YASKAWA

Software

SW | SW300I0EA V1.0.0 | Manual

HB143 | SW | SW300I0EA V1.0.0 | en | 26-02

IO-Link Manager - SW300I0EA

YASKAWA Europe GmbH
Philipp-Reis-Str. 6
65795 Hattersheim
Germany
Tel.: +49 6196 569-300
Fax: +49 6196 569-398
Email: info@yaskawa.eu
Internet: www.yaskawa.eu.com

SW300I0EA_000_IO-Link Manager,2,EN - © 2026

Table of contents

1 General. 4
1.1 About this manual. 4
1.2 Copyright © YASKAWA Europe GmbH. 5
1.3 Safety instructions. 6
1.4 Industrial security in information technology. 9
1.4.1 Protection of hardware and applications. 10
1.4.2 Protection of PC-based software. 11
2 Installation. 12
2.1 System requirements. 12
2.2 Install *IO-Link Manager* 12
2.3 Uninstall *IO-Link Manager* 12
3 Deployment. 13
3.1 Overview. 13
3.2 Main menu. 14
3.3 IODD. 15
3.4 IO-Link master management. 15
3.4.1 Overview. 15
3.4.2 Add IO-Link master. 16
3.4.3 IO-Link master context menu ⚙. 16
3.4.4 Online status. 17
3.4.5 Master Control. 17
3.4.6 Port x. 27

1 General

1.1 About this manual

Objective and contents

This manual describes the IO-Link Manager from Yaskawa.

- Installation and application are described.
- The manual is written for users with good basic knowledge of automation technology and profound knowledge of IO-Link communication.
- The manual does not replace sufficient basic knowledge of automation technology or sufficient familiarity with the specific product.
- The manual consists of chapters. Each chapter describes a completed topic.
- The following guides are available in the manual:
  - An overall table of contents at the beginning of the manual.
  - References with pages numbers.

    To be able to return to the previous view from a reference in the PDF, you should activate the page navigation in your PDF viewer.

Validity of the documentation

Product	Order no.	as of version:
IO-Link Manager	SW300I0EA	V1.0.0

Documentation

In the context of the use of the pertinent Yaskawa product, the manual is to be made accessible to the pertinent qualified personnel in:

- Project engineering
- Installation department
- Commissioning
- Operation

Icons and 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.

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.

Supplementary information and useful tips.

1.2 Copyright © YASKAWA Europe GmbH

All rights reserved

This document contains protected information of Yaskawa and may not be disclosed or used outside of an agreement made in advance with Yaskawa and only in accordance with that agreement.

This document is protected by copyright laws. Reproduction, distribution, or modification of this document or excerpts thereof is not permitted without the written consent of Yaskawa and the owner of this document, except in accordance with applicable agreements, contracts or licenses.

For permission to reproduce or distribute, please contact: YASKAWA Europe GmbH, European Headquarters, Philipp-Reis-Str. 6, 65795 Hattersheim, Germany

Tel.: +49 6196 569 300
Fax.: +49 6196 569 398
E-mail: info@yaskawa.eu
Internet: www.yaskawa.eu.com

Download Center

By entering the product order number in the *'Download Center'* at www.yaskawa.eu.com, the pertinent manuals, data sheets, declarations of conformity, certificates and other helpful information for your product can be found.

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.

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

General terms of use

Every effort was made by Yaskawa to ensure that the information contained in this document was complete and correct at the time of publication. Nevertheless, the information contained therein is only owed by Yaskawa as it is available at Yaskawa. Correctness is not assured by Yaskawa, the right to change the information contained herein is always reserved by Yaskawa. There is no obligation to inform the customer of any changes. The customer is requested to actively keep this documentation up to date. The use of the products covered by these instructions, together with the associated documentation, is always at the customer's own risk, in accordance with the applicable guidelines and standards. This documentation describes the hardware and software components and functions of the product. It is possible that units are described which the customer does not have. The exact scope of delivery is described in the respective purchase contract.

Document support

Contact your local representative of YASKAWA Europe GmbH if you have errors or questions regarding the content of this document. You can reach YASKAWA Europe GmbH via the following contact:

Email: Documentation.HER@yaskawa.eu

Technical support

Contact your local representative of YASKAWA Europe GmbH if you encounter problems or have questions regarding the product. If such a location is not available, you can reach the Yaskawa customer service via the following contact:

YASKAWA Europe GmbH,
European Headquarters, Philipp-Reis-Str. 6, 65795 Hattersheim, Germany
Tel.: +49 6196 569 500 (hotline)
Email: support@yaskawa.eu

1.3 Safety instructions

General safety instructions

DANGER

Danger to life due to non-compliance with safety instructions

Non-compliance with the safety instructions in the manual can result in serious injury or death. The manufacturer is not responsible for any injuries or damage to the equipment.

CAUTION

Before commissioning and operating the components described in this manual, it is essential to note the following:

- Modifications to the automation system must only be done in a voltage-free state!
- Connection and modification only by trained electricians
- National regulations and guidelines in the respective country of use must be observed and complied with (installation, protective measures, EMC, etc.)

Intended use

- It is the customer's responsibility to comply with all pertinent standards, codes, or regulations applicable to the use of the software. This applies in particular to compliance with cyber security guidelines and regulations that apply when the Yaskawa software is used in combination with third-party software or in network structures.
- The customer must confirm that the Yaskawa-Software is suitable for the IT infrastructure and operating system environment for the customer's plant, machinery and equipment to be controlled.
- If the Yaskawa software is used, configured or modified in a way that is not described in this manual, the functional safety and protection of the overall system may be impaired and the use may result in material or immaterial damage.
- Contact Yaskawa to determine whether the use of the Yaskawasoftware is permitted in the following applications. If the use in the respective application is permissible, the Yaskawa software is to be used by considering additional risk assessments and specifications, and safety measures are to be provided to minimise the dangers in the event of a fault. Special caution is required and protective measures must be taken in the case of:
  - Use in unrestricted networks (Internet), environments with high electromagnetic interference of data transmission or IT environments that are not described in product catalogs or manuals.
  - Nuclear control systems, combustion systems, railway systems, aviation systems, automotive systems, medical devices, amusement machines and equipment that is specifically regulated by industry or government.
  - Systems, machines and devices that can pose a risk to life or e.g property.
  - Systems that require a high degree of reliability, such as gas, water or electricity supply systems or systems that operate 24 hours a day.
  - Other systems that require a similarly high level of security.
- Never use the Yaskawa software in an application where failure of the product could cause serious danger to life, limb, health or property without first ensuring that the system is designed to provide the required level of safety with risk warnings and redundancy to avoid the realisation of such dangers and that the Yaskawa software is properly installed.
- The connection examples and other application, programming examples and configuration templates described in the product catalogs and manuals of Yaskawa are for reference purposes. Check the functionality and logic as part of a commissioning/simulation before the Yaskawa software is used productively.
- To avoid accidental harm to third parties, read and understand all prohibitions on use and precautions, and operate the Yaskawa software correctly.

Field of application

- The Yaskawa software is not suited for use in life-support machines or systems.
- Please contact your Yaskawa representative or Yaskawa distributor if considering the use of the Yaskawa software for special purposes, such as machines or systems used in passenger cars, in medical, aircraft and aerospace applications, for power supply of networks, for electrical power distribution or for switching underwater relays.

DANGER

The Yaskawa software is not permitted for use with devices

- in explosive environments (EX zone)

When used properly and in accordance with the operating instructions, the Yaskawa software is intended for:

- communication, process control and parametrization of dedicated Yaskawaproducts
- general control and automation tasks
- industrial use
- operation on the specified hardware and firmware versions
- use exclusively by trained specialist personnel

DANGER

If this Yaskawa software is used in applications where failure of the Yaskawa software or of the device can result in the loss of human life, a serious accident or physical injury, you must install appropriate safety devices.

- Death or serious injury can result if you do not install the safety devices properly.

Disclaimer

(1) The contractual and legal liability of Yaskawa and the legal representatives and vicarious agents of Yaskawa for compensation and reimbursement of expenses in relation to the content of this documentation is excluded or limited as follows:

a) For slightly negligent breaches of *Essential Contractual Duties* arising from the contractual obligation, for Yaskawa the amount of liability is limited to the foreseeable damage typical for the contract. *'Essential Contractual Duties'* are those duties that characterise the performance of the contract and on which the Yaskawa customer may reasonably rely.

