IO-Link – Gateway Management

Guideline for review

Draft Version 0.9.0
December 2020

Order No: 10.192

File name: IO-Link – Gateway Management_10192_dV090_Dec20

The IO-Link Integration group developed this document as a guideline how to coordinate and prioritize the various integration technologies such as fieldbus/PLC, OPC UA, JSON, Webserver, and others when accessing SMI services. Deadline for the review of this draft version is 31-Mar-2021.

Any comments, proposals, requests on this document are appreciated through the IO-Link CR database www.io-link-projects.com. Please provide name and email address.
Login: *IOL-Gateway*
Password: *Report*

Important notes:

NOTE 1 The IO-Link Community Rules shall be observed prior to the development and marketing of IO-Link products. The document can be downloaded from the www.io-link.com portal.

NOTE 2 Any IO-Link Device shall provide an associated IODD file. Easy access to the file and potential updates shall be possible. It is the responsibility of the IO-Link Device manufacturer to test the IODD file with the help of the IODD-Checker tool available per download from www.io-link.com.

NOTE 3 Any IO-Link devices shall provide an associated manufacturer declaration on the conformity of the device. A corresponding form with references to relevant documents is available per download from www.io-link.com.

Disclaimer:

The attention of adopters is directed to the possibility that compliance with or adoption of IO-Link Community specifications may require use of an invention covered by patent rights. The IO-Link Community shall not be responsible for identifying patents for which a license may be required by any IO-Link Community specification, or for conducting legal inquiries into the legal validity or scope of those patents that are brought to its attention. IO-Link Community specifications are prospective and advisory only. Prospective users are responsible for protecting themselves against liability for infringement of patents.

The information contained in this document is subject to change without notice. The material in this document details an IO-Link Community specification in accordance with the license and notices set forth on this page. This document does not represent a commitment to implement any portion of this specification in any company's products.

WHILE THE INFORMATION IN THIS PUBLICATION IS BELIEVED TO BE ACCURATE, THE IO-LINK COMMUNITY MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS MATERIAL INCLUDING, BUT NOT LIMITED TO ANY WARRANTY OF TITLE OR OWNERSHIP, IMPLIED WARRANTY OF MERCHANTABILITY OR WARRANTY OF FITNESS FOR PARTICULAR PURPOSE OR USE.

In no event shall the IO-Link Community be liable for errors contained herein or for indirect, incidental, special, consequential, reliance or cover damages, including loss of profits, revenue, data or use, incurred by any user or any third party. Compliance with this specification does not absolve manufacturers of IO-Link equipment, from the requirements of safety and regulatory agencies (TÜV, IFA, UL, CSA, etc.).

IO-Link ® is registered trademark. The use is restricted for members of the IO-Link Community. More detailed terms for the use can be found in the IO-Link Community Rules on www.io-link.com.

Conventions: In this specification the following key words (in **bold** text) will be used:

may:	indicates flexibility of choice with no implied preference.
should:	indicates flexibility of choice with a strongly preferred implementation.
shall:	indicates a mandatory requirement. Designers **shall** implement such mandatory requirements to ensure interoperability and to claim conformity with this specification.
highly recommended:	indicates that a feature shall be implemented except for well-founded cases. Vendor shall document the deviation within the user manual and within the manufacturer declaration.

Publisher:
IO-Link Community
c/o PROFIBUS Nutzerorganisation
Haid-und-Neu-Str. 7
76131 Karlsruhe
Germany
Phone: +49 721 / 96 58 590
Fax: +49 721 / 96 58 589
E-mail: info@io-link.com
Web site: www.io-link.com

CONTENTS

1 Introduction

1.1 Scope

This document is for those designers and implementers, who want to build a gateway between an IO-Link Master with its Standardized Master Interface (SMI) as a service provider to Ports and Devices on one side and usually divers clients on the other side. The classic approach provides a fieldbus interface to one or more PLCs with deterministic cyclic exchange of Process Data and an interface to a Master tool (PDCT) with acyclic access upon request. Due to the advent of Ethernet-based fieldbuses, nowadays approaches are more complex and additional types of clients such as asset management, audit trailing, cloud systems, and alike are showing up via e.g. OPC UA or JSON.

The number of possible approaches in this field is currently not manageable and thus this document cannot be a specification with detailed information on how to implement but rather a guideline on how to approach and how to avoid traps and pitfalls. The resulting recommendations represent a particular architecture and a set of current best practice patterns. A manufacturer is free to choose any gateway or integration technology and thus is responsible for the gateway testing.

