

SIMATIC Ident

RFID systems
SIMATIC RF185C, RF186C,
RF188C, RF186CI, RF188CI

Operating Instructions

<u>Introduction</u>	1
<u>Security recommendations</u>	2
<u>Description</u>	3
<u>Mounting</u>	4
<u>Connection</u>	5
<u>Configuring</u>	6
<u>Configuring with the WBM</u>	7
<u>Programming via SIMATIC controller</u>	8
<u>Programming via XML</u>	9
<u>Programming via OPC UA</u>	10
<u>Programming via Rockwell controller</u>	11
<u>Service and maintenance</u>	12
<u>Technical data</u>	13
<u>Dimension drawings</u>	14
<u>Appendix</u>	A
<u>Syslog messages</u>	B
<u>Service & Support</u>	C

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Table of contents

1	Introduction	7
2	Security recommendations	9
3	Description.....	15
3.1	Properties of the communications modules	15
3.2	I/O functions of the CI device versions	17
3.3	User-specific procedure	17
3.4	Design	19
4	Mounting.....	21
4.1	Installation dimensions and position	21
4.2	Mounting the communications module	22
4.3	Use at altitudes over 2,000 m	24
5	Connection	27
5.1	Network topology	28
5.2	Operation of the CM on grounded/ungrounded power supply	30
5.3	Electrical design of the CM	33
5.4	Connecting CM to functional ground	36
5.4.1	Mounting the CM on a conductive base	36
5.4.2	Mounting the CM on a non-conductive base	38
5.5	Connecting the communications module.....	40
5.6	Supply voltage and PROFINET IO loop-through	45
5.7	Effect of cable length on the supply voltage	46
6	Configuring	47
6.1	Assign the IP address / device name	47
6.1.1	Assigning the IP address / device name with STEP 7.....	47
6.1.2	Assigning the IP address / device name with SINEC PNI	50
6.1.3	Assigning an IP address via DHCP	51
6.2	Configuration via PROFINET IO.....	52
6.3	Configuration via XML.....	59
6.4	Configuration via OPC UA	59
6.5	Configuring with Studio 5000 Logix Designer.....	60
7	Configuring with the WBM.....	61
7.1	Starting WBM	61
7.2	The WBM	63

7.3	The menu items of the WBM	68
7.3.1	The "Start page" menu item	68
7.3.2	The "Settings - General" menu item	70
7.3.3	The "Settings - Reader Interface" menu item	71
7.3.4	The "Settings - Digital outputs" menu item	78
7.3.5	The "Settings - Communication" menu item	80
7.3.6	The menu command "Diagnostics - Hardware diagnostics"	93
7.3.7	The "Diagnostics - Log" menu item.....	97
7.3.8	The "Diagnostics - Service Log" menu item	99
7.3.9	The "Diagnostics - Syslog logbook" menu item	101
7.3.10	The "Edit transponder" menu item	102
7.3.11	The "User management" menu item.....	104
7.3.12	The menu item "System - System settings"	108
7.3.13	The menu command "System - Reader firmware"	110
7.3.14	The "Help" menu item	110
8	Programming via SIMATIC controller	111
8.1	Digital inputs/outputs.....	111
9	Programming via XML.....	113
10	Programming via OPC UA	115
10.1	Supported methods/functions	116
10.2	OPC UA variables	122
10.2.1	Description of the variables.....	122
10.2.2	ExecuteScan	122
10.2.3	SimaticIdentModelVersion	123
10.2.4	CommonSettings.....	123
10.2.5	RfidSettings.....	124
10.2.6	Diagnosis	125
10.2.7	DigitalIOPorts	133
10.3	OPC UA events.....	135
10.3.1	Description of the events	135
10.3.2	AutoldPresenceEvent	136
10.3.3	RfidLastAccessEvent	137
10.3.4	AutoldLastLogEntryEvent	142
11	Programming via Rockwell controller.....	143
12	Service and maintenance.....	145
12.1	Diagnostics.....	145
12.1.1	Diagnostics via the LED display.....	146
12.1.2	Diagnostics via SNMP	149
12.1.3	Diagnostics using the WBM	150
12.1.4	Diagnostics using the TIA Portal (STEP 7 Basic / Professional)	150
12.1.5	Diagnostics via XML	152
12.1.6	Diagnostics over OPC UA.....	152
12.1.7	Diagnostics using Studio 5000 Logix Designer	153
12.1.8	Parameterization of the diagnostics.....	153
12.2	Error messages.....	155
12.2.1	Error messages of the communications module.....	155
12.2.2	Reading out error messages using the WBM	163

12.2.3	XML error messages.....	163
12.2.4	OPC UA error messages	163
12.3	Firmware update	166
12.3.1	Updating the firmware via WBM	167
12.3.2	Update firmware via TIA Portal (STEP 7 Basic / Professional)	168
12.3.3	Updating firmware of the readers using the TIA Portal (STEP 7 Basic / Professional)	169
12.4	Factory defaults	171
12.4.1	Restoring the factory settings via WBM	171
12.4.2	Reset the factory setting with SINEC PNI.....	172
12.4.3	Restoring the factory settings manually	173
12.5	Module replacement	174
12.5.1	Backup configuration data	175
12.5.2	Replacing a module	177
13	Technical data	179
13.1	Technical specifications RF185C, RF186C, RF188C	179
13.2	Technical specifications for RF186CI, RF188CI.....	181
14	Dimension drawings.....	183
A	Appendix.....	185
A.1	System planning	185
A.2	Connecting cables	186
A.2.1	Standard cables	186
A.2.2	Custom assembled connecting cables	186
A.3	Operation of optical handheld readers, access control readers or serial devices	188
A.3.1	Compatible Ident devices	188
A.3.2	Connecting handheld readers / access control readers / serial devices	188
A.3.3	Hardware configuration.....	189
A.3.4	Functions and commands.....	191
A.3.5	Block-specific error messages	193
A.4	Compatibility with SIMATIC RF180C.....	194
A.5	Ordering data	196
A.6	Certificates & approvals	199
B	Syslog messages.....	201
B.1	Structure of the Syslog messages	201
B.2	Variables in Syslog messages	202
B.3	List of Syslog messages	203
C	Service & Support.....	207

Introduction

Purpose of these operating instructions

The information provided in these operating instructions enables you to commission the SIMATIC RF18xC and RF18xCI communication modules.

Basic knowledge required

These operating instructions assume general knowledge of automation engineering and identification systems.

Scope of validity of this documentation

These operating instructions are valid for the SIMATIC RF185C, RF186C, RF188C, RF186CI, and RF188CI communication modules as of product version "01", firmware version V1.3 and delivery date as of 05/2020.

Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

SIMATIC ®, SIMATIC RF ®, MOBY ®, RF MANAGER ®, SIMATIC Sensors ®

Orientation in the documentation

In addition to these operating instructions, you require the operating instructions for the S7-300, S7-400, S7-1200 or S7-1500 controller used. When using an S7 controller, you can find information on programming the module and a complete error description in the description of the "Ident profile and Ident blocks" function blocks, the RFID standard profile and the FB 45.

You can find all relevant information for XML configuration and programming in the "XML Programming for SIMATIC Ident" manual. You can find the information on configuring and programming over EtherNet/IP in the "Ident profile, Add-on instruction for Rockwell systems" manual.

You can find information on the readers and optical readers to be connected in the manual of the respective product family (RF200, RF300, MV400, and MV500).

You can find the current versions of the various manuals on the pages of the Siemens Industry Online Support (<https://support.industry.siemens.com/cs/ww/en/ps/14970/man>).

Abbreviations and naming conventions

The following terms/abbreviations are used synonymously in this document:

Transponder, tag

Data medium, mobile data storage (MDS)

Communication module (CM)

Interface module (ASM)

Recycling and disposal



The products are low in harmful substances, can be recycled and meet the requirements of the Directive 2012/19/EU for disposal of waste electrical and electronic equipment (WEEE).

Do not dispose of the products at public disposal sites.

For environmentally compliant recycling and disposal of your electronic waste, please contact a company certified for the disposal of electronic waste or your Siemens representative.

Adhere to the various country-specific regulations.

Security recommendations

To prevent unauthorized access, observe the following security recommendations when working with the communication module and WBM (Web Based Management).

General

- Check regularly that the device complies with these recommendations and/or other internal security policies.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.

Physical access

- Restrict physical access to the device to qualified personnel.
- Lock unused physical ports (e.g. Ethernet ports) on the device. Unused ports can be used to access the system without authorization.

Software (security functions)

- Keep the software up to date. Keep yourself informed regularly about safety updates for the product.
You can find information about this at Link: (<https://www.siemens.com/industrialsecurity>).
- Activate only protocols that you actually need to use the device.
- Limit access to the device using a firewall or rules in an access control list (ACL).
- The configuration files are available in XML format for simple use. Make sure that the configuration files outside the device are suitably protected. You can, for example, encrypt the files, store them at a safe location and transfer them only via secure communication channels.

Passwords

- Activate user management and create new user profiles.
- Change all default passwords for users before operating the device.
- Only use passwords with high password strength. Avoid weak passwords, e.g. password1, 123456789, abcdefgh.
- Define rules for using devices and assigning passwords.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems.
- Update passwords and keys regularly to improve security.

Keys and certificates

This section deals with the security keys and certificates that you need to set up SSL.

- We urgently recommend creating your own SSL certificates and making them available. Preset certificates and keys are present in the device.

The preset and automatically created SSL certificates are self-signed. We recommend using certificates signed either by a reliable external certification authority or an internal certification authority.

The device has an interface via which you can import certificates and keys.

- We recommend using certificates with a key length of at least 2048 bits.
- If protocols support both certificates and keys, you should favor certificates.
- The following certificate formats are supported for the import:

Certificate	Supported formats
HTTPS OPC UA server	*.p12 *.pfx *.pem ¹⁾ *.cer *.cert *.der
OPC UA client OPC UA CA OPC UA issuer	*.pem ¹⁾ *.cer *.cert *.der

¹⁾ May contain a private key.

- The following algorithms are supported for encryption:

Protocol	Supported signature algorithms	Supported key and size
Web browser	SHA1 SHA256 with RSA SHA384 with RSA SHA512 with RSA	RSA 2048 bit RSA 4096 bit
OPC UA	SHA256 with RSA SHA384 with RSA SHA512 with RSA	RSA 2048 bit RSA 4096 bit

- The following cipher suites are supported for HTTPS:

OpenSSL name	Value	Browser
ECDHE-RSA-AES128-GCM-SHA256	0x2F	Chrome, Firefox
ECDHE-RSA-AES256-GCM-SHA384	0x30	Chrome, Firefox
ECDHE-RSA-AES128-CBC-SHA256	0x27	Internet Explorer 11
ECDHE-RSA-AES256-CBC-SHA384	0x28	Internet Explorer 11

Firmware encryption

The firmware itself is signed and encrypted. This ensures that only authentic firmware can be downloaded to the device.

Secure/non-secure protocols

- Check whether it is necessary to use SNMPv1. SNMPv1 is classified as non-secure. Make use of the possibility to prevent write access. The product offers corresponding settings for this.
- If SNMP is activated, change the community names. If unrestricted access is not necessary, limit access via SNMP.
- Use secure protocols if access to the device is not protected by means of physical safeguards.

The following protocols provide secure alternatives:

HTTP → HTTPS

- To prevent unauthorized access to the device or network, set up appropriate safeguards against non-secure protocols.
- Enable only the services (protocols) that will actually be used on the device. The same applies to the installed interfaces/ports. Unused ports could be used to access the network downstream from the device.

List of available protocols

All available protocols and their ports that are used with SIMATIC RF18xC, RF18xCI are listed below.

Table 2- 1 List of available protocols

Service/ Protocol	Protocol/ Port number	Preset port status	Port status configurable	Port number configurable	Authentication	Encryption
DHCP	UDP/68	Open	✓	--	No	No
PROFINET	UDP/34964 UDP/49152- 65535	Open	✓	--	No	No
HTTP	TCP/80	Open	--	--	No	No
HTTPS	TCP/443	Open	--	--	Yes	Yes
NTP	UDP/123	Closed	✓	--	No	No
SNMP	UDP/161	Closed	✓	--	No	No
OPC UA	TCP/4840	Open	✓	✓	Yes (when configured)	Yes (when configured)
EtherNet/IP	TCP/44818 UDP/44818 UDP/2222	Open	✓	--	No	No
XML	TCP/10001	Open	✓	✓	No	No
XML	TCP/10002	Closed	✓	✓	No	No
XML	TCP/10003	Closed	✓	✓	No	No
XML	TCP/10004	Closed	✓	✓	No	No
Syslog	UDP/514	Open	✓	--	No	No

Explanation of the table:

- Authentication

Specifies whether authentication of the communication partner takes place.

- Encryption

Specifies whether the transfer is encrypted.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit

Link: (<https://www.siemens.com/industrialsecurity>)

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15247/pm>)

Description

3.1 Properties of the communications modules

Area of application

The SIMATIC RF185C, RF186C, RF188C, RF186CI and RF188CI communication modules are designed for use in all areas of automation. It covers all areas in which SIMATIC Ident RFID readers and optical readers are operated. Due to the large variety of interfaces - PROFINET, EtherNet/IP, OPC UA, and XML - the application can run at the field level on an S7/Rockwell controller, on a PC or at the IT level. This means diagnostic data, such as processed transponder data or log entries, can be transferred to higher-level systems via OPC UA or XML parallel to regular operation.



Figure 3-1 Communication modules SIMATIC RF185C, RF186C, RF188C as well as RF186CI and RF188CI

Due to the high degree of protection, mounting without a protective enclosure is possible directly near the RFID read points. The small mounting surface of the communication module facilitates installation in confined spaces.

Two connections each for Ethernet and power supply allow configuration in a line structure in addition to a star structure. The L-coded M12 connectors for the power supply allow a high feed-through current in a line structure. The SIMATIC RF18xCI communication modules have an additional I/O interface over which up to 8 inputs or outputs can be connected. In addition to the familiar configuration types via TIA Portal and GSDML, these communication modules also feature integrated Web Based Management (WBM), which enables devices to be set via a standard browser. The WBM supports you during commissioning, diagnostics and servicing. It also displays information about the connected readers and enables the reading/writing of transponder data.

3.1 Properties of the communications modules

You can find additional information on the various RFID devices and optical readers on the Internet on the "Siemens Industry Online Support (<https://support.industry.siemens.com/cs/ww/en/ps/14970/man>)" page.

Features

The following features characterize the RF18xC and RF18xCI communication modules:

Table 3- 1 Features of the communication modules

Features	RF185C	RF186C	RF188C	RF186CI	RF188CI
Number of connectable devices	1	2	4	2	4
Supported product families	RF200, RF300, RF1000, MV300, MV400, MV500				
Reader interfaces	RS422 Transfer speed: 19.2 ... 921.6 Kbaud				
I/O interface	--			✓	
Ethernet interface	2x M12, switch integrated Transmission speed: 100 Mbps				
Degree of protection	IP67				
Application protocols	PROFINET IO, EtherNet/IP, OPC UA, XML				
Configuration/ diagnostic options	STEP 7 (TIA Portal), GSDML, WBM (Web browser)				
Function blocks	Ident profile, FB 45, faceplate for PCS 7				
Supported SIMATIC controllers	S7-300, S7-400, S7-1200, S7-1500				
Supported third-party controllers	Source code of the Ident profile available. All controllers with PROFINET-, EtherNet/IP and IEC61131 programming are supported.				

NOTICE

IRT is not supported

Note that the communication modules do not support IRT (Isochronous Real Time). The communication modules can also not function as IRT conductors (e.g. in a bus structure).

The communication modules can be configured as clients in MRP rings. Network diagnostics via SNMP is supported by the communication modules.