(b) In each case, Yaskawa is not liable for (i) the slightly negligent breach of duties arising from the duties that are not *Essential Contractual Duties*, as well as (ii) force majeure, i.e. external events that have no operational connection and cannot be averted even by exercising the utmost care that can reasonably be expected.

(2) The aforementioned limitation of liability does not apply (i) in cases of mandatory statutory liability (in particular under the product liability law), (ii) if and to the extent that Yaskawa has assumed a guarantee or same as guaranteed procurement risk according to § 276 BGB, (iii) for culpably caused injuries to life, limb and/or health, also by representatives or vicarious agents, as well as (iv) in case of delay in the event of a fixed completion date.

(3) A reversal of the burden of proof is not associated with the provisions above.

1.4 Industrial security in information technology

Latest version

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

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.

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.

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*

1.4.1 Protection of hardware and applications

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.

1.4.2 Protection of PC-based software

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 Installation

2.1 System requirements

The minimum system requirements for installing the *IO-Link Manager* are:

- CPU with min. 800MHz clock frequency
- Working memory: At least 512MB of RAM
- Graphics card that supports DirectX 9
- Operating system: Microsoft® Windows® 7 and newer
- Microsoft® Microsoft .NET Framework 4.5 and newer

If Microsoft® .NET Framework is not available, it will be installed during setup. Internet access is required for this.

2.2 Install *IO-Link Manager*

- In order to install programmes, you may need to be logged in as an administrator or a user with administrator rights.
- You can find the software *IO-Link Manager* in the *'Download Center'* of www.yaskawa.eu.com at SW300I0EA.

1. Download the ZIP file to your PC and unzip it.
2. Run the msi file to install.
   ➡ *'The Setup Wizard'* opens.
3. Follow the on-screen instructions and start the installation.

The use of the IO-Link Manager assumes that you agree to the license agreement. During installation, you must confirm this.

➡ *IO-Link Manager* is installed and a programme link is added to the desktop.

Please note that Microsoft®.NET Framework is required for operation. You can download this from the Microsoft® web page.

2.3 Uninstall *IO-Link Manager*

You can uninstall the *IO-Link Manager* in the control panel. Click *'Uninstall'* and follow the instructions.

Please note that Microsoft®.NET Framework is not uninstalled during uninstallation.

3 Deployment

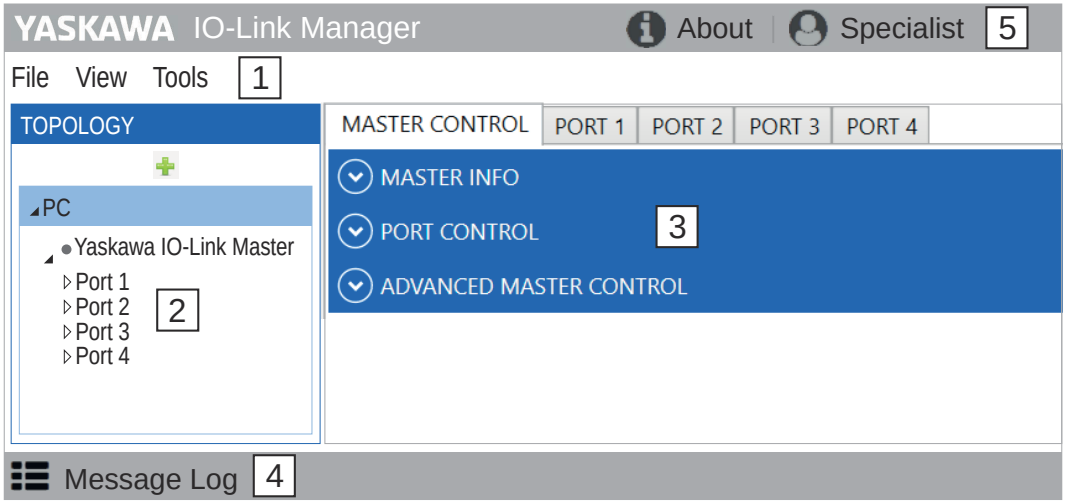
3.1 Overview

Properties

IO-Link Manager is a software for configuring theYaskawa IO-Link masters with the following features:

- Configuration of several IO-Link masters/devices online and offline.
- Diagnostic option for IO-Link masters/devices.
- Status indication IO-Link master/ports in the topology area.
- Controlled access via defined user roles.
- Read/write access to process data.
- Variable port mapping.
- IODD catalog management for the IO-Link devices.
- IODD-supported process data representation, diagnostics and parametrization.
- Process data representation, diagnosis and parametrization also possible without IODD.
- Firmware update for IO-Link masters/devices.

Working environment



1 Main menu Here you have access to the main functions of the *IO-Link Manager*.
2 *'TOPOLOGY'*: The IO-Link masters are listed here with the corresponding ports.
3 Editor area with properties dialogs for parametrization and information areas.
4 Message Log: When accessed, all messages are listed here.
5 : Here you will find version information about the software and the installed components.
: Here you can set the corresponding user role.

Please note that program processing can be blocked by a dialog window in the background. The blockage is only removed again by closing the dialog window.

Editor area

- The editor area always refers to the currently active IO-Link master. This is highlighted accordingly in the *'TOPOLOGY'* area.
- The editor area is divided into tabs for the IO-Link master and its ports.
- Within the dialogs, the information and parameters are summarized in functional areas that you can open or close via or . Extensive information within the functional areas can be subdivided into additional tabs.

User roles

Via you can set the corresponding user role. When using IODDs, the device manufacturers can assign task areas and access rights corresponding to the user roles. There are the following user roles:

- Operator
  - This user role should cover the area of operation and monitoring.
- Maintenance
  - This user role focuses on commissioning and parametrization.
- Specialist
  - By selecting *'Specialist'* you should be able to access the full range of services.

Message Log

Via you can access a message window. Occurring events are listed there accordingly. You can export and delete the message log. By double-clicking on a message, the details of the message are shown in a separate dialog.

3.2 Main menu

File

- Save Project
  - You can use this to save the configuration of the IO-Link master currently selected at *'TOPOLOGY'* on your PC.
- Open Project
  - You can use this to load an IO-Link master configuration. Here, in an existing project, the loaded IO-Link master configuration is placed at the lower end in *'TOPOLOGY'*.
- Exit
  - Exit ends the program without saving. Please note that if you have not previously saved your project with *'Save Project'*, these changes will be discarded with *'Exit'*!

View

- *'Topology → Show / Hide'*
  - By temporarily hiding the *'TOPOLOGY'*, you can extend the editor area to the width of the screen.

Tools

- Manage Plugins
  - Here you will find information about the installed plugins. Standard plugins cannot be removed.
- Communication Module Manager
  - Here you will find information about the installed communication modules. Standard communication modules cannot be removed.
- Options
  - Here you can view or adjust the basic settings and file paths of the *IO-Link Manager*. Press [Apply] to apply the changes.

3.3 IODD

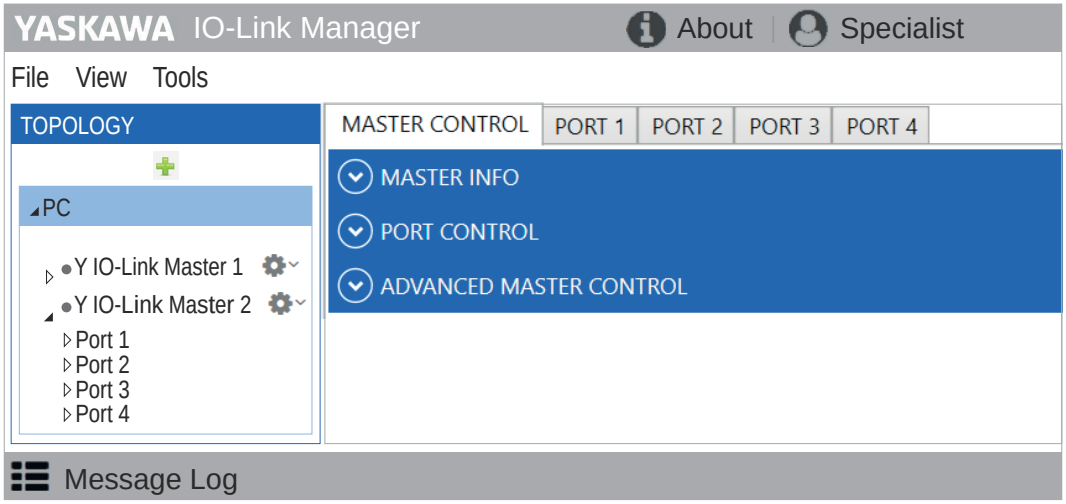
IODD - Device description

- For integration into the *IO-Link Manager*, you will receive an IODD file (**IO D**evice **D**escription) from the manufacturer of the corresponding IO-Link device.
- The IODD file contains device-specific properties of the corresponding IO-Link device, which are available after integration in *IO-Link Manager*.
- In the *IO-Link Manager* you have the possibility to configure, control and monitor a device IODD-supported or without IODD.
- If an IODD is loaded for the corresponding device, all information and parameters are prepared and shown according to the IODD specifications of the device manufacturer for the respective user role.
- At *'MASTER CONTROL → PORT CONTROL' 'Selected Device'* you can access the*'IODD Catalog'* via . Here you can install the corresponding IODD files via the [Import IODD File] button.