This guideline strives for a maximum of decoupling of the gateway or integration technologies. That means, integration technology A shall not interfere with integration technology B when using the SMI services. However, concurrent access of several clients within one integration technology shall be coordinated within that particular integration technology, for example within an OPC UA server.

The assignment of access rights is based on a user-role model. A manufacturer or user, respectively, can adapt this role model via parameterization depending on the application.

1.2 List of affected patents

There are no affected patents known by the members of the IO-Link gateway management working group. The list is empty. The IO-Link Community does not guarantee the completeness of this list.

2 References

The following document, in whole or in part, is referenced in this document and is indispensable for its application:

IO-Link Community, *IO-Link Interface and System,* V1.1.3, June 2019, Order No. 10.002

3 Terms, definitions, symbols, abbreviated terms and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 61131-9 as well as the following apply.

3.1.1
Integration technology
standardized communication and object model interacting with the IO-Link system

3.1.2
Integration interface
access for clients of the integration technology

3.1.3
Client
user application accessing IO-Link data via an integration interface

45 **3.1.4**
46 **Gateway**
47 component having at least one Ethernet connection point and n IO-Link Ports with connected
48 IO-Link Devices

49

50 ## 3.2 Symbols and abbreviated terms

IE	Industrial Ethernet
Device	IO-Link Device according IEC 61131-9
IODD	Input Output Device Description
ISDU	Index Service Data Unit
IT	Information technology
Master	IO-Link Master according IEC 61131-9
OPC UA	Open Platform Communications Unified Architecture
OT	Operational technology
PDCT	Port and Device Configuration Tool ("Master Tool")
PLC	Programmable logic controller
Port	IO-Link Port according IEC 61131-9

51

52 # 4 Involved technologies

53 ## 4.1 IO-Link technology

54 The system technology (IO-Link) for low-cost sensors and actuators is standardized within IEC
55 61131-9 and supported by IO-Link Community documents (see [1]). It provides an easy and
56 low-cost digital communication for these devices to exchange Process Data, diagnosis infor-
57 mation and parameters with a controller (PC or PLC), while maintaining backward compatibility
58 with DI/DO signals as defined in IEC 61131-2.

59 Communication is "point-to-point" from an IO-Link Master Port to an IO-Link Device. An IO-Link
60 Master can have several Ports and thus communicate quasi-simultaneously with several
61 Devices.

62 Version V1.1.3 (see [1]) of the core IO-Link technology specification introduced a Standardized
63 Master Interface (SMI) in order to harmonize the behaviour of Masters of different brands and
64 to facilitate integration into upper level networks. Now it is possible to just map the integration
65 services to IO-Link objects.

66 ## 4.2 Integration technologies

67 Ever since most fieldbuses moved to Ethernet as basis for their communication more and more
68 integration projects opened Master for access through the Internet (see Figure 1). In the
69 meantime, several different approaches have been standardized or are going to be
70 standardized. Basically, services and data structures are mapped to the IO-Link object world.

71 Within the IO-Link Community, the following integration technologies are currently being
72 standardized. That means, these technologies provide an open/standardized object model in
73 terms of IO-Link and a standardized communication protocol (based on Ethernet as carrier).

74 • Fieldbus integration technologies (IEC 61158 and IEC 61784-1/2), see [5], [6], and [7]
75 • OPC UA technology (Companion standard for IO-Link), see [8]
76 • JSON mapping for IO-Link, see [9]
77 • IO-Link Master tester interface, see [2]

78

In addition, the manufacturer of a gateway is free to realize proprietary access points. For example, webserver integration, cloud connectors, etc.