NOTICE

Operation in VLANs

Note that the communication modules cannot be operated in VLANs whose ID is $\neq 0$.

3.2 I/O functions of the CI device versions

Unlike the C device versions, the CI device versions SIMATIC RF186CI and RF188CI have an I/O interface. You can use this interface either as a single digital input or output or for the connection of an IO-Link module (e.g. IO-Link module K20).

The I/O interface can, for example, also be used as an alternative to the digital inputs/outputs of the controller. One such application example is the configuration of automatisms that are triggered by an event or changed status, for example, by a transponder that was recognized. Unlike with the digital inputs/outputs of the S7 controller, the status is changed by the event that occurs and remains in this status until a new event occurs. Note that the reaction time of the digital outputs (and inputs) of the communication module depends on the CM load and is 50 - 100 ms on average.

If the I/O interface is used for connecting an IO-Link module, the CM can use up to 8 digital inputs/outputs of each of the modules. Only DI/DO modules with a maximum of 16 bits of cyclic process data are supported (input and output data). Note that the SIMATIC RF200 IO-Link Ident readers cannot be operated via SIMATIC RF186CI/RF188CI.

3.3 User-specific procedure

As described above, the communication modules are designed for different environments and requirements.

If you operate the communication modules in an automation environment, they are configured and programmed from the perspective of an S7 user. Integration in third-party controllers (e.g. Rockwell controllers) is, of course, also possible. In this case, the configuration, engineering, and programming is performed from the point of view of a Rockwell user. If you operate the communication modules in an OPC UA or XML environment, the configuration and programming are made from the perspective of an OPC UA or XML user.

If you want to adapt the communication modules to your requirements, we recommend the following user-specific procedure:

Procedure as S7 user



1. Connect the hardware

You can find information on this in the section "Connection (Page 27)".

2. Assign the IP address / device name

You can find information on this in the section "Assign the IP address / device name (Page 47)".

3. Configure communication module

You will find information on this in the section "Configuration via PROFINET IO (Page 52)" or "Configuring with the WBM (Page 61)".

4. Program reader commands

You can find information on this in the section "Programming via SIMATIC controller (Page 111)".

Procedure as an OPC UA user



1. Connect the hardware

You can find information on this in the section "Connection (Page 27)".

2. Assign the IP address / device name

You can find information on this in the section "Assigning the IP address / device name with SINEC PNI (Page 50)".

3. Configure the communication module

You can find information on this in the section "Configuring with the WBM (Page 61)".

4. Program reader commands

You can find information on this in the section "Programming via OPC UA (Page 115)".

Procedure as XML user



1. Connect the hardware

You can find information on this in the section "Connection (Page 27)".

2. Assign the IP address / device name

You can find information on this in the section "Assigning the IP address / device name with SINEC PNI (Page 50)".

3. Configure the communication module

You can find information on this in the section "Configuring with the WBM (Page 61)".

4. Program the reader commands

You can find information on this in the section "Programming via XML (Page 113)".

Procedure as Rockwell user



1. Connect the hardware

You can find information on this in the section "Connection (Page 27)".

2. Assign the IP address / device name

You can find information on this in the section "Assigning the IP address / device name with SINEC PNI (Page 50)" or "Assigning an IP address via DHCP (Page 51)".

3. Configure the communication module

You can find information on this in the section "Configuring with Studio 5000 Logix Designer (Page 60)" and "Configuring with the WBM (Page 61)".

4. Configure / program the reader commands

You can find information on this in the section "Programming via Rockwell controller (Page 143)".

Orientation in the document

Later in the document, these symbols will help your orientation and will show you whether the section is of interest to you or not. Only the sections with user-specific content, in other words, content that is interface-specific, contain these symbols. Sections without these symbols are general and relevant for all areas of application.

3.4 Design

The following figure shows the basic design of the RF18xC/RF18xCI.

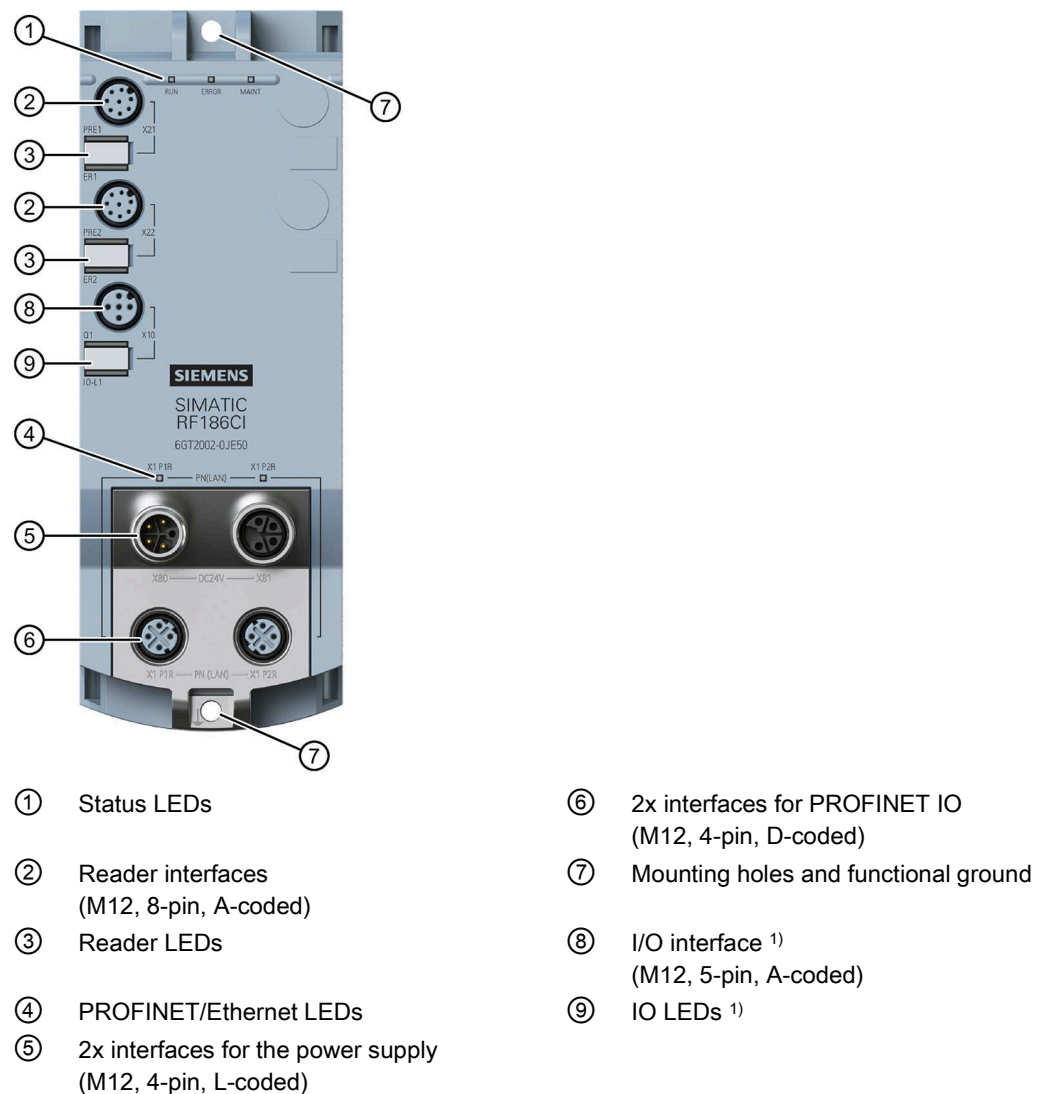


Figure 3-2 Design of the communication module

¹⁾ The I/O interface and I/O-LEDs are only a feature of the CI devices.

Integration

The following figure shows an example of an RF188C connection to an automation system.

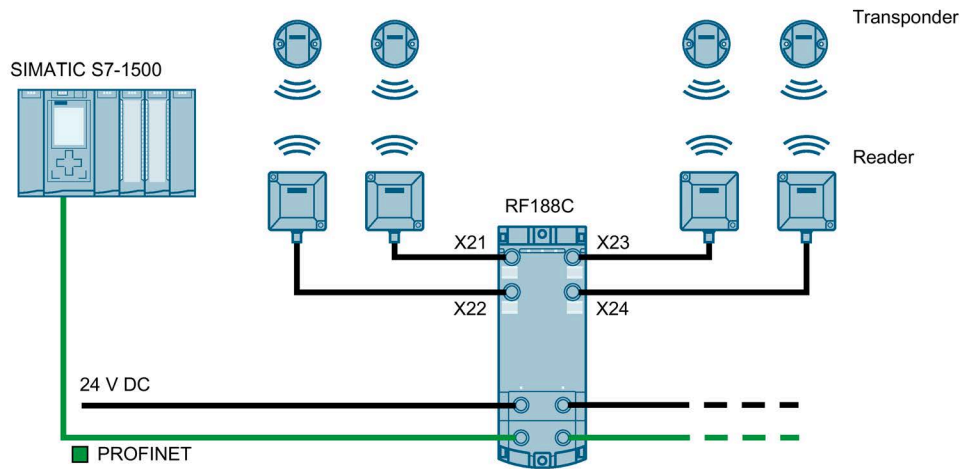


Figure 3-3 Configuration graphic RF188C

As of STEP 7 Basic / Professional V15.1, the RF18xC communication modules are integrated into the TIA Portal; as of STEP 7 Basic / Professional V16, the RF18xC communication modules are integrated into the TIA Portal. Integration into older STEP 7 versions and third-party systems is performed via a GSDML file. The communication module can then be configured via the TIA Portal or another engineering system. The GSDML file is stored on the communication module and can be downloaded from it using a Web browser. You can also find the GSDML file at the website of Siemens Industry Online Support.

Mounting

The RF18xC/RF18xCI communication modules are designed for easy installation.

NOTICE
Installation outdoors Please note that the communication module needs to be installed in a protected area. In the case of installation outdoors, make sure that the device is protected from direct sunlight, precipitation and wind.

4.1 Installation dimensions and position

The RF18xC/RF18xCI communication modules have the following installation dimensions (W × H × D): 60 × 165 × 45 mm.

You can mount the communication modules in any mounting position.

Minimum clearances

When installing the communication modules, keep a minimum distance of 1 cm from an adjacent device or another device.

Mounting rules

Note**Mounting the communication modules**

Only install the communication module when supply voltages are switched off.

You do not have to observe any special rules when installing the communication modules.

4.2 Mounting the communications module

Introduction

The communication modules are designed for mounting on a flat, solid surface. Alternatively, you can use the axially symmetrical drill holes of the modules to fasten them to an aluminum profile using sliding blocks.

Note

Functional ground

If a grounded metal mounting surface is used, the bottom mounting screw of the RF18xC/RF18xCI module already establishes a reliable grounding connection. This eliminates the need for a separate ground conductor. If you use the fixing screw as grounding connection, the thread of the fixing screw or the contact facing of the fastening nut on the base must be unpainted. This ensures a low-resistance connection.

Requirements

The following table shows and explains the types of screws you need to mount the modules.

Table 4- 1 Recommended screw types

Screw type	Description
Cylinder head screw M4 according to DIN EN ISO 1207 / DIN EN ISO 1580	The minimum screw length should be 35 mm. If you need washers, use washers conforming to DIN EN ISO 7089 / DIN EN ISO 7090.
Cylinder head screw with M4 hex socket according to DIN EN ISO 4762	

Fasten the communication module with the screws on a solid level surface. The device must be screwed (≤ 1.2 Nm) onto the panel at both fastening points (front top and bottom).

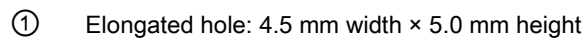


Figure 4-1 Installing RF18xC/RF18xCI communication module

Fastener for cable ties

All communication modules have integrated fastening points for cable ties. The fastening points are located at all four corners of the modules.

The following figure shows the upper left fastening point for 2.5 mm wide cable ties.

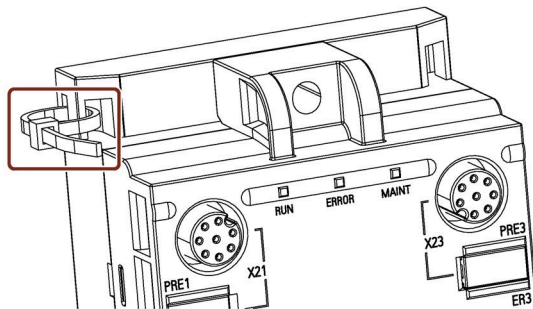


Figure 4-2 Fastening the RF18xC/RF18xCI communication module with cable ties

4.3 Use at altitudes over 2,000 m

The RF18xC/RF18xCI communication modules can be used at altitudes > 2,000 m. See the following information and restrictions in this regard.

Restrictions of the maximum specified ambient temperature

Table 4- 2 Restrictions of the maximum specified ambient temperature with regard to the altitude

Altitude	Derating factor	Max. permissible ambient temperature
-1000 ... 2000 m	1.0	55 °C
2000 ... 3000 m	0.9	49 °C
3000 ... 4000 m	0.8	44 °C
4000 ... 5000 m	0.7	38 °C

The standard IEC 61131-2:2017 forms the basis for the derating factor and the calculated maximum permissible ambient temperature.

A linear interpolation between altitudes is permissible. The derating factors compensate for the reduced cooling effect of air at higher altitudes due to the reduced density.

Note

Suitability of the power supply

Make sure that the power supply units you use are also suitable for altitudes > 2,000 m.

Effects on the module availability

When the module is operated at altitudes above 2,000 m, the stronger cosmic radiation starts having an effect on the error rate of electronic components (so-called Soft Error Rate). In rare cases this may result in the module entering the safe state; this is especially true for safety modules. However, the functional safety of the module remains completely unaffected.

Currently valid markings and approvals

Note**Information on the nameplate**

You will find the currently valid markings and approvals on the nameplate of the communication module. All other markings and approvals are currently based on an altitude up to 2,000 m.

Connection

Proper use

Only use the device for its intended purpose. If unspecified devices are connected to the RF18xC/RF18xCI, the connected device may be destroyed.

PROFINET IO connection system

You can find detailed information on connecting the RF18xC/RF18xCI on PROFINET IO in the "SIMATIC PROFINET system description (<https://support.industry.siemens.com/cs/ww/en/view/19292127>)".

CAUTION

Power supply for devices with PROFINET interfaces

Modules with PROFINET interfaces may only be operated in LANs (Local Area Networks) in which all connected devices are equipped with SELV/PELV power supplies (or have equivalent protection).

A data transfer terminal (modem, for example) is required to access the WAN (Wide Area Network) in order to ensure compliance with this safety standard.

All supply and signal voltages must be safety extra low voltage (SELV/PELV according to IEC 61140).

Reader connector system

A reader always occupies one M12 socket on the RF18xC/RF18xCI. You can connect the reader to the communication module using a preassembled cable. The connection cable is available in lengths of 2, 5, 10, 20 and 50 m as standard. If necessary, these can be extended.