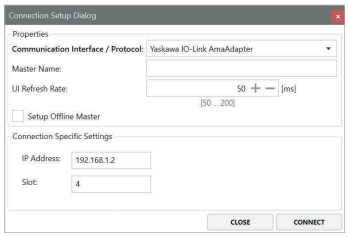
3.4 IO-Link master management

3.4.1 Overview

- The *IO-Link Manager* can communicate with several IO-Link masters in parallel.
- The IO-Link masters are created and managed in the *'TOPOLOGY'* area.
- Each *'TOPOLOGY'* tree node represents an IO-Link master by its specified number of IO-Link ports, including information about the current C/Q and I/Q status and the names of the connected IO-Link devices.
- The editor area always refers to the currently active IO-Link master. This is highlighted accordingly in the *'TOPOLOGY'* area.



3.4.2 Add IO-Link master

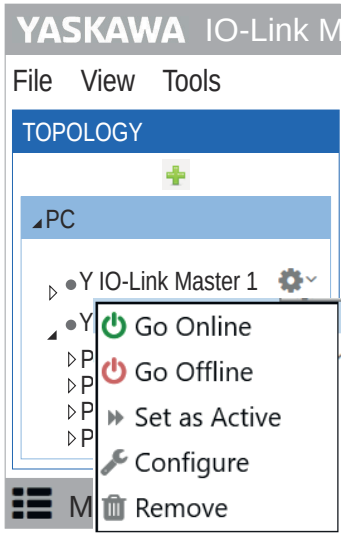


To add an IO-Link master, click in the *'TOPOLOGY'* area . The *'Connection Setup Dialog'* opens with the following parameters, which are required to establish a connection with the IO-Link master:

- *'Communication Interface / Protocol'*
  The Yaskawa communication protocol for the IO-Link master is fixed here.
- *'Master Name'*
  Here you can specify a user-friendly name for the IO-Link master that is to be shown in the *'TOPOLOGY'* area.
- *'UI Refresh Rate'*
  This parameter allows you to specify the refresh rate for the user interface. This property specifies the update frequency of the port status and process data from each port of the IO-Link master.
- *'Setup Offline Master'*
  If you only want to set up the connection but do not want to connect to the IO-Link master immediately, you can activate this option. Here you must specify the number of ports.
- *IP Address*
  Enter here the IP address via which you are connected to the head module of the System SLIO.
- *Slot*
  Enter the slot of your IO-Link master in the System SLIO, here. The counting starts with 1 right after the head module. Please consider the System SLIO power and clamp modules do not have any module ID. These cannot be recognised by the head module and are therefore not taken into account in the count.

Press [Connect] to accept the data and the IO-Link master is listed in the *'TOPOLOGY'* area.

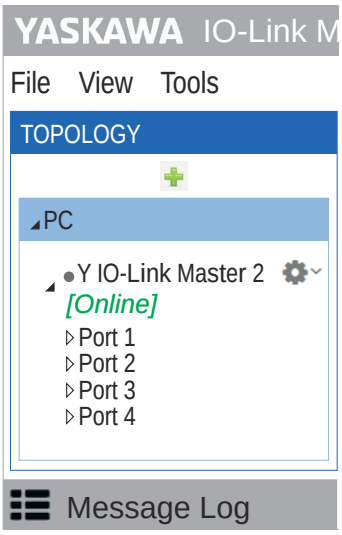
3.4.3 IO-Link master context menu



The IO-Link masters listed in the *'TOPOLOGY'* area have a context menu with the following functions:

- Go Online
  This establishes an online connection with the IO-Link master. The specified connection data are used here.
- Go Offline
  This ends the online connection.
- Set as Active
  The editor area always refers to the currently active IO-Link master. You can switch it to active by double-clicking on the IO-Link master or via *'Context menu → Set as Active'*. This is highlighted accordingly in the *'TOPOLOGY'* area.
- Remove
  This allows you to remove the selected IO-Link master with its port configuration from the *'TOPOLOGY'* area.

3.4.4 Online status



In the *'TOPOLOGY'* area, the IO-Link masters and their status are visualised. If an IODD is loaded, the port states and the IO-Link device names are also shown. The following states are defined for IO-Link masters:

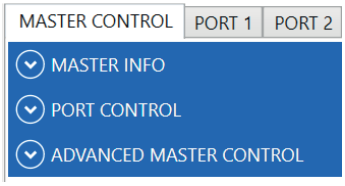
States IO-Link master:

- Online
  There is an online connection to the IO-Link master.
- Offline
  There is an online connection to the IO-Link master.
- Connecting
  An attempt is made to establish an online connection to the IO-Link master.
- Disconnecting
  An attempt is made to terminate an existing online connection to the IO-Link master.
- Busy
  IO-Link Manager waits for a response from the IO-Link master.
- Communication lost
  An existing online connection was interrupted.
- Bootloader mode
  The IO-Link master is in *Bootloader Mode* during a firmware update. If the IO-Link master is still in *Bootloader Mode* after the firmware update, an error has occurred. Check that the firmware file matches your IO-Link master and run the update again.
  ➦ *'Firmware update'...page 24*
  If the error persists, please contact the Yaskawa hotline!

States of the ports

- Deactivated
  The IO-Link port is disabled.
- Diagnosis
  The IO-Link port is in the *'Port Diagnosis'* status.
- No Device
  There is no communication but the IO-Link port is configured as *'IO-Link Autostart'* respectively *'IO-Link Manual'*.
- Not available
  No status information is available.
- DI
  The IO-Link port is enabled as a digital input and works correctly.
- DO
  The IO-Link port is enabled as a digital output and works correctly.
- Operate
  The port is enabled as IO-Link and works correctly.
- Device starting
  The device is in the start-up phase.

3.4.5 Master Control



The tab *'Master Control'* is located in the editor area. The dialog window contains information about the corresponding IO-Link master and offers access to its port functionalities.

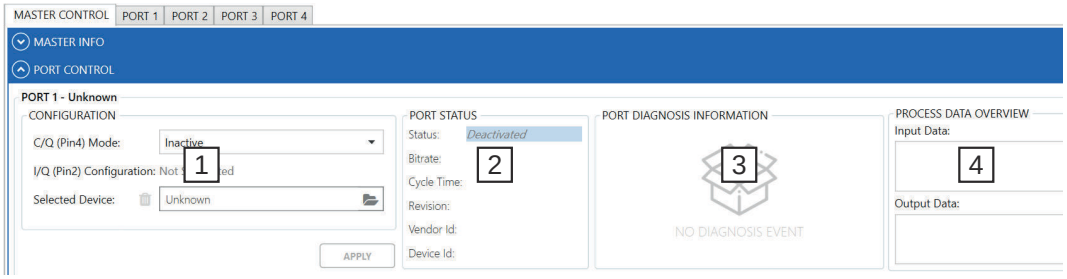
- The editor area is divided into tabs for the IO-Link master and its ports.
- Within the dialogs, the information and parameters are summarized in functional areas which you can open respectively close via ⌄ respectively ⌃. Extensive information within the functional areas can be subdivided into additional tabs.

3.4.5.1 Master Info

- *'Master Info'* shows information about the IO-Link master. This information is extracted from the SMI service "MasterIdent".
- The IO-Link master adapts the available control functions to the supported services.

3.4.5.2 Port Control

The *'Port Control'* dialog allows access to the functionality of the port of the IO-Link master and provides an overview of the status of the port together with diagnostic information and the current process data.