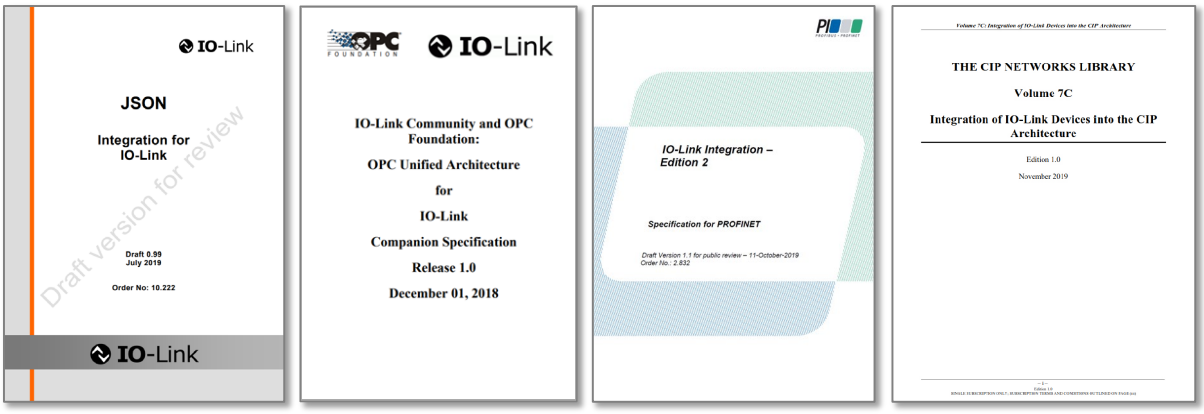

Figure 1 – Sample integration documents

Scope of the corresponding integration documents (see samples in Figure 1) usually is:

- Use of protocols (access via standard communication protocols)
- Object mapping
- Concurrency inside the same type (e.g. access of more than one OPC UA client)
- Security aspects (if necessary)
  - Authorization – access to the functionality
  - Authenticity – reliability
  - Encryption – interception protection
- Handling of multiple master instances (Multi IO-Link Master)

Conversion of these mappings takes place in an IO-Link gateway layer within a hardware component hosting the IO-Link Master as well. This component, as shown in Figure 2, has at least one "Ethernet" connection point (Ethernet port) and n IO-Link Ports for connecting IO-Link Devices. For the sake of simplicity, the component mostly is called "IO-Link Master".

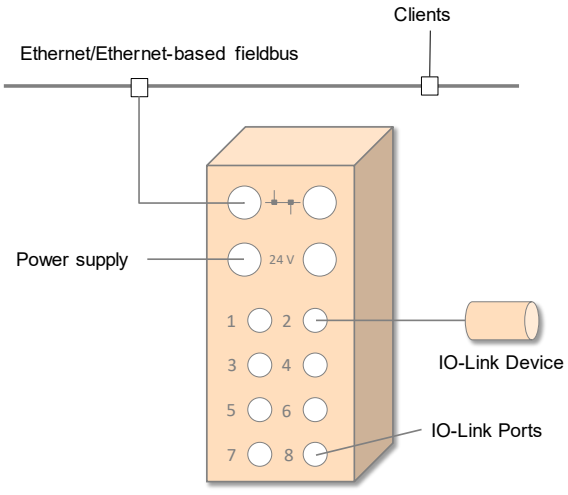

Figure 2 – Hardware component hosting gateway(s) and Master(s)

4.3 IO-Link Gateways

4.3.1 General

IO-Link Gateways are agents between application programs such as PLC programs, asset management, data mining, quality control, or Event logger and IO-Link Devices on an IO-Link Master via adequate integration interfaces and integration technologies.

It can contain one or more IO-Link Master instances. Addressing of the Master instances is provided by the integration technology. The gateway management handles the access rights individually, which means each master can receive different access rights ("AR"). Each Master instance supports its own SMI interface and Master gateway management.

Within this section the descriptions are dealing only with one Master instance.

4.3.2 Classic fieldbus-based automation hierarchy

Within the classic fieldbus-based automation hierarchy according to Figure 3, all Devices are controlled exactly by one client – usually by the fieldbus application. This fieldbus application essentially has unrestricted access to the functionality of the Device. Concurrent accesses are handled within the gateway (fieldbus).

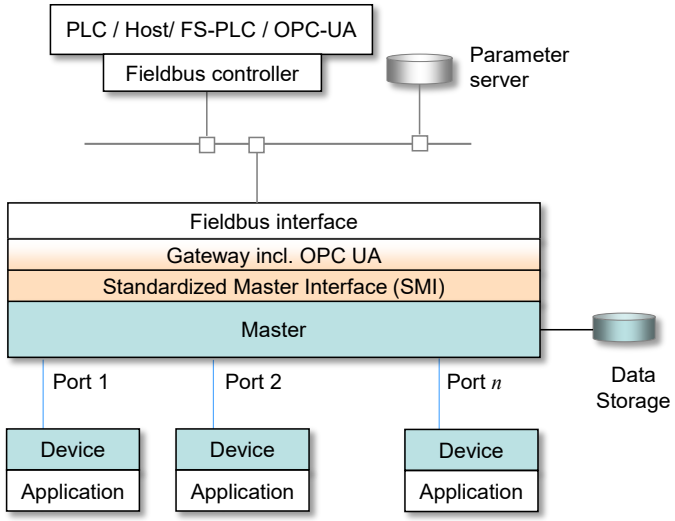

Figure 3 – "Classic" fieldbus-based automation hierarchy

4.3.3 Extended sharing automation hierarchies

Due to Ethernet-based automation communication, office applications (Internet Technology = IT) can easily get access to IO-Link Devices as already mentioned in 4.3.1. That means, the IO-Link resources are shared between several clients as shown in Figure 4.