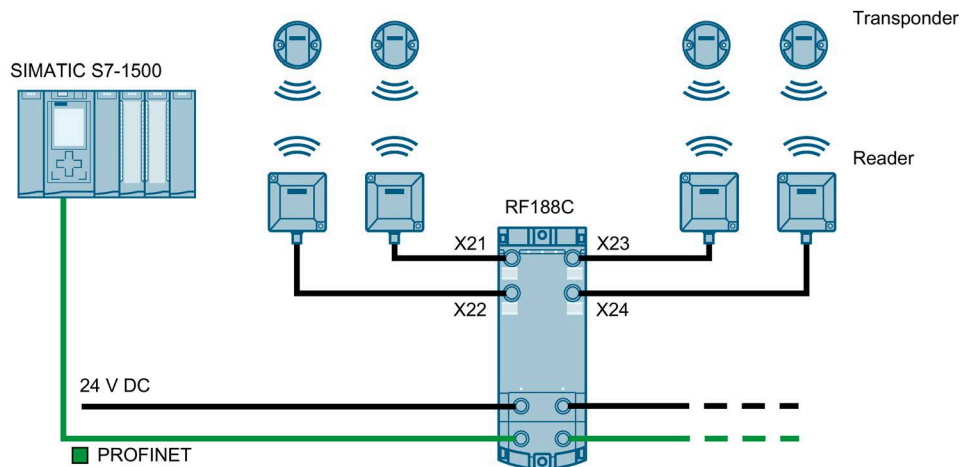


Figure 5-1 Overview of connections

5.1 Network topology

The communication network can be designed as line/series, star or ring topology. Also, note the information in the section "Supply voltage and PROFINET IO loop-through (Page 45)".

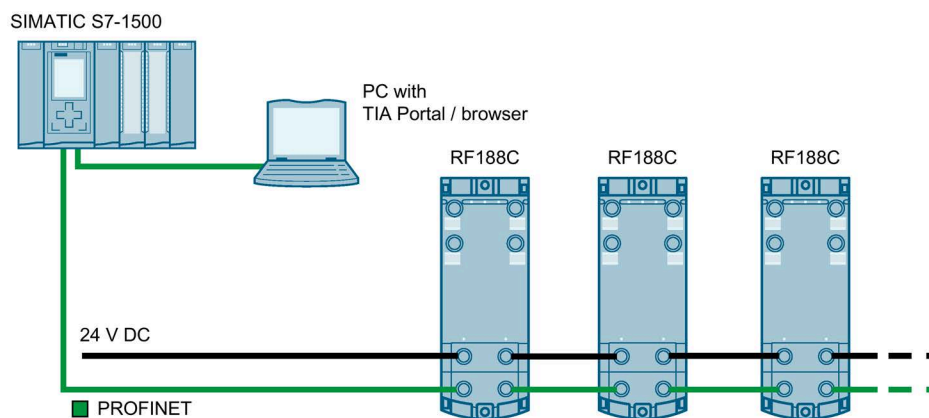


Figure 5-2 Configuration graphic of a line/series topology

With a line/series topology, remember that if the communication connection of a communication module to the controller is interrupted, the communication connection to all downstream communication modules is also interrupted.

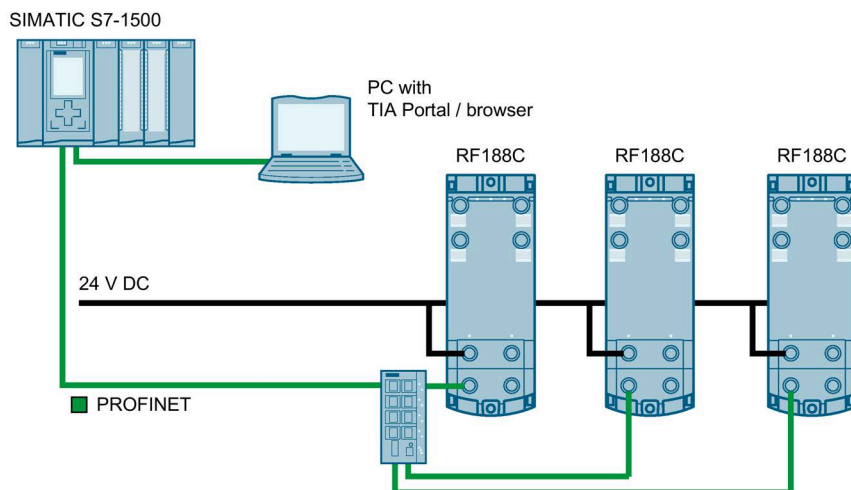


Figure 5-3 Configuration graphic of a star topology

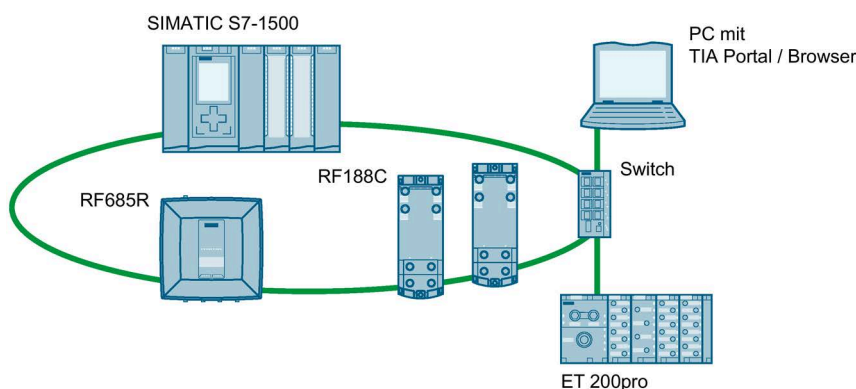


Figure 5-4 Configuration graphic of a ring topology

Media redundancy

Media redundancy is a function that ensures network and system availability. Redundant transmission links in the MRP topology ensure that an alternative communication path is made available if a transmission link fails. To make this possible you need to configure the communication modules as a client of the Media Redundancy Protocol (MRP) in STEP 7 (Basic / Professional).

MRP is part of PROFINET standardization according to IEC 61158.

Setup of an MRP ring topology

To set up an MRP ring topology with media redundancy, you must join both free ends of a line topology in the same device. The closing of the line topology to form a ring is via two network ports of one of the devices (ring ports). The communication modules can be integrated as clients in an MRP ring topology via the network ports "X1P1R" and "X1P2R".

You will find additional information on setting up an MRP ring topology in the STEP 7 online help and in the "SIMATIC PROFINET system description (<https://support.industry.siemens.com/cs/ww/en/view/19292127>)".

5.2 Operation of the CM on grounded/ungrounded power supply

Below, you can find information on the overall configuration of an RF18xC/RF18xCI communication module on a grounded power supply (TN-S network). The specific subjects discussed here are:

- Supply voltages of the communication module
- Disconnecting devices, short-circuit and overload protection according to IEC 60364 (corresponds to DIN VDE 0100) and IEC 60204 (corresponds to DIN VDE 0113)
- Load voltage supplies and load circuits

Grounded power supply

For grounded power supplies, the neutral conductor of the supply system is grounded. A short-circuit to ground of a live conductor, or of a grounded part of the system, trips the protective devices.

Supply voltages

Two supply voltages are available for the communication module:

- 1L+: Power supply
- 2L+: Load voltage

Note that the power supply (1L+) supplies the communication module and the readers with power. The load voltage (2L+) has no direct effect on the RF18xC communication modules. For RF18xCI, the actuators and connected IO-Link devices (connectors with Class B assignment) are supplied with power over the load voltage (2L+). If the load voltage (2L+) is not connected, the channel fault LED (IO-L1) is continuously lit in red. This voltage is looped through to further consumers via the L-coded plug-in connectors.

Safe electrical isolation (SELV/PELV according to IEC 61140)

Power supply units/power supply modules with safe electrical isolation are required for operation of the communication module. This protection is referred to as SELV (Safety Extra Low Voltage) / PELV (Protective Extra Low Voltage) according to IEC 61140.

Setting up RF18xC/RF18xCI with grounded reference potential

When the communication module is set up with grounded reference potential, any interference currents that occur are diverted to functional ground. The connections must be connected externally (connection between 1M and FE).

Setting up RF18xC/RF18xCI with ungrounded reference potential

When the communication module is set up with ungrounded reference potential, any interference currents occurring are conducted to functional ground via an internal RC network (no external connection between 1M and FE).

RF18xC/RF18xCI in total configuration

The following figure shows the communication module in its overall electrical design.

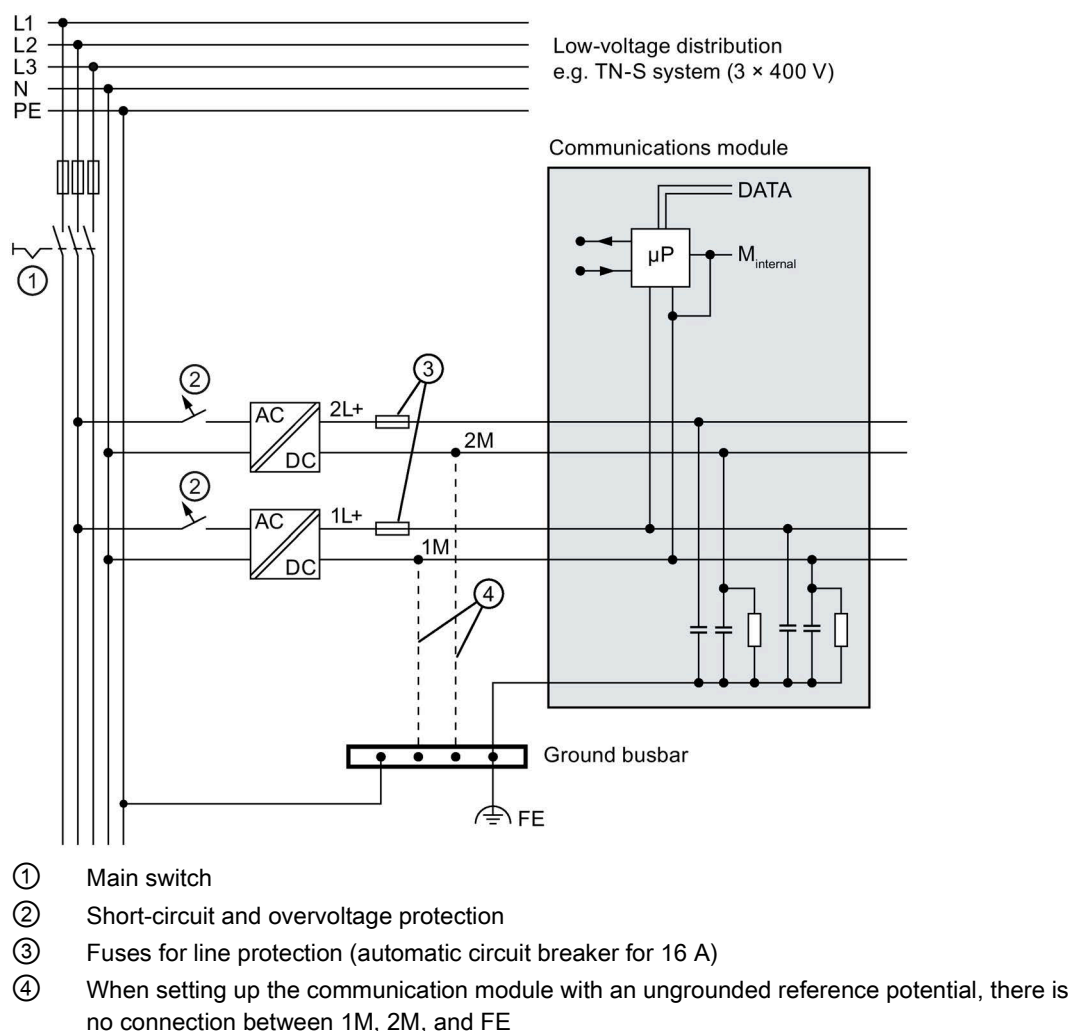


Figure 5-5 Electrical design

Components and protective measures

Various components and protective measures are prescribed for plant installations. The types of components and the degree to which the protective measures are mandatory depend on the IEC regulation that applies to your plant setup.

The following table shows the components of the electrical design with reference to the previous figure and compares the IEC regulations.

Table 5- 1 Components of the electrical design

Screen number	Components	IEC 60364	IEC 60204
①	Disconnecting device for controller, sensors, and actuators	Main switch	Disconnecter
②	Short-circuit and overload protection	Single-pole protection of circuits. Protect all power supply lines with a 24 V DC / 16 A circuit breaker.	Single-pole protection must be used for a grounded secondary circuit.
③	Circuit breaker	Protection of cables and lines against overcurrent	--

Insulation monitoring

Isolation monitoring must be provided in the following cases:

- Design of the communication module with an ungrounded reference potential
- If hazardous plant states can be expected as a result of faults.

5.3 Electrical design of the CM

Electrical isolation

In the electrical design of the communication module, electrical isolation is provided between:

- Load voltage 2L+ and all other circuit components
- Communication interfaces (PROFINET) of the communication module and all other circuit components

The following figure shows the potential relationships of the communication modules.

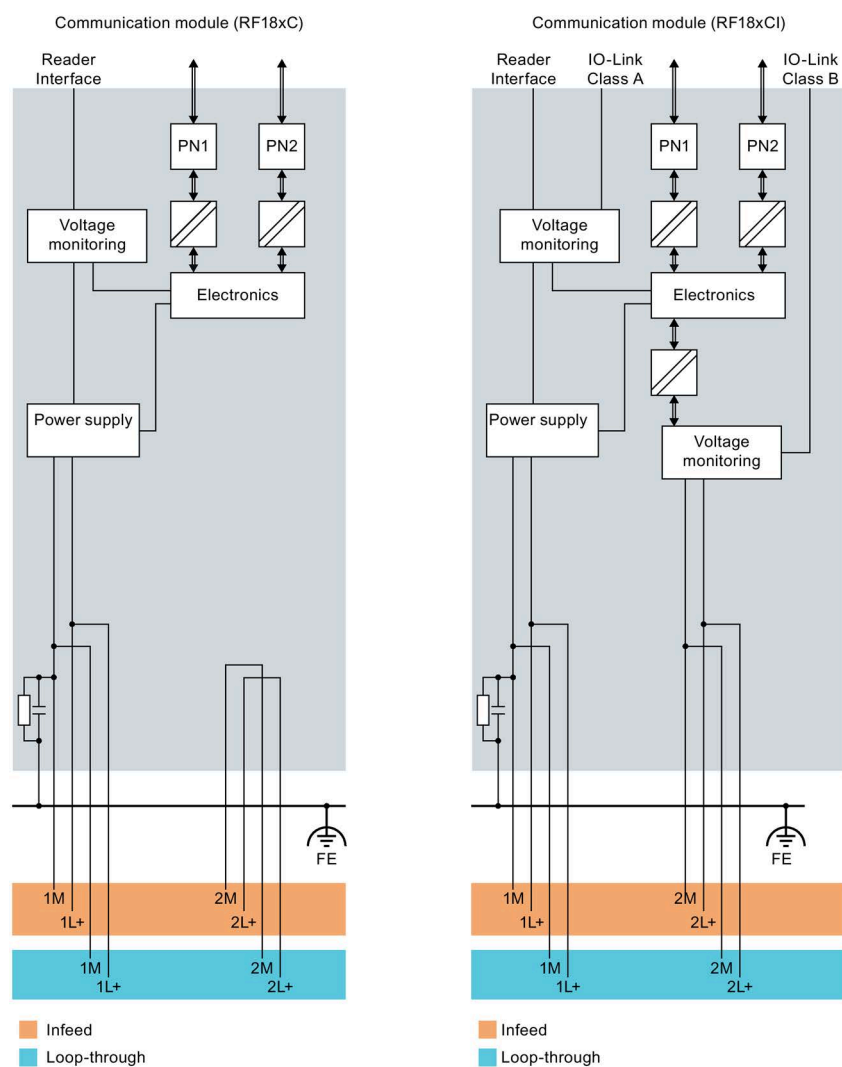


Figure 5-6 Potential relationships of the communication modules

Circuit breaker

According to IEC 60364, line protection is required, i.e. the supply lines must always be protected externally.

All supply voltages must be protected with a UL/IEC approved fuse 24 V DC / 16 A (tripping characteristic type B or C). At ambient temperatures of 40 °C to 55 °C, the power supplies must be protected with a UL/IEC approved fuse 24 V DC / 12 A.

Power supply of the assembly

Two voltage groups are available for the communication module, 1L+ (supply voltage) and 2L+ (load voltage).

