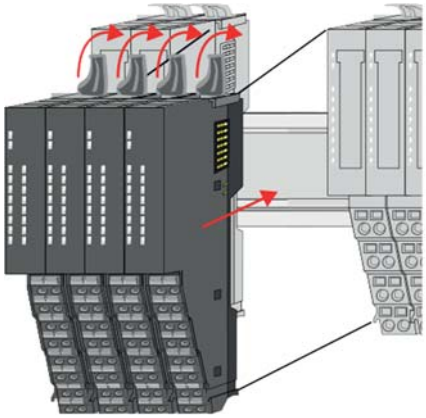


Information In contrast to 8x periphery modules, you can directly demount and mount 16x periphery modules.

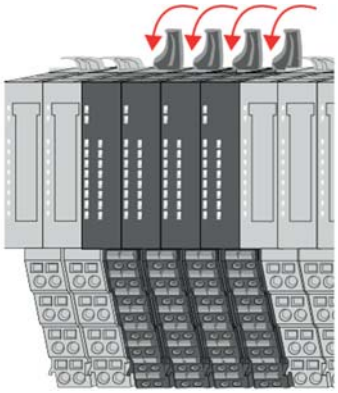
4. **Pull the module group forward.**



5. **For mounting turn all the locking lever of the module group to be mounted upwards.**
6. **To mount the module group put it to the gap between the both modules and push it, guided by the stripes at both sides, to the mounting rail.**



7. **Turn all the locking lever downward, again.**



8. **Wire your module group respectively plug the wired terminal blocks again.**

   Now you can bring your system back into operation.

2.7 Device Replacement and Repair

2.7.1 Device Replacement

(1) Notes

NOTICE

When changing the safety CPU, always observe the corresponding checklist!

Replacement with an incompatible unit is not permitted!

Information If the firmware version of the CPU is newer than the firmware version of the CPU to be replaced, you might have to recompile your user program in iCube Engineer. If this is required, you will be informed with the corresponding firmware version.

(2) Proceeding

The new CPU must meet the following conditions:

- Same device type.
- Same or higher firmware version.

1. **Demount the CPU to be replaced.** *2.6 Demounting on page 67*
2. **Remove the Yaskawa SD card, if exists.**
3. **Mount the new CPU.** *2.4 Mounting on page 52*
4. **If exists, you can transfer your project with all access data and IP address to the new CPU by inserting the Yaskawa SD card.**
5. **To complete the device replacement, proceed according to the checklist modification and retrofitting .**

(3) Module Replacement FSoE Slave

NOTICE

Please note that when replacing the module of an FSoE slave, all of the manufacturer's requirements must be adhered to!

2.7.2 Device Repairs and Defects

Repairs may only be carried out by Yaskawa.

- Always contact your national representative of Yaskawa before returning the product.
- Return defective devices to the national representative of Yaskawa for repair or to obtain a replacement device.
- If possible, use the original packaging when returning the product.

2.8 Industrial Security and Installation Guidelines

2.8.1 Industrial Security in Information Technology

(1) Latest Version

This chapter can also be found as a guide [Industrial IT Security] in the [Download Center] of www.yaskawa.eu.com

(2) Hazards

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:

- 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.

(3) Precautions

The most important precautions to prevent manipulation and loss of data security in the industrial environment are:

- 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 save channels.
- Segmenting in protected automation cells, so that only devices in the same group can exchange data.
- Deactivation of unnecessary hardware and software.

(4) Further Information

You can find more information about the measures on the following websites:

- Federal Office for Information Technology www.bsi.bund.de
- Cybersecurity & Infrastructure Security Agency us-cert.cisa.gov
- VDI / VDE Society for Measurement and Automation Technology www.vdi.de
- IEC 62443 Security for industrial automation and control systems https://www.iec.ch/blog/understanding-iec-62443

(5) 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.

(6) 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.

2.8.2 Installation Guidelines

(1) General

The installation guidelines contain information about the interference free deployment of a PLC system. 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 aluminum parts. Aluminum 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 favourable.
  - 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 metallised 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 metallised 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

2.9 General Data for iC9200 Series

Conformity and approval		
Conformity		
CE	2014/30/EU	EMC directive
Approval		
UL	UL 61010-2-201	UL File Number: E184524
Others		
RoHS	2011/65/EU	Directive on the restriction of the use of certain hazardous substances in electrical and electronic equipment

Protection of persons and device protection		
Type of protection	-	IP20
Electrical isolation		
to the field bus	-	electrically isolated
to the process level	-	electrically isolated
Insulation resistance	EN 61010-2-201	-
Insulation voltage to reference earth		
Inputs / outputs	-	DC 24V, test voltage AC 500V
Protective measures	-	against short circuit

Environmental conditions to EN 61131-2		
Climatic		
Storage / transport	EN 60068-2-14	-40…+70°C
Operation		
Horizontal installation hanging	EN 61131-2	0…+60°C
Air humidity	EN 60068-2-30	RH1 (without condensation, rel. humidity 10…95%)
Pollution	EN 61131-2	Degree of pollution 2
Installation altitude max.	-	2000m
Mechanical		
Oscillation	EN 60068-2-6	1g, 9...150Hz
Shock	EN 60068-2-27	15g, 11ms

Mounting conditions		
Mounting place	-	Control cabinet or switch box of protection class IP54 or higher on a 35 mm (Height 15mm） standard mounting rail.
Mounting position	-	Horizontal *2.4.1 (2) Assembly Possibilities on page 53*

EMC	Standard		Comment
Emitted interference	EN 61000-6-4		Class A (Industrial area)
Noise immunity Zone B	EN 61000-6-2		Industrial area
		EN 61000-4-2	ESD 8kV at air discharge (degree of severity 3), 4kV at contact discharge (degree of severity 2),
		EN 61000-4-3	HF irradiation (casing) 80…1000MHz, 10V/m, 80% AM (1kHz) 1.4...6.0GHz, 3V/m, 80% AM (1kHz)
		EN 61000-4-6	HF conducted 150kHz…80MHz, 10V, 80% AM (1kHz)
		EN 61000-4-4	Burst, degree of severity 3
		EN 61000-4-5	Surge, degree of severity 2[1]
1) Due to the high-energetic single pulses with Surge an appropriate external protective circuit with lightning protection elements like conductors for lightning and over-voltage is necessary.			

2.9.1 Use in Difficult Operating Conditions

Information

Without additional protective measures, the products must not be used in locations with difficult operating conditions; e. g. due to:

- dust generation
- chemically active substances (corrosive vapors or gases)
- strong electric or magnetic fields

3

Hardware Description

3.1 Properties

Hardware	Properties
CPU iC9226M-FSoE	• Programmable in IEC 61131 via Yaskawa iCube Engineer. • Slot for external Yaskawa SD card. • Status LEDs for operating state and diagnostics. • X5: EtherCAT master functionality. • X6: Ethernet interface for future extensions. • X3/X4: Ethernet (switch) - PROFINET optional. • Up to 64 System SLIO modules can be connected via *SliceBus*.
Memory	– 2GB working memory (RAM). – 12MB program memory. – 32MB data memory. – 3072kB retentive data memory.

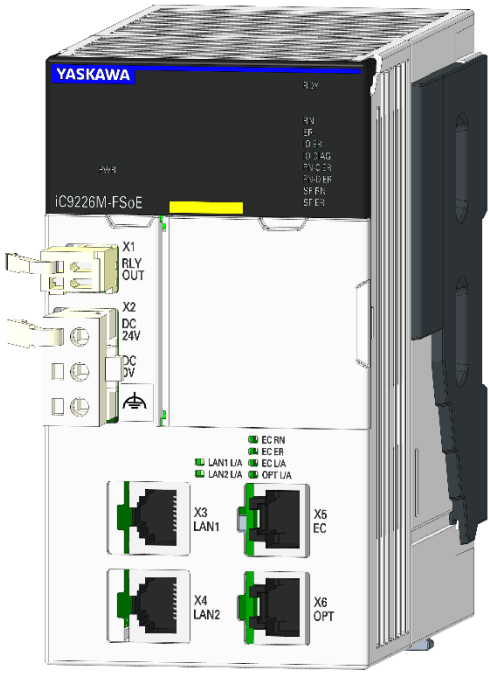
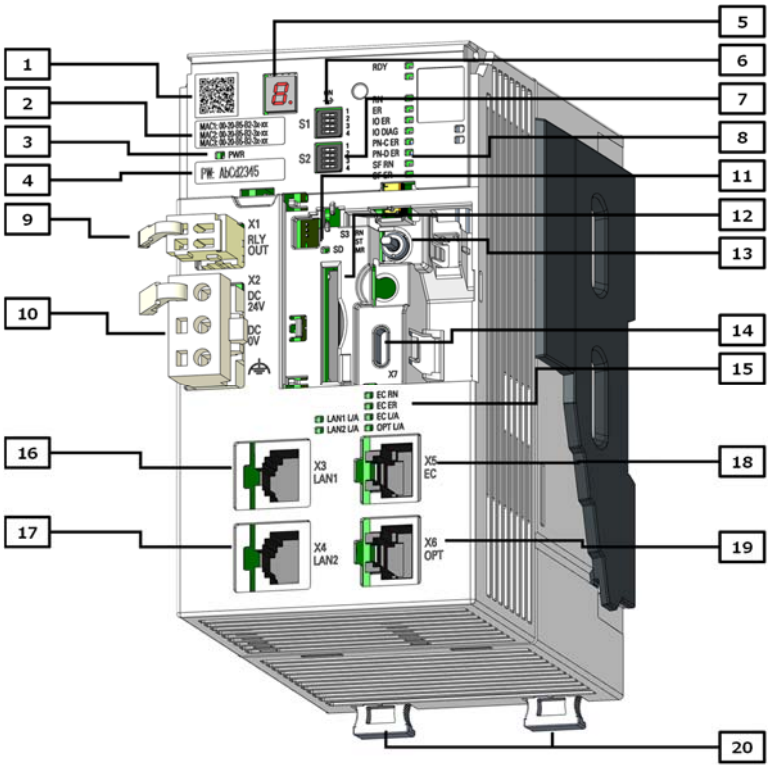


Table 3.1 Ordering data

Type	Order number	Description
CPU iC9226M-FSoE	JEYRM-MPX022SE10L32-2	CPU iC9226M-FSoE with EtherCAT FSoE master.

3.2 Structure

3.2.1 CPU iC9226M-FSoE



1	QR code
2	MAC address X3, X4, and X6 connector
3	Power indicator
4	Password
5	7-segment display
6	S1: DIP switch
7	S2: DIP switch
8	Status LEDs
9	X1: Relay out connector
10	X2: DC 24V power supply connector
11	SD indicator
12	Slot for Yaskawa SD card
13	Operating mode switch
14	X7: USB-C jack
15	Status LEDs
16	X3: Ethernet connector
17	X4: Ethernet connector
18	X5e: EtherCAT connector
19	X6: Optional
20	Locking brackets

1 to 8 and 11 to 14 are located under the front flap.

Information **Direct access to product information**

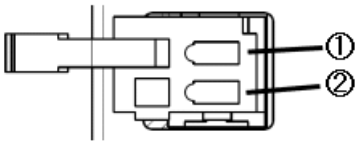
The QR code 1 at the front takes you to the product-specific website. You will find there all information for deployment and operation of the CPU.

3.2.2 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.



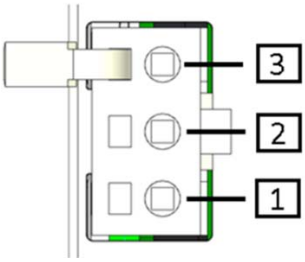
Name	Model	Color
Rlyout Connector	734-302	White

(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. (Ground to 100 Ω max.)

(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.

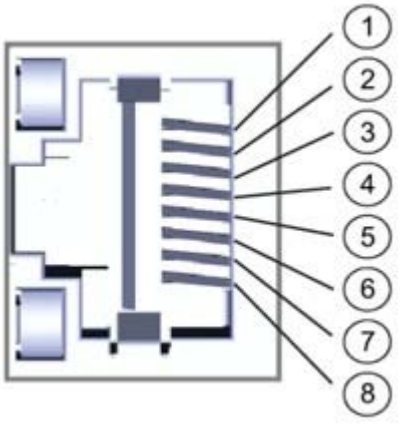


Table 3.2 8pin RJ45 jack:

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 processors with EtherCAT controller.
- You can use the EtherCAT controller in an EtherCAT system as an EtherCAT master.
- It is connected via the integrated EtherCAT port X5.
- Connect this interface with the RJ45 jack "IN" of your EtherCAT slave 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 master and a various number of EtherCAT slaves (coupler).
- Each EtherCAT slave has an "IN" and "OUT" RJ45 jack. The arriving EtherCAT cable from the direction of the master 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.

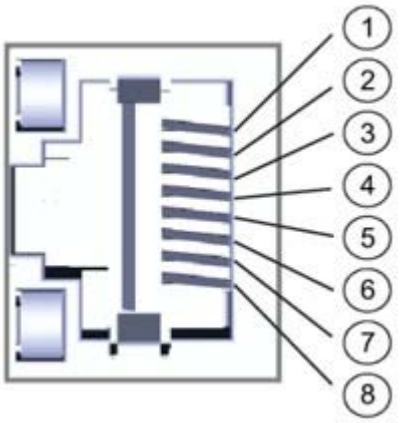


Table 3.3 8pin RJ45 jack:

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.

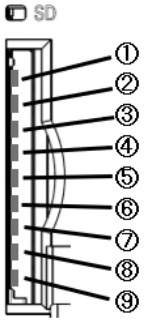


Table 3.4 SD Card Slot Pin Assignments

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

(6) USB Type-C Connector (For future use)

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

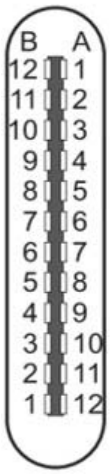


Table 3.5 24pin USB-C jack

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.

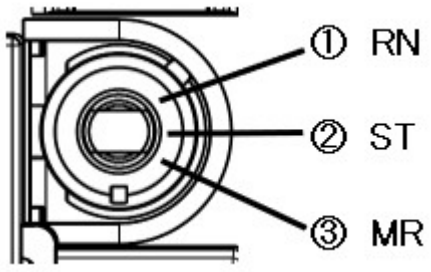
3.2.3 Switches

The iC9226M has the following three switches.

- Operating mode switch: S3
- DIP switch: S1, S2
- SD/STOP switch: S4 (For future use)

(1) Operating Mode Switch: S3

This switch primarily sets the operating mode of the iC9226M.



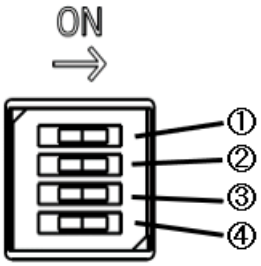
- With the operating mode switch, you can select between the operating modes ST (STOP) and RN (RUN) on the CPU.
- With the button position MR (Memory Reset) you can request a reset of the CPU in different levels. *4.7 'MRESET and reset to factory settings' page 131*

Switch Position: Name	Operating Mode	Default
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 iC92226M.

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



(a) S1 (Top DIP Switch)

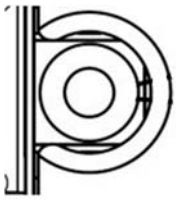
Name	Status	Operating Mode	Default	Remarks
1	OFF	Normal startup	OFF	Software control
	ON	Safe mode startup		
2	OFF	Normal startup	OFF	Software control
	ON	Type 1 reset		
3	OFF	Normal startup	OFF	OFF
	ON	TBD		
4	OFF	Normal startup	OFF	OFF
	ON	TBD		

(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	TBD		
3	OFF	Normal startup	OFF	OFF
	ON	TBD		
4	OFF	Normal startup	OFF	OFF
	ON	TBD		

(3) SD/STOP switch: S4

For future use.



3.2.4 Memory

(1) Internal memory

The CPU has an integrated memory. You will find information on the memory sizes in the technical data.
3.3 Technical Data on page 104

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.

4.6 Memory management on page 128

(2) Slot for Yaskawa SD card

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

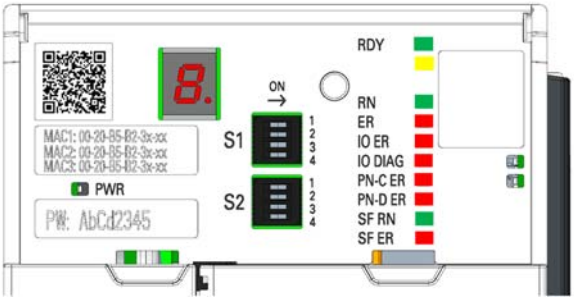
3.2.5 Buffering Mechanisms

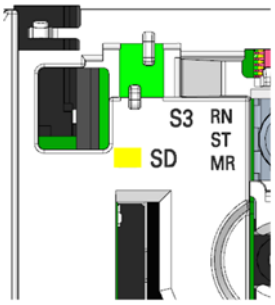
- The iC9200 Series CPU has a capacitor-based mechanism to buffer the internal clock in case of power failure for 28 days.
- The retentive data defined during configuration are automatically saved in the non-volatile memory in the event of a power failure.

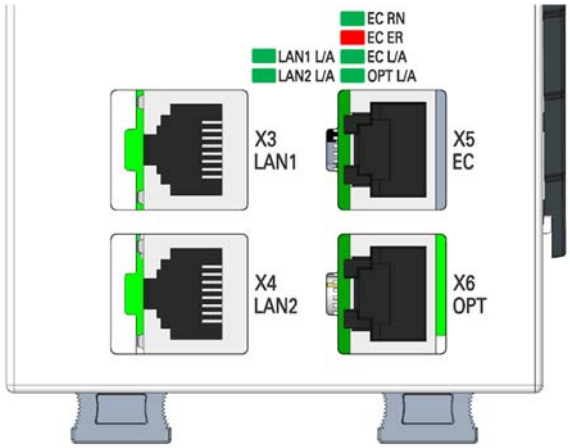
3.2.6 LEDs

(1) Status Indicators

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







Function	Reference
POWER LED	*(a) POWER LED on page 98*
Uboot	*(b) Uboot on page 98*
Linux and Overlay File System	*(c) Linux and Overlay File System on page 99*
Firmware Update	*(d) Firmware Update on page 100*
Factory Reset	*(e) Factory Reset on page 100*

Function	Reference
SliceBus	*(f) SliceBus on page 100*
PROFINET Controller	*(g) PROFINET Controller on page 100*
PROFINET Device	*(h) PROFINET Device on page 101*
PROFINET System	*(i) PROFINET System on page 101*
Safety PLC ☞	*(j) Safety PLC on page 101*
SD Card ☞	*(k) SD Card on page 102*
EtherCAT Operation ☞	*(l) EtherCAT Operation on page 102*
Ethernet Link ☞	*(m) Ethernet Link on page 102*
EtherCAT Link ☞	*(n) EtherCAT Link on page 102*

(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											
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 RUN (green)	EC ERR (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											
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 RUN (green)	EC ERR (red)	
Not lit	Not lit	Not lit	Flashing red 0.5 Hz interval	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 interval	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 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	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 0.2sON/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 interval	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											
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 RUN (green)	EC ERR (red)	
Not lit	Not lit	Flashing 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											
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 RUN (green)	EC ERR (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	Release switch to start factory reset type 1
Not lit	Not lit	Flashing green 2 Hz interval	Lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Release switch to start factory reset type 2
Not lit	Not lit	Flashing green 2 Hz interval	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Not lit	Factory reset type 2 is being performed

(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 inteval	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) Safety PLC

LED Behavior		Controller State
SF RN (green)	SF ER (red)	
Not lit	Not lit	Safety PLC isn't ready for operation (HW reset or init state)
Lit	Lit	Safety PLC isn't ready for operation (HW reset or init state)
Flashing green 1 Hz interval	–	The following status is shown depending on the operating mode: • PowerON - Initialization – The Safety PLC is in the SAFE-STOP state. – Project data is transferred from the parametrization memory to the internal memory of the Safety PLC. • Data transfer – With iCube Engineer, a project is transferred to the Safety PLC. • Debug – The Safety PLC is in the DEBUG-STOP state. – The Safety PLC is in the DEBUG-HALT state.
Flashing green 2 Hz interval	Not lit	Safety PLC is in DEBUG-RUN state
Lit	Not lit	Safety PLC is in SAFE-RUN state
–	Not lit	A Failure State isn't present
–	Flashing red 1 Hz interval	Switched to the safe state due to a configuration error
Not lit	Lit	Switched to the safe state due to a critical error

(k) SD Card

LED Behavior												Controller State
RDY (green)	Resvd (yellow)	RN (green)	ER (red)	IO ER (red)	IO DIAG (red)	PN-CER (red)	PN-DER (red)	SD (yellow)	EC RUN (green)	EC ERR (red)	RLY (green)	
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	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	Not lit	SD card used for overlay file system

(l) 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	Slaves configured, link available but topology not ok
–	Lit	Slaves configured, link not available

(m) 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

(n) 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

3.3 Technical Data

3.3.1 iC9226M-FSoE – JEYRM-MPX022 SE10L32-2

Model Number.	JEYRM-MPX022SE10L32-2
Type	iC9226M-FSoE
Technical data power supply	
Power supply (rated value)	DC 24 V
Power supply (permitted range)	DC 20.4...28.8 V
Reverse polarity protection	yes
Current consumption (rated value)	2.1A
Inrush current	10A, 0.1ms max
I^2t	e-
Max. current drain at backplane bus	3A
Max. current drain load supply	-
Power loss	12.9W
Hardware	
CPU	Triton (ARM A17)
CPU cores	3
Frequency	1.26 GHz
RAM	2 GB
eMMC	8 GB
Operating controls	LEDs, Three-point switch, DIP-switches
Integrated SliceBus supply	yes
Connectors	
SliceBus	yes
Number of RJ45 interfaces	4 Ports
External SD card	
External SD card	For future use
Operating system	

Continued on next page.

Continued from previous page.

Order no.	JEYRM-MPX022SE10L32-2
Operating system	Linux with RT Kernel
Overlay filesystem on internal eMMC	yes
Overlay filesystem on internal eMMC, Capacity	1.5 GB
Overlay filesystem on external SD card	-
Overlay filesystem on external SD card, Capacity	-
Firewall	yes
SSH/SFTP	yes
Synchronization via Ethernet (NTP)	yes-
DNS	yes
IEC 61131 runtime system	
Program memory	12 MB
Data memory	32 MB
Retain memory	3072 kB
Realtime clock	
Realtime clock	yes
Accuracy Realtime clock	1 minute deviation per month
Buffered time	28 days @ 25°C
Execution and Synchronization Manager (ESM)	
Execution and Synchronization Manager (ESM)	yes
Min. task cycle time (ESM)	500 us
ESM cores	1
Maximum parallel tasks	16
SliceBus	
Amount of process data per module	up to 60 bytes
Max number of modules	64
Cycle time [ms]	500 µs … 16 ms
OPC UA	
OPC UA	yes
Server	yes
Max parallel sessions	5
Sampling rates	100 ms – 5 s
Encryption suite Basic128Rsa15	yes
Encryption suite Basic256	yes
Encryption suite Basic256Sha256	yes
Encryption suite Aes256Sha256RsaPss	yes
Encryption suite Aes128Sha256RsaOaep	yes
Programming	
IEC 61131-3	yes
Web Based Management (WBM)	
Web Based Management (WBM)	yes

Continued on next page.

Continued from previous page.

Order no.	JEYRM-MPX022SE10L32-2
Ethernet	
Ethernet-capable ports	X3/X4: 2 Ports x 10/100 Mbit/s (half/full duplex)
EtherCAT Master	
Number of EtherCAT-slaves	512
Update time	500 µs … 512 ms
EoE support	yes
CoE support	yes
FoE support	yes
Distributed Clock support	yes
Hotconnect Slaves	yes
Isochronous mode	yes
Functional safety	
Minimum time	5 ms
Maximum time	15 ms
Program memory safe program	64 KB
Data memory	16 KB
Safety protocol	FSoE
Number of FSoE devices	32
Safety related input data	512 Byte
Safety related output data	512 Byte
Standard input data	128 Byte
Standard output data	128 Byte
Max. number of FB instances	512
Safety requirements	SIL CL 3, PL e, Cat 4
Motion	
Default Axis Count	4 servo + 4 virtual
Cyclic Motion Update Performance	Up to 8 servo + 8 virtual @ 500µs Up to 16 servo + 16 virtual @ 1ms Up to 32 servo + 32 virtual @ 2ms Up to 64 servo + 64 virtual @ 4ms
Cam/Gear Cascade Depth	Up to 4
Axes Group Count	Up to 16 axes groups Up to 32 axes per group
PROFINET System	
VendorID	0x0111
DeviceID	0x0368
Specification	Version 2.3
PROFINET-capable ports	X3/X4 (licensable)
Controller	yes
- Max. number of devices	64@16ms, 32@8ms, 16@4ms, 8@2ms, 4@1ms
- Cycle time	1 ms .. 512 ms

Continued on next page.

Continued from previous page.

Order no.	JEYRM-MPX022SE10L32-2
- System Redundancy	yes
- Fast Startup	yes
- Fast Startup, Max. number of devices	32
- Topology	yes
Device	yes
- Device I/O Data	512 Byte / 512 Byte
- Cycle time	1 ms … 512 ms
- MRP Client supported	yes
Housing	
Material	PPE
Mounting	Profile rail 35mm　(Height 15mm)
Mechanical data	
Dimensions (WxHxD)	70 mm x 130 mm x 130 mm
Net weight	0.6 kg
Weight including accessories	0.62 kg
Gross weight	1.90 kg
Environmental conditions	
Operating temperature	0 °C to 60 °C
Storage temperature	-40 °C to 70 °C
Certifications	
UL certification	Yes
KC certification	-
UKCA certification	Yes
ChinaRoHS certification	Yes

4

Deployment CPU iC9226M-FSoE

4.1 Safety Instructions

⚠ WARNING

Depending on the application, improper use of the CPU can pose serious risks to the user

When handling the CPU, observe all safety instructions listed in this chapter.

Avoid danger - outputs can be set

- **Take appropriate measures to ensure that there is no danger from your plant/machine.**
- **In the "DEBUG-RUN" state, variables can be overwritten. These are then also transmitted to the FSoE output devices and output.**
- **Do not automatically acknowledge an operator acknowledge request from the user program. The acknowledgment must be triggered by a conscious user action.**
- **If you reintegrate passivated FSoE participants, safety-related outputs can be set! Take appropriate measures to ensure that your plant/machine is not at risk when passivated FSoE participants are reintegrated.**

Loss of electrical safety and safety function when using unsuitable power supplies

The CPU is designed exclusively for operation with protective extra-low voltage (PELV) according to EN 60204-1. Only protective extra-low voltages in accordance with the specified standard may be used for supply. The following applies to the network (FSoE and System SLIO) and the I/O devices used within it:

- **Only use power supplies that comply with EN 61204, with safe isolation with PELV voltage according to IEC 61010-2-201 (PELV). In these, a short circuit between the primary and secondary sides is excluded.**

NOTICE

The checklists listed in the appendix serve to support planning, assembly and electrical installation, commissioning and parametrization as well as validation of the safety CPU and the FSoE system.

Note that each F address must be unique within a network and overlaps are not permitted.

The value specified in iCube Engineer under [Watchdog] must not exceed TI/TO_{FSoEWD_MAX} *4.12.3 Maximum Permitted Watchdog Times on page 140* from *4.12 Response Times on page 138*!

The CPU is not suitable for applications that require increased availability, as operation will be stopped in the event of a fault.

The IP20 (IEC 60529/EN 60529) protection class of the CPU is intended for a clean and dry environment.

- **Do not subject the CPU to mechanical and/or thermal stress that exceeds the limits described.**
- **Please note that you must install the CPU in a lockable housing or a lockable control cabinet with at least protection class IP54 for proper operation.**

Incorrect use may cause property damage.

The CPU contains components that can be damaged or destroyed by electrostatic discharge.

- **When handling the CPU, observe the necessary safety measures against electrostatic discharge (ESD) in accordance with EN 61340-5-1 and IEC 61340-5-1.**

Foreign objects in the CPU may lead to malfunctions or even device failure.

- **Make sure that no foreign objects get into the CPU (e.g. into the ventilation openings).**

Operating the CPU outside the permissible ambient temperature range may lead to malfunctions or even device failure.

- **Make sure that the permissible ambient temperature of the CPU is observed during operation of the CPU. *1.17 Approvals, Directives, Standards on page 34***

NOTICE

Operating the CPU above the permissible vibration and shock specifications may result in malfunctions or even device failure.

- **Make sure that the permissible specifications for vibration and shock are observed during operation of the CPU.** ***1.17 Approvals, Directives, Standards on page 34***

Reversing the polarity puts a strain on the electronics and can lead to a defect in the CPU.

- **To protect the CPU, avoid reversing the polarity of the DC 24V supply.**

4.2 Mounting

Information More information on mounting and wiring *2 Basics and Mounting on page 39*.

4.3 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. *5 Web-Based Management - WBM on page 182*
- 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).

4.4 Programming and File System

4.4.1 PLCnext Technology

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

4.4.2 Programming

- The CPU may only be programmed and configured with iCube Engineer according to IEC 61131-3.

Information The scope of the language of the safety function block diagram and the safety function block library can be found in the iCube Engineer documentation.

4.4.3 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].
5.5.2 Firewall on page 208
- Please note that you only have access to the firewall settings as an administrator!

4.4.4 Install iCube Engineer

(1) Installation

The software iCube Engineer is required for commissioning the CPU.

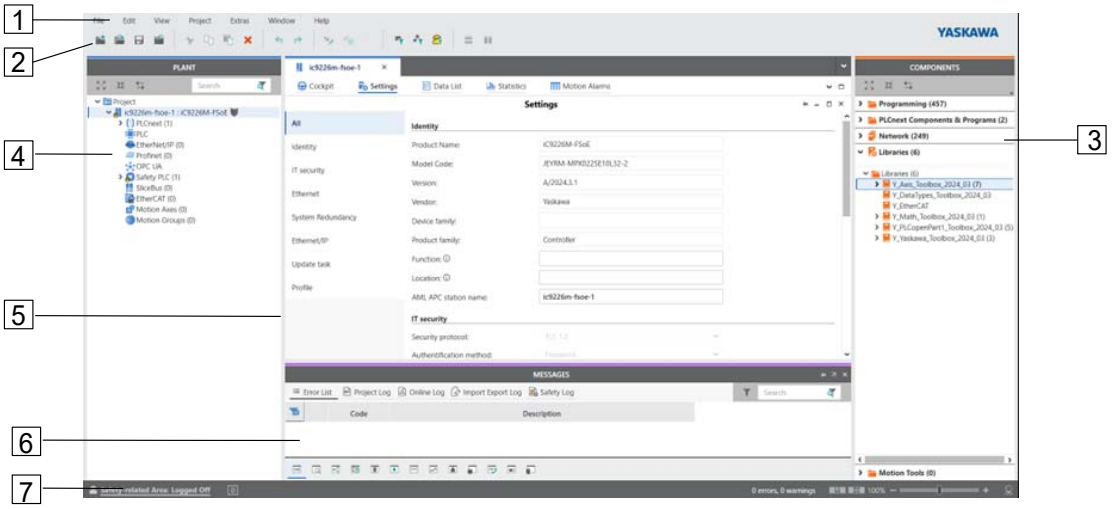
1. **Download the software iCube Engineer to your PC. You can find this at**
2. **https://www.icubecontrol.com/downloads.html**
3. **Unzip the file in your working directory and start the installation by double-clicking on the exe file.**
4. **Follow the instructions of the installation wizard.**

   The installation is started.
5. **When prompted, restart your system.**

   The installation is finished. You can start iCube Engineer now.

4.4.5 iCube Engineer User Interface

(1) Overview



1 Menu bar

2 Toolbar

3 [Components] area

4 [Plant] area

5 Editor area

6 Cross-functional area

7 Status bar

(2) Menu Bar

The menu bar provides access to a number of project-related commands that do not explicitly relate to a specific engineering task.

(3) Toolbar

The menu bar provides access to a number of project-related commands that do not explicitly relate to a specific engineering task. In addition, the various areas and editors have their own specific toolbars.

(4) [Components] Area

The [Components] area contains all components available for the project. The components can be divided into the following types based on their function:

- Develop program code (data types, programs, functions and function blocks).
- Show or add all devices available for the [Plant] area.
- Insert libraries such as firmware libraries, IEC user libraries, etc.

(5) [Plant] Area

In the [Plant] area, you map all the physical and logical components of your application as a hierarchical tree structure.

(6) Editor Area

- Double-clicking on a node in the [Plant] area or on an element in the [Components] area opens the associated editor group in the editor area.
- Editor groups are always shown in the center of the user interface.
- Each editor group contains several editors, which can be opened and closed using buttons in the editor group.
- You can identify the corresponding editor based on the color representation of the editor group:
  - Blue: Editor from the area [Plant].
  - Orange: Editor from the area [Components].

(7) Cross-Functional Area

The cross-functional area contains functions that extend across your entire project.

- ERROR LIST
  - All errors, warnings and messages of the current project are shown here.
- GLOBAL FIND AND REPLACE
  - Here you can find and replace text in the project.
- CROSS REFERENCES
  - All cross references within the project are shown here, such as the use and declaration of all variable types.
- WATCH WINDOW
  - Debug tool - the current values of the added variables are shown here in online mode.
- BREAKPOINTS
  - Debug tool - here you can set and reset breakpoints for troubleshooting.
- CALL STACKS
  - Debug tool - the sequence of calls when the code is executed is shown here and commands for debugging with breakpoints are made available.
- LOGIC ANALYSIS
  - Here variable values can be recorded and visualized during runtime.
- PROTOCOL
  - All errors, warnings and messages are output here.
    [Online]: Messages from the runtime environment as well as other errors and warnings relating to online communication.
  - [Engineering]: Non-project-related messages about events that affect the software such as device files GSDML etc.
- RECYCLE BIN
  - Items that you have recently deleted from the [Plant] or [Components] areas are moved to the recycle bin.
  - If necessary, you can restore deleted items.

(8) Status Bar

Detected errors and warnings are shown here. In addition, you have a zoom function here for graphical applications.

4.4.6 Create a New Project

(1) Proceeding

NOTICE

The parametrization of the safety parameters is secured by a safety password, which you must assign when creating a project with safety components. Ensure that the safety password is appropriately protected and only pass on the safety password to authorized personnel!

1. **Start iCube Engineer.**
2. **Click on [New project ...] or open a project template from the left side and proceed with step 4**

   The iCube Engineer user interface is opens.
3. **At [Components] select the corresponding safety CPU and drag&drop it onto the [Plant] [Project].**

   To access the safety-related area, you must now assign a safety password.

   - Use strong passwords consisting of upper/lower case, numbers and special characters.
   - The use of a password generator or manager is recommended.
   - The password in the templates of iCube Engineer is "safety".

   Once the password is assigned, the CPU is added to your project.
4. **Save your project via [File] - [Save as]. Assign a meaningful name for your project and close the dialog with [Save].**

4.4.7 Parametrization of the Safety Parameters

(1) Safety Instructions

NOTICE

There is a memory area on the CPU for safety variable assignments. Please take the following limitations into account:

- **Each safety variable assignment, which is mapped into the process data, occupies 16 bytes.**
- **Each variable assignment, which is mapped into the process data, occupies 8 bytes.**
- **The total of all variable assignments, which are mapped into the process data, must not exceed 19980 bytes.**

Please note that the [FSoE device address] or [F address] of the local and Ethernet-connected safety modules is unique and may only be assigned once!