In addition to the classic interfaces, more and more "cloud connectors" are supported, which ensure the coupling to corresponding cloud infrastructures. Multiple client instances (e.g. Internet/web browsers) can connect to an integrations interface (for example a built-in Web-server).

Figure 4 shows an IO-Link gateway/Master with 6 integration interfaces and 8 clients running concurrently. "SMI_xyz ()" represents one of the SMI services specified in [1]. ClientIDs are assigned by the Standardized Master Interface at invocation of an SMI service.

Hint: The IO-Link Master tester is currently not assigned to take over testing of gateway features. However, in case of FS-Masters, the safety gateway is partly tested by the FS-Master tester (see [3]).

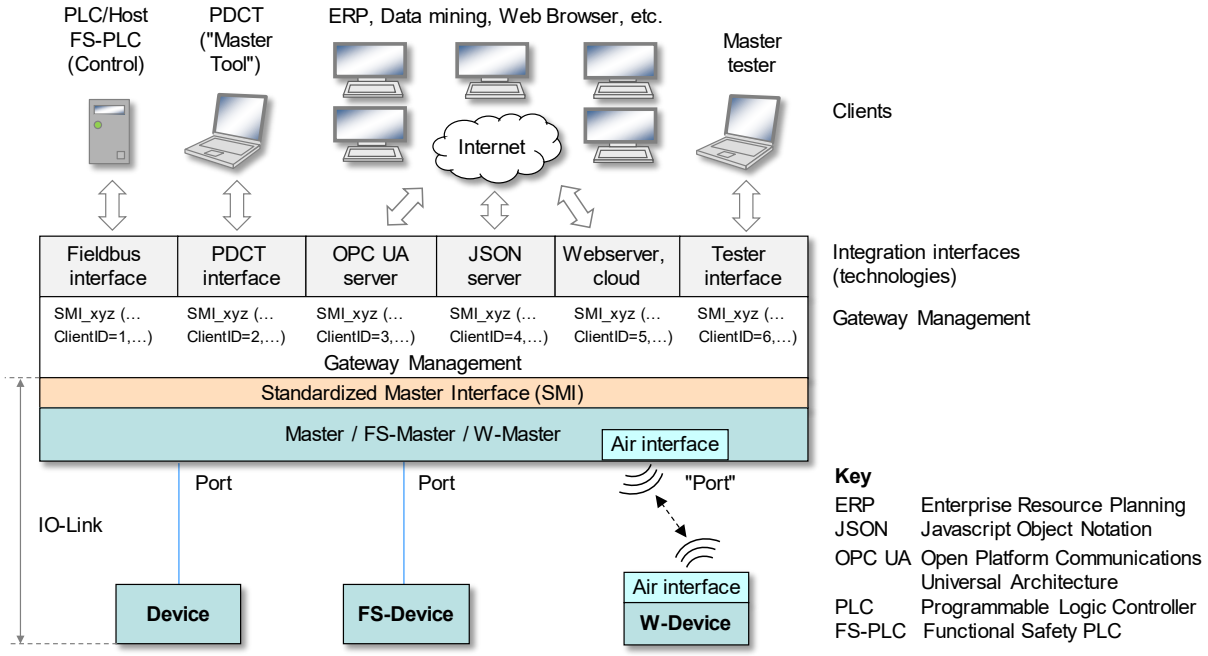

Figure 4 – Extended sharing automation hierarchies

5 Status and line of actions

5.1 Access conflicts

Currently, there is no "standardized" access coordination specified for integration interfaces within the gateway in IO-Link specifications. Thus, client applications on different integration interfaces can in fact access one and the same Device (object) simultaneously and concurrently (see Figure 4).

For example, a client application could change the Port configuration of one particular Device and another client application could change its parameters at the same time.

In order to avoid undefined reactions of an automation system and thus possible expensive damages, gateway manufacturers would be forced to design and implement proprietary coordination rules and means.

However, this would lead automatically to unacceptable different system behaviors for customers and users.

5.2 Two tier approach

Objective of this document is creating a uniform method for the coordination of different integration interfaces. This has the two aspects of

a) how this coordination feature is presented to the customers/users, and

b) which kind of algorithms and software technologies should be implemented.

A two-tier approach shall lead to a final specification. The first tier is heading for an agreed upon user view and the second tier will comprise implementation recommendations.