Another power supply may be required in order to supply all communication modules of an assembly with the required voltage. Another voltage supply of 1L+ and 2L+ may be needed to form different potential groups, or because the voltage is insufficient for all communication modules due to the voltage drop. Create a power budget for the selection of the supply point of the voltage.

Note

Switching 1L+ and 2L+ on and off

Note that the power supply (1L+) supplies the communication module and the readers with power. The load voltage (2L+) has no direct effect on the RF18xC communication modules. For RF18xC, the actuators and connected IO-Link devices (connectors with Class B assignment) are supplied with power over the load voltage (2L+). If the load voltage (2L+) is not connected, the channel fault LED (IO-L1) is continuously lit in red. This voltage is looped through to further consumers via the I/O interface.

The following figure shows a configuration with another voltage supply for the communication modules. The different potential groups are highlighted in gray.

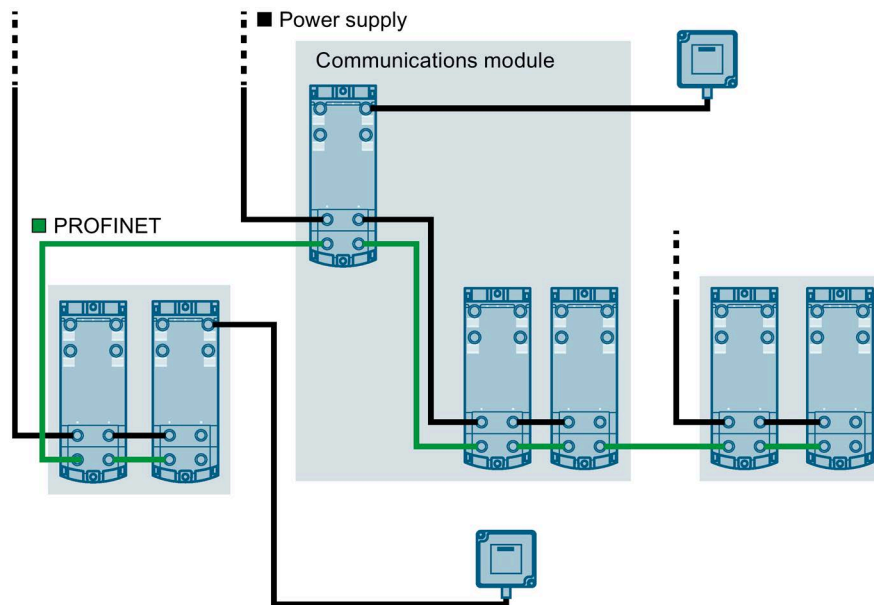


Figure 5-7 Wiring of the power supply

5.4 Connecting CM to functional ground

You need to connect the RF18xC/RF18xCI communication module to functional ground. For this purpose, a grounding screw for one ground conductor is provided on the communication module.

If a grounded metal mounting surface is used, the bottom mounting screw of the RF18xC/RF18xCI module already establishes a reliable ground connection. This eliminates the need for a separate ground conductor.

This connection to functional ground is also required to discharge any interference currents to ground and for EMI resistance.

Protection against external electrical influences

Below is a description of what you must pay attention to in terms of protection against electrical impacts and/or faults:

- In all plants or systems in which the communication module is installed, you must ensure that the plant or the system for dissipating electromagnetic interference is connected to functional ground.
- For supply, signal and bus lines, you must ensure that the laying of the lines and the installation is correct.
- For signal and bus lines, you must ensure that a wire/cable breakage or a cross-circuit does not lead to undefined states of the plant or system.

5.4.1 Mounting the CM on a conductive base

Requirement

Conductive base for mounting the module.

Required tools

You need the following tool to connect to the functional ground:

- Screwdriver

Accessories required

You need the following accessories to connect to the functional ground:

- Fastening screw (M4) and washer

Mounting

Proceed as follows to connect the communications module to functional ground via a conductive mounting base:

1. Drill 2 mounting holes with a distance of 155.6 mm.
2. Screw the module together with the M4 fastening screws with a torque of 1.2 Nm.

NOTICE

Grounding with a conductive mounting base

If you fasten the communications module to a conductive, grounded base, the lower fastening screw provides a conductive connection to the ground potential.

Ensure there is a low-impedance connection between the communications module and the conductive base and between the conductive base and functional ground.

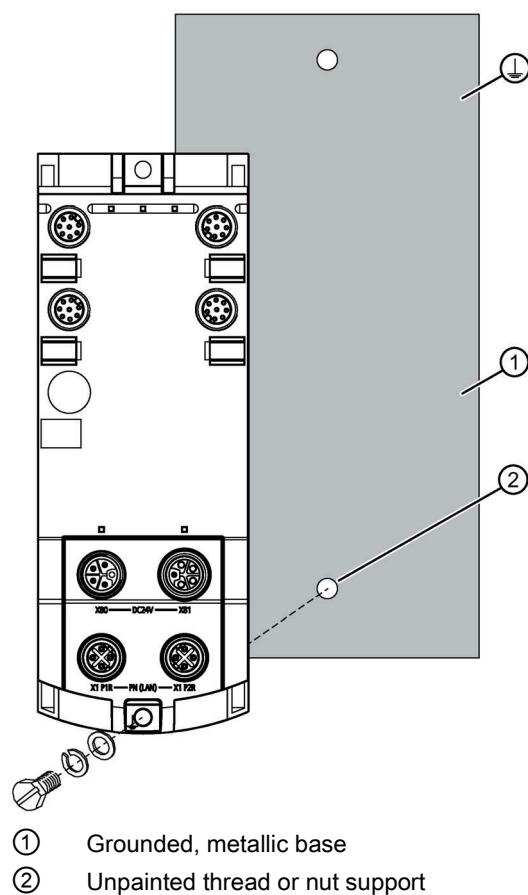


Figure 5-8 Mounting the CM on a conductive base

5.4.2 Mounting the CM on a non-conductive base

Requirement

Non-conductive base for mounting the module.

Required tools

You need the following tools to connect to the functional ground:

- Screwdriver
- Stripping tool
- Crimp tool

Accessories required

To connect to functional ground with a non-conductive mounting base, you can need the following accessories:

- Fastening screw (M4) and washer
- Cable lug suitable for M4 screws
- Ground conductor cable (copper braid) with a minimum cross-section of 4 mm²

Mounting

Proceed as follows to connect the communications module to functional ground via a ground conductor:

1. Drill 2 mounting holes with a distance of 155.6 mm.
2. Insulate the ground conductor.
3. Attach the cable lug to the ground conductor.
4. Screw the module and the cable lug together with the M4 fastening screws with a torque of 1.2 Nm.

NOTICE

Grounding with non-conductive mounting base

Ensure a low impedance connection between the communications module and functional ground.

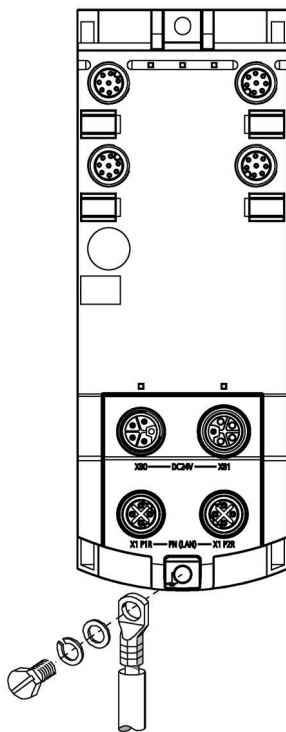
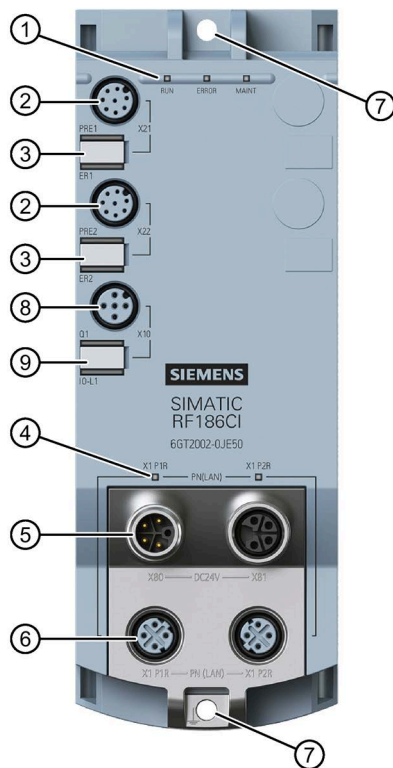


Figure 5-9 Mounting the CM on a non-conductive base / connection to functional ground

5.5 Connecting the communications module

Interfaces



- | | |
|---------------------------------------------------------------------------|----------------------------------------------------------------------------|
| ① Status LEDs | ⑥ 2x interfaces for PROFINET IO
X1 P1R, X1 P2R
(M12, 4-pin, D-coded) |
| ② Reader interfaces
X21-X24
(M12, 8-pin, A-coded) | ⑦ Mounting holes and functional ground |
| ③ Reader LEDs | ⑧ I/O interface ¹⁾
X10
(M12, 5-pin, A-coded) |
| ④ PROFINET/Ethernet LEDs | ⑨ IO LEDs ¹⁾ |
| ⑤ 2x interfaces for the power supply
X80, X81
(M12, 4-pin, L-coded) | |

Figure 5-10 Design of the communication module

¹⁾ The I/O interface and the associated LEDs are only a feature of the CI devices.

You can loop the supply voltages and PROFINET IO via the M12 round sockets ⑤ + ⑥.

The pin assignments of the various interfaces are lasered on the side of each communication module at the factory.

Requirement

Only wire the communication module when the supply voltage is switched off.

Required tools

When using preassembled cables, you need the following tool:

- Torque wrench set (e.g. from Peres; M12/M8, can be set; PER091) for wiring the reader connections

Note

Using preassembled cables

When connecting the supply voltage, we recommend the cables specified in the section "Ordering data (Page 196)" (4 x 1.5 mm² preassembled).

If you want to make the cable yourself, ensure that the conductor cross-section matches the system setup or the corresponding protection (1.5 mm²).

When using cables that are not preassembled, you need the tool for the specific cable/connector, for example, an insulation stripper, screwdriver or Allen wrench.

Accessories required

You need the following accessories:

- for the reader connection
M12 plug (8-pin, A-coded) and 6-wire cable (6 x 24 AWG)
- for connecting digital inputs/outputs
M12 plug (3-pin, A-coded) and 3-wire cable (3 x 22 AWG) or
M12 plug (5-pin, A-coded) and 5-wire cable (5 x 22 AWG)
- for connecting the power supply
M12 plug (4-pin, L-coded) and 4-wire cable (4 x 1.5 mm²)
- for PROFINET IO connection
M12 plug (4-pin, D-coded) and 4-wire Ethernet cable (Twisted Pair, shielded)

You can find the associated article numbers in the section "Ordering data (Page 196)".

Wiring interfaces/connectors

The following tables show the pin assignment for the interfaces/connectors.

Table 5- 2 Pin assignment PROFINET IO; M12 socket (4-pin, D-coded)

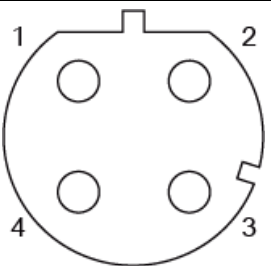
Pin	Assignment	View of M12 socket, 4-pin
1	Data line TxP	
2	Data line RxP	
3	Data line TxN	
4	Data line RxN	

Table 5- 3 Pin assignment power supply; M12 socket (4-pin, L-coded)

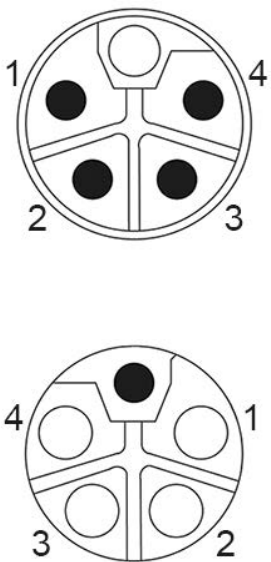
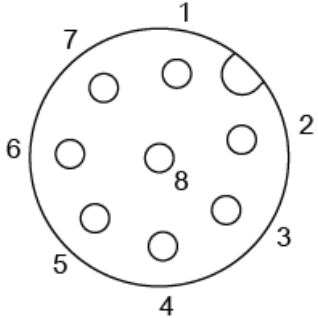
Pin	Assignment	View of M12 socket, 4-pin
1	L1: +24 V (brown)	
2	N2: 0 V load supply (white) Relevant for RF18xC1 devices	
3	N1: 0 V (blue)	
4	L2: +24 V (black)	

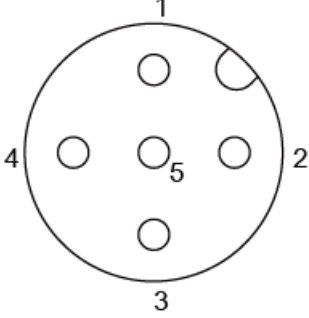
Table 5- 4 Pin assignment reader interface; M12 socket (8-pin, A-coded)

Pin	Assignment		View of M12 socket, 8-pin
	RS422	RS232	
1	+24 V	+24 V	
2	-RxD	--	
3	0 V	0 V	
4	+RxD	RxD	
5	+TxD	+5 V	
6	-TxD	--	
7	--	TxD	
8	Functional ground / shielding	Functional ground / shielding	

I/O interface (RF18xCi)

Note that a single input, a single output or an IO-Link module (e.g. IO-Link module K20) can be connected to the I/O interface.

Table 5- 5 Pin assignment I/O interface; M12 socket (5-pin, A-coded)

Pin	Assignment	View of M12 socket, 5-pin
1	1L+: +24 V, IO-Link	
2	2L+: +24 V, for IO-Link module Class B	
3	1N: GND, IO-Link	
4	C/Q: Data cable for <ul style="list-style-type: none"> IO-Link a single digital input a single digital output 	
5	2N: GND, for IO-Link module Class B	

Connect the plug

Proceed as follows to connect the device:

1. Push the respective plug into the corresponding round socket on the communication module.

Ensure that the correct stop is provided between the connector and bush (groove and spring).

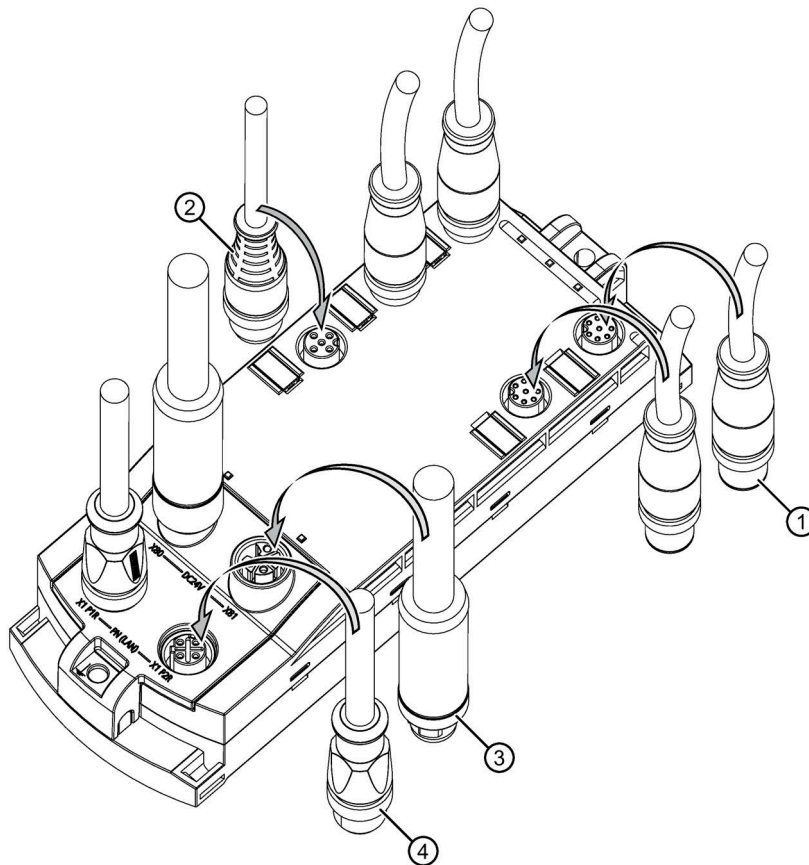
2. Fasten the connector by tightening the knurled locking ring.