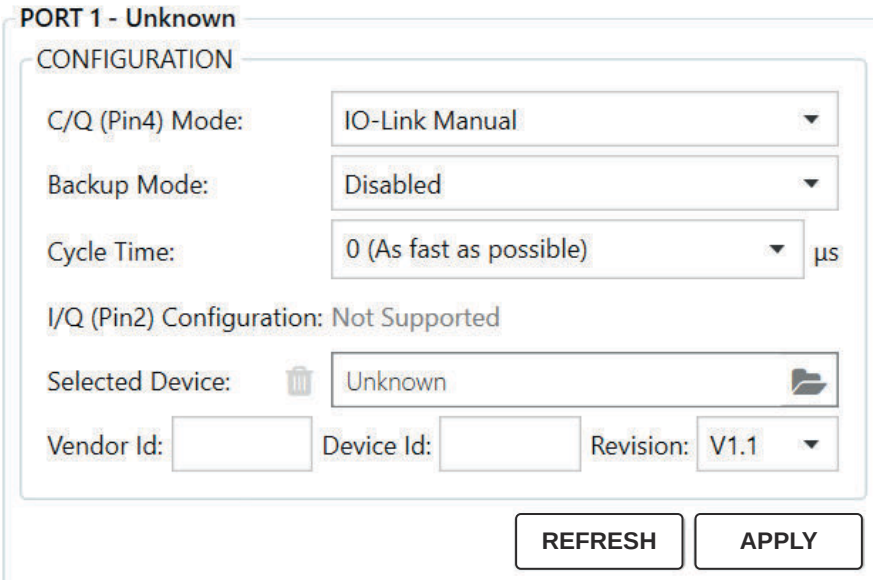


The ports dialog consists of four parts:

1 Configuration	- Allows configuration of the IO-Link port.
2 Port Status	- Shows the current port status.
3 Port Diagnosis Information	- Contains the diagnostic information about the IO-Link port.
4 Process Data Overview	- Shows the current process data input/output raw values (if the port is configured as IO-Link mode) or the SIO level (if the port is configured as digital input or output mode).

3.4.5.2.1 Configuration

Here you can define the configuration of the IO-Link port according to the specification. Press [Apply] to transfer the data to the IO-Link master.



C/Q (Pin4) Mode

C/Q (Pin4) Mode	Description
Deactivated	The port is disabled.
Digital Input	The port is in *SIO mode* and works as a standard digital input.
Digital Output	The port is in *SIO mode* and works as a standard digital output.
IO-Link Autostart	The port is in *IO-Link mode*. Every connected IO-Link device is accepted here. Please note possible effects on your process image in your user program.
IO-Link Manual	The port is in *IO-Link mode*. The IO-Link master only accepts IO-Link devices that correspond to the specified *'Device ID'*, *'Vendor ID'* and *'Revision ID'*.

Backup Mode

- *'Backup Mode' is only available when 'IO-Link Manual' mode is selected.*
- *Storage of the IO-Link device parameters in the backup of the IO-Link master is only possible for IO-Link devices with an IO-Link revision from 1.1.*

The parameters set in the IO-Link device can also be stored in the IO-Link master. When using the restore function of the IO-Link master, the saved parameters are automatically made available to the new IO-Link device when the IO-Link device on the corresponding port is replaced.

Here, a distinction is made between the following modes:

Backup Mode	Description
Disabled	Automatic parameter backup/restore is disabled. ■ The IO-Link device parameters stored in the IO-Link master are deleted. ■ The IO-Link device parameters are not stored in the IO-Link master. ■ When the IO-Link device is changed, no parameters are transferred to the new IO-Link device.
Restore	Automatic parameter restore is enabled. ■ If no IO-Link device parameters have been stored in the IO-Link master yet, the current IO-Link device parameters are retentively stored once in the IO-Link master as a backup. ■ Changes to individual IO-Link device parameters are not transferred to the backup. ■ When the IO-Link device is changed, the parameters stored during the last backup are automatically transferred to the new IO-Link device (restore).

Backup Mode	Description
Backup/Restore	Automatic parameter backup/restore is enabled. ■ If no IO-Link device parameters have been stored in the IO-Link master yet, the current IO-Link device parameters are retentively stored once in the IO-Link master as a backup. ■ Changes to individual IO-Link device parameters are not transferred to the backup. ■ If IO-Link device parameters are also to be stored in the IO-Link master (backup), you have to transfer them to the IO-Link device with the [Write All] button. ■ When the IO-Link device is changed, the parameters stored during the last backup are automatically transferred to the new IO-Link device (restore).

Create a backup in the IO-Link master

1. Set at *'Master Control → Port Control → Port ...'* for the corresponding port *'C/Q (Pin4) Mode'* to *'IO-Link Manual'*.
   ➡ The *'Backup Mode'* parameter is shown.
2. Set *'Backup Mode'* to *'Disabled'*.
   ➡ The IO-Link device parameters stored in the IO-Link master are deleted.
3. Select your IO-Link device at *'Selected Device'*.
4. Set the IO-Link device parameters for the corresponding port at *'Port ... → Parameters'*.
5. Once you have entered all the parameters, navigate back to *'Master Control → Port Control → Port ...'*, set the according mode *'Restore'* or *'Backup / Restore'* for the corresponding port and confirm your entry with [Apply].
   ➡ The IO-Link device parameters are stored retentively in the IO-Link master (backup). When the IO-Link device is changed, the parameters stored during the last backup are automatically transferred to the new IO-Link device.

For productive operation, you should operate the IO-Link device in 'Manual', 'Restore' mode. If the IO-Link device is replaced due to a defect, for example, the new IO-Link device is automatically supplied with the parameters stored in the backup.

Cycle Time

Here you can specify a fixed cycle time for communication with the IO-Link device. The value 0 means as fast as possible. Otherwise values between 400µs and 132800µs are accepted. The typical response time for an IO-Link device results from the cycle time of the IO-Link device and the typical internal processing time of the master.

– *The 'Cycle Time' parameter is only available if the 'IO-Link Manual' mode is selected.*

I/Q (Pin2) Configuration

A Pin2 configuration is not supported by the IO-Link master.

Vendor, Device and Revision Id

These parameters must match the values read from the IO-Link device. If an IODD is selected, these fields are filled in automatically.

Vendor ID - ID number of the IO-Link device manufacturer.

Device ID - ID number of the IO-Link device.

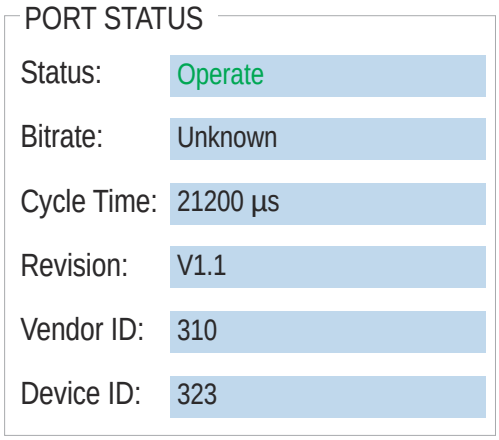
Revision - IO-Link revision of the IO-Link device.

– *These parameters are only available if the 'IO-Link Manual' mode is selected.*

IODD Selection

Use to access the *'IODD Catalog'*. Here you can install the corresponding IODD files via the [Import IODD File] button. If the device goes into *'OPERATE '* (online) state and the IODD is not selected but is present in the catalog, it will be automatically selected.

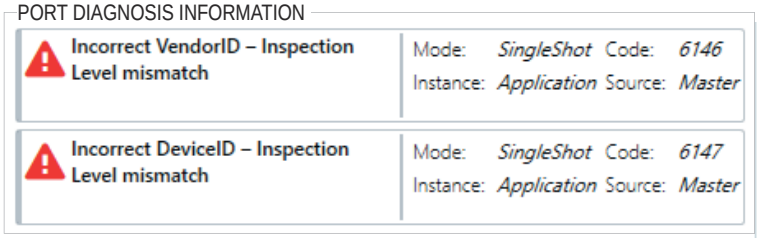
3.4.5.2.2 Port Status



The current status information of the connection is shown in this area. The connection status is updated cyclically at the set refresh rate of the user interface. The vendor, device and revision ID determined from the port status must match the IODD. Deviations are marked accordingly with *'!'*.

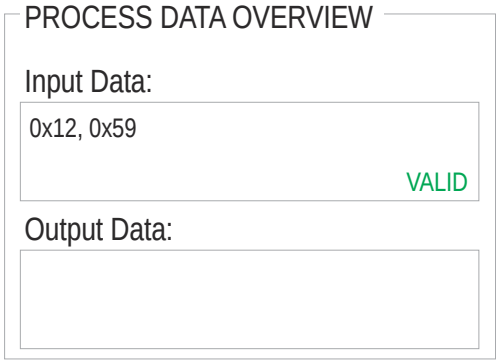
3.4.5.2.3 Port Diagnosis Information

The port-related diagnostic entries reported by the IO-Link master are listed here. The following example shows the reported diagnostic events in the C/Q (pin 4) mode *'IO-Link Manual'* with incorrectly set vendor and device ID.