It is not an objective of this document to coordinate different clients within one integration technology/interface. For example, the question how to deal with different clients using the OPC UA server is responsibility of this integration technology document.

5.3 Generic vs. user-controlled behavior

Two principles for coordination are possible and for the IO-Link gateway it has not been decided, which to follow.

Basically, it would always be the most convenient way for customers/users, if coordination could be achieved automatically via a generic behavior. However, since the gateway cannot acquire information on how clients are using the integration interfaces, a generic behavior is difficult to design, and the method would be most likely error prone.

The other method provides a configuration tool to the user for the assignment of authorizations/prioritizations to achieve a stable system behavior. It assumes the user can assign the access rights based on user-roles.

5.4 User-roles and Access Rights

5.4.1 General

Which function will/shall be available at which interface (client) can only be defined

- by the gateway manufacturer, or
- by the customer/user

In this document, a user-role approach is specified.

5.4.2 User-roles

The user can determine via user-roles, which feature shall be performed at which interface, or which feature shall be blocked. The supported features are linked to the user-roles in an abstract and comprehensible way as shown in Table 1.

Table 1 – User-roles

User-role	Use case	Access	Clients
IOL-Master superuser	Client (Application) gets all rights starting from Master/Port/Device commissionig up to the control of output Process Data	- Writable access to all services of Master/Port/Device - Readable access to all services of Master/Port/Device	Control applications (e.g. PLC) responsible for IO-Link Master/Device configuration and input/ output control
IOL-Master commissioning	Client gets rights for Port /Device commissionig except for “output Process Data control”	- Writable access to all services of Master/Port/Device except for output data - Readable access to all services of Master/Port/Device	Tool applications (PDCT) which are responsible for Port and Device commissioning
IOL-Port superuser	Client (Application) gets all rights for Device commissionig up to the control of output Process Data	- Writable access to all services of Device - Readable access to all services of Master/Port/Device	Control applications (e.g. PLC) not responsible for Port configuration
IOL-Device commissioning	Client (Application) gets all rights for Device commissionig except for output Process Data	- Writable access to all services of Device except for output data - Readable access to all services of Master/Port/Device	Tool applications (PDCT) responsible for IO-Link Device commissioning without Port configuration
IOL-Monitoring	Client (Application) gets all rights to read Port/Device objects	- Readable access to all services of Master/Port/Device	Asset/Diagnosis/Monitor clients responsible to show information
Access denied	Client (Application) get no rights to read Port/Device objects	Gateway management blocks the whole functionality (read/ write). Therefor the IO-Link system is not visible from client point of view.	For example, in production the test functionality is not visible until the functionality is enabled.

5.4.3 Access Rights of user-roles

There are several areas where access rights are handled. At first the manufacturer of a gateway, who considers the availability of access rights at the integration interfaces. Then the provider of a particular application, who defines its necessary access rights. Finally, the user configures the gateway accordingly. Table 2 shows the handling principles of access rights.

183 **Table 2 – Handling of Access Rights**

Stage	Responsible	Responsibility
1	Manufacturer of gateway	Defines the access rights of the integration interfaces (upon customer demands)
2	Original Equipment Manufacturer	Assigns the access rights for a particular application
3	User	Final allocation of access rights within the deployed gateway

184

185 The user shall be informed not to establish Access Rights higher than required for a particular
186 application. Otherwise, undefined states of the automation system can occur.

187 Table 3 illustrates the effects of rules for user-roles/access rights.

188 **Table 3 – Effects of Access Rights/user-roles**

No	Rule	Effect
1	Only one client with the role "IOL-Master superuser" or "IOL-Device superuser" is permitted	Only one client can control the Device outputs
2	Only one client with the role "IOL-Master superuser" or "IOL-Master commissioning" is permitted	Only one client can set up the Port configuration
3	An unlimited number of clients with the roles "IOL-Device commissioning" are permitted	Several clients can handle Device functionality (write/read)
4	An unlimited number of clients with the role "IOL-Monitoring" are permitted	Several clients can monitor IO-Link functionality (read)
5	It is possible to prevent a client from Device access	Access to Devices blocked

189

190 ### 5.4.4 Dynamic assignment of user-roles

191 Normally, the user-roles are assigned statically and remain unchanged during operation. The
192 user-roles could only be changed during reconfiguration of the gateway.

193 In special cases it is necessary to change roles during operation by authorized clients via the
194 gateway management (administration?) object. Table 4 shows the options.