The parametrization of the safe parameters is protected by a safety password, which you specified when creating the project. Ensure that the safety password is appropriately protected and only pass on the safety password to authorized personnel!

Please note that the safety CPU generally supports 2-channel safety functions. When designing the safety functions, take into account how far the connected safety components provide 2-channel safety functions. There is no information about this in the safety CPU. More information can be found in the corresponding manufacturer documentation of the safety component.

Information 2-channel capability is required to achieve SIL3/Cat.4/PLe. For SIL2/Cat.3/PLd, 1 channel is sufficient. Please consider the specifications for the test rate and request rate. Further information can be found in the corresponding manufacturer documentation for the safety component.

Information If a connected safety component only provides 1-channel safety functions, you can use the [SF_Antivalent...] and [SF_Equivalent...] handling blocks to generate a 2-channel signal from two 1-channel signals. The blocks can be found in the [SF Library], which must be installed if necessary. Information on using the blocks can be found in the corresponding online help.

(2) Preparation

Carry out the hardware configuration of your system by double-clicking on the corresponding component in your project under [Plant] and selecting the relevant [Typ] in the editor. Select your safety modules in the same way.

Information By entering parts of the order number or the module name, you will get a module selection list, which adapts dynamically as you enter.

1. **If available, configure the System SLIO modules, which are connected locally to the backplane bus. To do this, double-click under [Plant] on [SliceBus].**
   The [SliceBus] editor opens. Here at [Type] you can specify the module for the corresponding slot.
2. **To configure your EtherCAT FSoE system, double-click under [Plant] on [EtherCAT].**
   The editor [EtherCAT] - [Device list] opens.
3. **Select the corresponding EtherCAT coupler.**
   At [Plant] - [EtherCAT] the corresponding EtherCAT coupler is created.
4. **Double-click at [Plant] - [EtherCAT] on the newly created EtherCAT coupler.**
   The [Module list] editor opens. Here at [Type] you can specify the module for the corresponding slot.

(3) Parametrization

(a) Switching the Language

Information Please note that due to the system, the parametrization of the safety parameters is only possible in the English language view.

1. **To switch languages, open in iCube Engineer via [Extras] - [Options] the options dialog.**
2. **Under [International], select [English] as language.**
3. **Save your project and restart iCube Engineer with your project.**

(b) Setting of the F-address

NOTICE

Please note that the [FSoE device address] or [F address] of the local and Ethernet-connected safety modules is unique and may only be assigned once!

1. **Set the F-address at the F device. For more information on the procedure, please refer to the corresponding documentation.**
2. **Start iCube Engineer with your project.**
3. **At Plant, navigate to your F device.**
4. **Double-click on the corresponding F device in your project.**
   The [Safety Parameters] editor opens.
5. **After requesting the password for the safety area, enter the F address that you have set on your F device at [FSoE device address].**

(c) Setting the Safety Parameters

1. **At [Safety parameters], you can set the required safety parameters that are provided by the F device.**
2. **Save and transfer your project to the safety CPU.**

Information For more information on the procedures, refer to *4.13 Sample Application on page 144*.

4.4.8 Assigning Safety Process Data

NOTICE

When wiring sensors and actuators, ensure that:

- **the correct safety-related sensors and actuators are correctly connected.**
- **the parametrization of the inputs and outputs as well of all devices respectively modules is correct.**
- **the linking of the block inputs and outputs with the signals of the safety-related sensors respectively actuators is correct on 1/2 channels.**
- **cross-circuit and line break monitoring is implemented in your application if required.**
- **all safety-related function blocks and functions in the safety-related code are connected correctly.**

Information Further information on the parametrization of inputs and outputs as well as all devices or modules can be found in the device-specific user documentation.

Information The detailed procedure for I/O assignment of process data is described in the application example. *4.13 Sample Application on page 144*

4.5 Commissioning

4.5.1 Notes on Commissioning

⚠ WARNING

Prevent automatic start-up

- **Take appropriate measures to ensure that automatic start-up of your plant/machine is prevented.**

Avoid danger during commissioning

- **Take appropriate measures to ensure that there is no danger from your plant/machine during commissioning and validation.**

Safety function only ensured after validation

- **The planned safety function of the plant/machine is only ensured after validation.**

Organizational or technical measures required for compensation of the CRC checksum

Take technical or organisational measures to ensure that the correct project for the application is started in the CPU by comparing the CRC checksum:
4.5.4 Comparison of the Checksums on page 127

- **After transferring a project to the CPU.**
- **After removing the SD card.**
- **After inserting or changing the SD card.**

If you use a technical measure to check the CRC checksum, it must be implemented in such a way that the check done by a third technical instance outside the safety CPU.

Safety and availability of the plant/machine

- **Ensure the safety and availability of your plant/machine by selecting the appropriate watchdog time FSoE_WD_Time.**
- **Select the watchdog time high enough so that the safety of your plant/machine is still guaranteed with the highest possible availability.**

Avoid danger caused by triggering the safety function too late

- **Ensure that the maximum permissible values TI_{FSoEWD_MAX} and TO_{FSoEWD_MAX} are not exceeded.** ***4.12.3 Maximum Permitted Watchdog Times on page 140***

Debug operation

- **Switching to debug operation means leaving normal operation.**
- **Make sure that your plant/machine does not pose any danger to people during debug operation and that no damage can be caused.**

NOTICE

Make sure that commissioning only takes place after the CPU and the associated modules have acclimatized!

Improper handling may lead to damage.

- **Handle the CPU and components with care!**
- **When installing the CPU and components, ensure that mechanical damage is avoided!**

To ensure that the CPU starts up properly, the supply voltage must not be switched on until at least 30 seconds after the device LEDs go out.

In the commissioning phase, the values for program runtime and cycle time determined offline in the planning phase must be verified online.

Information Always take the associated checklist into account when commissioning.

Information Operation and programming may only be carried out by qualified personnel!

Information Operation and programming may only be carried out via iCube Engineer!

Information Ensure that a PC system with running iCube Engineer is always available during the entire time of operation! Otherwise, no later modifications can be done.

Information Ensure legally compliant documentation and archiving of your engineering project!

(1) Notes on Initial Commissioning

⚠ WARNING

Safety-related steps

The following steps include safety-related activities in the iCube Engineer software and the safety validation of the FSoE system.

- **Please also note the checklists listed in the appendix for the following steps.**
- **Please also refer to the online help of the iCube Engineer.**

Carry out verification in accordance with safety standards

- **For all steps in creating the security program for your application, carry out verification in accordance with the security standards applicable to your application.**

NOTICE

Access to the SD card is possible so that data can be read and manipulated.

- **Please note *1.7.2 Notes on Security on page 22*, especially with regard to access protection for the SD card.**

4.5.2 Online Access to the CPU

(1) IP Address Parameters for Communication

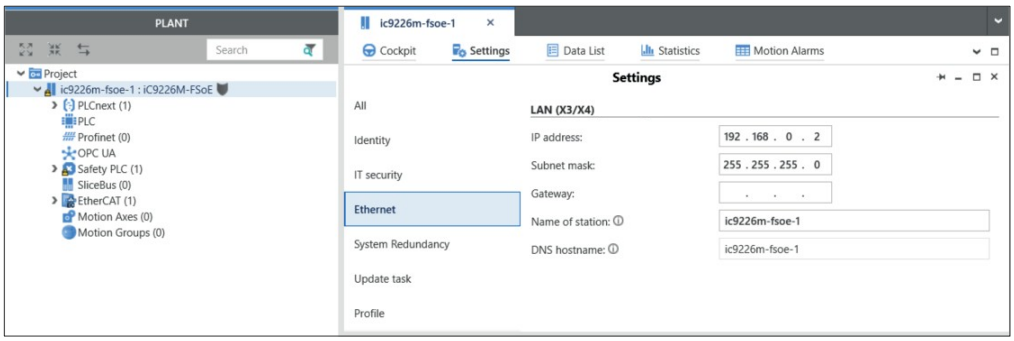
On delivery the following IP address parameters for the communication are preset in the project template of the CPU:

- 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 via the following procedure:

1. **Open your project.**
2. **In the [Plant] area, double-click the CPU node**
   The CPU editor group opens.
3. **Select the [Settings] editor.**

4. **Select the [Ethernet] view.**



5.

- At [LAN (X3/X4)] the IP address parameters for the connection via the Ethernet-Port (X3/X4) can be set.

When establishing an Ethernet connection to the CPU, the IP address parameters specified here are used by iCube Engineer for the corresponding interface.

(2) Connecting to the CPU

Information Please note that the online search is currently only supported by port X3/X4!

Connect port X3 or X4 to the Ethernet interface of your PC. Please note that for communication via iCube Engineer the network card of the PC and the Ethernet interface of the CPU are in the same IP circle. If necessary, contact your network administrator.

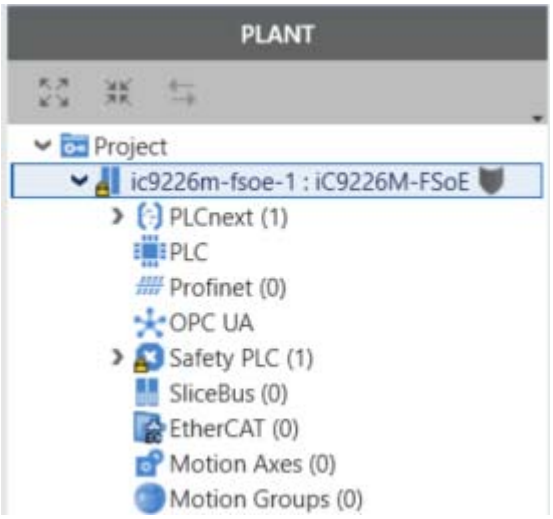
1. **Open your project.**
2. **In the editor group of the CPU, select the editor [Cockpit].**
3. **Set the interface [LAN (X3/X4)] and click on**  **.**

A connection between iCube Engineer and your CPU is established, by means of the IP address parameters, and the login dialog for authentication is opened.

4. **Enter your login details and click on**  **.**

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.

Now you can access your CPU. An existing connection is shown in the Plant area at the node of the CPU by  .



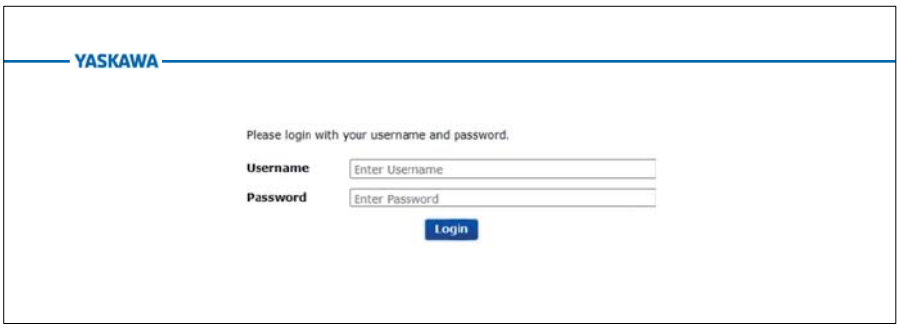
(3) Assigning New IP Address Parameters

(a) Assignment via WBM

As soon as you are online connected to the CPU, you can assign new IP address parameters to it via WBM (Web-based management).

1. **To access WBM, click in the [Cockpit] editor at**  **.**

The WBM login page opens.



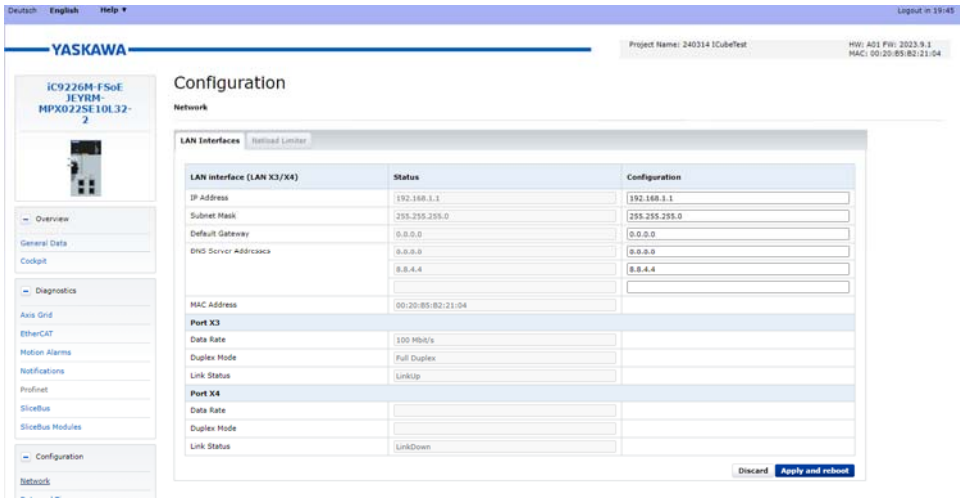
2. **Enter your login details and click on [Login].**

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.

3. **Navigate to Network in the Configuration area.**

Here you can change the current IP address parameters in the [Configuration] column.



4. **Enter your new IP address parameters in the [Configuration] column.**

> **⚠ CAUTION**
>
> **When assigning the IP address parameters, please note that the number ranges of the IP addresses of X3 and X4 must not overlap if they exist!**

5. **Click on [Apply and Reboot].**

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

   Information The CPU can now only be reached via the new IP address parameters. Please note that these new data are currently not automatically transferred in the settings of iCube Engineer. You have to manually adjust these in the settings there.

4.5.3 Validation of the System

(1) General

With the first commissioning all the safety functions and the proper functionality of the programmed and installed system must be checked. And the check of the system must be documented.

> **⚠ WARNING**
>
> **Danger with commissioning!**
>
> **The control system may be operated only after successful testing by a competent person.**
>
> - **Perform a complete functional test and check the correct assignment of the connected safety components.**
> - **Validate the system according to the commissioning, parameterisation and validation checklist and document the process.**
> - **Make sure that the service personnel is trained in the handling of the control system.**

(2) Functional Test

(a) Overview

The functional test is an essential part of the validation of the entire system. The functional test can be used to determine the correct assignment of the network's safety components and the programmed logic of the system. Depending on the complexity of the linking logic of the respective project, it is recommended to make graduated functional tests. The following procedure is recommended for functional tests:

- Only connect the actuators and drives to the safety output terminals when no faults have been detected during the wiring check.
- Make a complete I/O test. This means that you set each sensor to all of its possible switching states one by one (usually on and off, or actuated not actuated).
  - Check whether the specified and expected signal state corresponds to the real state.
  - In addition, check whether the assigned variable status also changes accordingly in the connected safety PLC.
  - The same procedure must be followed when controlling the actuators via the safety output modules. Here too, every process state specified in the safety application must be tested.
- Examine a fully functional test with the entire sensors (initiators), switches, actuators and drives.
- Document the result of the functional test.
- For the functional test, trigger all safety functions in sequence and document the reaction of the system. Check whether the reaction corresponds to the expected behavior.

In the iCube Engineer, the following functions support you during the function test:

- Monitoring mode
- Debug mode

Information You will find more information in the online help of iCube Engineer.

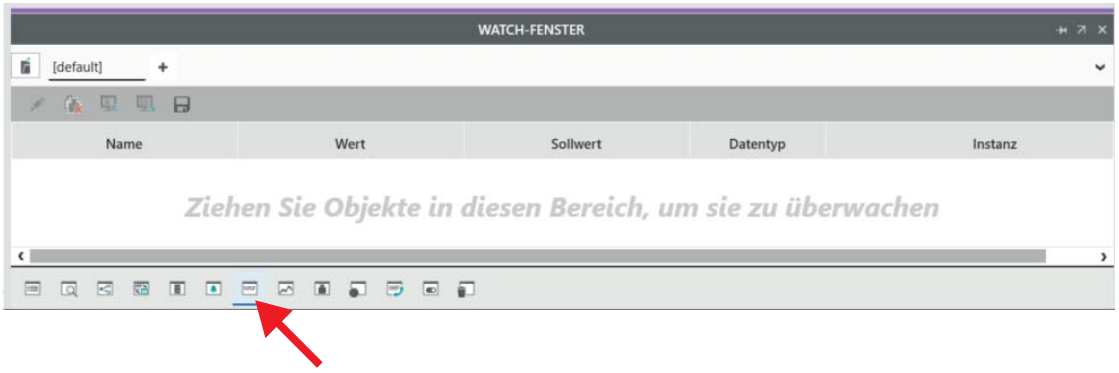
(b) Online access

With online access, a distinction is made between safety-related functionality and standard functionality. Access is controlled by double-clicking on the corresponding node below [Plant]. The cockpit of the safety-related CPU can be accessed via the [Safety PLC] node. The access is protected by the safety password you have assigned.

(c) Monitoring Mode

Information The monitoring mode enables read-only access to the safety-related PLC. Since the execution of the application cannot be influenced by debug commands, the monitoring mode is considered as a safe mode.

1. **Load your project.**
2. **Double-click in the [Plant] area on [Safety PLC] node.**
   The cockpit of the safety PLC is opened.
3. **Go online with your Safety CPU via**  **.**
4. **In the Cross-functional area in the toolbar at the bottom, click on**  **.**



The [Watch window] opens. In the watch window you can collect variables and clearly show and monitor the online values while the application is running. You can create multiple watch lists within the

WATCH window. Each list can be saved and loaded. In addition, the current online value of list elements can be loaded from the control and used as a setpoint.

5. **Drag the variables you want to monitor into the Watch window.**

6. **Activate the monitoring mode with .**

   You now have read access to the variables in your project.

(d) Debug Mode

⚠ DANGER

Unintended operating state of the CPU

In contrast to the monitoring mode, the debug mode also grants write access to the safety-related PLC. Since the execution of the application can be influenced by debug commands, debug mode must be considered as non-safe mode.

- **Ensure that no hazards can arise from intentional or unintentional operations of the safety-related PLC.**
- **Please also refer the *4.5.1 Notes on Commissioning on page 121*.**

1. **Load your project.**
2. **Double-click in the [Plant] area on [SafetyPLC] node.**

   The cockpit of the safety PLC is opened.

3. **Go online with your Safety CPU via .**

4. **Activate debug mode with .**

   You now have the opportunity to debug your user program and control variables. You can use the force function to specify fixed variable values. You can set breakpoints to temporarily stop your user programme.

4.5.4 Comparison of the Checksums

(1) Proceeding

As soon as you place safety components in your project, a checksum is automatically calculated for your safety project. After the project transfer, the checksum of your project and the CPU, which is connected online, must be identical. The checking procedure is as follows:

1. **Establish an online connection to the CPU.**
2. **Double-click on [SafetyPLC].**
3. **Select the [Safety cockpit] editor and click on [Overview].**

   The following checksums must be identical:

   - Checksum CPU: [Safety PLC project information]
   - Checksum Project: [Engineering project information]

4.6 Memory Management

4.6.1 Internal Memory

(1) Overview

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

Memory

- iC9226M-FSoE:
  - 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. *4.7.1 MRESET on page 131*

(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. *4.7.2 Reset to Factory Settings Type 1 on page 131*
- 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. *4.7.3 Reset to Factory Settings Type 2 on page 133*

⚠ 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

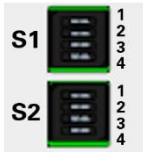
If, during operation or when starting up the CPU, the error indication occurs that the memory of the overlay file system in the parametrization memory has overflowed, the CPU can be restarted via Safe Mode as follows:

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

S1	S1-1	S1-2	S1-3	S1-4	Action
e 	ON	OFF	OFF	OFF	After PowerON the CPU starts in Safe Mode.

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

   The CPU starts in *4.9 Safe Mode on page 135*. 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. Use an SSH client to access the file system and delete the causing files if necessary. Then start in Standard Mode again.**
5. **For this, switch off the power supply to the CPU.**
6. **Set the DIP switches S1 to the default position:**

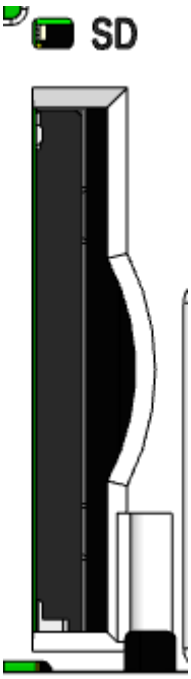
S1	S1-1	S1-2	S1-3	S1-4	Action
	OFF	OFF	OFF	OFF	After PowerON the CPU starts in Standard Mode - default setting.

7. **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.

4.6.2 Slot for Yaskawa SD Card

For future use



4.7 MRESET and Reset to Factory Settings

4.7.1 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.

4.7.2 Reset to Factory Settings Type 1

- 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.

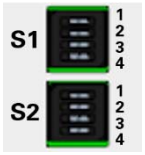
(1) With Operating Mode Switch

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 sup- ply 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-CER (red)**	**PN-DER (red)**	**SD (yellow)**	**EC RUN (green)**	**EC ERR (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) With DIP Switch S1

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

S1	S1-1	S1-2	S1-3	S1-4	Action
	OFF	ON	OFF	OFF	After PowerON the CPU executes a reset to factory settings type 1.

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

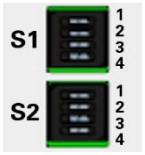
   After the start-up of the CPU it performs a reset to factory setting type 1 and shows the following LED behavior:

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 RUN (green)	EC ERR (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 RUN (green)	EC ERR (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	Not lit	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:**

S1	S1-1	S1-2	S1-3	S1-4	Action
	OFF	OFF	OFF	OFF	After PowerON the CPU starts in Standard Mode - Default setting.

6. **\witch on the power supply of the CPU again.**

   The CPU starts in Standard Mode.

4.7.3 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 RUN (green)**	**EC ERR (red)**	
Not lit	Not lit	Flashing green 2Hz 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.

4.8 Firmware Update

You can update the firmware via the Web-based management WBM. *5.6.2 Firmware Update on page 220*

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

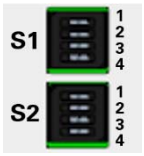
4.9 Safe Mode

4.9.1 Start-Up in Safe Mode

By means of the DIP switch [S1] beneath the front flap you can start your CPU in Safe Mode. This has nothing to do with the functional safety operation. It is only related to the non-safe CPU functionality. 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 DIP switches S1 under the front flap to the following position:**

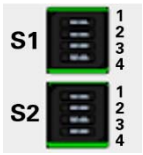
S1	S1-1	S1-2	S1-3	S1-4	Action
	ON	OFF	OFF	OFF	After PowerON the CPU starts in Safe Mode.

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

   The CPU starts in Safe Mode and shows this exclusively during online access.

4.9.2 Start-up in Standard Mode

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

S1	S1-1	S1-2	S1-3	S1-4	Action
	OFF	OFF	OFF	OFF	After PowerON the CPU starts in Standard Mode - Default setting.

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

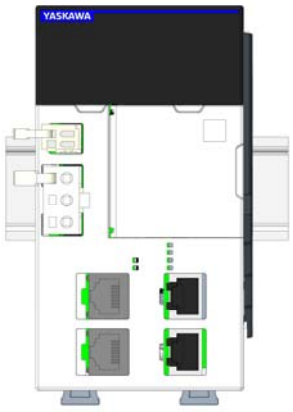
   The CPU starts in Standard Mode again. If a project was loaded in Safe Mode, it is executed in RUN.

4.10 Temperature Behavior

The safety CPU has an integrated temperature monitoring function. The following temperature ranges respectively limits are specified here:

- 0°C to 60°C: Ambient temperature
- < -2°C and > 78°C: Warning limit
- < -7°C and > 83°C: Error limit

4.10.1 Operating Temperature



Do not mount the CPU in any direction other than the specified direction. (see chapter 2.4.1)

4.10.2 Warning Limits

If the temperature falls below -2°C or exceeds 78°C, a warning message is added to the error stack and the log file of the safety CPU.

4.10.3 Error Limit

If the temperature falls below -7°C or exceeds 83°C, the safety CPU switches to the Hard fail safe state.
4.11 Fail Safe States on page 137

4.11 Fail Safe States

4.11.1 Behavior on Error

All detected, serious errors in the CPU that could lead to loss or malfunction of the programmed safety function result in a transition to the safety state (fail safe state). A distinction is made between Soft fail safe and Hard fail safe states. Here the CPU shows different behavior:

- State Soft fail safe
  Behavior
  - The safety outputs of the F devices are set to zero (FALSE).
  - The red SF_ER LED blinks with 1Hz.
  - If you are connected online to the iCube Engineer on error, information about the error is also shown in the software.

  Possible reason
  - Error in parametrization

  Acknowledgement
  - Bug fixing in the project and new upload.
- State Hard fail safe
  Behavior
  - The safety outputs of the F devices are set to zero (FALSE).
  - The red SF_ER LED is on.
  - Communication with the CPU is no longer possible.

  Possible reason
  - Hardware error, exceeding the switch-off thresholds of the temperature limits.

  Acknowledgement
  - Check your hardware setup and perform a power cycle.

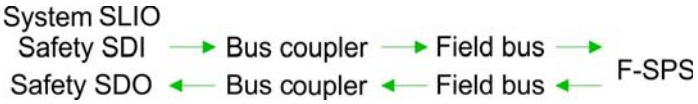
NOTICE

If your CPU is still in the Hard fail safe state after a power cycle and this does not change even after a reset *4.7 MRESET and Reset to Factory Settings on page 131*, please contact the Yaskawa hotline.

4.12 Response Times

4.12.1 There is No Error

Without an error, it is assumed that none of the watchdogs respond and the passage of a signal from the input connector of a safety input module to the output connector of a safety output module is considered:



(1) Maximum Expected Response Time in the Case without Errors

$$T_{maxNF} = TI_{ST} + TI_{WCDT} + TI_{Slave} + TI_{BUS} + T_{CL} + T_{FPROG} + TO_{BUS} + TO_{Slave} + TO_{WCDT}$$

4.12.7 Designations on page 142

4.13.4 Response time example on page 163

T_{maxNF} :

Max. response time without errors (**max N**o

Fault). **TI_{ST} :**

Input smoothing time of the inputs of the safety SDI (**S**moothing **T**ime).

TI/TO_{WCDT} :

Max. response time without errors (**W**orst **C**ase **D**elay

Time). **TI_{Slave} :**

Max. Response time of the local or decentralized periphery system, i.e. delay caused by the FSoE EtherCAT coupler and the backplane bus.
For local periphery this response time is the SliceBus cycle time from iCube Engineer

For decentralized EtherCAT periphery this response time results from EtherCAT cycle time from iCube Engineer + delay time of the slave according to the slave's manual**TI_{BUS} :**

EtherCAT cycle time for EtherCAT bus communication. The EtherCAT cycle time results from the cycle times of all connected EtherCAT slaves + cycle time for the EtherCAT master (this is the EtherCAT cycle time from iCube Engineer).

T_{CL} :

Cycle time of the safety CPU.

T_{FPROG} :

Cycle time safety program.

Table 5.1 For plant design sensor and actuator run times are to be taken into account:

$$T_{maxNFSA} = T_{SensorDLY} + T_{maxNF} + T_{ActuatorDLY}$$

4.12.7 Designations on page 142

4.13.4 Response time example on page 163

$T_{maxNFSA}$:

Max. response time without errors with sensor and actuator (**max N**o **F**ault **S**ensor **A**ctuator).

$T_{SensorDLY}$:

Delay time of the sensor (**S**ensor

De**L**a**Y**). **T_{maxNF} :**

Max. response time without errors (**max N**o

Fault). **$T_{ActuatorDLY}$:**

Delay time of the actuator (**A**ctuator **D**e**L**a**Y**).

You find an response time example in chapter 4.13.4.

4.12.2 There Is an Error

(1) Possible Single Errors

On error, it is assumed that a watchdog responds and triggers the corresponding error response. Possible causes include errors in the system, incorrect runtime information in the documentation of the standard system or anextension of the runtime beyond the value used in the calculation by changing the configuration of the standard system. The total response time in the error-free case increases by the maximum duration of the possible single errors:

- Discrepancy error in safety SDI. Here, the discrepancy time must also be taken into account: (TI_{DIS})
- A single error occurs in the safety SDI. Here the possibly larger max. response time during an error (TI_{OFDT}) is to be considered with the max. response time in error free case (TI_{WCDT}): (TI_{OFDT} - TI_{WCDT})
- Once or permanent interrupted communication between safety SDI and the safety CPU. The FSoE watchdog time of the Safety SDI and the configured cycle time of the PLC must be considered: (TI_{FSoEWD} + T_{CL})
- Once or permanent interrupted communication between safety SDO and the safety CPU or failure of the safety CPU. Here the watchdog time of the safety SDO and acknowledge time of the safety SDO must be considered: (TO_{FSoEWD} + TO_{DAT})
- A single error occurs in the safety SDO. Here the possibly larger max. response time during an error (TO_{OFDT}) is to be considered with the max. response time in error free case (TO_{WCDT}): (TO_{OFDT} - TO_{WCDT})

(2) Max. Response Time on Error

$$T_{maxOF} = T_{maxNF} + MAX((TI_{DIS}), (TI_{OFDT} - TI_{WCDT}), (TI_{FSoEWD} + T_{CL}), (TO_{FSoEWD} + TO_{DAT}), (TO_{OFDT} - TO_{WCDT}))$$

4.12.7 Designations on page 142

T_{maxOF} :

Max. response time on error (**max** **O**ne **F**ault).

T_{maxNF} :

Max. response time without errors (**max** **N**o **F**ault).

TI_{DIS} :

With 2-channel evaluation discrepancy time, otherwise 0 (**DIS**crepancy).

TI/TO_{OFDT} :

Max. response time on error (**O**ne **F**ault **D**elay **T**ime).

TI/TO_{WCDT} :

Max. response time without errors (**W**orst **C**ase **D**elay **T**ime).

TI/TO_{FSoEWD} :

Configured FSoE watchdog time (**FSoE** **W**atch**D**og).

T_{CL} :

Cycle time of the safety CPU.

TO_{DAT} :

Max. acknowledgement time (**D**evice **A**cknowledgement **T**ime).

Table 5.2 For plant design sensor and actuator run times are to be taken into account:

$$T_{maxOFSA} = T_{SensorDLY} + T_{maxOF} + T_{ActuatorDLY}$$

4.12.7 Designations on page 142

$T_{maxOFSA}$:

Max. response time on error with sensor and actuator (**max** **O**ne **F**ault **S**ensor**A**ctuator).

$T_{SensorDLY}$:

Delay time of the sensor (**S**ensor **D**e**L**a**Y**).

T_{maxOF} :

Max. response time on error (**max** **O**ne **F**ault).

$T_{ActuatorDLY}$:

Delay time of the actuator (**A**ctuator **D**e**L**a**Y**).

4.12.3 Maximum Permitted Watchdog Times

(1) Dimensioning

Table 5.4 The following formula applies for dimensioning TI/TO_{FSoEWD_MAX} in the FSoE system:

$TI_{FSoEWD\_MAX} + TO_{FSoEWD\_MAX} \geq T_{maxRTSA} - TI_{WCDT} - TO_{WCDT}$

4.12.7 Designations on page 142

TI/TO_{FSoEWD_MAX} :

Maximum permitted FSoE watchdog time (**FSoE W**atch**D**og **MAX**imum).

$T_{maxRTSA}$:

Max. response time on error with max. runtime with sensor and actuator (**max R**un**T**ime **S**ensor **A**ctuator).

TI/TO_{WCDT} :

Max. response time without errors (**W**orst **C**ase **D**elay **T**ime).

Information Based on the information in the device-specific user documentation of the F devices, consider whether further information on watchdog times is available within the internal device function.

Timer functions that are used in the safety-related application programme within the safety function must also be taken into account for the calculation.

Information You can find more information on calculating and optimizing the watchdog time in the documentation of the iCube Engineer.

4.12.4 Variable Runtimes for Single Errors

(1) Times to Be Considered

At variable run times of the standard system in addition to an existing error, it is assumed that the values of all the relevant run times are nearby the limit of the monitored times.

- The max. processing time to and in the safety SDI: ($TI_{ST} + TI_{DIS} + TI_{WCDT} + TI_{FSoEWD}$)
- The smallest of the possible monitoring times, from this moment the defined behaviour of an error takes effect: (MIN (TI_{FSoEWD}, T_{CL_MAX}, TO_{FSoEWD}))
- The max. processing time to and in the safety SDO: ($TO_{WCDT} + TO_{FSoEWD}$)
- The possibly increased processing times in case of an error within the safety modules, here only the larger of them, because it is assumed that there is a single error: (MAX (($TI_{OFDT} - TI_{WCDT}$), ($TO_{OFDT} - TO_{WCDT}$)))
- For the entire process chain a good FSoE telegram could be sent just before to the safety SDI or SDO. Here the largest of the two timeouts must be considered: (MAX (TI_{FSoEWD}, TO_{FSoEWD}))

(2) Max. Response Time for Any Run Time at One Error

$$T_{maxRT} = TI_{ST} + TI_{DIS} + TI_{WCDT} + TI_{FSoEWD} + MIN\ (TI_{FSoEWD}, T_{CL\_MAX}, TO_{FSoEWD}) + TO_{WCDT} + TO_{FSoEWD} + MAX\ ((TI_{OFDT} - TI_{WCDT}), (TO_{OFDT} - TO_{WCDT})) + MAX\ (TI_{FSoEWD}, TO_{FSoEWD})$$

4.12.7 Designations on page 142

T_{maxRT} :

Max. response time on error with max. runtime (**max R**un**T**ime). **TI_{ST} :**

Input smoothing time of the inputs of the safety SDI (**S**moothing **T**ime).

TI_{DIS} :

With 2-channel evaluation discrepancy time, otherwise 0 (**DIS**crepancy).

TI/TO$_{WCDT}$:

Max. response time without errors (**W**orst **C**ase **D**elay **T**ime).

TI/TO$_{FSoEWD}$:

Configured FSoE watchdog time (**FSoE W**atch**D**og).

T$_{CL_MAX}$:

Cycle monitoring time of the safety CPU.

TI/TO$_{OFDT}$:

Max. response time on error (**O**ne **F**ault **D**elay **T**ime).

Table 5.3 For plant design sensor and actuator run times are to be taken into account:

$T_{maxRTSA} = T_{SensorDLY} + T_{maxRT} + T_{ActuatorDLY}$

4.12.7 Designations on page 142

T$_{maxRTSA}$:

Max. response time on error with max. runtime with sensor and actuator (**max R**un**T**ime **S**ensor **A**ctuator).

T$_{SensorDLY}$:

Delay time of the sensor (**S**ensor **D**e**L**a**Y**).

T$_{maxRT}$:

Max. response time on error with max. runtime (**max R**un**T**ime).

T$_{ActuatorDLY}$: Delay time of the actuator (**A**ctuator **D**e**L**a**Y**).

4.12.5 Cycle Time T$_{CL}$ Safety CPU

(1) Dimensioning

iCube Engineer:

Table 5.5 The following formula applies to the cycle time:

$T_{CL} = T_{FPROG} / 0.7$

T_{FPROG} is to be estimated. The following specifications for totalization apply:

- Add 70µs per F device.
- Add 20µs per safety-related function block instances.