3.4.5.2.4 Process Data Overview

Depending on the port configuration, the current process data of the inputs and outputs are shown here in the *'Operate'* state. Here, valid data are marked with *'VALID'*. Invalid data are marked with *'INVALID'*.

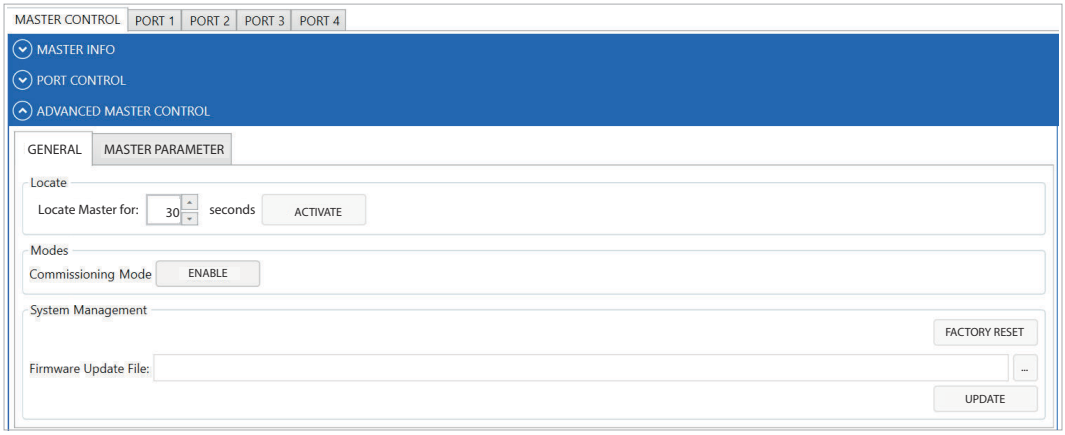


3.4.5.3 Advanced Master Control

3.4.5.3.1 General

Overview

In this dialog, you can basically apply operations to your IO-Link master.



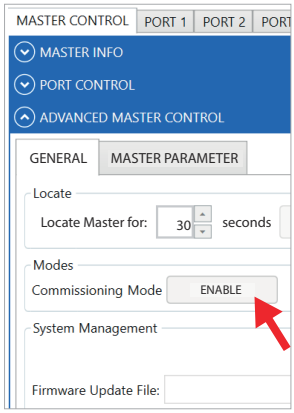
IO-Link master identification

To identify your IO-Link master on the System SLIO backplane bus, you can set a time period in seconds at *'Locate Master...'*. Clicking on [ACTIVATE] starts the *localisation* with device-specific blinking behavior on the IO-Link master.

Commissioning Mode

Commissioning Mode enable

In normal operation (*Commissioning Mode* disabled), the IO-Link Manager has no write access to the process data of an IO-Link device. Please note that in order to be able to send process data from the IO-Link Manager to an IO-Link device, you have to enable the *'Commissioning Mode'* for the corresponding IO-Link master!



1. Select the corresponding IO-Link master in *'Topology'*.
2. In the editors area, navigate to the *'Modes'* area via *'Master Control → Advanced Master Control → General'*.
3. At *Commissioning Mode*, click [ENABLE].

➡
- The button changes to [DISABLE].
- The *Commissioning Mode* for the corresponding IO-Link master is enabled.
- The output data are set to "0" and the output data coming from the header module are ignored.
- The IO-Link Manager has write access to the process data of the associated IO-Link devices.

Commissioning Mode disable

1. Select the corresponding IO-Link master in *'Topology'*.
2. In the editors area, navigate to the *'Modes'* area via *'Master Control → Advanced Master Control → General'*.
3. At *Commissioning Mode*, click [DISABLE].

➡
- The button changes to [ENABLE].
- The *Commissioning Mode* for the corresponding IO-Link master is disabled again.
- The IO-Link Manager has no write access to the process data of the associated IO-Link devices.

Reset to factory settings

Proceeding

1. Switch on the power supply for your system.
2. Open the *IO-Link Manager and establish an online connection to your IO-Link master via the head module.*.
3. Select the corresponding IO-Link master in *'Topology'*.
4. Navigate to the reset dialog via *'Master Control → Advanced Master Control → General'*.

> *To identify the IO-Link master, you can localize it on the System SLIO bus. To do this, enter a period of time in seconds at "Locate Master ..." and click on [ACTIVATE]. This starts the localisation with device-specific blinking behavior at the corresponding IO-Link master for the set period of time.*

5. With the [FACTORY RESET] button at *'System Management'*, you can trigger the reset to Factory setting.

➡ Reset to Factory setting is done and the IO-Link master is restarted without configuration with default parameters.

Firmware update

Here you can apply a firmware update for your IO-Link master.

- You can only apply a firmware update via the IO-Link Manager.
- You can find current firmware versions in the *'Download Center'* of www.yaskawa.eu.com

CAUTION

– When installing a new firmware you have to be extremely careful. In certain circumstances, your CP 042 IO-Link may become unusable if, for example, the power supply is interrupted during transmission or the firmware file is faulty. In this case, please call the Yaskawa hotline!

– *The update deletes the port configurations saved in the IO-Link master and resets the parameters to their default values.*

Proceeding

1. Go to the *'Download Center'* of www.yaskawa.eu.com.
2. Download the corresponding zip file for your IO-Link master to your PC at *'Firmware'*, by stating the order number.
3. Extract the zip file into your working directory.
4. Switch on the power supply for your system.
5. Open the *IO-Link Manager and establish an online connection to your IO-Link master via the head module.*.
6. Select the corresponding IO-Link master in *'Topology'*.
7. Navigate to the firmware update dialog via *'Master Control → Advanced Master Control → General'*.

   To identify the IO-Link master, you can localize it on the System SLIO bus. To do this, enter a period of time in seconds at "Locate Master ..." and click on [ACTIVATE]. This starts the localisation with device-specific blinking behavior at the corresponding IO-Link master for the set period of time.

8. At *'System Management'* navigate with [...] your firmware file in the working directory.
9. Start the firmware update with [Update].

   ➥ During the firmware update, the LEDs C1, F3 and C2, F4 are blinking alternately. After the update, the IO-Link master is restarted without configuration with default parameters.

   If only the LEDs C1 and C2 are blinking alternately, an error has occurred, the IO-Link master is still in Bootloader Mode and indicates this at 'TOPOLOGY'. Check that the firmware file matches your IO-Link master and run the update again. If the error persists, please contact the Yaskawa hotline!

3.4.5.3.2 Master Parameter

Here you can adapt the mapping of the process data accordingly.

CAUTION

Port mapping necessary

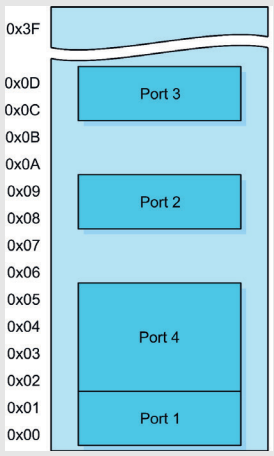
Please note that the port mapping of the process data must always be applied and is not done automatically!

With [WRITE MAPPING] respectively [READ MAPPING] you can transfer your settings to the IO-Link master respectively import them from the IO-Link master.

- By activating *'EnablePqi'*, the input data of devices in *IO-Link* mode are extended by the PQI byte at the end.
- In *'Toggle Bit Interval'* you can specify the interval for changing the status of the toggle bit. A failure on the field side can be detected by cyclically querying the toggle bit (bit 7) in the STATUS byte of the IO-Link master.
- By double-clicking on an entry at *'Mapping'*, you can specify the mapping data for the corresponding port.
  - *'Input/Output Offset'*
    Offset of the input/output data for the corresponding port.
  - *'Input/Output Length (in Byte)'*
    Length of the input/output data.
- The mapping data of the ports are listed with the corresponding colors at *'Mapping Alignment'*.
- Overlaps are detected and marked in red. Data that overlap cannot be transferred.
- Consistency checks are made according to the following rules:
  - The process data of each port must be within the input respectively output process image of the IO-Link master. If *'EnablePqi'* is enabled, the additional PQI byte must be taken into account accordingly for the input data of IO-Link devices in *IO-Link mode*.
  - The process data of the individual ports must not overlap in the input or output process image of the IO-Link master.
  - The process input data of the individual ports must not overlap with the status byte of the IO-Link master.