195 **Table 4 – Access to gateway management object**

Option	Access to gateway management object
Read	Each client/integration interface can have read access to the gateway management object to acquire the Access Rights of the client
Change	Each authorized client can change the Access Rights using the gateway management object
Default	Predefined configuration of the gateway management object is: Fieldbus is "IOL-Master superuser", all other supported interfaces are set to Access Rights "IOL-Monitoring"

196

197 ## 5.5 Basic use cases

198 ### 5.5.1 PLC-based Master/Port configuration

199 Figure 5 shows an example of how to use the user-roles/Access Rights mechanism for use
200 case: "PLC-based Master configuration".

201 The *Fieldbus/PLC/Host* client gets the user-role/Access Right "IOL-Master superuser", which
202 means, the output Process Data access and change of Port configuration is only possible in
203 this example via PROFINET (Fieldbus) interface.

PDCT ("Master Tool") gets the user-role/Access Right "IOL-Device commissioning", which means, the Tool can read all IO-Link objects and additionally can start and test Devices via Device parametrization (full access to the Device).

Master tester interface should be hidden during operation. Therefore, the Tester interface gets the user-role/Access Right "Access denied". It is up to the Master/gateway manufacturer to enable the interface in special test situations.

Clients providing only the display of e.g. Process Data and parameter values get the user-role/Access Rights "IOL-Monitoring". For example, if an OPC UA interface is only used for showing diagnosis and identification data.

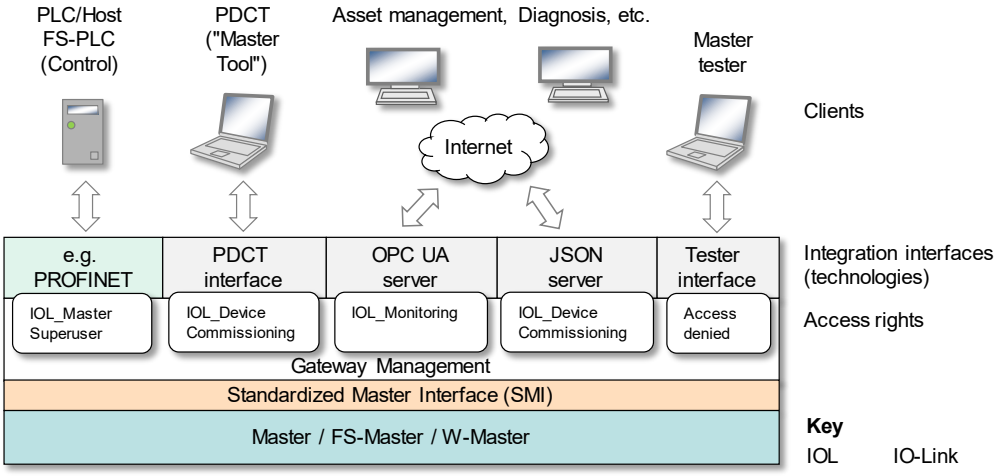

Figure 5 – PLC-based Port configuration

5.5.2 Tool-based Port configuration

Figure 6 shows an example of how to use the user-roles/Access Rights mechanism for use case: "PDCT-based Master configuration".

The *Fieldbus/PLC/Host* client gets the user-role/Access Right "IOL-Device superuser", which means, the output Process Data access is only possible in this example via PROFINET (Fieldbus). However, Port configuration *cannot* be changed by the *Fieldbus/PLC/Host* client.

PDCT ("Master Tool") gets the user-role/Access Right "IOL-Master commissioning", which means, *PDCT* can adapt the Port configuration and start und test Devices via parameterization.