To guarantee the degree of protection, you must fasten all connectors with ≈ 1.0 Nm.

NOTICE

Ensuring the degree of protection

You need to close all unused sockets with M12 sealing caps to ensure IP65 or IP67 degree of protection. You can find the order data of the sealing caps in the section "Ordering data (Page 196)".



- ① Connector for the reader connection (M12, 8-pin, A-coded)
- ② Connector for connecting digital inputs/outputs (M12, 5-pin, A-coded)
- ③ Connector for the power supply (M12, 4-pin, L-coded)
- ④ Connector for PROFINET IO connection (M12, 4-pin, D-coded)

Figure 5-11 Connect the plug

5.6 Supply voltage and PROFINET IO loop-through

The RF18xC/RF18xCI communication modules each have two M12 connectors for the supply voltage and PROFINET IO. Supply takes place via the 1st connection, the supply voltage and PROFINET IO can be forwarded to another device via the 2nd connection.

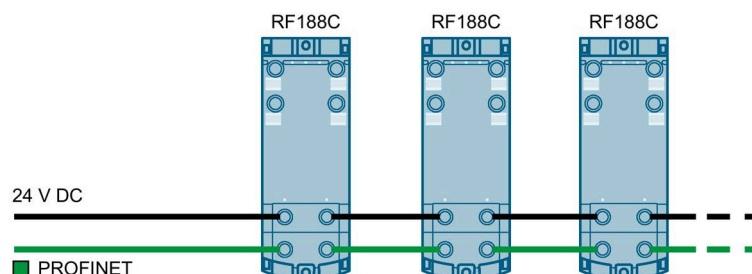


Figure 5-12 Supply voltage and PROFINET IO loop-through

Notes for wiring

- When wiring your assembly, you need to take into account the effect of the cable length on the supply voltage at the RF18xC/RF18xCI.
- The maximum supply current of the communication module is 16 A at 1L+ and 2L+ for a maximum ambient temperature of 40 °C. At ambient temperatures of 40 °C to 55 °C, the maximum supply current is 12 A. These values must not be exceeded. Take note of the derating factor when operating at elevations above 2000 m (Page 24).
- Adhere to the current carrying capacity of the connected cables, which depends on the conductor material, the conductor cross-section and the ambient temperature.

NOTICE

Damages by using power supply cables that are not permitted

Only use power supply cables that have been approved for the operation of the device. In case of cables you have assembled yourself or third-party products, make sure that the cable cross-section is at least 1.5 mm².

If you do not observe the maximum permissible supply current and the cable cross-section required, this may result in the cable isolation and contacts overheating and in the device being damaged.

5.7 Effect of cable length on the supply voltage

When wiring your assembly, you need to take into account the effect of the cable length on the supply voltage of the communication module.

The following figure shows the voltage drop as a function of the cable length for 2, 4, 8 and 16 amperes, using the example of a copper cable with $\varnothing 1.5 \text{ mm}^2$. A simple copper line is used as an example. Depending on the design, the power supply line and the ground line must be taken into account.

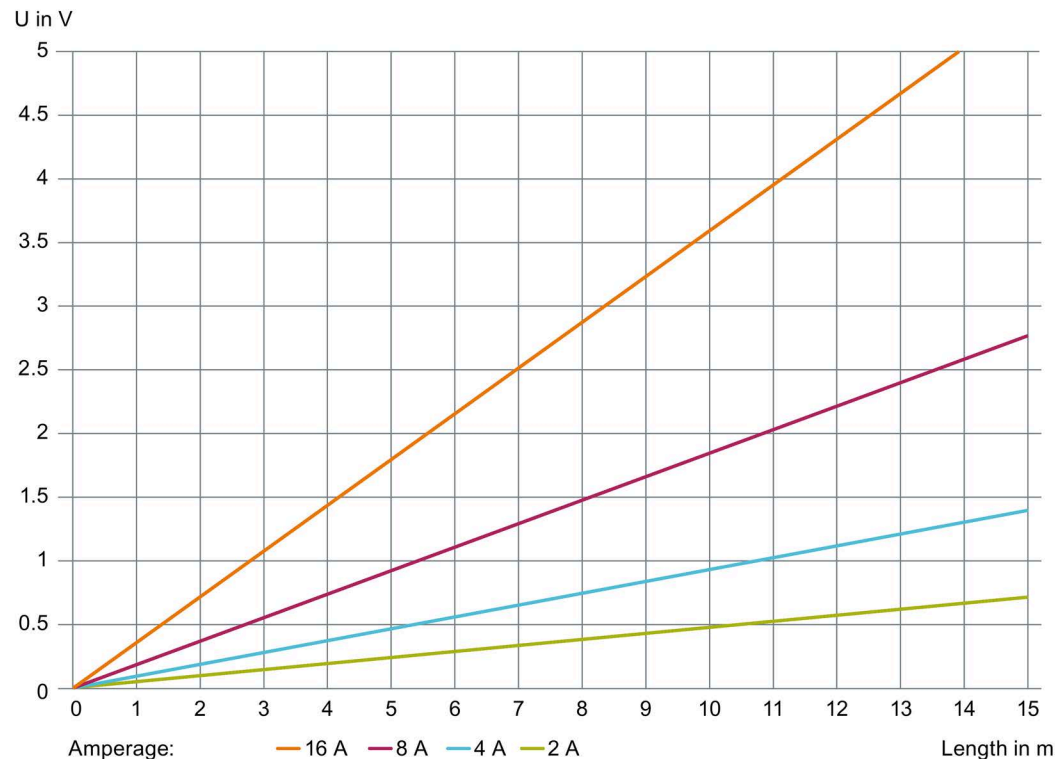


Figure 5-13 Voltage drop with copper cables with a cross-section of 1.5 mm^2

To estimate the voltage drop in your communication module, you must add the voltage drops of the cables.

Example

With 16 A the voltage drop via the two L-coded M12 plug-in connectors and in the communication module is approximately 0.2 V. The value can vary significantly depending on the plug connection or condition.

When using a 7 m power cable with $\varnothing 1.5 \text{ mm}^2$, the voltage drop is approx. 2.6 V with a 16 A load.

Configuring

Synchronize device time

Note that the time of the device clock corresponds to UTC time and cannot be adjusted to time zones. It is recommended to synchronize the time with an NTP server to obtain unique time information. The time is reset with a device restart and must be synchronized.

6.1 Assign the IP address / device name

To ensure functioning communication between the controller and the communication module, you must assign unique IP addresses or device names to the individual communication modules. Depending on the infrastructure in which you want to operate the communication module, the following different procedures are available:

- Operate the communication module as an S7 user in an automation environment.
The unique assignment is made via the device name using the TIA Portal (from STEP 7 Basic / Professional V15).
- Operate the communication module as XML or OPC UA user in an IT environment.
The unique assignment is based on DHCP or the IP address using SINEC PNI.
- Operate the communication module as a Rockwell user (EtherNet/IP) in an automation environment.
The unique assignment is made with the IP address using a DHCP server.

Each communication module receives a unique device identification (MAC address) at the factory.

6.1.1 Assigning the IP address / device name with STEP 7

Requirements



STEP 7 Basic / Professional is installed, the communications module is connected and has started up.

Procedure

Proceed as follows to assign a unique device name to the communications module:

1. Open the TIA Portal with "Start > All Programs > Siemens Automation > TIA Portal Vxx".
2. Create a new project.
3. Change to the Project view.

4. Using the project tree, insert a SIMATIC controller in the project with the "Add new device" menu command.

Reaction: The device view opens and the controller is displayed.

5. Go to the network view and drag the communications module from the hardware catalog into the project.
6. Assign the communications module to the controller.
7. Right-click on the communications module.
8. In the shortcut menu, select the menu command "Assign device name".

Reaction: The "Assign PROFINET device name" window opens.

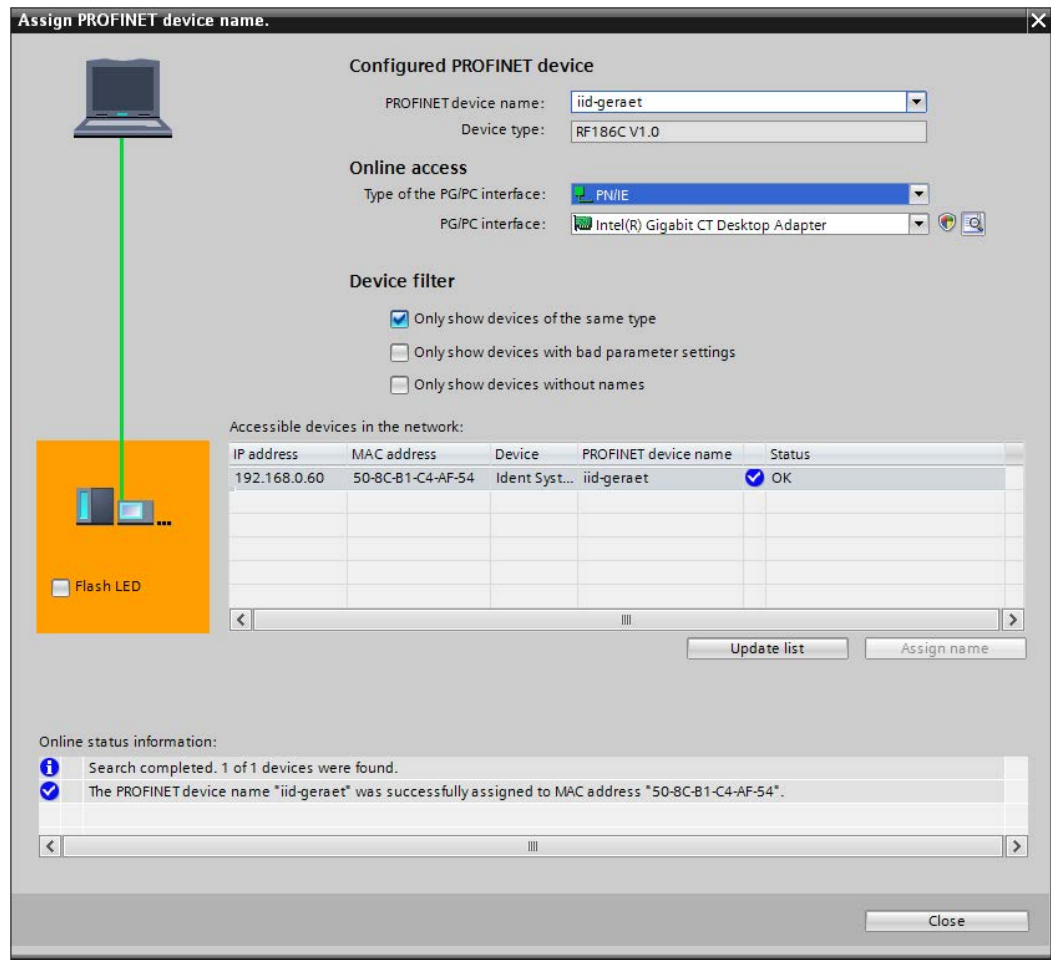


Figure 6-1 Assign device name

9. Select the connection type in the "Online access" area in the "Type of the PG/PC interface" drop-down list.
10. In the "PG/PC interface" drop-down list in the "Online access" area, select the network adapter via which the communications module is connected to the PG/PC.
11. Click the "Update list" button to display all reachable devices in the network.

12. Select the required node from the list.

13. Now click the "Assign Name" button to assign the PROFINET device name to the communications module.

Result: The configured PROFINET device name from the project is assigned to the communications module.

Note**Assigning a device name when replacing a module**

When you replace a module, you can assign the device names automatically. You will find more information on this in the section "Module replacement (Page 174)".

Device flash test using the TIA Portal

If several IO devices are connected to the controller, it is possible to make the LEDs of the device flash. In this case, compare the MAC address of the device with the MAC address displayed and then select the desired IO device. With the help of the device flash test you can quickly and easily identify the desired IO device.

Proceed as follows to identify the relevant IO device using the flashing test:

1. In the project tree, select the menu command "Online access > Your online access > Update accessible devices".

The available devices are displayed.

2. Select the required RF18xC/RF18xCI and click the entry "Online & Diagnostics" in the folder of the selected device.
3. Select the option "Functions > Assign name".
4. Click the "Flash LED" button.

Reaction: The LEDs on the selected communications module flash.

5. Click the "Flash LED" button again to stop the flashing.

6.1.2 Assigning the IP address / device name with SINEC PNI

Requirements



SINEC PNI is installed and the communication module is connected and running. You can find the SINEC PNI on the pages of the "Siemens Industry Online Support (<https://support.industry.siemens.com/cs/ww/en/ps/26672/dl>)".

Procedure



Proceed as follows to assign a new, unique IP address and a unique device name to the communication module:

1. Start SINEC PNI.
2. In the "Settings" menu, select the "network adapter" via which the communication module is connected to the PC.
3. Make sure that the "Scan protocol > PROFINET devices" is selected.

Note: Note that the function "Fetch additional information" can take some time when the network includes many devices.

4. Click on the "Save" button.
5. Switch to the "Device list" menu.
6. Click on the "Start network scan" button on the toolbar.

Reaction: The network is scanned for connected devices and all recognized devices are displayed in the device list.

7. Select the desired communication module in the device list.
8. Click on the "Configure device" button on the toolbar.

Reaction: The "Device configuration" window opens.

9. Enter a new, unique IP address for the communication module in the "IP address" input box.
10. Enter the subnet mask of your network in the "Subnet mask" input box.
11. Switch to the "PROFINET" tab.
12. Enter a device name in the "PROFINET device name" input box.
13. Click the "Load" icon to transfer the settings to the communication module.

Result: The communication module is assigned the new IP address, subnet mask, and a new device name.

Device flash test using SINEC PNI

If several communication modules are connected to the network/PC, it is possible to make the LEDs of the device flash. Using the device flash test, you can identify the required communication module quickly and simply.

Proceed as follows to identify the relevant communication module using the flash test:

1. Select the desired module from the device list in the "Device list" menu.
2. Click on the "Flash LED" button on the toolbar.

Reaction: The LEDs on the selected communication module flash.

3. Click the "Stop" button to stop the flashing.

6.1.3 Assigning an IP address via DHCP

This section is intended for all user types but primarily for Rockwell users.

In Rockwell controllers, the IP address is assigned with the aid of a DHCP server. The communication module functions as a DHCP client in this case. To assign the communication module an IP address via DHCP, a DHCP server must be configured in the same subnet. Rockwell Automation™ makes a BOOTP / DHCP server for Windows available to assign IP address data to the MAC address of the reader.

Requirement

Studio 5000 Logix Designer and a current version of the BOOTP / DHCP server are installed, the communication module is linked in and the communication module is connected and has started up. The BOOTP / DHCP server is preconfigured and is available.

You will find further information on linking the communication module into Studio 5000 Logix Designer in the section "Configuring with Studio 5000 Logix Designer (Page 60)".