In iCube Engineer, the value is to be specified at [Plant] - [Safety PLC]: [Tasks and Events] - [Intervall] in the range of 5 ... 15ms.

4.12.7 Designations on page 142

T$_{CL}$:

Cycle time of the safety CPU.

T$_{FPROG}$:

Cycle time safety program.

4.12.6 Cycle Monitoring Time T$_{CL_MAX}$ Safety CPU

(1) Dimensioning

Table 5.6 The following formula applies to the cycle monitoring time:

$T_{CL\_MAX} \geq T_{FPROG} / 0.7$

T_{FPROG} is to be estimated. The following specifications for totalization apply:

- Add 70µs per F device.
- Add 20µs per safety-related function block instances.

In iCube Engineer, the value is to be specified at [Plant] - [Safety PLC]: [Tasks and Events] - [Watchdog].

4.12.7 Designations on page 142

T_{CL_MAX} :

Cycle monitoring time of the safety CPU.

T_{FPROG} :

Cycle time safety program.

4.12.7 Designations

Table 5.7 Abbreviations sorted by components

Component	Time[1]	Description	Where from
Sensor	$T_{SensorDLY}$	Delay time of the sensor (**S**ensor **D**e**L**a**Y**).	Documentation of the sensor.
Safety SDI	TI_{ST}	Input smoothing time of the inputs of the safety SDI (**S**moothing **T**ime).	Configuration of the F periphery, adapted to the sensor used.
Safety SDI	TI_{DIS}	With 2-channel evaluation discrepancy time, otherwise 0 (**DIS**crepancy).	Configuration of the F periphery, adapted to the sensor used.
Safety SDI Safety SDO	TI_{WCDT} TO_{WCDT}	Max. response time without errors (**W**orst **C**ase **D**elay **T**ime).	Documentation safety module.
Safety SDI Safety SDO	TI_{OFDT} TO_{OFDT}	Max. response time on error (**O**ne **F**ault **D**elay **T**ime).	Documentation safety module.
Safety SDI Safety SDO	TI_{DAT} TO_{DAT}	Max. acknowledgement time (**D**evice **A**cknowledgement **T**ime).	Documentation safety module.
Safety SDI Safety SDO	TI_{FSoEWD} TO_{FSoEWD}	Configured FSoE watchdog time (**FSoE W**atch**D**og).	Documentation safety module.
Safety SDI Safety SDO	TI_{FSoEWD_MAX} TO_{FSoEWD_MAX}	Maximum permitted FSoE watchdog time (**FSoE W**atch**D**og **MAX**imum).	see formula
Bus coupler	TI_{Slave} TO_{Slave}	Max. Response time of the decentralised periphery system, i.e. delay caused by the FSoE EtherCAT coupler and the back-plane bus.	Documentation FSoE EtherCAT coupler
EtherCAT field bus	TI_{BUS} TO_{BUS}	EtherCAT cycle time for EtherCAT bus communication. The EtherCAT cycle time results from the cycle times of all connected EtherCAT slaves.	EtherCAT slave documentation iCube Engineer: Value is to be specified at: [Plant] - [EtherCAT]: [Settings] - [Cycle time]
F-PLC / F-Logic	T_{CL}	Cycle time of the safety CPU. $T_{CL} = T_{FPROG}/0.7$	iCube Engineer: Value to be specified at [Plant] - [Safety PLC]: [Tasks and Events] - [Intervall] in the range of 5 ... 15ms.
F-PLC / F-Logic	T_{CL_MAX}	Cycle monitoring time of the safety CPU. $T_{CL\_MAX} \geq T_{FPROG}/0.7$	iCube Engineer: Value to be specified at [Plant] - [Safety PLC]: [Tasks and Events] - [Watchdog].
F-PLC / F-Logic	T_{FPROG}	Cycle time safety program. This value must be estimated. The following specifications for totalization apply: • Add 70µs per F device. • Add 20µs per safety-related function block instances.	Value is estimated.
Actuator	$T_{ActuatorDLY}$	Delay time of the actuator.	Documentation of the actuator

Continued on next page.

Continued from previous page.

Component	Time[1]	Description	Where from
Total Input to output	T_{maxNF}	Max. response time without errors (**max N**o **F**ault).	See formula
Total Sensor to actuator	$T_{maxNFSA}$	Max. response time without errors with sensor and actuator (**max N**o **F**ault **S**ensor **A**ctuator).	See formula
Total Input to output	T_{maxOF}	Max. response time on error (**max O**ne **F**ault).	See formula
Total Sensor to actuator	$T_{maxOFSA}$	Max. response time on error with sensor and actuator (**max O**ne **F**ault **S**ensor**A**ctuator).	See formula
Total Input to output	T_{maxRT}	Max. response time on error with max. runtime (**max R**un**T**ime).	See formula
Total Sensor to actuator	$T_{maxRTSA}$	Max. response time on error with max. runtime with sensor and actuator (**max R**un**T**ime **S**ensor **A**ctuator).	See formula

1) "I" or "O" after the "T" represent input or output.

4.13 Sample Application

4.13.1 Precondition

(1) Hardware and Software

This application example describes the use of the iC9226M-FSoE via EtherCAT. The following hardware and software is required for the application example:

Hardware	Device / module	Designation / order number
Central unit	iCube CPU with integrated EtherCAT (FSoE) safety Master	iC9226M-FSoE
Local SLIO modules	System SLIO DI	SM 021 (021-1BF00)
	System SLIO DO	SM 021 (022-1BF00)
	System SLIO Safety DI	SM 021 (021-1SD10)
	System SLIO Safety DO	SM 022 (022-1SD10)
EtherCAT slave system	System SLIO bus coupler	IM 053EC Slave (053-1EC01)
	System SLIO DI	SM 021 (021-1BF00)
	System SLIO DO	SM 022 (022-1BF00)
	System SLIO safety DI	SM 021 (021-1SD10)
	System SLIO safety DO	SM 022 (022-1SD10)
Software	**Function**	
iCube Engineer	iCube Engineer supports the programming and configuration of PLCs of the iC9200 Series generation and their FSoE variants.	

(2) F Addresses

Before installing the following modules, set the corresponding F address using the DIP switch:

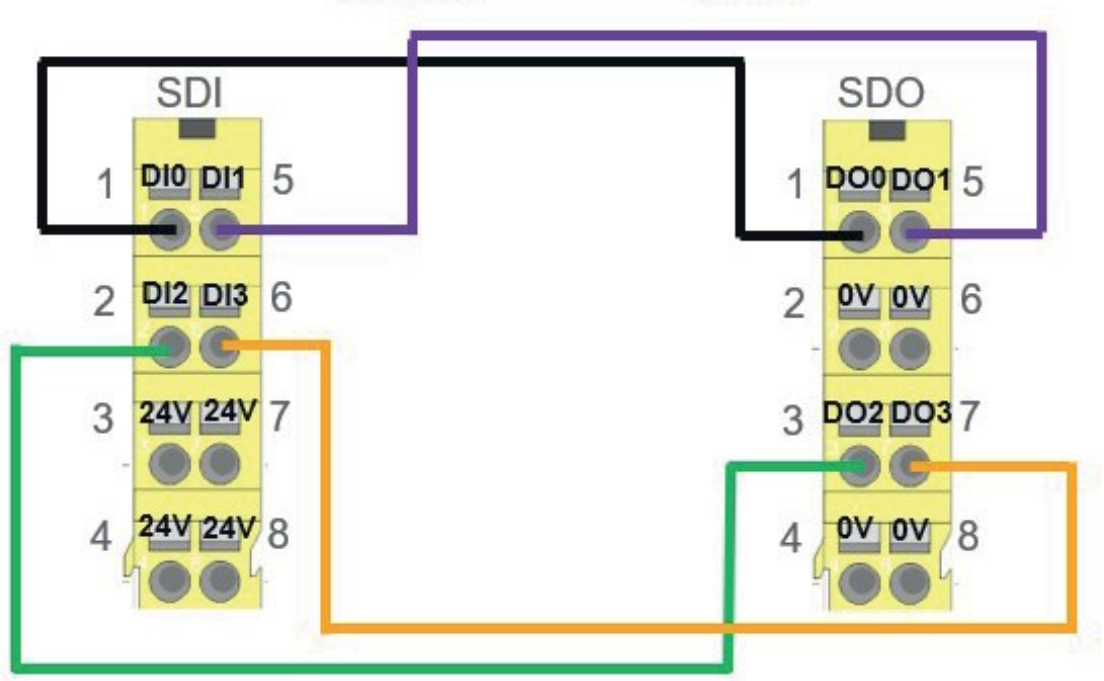
Module	F address decimal	Switch setting
System SLIO DI local	1	0000 0000 0001
System SLIO DO local	2	0000 0000 0010
System SLIO DI EtherCAT	3	0000 0000 0011
System SLIO DO EtherCAT	4	0000 0000 0100

NOTICE

Please note that the [FSoE device address] or [F address] of the local and Ethernet-connected safety modules is unique and may only be assigned once!

(3) Wiring FSoE Modules

Wire the FSoE modules as shown below:

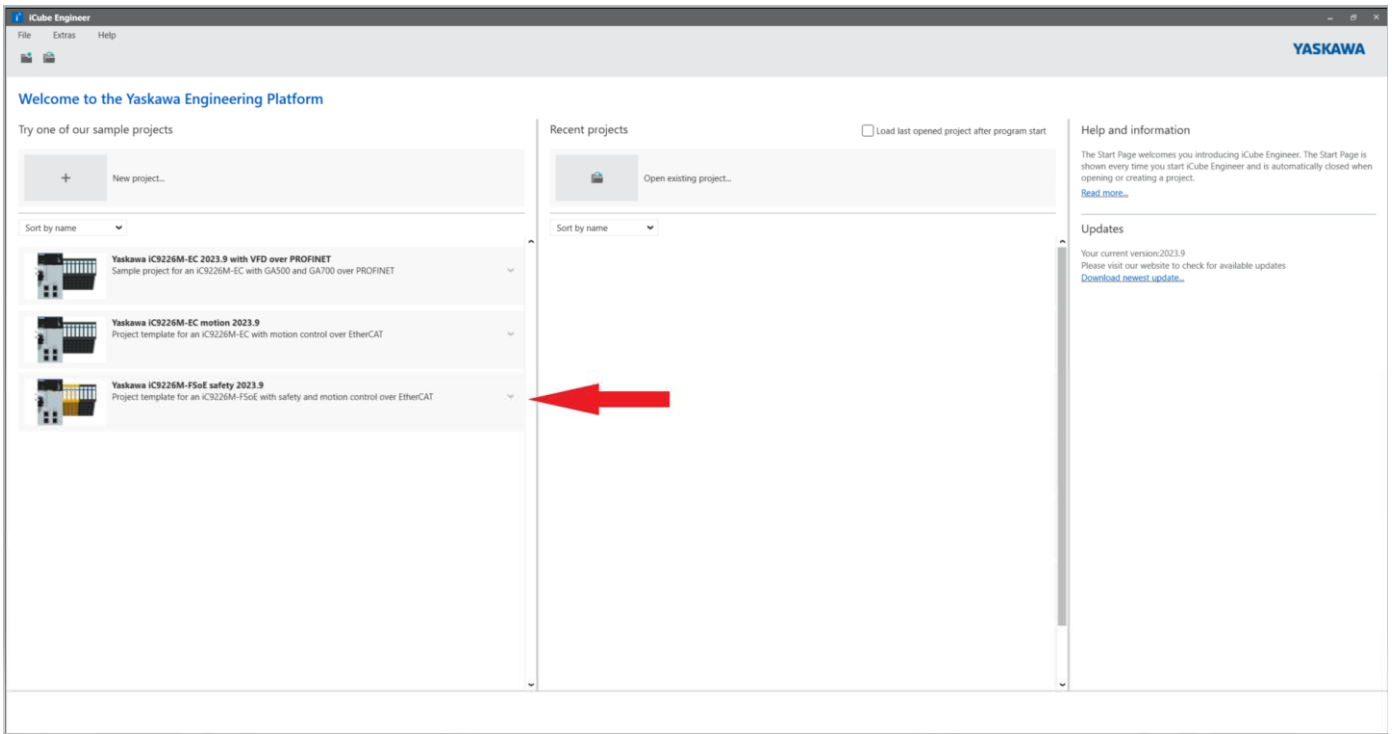


4.13.2 Configuration in iCube Engineer

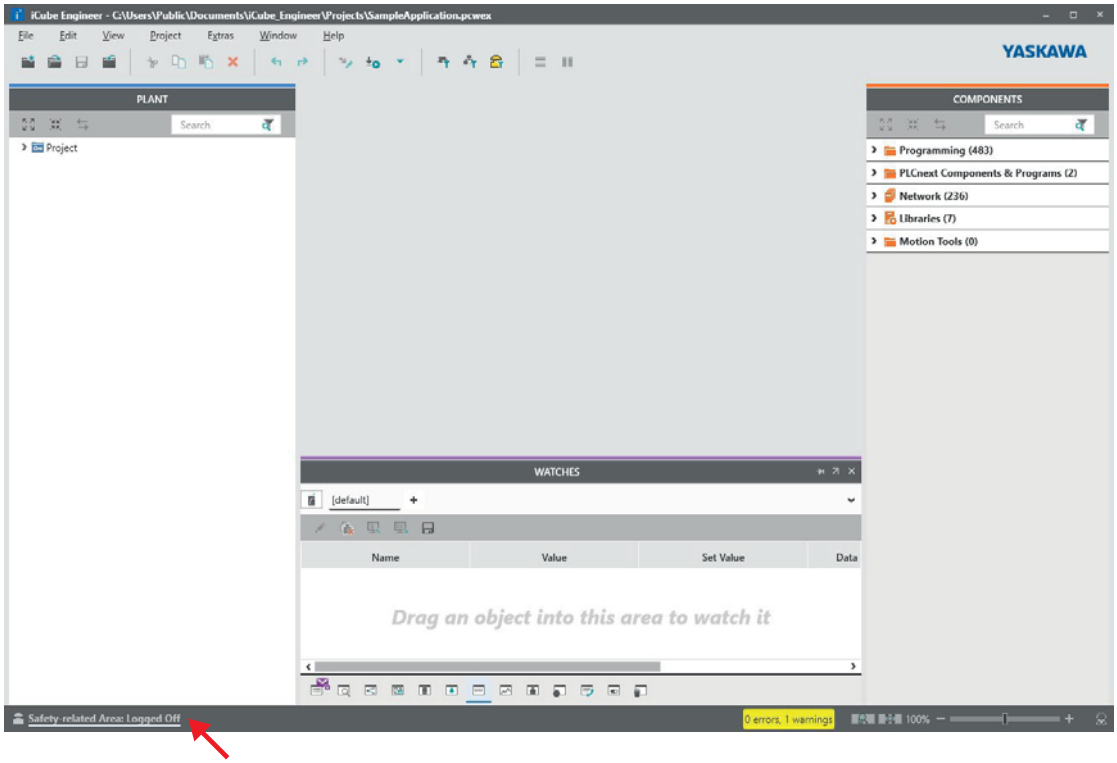
(1) Proceeding

Information Further information on the procedure can be found at *4.4 Programming and File System on page 115*.

1. **Open iCube Engineer and select the template for your safety CPU.**

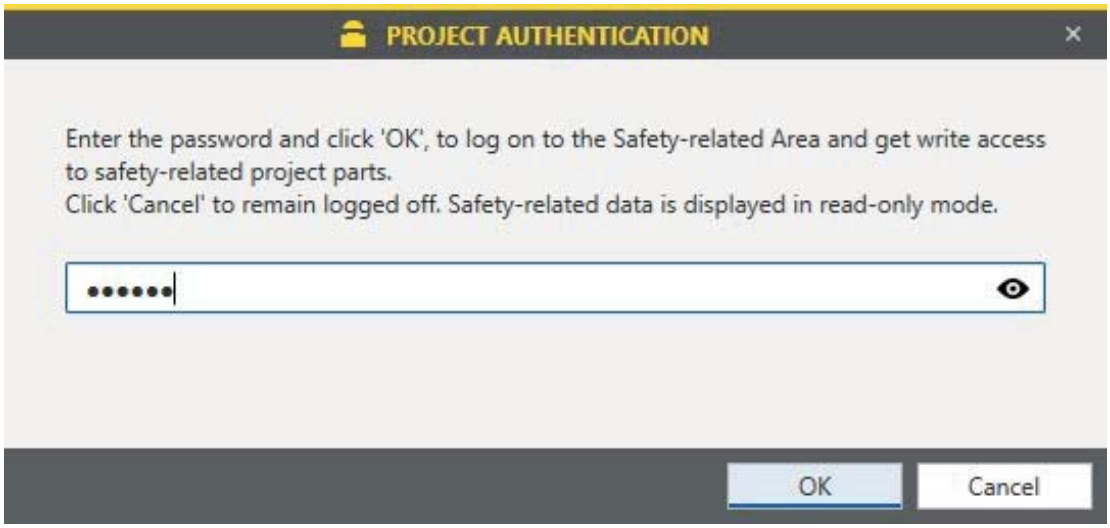


2. **Save the project under a suitable project name. Leave the Project path unchanged.**

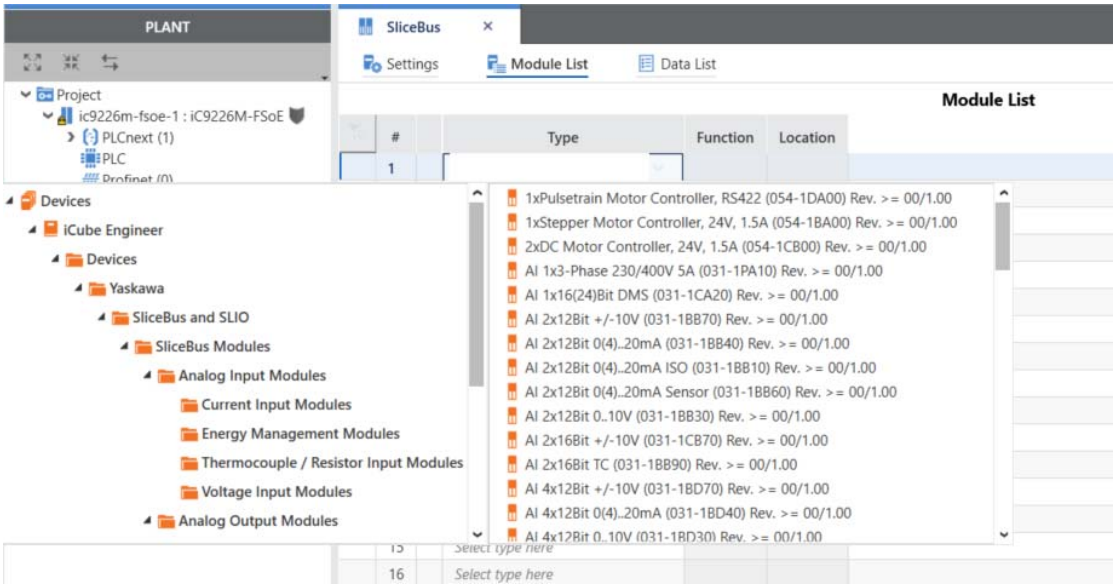


3. **Click on [Safety-related Area] and enter the safety password. The password "safety" is used in the template.**

Click [OK].

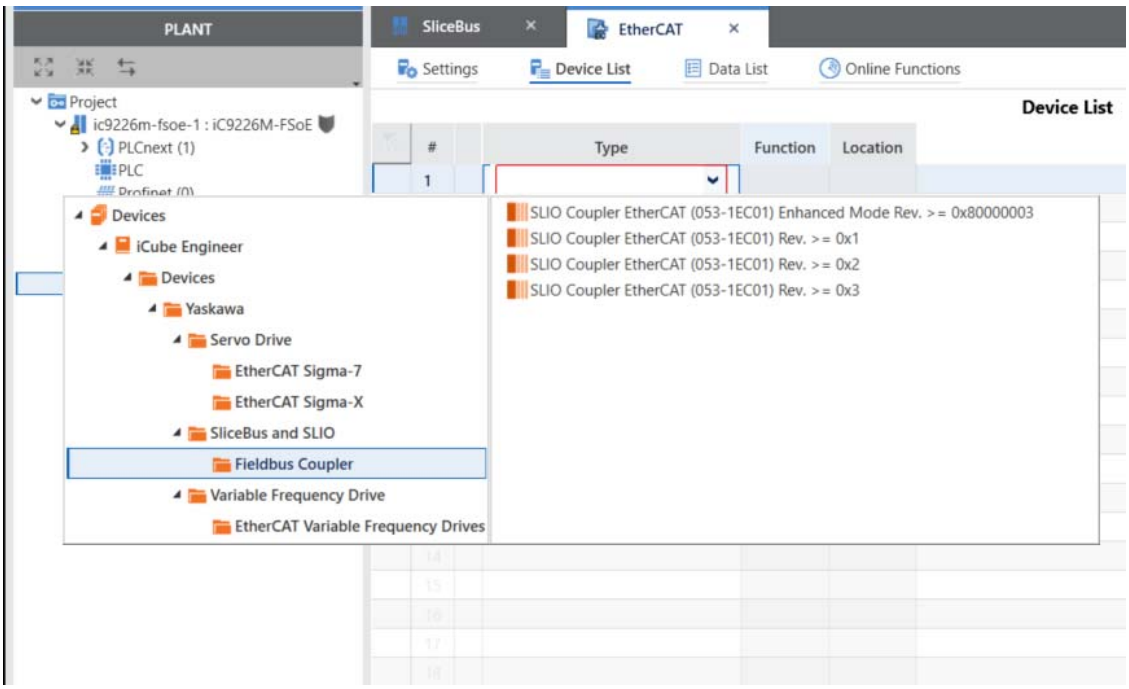


4. **Double-click at [Plant] in your project, on [SliceBus] and add your local SLIO modules by entering a relevant part of the name and clicking on a suggested module.**

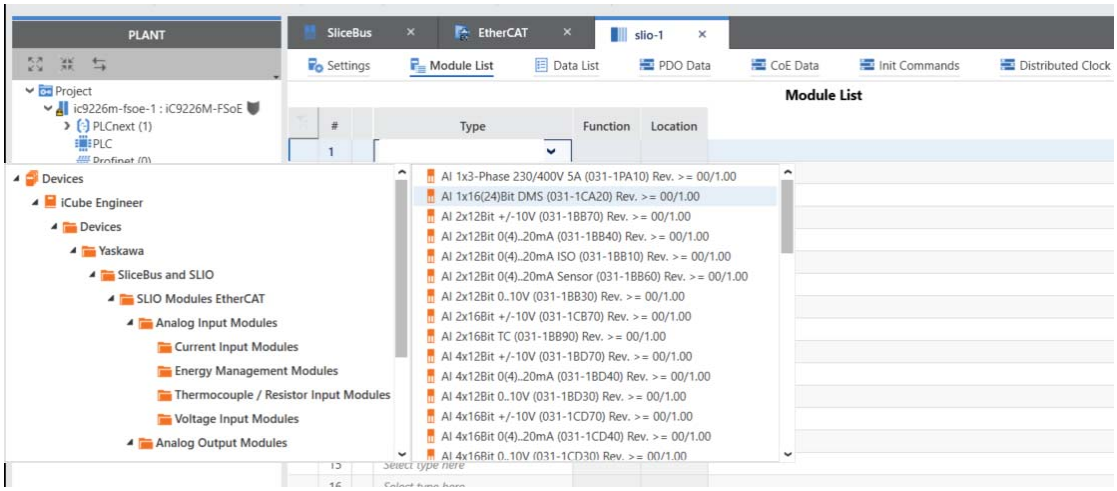


5. **Double-click under [Plant] in your project on [EtherCAT] and add your coupler by entering a relevant part of the name and clicking on a suggested version or the coupler with Enhanced Mode.**

Information Alternatively, you can perform an [EtherCAT bus scan] using the right mouse button. In this case, iCube Engineer must not also be connected online to the safety CPU.



6. **During the bus scan, the modules are inserted directly. For manual placement, double-click under [Plant] the EtherCAT coupler in your project and add your SLIO modules by entering a relevant part of the name and clicking on a suggested module.**

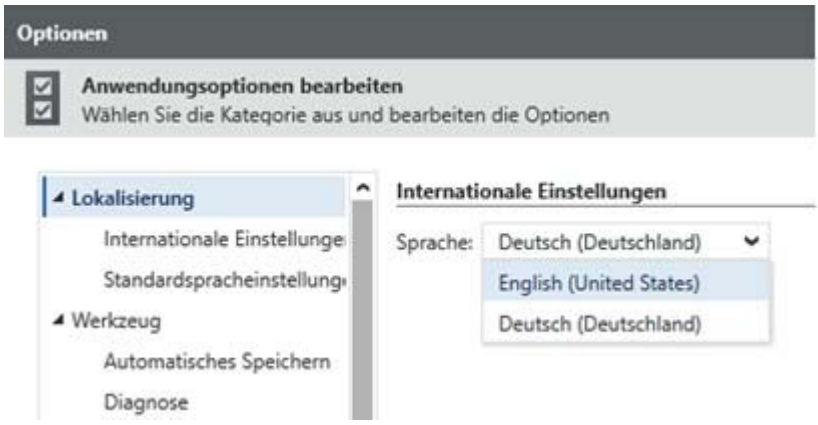


7. **Your hardware configuration is now complete.**

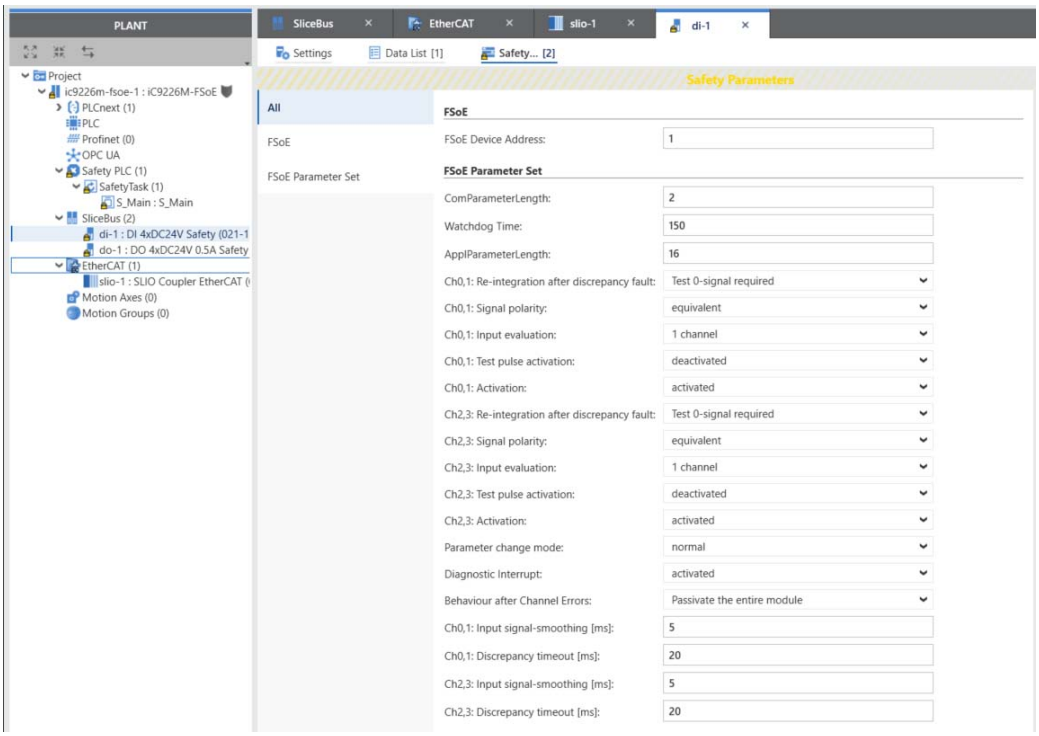
   Save your project.

8. **To switch languages, open the menu [Extras] - [Options] and set the language to [English] at [International].**

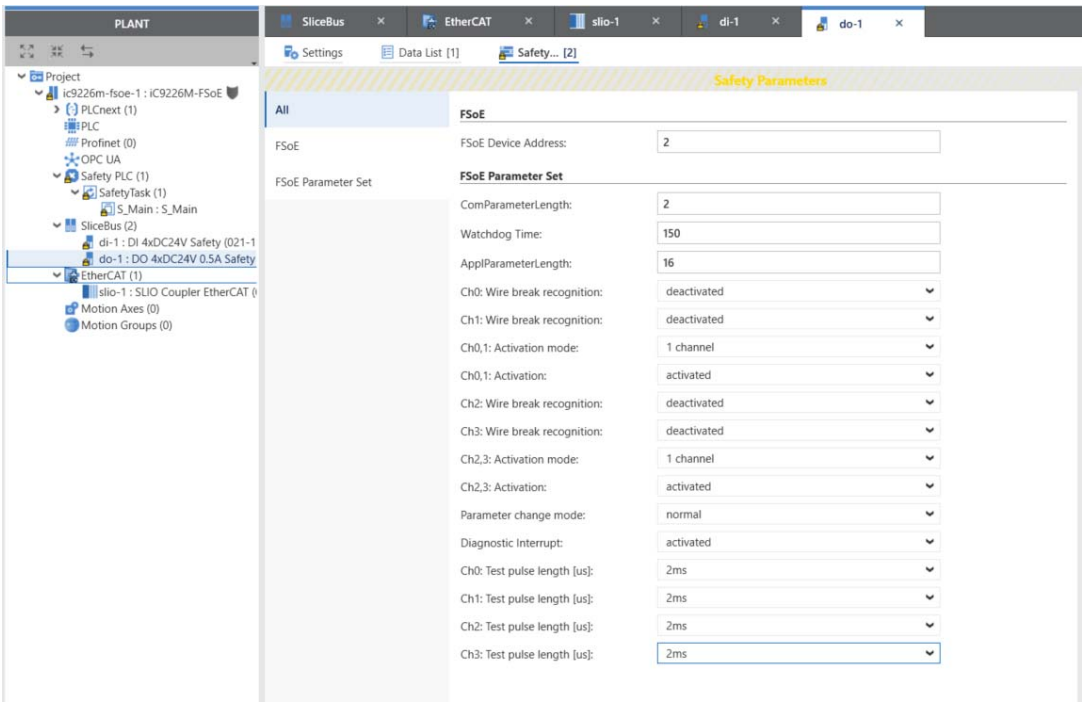
   Information Please note that, due to the system, the parametrization of the safety module parameters is only possible via the English language view.



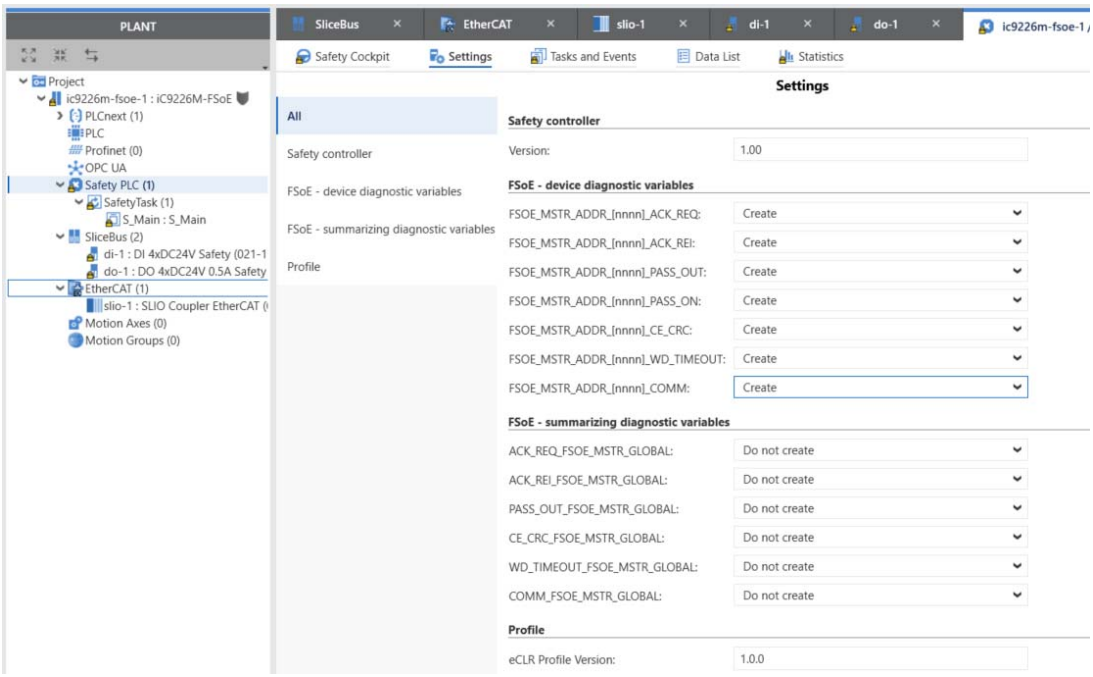
9. **Save your project.**
10. **Restart iCube Engineer with your project.**
11. **To set the module parameters, double-click on the local safety DI module.**
12. **Enter the safety password and set the following module parameters:**
    - Input evaluation: 1 channel
    - Input signal-smoothing: 5ms
    - Test pulse activation: deactivated



13. **To set the module parameters, double-click on the local safety DO module.**
14. **Set the following module parameters:**
    - Activation Mode: 1 channel
    - Test pulse length: 2ms



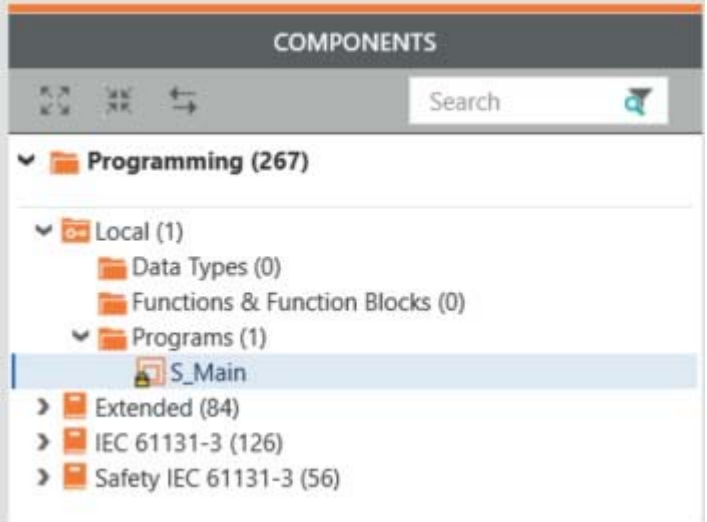
15. **Repeat the parametrization for the safety modules on the FSoE EtherCAT coupler.**
16. **At [Plant], double-click on the [Safety PLC] in your project and open the settings.**
17. **Enable all [FSoE device diagnostic variables] there by activating [Create].**



Your parametrization is now complete.