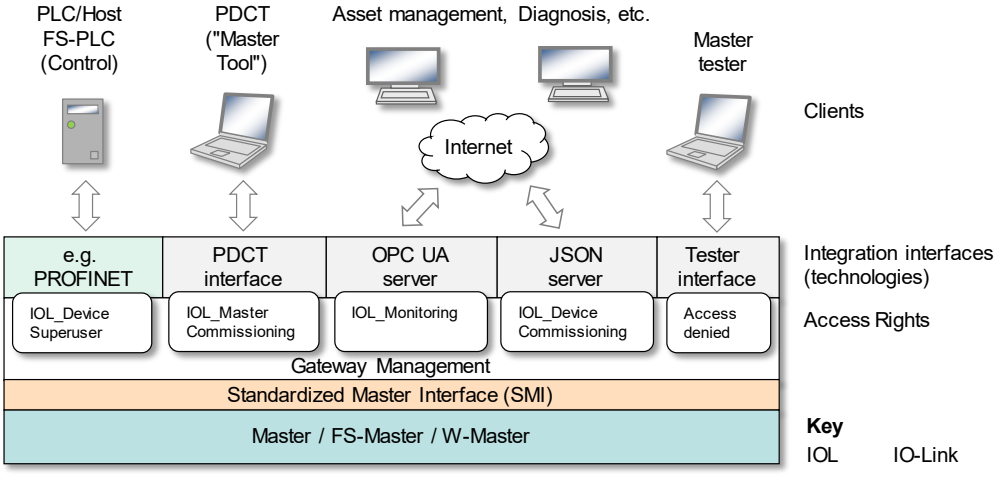

Figure 6 – Tool-based Port configuration

Master tester interface and clients providing only the display of values are already described in 5.5.1.

6 Client/Interface coordination

6.1 Client/interface coordination mechanism

The gateway must ensure the SMI services are performed conflict-free in order to guarantee a reliable automation system.

The SMI specification in [1] per se supports a client coordination mechanism using a unique ClientID handle in each SMI service invocation for responding to the correct invoking client (see Figure 7).

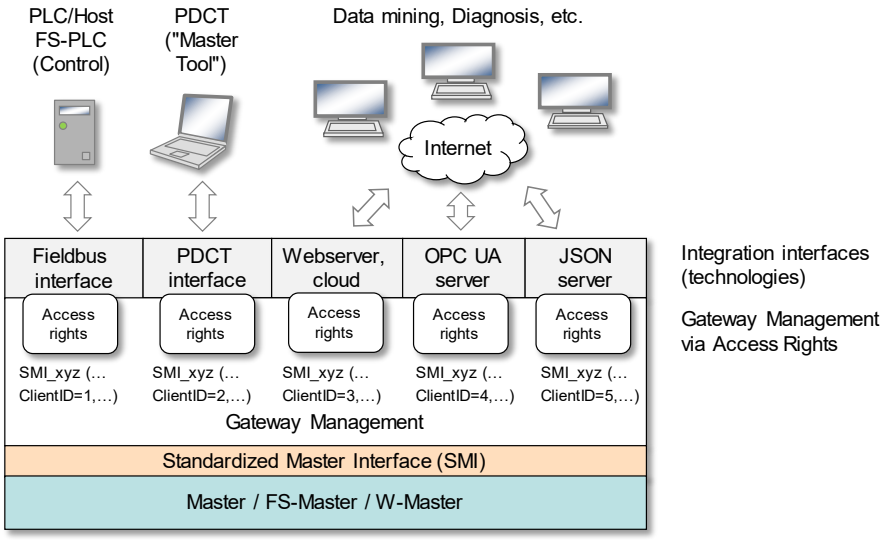

Figure 7 – Interface coordination via ClientIDs

6.1.1 Push services

Gateway management is responsible to forward the push services SMI_DeviceEvent and SMI_-PortEvent to all registered interfaces concurrently.

6.1.2 Concurrency and prioritization of SMI services

This concept is specified in clause 11.2.3 of [1]. It describes the concurrency mechanism of SMI that shall be implemented in each SMI layer.

Table 5 shows the rules for concurrency of SMI services when accessing attributes.

Table 5 – Rules for accessing attributes

Rule	Description
aa1	All SMI services with different Port number access different Port objects (disjoint operations)
aa2	Different SMI services using the same Port number access different attributes/methods of a Port object (concurrent operations)
aa3	Identical SMI services using the same Port number and different ClientID access identical attributes concurrently (consistency)

Table 6 shows the rules for SMI services when accessing methods.

Table 6 – Rules for accessing methods

Rule	Description
am1	SMI services for methods using different Port numbers access different Port objects (disjoint operations)

Rule	Description
am2	SMI services for methods using the same Port number and different ClientIDs create job instances and will be processed in the order of their arrival (*n* Client concurrency)
am3	SMI_ParamWriteBatch (ArgBlock "DeviceBatch") shall be treated as a job instance that shall not be interrupted by any SMI_DeviceWrite or SMI_DeviceRead service.

Prioritization of SMI services within the Standardized Master Interface is not performed. All services accessing methods will be processed in the order of their arrival (first come, first serve).

6.2 Client coordination mechanisms

6.2.1 Overview

To ensure reliability, a client coordination mechanism shall be carried out as described in clause 5. Therefore, the gateway provides a component "gateway management", which is responsible to manage the Access Rights of each interface.

6.2.2 User view of gateway management

The user can assign the corresponding Access Rights interface specific. Figure 8 shows an exemplary display for a user dialog. The user can assign a role to each interface, which also defines the Access Rights.