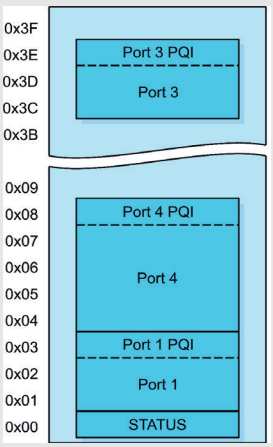
Example of valid port mapping

Output process image



Port	Offset	Length
Port 1	0x00	0x02
Port 2	0x04	0x02
Port 3	0x06	0x02
Port 4	0x3C	0x04

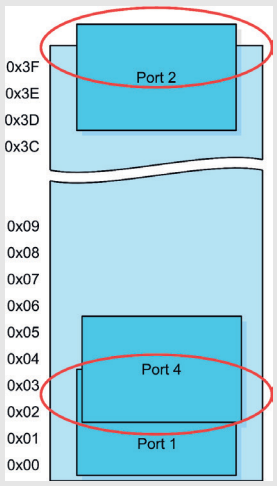
Input process image



Port	Offset	Length
Port 1	0x01	0x02
Port 2	n/a	n/a
Port 3	0x3C	0x02
Port 4	0x04	0x04

Example of incorrect port mapping

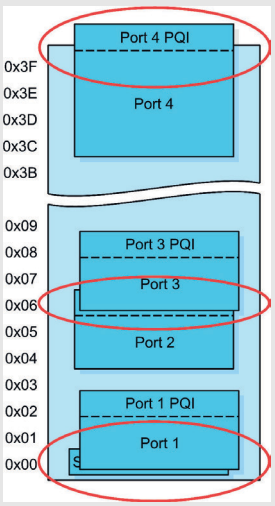
Output process image



Port	Offset	Length
Port 1	0x00	0x04
Port 2	0x3D	0x04
Port 3	n/a	n/a
Port 4	0x02	0x04

- The output mapping of port 2 is partly outside the output process image of the IO-Link master.
- The ranges of port 1 and port 4 overlap.

Input process image



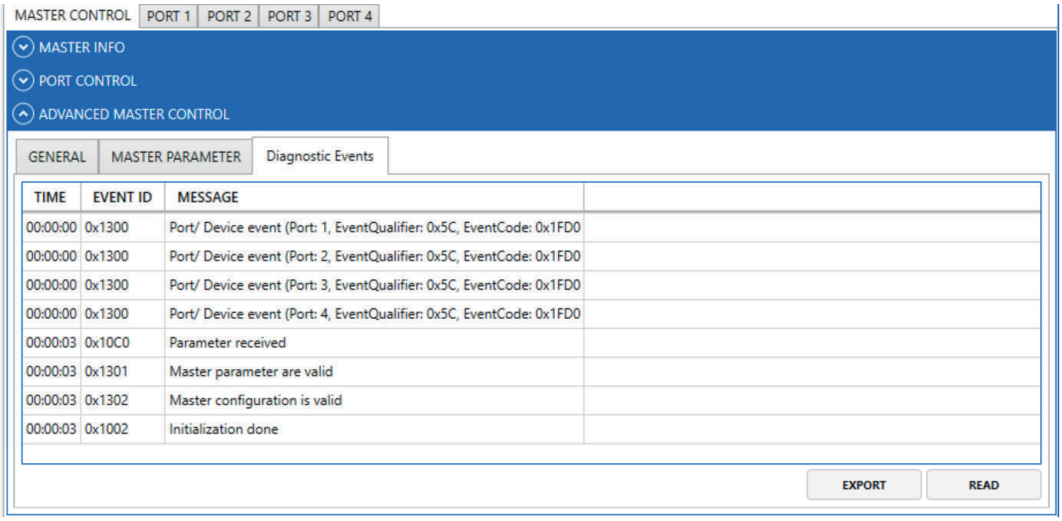
Port	Offset	Length
Port 1	0x01	0x02
Port 2	n/a	n/a
Port 3	0x3C	0x02
Port 4	0x04	0x04

- If PQI is enabled, the port 4 input mapping is outside of the input process image.
- If PQI is enabled, port 2 and port 3 overlap.
- Port 1 overlaps with the status byte.

3.4.5.3.3 Diagnostic Events

In this dialog, all events of the IO-Link master application and the connected IO-Link devices are listed in table form.

- Export
  - With this you can export all event messages to a text file.
- Read
  - You can use this button to refresh the events table.



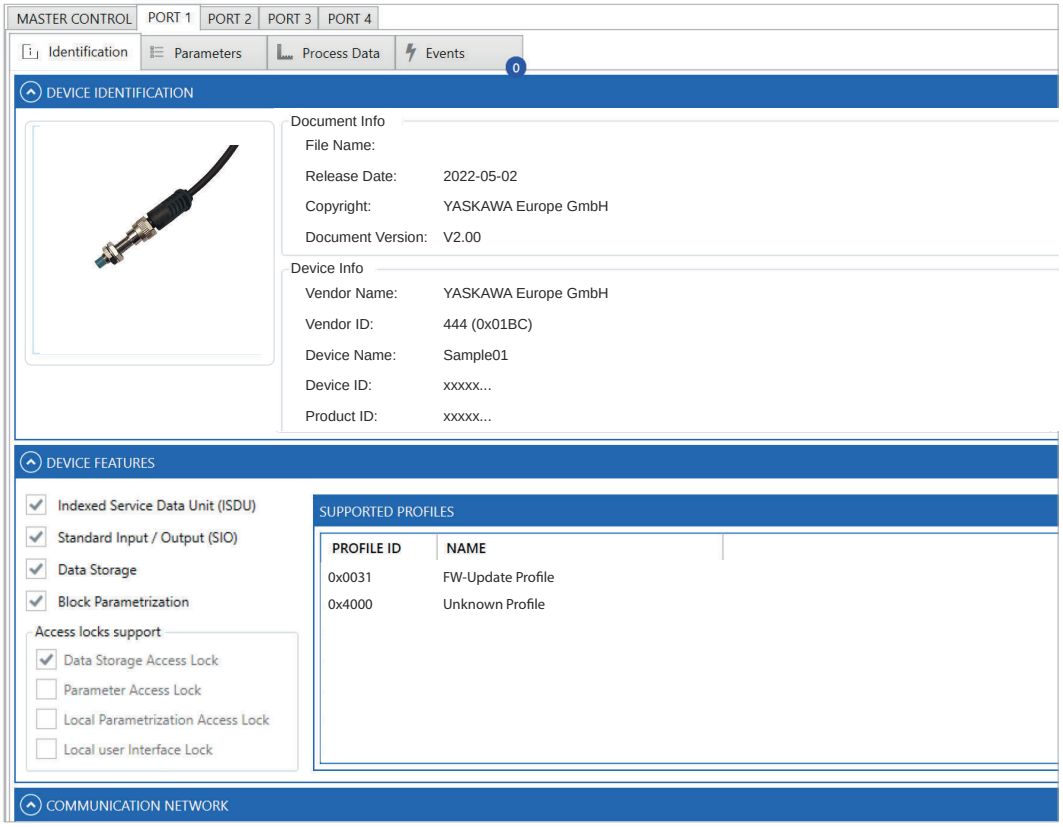
More detailed information on the port events with event ID 0x1300 can be accessed via the tabs 'Port x → Events'. ➦ *'Events'...page 34*

3.4.6 Port x

In the editor area, the *'Port...'* tabs are listed after the *'Master Control'* tab. Here you can parametrize the connected IO-Link device, have access to the status and can retrieve information about the IO-Link device.