18. **Save your project.**

19. **Navigate via [Components] to [Programming] - [Local] - [Programmes] and open [S_ Main].**

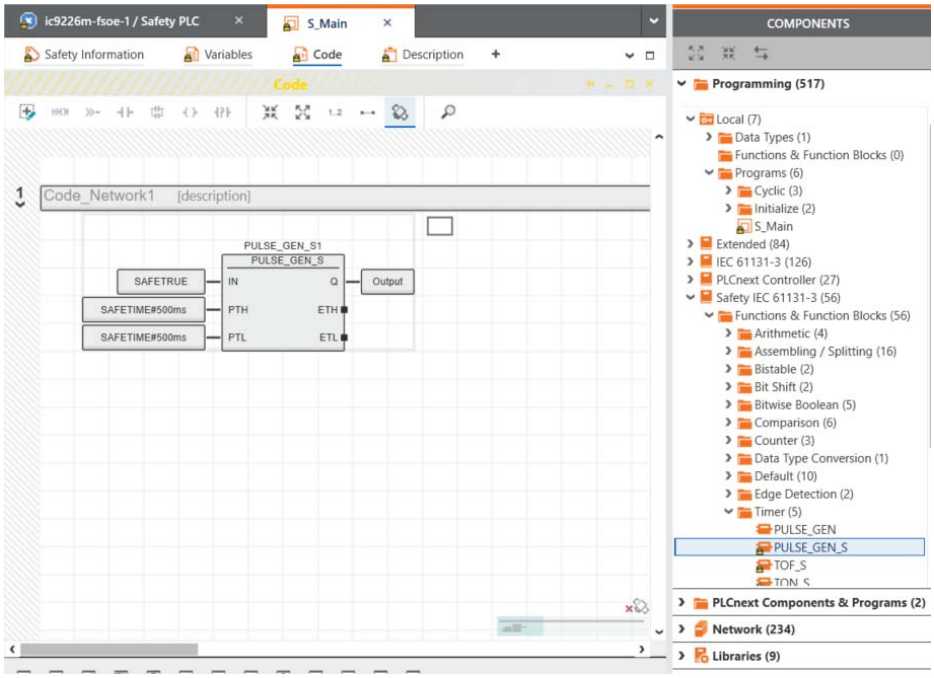


The program editor for your safety application opens.

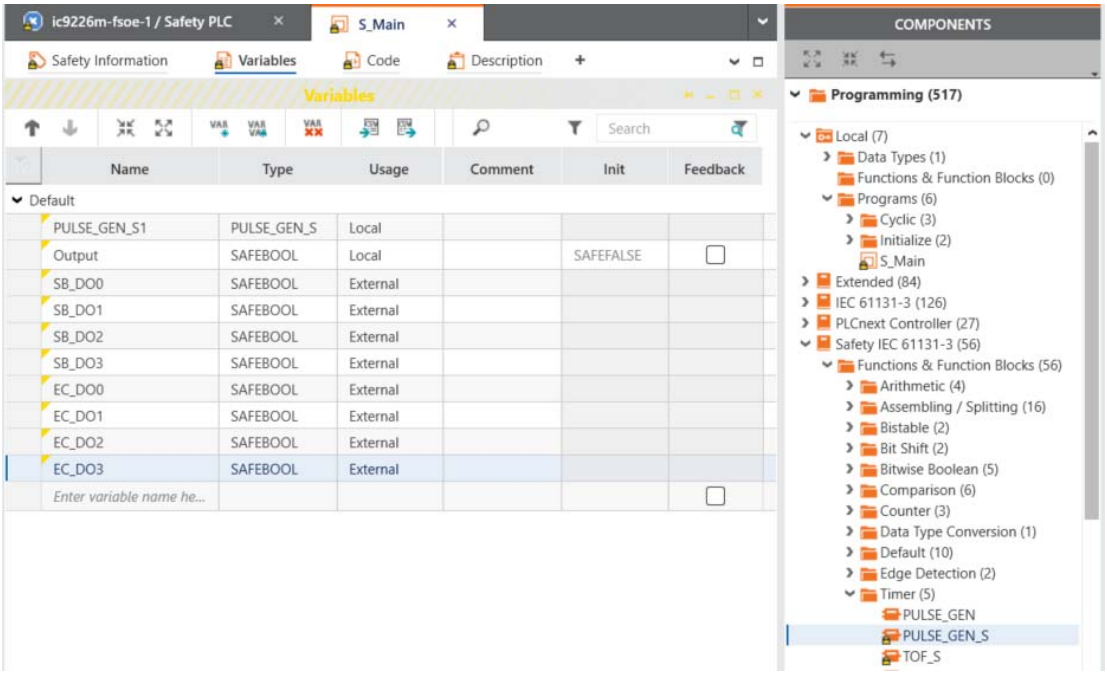
20. **Enter the safety password and click [OK].**

21. **Program your application in the following order:**

- Drag a PULSE_GEN_S into the editor.
- Supply the input parameter IN with SAFETRUE.
- Supply the two time parameters with SAFETIME#500ms.
- Name the output Q as Output.
- Right-click on Output [Create new variable] - [Local] to create a new local variable.

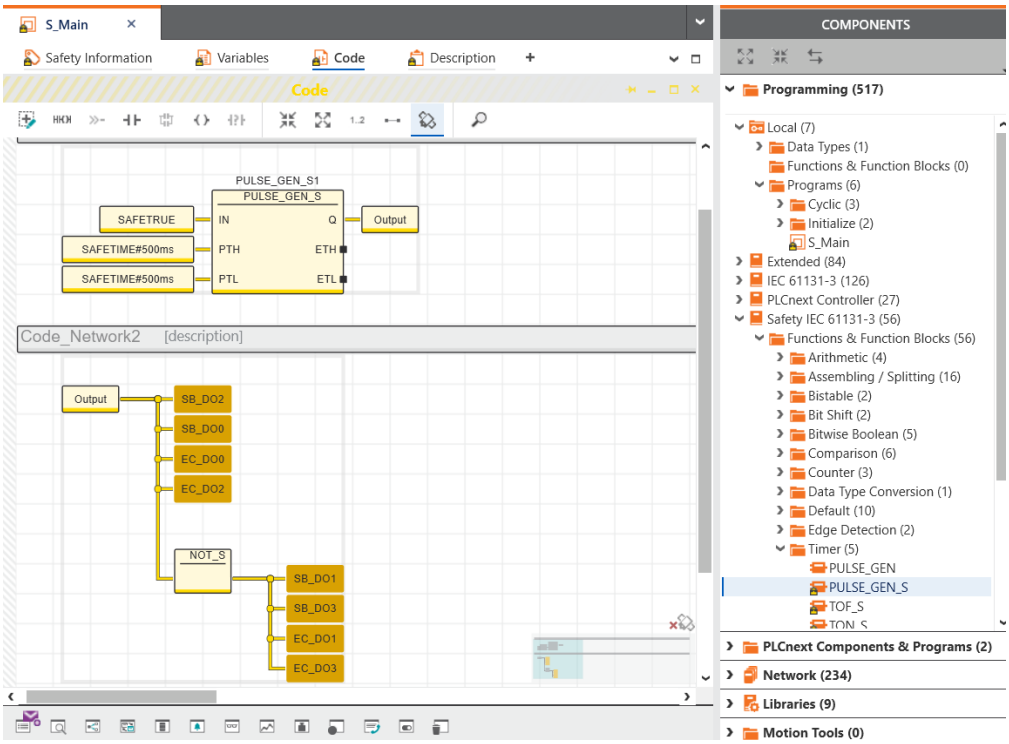


22. **Switch to the [Variables] tab and create 8 external variables that will later be assigned to the outputs. Here you can copy the created variables.**

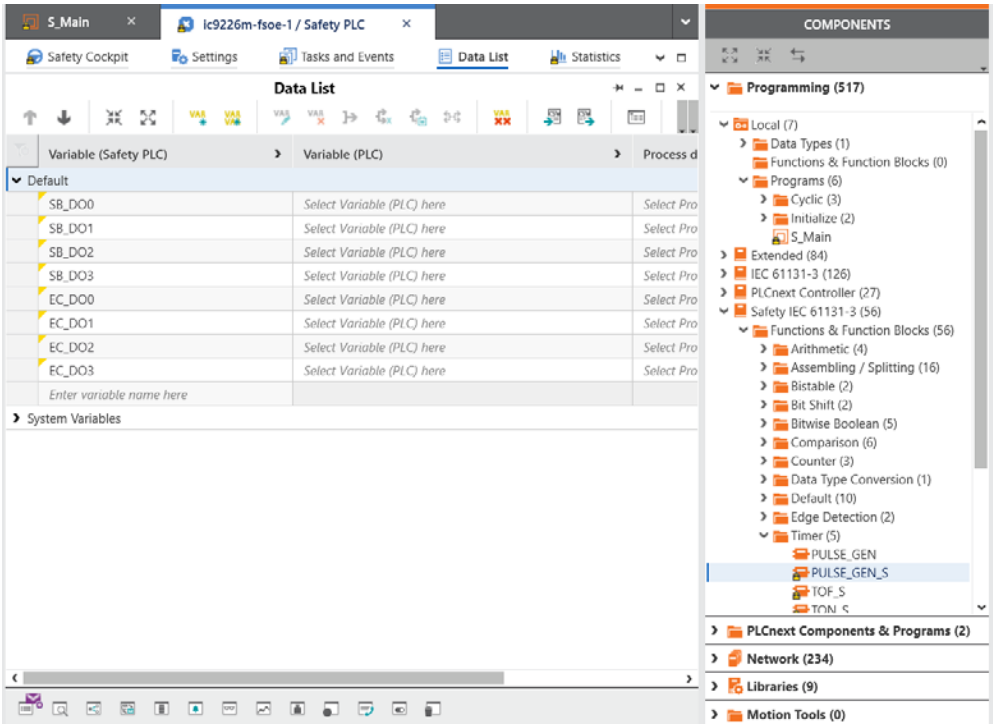


23. **Switch to the [Code] tab, insert the Output variable and assign it to the output variable with even numbering.**

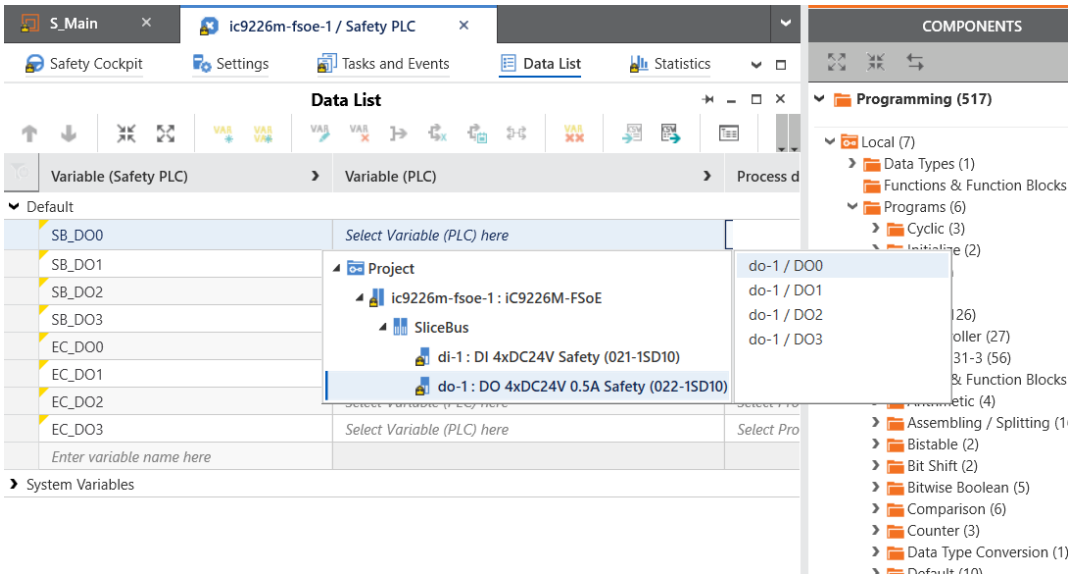
Invert the output variable with a NOT_S and assign it to the output variable with odd numbering.



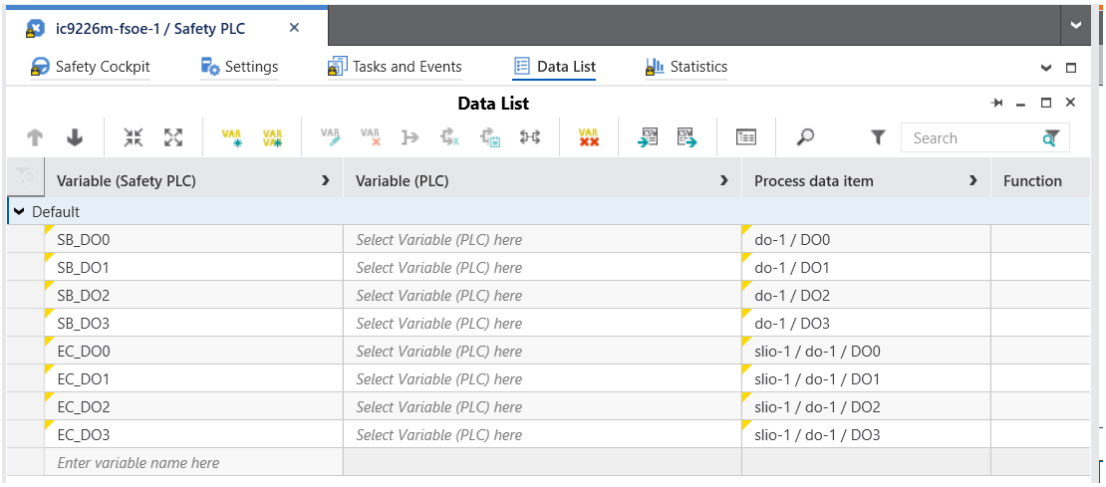
24. **Double-click on the [Safety PLC] and switch to the [Data list] tab.**



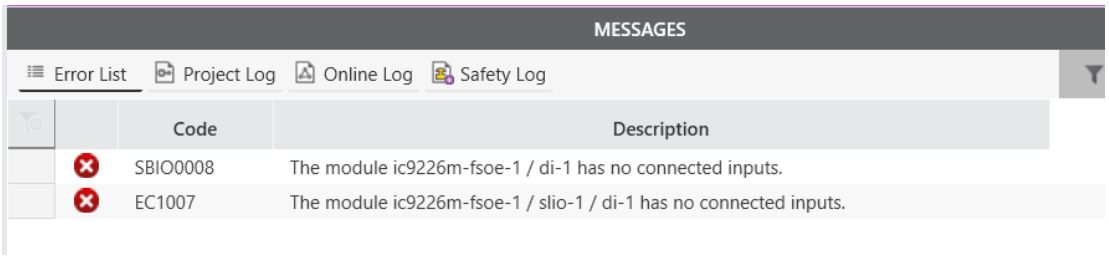
25. **Click in the [Process data item] field of the first output variable and select the safety DO on the [SliceBus] for better filtering.**



26. **Assign all 8 safety outputs.**



You will receive the following error message:

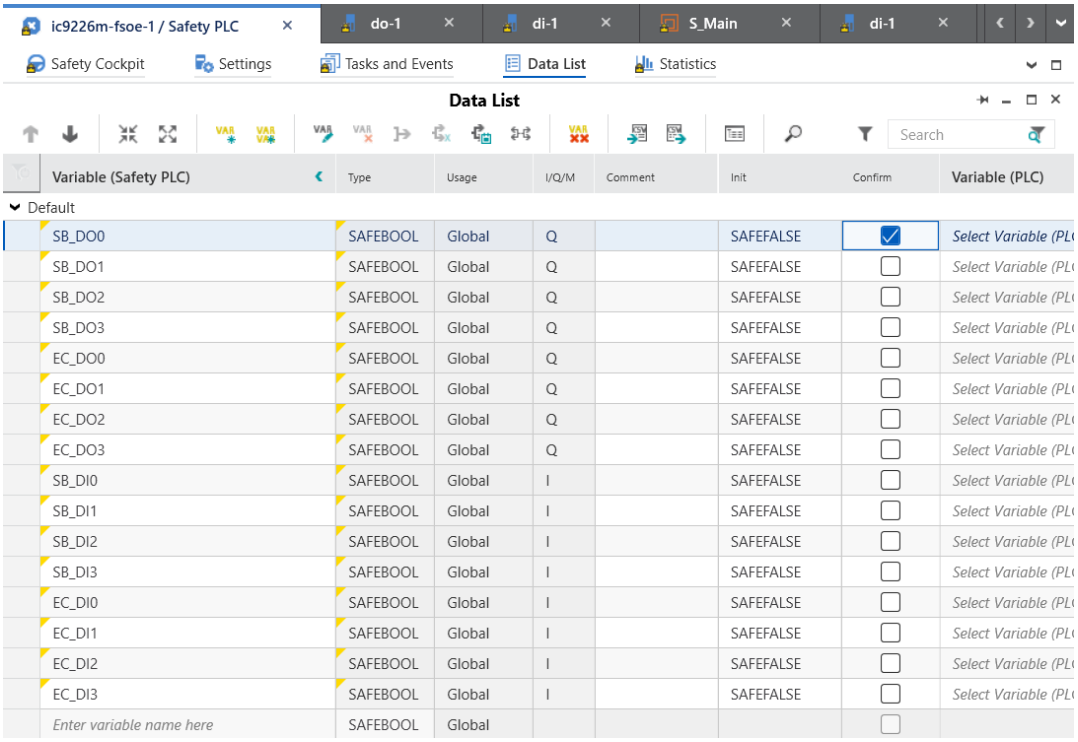


27. **To avoid error messages, create 8 external variables in [S_Main], which you link to the safety inputs.**
28. **Once the mapping of the process data is complete, save the project.**
29. **With Save and rebuild, the number of warnings has now increased.**

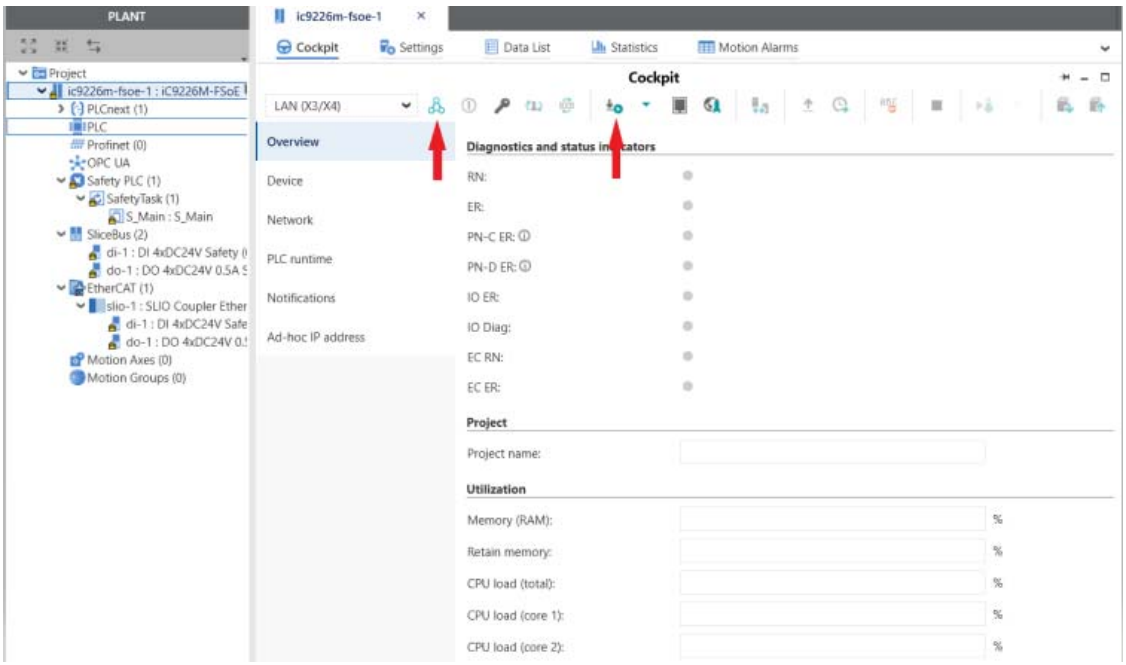
    Double-click on the first message in which the user's address is not validated.

    The cursor jumps to the first variable in the [Safety PLC] data list.
30. **To show additional table columns, click on the [>] icon in the table header.**

31. **Navigate to the [Confirm] column and enable the checkboxes for all 16 variables.**



32. **In the [Plant] area, double-click the Controller in your project and switch to [Cock- pit] tab.**

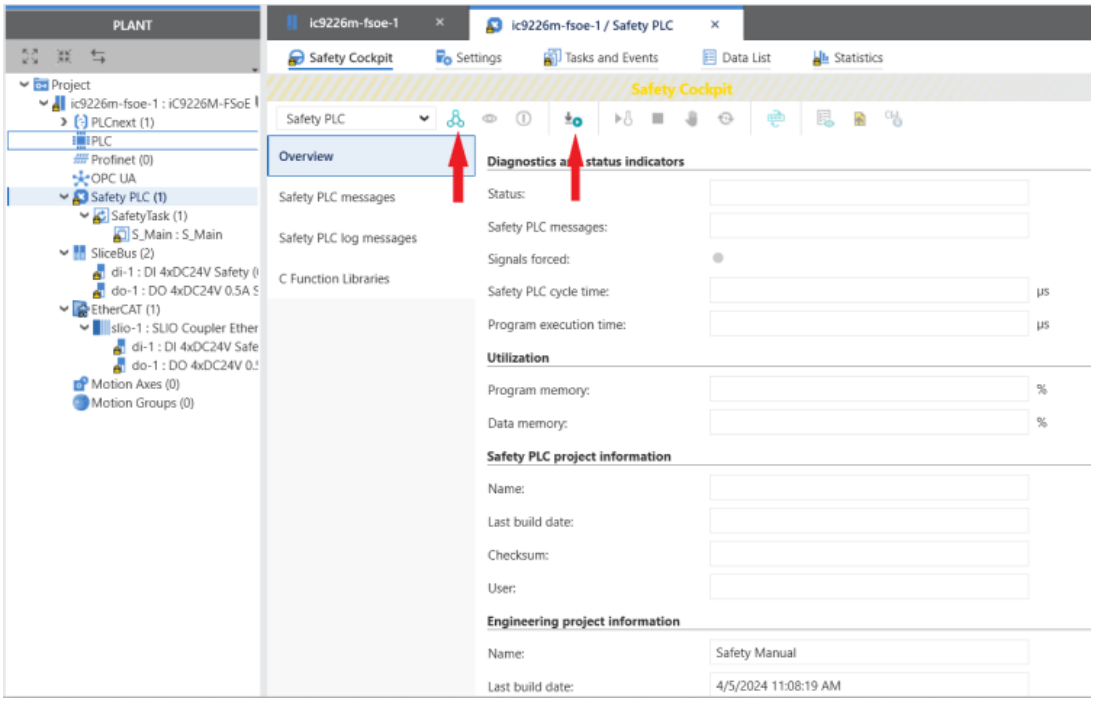


33. **Go online via the**  **symbol.**

34. **Enter the name "Admin" and the printed device password.**

35. **Use the**  **symbol to transfer the project to the standard component of the safety CPU.**

36. **Double-click in the [Plant] area, on your [Safety PLC] and switch to the [Safety Cockpit] tab.**



37. **Go online with the**  **symbol.**

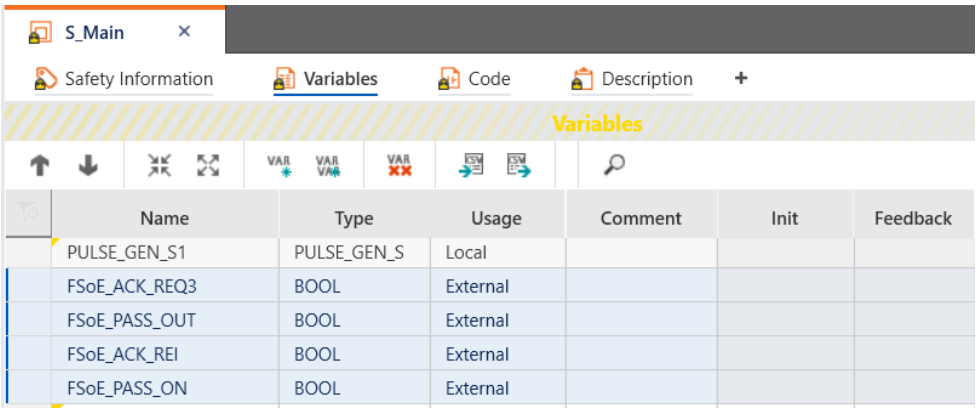
38. **Use the**  **symbol to transfer the project to the safety component of the safety CPU.**

A password query for the safety CPU appears. Assign a new password or enter a password that authorizes you to overwrite the project on the safety CPU.

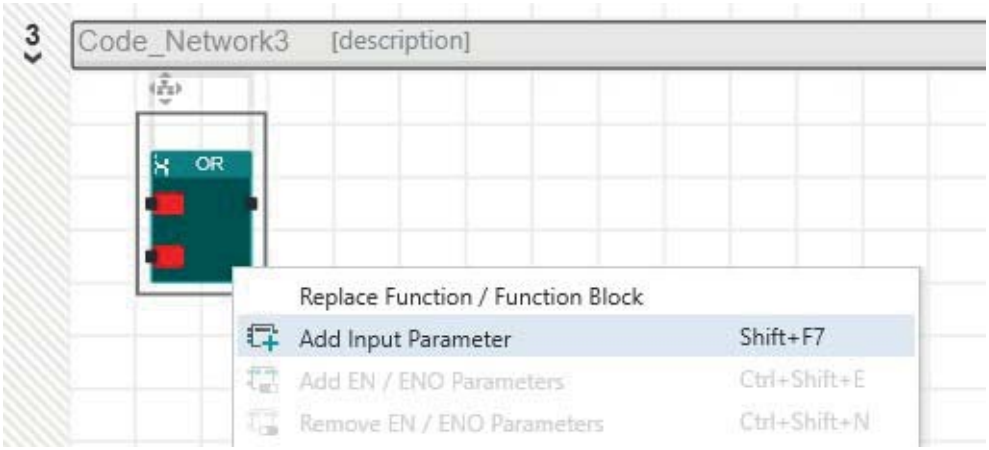
4.13.3 Modification

- Evaluation of the FSoE device diagnostic variables
- Resetting a passivation

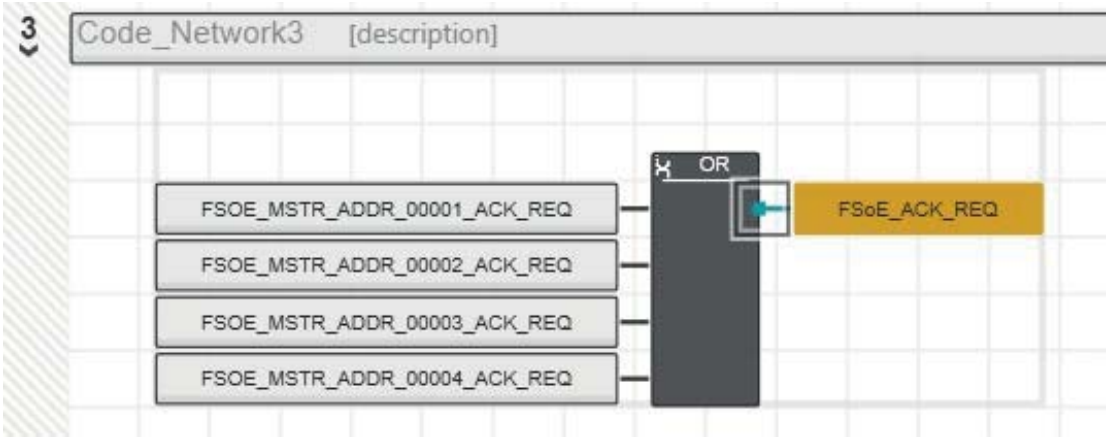
1. **Open the [Variables] tab in [S_Main] and add the following variables:**
   - FSoE_ACK_REQ
   - FSoE_PASS_OUT
   - FSoE_ACK_REI
   - FSoE_PASS_ON



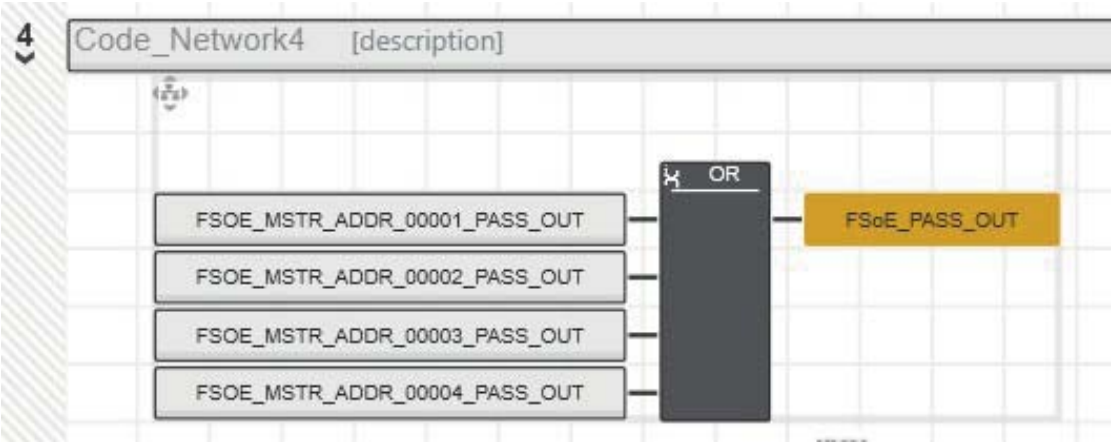
2. **Open the [Code] tab in [S_Main], drag in an OR and add two more input parameters.**



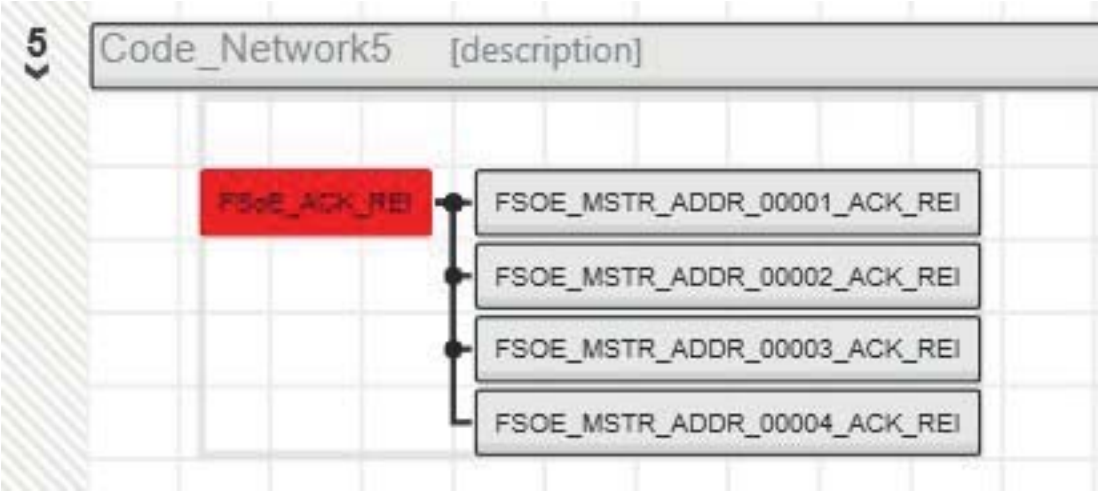
3. **Use [Add input parameter] to add the input parameters FSOE_MSTR_ADDR_0000x_ ACK_REQ and the output FSoE_ACK_REQ.**



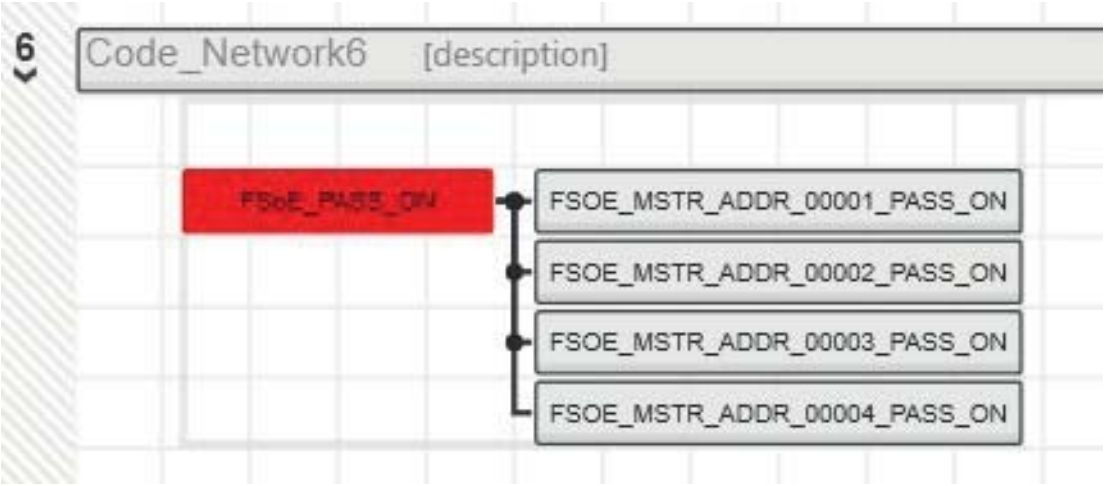
4. **Add another OR and proceed in the same way with FSOE_MSTR_ADDR_0000x_PASS_OUT and FSoE_PASS_OUT.**



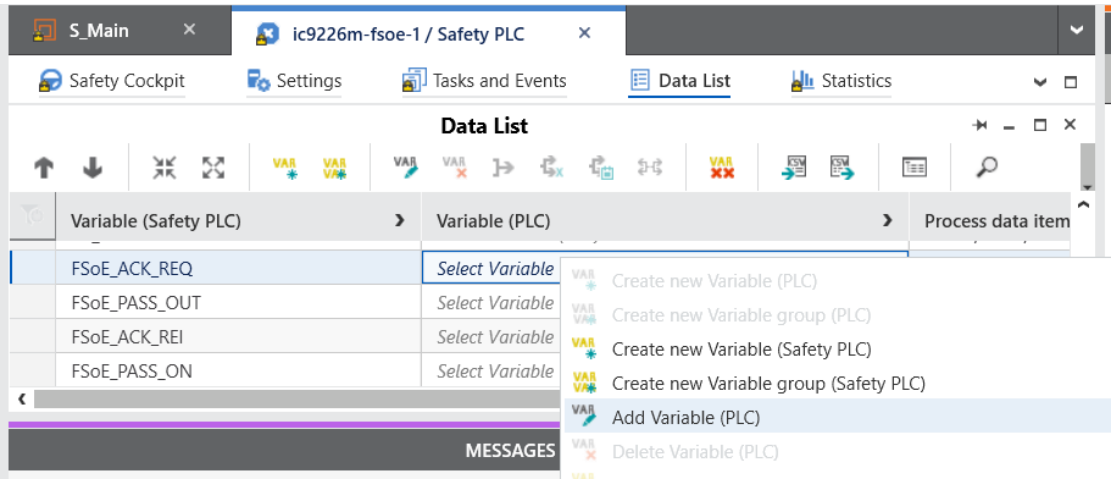
5. **Insert FSoE_ACK_REI and connect it to all FSOE_MSTR_ADDR_0000x_ACK_REI.**