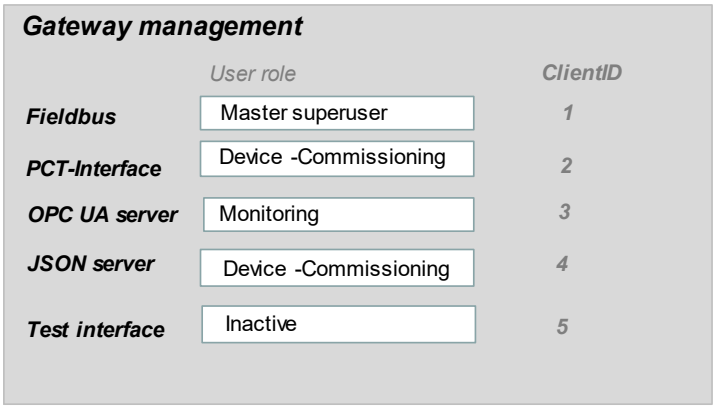

Figure 8 – Gateway management dialog

The rules for the gateway management are shown in Table 7.

Table 7 – Rules for gateway management

Rule	Description
gm1	Each interface offers access to Master object "Gateway management"
gm2	Each interface (integration) provides readable access to the Master object "Gateway management"
gm3	One or more interfaces can be used for Write access in order to change the Access Rights
gm4	It is up to the gateway manufacturer to decide which interface can be written

6.2.3 Access Rights check

The component "gateway management" (middleware) shall check the Access Rights of each client.
Each client/interface invokes SMI services. The gateway management instance checks the permission to perform this service with respect to the user-role of the interface. The SMI service

will be performed in case of permission, it will be blocked in case of no permission and an ErrorCode "Access Right Error" will be issued as shown in Table 8.

Table 8 – Mapping of user-roles

SMI service name	User-roles				
	IOL-Master superuser	IOL-Master commisioning	IOL-Device superuser	IOI-Device commisioning	IOL-Monitoring
SMI_MasterIdentification	x	x	x	x	x
SMI_PortConfiguration	x	x	AR error	AR error	AR error
SMI_ReadbackPortConfiguration	x	x	x	x	x
SMI_PortStatus	x	x	x	x	x
SMI_DSToParServ	x	x	x	x	x
SMI_ParServToDS	x	x	x	x	AR error
SMI_DeviceWrite	x	x	x	x	AR error
SMI_DeviceRead	x	x	x	x	x
SMI_ParamWriteBatch	x	x	x	x	AR error
SMI_ParamReadBatch	x	x	x	x	x
SMI_PortPowerOffOn	x	x	AR error	AR error	AR error
SMI_DeviceEvent	x	x	x	x	x
SMI_PortEvent	x	x	x	x	x
SMI_PDIn	x	x	x	x	x
SMI_PDOut	x	AR error	x	AR error	AR error
SMI_PDInOUT	x	x	x	x	x
SMI_PDInIQ	x	x	x	x	x
SMI_PDOutIQ	x	AR error	x	AR error	AR error
SMI_PDReadbackOutIQ	x	x	x	x	x

Bibliography

[1] IO-Link Community, *IO-Link Interface and System*, V1.1.3, June 2019, Order No. 10.002

[2] IO-Link Community, *IO-Link Test*, V1.1.3, in progress, Order No. 10.012

[3] IO-Link Community*, IO-Link Safety System Extensions with SMI,* Version 1.1, April 2018, Order No. 10.092

[4] IO-Link Community*, IO-Link Wireless System Extensions,* Version 1.1, March 2018, Order No. 10.112

[5] PI specification, *IO-Link Integration* – Edition 2, Version 1.1, December 2019, Order No. 2.832

[6] ODVA, *CIP Common Specification volume 7C*, November 2019

[7] EtherCat Technology Group, *Modular Device Profile – Part 6220: IO-Link Master*, V1.0.5, April 2017, Order No. ETG 5001.6220

[8] OPC Foundation Companion Specification, *OPC UA for IO-Link*, Version 1.0, December 2018

[9] IO-Link Community, JSON – Integration for IO-Link, Version 1.0, January 2020

_____

IO-Link Community
c/o PROFIBUS Nutzerorganisation e.V.
Haid-und-Neu-Str. 7
76131 Karlsruhe
Germany
Phone: +49 (0) 721 / 96 58 590
Fax: +49 (0) 721 / 96 58 589
e-mail: info@io-link.com
http://www.io-link.com/

IO-Link