3.4.6.1 Identification

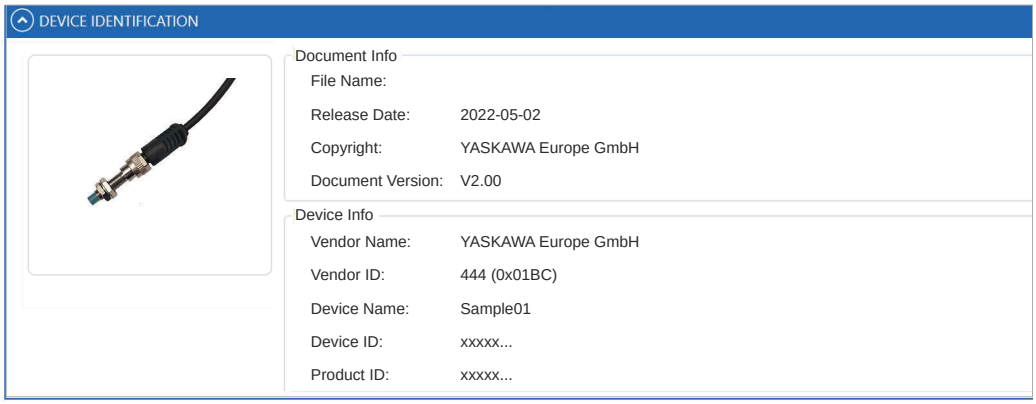
All information from the IODD is processed here and summarized in functional areas.



3.4.6.1.1 Device Identification

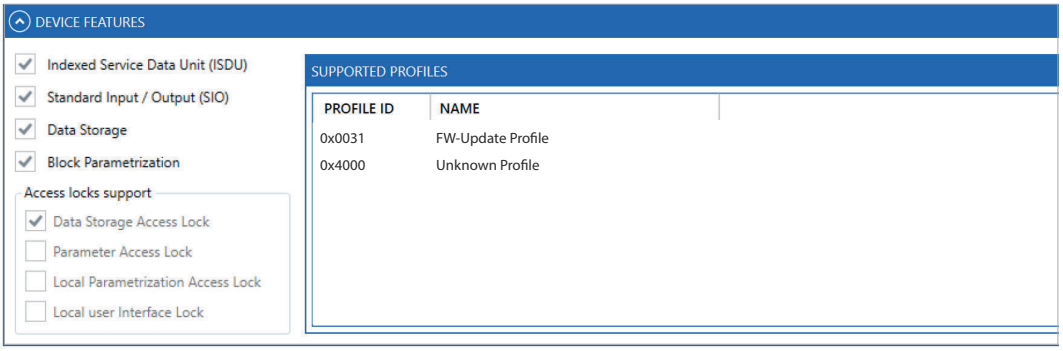
The following data are shown here:

- Document Info
  - Information about the IODD file such as file name, creation date, copyright and version.
- Device Info
  - Information about the IO-Link device such as manufacturer name and ID, device name and ID and product ID.



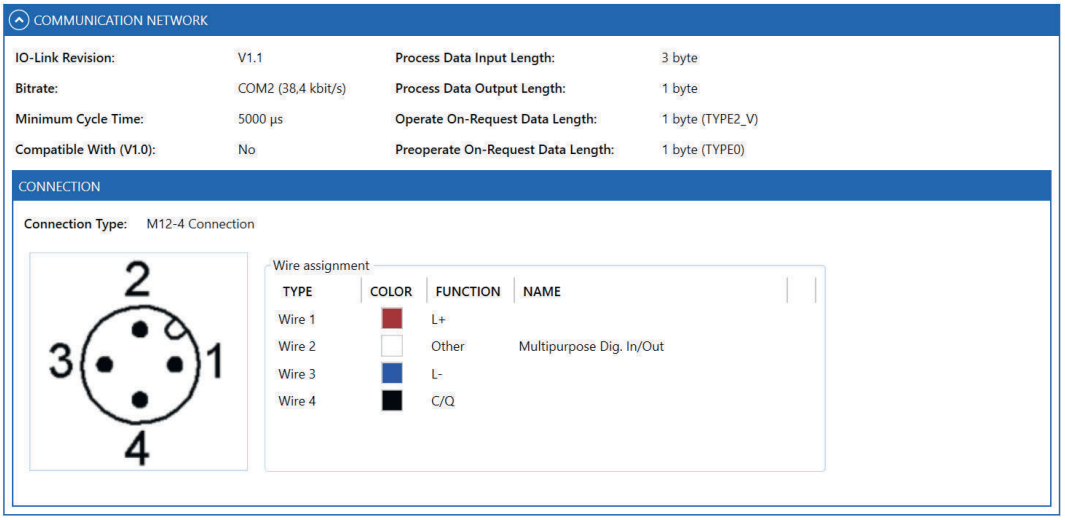
3.4.6.1.2 Device Features

The supported standard functions and profiles are listed here.



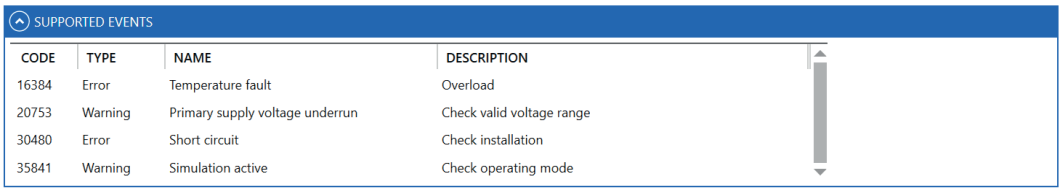
3.4.6.1.3 Communication Network

Here you will find information about the communication such as bit rate, shortest cycle time and process data length. If available, information on the pin assignment is shown at *'Connection'*.



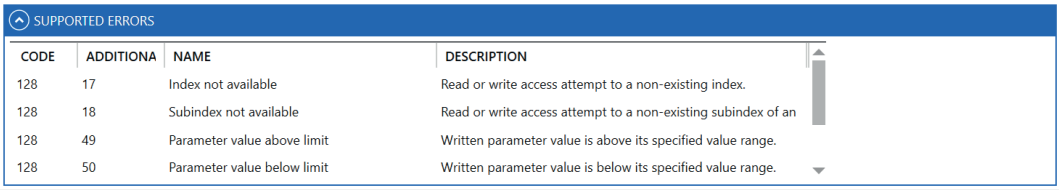
3.4.6.1.4 Supported Events

In this table you will find all event messages that are supported by the IO-Link device.



3.4.6.1.5 Supported Errors

In this table you will find all error messages that are supported by the IO-Link device.



3.4.6.2 Parameters

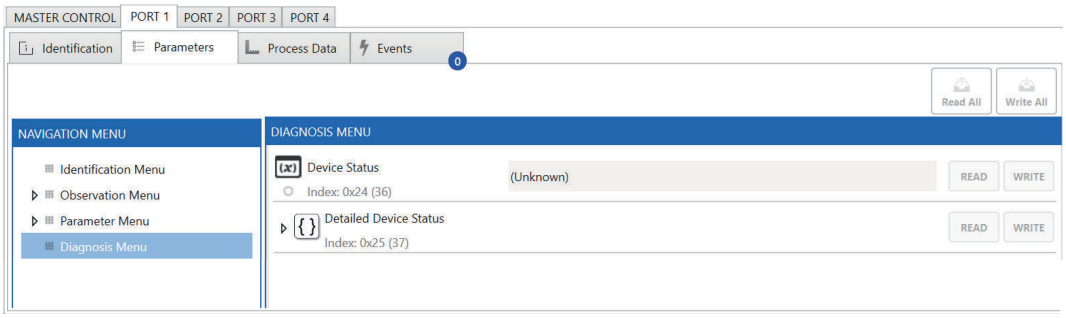
In this dialog window you can parametrize your IO-Link device. To do this, the IO-Link device must be in the *'Operate'* state.

- If an IODD is available, the menu structure and parameter range of the IO-Link device manufacturer are shown.
  - In the menu area you will find all elements that are defined for the set user role.
  - Depending on the selected menu item, the corresponding parameters are listed in the parameter area.
- If no IODD is available, by specifying index and subindex, you can apply an ISDU write or read request for parametrization.

With 'View → Topology → Show / Hide' you can hide the 'TOPOLOGY' area and show the menu structure and parameter area side by side.

3.4.6.2.1 Use with IODD

- The parameters are shown according to the format defined for them in the IODD. These can be input fields, selection fields or buttons.
- Some parameters can only be read or read and written.
- Reading or writing of individual parameters is done with the associated buttons [READ] or [WRITE].
- All currently shown parameters are read or written with the [Read All] or [Write All] buttons.
- If the menu structure changes due to a value change of a conditional parameter, this is recognized by the *IO-Link Manager* and the menu structure is refreshed.