Procedure



Proceed as follows to assign a unique device name to the communication module:

1. Call up the BOOTP / DHCP server.
2. Click on the menu command "Tools > Network Settings".
The input screen "Network Settings" is opened.
3. Enter the subnet mask of the server in the input box "Subnet Mask".
4. Enter the gateway of the server in the input box "Gateway".
5. Confirm your entry with "OK".
6. Double click on an entry in the "Request History" area.
The input screen "New Entry" opens.
7. In the input box "IP Address" enter a new unique IP address.

8. Confirm your entry with "OK".

The entry was assigned the IP address in the "Request History" area.

The entry is also displayed in the "Relation List" area.

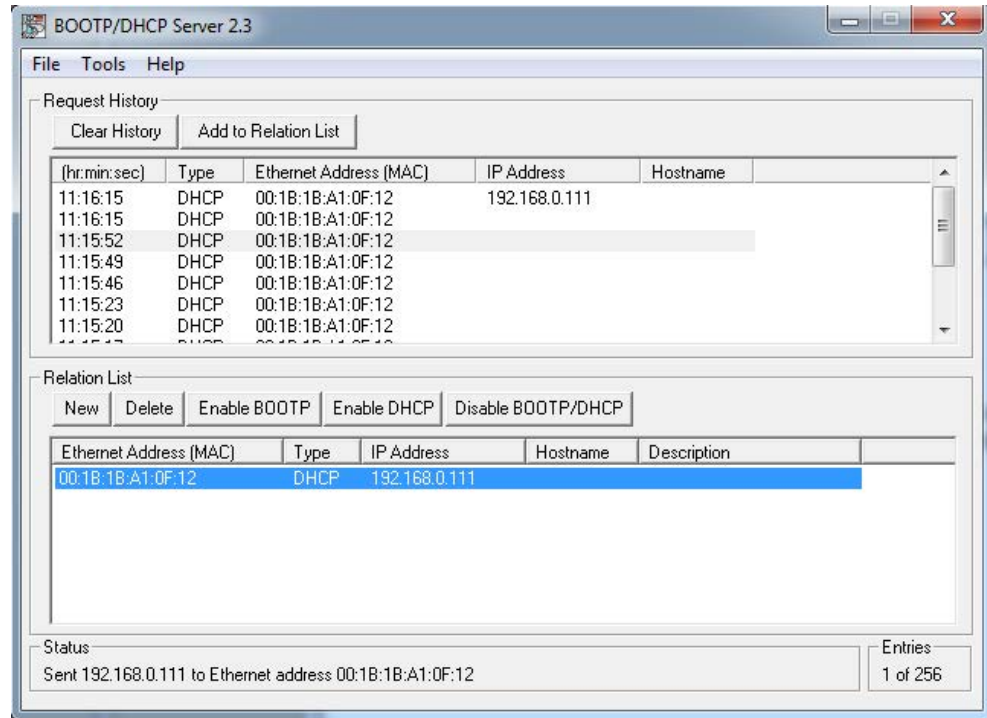


Figure 6-2 BOOTP / DHCP server software

9. Click the "Disable BOOTP/DHCP" button to save the IP address on the communication module.

Result: The communication module is assigned the IP address statically.

6.2

Configuration via PROFINET IO



As of STEP 7 Basic / Professional V15.1, the RF18xC communication modules are integrated into the TIA Portal; as of STEP 7 Basic / Professional V16, the RF18xC communication modules are integrated into the TIA Portal and can be linked to SIMATIC automation systems. Integration into older STEP 7 versions is performed via a GSDML file. The connection is made via PROFINET, the configuration via the TIA Portal and operation of the communication module via the Ident blocks of the TIA Portal. You can further configure the communication modules using WBM.

The GSDML file corresponding to the communication module is stored on the communication module and can be downloaded from it via WBM. You can also find the GSDML file at the website of Siemens Industry Online Support.

Requirements

STEP 7 Basic / Professional is installed and started, and a project is open. The communication module is connected to the controller or PC via Industrial Ethernet or PROFINET and has been powered up.

The communication module has a valid IO device name.

Procedure

Follow these steps to configure the communication module via PROFINET IO using the TIA Portal:

1. Change to the Project view.
2. Using the project tree, insert a SIMATIC controller in the project with the "Add new device" menu command.
The device view opens and the controller is displayed.
3. Go to the network view and drag the communication module from the hardware catalog into the project.
4. Optional: Switch to the device view and delete an existing module (e.g. "Reader_1") if necessary and drag a suitable module from the hardware catalog into the corresponding module column.
5. Connect the communication module with the controller.
6. Configure the communication module (e.g. device name, address range).
7. Assign parameters to the communication module (e.g. module parameters).
8. Save the configuration, or download it to the PROFINET IO controller.

You can find additional information in the section "Assign the IP address / device name (Page 47)".

Parameter assignment with the device configuration

You can set the basic parameters of the communication module, as well as the parameters of the readers connected to the communication module, using the properties window of the communication module. You can set all module-specific parameters using the following parameter groups.

"Web Based Management" parameter group

You can start Web Based Management in this parameter group.

Table 6- 1 Parameters of the "Web Based Management" parameter group

Parameter	Description
Web Based Management	<p>Start Web Based Management of the communication module.</p> <p>Web Based Management (WBM) offers extensive functions for configuring the communication module.</p> <p>Note: WBM can only be started when the IP address stored in the project has been assigned to the communication module. This means that the device name must have been assigned and the TIA configuration must be loaded into the SIMATIC controller.</p>

"Configuration management" parameter group

You can load or save configuration data in this parameter group.

Table 6- 2 Parameters of the "Configuration management" parameter group

Parameter	Description
User name ¹⁾	<p>User name of a user created on the communication module</p> <p>Note that the user must have the required rights.</p>
Password ¹⁾	Enter the password for the user
Load configuration to device	Load configuration data from the STEP 7 project into the communication module.
Save configuration in project	Save configuration data of the communication module in the current STEP 7 project.

¹⁾ User name and password must only be entered when the user management of the WBM is enabled.

Requirement

The following requirements must be met so that configuration data can be loaded or saved:

- The "PROFINET interface [X1]" entry contains the correct IP address of the communication module.
- The specified user has the required rights to perform the download/upload.

Note**User name and password only necessary if user management is enabled**

The "User name" and "Password" text boxes only need to be completed if the user management of the CM in the WBM is enabled.

"Module parameters" parameter group

In this parameter group, you can configure all module-specific parameters of the communication module.

Table 6- 3 Parameters in the "Module parameters" parameter group

Parameter	Parameter value	Default value	Description
Diagnostic interrupt	Off On	On	Switching diagnostic interrupt messages of the communication module on and off.

Parameter group "Module parameters > General parameters" of the submodules (connected readers)

In this parameter group, you can configure all module-specific parameters of the connected readers. Please note that some of the following parameters are module-specific. For some module types, not all parameters are displayed.

Depending on the Ident device that is connected to the respective interface (X21-X24), you must use the matching submodule.

If no device is connected to interface X21, you need to assign an "Empty" module to this interface.

Table 6- 4 Parameters of the parameter group "Module parameters > General parameters" of the submodules (connected readers)

Parameter	Parameter value	Default value	Description
User mode	Ident profile/RFID standard profile FB 45	Ident profile/RFID standard profile	With this parameter, you select the block: <ul style="list-style-type: none"> Ident profile/RFID standard profile: <p>Single tag / multitag mode. The program block for the Ident profile is used in the controller.</p> FB 45: <p>Single tag mode. FB 45 is used in the controller</p>
MOBY mode	RF200/RF300/RF600; MV400/MV500; MOBY U/D normal addr.	RF200/RF300/RF600; MV400/MV500; MOBY U/D normal addr.	With this parameter, you set the mode of the communication module. <ul style="list-style-type: none"> RF200/RF300/RF600; MV400/500; MOBY U/D normal addr. <p>Normal addressing: The transponder is addressed with physical addresses.</p>
Transmission speed	19.2 kBd 57.6 kBd 115.2 kBd 921.6 kBd	115.2 kBd	With this parameter, you set the data transmission speed between the communication module and the reader. <p>When an optical reader is connected: The transmission speed selected here must match the transmission speed selected for the reader.</p>

Parameter	Parameter value	Default value	Description
Diagnostics messages	None Hard errors Hard/soft errors	None	<p>With this parameter, you determine the extent to which the reader-related diagnostic interrupt messages are to be reported.</p> <ul style="list-style-type: none"> • None: No alarms are generated. • Hard errors: Critical hardware errors/faults are reported by the S7 diagnostics. • Hard/soft errors: Critical hardware faults and errors occurring when processing commands are reported by the S7 diagnostics.
IO mode ¹⁾	Input Output IO-Link	Input	<p>You use this parameter to specify the mode of the I/O interface of the communication module:</p> <ul style="list-style-type: none"> • Input: Single digital input • Output: Single digital output • IO-Link: Mode for connection of an IO-Link device with digital inputs/outputs.

¹⁾ This parameter is only included for CI communication modules.

Parameters of the parameter group "Module parameters > Frame" of the submodules (connected readers)

This parameter group is displayed when you have selected the "Freeport" submodule. In this parameter group, you can configure all parameters specific to the "Freeport".

Table 6- 5 Parameters of the parameter group "Module parameters > Frame" of the submodules (connected readers)

Parameter	Parameter value	Default value	Description
Parity	None Odd Even Fixed value 1 Fixed value 0	None	<p>Parity selection</p> <p>A sequence of data bits can be expanded by a parity bit. With its value "0" or "1", the parity bit is added to the sum of all bits (data bits and parity bits) to form a defined status. This increases data reliability.</p> <ul style="list-style-type: none"> None: Data is sent without a parity bit. Odd: The parity bit is set so that the sum of the data bits (including the parity bit) is odd when the signal state is "1". Even: The parity bit is set so that the sum of the data bits (including the parity bit) is even when the signal state is "1". Fixed value 1: The parity bit is set permanently to the value "1". Fixed value 0: The parity bit is set permanently to the value "0".
Data bits	7 8	8	Selection of the number of bits to which a character is mapped.
Stop bits	1 2	1	<p>Selection of the number of stop bits that indicate the end of a character.</p> <p>The stop bits are appended to every transferred character during transmission.</p>
Interface	RS422 RS232	RS422	Selection of the interface type that the connected hardware (reader / optical readers) uses.

Parameter	Parameter value	Default value	Description
Specifying end detection	After character delay time elapses On receipt of fixed number of characters On receipt of the end delimiter(s)	After character delay time elapses	Specifies the end detection of a received frame: <ul style="list-style-type: none"> After character delay time elapses: The frame has neither a fixed length nor defined end delimiters. The end of a frame is indicated by a gap in the character sequence. The size of this gap is specified by the character delay time. On receipt of fixed number of characters: The length of the received frames is always the same. When data is received, the end of the frame is recognized when the set number of characters has been received. On receipt of the end delimiter(s): At the end of the frame, there are one or two defined end delimiters. When data is received, the end of the frame is recognized when the configured end delimiter(s) is/are received.
No. of end delimiters	1 2	1	Selection of the number of end delimiters. A maximum of 2 end delimiters can be configured. When data is received, the end of the frame is recognized when the selected end delimiter combination is received.
1st end delimiter	0...255	3	Entry of the first end delimiter of a maximum of two end delimiters for the end criteria "On receipt of the end delimiter(s)". The selected end delimiter or the selected end delimiter combination limits the length of the frame. Parameter value depending on the "Data bits" parameter.
2nd end delimiter	0...255	0	Entry of the second end delimiter of a maximum of two end delimiters for the end criteria "On receipt of the end delimiter(s)". The selected end delimiter combination limits the length of the frame. Parameter value depending on the "Data bits" parameter.
Frame length	1...233 / 1...229	233	Entry of the frame length in bytes for the end criterion "On receipt of fixed number of characters".
Character delay time	0...65535	15	Entry of the time [ms] that can elapse until a frame end is recognized. Select the character delay time dependent on the sending behavior of your communication partner. Depending on the data transmission speed the character delay time is limited to a minimum value. Note that the ASCII driver also pauses between two frames during transmission.

Description of block commands

You can find a description of the block-specific commands in the respective block manuals:

- FB 45 for RF200, RF300
- RFID standard profile; standard function for RFID systems
- Ident profile and Ident blocks, standard function for Ident systems

6.3 Configuration via XML



This section is intended only for XML users.

Configuration of the communication module is not necessary for pure XML work. You can continue directly with configuration via WBM and with programming via XML. You can find detailed information on the XML diagnostic functions in the "XML programming for SIMATIC Ident (<https://support.industry.siemens.com/cs/ww/en/ps/14971/man>)" manual.

6.4 Configuration via OPC UA



This section is intended only for OPC UA users.

Configuration of the communication module is not necessary for pure OPC UA work. You can continue directly with configuration via WBM and with programming via OPC UA.

6.5

Configuring with Studio 5000 Logix Designer



This section is intended only for users of Rockwell controllers.

You can configure the communication modules using add-on instructions via a Rockwell controller. You can find a detailed description of the Ident profile and the add-on instructions in the "Ident profile and Ident blocks, standard function for Ident systems (<https://support.industry.siemens.com/cs/ww/en/view/109762333>)" function manual.

Note

Serial number in Studio 5000 Logix Designer

Note that the serial number specified in the Studio 5000 Logix Designer does not match the communication module serial number. The serial number specified in the Logix Designer forms the last 4 bytes of the MAC address of the communication module.

Note

Tested programs

The content described in this section was tested with the programs "Studio 5000 Logix Designer" (V21 to V28) and "RSLogix 5000" (V20).

Configuring with the WBM

The communication modules are equipped with a Web server that provides Web Based Management (WBM) to the Web client for configuring the communication modules. The WBM can be called via the Web browser of a PC/laptop.

The WBM server provides the Web client (PC/laptop) with the parameter data of the communication module and accepts parameter changes from the Web client. Note that changed parameter values are not automatically transferred to the communication module. You must always manually transfer changes to the configuration to the communication module.

In the following, the term "WBM" is used to represent the WBM interface displayed in the Web browser.

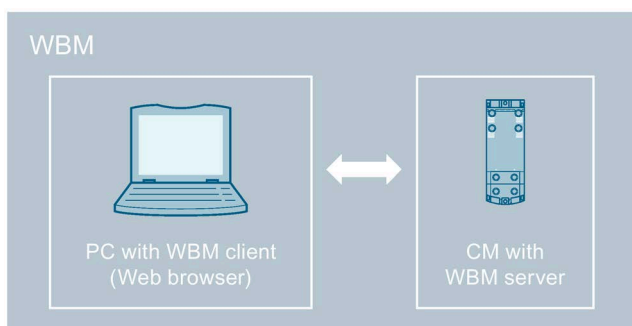


Figure 7-1 Design and function of the WBM

7.1 Starting WBM

Note

Up-to-date screenshots

Note that the following screenshots may not reflect the current firmware version.

Requirement

The communication module is connected, turned on and ready for operation ("RUN" LED is lit or flashing green) and the relevant communication module has been assigned an IP address.

To achieve a good workflow with the WBM, we recommend that you use a PC that meets the following minimum requirements:

- CPU: DualCore
- RAM: 2 GB

You can call WBM using the versions of the following Web browsers current at the time of publication of this manual: Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox and Google Chrome. The user interface of the WBM is designed for a screen resolution of 1366 x 768 pixels.

Procedure

Proceed as follows to start the WBM:

1. Start your Web browser.
2. Enter the IP address of the communication module in the address field of your browser.
3. Confirm your entry by pressing the <Enter> key.

Result: WBM of the communication module opens.

Alternatively, you can also open the WBM from the TIA Portal.