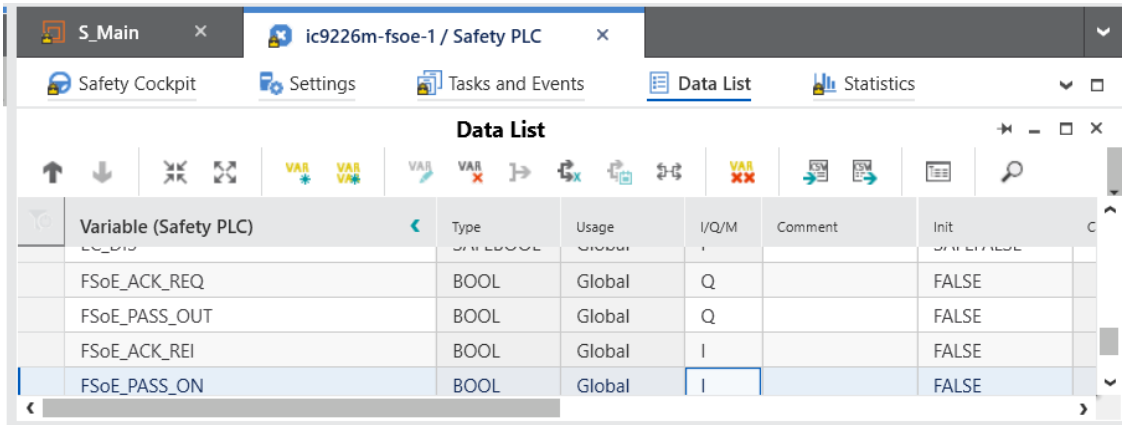
6. **Insert FSoE_PASS_ON and connect it to all FSOE_MSTR_ADDR_0000x_PASS_ON.**



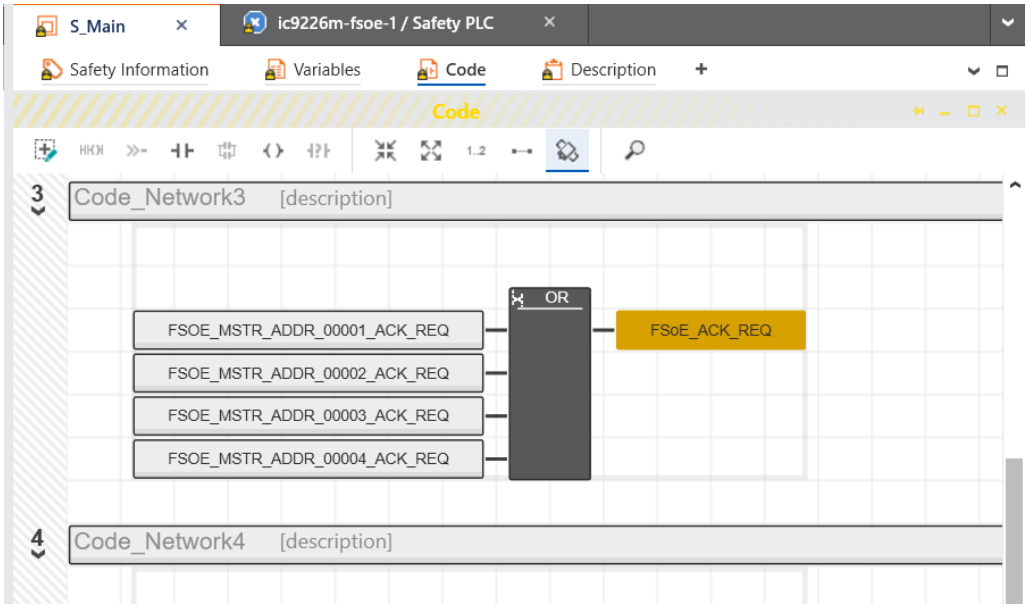
7. **Open the [Data list] of the [Safety PLC] and add the four FSoE variables to the standard component of the safety CPU via [Add variable (PLC)].**



8. **Select the data direction at [I/Q/M], [Q] for output and [I] for input.**

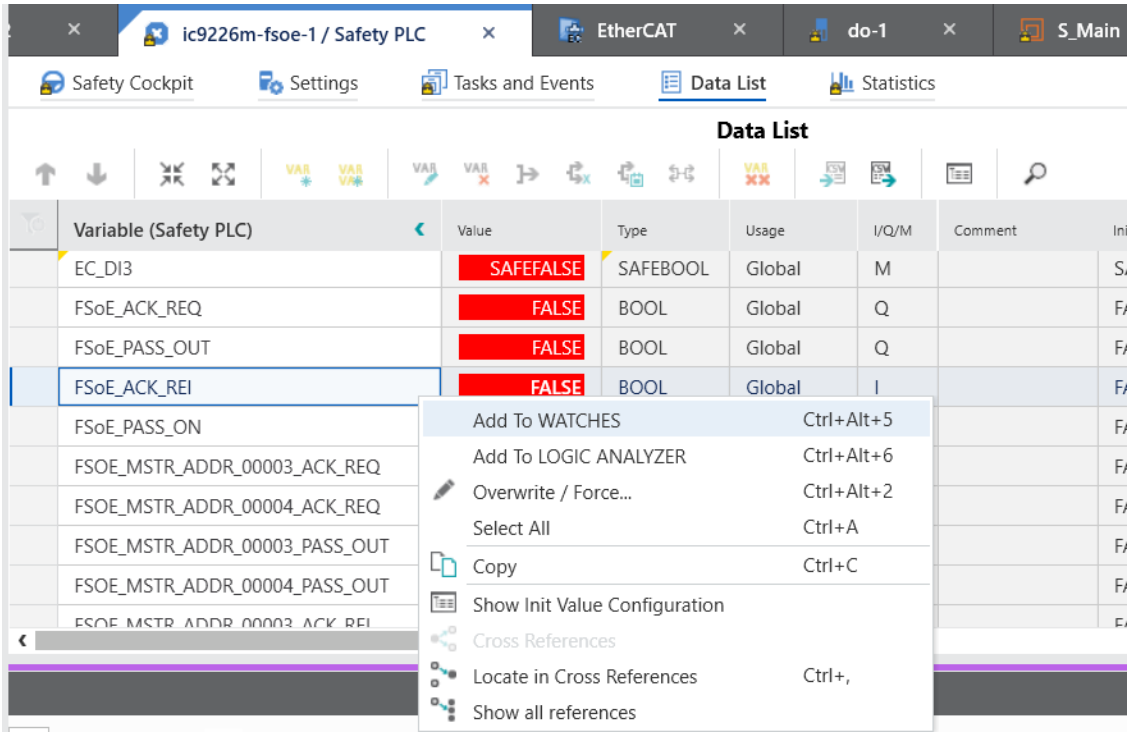


9. **Nothing should now be highlighted in red in the [S_Main] code.**

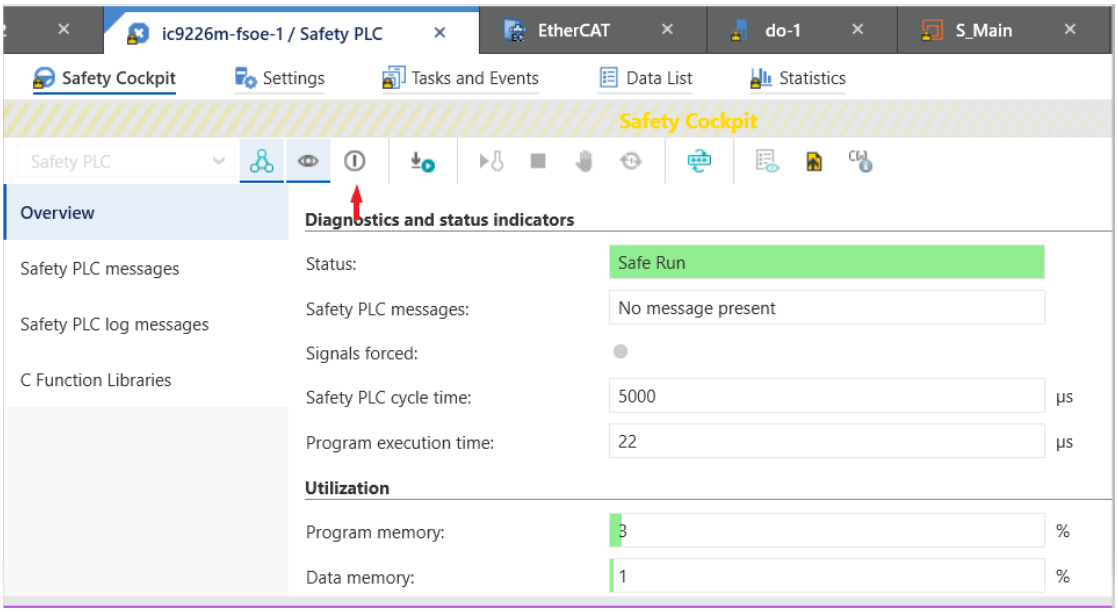


10. **Save your project and write to controller.**

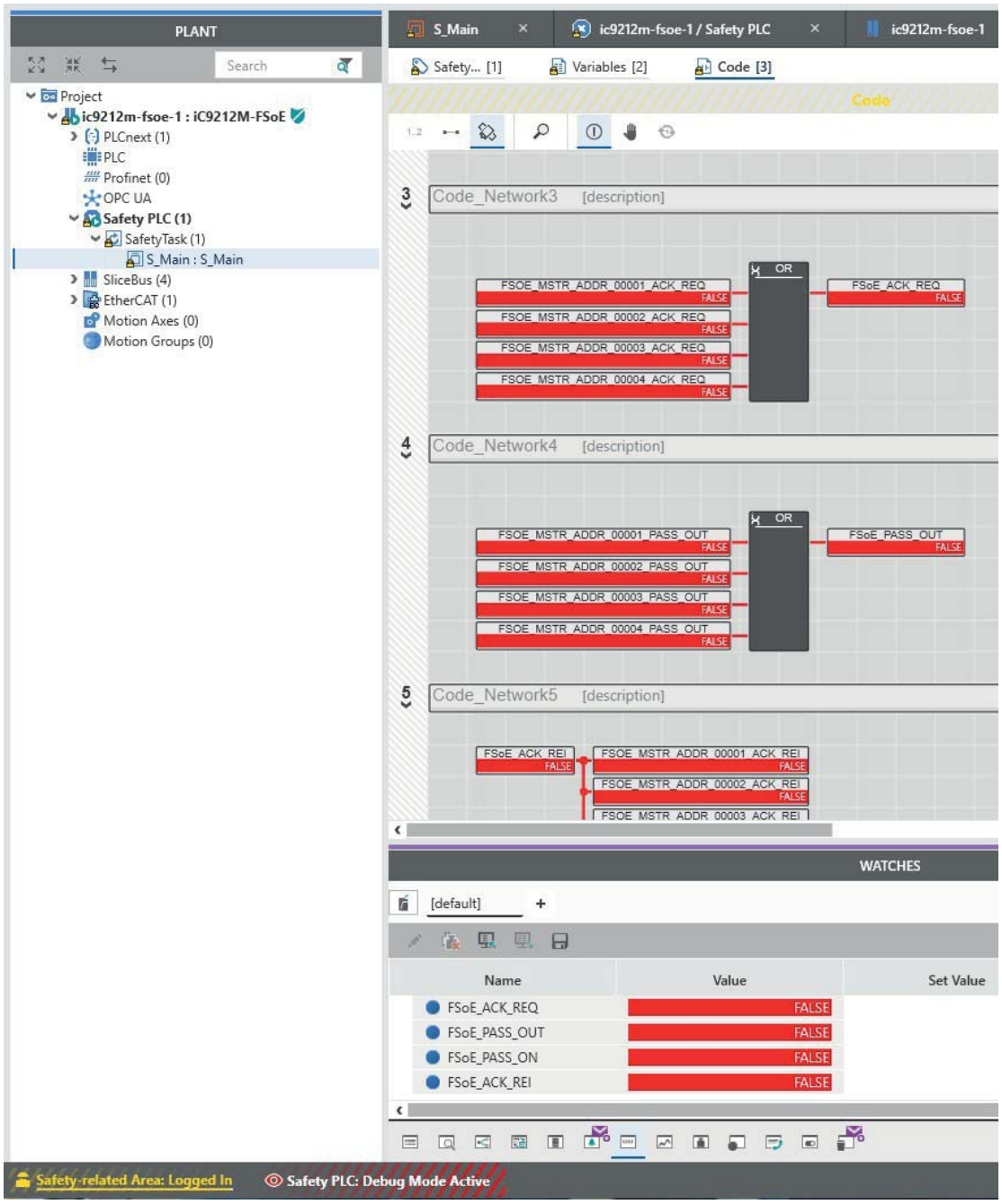
11. **Add all four variables to the [Watch window] via [Insert in watch window].**



12. **Open the [Cockpit] of the Safety PLC [Safety cockpit] and check whether you are online and also switch on the debug mode via**  **.**

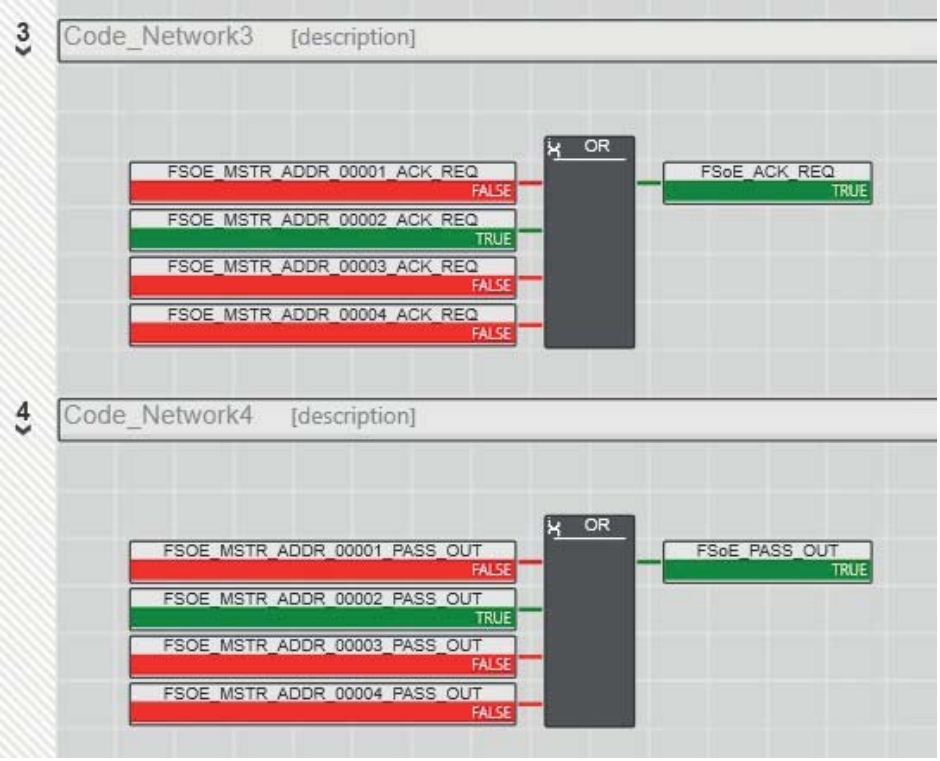


13. **Open in [Safety PLC] [S_Main:S_Main].**

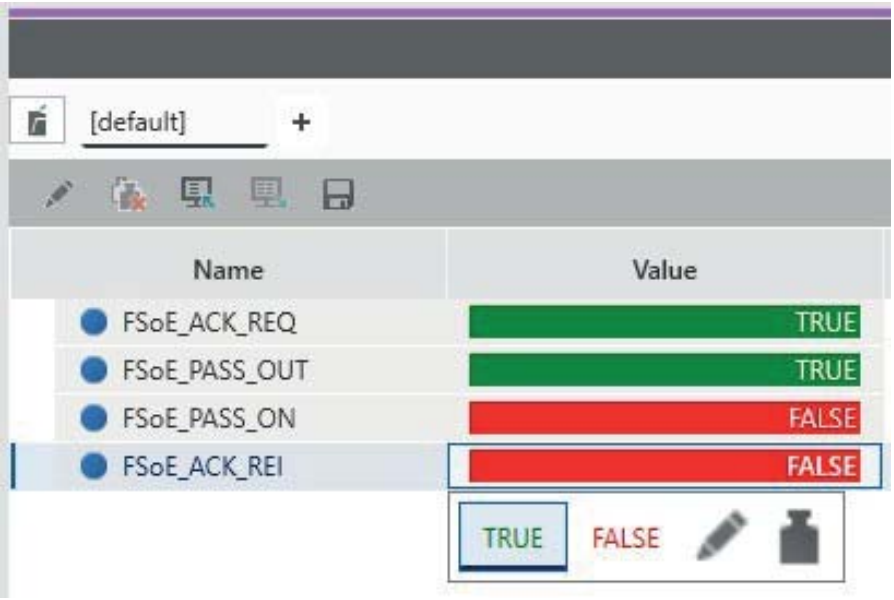


14. **Briefly switch the DC 24V power section supply of the IO modules at the backplane bus off and on again.**

The safety DO is passivated.



15. **To re-integrate, set FSoE_ACK_REI to True in the [Watch window].**



16. **As soon as the re-integration is successful, set FSoE_ACK_REI back to False in the [Watch window].**

4.13.4 Response time example

Measurement on:	SliceBus		EtherCAT	
Cycle time	2ms	8ms	1ms	8ms
Ø from 6 measurements	33.40ms	50.07ms	36.72ms	81.53ms
Calculated Value	39.87ms	51.87ms	42.02ms	84.02ms

4.14 Functional Safety - Safety Relevant Parameters

4.14.1 General

This chapter describes characteristics associated to functional safety. According to IEC 61508, safety initially means that the overall system has a residual error probability smaller than the limits specified in the standard. In relation to the overall application, internal safety-relevant device faults must be recognised and lead to a safe state.

4.14.2 Safety Relevant Parameters

The values specified here refer exclusively to the safety CPUs specified in this manual. Safety-relevant parameters can always be found in the corresponding manuals of the modules.

NOTICE

After expiry of the device life time, the safety CPU must be decommissioned and returned to the vendor!

Parameters according to DIN EN ISO 13849-1	Value	Meaning
Performance level	max. e	Measure of the reliability of a safety function.
Category	max 4	Measure of resistance to errors.
PFH_D	1 * 10-9/h	**P**robability of **F**ailure per **H**our, **D**angerous: Probability of dangerous error per hour.
DCavg	99%	**D**iagnostic **C**overage **av**era**g**e: Medium level of diagnostic coverage.
$MTTF_D$	> 80 years	**M**ean **T**ime **T**o **d**angerous **F**ailure: Average time to a dangerous failure.
Parameters according to IEC 61508	**Value**	**Meaning**
SIL	max 3	**S**afety **I**ntegrity **L**evel Safety requirement level for the classification of functional safety.
PFH_D	1 * 10-9/h	**P**robability of **F**ailure per **H**our, **D**angerous: Residual error rate of dangerous error per hour.
HFT	1	Hardware Fault Tolerance Number of faults that can result in a loss of the safety function.
Lifetime	300 months	Device lifetime No maintenance is required during the expected device lifetime.

Continued from previous page.

NOTICE

The manufacturing year and month are given as part of the serial number.

S/N D0 2 3 6 H0 9 5 6 1 0 0 0 4

3rd+4th digits | 5th digit

3rd+4th digits Manufacturing Year

The last two digits of the manufacturing year are given.

Example

23: 2023
24: 2024

5th digit Manufacturing Month

The manufacturing month is given using the codes listed in the following table.

Code	Manufacturing Month
1	January
2	February
3	March
4	April
5	May
6	June
7	July
8	August
9	September
X	October
Y	November
Z	December

4.15 System Variables and Status Information

4.15.1 General

- This chapter describes system variables that are available for the CPU.
- The CPU has a register set that is used for diagnostics and simple control of the CPU.
- The diagnostic data are stored in the diagnostic status register and in the diagnostic parameter register. These registers are available to the application program as system variables (system flags, global variables).

(1) Access to System Variables and Data Structures

- Some system variables of the CPU are organized as data structures. The data structure of such a system variable contains further system variables.
- In the [Init Value Configuration] of iCube Engineer you can see which system variables belong in detail to a system variable organized as a data structure.

To open the [Init Value Configuration] for a system variable organized as a data structure, proceed as follows:

1. **In the Plant area, double-click the SPS node.**

   The CPU/SPS editor group opens.

2. **Select the editor Data list.**

   Information Alternatively, you can open the Data list editor in the area Plant via the CPU node.

3. **Open the System variables section.**

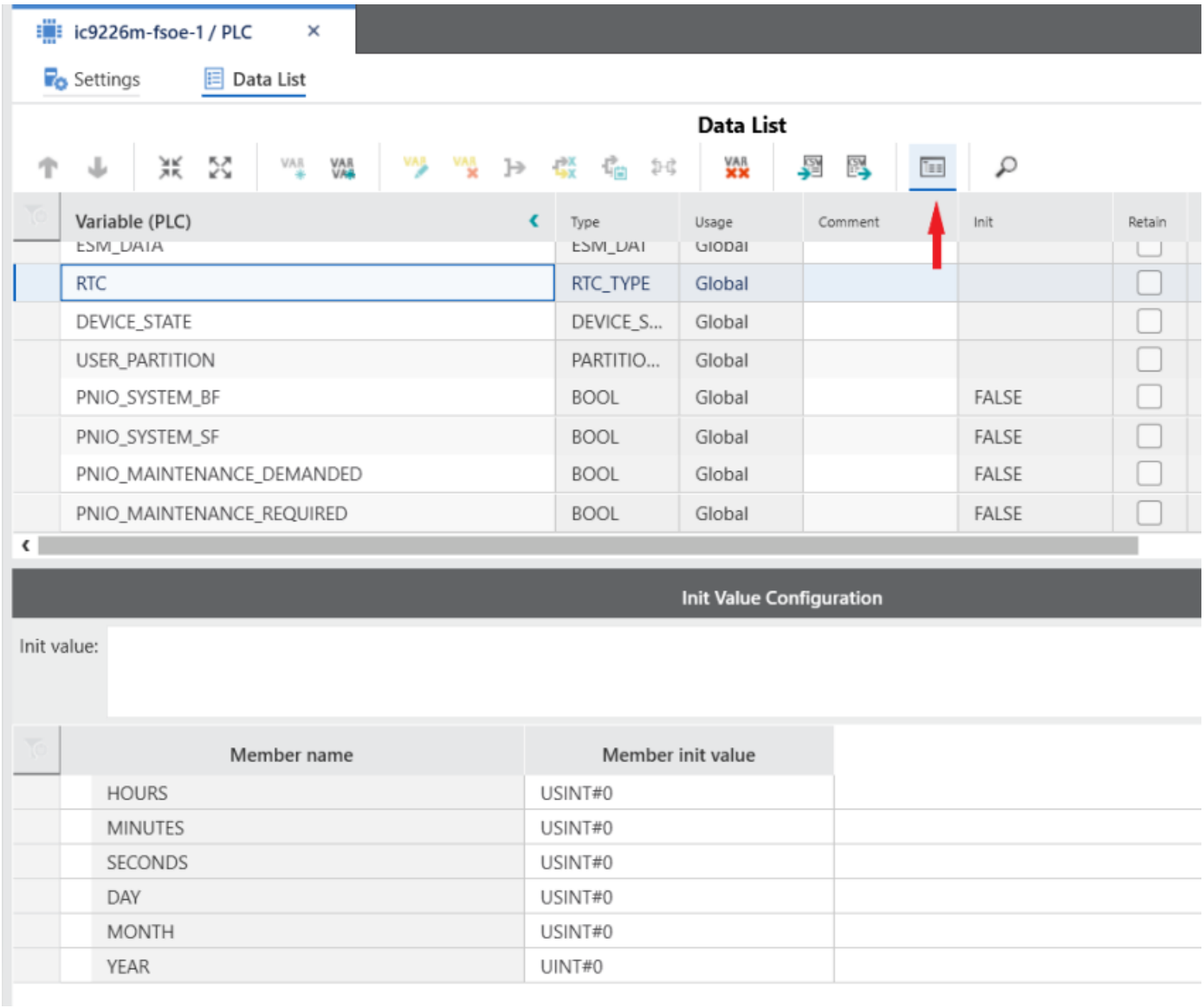
4. **Click on the arrow in the Variable (PLC) column to show the extended information.**

   The data type of the system variable is shown in the extended information column Type.

5. **Select the line of the system variable organized as a data structure whose associated system variables you want to see. To do this, click on the first column in the row of the system variable organized as a data structure.**

6. **Click the**  **button.**

   The [Init Value Configuration] of the selected system variable organized as a data structure is opened below the Data list editor.



In [Init Value Configuration] column Element name lists all system variables which are contained in the system variable organized as a data structure.

4.15.2 System Variables

(1) System Time

- The system variable RTC is a system variable organized as a data structure.
- You can use the RTC system variable to retrieve information about the system time of the device-internal real-time clock.

System variable		Type - description
RTC		RTC_TYPE - data structure
	HOURS	USINT - system time (hours)
	MINUTES	USINT - system time (minutes)
	SECONDS	USINT - system time (seconds)
	DAY	USINT - system time (day)
	MONTH	USINT - system time (month)
	YEAR	UINT - system time (year)

(2) Function Blocks TLS_SOCKET_2 UDP_SOCKET_2

- With the TLS_SOCKET_2 function block, you open and close IP sockets for IP communication via TCP (**T**ransmission **C**ontrol **P**rotocol - not secure or TLS (**T**ransport **L**ayer **S**ecurity - secure). You can control this with the START_TLS input parameter (FALSE: TCP, TRUE: TLS).
- Use the UDP_SOCKET_2 block to open and close IP sockets for IP communication via UDP (**U**ser **D**atagram **P**rotocol).
- You can retrieve the number of open IP sockets using the following system variables:

System variable	Type - description
IP_ACTIVE_SOCKETS	UINT - Number of TCP/UDP sockets opened with the TLS_SOCKET_2 and UDP_SOCKET_2 function blocks.
TLS_ACTIVE_SOCKETS	UINT - Number of TLS sockets opened with the TLS_SOCKET function block.

(3) Device State

- The system variable DEVICE_STATE is a system variable organized as a data structure.
- You can use the DEVICE_STATE system variable to retrieve various information about the device status of the CPU.

System variable			Type - description
DEVICE_STATE			DEVICE_STATE_X152_TYPE - data structure
	BOARD_TEMPERATURE		SINT - temperature inside the housing (in °C).
	reserved1		BOOL - reserved
	reserved2		USINT - reserved
	CPU_LOAD_ALL_CORES		USINT - average current utilization of all processor cores (in %).
	CPU_LOAD_PER_CORE		CPU_LOAD_PER_CORE_ARRAY - Information on the utilization of each processor core.
		[1]	USINT - current utilization of processor core 1 (in %).
		[2]	USINT - current utilization of processor core 2 (in %).

(4) Partition

- The system variable USER_PARTITION is a system variable organized as a data structure.
- You can use the USER_PARTITION system variable to retrieve various information and memory statistics on the user partition (overlay file system).
- The partition can be on the external Yaskawa SD card or on the internal memory.
- The memory is organized in blocks.
- A block has a constant, fixed size and a file always uses one or more blocks.
- A certain number of blocks are reserved in the Linux system for the root user. These reserved blocks are only available for the root user and ensure his ability to act even if the memory is occupied (e.g. for log outputs).

System variable		Type - description
USER_PARTITION		PARTITION_INFO - data structure
	MEM_TOTAL	ULINT - total memory of the partition in bytes (including reserved blocks).
	MEM_FREE	ULINT - free, available memory in bytes (without reserved blocks).
	MEM_USED	ULINT - used memory in bytes (including reserved blocks).
	MEM_USAGE	ULINT - used memory in % (without reserved blocks).

(5) Task Handling

- In iCube Engineer programs and program parts are treated as tasks.
- The **E**xecution & **S**ynchronization **M**anager (ESM) is responsible for coordinating and processing the individual tasks.
- You can use the ESM_DATA system variable to retrieve information about the ESM's task handling.
- ESM_DATA is a system variable organized as a data structure.

System variable	Type - description
ESM_DATA	ESM_DAT - data structure
ESM_COUNT	USINT - number of ESM (one ESM per processor core).
ESM_INFOS	ESM_INFO_ARRAY
[1] ... [2]	ESM_INFO - Information about the ESM [1 ... 2][2].
TASK_COUNT	UINT - number of tasks that were configured for the ESM.
TICK_COUNT	UDINT - always 0.
TICK_INTERVAL	UDINT - always 0.
TASK_INFOS	TASK_INFO_ARRAY
[1] ... [16]	TASK_INFO - Information about the tasks [1 ... 16].
INTERVAL[1]	LINT - time interval • With cyclic tasks: Time interval in µs • With acyclic tasks: 0
PRIORITY[1]	INT - priority of the task
WATCHDOG[1]	LINT - watchdog time in µs (0 = no watchdog). • Watchdog time you define for the sum of the execution time and the delay time. • If the watchdog time is exceeded, the watchdog is triggered.
LAST_EXEC_DURATION	LINT - execution time of the task in the previous cycle in µs. • This also includes interruptions due to higher-priority tasks.
MIN_EXEC_DURATION	LINT - Minimum execution time of the task in µs. • This also includes interruptions due to higher-priority tasks.
MAX_EXEC_DURATION	LINT - Maximum execution time of the task in µs. • This also includes interruptions due to higher-priority tasks.
LAST_ACTIVATION_DELAY	LINT - delay time of the task in the previous cycle in µs. • A delay occurs when higher priority tasks are pending at the time of task activation.
MIN_ACTIVATION_DELAY	LINT - Minimum delay time of the task in µs. • A delay occurs when higher priority tasks are pending at the time of task activation.
MAX_ACTIVATION_DELAY	LINT - Maximum delay time of the task in µs. • A delay occurs when higher priority tasks are pending at the time of task activation.
EXEC_TIME_THRESHOLD[1]	LINT - threshold that you can define for the sum of the execution time and the delay time.
EXEC_TIME_THRESHOLD_CNT	UDINT - If the defined threshold EXEC_TIME_THRESHOLD is exceeded, the value of the variable EXEC_TIME_THRESHOLD_CNT is incremented.
NAME[1]	STRING - name of the task.
EXCEPTION_COUNT	USINT - number of exceptions.
EXCEPTION_INFOS	ESM_EXCEPTION_INFO_ARRAY
[1] ... [2]	ESM_EXCEPTION_INFO - Information on the exceptions [1 ... 2][2].
TYPE_ID	UDINT - ID of the exception.
SUB_TYPE	STRING512 - exception type.
SUB_TYPE_ID	UDINT - ID of the task in which the exception occurred.
TASK_NAME	STRING - name of the task in which the exception occurred.
PROGRAM_NAME	STRING512 - name of the program instance in which the exception occurred.
INFORMATION	STRING512 - information about the exception that occurred.

1) You can set the system variable in the Tasks and events editor of the software iCube Engineer.

2) Please note that some CPUs only support ESM1. *3.3 Technical Data on page 104*

(6) SliceBus System Variables

Information
- Please consider the System SLIO power and clamp modules do not have any module ID. These cannot be recognized and are therefore not taken into account when listing or assigning the slots.
- The counting of the slots starts at 1, i.e. the 1st slot corresponds to bit 0 in the corresponding diagnostic register.
- A diagnostic interrupt is not automatically acknowledged. The acknowledgement happens by reading the diagnosis. As long as a diagnostic interrupt is not acknowledged, no further diagnostic interrupt is issued at this slot.

Diagnostic interrupt handling

- As soon as a module reports a diagnostic interrupt via the backplane bus, this is automatically recognized by the CPU and in SB_DIAG_ALARM_STATUS the register bit corresponding to the slot is set.
- The diagnostic interrupt must be enabled for the module in iCube Engineer.
- You can acknowledge a diagnostic message by reading record set 0x00 (diagnostics) or 0x01 (extended diagnostics) from the corresponding slot. Information concerning the structure of the diagnostic data may be found in the manual of the corresponding System SLIO module.
- In iCube Engineer you can use the Y_SB_DataRecordRead block from the system library to read the corresponding record set. To do this, you must first add the [Y_SliceBus.pcwlx] system library to your project.

System variable	Type - description
SB_DATA_VALID	BOOL - bus activity • This variable is set if data transfer via SliceBus is active.
SB_TOPOLOGY_OK	BOOL - bus topology • This variable is set when the plugged modules on the SliceBus match the configuration.
SB_DIAG_ALARM_STATUS	ULINT - diagnostic status of the modules • As soon as a module reports a diagnostic alarm on the SliceBus, according to the slot position the corresponding bit is set in the 64-bit register.
SB_DIAG_ALARM_ACK_PENDING	ULINT - acknowledgement diagnostic status of the modules • As soon as a module on the SliceBus requests an acknowledgement of the diagnostic alarm, according to the slot position the corresponding bit is set in the 64-bit register.

(7) EtherCAT System Variables

The system variables for diagnostics of the EtherCAT master and the connected EtherCAT slaves are listed below.

System variable	Description
EC_MASTER_STATE	BYTE - master state • Returns the state of the EtherCAT master: – 00h: Unknown - the state is unknown. – 01h: INIT – 02h: PreOp – 04h: SafeOp – 08h: OP
EC_MASTER_LINK_CONNECTED	BOOL - physical connection • Set when an Ethernet cable is connected to the EtherCAT master.
EC_TOPOLOGY_OK	BOOL - topology OK • Set when current topology and configured topology match.
EC_DC_IN_SYNC	BOOL - distributed clocks • Set when the distributed clocks are synchronized.
EC_CYCLIC_LOST_FRAMES	DWORD - missing frames (cyclic) • Returns the number of frames lost during cyclic communication.
EC_ACYCLIC_LOST_FRAMES	DWORD - missing frames (acyclic) • Returns the number of frames lost during acyclic communication.
EC_NUM_CONFIGURED_SLAVES	WORD - configured number of slaves • Returns the number of configured EtherCAT slaves.

Continued on next page.

Continued from previous page.

System variable	Description
EC_NUM_AVAILABLE_SLAVES	WORD - number of slaves in the network • Returns the number of EtherCAT slaves found when searching the EtherCAT network.
EC_SLAVES_IN_MASTER_STATE	BOOL - EtherCAT slaves in master state • Set when all EtherCAT slaves on the EtherCAT master have the state of the EtherCAT master.
EC_SLAVE_STATION_ADDRESS	ARRAY[0…512] OF WORD[1] - slave addresses • Returns all addresses of the EtherCAT slaves connected to the EtherCAT master.
EC_SLAVE_STATE	ARRAY[0…512] OF BYTE[1] - slave states • Returns all states of the EtherCAT slaves connected to the EtherCAT master: – 00h: The state is unknown. – 01h: INIT – 02h: PreOp – 03: BootStrap – 04h: SafeOp – 08h: OP
EC_SLAVE_LAST_AL_STATUS_CODE	ARRAY[0…512] OF WORD[1] - Slave AL Status codes • Returns last read AL Status Codes of the EtherCAT slaves connected to the EtherCAT master.
1) Index 0 is reserved. The 1. EtherCAT slave is assigned to Index 1.	