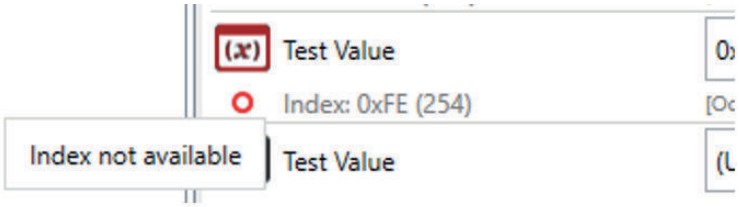
There is the following color assignment for the shown values of the parameters:

- Black
  Parameter value is not known or no value has been transferred and the shown value is a default value.

- Blue
  Parameter value has been adjusted but not yet transferred.

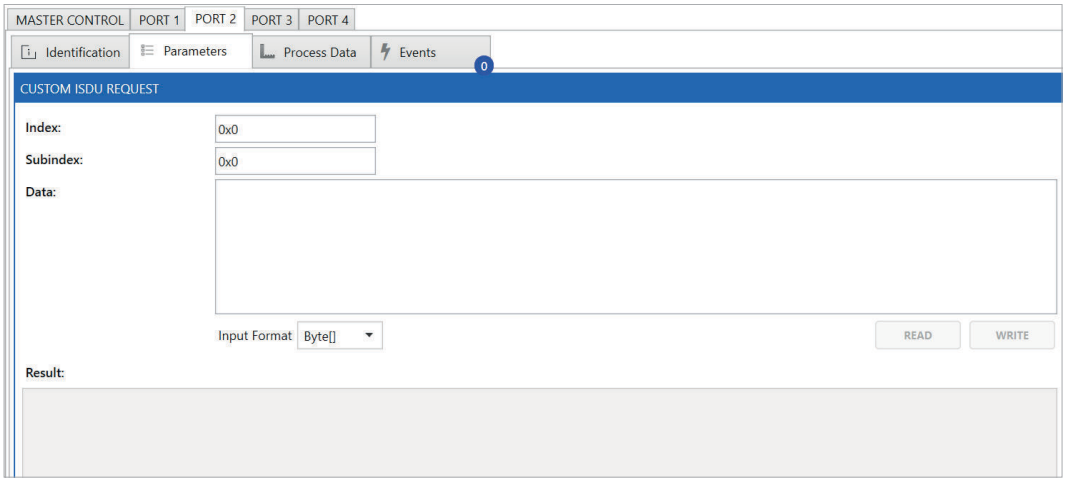
- Green
  The currently shown parameter value also corresponds to the transmitted value.

- Red
  An error occurred when transferring the parameter value. As soon as you move the mouse pointer over the red symbol, the error message is shown as a tool tip.



3.4.6.2.2 Use without IODD

If no IODD is loaded, you still have the option of parametrizing. By specifying index and subindex, you can apply an ISDU write or read request for parametrization.



- *Index*

  The entry for the index can be decimal or hexadecimal. The prefix 0x is to be used for this.

  Range of values: 0 ... 65535
- *Subindex*

  The entry for the index can be decimal or hexadecimal. The prefix 0x is to be used for this.

  Range of values: 0 ... 255
- *Data*

  Enter the data to be written here.

  The input format is a byte array decimal or hexadecimal (prefix 0x) or a string in UTF-8 format.
- *Result*

  The result of the query is shown here as a byte array or ASCII text.

3.4.6.3 Process Data

In this dialog window you have access to the input respectively output data of the IO-Link device. If an IODD is available, the data are processed and listed according to the IODD. Here you can switch between the defined process data elements or select the requested process date from possibly existing combo boxes. Otherwise, the output data must be specified at *'RAW DATA'* as a hexadecimal byte array (prefix 0x).

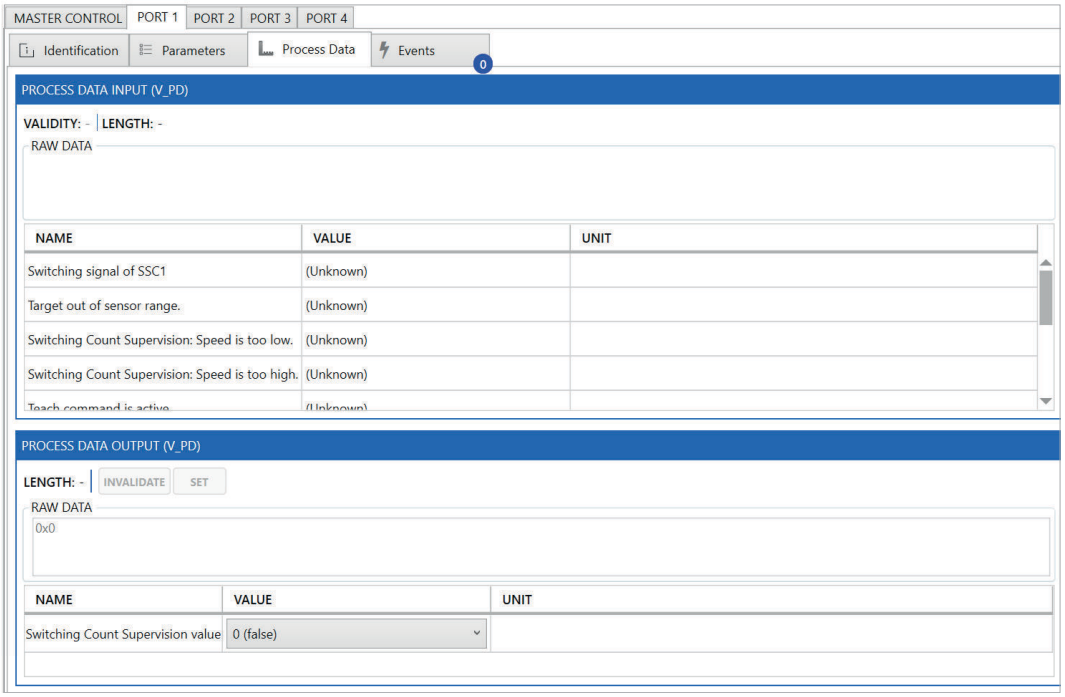
- *Process Data Input*

  Here you will find the input data that the IO-Link device sends to the IO-Link master.
- *Process Data Output*

  Here you can specify output data. With the [SET] button, these are taken from *'RAW DATA'* and transferred to the IO-Link device.

  You can discard the output data with the [Invalidate] button.

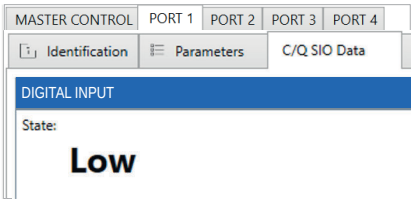
Please note that in order to be able to send process data from the IO-Link Manager to an IO-Link device, you must activate the Commissioning Mode for the corresponding IO-Link master! ➥ *'Commissioning Mode'...page 23*

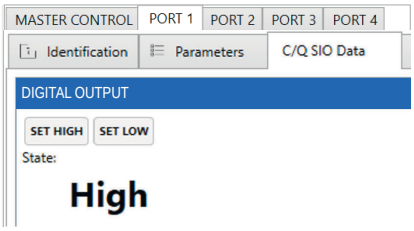


3.4.6.4 SIO Data

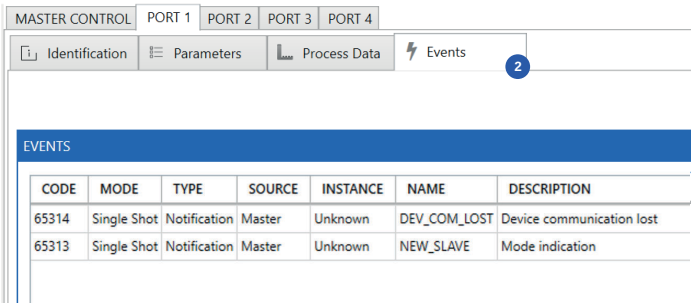
If the port was configured as a digital input or digital output, you can use this dialog to retrieve the status of the input or set and reset the output via the [SET HIGH] and [SET LOW] buttons.

Please note that in order to be able to send process data from the IO-Link Manager to an IO-Link device, you must activate the Commissioning Mode for the corresponding IO-Link master! ➥ *'Commissioning Mode'...page 23*





3.4.6.5 Events

All events for the corresponding port are listed here.

- The last entry in the table is always the most recent message. Sorting is from old to new.
- You can delete all entries with the [Clear] button.
- The table of messages is refreshed with the [Refresh] button.
- The number on the *'Events'* tab indicates the number of messages and the color indicates the urgency.
  - Blue
    The table only contains notifications.
  - Orange
    The table contains at least one warning message.
  - Red
    The table contains at least one error message.