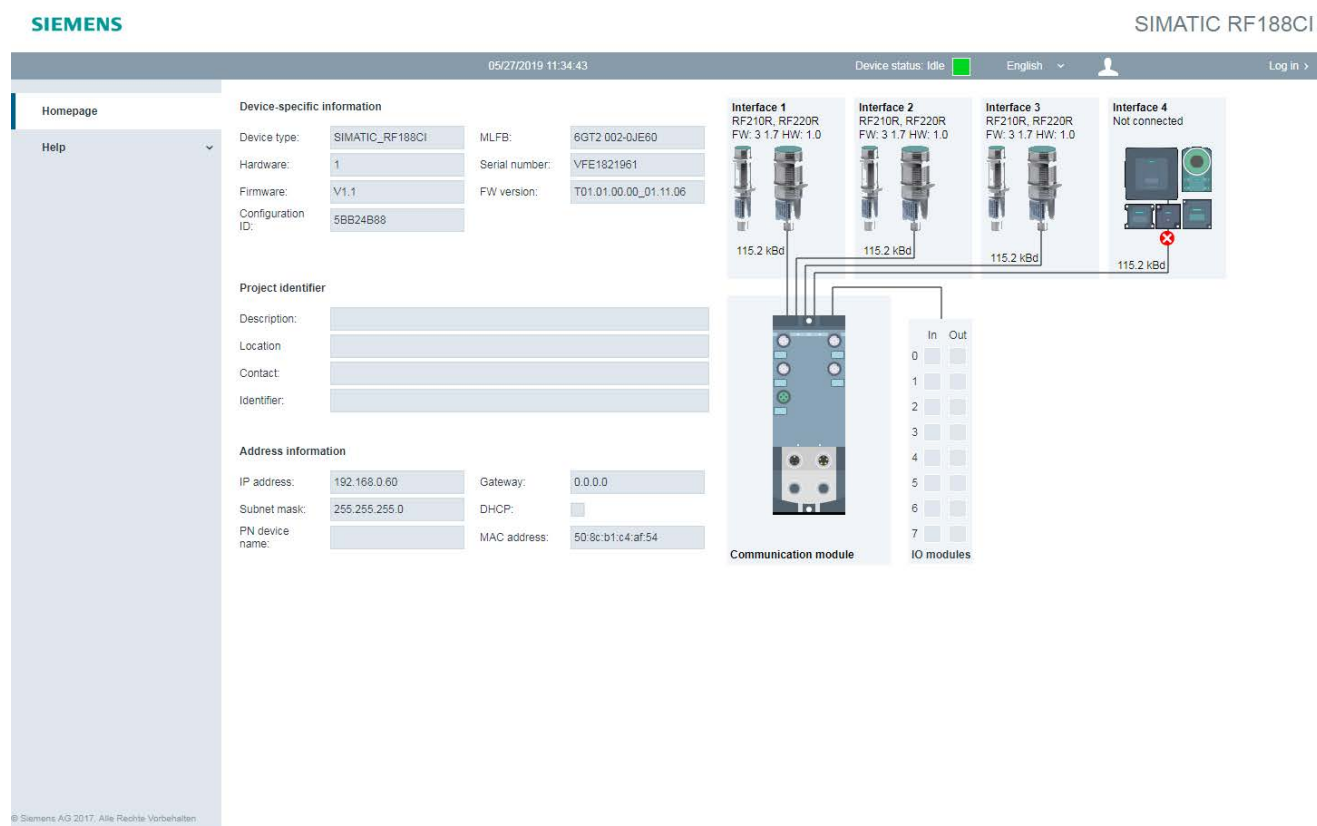


Figure 7-2 The start page of the WBM

Note**Connection to the communication module cannot be established**

If a connection to the communication module cannot be established, check the following points:

- Make sure that all cables are correctly connected.
- Ensure that the communication module has started up ("RUN" LED lit/flashing green).
- Check the IP addresses of the PC and the communication module as well as the subnet mask. Both IP addresses must be located in the same subnet.
- Make sure that the connection is not blocked by a firewall.
- Use a ping request to check the connection between the PC and the communication module.

7.2

The WBM

You can use the WBM to configure the SIMATIC RF18xC/RF18xCI communication modules.

NOTICE**Security recommendation: Enable user management**

After starting the WBM the first time, no user management is enabled. To make sure that no unauthorized persons can access the communication module settings, we recommend that you enable the user management and create new user profiles after the first login. Note that user administration can only be enabled by an administrator.

During your first login as administrator (User: admin / password: admin), you must change the password for security reasons.

For further information on logging in to WBM and creating/deleting user profiles, refer to the section "The "User management" menu item (Page 104)".

NOTICE**Access to the communication module**

Note that you can simultaneously access a communication module via multiple WBM clients (Web browsers) but this is not recommended.

If changes are made when two WBM clients are accessing a reader at the same time, this can lead to errors in the configuration or an undesired result.

When you have created new user profiles you need to log in with one of these user profiles when you restart the WBM.

Layout of the WBM

Once the connection to the communication module has been successfully established, the WBM start window appears:



The WBM start window is divided into the following areas:





- ① Toolbar/status bar and log-on
- ② Menu tree
- ③ Main window
- ④ Message area
- ⑤ Information bar

Figure 7-3 Start window of the WBM

Toolbar and status bar

On the left above the main window, there are four buttons for transferring/loading/storing the displayed configuration. You can also operate these buttons directly with key combinations.

Table 7- 1 The toolbar of the WBM

Icon	Description
	Transfer configuration to communication module With this button, you can transfer the configuration data set in the WBM to the communication module. Key combination: Ctrl + L
	Load configuration from communication module With this button, you can load the configuration data currently set on the communication module into the WBM. Key combination: Ctrl + G
	Save configuration as With this button, you can save the configuration data set in the WBM on the PC. Key combination: Ctrl + S
	Load configuration from PC With this button, you can load the configuration data stored on the PC in the WBM. Remember that this data is only loaded in the WBM. To transfer the data to the communication module, you also need to click the "Transfer configuration to communication module" button. Key combination: Ctrl + O

Note

Transferring a configuration

Please note that transferring a configuration can disrupt running user applications. In WBM, an orange bar in the information area warns you when this is the case.

Note

Loading a configuration

Note that you cannot use the configuration file to transfer user profiles and passwords to other communication modules. After loading the configuration file into a new communication module, you may need to enable user management and create new user profiles and passwords.

On the right above the main window there is the status bar with the following information:

- Date/time display of the communication module
- Display of the device status
- Drop-down list for selecting the user interface language
- Logon/logoff area (with active user administration)

Menu tree

The menu tree is located in the left margin of the WBM. The currently selected menu item is highlighted in color.

The following table provides an overview of the menu items and the functions they provide.

Table 7- 2 The menu structure of the WBM

Menu items		Functions
Start page		<ul style="list-style-type: none"> • System overview • Viewing device-specific information • Entering customer-specific plant designation
Settings		
	General	Enabling/disabling categories of log events
	Reader interface	Configuring connected readers
	Digital outputs	Setting the behavior of the digital outputs ¹⁾
	Communication	Making communication settings
Diagnostics		
	Hardware diagnostics	Interface-specific diagnostics function
	Log	Overview of log entries
	Service log	Information for service cases
	Syslog log	Overview of Syslog messages
Edit transponder		Reading out and writing transponder data
User management		<ul style="list-style-type: none"> • Enabling/disabling user management • Creating and deleting user profiles • Changing passwords
System		
	System settings	<ul style="list-style-type: none"> • Performing a firmware update for the communication module • Restoring the factory settings for the communication module • Specifying the IP address • Importing HTTPS certificates • Downloading device description files
	Reader firmware	Updating the firmware for connected readers
Help		
	Service and Support	Additional information about the communication module
	Manual	Manual for the communication module

¹⁾ Only with CI products.

If you are logged in to the WBM with the "User" role, some menu items can only be used with restrictions. You will find a list of the restrictions in the section "The "User management" menu item (Page 104)".

Main window

The main window shows the contents of the selected menu items. Here, you can configure the various menu-dependent parameters.

Note

Entering values in text boxes

Apart from manual entry of values, you can also change values with the following buttons:

- Arrow up / down
The value is increased or decreased by one increment.
 - PgUp / PgDn
The value is increased or decreased by ten increments.
 - Home / End
The value is set to the minimum or maximum value.
-

Message area

The message area displays all WBM-related error messages and warnings (e.g. transfer errors).

Information bar

The information bar displays deviations between the settings in the user interface of the WBM and the configuration stored on the connected communication module. Minor deviations are designated by a yellow symbol. Changes that lead to a restart of the communication module are designated by an orange symbol.

While you are accessing the communication module via the WBM, if changes are being made to the communication module via the connected controller at the same time, these changes are indicated by a turquoise symbol.

7.3 The menu items of the WBM

7.3.1 The "Start page" menu item

The "Start page" menu item is divided into the following areas.

- Device-specific information
- Project ID
- Address information
- Device clock
- Configuration display

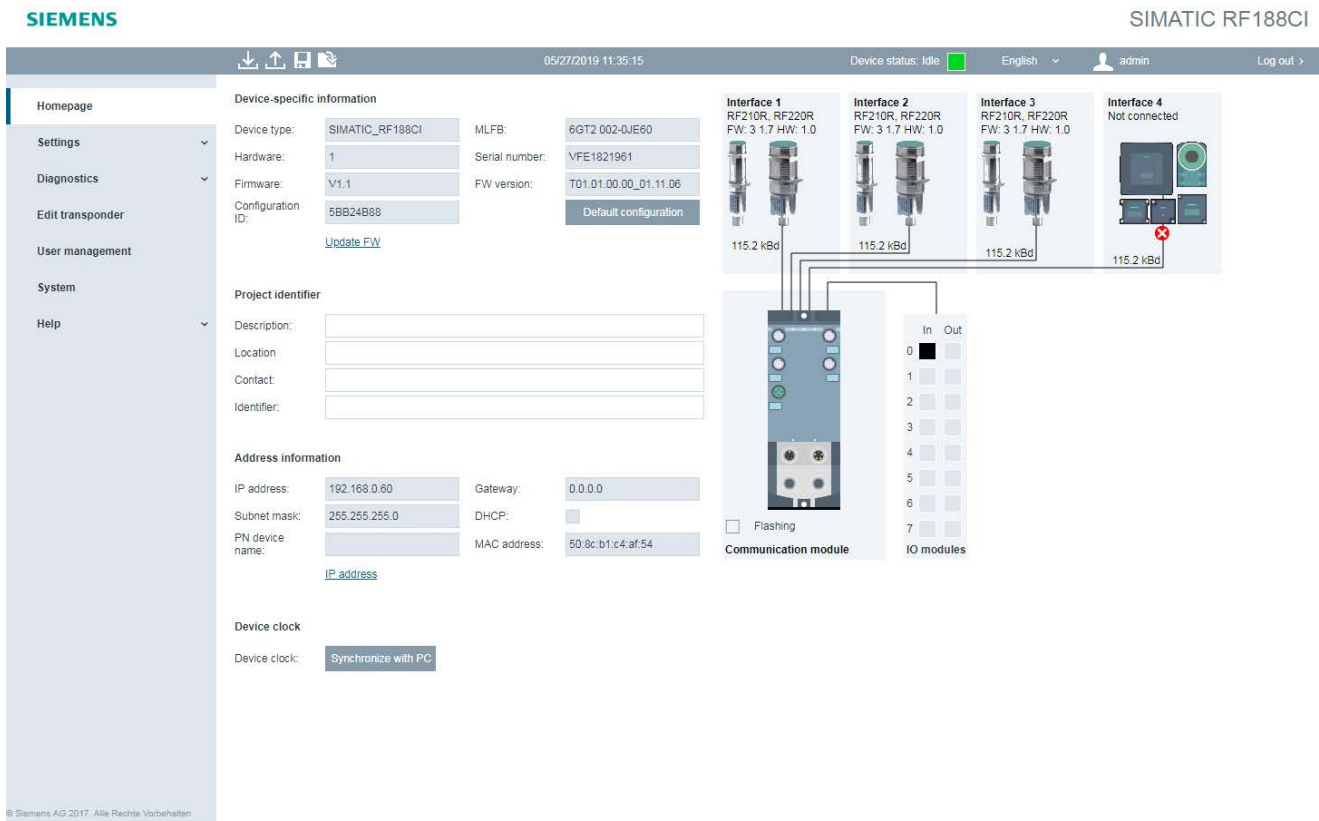


Figure 7-4 The "Start page" menu item

Device-specific information

The first area contains device-specific information. The "Device type", "MLFB", "Hardware" and "Serial number" boxes are specified in the factory. The content of the "Firmware" and "Firmware version" boxes depends on the firmware stored on the communication module. Using the "Update firmware" link, you jump to the "System" menu item in which you can update firmware. The "Configuration ID" box contains a unique identifier for the configuration that was last activated on the communication module or loaded into the communication

module. Click the "Default configuration" button to reset the parameters shown in the user interface to the default values. When you restore the default configuration, address information (IP address, device name) is retained.

Project ID

The second area contains text boxes that you can use to store your own device-specific information in the communication module. Among other things, these should help you to more easily identify the individual communication modules.

Address information

The third area contains all important address information via which the PC or the controller can reach the communication module. You can assign the IP address and PN device names to the communication module using "SINEC PNI" and "STEP 7". Via the link "IP Address" you jump to the "System" menu item in which you can also reassign the IP address.

Device clock

With the "Synchronize with PC" button, you can synchronize the device clock with the time in your operating system.

Note




The device time always corresponds to UTC time

Note that the time of the device clock corresponds to UTC time and cannot be adjusted to time zones. Clicking the button transfers the local time stored in your operating system to the communication module. Because the time synchronized with the PC is lost when the power supply is terminated, we recommend synchronizing the time with an NTP server.

Configuration display

The current configuration is shown to the right of the four areas. The schematic diagram contains information on the connected communication module type, the readers and the digital inputs/outputs.

Table 7- 3 States of the digital inputs/outputs

	The input/output is not configured.
	The input/output is configured but not connected.
	The input/output is configured and connected.

With the "Flash" check box, you can have the LEDs of the communication module and the readers connected to it flash. This enables you to quickly and easily identify the connected devices on sight. Note that this function is not supported by all readers.