(8) PROFINET System Variables Optional

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

Table 5.8 PROFINET system variables - PROFINET controller functionality

System variable	Type - description
PNIO_SYSTEM_BF	BOOL - Missing connection to a configured PROFINET device. • An error has occurred in the PROFINET network, i.e. no connection could be established to at least one configured PROFINET device. • This value is not set if the "Control BF" parameter on a PROFINET device was set to FALSE. The PROFINET device was thus removed from the connection monitoring.
PNIO_SYSTEM_SF	BOOL - Diagnostic interrupt on a configured PROFINET device. • At least one PROFINET device reports a system error as a diagnostic interrupt or maintenance alarm. • The error priority can be found in the variables PNIO_DIAG_AVAILABLE, PNIO_MAINTENANCE_DEMANDED and PNIO_MAINTENANCE_REQUIRED.
PNIO_MAINTENANCE_DEMANDED	BOOL - maintenance demand • At least one PROFINET device reports a "maintenance demand" - maintenance alarm with high priority when the connection is active. • The PROFINET device can be identified by means of the RALRM diagnostic block.
PNIO_MAINTENANCE_REQUIRED	BOOL - maintenance required • At least one PROFINET device reports a "maintenance required" - maintenance alarm with low priority when the connection is active. The PROFINET device can be identified by means of the RALRM diagnostic block.
PNIO_FORCE_FAILSAFE	BOOL - All PROFINET devices are prompted to set their configured substitute values. • The system variable can be written/set from the program if required.
PNIO_CONFIG_STATUS	WORD - configuration status of the PROFINET controller.

Continued on next page.

Continued from previous page.

System variable	Type - description
PNIO_CONFIG_STATUS_READY	BOOL - PROFINET controller initialized. • This variable is set if the PROFINET controller could be initialized without errors. • No target iCube Engineer configuration has been loaded yet.
PNIO_CONFIG_STATUS_ACTIVE	BOOL - target configuration loaded. • This variable is set when a target configuration was uploaded to the PROFINET controller. • In this state, the PROFINET controller tries to establish a connection cyclically to all devices of the target configuration.
PNIO_CONFIG_STATUS_CFG_FAULT	BOOL - target configuration error. • The target configuration of the PROFINET controller was not accepted due to a serious error. • Please contact our support!
PNIO_FORCE_PRIMARY	BOOL - This variable is used by function blocks for applicative redundancy to specify the SRL role of the PROFINET controller.

Table 5.9 PROFINET system variables - PROFINET device functionality

System variable	Type - description
PND_S1_PLC_RUN	BOOL - Status of the higher-level PROFINET controller. • Information whether the higher-level PROFINET controller is active. • The value is TRUE if the higher-level PROFINET controller is in RUN state and the program is being processed. • The indication is only valid with existing PROFINET connection (PND_S1_VALID_DATA_CYCLE).
PND_S1_VALID_DATA_CYCLE	BOOL - the higher-level PROFINET controller has established the connection. • Information whether a connection exists and cyclic data is exchanged between PROFINET controller and PROFINET device and the last received frame contained valid data.
PND_S1_OUTPUT_STATUS_GOOD	BOOL - IOP status of the higher-level PROFINET controller. • Information whether the PROFINET device has received the input process data (PND_S1_INPUTS) with the status "valid". • The value is TRUE if the output data of the higher-level PROFINET controller are valid (provider status).
PND_S1_INPUT_STATUS_GOOD	BOOL - IOC status of the higher-level PROFINET controller.
PND_S1_DATA_LENGTH	WORD - process data length which was configured for the PROFINET device.
PND_S1_OUTPUTS	PND_IO_512 - output process data • Memory area for output process data that the PROFINET device sends to the higher-level PROFINET controller.
PND_S1_INPUTS	PND_IO_512 - input process data • Memory area for input process data that the PROFINET device receives from the higher-level PROFINET controller.
PND_IO_DRIVEN_BYPLC	INT - Applicative system redundancy • Number of the PROFINET controller currently connected to the PROFINET device. • Indication from which higher-level PROFINET controller the data in the PROFINET device come from. – 0: No PROFINET controller – 1: PROFINET controller A – 2: PROFINET controller B

4.15.3 System Variables Safety

(1) System Variable SPLC

- The system variable SPLC is a system variable organized as a data structure.
- The SPLC system variable provides the following information about the safety CPU using the SPNSV2_TYPE data structure.

System variable			Type - description
SPLC			SPNSV2_TYPE - Data structure
	PRJ		
		Name	STRING - Name of the iCube Engineer project.
		CRC	DWORD - Project CRC (32-bit) of the safety CPU boot project.
		EXEC_TIME	UDINT - Runtime of the safety CPU programme cycle in µs.
		HAS_PRJ	BOOL - Set if safety-related application program and program sources exist in the memory of the safety CPU.
	DIAG		
		STATUS_REG	WORD - Diagnostic status register of the safety CPU. • Contains the status information of the safety CPU. It reflects the status of the safety CPU including any error states of the safety CPU that may have occurred at any time. • Additional information and error parameters, especially in the fail safe, are contained in the associated diagnostic parameter registers of the safety CPU (elements SPNS.DIAG.PARAM_REG and SPNS.DIAG.PARAM_2_REG). *4.15.3(2) Diagnostic Status Register SPLC.DIAG.STATUS_REG.xxx on page 175*
		PARAM_REG	WORD - Diagnostic parameter register 1 of the safety CPU (error code).
		PARAM_2_REG	WORD - Diagnostic parameter register 2 of the safety CPU (additional error messages for service/support).
		EXT_PARAM_REG	DWORD - Extended diagnostic parameter register of the safety CPU (additional error messages for service/support).
		CH2_PARAM_REG	WORD - Diagnostic parameter register 1 of the safety CPU channel 2 (CH2) (error code).
		CH2_PARAM_2_REG	WORD - Diagnostic parameter register 2 of the safety CPU channel 2 (CH2) (additional error messages for service/support).
		CH2_EXT_PARAM_REG	DWORD - Extended diagnostic parameter register of the safety CPU channel 2 (CH2) (additional error messages for service/support).

Continued on next page.

Continued from previous page.

System variable	Type - description
INFO	
CYCLE_TIME	UDINT - Safety CPU cycle in µs.
TEMP	
TEMP_CURRENT	INT - Current measured temperature of the safety CPU.
TEMP_MIN	INT - Minimum measured temperature of the safety CPU since the last PowerON of the device.
TEMP_MAX	INT - Maximum measured temperature of the safety CPU since the last PowerON of the device.
STATUS_REG	WORD - Safety CPU temperature status register. • 0x0000: TThe temperature of the safety CPU is in uncritical range. • 0x0080: The temperature of the safety CPU is close to the tolerance limit in the critical range. The CPU remains in the RUN state and returns a warning with the error code 0xFA41. • 0x8000: The temperature of the safety CPU is exceeding the permissible range. The safety CPU switches to the safety state and returns an error with the error code 0x924D.
CPU	
LOAD_CURRENT	INT - Current CPU load of the safety CPU.
LOAD_MIN	INT - Minimum CPU load of the safety CPU since the last PowerON of the device.
LOAD_MAX	INT - Maximum CPU load of the safety CPU since the last PowerON of the device.
STATUS_REG	WORD - CPU status register of the safety CPU.
FW_VERSION	
VERSION_MAJOR	BYTE - Main version of the safety CPU firmware (major version).
VERSION_MINOR	BYTE - Side version of the safety CPU firmware (minor version).
VERSION_BUILD	WORD - Build number of the safety CPU firmware.
FPGA_VERSION	
VERSION_MAJOR	BYTE - Major version of the Safety CPU hardware FPGA (major version).
VERSION_MINOR	BYTE - Side version of the safety CPU hardware FPGA (minor version).
VERSION_BUILD	WORD - Build number of the safety CPU hardware FPGA.
FW_UPDATE_STATUS	UINT - Status of the safety firmware update.
SOFT_RESET_REG	WORD - Software reset register of the safety CPU.

NOTICE

The warning threshold for CPU load is 70%, the switch-off threshold is 90%. If the 90% CPU load is exceeded, the safety CPU switches off.

(2) Diagnostic Status Register SPLC.DIAG.STATUS_REG.xxx

- The following table describes the information of the bits (0 ... 15) in the diagnostic status register (SPLC.DIAG.STATUS_REG.xxx).

System variable/elements	Type - description
SPLC	SPNSV2_TYPE - Data structure
DIAG	
STATUS_REG	
DBG[2]	BOOL - Non-safe debug operation of the safety CPU. • The safety CPU is in one of the two DEBUG states (DEBUG-RUN or DEBUG-STOP/DEBUG-HALT).
EST	BOOL - There is an entry in the error memory of the safe operating system (error stack) of the safety CPU. Diagnostic and error messages from the safe operating system of the safety CPU are available. • These messages can be read and analyzed via iCube Engineer. • The variable always has the value TRUE if at least one entry is contained in the error memory of the safety operating system. • As soon as the error memory was read via iCube Engineer and thus cleared, the value of the variable changes to FALSE.
FS	BOOL - Failure state of the safety CPU. • An error was detected that puts the safety CPU in fail safe state. *4.11 Fail Safe States on page 137* • In this state, the associated, more detailed error code is contained in the diagnostic parameter registers of the safety CPU (SPLC.DIAG.PARAM_REG and SPLC.DIAG.PARAM_2_REG).
INIT[1]	BOOL - Initialization of the safety CPU. • The initialization of the safety CPU firmware (safe operating system) was completed without errors.
IO[1]	BOOL - Initialization of the safety I/O channel communication. • The initialization of the FSoE communication to the I/O devices was completed without errors.
PON[1]	BOOL - PowerON process. • The safety CPU is powered. The firmware was loaded into the RAM memory of the safety CPU and booted up. The self-test routines of the safety CPU were completed without errors.
POST	BOOL - PowerON self-test of the safety CPU (**P**OWER **O**N **S**ELF **T**EST). • Self-test of the safety CPU active after PowerON.
PRO[1]	BOOL - Load and start the safety application program. • The safety-related application programme created with iCube Engineer was loaded into the safety operating system of the safety CPU and started without errors.
RUN[2]	BOOL - Execution of the safety application program (RUN). • The safety CPU executes the safety application program and is in one of the two RUN states (SAFE-RUN or DEBUG-RUN).
SYN[1]	BOOL - Synchronization of safety and standard components within the safety CPU. • The synchronization of the safety and standard components within the safety CPU was successfully completed.
WARN	BOOL - Safety CPU warning. • There is a collective warning message from the safety CPU.

- 1) The variables reflect the startup status of the safety CPU. The start-up sequence is as follows:
  - PowerON process
  - Initialization of the safety CPU.
  - Loading and starting the safety application program.
  - Synchronization of safety and standard components within the safety CPU.
  - Initialization of safety I/O channel communication.
- 2) The variables indicate the RUN and DEBUG safety CPU operating states.

(3) Meaning of the Bits

The diagnostic status register SPLC.DIAG.STATUS_REG contains the status information of the safety CPU. It reflects the status of the safety CPU including any error states of the safety CPU that may have occurred at any time. Additional information and error parameters, especially in the fail safe (FS) state, are contained in the associated diagnostic parameter registers of the safety CPU (SPLC.DIAG.PARAM_REG and SPLC.DIAG.PARAM_2_REG) and in the extended diagnostic parameter register (SPLC.DIAG.EXT_PARAM_REG).

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
FS	POST	res.	EST	res.	res.	res.	res.	WARN	DBG	RUN	I/O	SYN	PRO	INIT	PON

- Bit 4 ... 0: Start-up status of the safety CPU.
  - PON - Power ON process completed.
    This bit is set as soon as the safety CPU is powered. The firmware was loaded into the RAM memory of the safety CPU and booted up. The self-test routines of the safety CPU were successfully completed.
  - INIT - Initialization of the safety CPU completed.
    This bit is set as soon as the initialization of the safety CPU firmware (safe operating system) was completed without errors.
  - PRO - Safety user program loaded and started.
    This bit is set as soon as the safety user program, which was created with iCube Engineer, was loaded into the safety operating system of the safety CPU and started without errors.
  - SYN - Synchronization of safety and standard components of the safety CPU.
    The bit is set when the safety and standard components of the safety CPU are synchronized.
  - I/O - I/O channel communication initialized.
    This bit is set as soon as the initialization of the safety CPU firmware (safety operating system) was completed without errors.
- Bit 6, 5: Operating status of the safety CPU:
  - RUN - RUN operation of the safety CPU.
    This bit is set if the safety CPU is executing the safety user program and is in one of the two RUN states (SAFE-RUN or DEBUG-RUN).
  - DBG - Non-safe debug operation of the safety CPU.
    This bit is set if the safety CPU is in one of the two DEBUG states (DEBUG-RUN or DEBUG-STOP/DEBUG-HALT). This bit is not set in the SAFE-STOP and SAFE-RUN states.
- Bit 7: Warning
  - WARN - The set WARN bit (WARNING) indicates a collective warning message from the safety CPU.
- Bit 11 ... 8: reserved
- Bit 12: Error stack
  - EST - The EST (error stack) bit indicates that diagnostic and error messages are present from the safety operating system of the safety CPU.
    This bit is set if there is at least one entry in the error memory of the safety operating system. These messages can be read and analyzed via iCube Engineer. As soon as the error memory was read via iCube Engineer and thus cleared, this bit is automatically reset.
- Bit 13: reserved
- Bit 14: POST
  - POST - POWER ON SELF TEST
    This bit is set for the duration of the **P**ower-**O**N-**S**elbst**T**est of the safety CPU. After the self-test is completed, it is reset.
- Bit 15: Fail safe state
  - FS - Failure State
    This bit is set as soon as an error is detected that sets the Safety CPU to the Fail Safe state. *4.11 Fail Safe States on page 137* In this state, the corresponding further error code is contained in the diagnostic parameter registers of the safety CPU (SPLC.DIAG.PARAM_REG and SPLC.DIAG.PARAM_2_REG).

(4) System Variables SPLC_CONTROL_COMMAND and SPLC_CONTROL_CONFIRM

- The system variable SPLC_CONTROL_COMMAND is used to request the resetting of diagnostic values from the non-safety project.
- Via the system variable SPLC_CONTROL_CONFIRM, the safety CPU confirms in the non-safety project that the diagnostic values were reset.

Table 5.10 SPLC_CONTROL_COMMAND

System variable		Type - description
SPLC_CONTROL_COMMAND		SPLC_CONTROL _TYPE - Data structure with 32 bits for enabling functions of the safety CPU.
	CODE	• DWORD - Bit 0: Request resetting of the minimum and maximum safety round trip times (SRT_MIN, SRT_MAX). – Data direction within the Safety CPU: Standard component ☒ Safety component
	PARAM	• DWORD - Bit 31 ... 1: Reserved

Table 5.11 SPLC_CONTROL_CONFIRM

System variable		Type - description
SPLC_CONTROL_CONFIRM		SPLC_CONTROL _TYPE - Data structure with 32 bits for confirming functions of the safety CPU that were requested via the variable SPLC_CONTROL_COMMAND.
	CODE	• DWORD - Bit 0: Confirmation resetting the minimum and maximum safety round trip times (SRT_MIN, SRT_MAX). – Data direction within the Safety CPU: Safety component ☒ Standard component
	PARAM	• DWORD - Bit 31 ... 1: Reserved

(5) System Variables FDEV_INx and FDEV_OUTx (x = 0 ... 7)

These system variables are used for data exchange between the standard and safety components of the safety CPU.

- The system variables FDEV_IN0 to FDEV_IN7 contain the input process data (8 * 1 byte) of the safety component of the safety CPU.
- The system variables FDEV_OUT0 to FDEV_OUT7 contain the output process data (8 * 1 byte) of the safety component of the safety CPU.

Data direction

- FDEV_INx = I
- FDEV_OUTx = Q

Table 5.12 FDEV_INx and FDEV_OUTx (x = 0 ... 7)

System variable	Type - description
FDEV_IN0 ... FDEV_IN7	SAFEBYTE - Input process data of the safety component of the safety CPU.
FDEV_OUT0 ... FDEV_OUT7	SAFEBYTE - Output process data of the safety component of the safety CPU.

4.15.4 FSoE Diagnostic Variables

(1) General

Status information is forwarded to the SafeOS Diag IN (DI) area for each FSoE master connection. The FSoE master connection can be controlled by the SafeOS Diag OUT (DQ) area. There are connection-specific diagnostic variables for each FSoE connection and global diagnostic variables. The following table lists the connection-specific diagnostic variables for each FSoE connection. The xxxxx placeholder represents the respective configured-FSoE-address.

Table 5.13 FSoE connection-specific diagnostic variables

Variable name	Data direction
FSOE_MSTR_ADDR_xxxxx_ACK_REQ	DI
Acknowledge request • 1: Variable is set to 1 if a previously occured FSoE communication error was resolved and can be acknowledged. This is recognized by an edge change in SAPL_DataValidChangedClbk() from FailSafeData to ProcessData. As long as variable = 1, – fail safe values are forwarded to the SafeOS process image inputs for this communication instance. This also applies if the communication instance has already returned process data (signalled by SAPL_DataValidChangedClbk() ProcessData). – the outgoing PDU for the communication instance is set via SSD_IoDataCmdSet() to fail safe status. • 0: Variable is set to 0 if the acknowledge request is confirmed by FSOE_MSTR_ADDR_xxxx_ACK_REI = 1. As long as variable = 0, – the SafeData(FailSafeData on ProcessData) for this communication instance are directly forwarded to the SafeOS process image inputs.	
FSOE_MSTR_ADDR_xxxxx_ACK_REI	DQ
Acknowledge reintegration • 1: The variable FSOE_MSTR_ADDR_xxxx_ACK_REQ is set to 0. • 0: There ist no action.	
FSOE_MSTR_ADDR_xxxxx_PASS_OUT	DI
Passivation enabled on input side: The connected FSoE slave sends fail safe on this FSoE connection • 1: The variable is set to 1 if SAPL_DataValidChangedClbk() returns FailSafeData. • 0: Variable is set to 0 if SAPL_DataValidChangedClbk() returns ProcessData.	
FSOE_MSTR_ADDR_xxxxx_PASS_ON	DQ
Passivation enabled on output side: The FSoE master sends fail safe on this FSoE connection. • 1: If the variable = 1, the output message of this communication instance is set to FailSafeData. In addition, FSOE_MSTR_ADDR_xxxx_PASS_OUT = 1 is set (input data to fail safe). • 0: If the variable = 0, the output message of this communication instance ProcessData is set.	

⚠ WARNING

Resetting FSOE_MSTR_ADDR_xxxxx_PASS_ON

Resetting this variable results in the immediate transfer of the safety input and output data. Take appropriate measures to ensure that there is no danger to your plant/machine when the passivation of the F device is deactivated.

Variable name	Data direction
FSOE_MSTR_ADDR_xxxxx_CE_CRC	DI
CRC error on input side: The FSoE master detected a CRC error in the incoming FSoE PDU. • 1: Variable is set to 1 if SAPL_FsoeErrorClbk() returns the following error: FSOE_k_COMM_ERR_INV_CRC • 0: Variable is set to 0 if – SAPL_DataValidChangedClbk() returns ProcessData. – SAPL_FsoeStateChangedClbk() signals that the data state was left.	
FSOE_MSTR_ADDR_xxxxx_WD_TIMEOUT	DI
Watchdog timeout on input side: The FSoE master has a watchdog timeout for the incoming FSoE PDU. • 1: Variable is set to 1 if SAPL_FsoeErrorClbk() returns the following error: FSOE_k_COMM_ERR_WD_EXPIRED. • Variable is set to 0 if – SAPL_DataValidChangedClbk() returns ProcessData. – SAPL_FsoeStateChangedClbk() signals that the data state was left.	

Continued on next page.

Continued from previous page.

Variable name	Data direction
FSOE_MSTR_ADDR_xxxxx_COMM	DI
Any other recoverable FSoE communication errors: • 1: Variable is set to 1 if SAPL_FsoeErrorClbk() returns the following error: – FSOE_K_COMM_ERR_LOCAL_RESET_OR_ACK – FSOE_K_COMM_ERR_INV_CMD – FSOE_K_COMM_ERR_UNK_CMD – FSOE_K_COMM_ERR_INV_CONNID – FSOE_K_COMM_ERR_INV_ADDRESS – FSOE_K_COMM_ERR_INV_DATA – FSOE_K_COMM_ERR_INV_COMMPARALEN – FSOE_K_COMM_ERR_INV_COMPARA – FSOE_K_COMM_ERR_INV_USRPARALEN – FSOE_K_COMM_ERR_INV_USRPARA – FSOE_K_COMM_ERR_INV_SAFEPARA_START • 0: Variable is set to 0 if – SAPL_DataValidChangedClbk() returns ProcessData. – SAPL_FsoeStateChangedClbk() signals that the data state was left.	

Table 5.14 Global diagnostic variables

Variable name	Data direction
ACK_REQ_FSOE_MSTR_GLOBAL	DI
Acknowledge request: At least one FSoE connection waits for an operator acknowledge request, e.g. after a change from fail-safe to process data communication. • Global equivalent to FSOE_MSTR_ADDR_xxxx_ACK_REQ. • At least one communication instance behaves as described in FSOE_MSTR_ADDR_xxxx_ACK_REQ.	
ACK_REI_FSOE_MSTR_GLOBAL	DQ
Acknowledge reintegration: All previous ACK_REQs for this FSoE connection are acknowledged. • Global equivalent to FSOE_MSTR_ADDR_xxxx_ACK_REI. • Set all communication instances as described in FSOE_MSTR_ADDR_xxxx_ACK_REI. • If a specific ACK_REI is set, the global ACK_REI must not be enabled.	
PASS_OUT_FSOE_MSTR_GLOBAL	DI
Passivation enabled on input side: At least one FSoE connection sends fail-safe. • Global equivalent to FSOE_MSTR_ADDR_xxxx_PASS_OUT. • At least one communication instance behaves as described in FSOE_MSTR_ADDR_xxxx_PASS_OUT.	
CE_CRC_FSOE_MSTR_GLOBAL	DI
CRC error on input side: At least one FSoE connection has recognized a CRC error in the incoming FSoE PDU. • Global equivalent to FSOE_MSTR_ADDR_xxxx_CE_CRC. • At least one communication instance behaves as described in FSOE_MSTR_ADDR_xxxx_CE_CRC.	
WD_TIMEOUT_FSOE_MSTR_GLOBAL	DI
Watchdog timeout on input side: At least one FSoE connection has a watchdog timeout. • Global equivalent to FSOE_MSTR_ADDR_xxxx_WD_TIMEOUT. • At least one communication instance behaves as described in FSOE_MSTR_ADDR_xxxx_WD_TIMEOUT.	
COMM_FSOE_MATR_GLOBAL	DI
• Global equivalent to FSOE_MSTR_ADDR_xxxx_COMM. • At least one communication instance behaves as described in FSOE_MSTR_ADDR_xxxx_COMM.	

5

Web-Based Management - WBM

5.1 Overview and First Steps

5.1.1 Accessing WBM

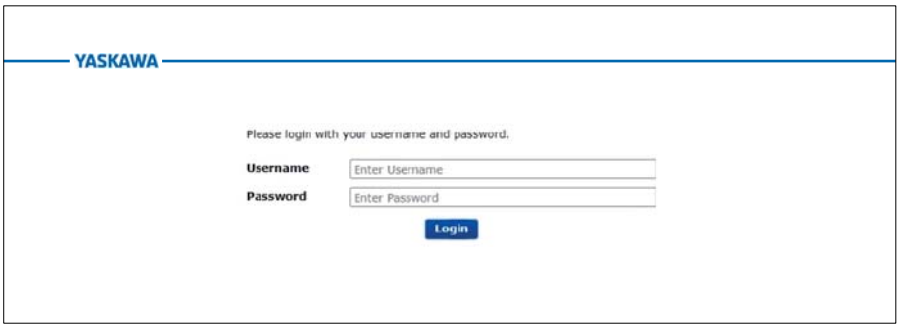
- The CPU has a web-based management (WBM). In the WBM you can access static and dynamic information and change certain settings. You may access WBM via the Ethernet interfaces of the CPU.
- The communication between the PC and CPU takes place via a security certificate, which must be located on the 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.

5.1.2 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 certificate generated by the CPU to your PC with the following proceeding:

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] .** ***5.4.4 Web Services on page 201***

   Information on as you change one of the IP addresses of the CPU, you must regenerate the certificate via [Re-gener- ate 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.** ***5.5.1 Certificate Authentication on page 204***
5. **Install the certificate according to your Windows system as a trusted root certification authority.**

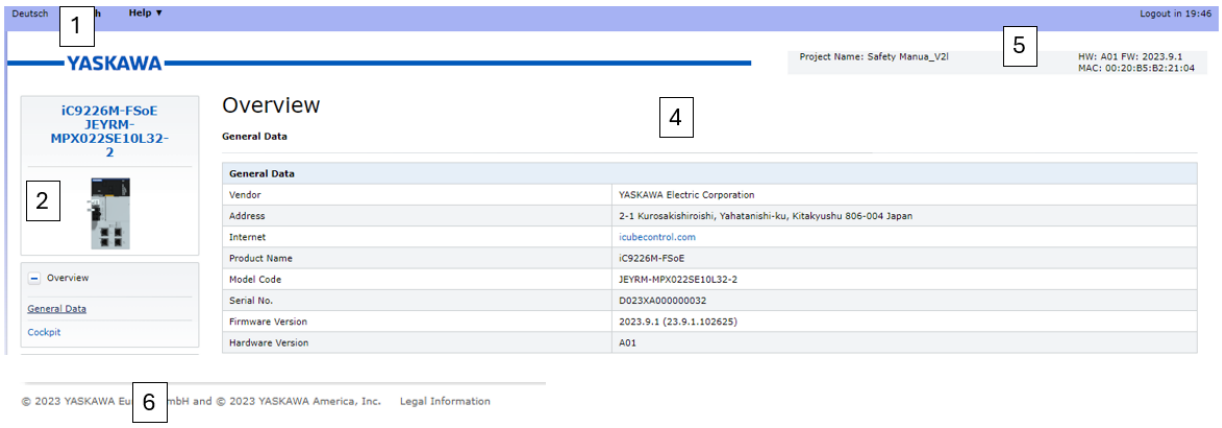
   After installation, communication between the PC and CPU takes place as a [secure connection].

⚠ 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!

5.1.3 Structural Design

The WBM is divided into the following areas:



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

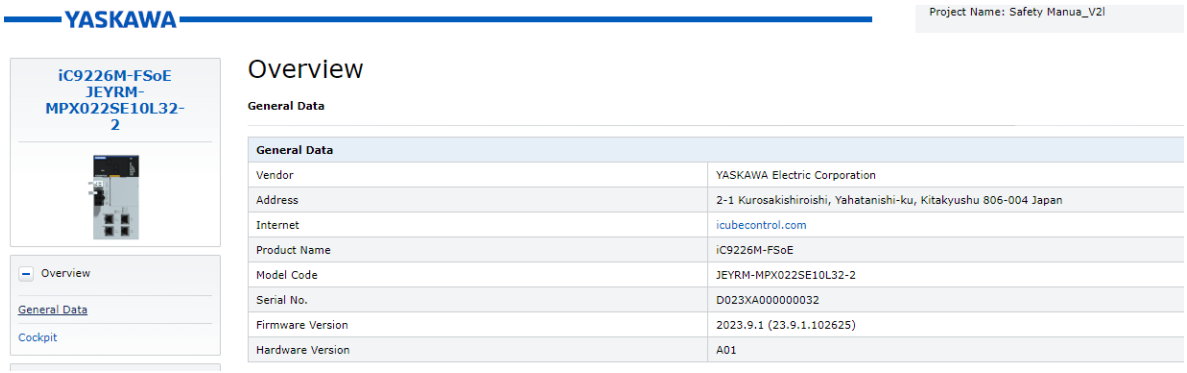
5 Shows the current hardware/firmware version and MAC address of the CPU.

6 Access to the Yaskawa software license conditions (**S**oftware **L**icense **T**erms - SLT) and the license information for the individual Linux packages.

5.2 Overview

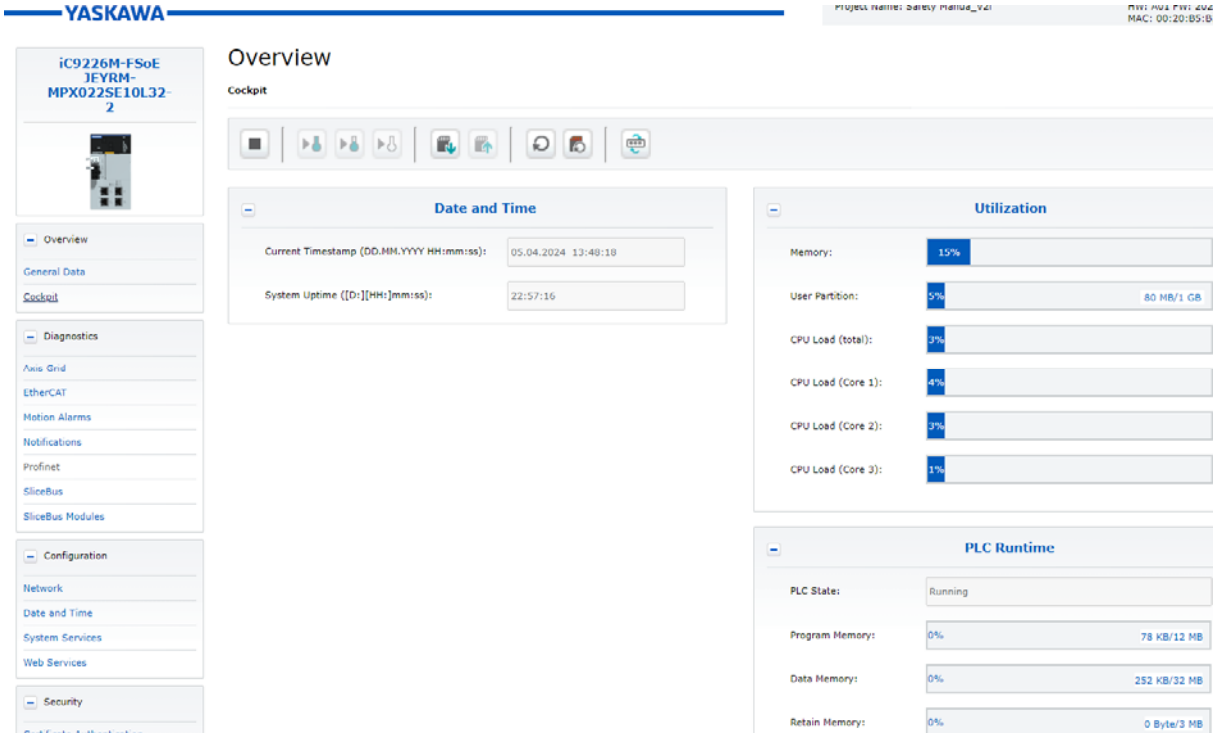
5.2.1 General Data

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



5.2.2 Cockpit

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



(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.
-  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 *5.4.2 Date and Time on page 200*.

(3) Utilization

CPU memory utilization and the CPU load are shown here.

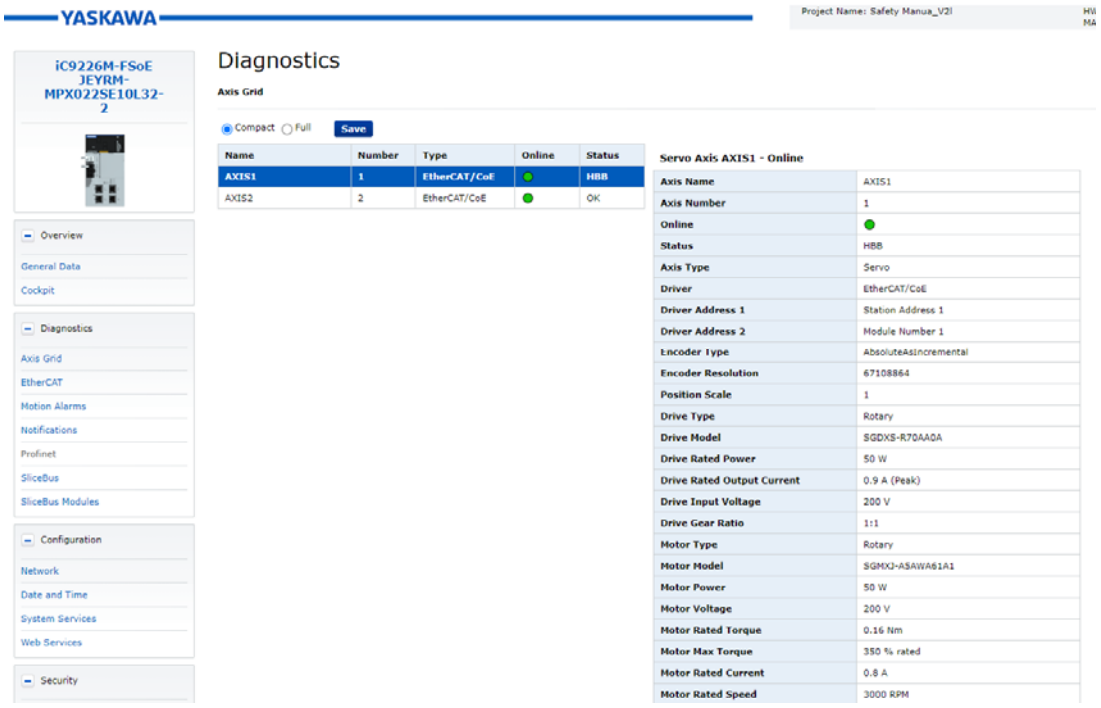
(4) PLC Runtime

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

5.3 Diagnostics

5.3.1 Axis Grid

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

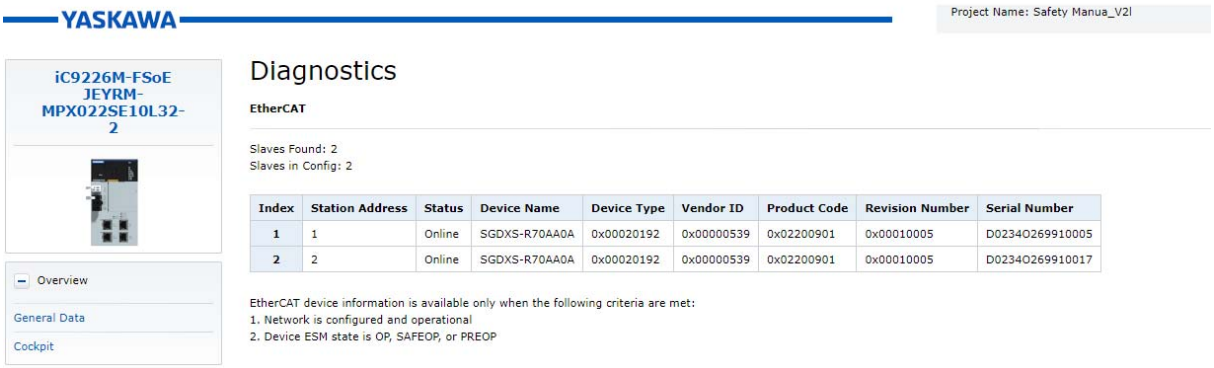


You have the following display options:

- 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.

5.3.2 EtherCAT

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

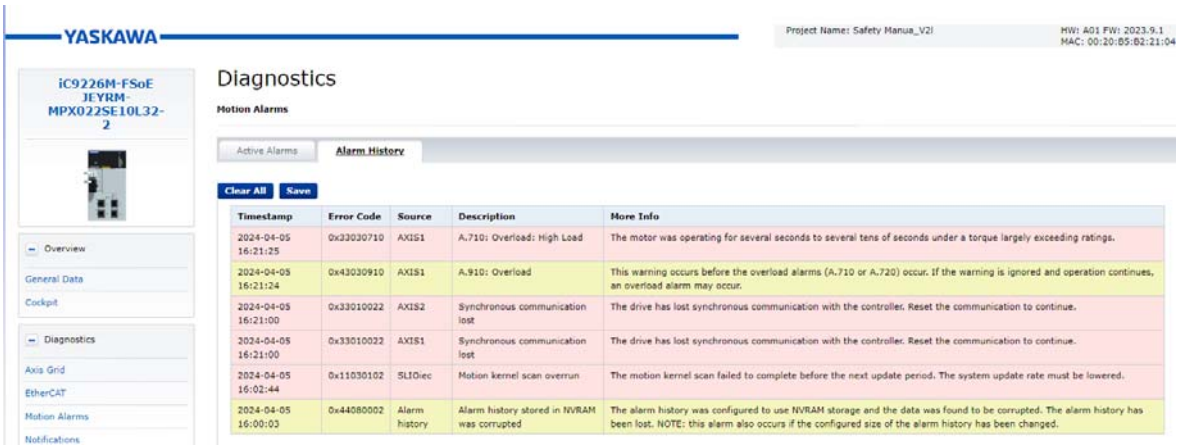


The following information is shown in tabular form:

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

5.3.3 Motion Alarms

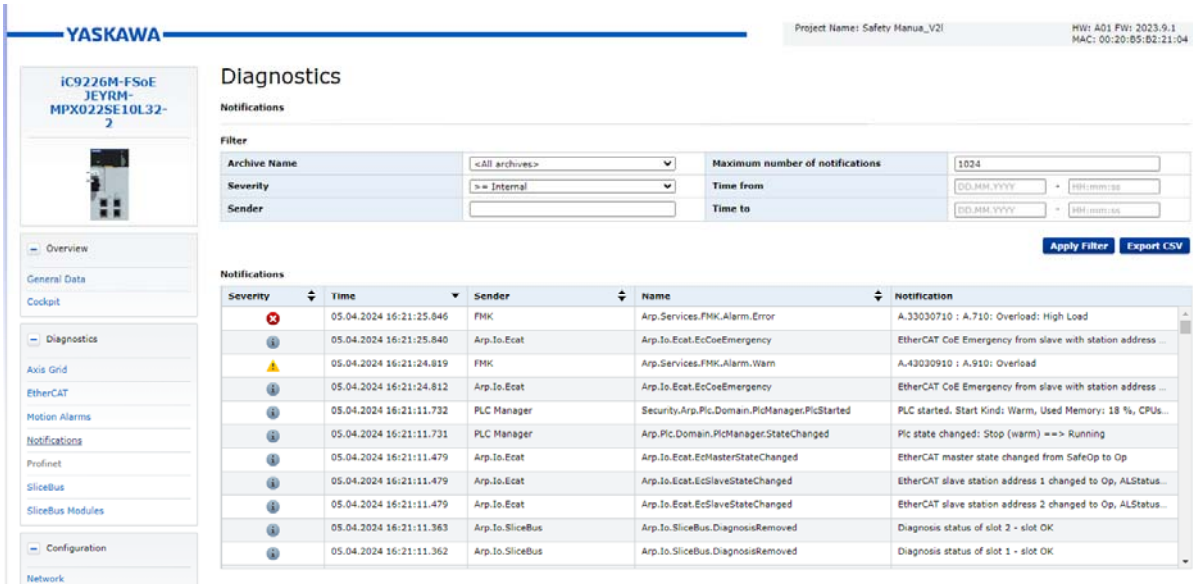
If you have connected a drive to your CPU, you will find the current motion alarms and their history here.



- [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.

5.3.4 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.



(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 :

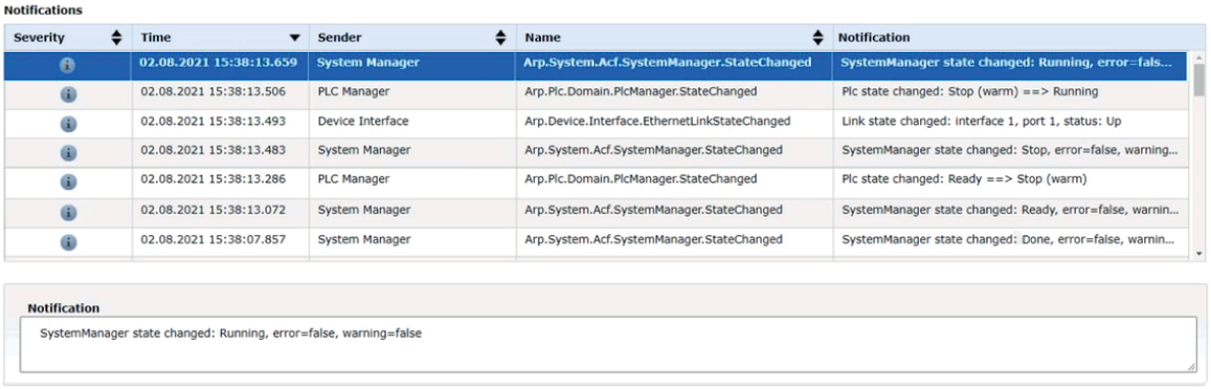
The table is sorted according to this column in ascending order.

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.



(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:

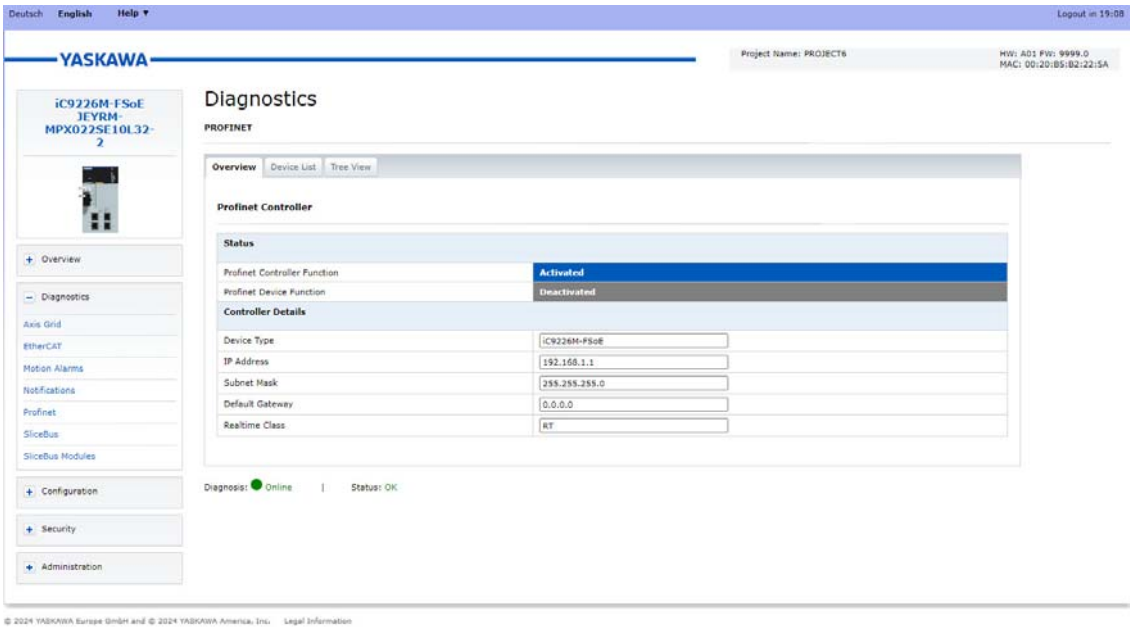
- Archive name
  - Here you can filter the message entries by specifying an archive name.
- Severity
  - Here you can limit the message entries based on their severity.
  - The limitation is based on the following graduation for the minimum severity:
    Internal ☒ Information ☒ Warning ☒ Error ☒ Critical 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.

5.3.5 PROFINET - Optional

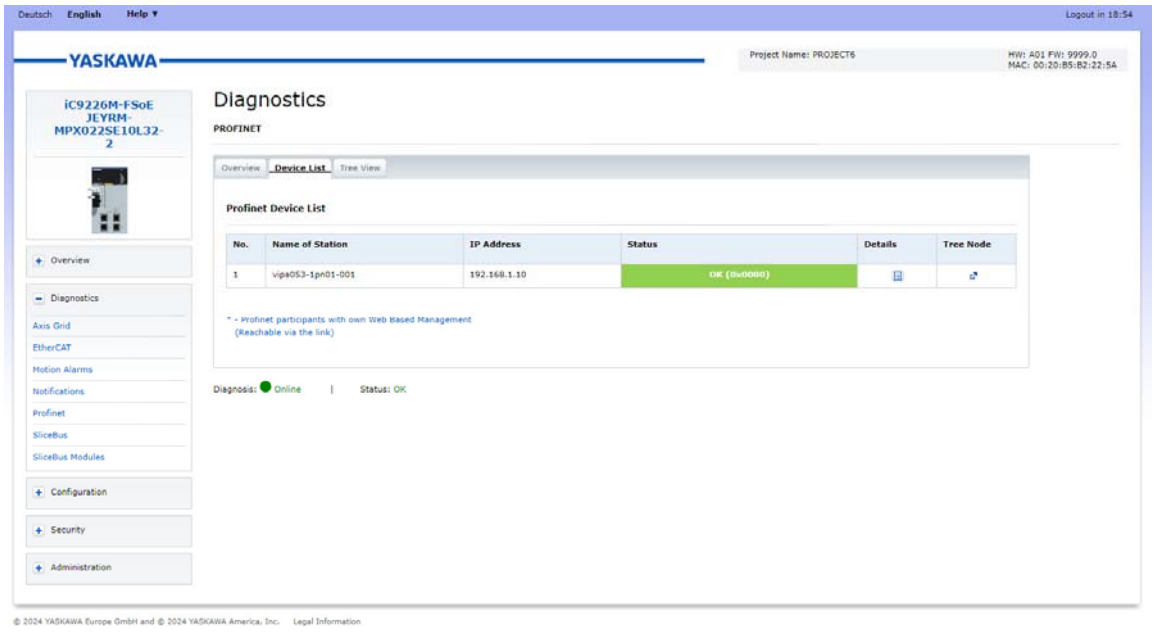
(1) Tab: [Overview]

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!



(2) Tab: [Device List]



(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.

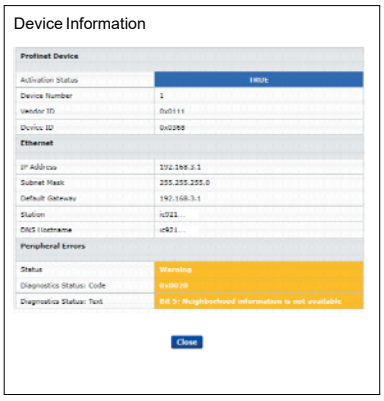
The WBM of the PROFINET device opens in a new tab in the web browser.

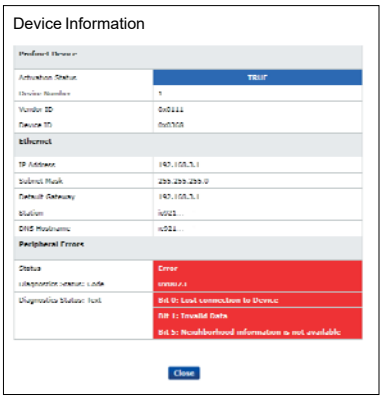
(3) Device Information

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 .

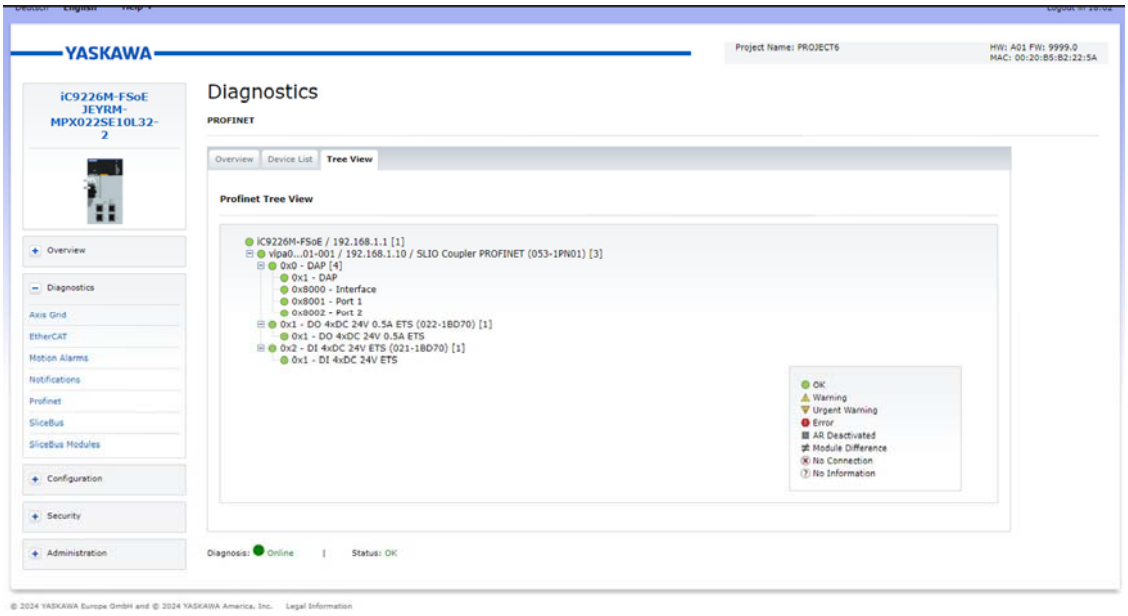
The Device Information view with the current information on IP settings and diagnostics is opened.





(4) Tab: [Tree View]

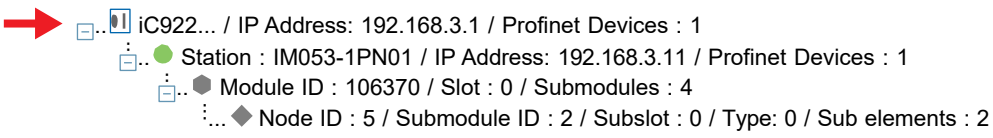
Here you have a tree view of all configured PROFINET devices. The overview contains the device names of the PROFINET devices, their current IP settings and the diagnostic status of the devices and modules. Via [+] and [-] you can open or close the next level of the Tree View.



(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



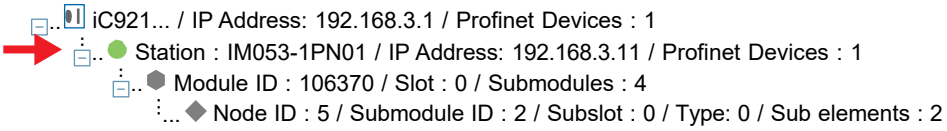
(6) Station Level

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:

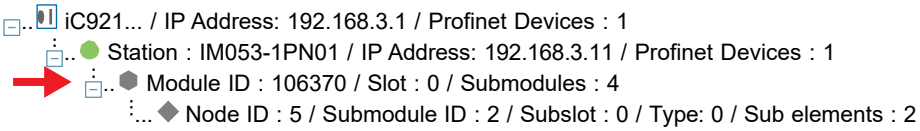
Symbol	Diagnostic status
	OK
	Warning
	Error



(7) Module Level

On module level you will find the following information:

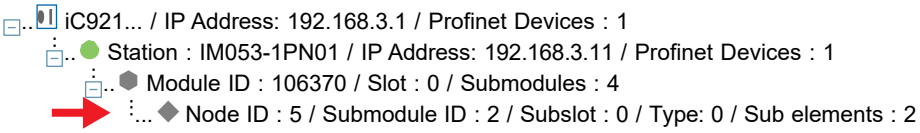
- Module ID - the ID of the module
- Slot - slot of the module
- Sub modules - the number of sub modules



(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	Bit 0 is set when there is no connection. • The PROFINET controller could not establish a connection with the PROFINET device or the AR was deactivated. – 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	Bit 1 is set if the data is invalid. • 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. – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
2	Bit 2 is set when a diagnostic message is pending. • The PROFINET device reports a diagnosis. – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.

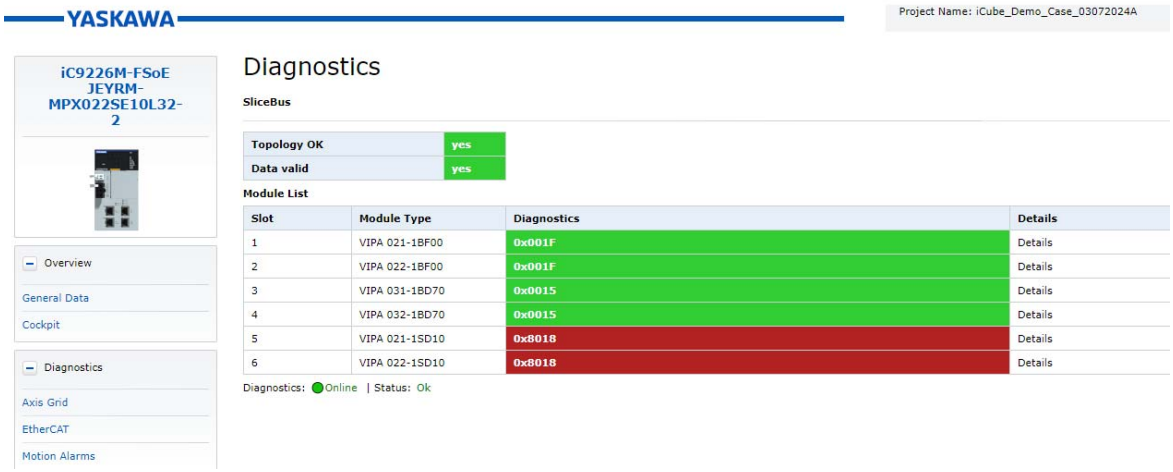
Continued on next page.

Continued from previous page.

Bit	Description and action recommendation
3	Bit 3 is set if the module deviates from the configured module. • When the PROFINET connection was initialized, a discrepancy was found between the target and current configuration. – Please check the configuration of the PROFINET device. In the iCube Engineer default setting, the connection remains established in the event of a configuration difference.
4	Bit 4 is set when the AR is disabled. • The PROFINET device is configured in the project, but the AR was disabled. – Check the PROFINET device settings and enable the AR.
5	Bit 5 is set if no neighbor information is available. • No neighbor information are available in the network used. – This is usually due to the use of components that are not at least compatible with PROFINET Conformance Class-B (CC-B). For a stable PROFINET network, you should only use CC-B or CC-C-compliant PROFINET devices.
6	Bit 6 is set if neighbor information are not uniform. • 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. – This is usually due to the use of components that are not at least PROFINET Conformance Class-B (CC-B) compatible (e.g. unmanaged switches).
7	Bit 7 is set if the alias name of a device being searched for is already being used by an AR. • 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. – This information is only an indication that the control program is probably trying to establish a connection with a device, although a connection is still active.
8	Bit 8 is set when a maintenance request is pending. • The PROFINET device has transmitted a maintenance request (maintenance alarm). – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
9	Bit 9 is set when a high-priority maintenance demand is pending. • The PROFINET device has transmitted a high-priority maintenance request (maintenance alarm). – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.
10	Bit 10 is set if a vendor- or channel-specific diagnosis is pending. • The PROFINET device has transmitted a vendor- or channel-specific diagnosis. – Please check the diagnosis of the PROFINET device and, if necessary, contact the vendor of the PROFINET device.

5.3.6 SliceBus

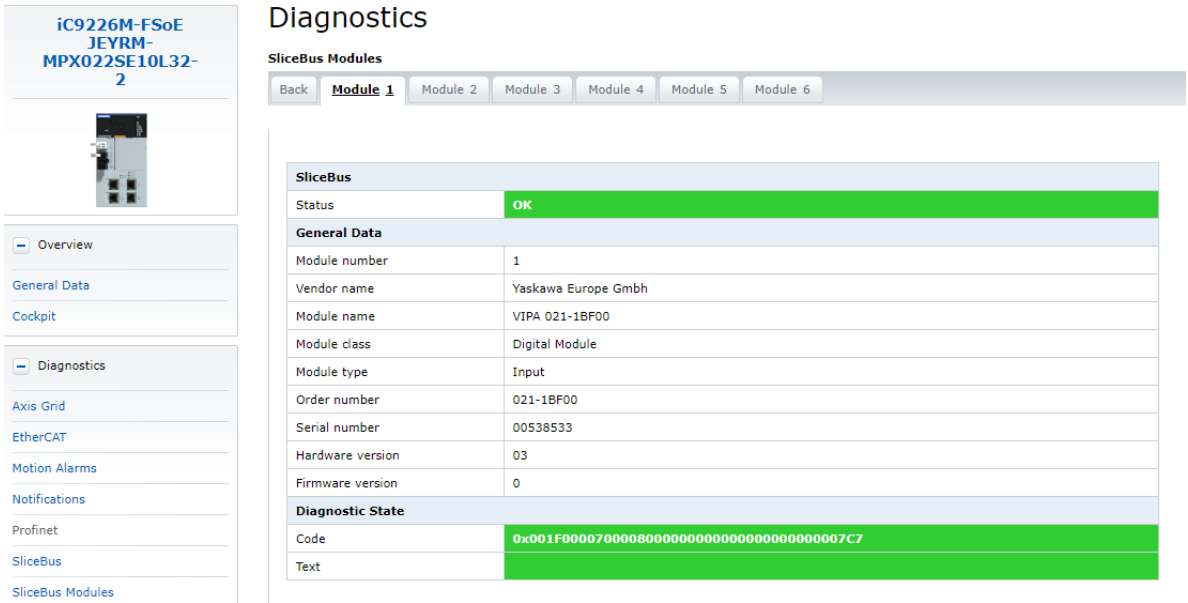
Here you will find information on the backplane bus and the connected modules.



- Topology OK
  - The topology is correct if the configured and existing modules are identical.
- Data valid
  - If the data from the backplane bus were transmitted without errors, these are valid.
- Module List
  - The connected modules and the first 2 bytes of the diagnostic data are listed here. You can find more detailed diagnostic information at [Details].

5.3.7 SliceBus Modules

Here you will find detailed information on the diagnoses of the connected modules. The content is dynamically structured and depends on the number of modules on the CPU.



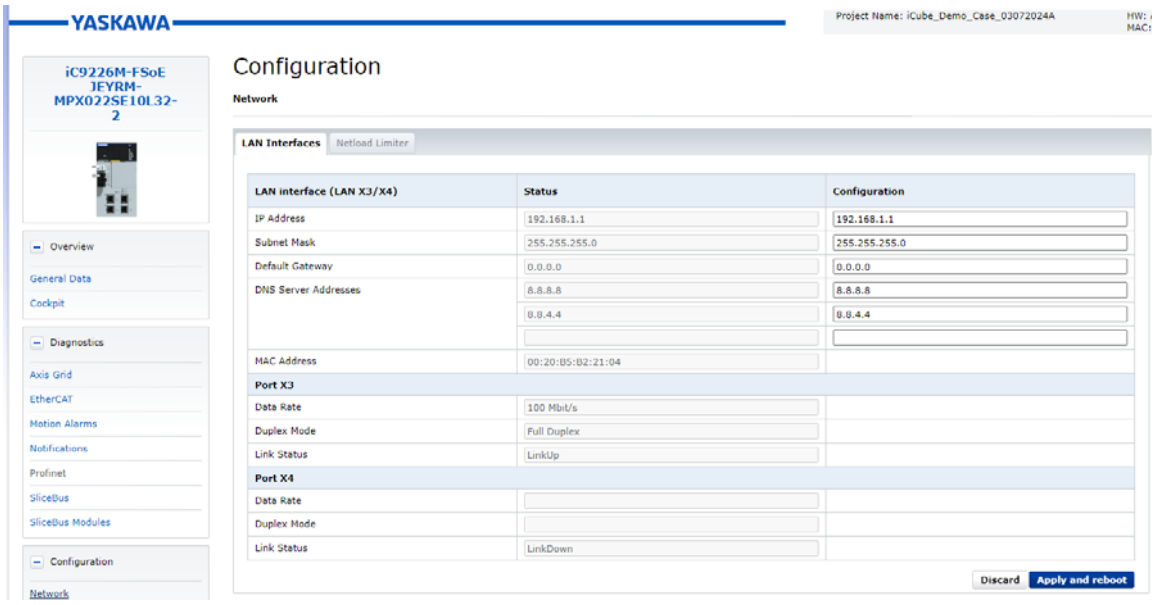
- Module …
  - Here you will find detailed information for the corresponding module:
    At [General] the general module information is listed such as order number, hardware and firmware version.
    At [Diagnostic State] you will find the diagnostic data. For more information on the structure of the diagnostic data, please refer to the corresponding manual of the module.
- [Back]
  With [Back] you can jump back to the SliceBus diagnosis.

5.4 Configuration

5.4.1 Network

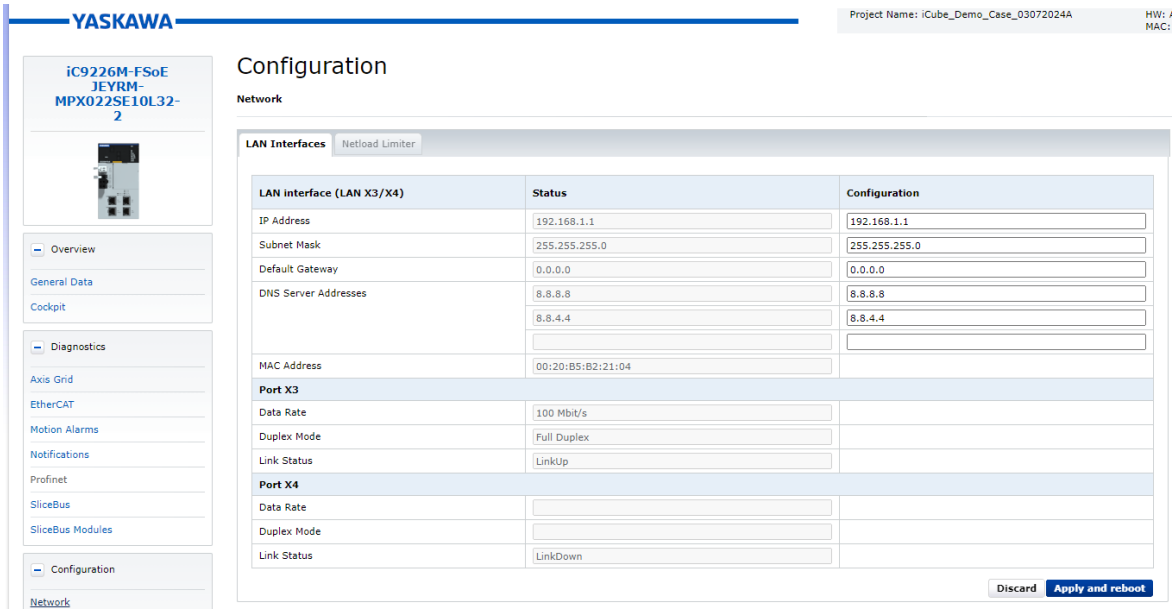
(1) User with Read Permission

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



(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.



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.

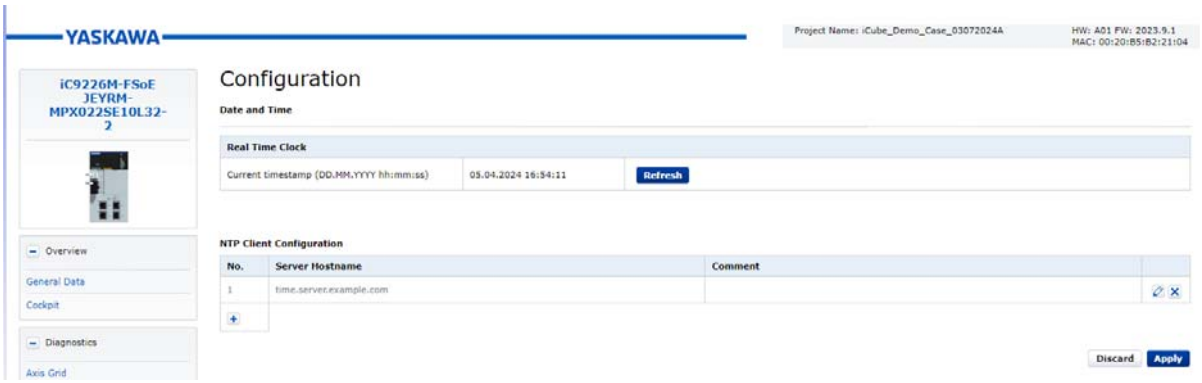
Information

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

5.4.2 Date and Time

The Date and Time page provides access to the NTP client configuration. NTP stands for **N**etwork **T**ime **P**rotocol 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.

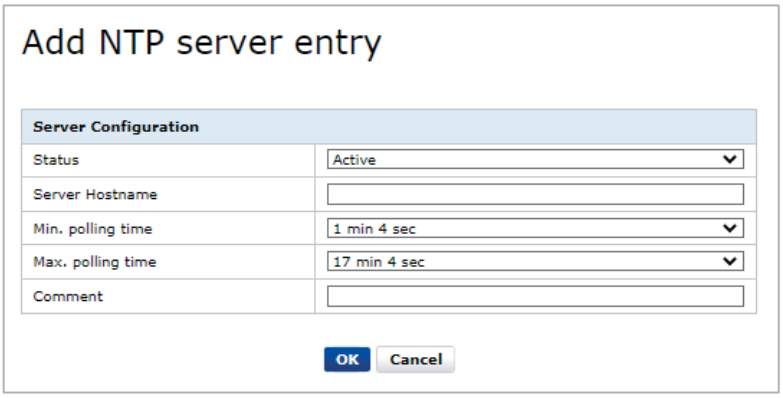
Information All iC9200 Series CPUs use UTC0 as the default setting, which corresponds to the coordinated world time UTC ±00:00.



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.



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  .

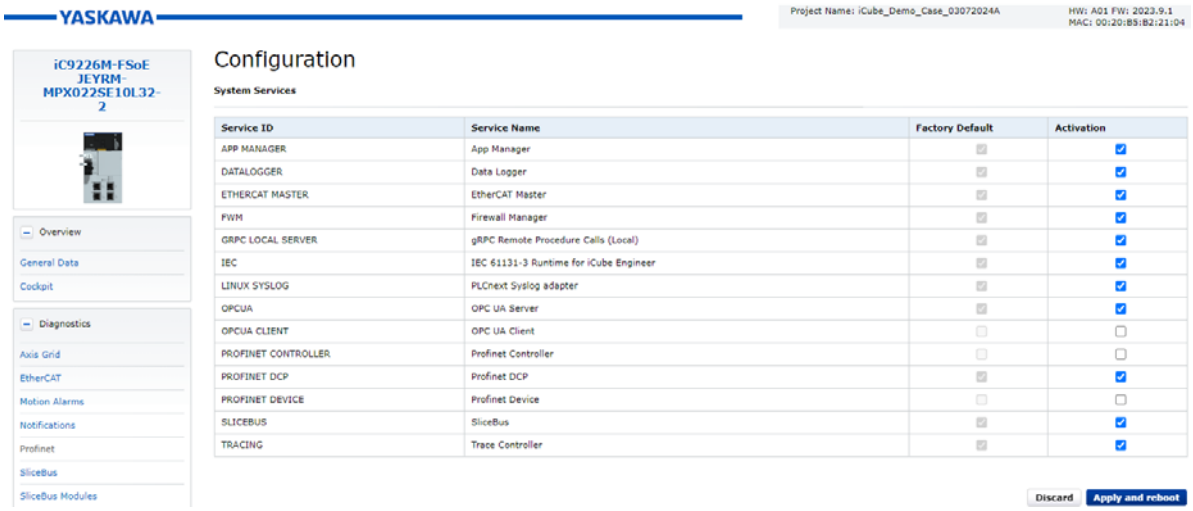
4. **Click on [Apply].**

   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.

5.4.3 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.



(1) Enable/Disable System Services

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.

5.4.4 Web Services

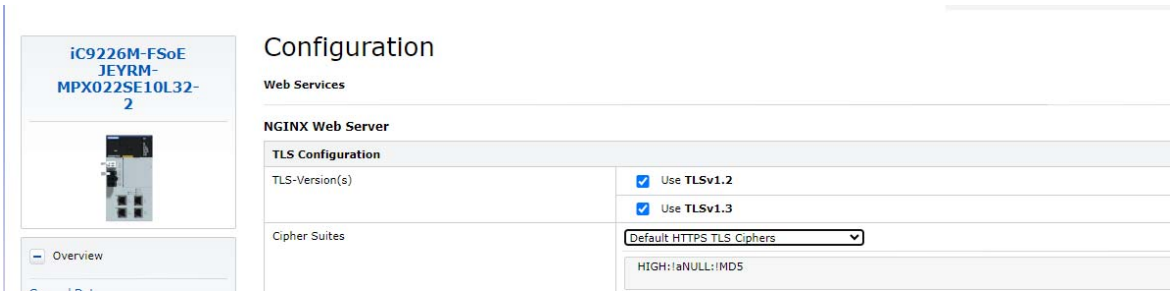
The page provides access to the configuration of web services, e.g. HTTPS certificate, which is used for the NGINX web server.

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.**

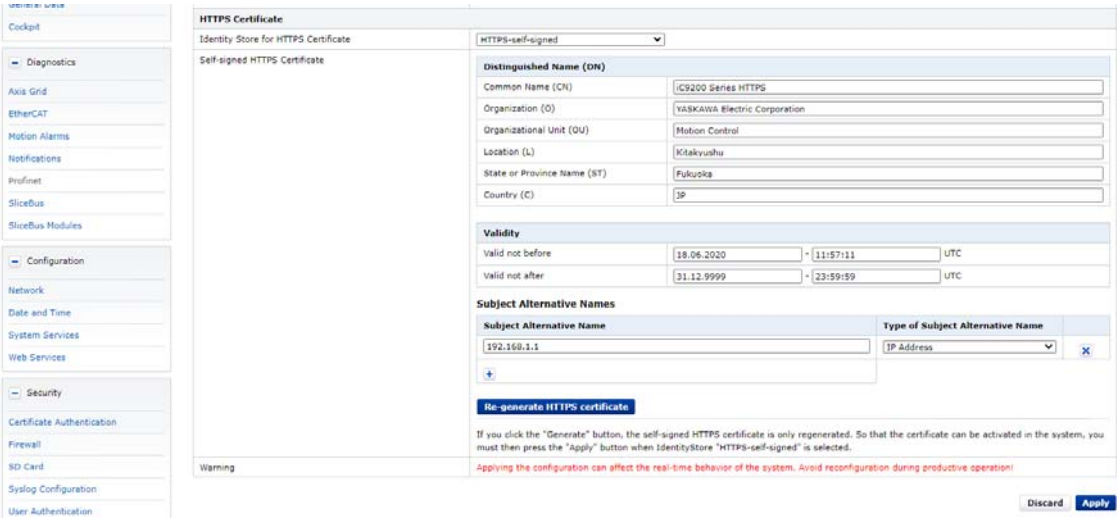
   The corresponding HTTPS certificate is selected.

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.

5.5 Security

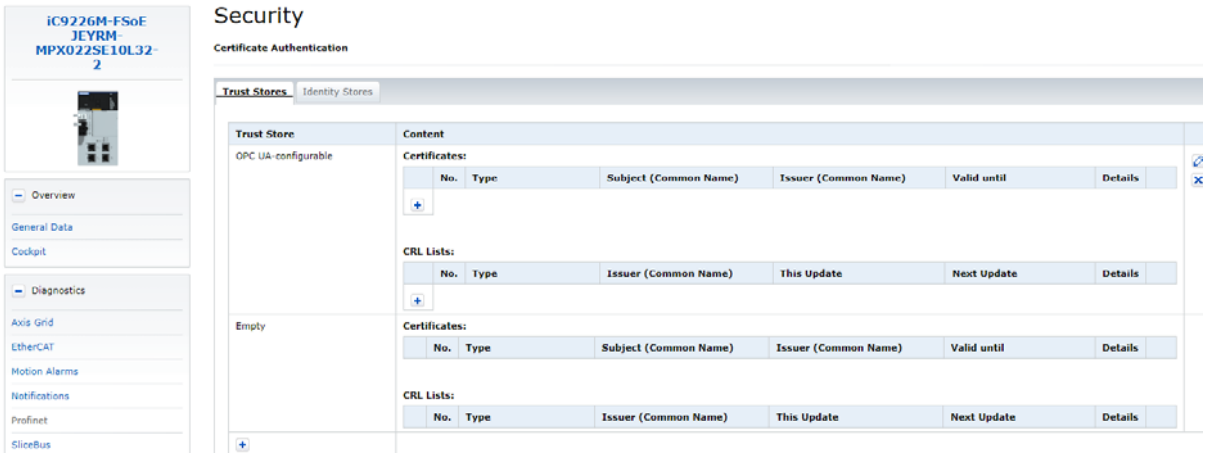
The safety-related settings for the CPU must be configured in the [Security] area of the WBM.

5.5.1 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.

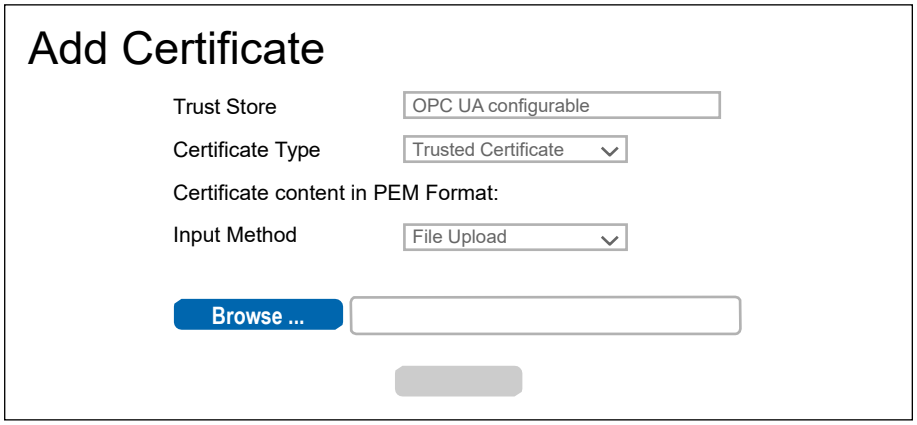
(a) Creating a Trust Store

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.**



- 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].**

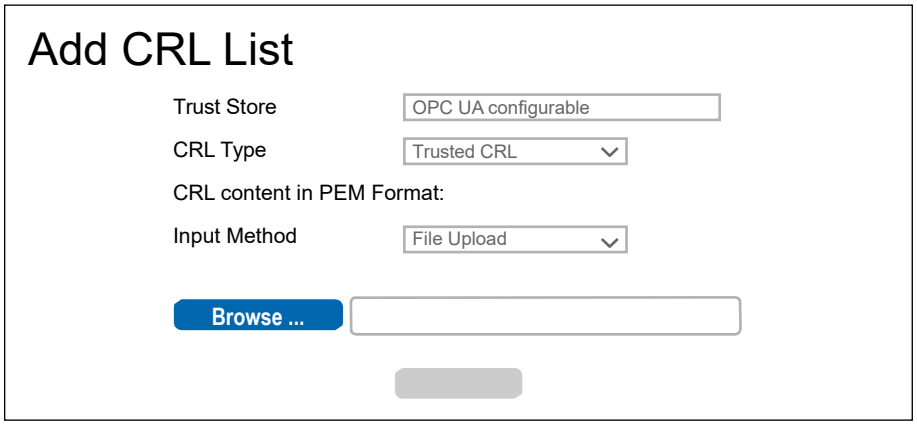
   The input dialog is closed and the certificate is added in text format.

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.



- 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  button for the relevant certificate or revocation list.**
2. **In the query dialog click on [Remove].**

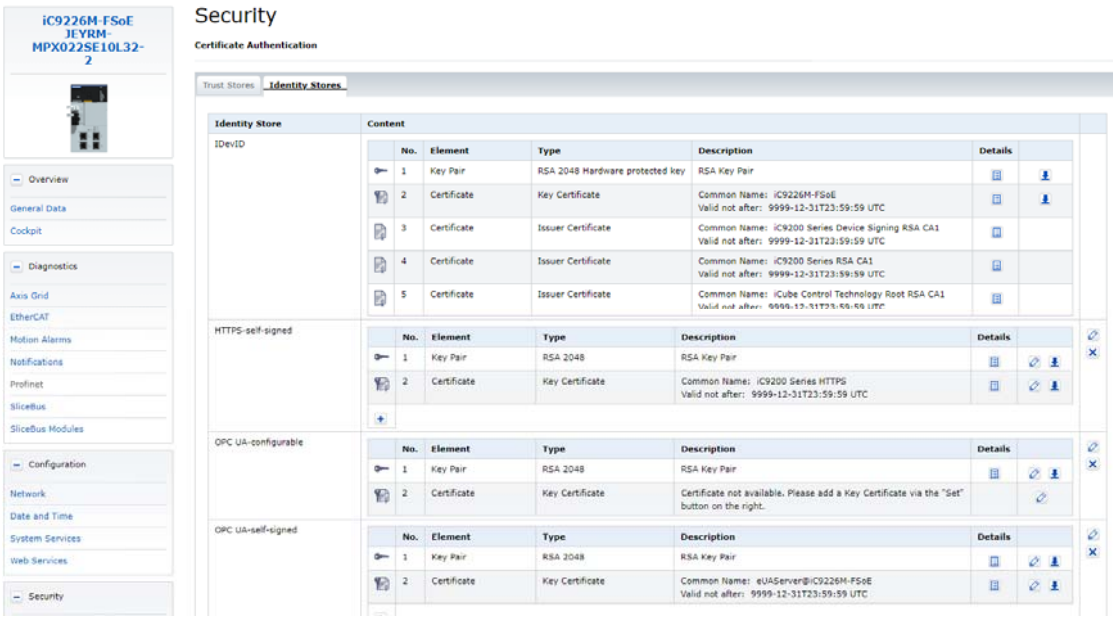
(e) Detail View

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].**

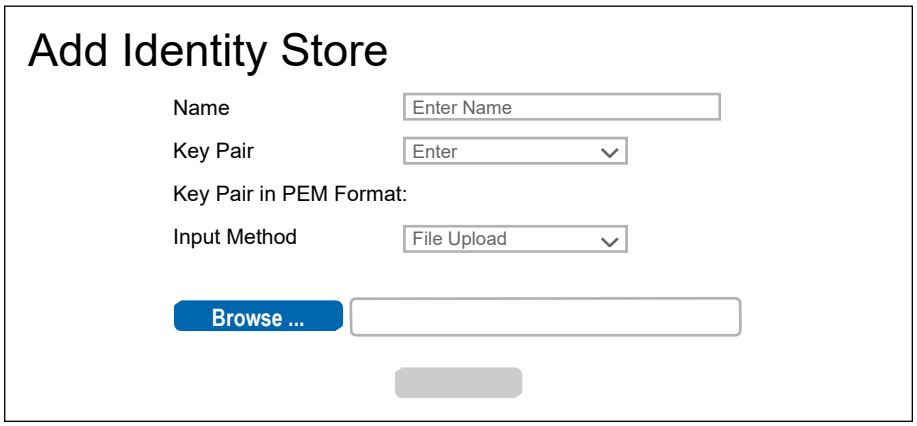
(2) Tab: Identity Store

- 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.



(a) Adding a Identity Store

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



- 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.

5.5.2 Firewall

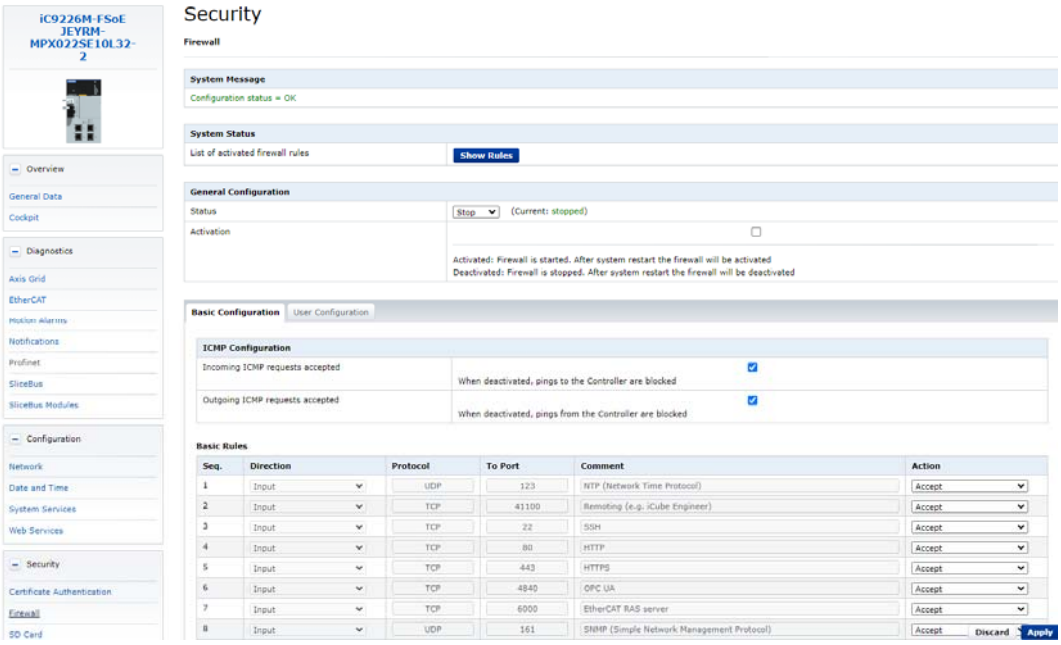
The CPU is delivered with a preset firewall. The Linux® firewall [nftables] is used here. As described below, you can create rules from predefined basic rules or create your own new ones.

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.



(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 warning 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:

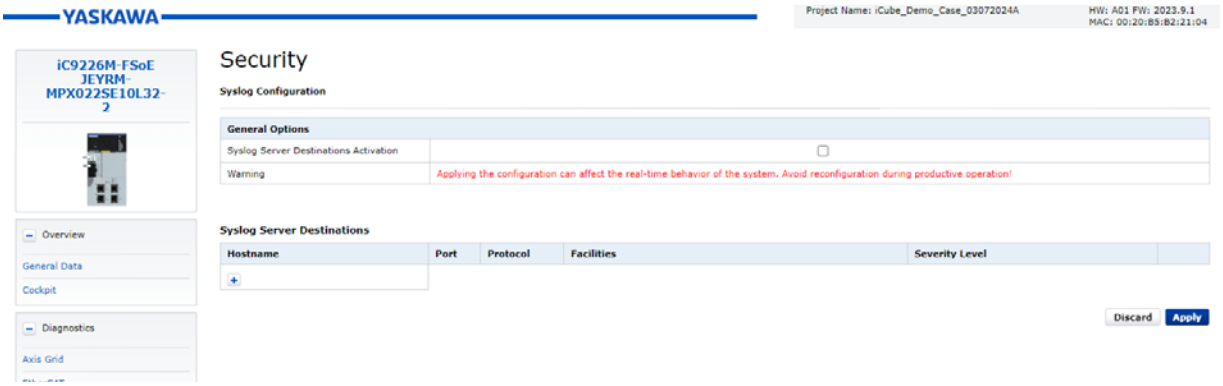
- [Seq.]
  - Numbers the order for the priority according to which the firewall rules are applied.
  - The rules are applied in ascending order from 1.
  - With  and  you can move the firewall rules accordingly.
- [Interface]
  - In the [Input Rules] tab you can select a single interface from a selection 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.

5.5.3 SD Card

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

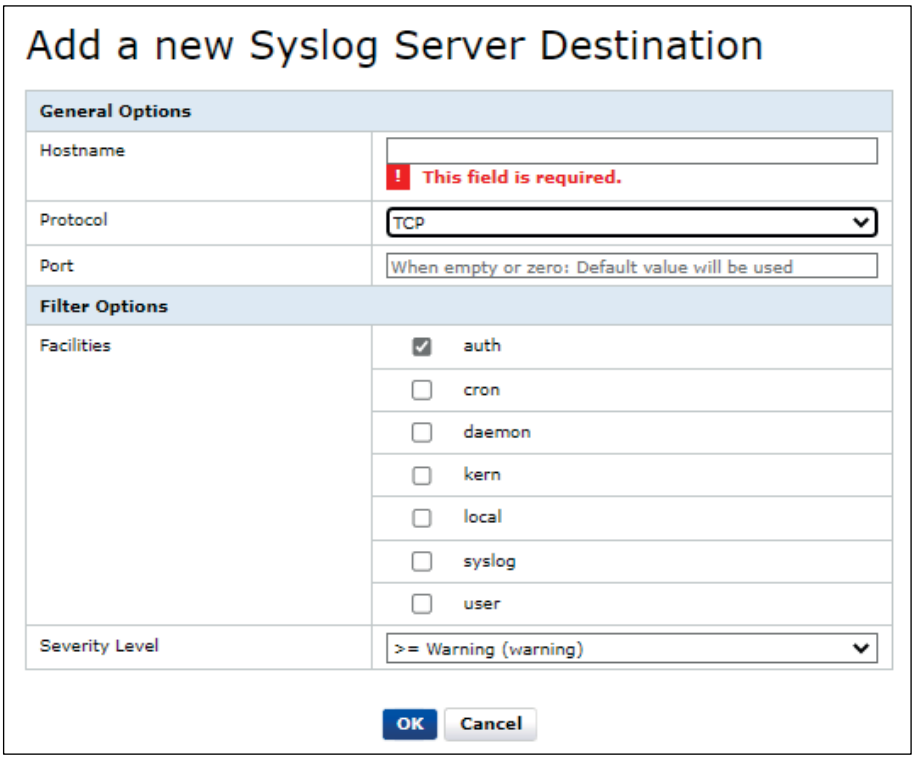
5.5.4 Syslog Configuration

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



(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.



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 *5.5.1 Certificate Authentication on page 204*.
       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. *5.5.2 Firewall on page 208*

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

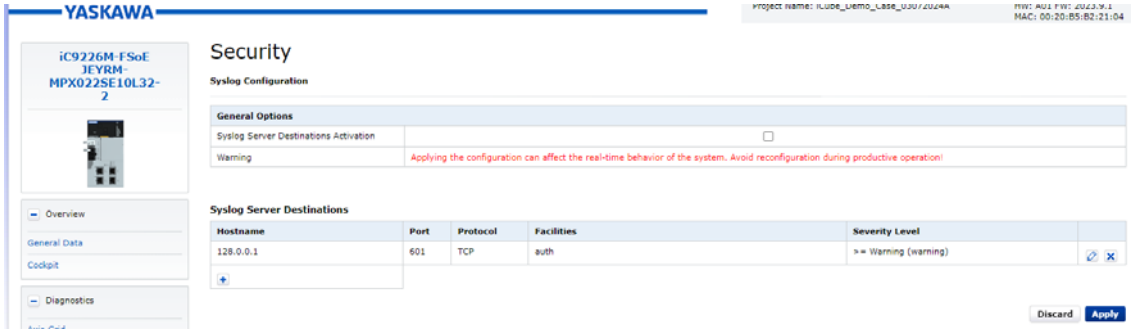
   - Facilities
     - Here you specify the system type of the log data.
   - Severity Level
     - Determine here the severity level from which the log data is sent to the Syslog server.
       Level 1: >= Internal (debug): All messages are sent.
       Level 2: >= Information (info): Messages >= level 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



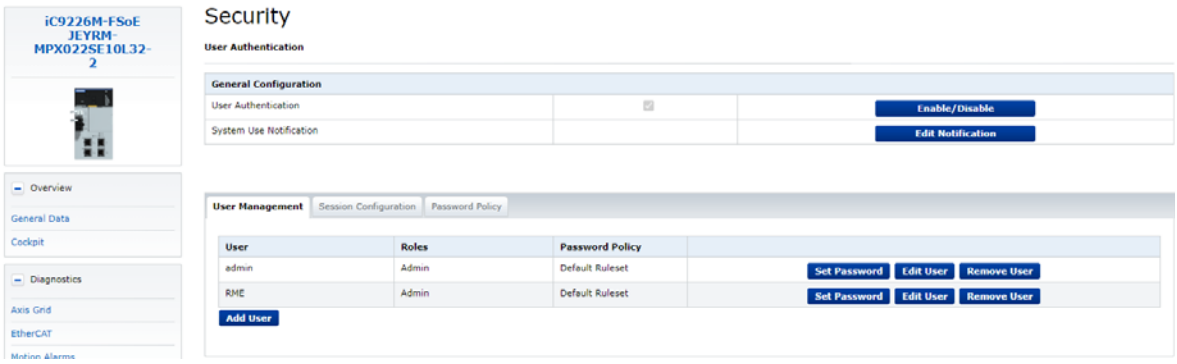
1. **By selecting or deselecting the control field of [Syslog Server Destination Activation] at [Syslog Configuration] you can enable respectively disable the Syslog server targets specified in the table.**
2. **Click on [Apply].**

   The settings are accepted.

5.5.5 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 deselecting 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

1. **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.
2. **Assign the corresponding roles to the user entry by selecting them.**
3. **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 Writer
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 Writer
Information - General Data	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - EtherCAT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - Motion Alarms	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - Notifications	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - PROFINET (optional)													
Diagnostics - SliceBus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Diagnostics - SliceBus Modules													
Configuration - Network			1			1	1	1					
Configuration - Date and Time			1	1	1	1	1	1	1	1	1		
Configuration - System Services	✓	✓											
Configuration - Web Services	✓	✓											
Security - Certificate Authentication													

Continued on next page.

Continued from previous page.

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.

5.6 Administration

5.6.1 iCube Apps

(1) Installed iCube Apps

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 programs provided to you by Yaskawa.

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 license 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

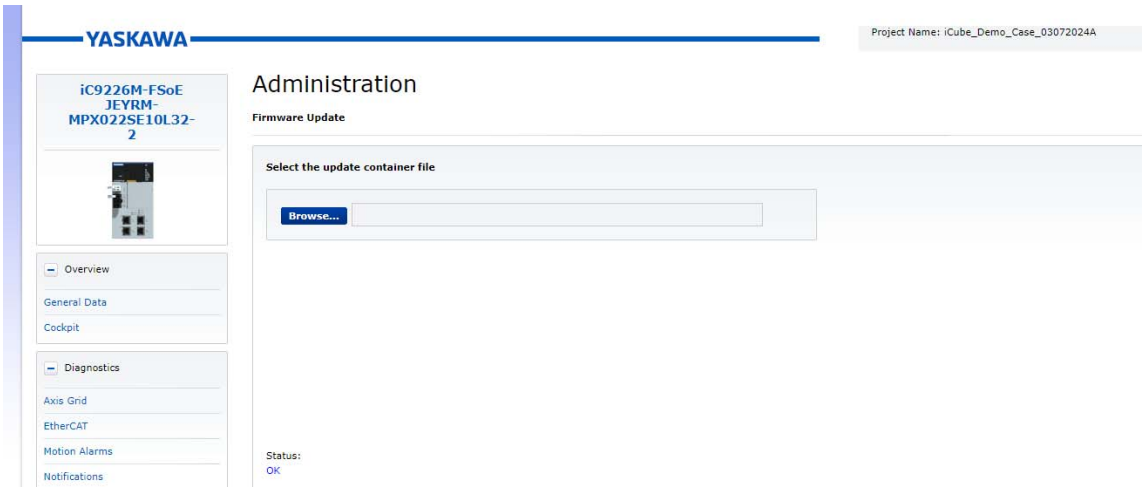
1. **To uninstall an app, you must quit it first. To do this, click in the table [Installed iCube Apps] at [Stop] behind the corresponding app.**
2. **To uninstall, click the following in the table [Installed iCube Apps] at [Uninstall] behind the corresponding app.**

   After a security prompt, the corresponding app is uninstalled.

5.6.2 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!



(1) Proceeding

⚠ CAUTION

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.*5.2.1 General Data on page 185*

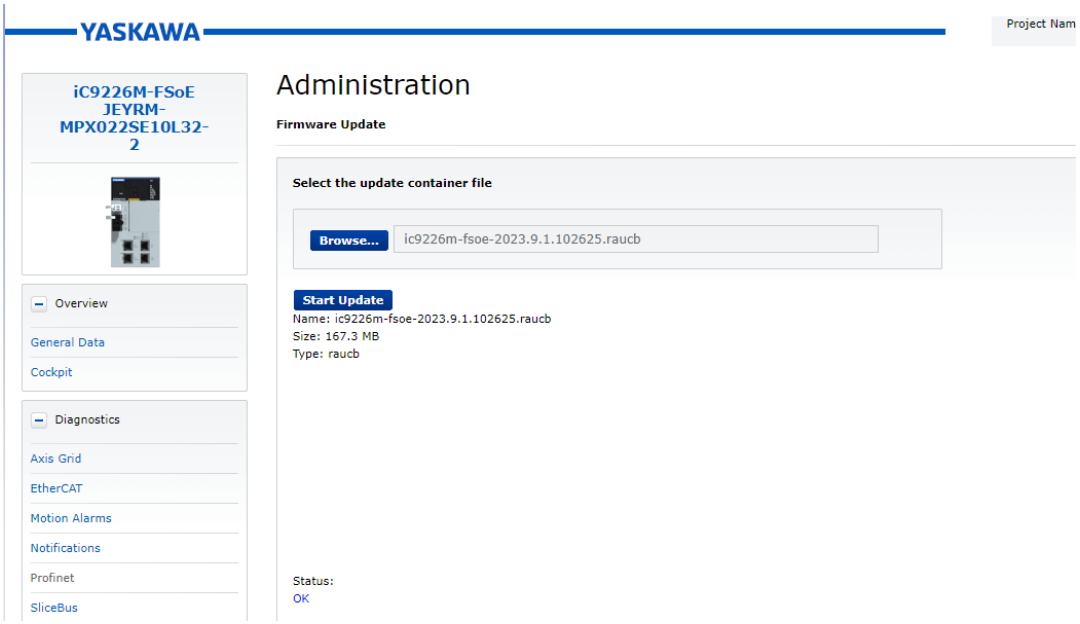
1. **The latest firmware can be found in the [Download Center] of www.yaskawa.eu.com under the corresponding order number.**

   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].**

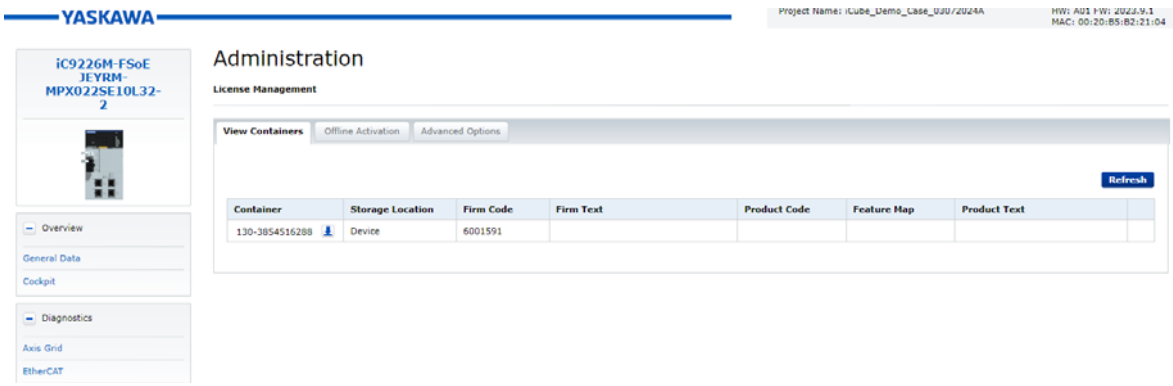
   The firmware file is transferred to the CPU and the firmware update is started. The status of the file transfer and the status of the update process are shown in the WBM as a progress bar.
6. **The connection to the CPU is interrupted during the firmware update. After the start-up of the CPU you have 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.** ***5.2.1 General Data on page 185***

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

5.6.3 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].

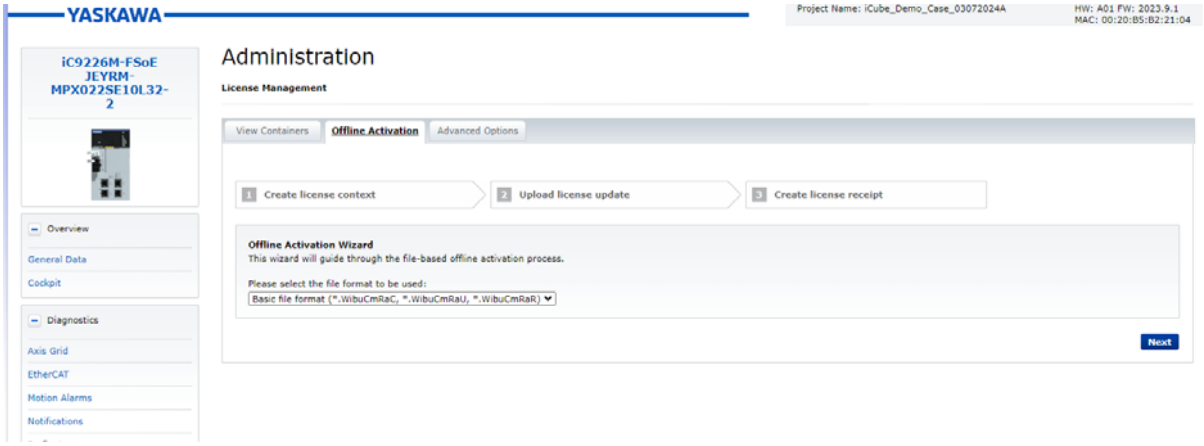


In the table all containers with the licenses are listed. The [Refresh] button reloads the list.

- 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]

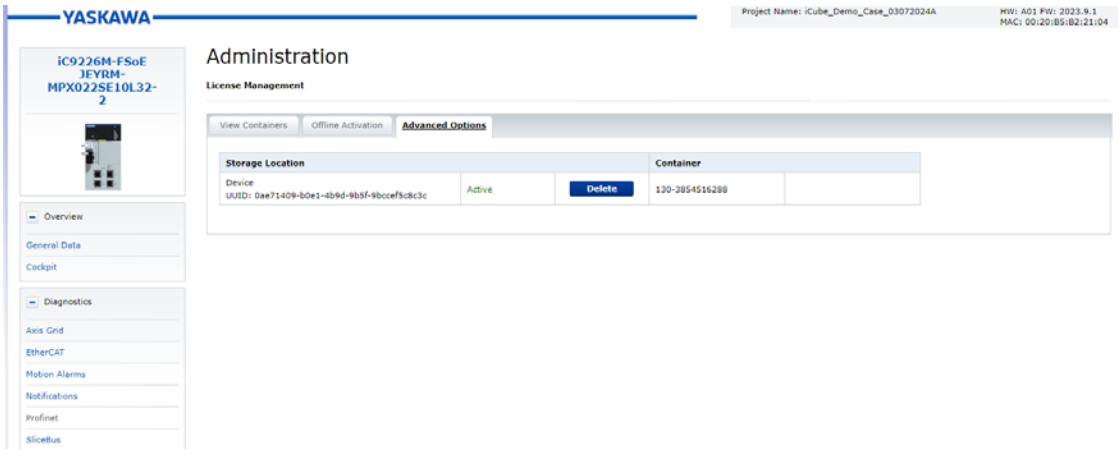
Here you can activate a previously purchased license offline by means of a license file. The term "offline" in this context means that the CPU on which the licensed software is running does not have to be connected to the Internet. The offline activation wizard guides you through the activation process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



(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. *5.4.3 System Services on page 201*

Appendix

A Checklist planning

Tab. 32: Checklist

Run. No.	Requirement	fulfilled		Notes
1	**Planning**	**yes**	**no**	
1.1	Was a risk evaluation established and were the required SIL and performance level according to DIN EN ISO 13849-1 or IEC 62061 determined?			
1.2	Are exclusively power supplies used according to PELV/SELV specification?			
1.3	Does the wiring take place after valid standards and guidelines?			
1.4	Is the power supply for the local I/O modules and field bus components correctly dimensioned?			
1.5	Do all the safety-related system components fulfill the requirements of the determined SIL (IEC 61508), performance level (DIN EN ISO 13849-1) and safety category (DIN EN 954-1)?			
1.6	Does the wiring of the safety components correspond to the requirements of the safety classification specified before?			
1.7	Do the performance data of the safety CPU correspond to the specifications of the application? ↳ *Chap. 3.3 'Technical data' page 104*			
1.8	Do the components fulfill the environmental conditions of the application?			
1.9	Does the system fulfill the necessary degree of protection?			
1.10	Is degree of pollution 2 kept?			
1.11	Was the maximally permissible response time of the safety functions determined by a hazard analysis?			
1.12	Is the maximally permissible response time reached? Was the proof established by means of a calculation?			
1.13	Is the system protected against mechanical overloading?			
1.14	Is the system protected against aggressive media?			
1.15	Are the specified electrical values of the output terminals kept?			
1.16	Are all the electromechanical sensors supplied with clock pulses for the recognition of short-circuits?			

Run. No.	Requirement	fulfilled		Notes
1.17	Was a list created, which contains all the parameters of the devices and its settings?			

Further information can be found at ↳ *Chap. 4.13 'Sample application' page 144.*

Date:.....Name: .....Sign: .....

B Checklist installation

Tab. 33: Checklist

Run. No.	Requirement	fulfilled		Notes
2	**Installation**	**yes**	**no**	
2.1	Do the components fulfill the environmental conditions of the application?			
2.2	Does the system fulfill the necessary degree of protection?			
2.3	Is degree of pollution 2 kept?			
2.4	Is the system protected against aggressive media?			
2.5	Are exclusively power supplies used according to PELV/SELV specification?			
2.6	Is it guaranteed that the safety switch devices are not short-circuited due to a wiring fault?			
2.7	Is it guaranteed that the safety switch devices are not short-circuited due to a wiring fault?			
2.8	Was the wiring checked by means of the installation plan?			
2.9	Are all the plugs labelled according to their allocation?			
2.10	Are the connecting terminals with screws applied with the specified breakaway torque?			
2.11	Is guaranteed that the isolation of the lines does not lead to a faulty contact?			
2.12	Was the reliability of all the clamp connections controlled by a mechanical tensile load?			
2.13	Was a visual inspection for any mechanical damage to the installed components done?			
2.14	Were necessary installation distances kept to other components?			
Date:.....Name: .....Sign:				

C Checklist commissioning, parametrization and validation

Tab. 34: Checklist

Run. No.	Requirement	fulfilled		Notes
3	**Commissioning**	**yes**	**no**	
3.1	Is guaranteed that all safe communication participants of a system have a clear safe device address (F-address)? This is valid also for participants, which belong to different safety controllers, if the controllers are connected by gateways (e.g. Ethernet).			
3.2	Was the cycle time T_{CI} of the safety CPU determined and adjusted in the safety CPU? ↳ *Chap. 4.12.5 'Cycle time TCL safety CPU' page 141*			
3.3	Was the maximum response time with the adjusted cycle time T_{CI} proofed by calculation? ↳ *Chap. 4.12 'Response times' page 138*			
3.4	Were the device parameters of the safety I/O modules validated? ↳ *Chap. 4.5.3 'Validation of the system' page 125*			
3.5	Was the correct project selected?			
3.6	Was a review of the safety programme done?			
3.7	Were the project data copied on a memory card?			
3.8	Was a complete functional test accomplished and documented?			
3.9	Was your engineering project documented and archived legally compliant?			
3.10	Was the service personnel instructed into the handling of the control system?			
Date:.....Name: .....Sign:				

D Checklist operation

Tab. 35: Checklist

Run. No.	Requirement	fulfilled		Notes
4	**Operation**	**yes**	**no**	
4.1	Is it guaranteed that no changes are made to the system configuration during operation of the safety CPU?			
4.2	Is it guaranteed that before expanding the system, removing individual system components and making changes to the wiring, the control system is set to a safe state dependent on the application by competent personnel?			
4.3	Are the ambient conditions specified in the technical data observed? ↳ *Chap. 3.3 'Technical data' page 104*			
4.4	Is the lifetime of all safety-related components specified by the manufacturer observed?			
4.5	Is it guaranteed that commissioning only takes place after acclimatisation of the safety CPU and the safety modules?			
4.6	Is it guaranteed that a PC system with executable iCube Engineer is available during the entire operating time?			
Date: ..... Name: .... Signature:				

E Checklist modification and retrofitting

Tab. 36: Checklist

Run. No.	Requirement	fulfilled		Notes
5	**Modification and retrofitting**	**yes**	**no**	
5.1	Is the modification/retrofitting compatible? Are the requirements of the checklists of planning, installation, commissioning and validation further fulfilled? *Appendix A page 225* *Appendix B page 227* *Appendix C page 228*			
5.2	Was the safety component to be replaced exchanged for a compatible safety component?			
5.3	If non-safety components are changed, is the checksum unchanged?			
5.4	Was the correct safety project loaded?			
5.5	Are the calculated reaction times further kept after modification/retrofitting? Proof necessary!			
5.6	Were the project data copied on a memory card?			
5.7	Was a complete functional test accomplished and documented?			
Date:.....Name: .....Sign:				

F Checklist decommissioning

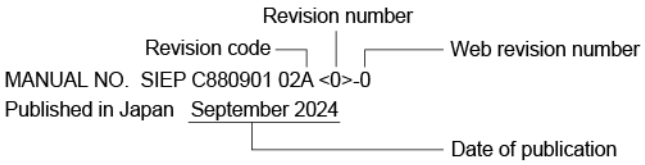
Tab. 37: Checklist

Run. No.	Requirement	fulfilled		Notes
6	**Decommissioning**	**yes**	**no**	
6.1	Is it guaranteed that the decommissioning is done by authorized and qualified personnel?			
6.2	Has the power supply been switched off at the device to be decommissioned?			
6.3	Has the wiring been removed from the device to be decommissioned?			
	Has the disassembly been carried out according to the disassembly description? *Chap. 2.6 'Demounting' page 67*			
6.4	Is it guaranteed that the defective decommissioned device is sent to Yaskawa for disposal in its original packaging?			

Date: ..... Name: .... Signature: ....

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.



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

iC9000 Series

iC9200

Safety 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

MANUAL NO. SIEP C880901 02A <0>-0

Published in Japan September 2024
24-5
Original instructions