7.3.2 The "Settings - General" menu item

The "Settings - General" menu item is divided into the following area:

- Log settings

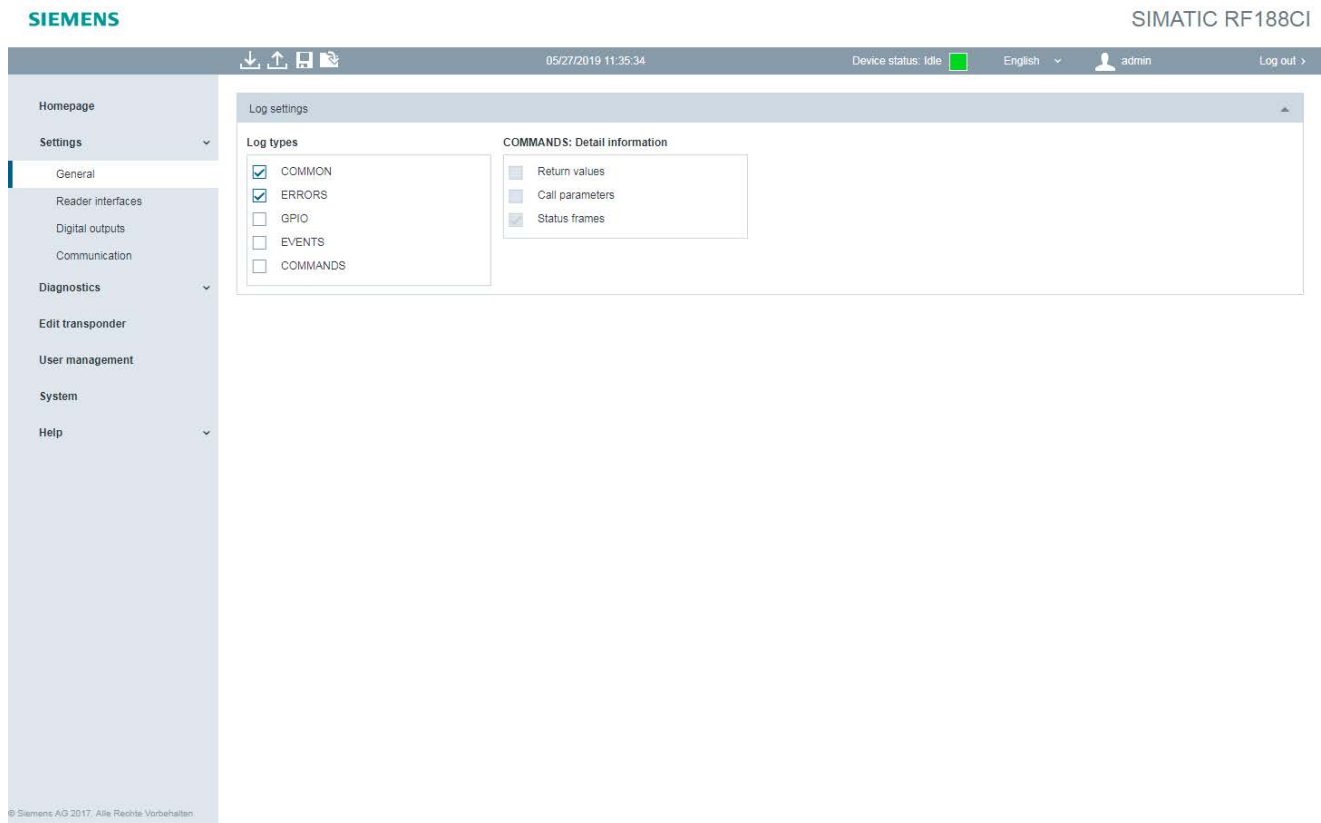


Figure 7-5 The "Settings - General" menu item

Log settings

In the "Log settings" area, you can use the check boxes to decide which events are entered in the log. The log is structured as a circular buffer. Bear in mind that with a high degree of detail of the data, the circular buffer fills up more quickly which can have a negative effect on the performance of the device.

Table 7- 4 Description of the parameters of the log

Parameter	Description
General	
COMMON	Messages relating to general events: e.g. reader startup, login to the WBM, ...
ERRORS	Errors and alarm messages of the communications module
EVENTS	Recording of all tag events
COMMANDS	Commands of the user application

Parameter	Description
Additional information	
Return value	Return values for the commands of the user application and for the written or read transponder data.
Call parameters	Call parameters for the commands of the user application
Status telegrams	Recording status commands in PLC communication. Can be switched off if the status commands are used as cable monitoring. In this way, the logbook is kept free for user data.

7.3.3 The "Settings - Reader Interface" menu item

With the "Settings - Reader interface" menu item, up to four readers can be defined depending on the communication module type. If the communication module is connected to an S7 controller, the configurations are made via the controller. In this case, the set values are only displayed in the WBM and cannot be edited.

The settings of each interface are identically structured and divided into the following areas:

- Basic settings
- Reader parameters

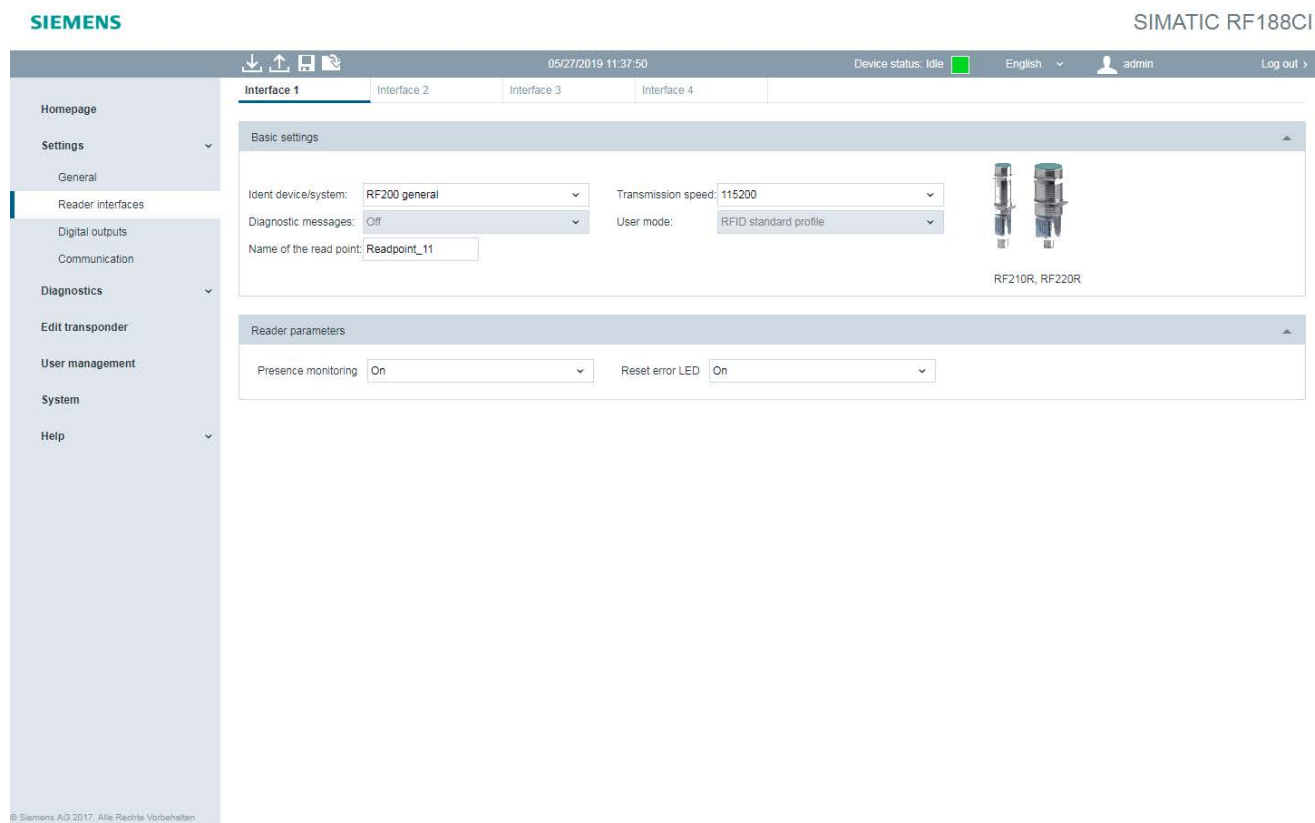


Figure 7-6 The "Settings - Reader Interface" menu item

Basic settings

In this section, you define the basic settings for the selected reader interface.

Table 7- 5 Description of the basic parameters

Parameter	Parameter value	Default value	Description
Ident system category	General reader RF300 fast protocol Freeport	General reader	Selection of the Ident system category. The various Ident system categories differ in the communication protocols they use. Depending on the selection made, different parameter values are displayed in the following "Ident devices/system" parameter. Note that the parameter value "Freeport" can only be used for a connection via PROFINET and EtherNet/IP.
Ident devices/system	Empty module General reader RF200 general RF290R RF300 general RF380R RF300 Gen 2 general RF380R Gen 2 MV400/MV500 General reader RF300 fast protocol RF380R fast protocol Freeport RF1000	General reader	Selection of the device/system connected to the communication module. Depending on the selection made, different parameters are shown or hidden in the following "Reader parameters" section. If no device is connected to the interface, select the "Empty module" parameter value.
Diagnostics messages	None Hard errors Hard/soft errors	None	Shows which diagnostic messages have been set in STEP 7 (cf. Section "Parameterization of the diagnostics (Page 153)"): <ul style="list-style-type: none"> None: Apart from standard diagnostics, no other alarms are generated. Hard Errors: Critical hardware errors/faults are reported by the S7 diagnostics. Hard/Soft Errors: Critical hardware errors and errors that occur during command processing are reported by the S7 diagnostics. The "Ext_Diag" bit is set.

Parameter	Parameter value	Default value	Description
Read point name	--	--	In the text box, you can assign a name to the read point(s) (for example, "Incoming goods gate 5" or "Welding robot 21"). Note that the name is required for addressing the reader via OPC UA.
Transmission speed	19.2 kBd 57.6 kBd 115.2 kBd 921.6 kBd	115.2 kBd / 921.6 kBd	Selection depends on the Ident device/system being used. With this parameter, you set the data transmission speed between the communication module and the reader.
User mode	Ident profile/RFID standard profile FB 45	Ident profile/RFID standard profile	Shows which block has been set in STEP 7: <ul style="list-style-type: none"> Ident profile/RFID standard profile: The program block for the Ident profile/RFID standard profile is used on the controller. FB 45: Single tag mode. FB 45 (PROFIBUS/PROFINET) is used in the controller.

The parameter values of the basic parameters can be preset automatically using the "Autoconfiguration" button. By pressing the button, the communication module automatically identifies the device connected to the interface and sets the appropriate parameter values.

Using the "Update firmware" link, you jump to the "System - Reader firmware" menu item in which you can update firmware for the connected reader.

Reader parameters

If you have selected the "General reader" parameter value in the "Ident devices/system" parameter, the reset parameters of the reader connected to the interface are displayed in hexadecimal format in this area. You can find more detailed information on this in the "Ident profile and Ident blocks, standard function for Ident systems (<https://support.industry.siemens.com/cs/ww/en/view/109762333>)" manual.

If you have set another parameter value in the "Ident devices/system" parameter and depending on the basic parameters set, you can configure the following reader parameters in the "Reader parameters" parameter group.

Table 7- 6 Parameters in the "Reader parameters" parameter group I

Parameter	Parameter value	Default value	Description
Presence check	On Off (RF field on) Off (RF field off)	On	<ul style="list-style-type: none"> On Presence is reported as soon as there is a transponder in the antenna field of the reader. Off (RF field on) The presence check on the FB is suppressed. The antenna on the reader is nevertheless turned on as long as it has not been turned off by a command. Off (RF field off) The antenna is turned on only when a command is sent and it then turns itself off again.
RF power ¹⁾	0.50 ... 5.00	1.00 1.25	Setting for the output power of the reader.
Reset error LED	On Off	Off	<ul style="list-style-type: none"> On The flashing of the error LED on the reader is reset by each reset and by a new OPC command. Off The error LED always indicates the last error. The display can only be reset by turning off the reader.
Max. number of transponders	1 ... 40	1	Number of transponders expected in the antenna field.
Reader mode	Normal operation P2P master P2P master + ISO P2P master + RF300 P2P slave	Normal operation	<p>Selection of the required reader mode. This parameter is intended for trained users. As a rule, the "Normal operation" operating mode of the reader is used.</p> <p>For P2P mode, one reader must be configured as a "P2P slave" and one reader as a "P2P master". If the P2P master also communicates with ISO or RF300 transponders, you must select the appropriate parameter value.</p>
ECC mode	On Off	Off	<p>Switching the ECC mode on/off</p> <p>In ECC mode, the reader can detect bit errors on the transponder with a high degree of probability and correct the sent data, if possible.</p>
Transponder type	¹⁾	¹⁾	Selection of the transponder types used.

¹⁾ You can find a detailed description of these parameters in the following paragraphs.

The "RF power" parameter

The selectable values depend on the value specified in the parameter "Ident device / system".

- RF290R
 - Value range: 0.50 ... 5.00 W
 - Default value: 1.00 W
- RF380R
 - Value range: 0.50 ... 2.00 W
 - Default value: 1.25 W

The "Transponder type" parameter

Selection of the transponders used. The selection depends on the value specified in the parameter "Ident device / system". The following transponder types can be selected:

Ident device / system	Value (transponder types)
RF290R	ISO 15693 MDS D3xx, Infineon
RF300 general RF380R	RF300 ISO 15693 General MDS D3xx, Infineon MDS D4xx, Fujitsu - 4 KB MDS D1xx, NXP MDS D2xx, TI MDS D261, STM
RF300 Gen 2 general RF380R Gen 2	
RF300, MOBY E	RF300 MOBY E RF300, MOBY E
ISO 15693	None ISO 15693 General MDS D3xx, Infineon MDS D4xx, Fujitsu - 4 KB MDS D1xx, NXP MDS D2xx, TI MDS D261, STM MDS D5xx, Fujitsu - 8 KB

Table 7- 7 Parameters in the "Reader parameters" parameter group II (Freeport)

Parameter	Parameter value	Default value	Description
Interface	RS422 RS232	RS232 / RS422	Selection of the interface type that the connected hardware (reader / optical readers) uses. The default value depends on the interface used:
Parity	None Odd Even Fixed value 1 Fixed value 0	None	<p>Parity selection</p> <p>A sequence of data bits can be expanded by a parity bit. With its value "0" or "1", the parity bit is added to the sum of all bits (data bits and parity bits) to form a defined status. This increases data reliability.</p> <ul style="list-style-type: none"> • None: Data is sent without a parity bit. • Odd: The parity bit is set so that the sum of the data bits (including the parity bit) is odd when the signal state is "1". • Even: The parity bit is set so that the sum of the data bits (including the parity bit) is even when the signal state is "1". • Fixed value 1: The parity bit is set permanently to the value "1". • Fixed value 0: The parity bit is set permanently to the value "0". <p>Note: The values "Fixed value 0" and "Fixed value 1" are not supported by Linux systems. In this case, the value "None" is used automatically.</p>
Data bits	7 8	8	Selection of the number of bits to which a character is mapped.
Stop bits	1 2	1	<p>Selection of the number of stop bits that indicate the end of a character.</p> <p>The stop bits are appended to every transferred character during transmission.</p>

Parameter	Parameter value	Default value	Description
Specifying end detection	After character delay time elapses On receipt of fixed number of characters On receipt of the end delimiter(s)	After character delay time elapses	Specifies the end detection of a received frame: <ul style="list-style-type: none"> After character delay time elapses: The frame has neither a fixed length nor defined end delimiters. The end of a frame is indicated by a gap in the character sequence. The size of this gap is specified by the character delay time. On receipt of fixed number of characters: The length of the received frames is always the same. When data is received, the end of the frame is recognized when the set number of characters has been received. On receipt of the end delimiter(s): At the end of the frame, there are one or two defined end delimiters. When data is received, the end of the frame is recognized when the configured end delimiter(s) is/are received.
No. of end delimiters	1 2	1	Selection of the number of end delimiters. A maximum of 2 end delimiters can be configured. When data is received, the end of the frame is recognized when the selected end delimiter combination is received.
1st end delimiter	0...255	3	Entry of the first end delimiter of a maximum of two end delimiters for the end criteria "On receipt of the end delimiter(s)". The selected end delimiter or the selected end delimiter combination limits the length of the frame. Parameter value depending on the "Data bits" parameter.
2nd end delimiter	0...255	0	Entry of the second end delimiter of a maximum of two end delimiters for the end criteria "On receipt of the end delimiter(s)". The selected end delimiter combination limits the length of the frame. Parameter value depending on the "Data bits" parameter.
Frame length	1...233 / 1...229	233	Entry of the frame length in bytes for the end criterion "On receipt of fixed number of characters".
Character delay time	0...65535	150	Entry of the time [ms] that can elapse until a frame end is recognized. Select the character delay time dependent on the sending behavior of your communication partner. Depending on the data transmission speed the character delay time is limited to a minimum value. Note that the ASCII driver also pauses between two frames during transmission.

7.3.4 The "Settings - Digital outputs" menu item

The menu item "Settings - Digital outputs" is only displayed for the RF186CI and RF188CI communication modules.

In the "Settings - Digital outputs" menu item, you can set the properties of the digital outputs and assign functions to the interface. The menu item is divided into the following areas:

- Basic settings
- Digital outputs

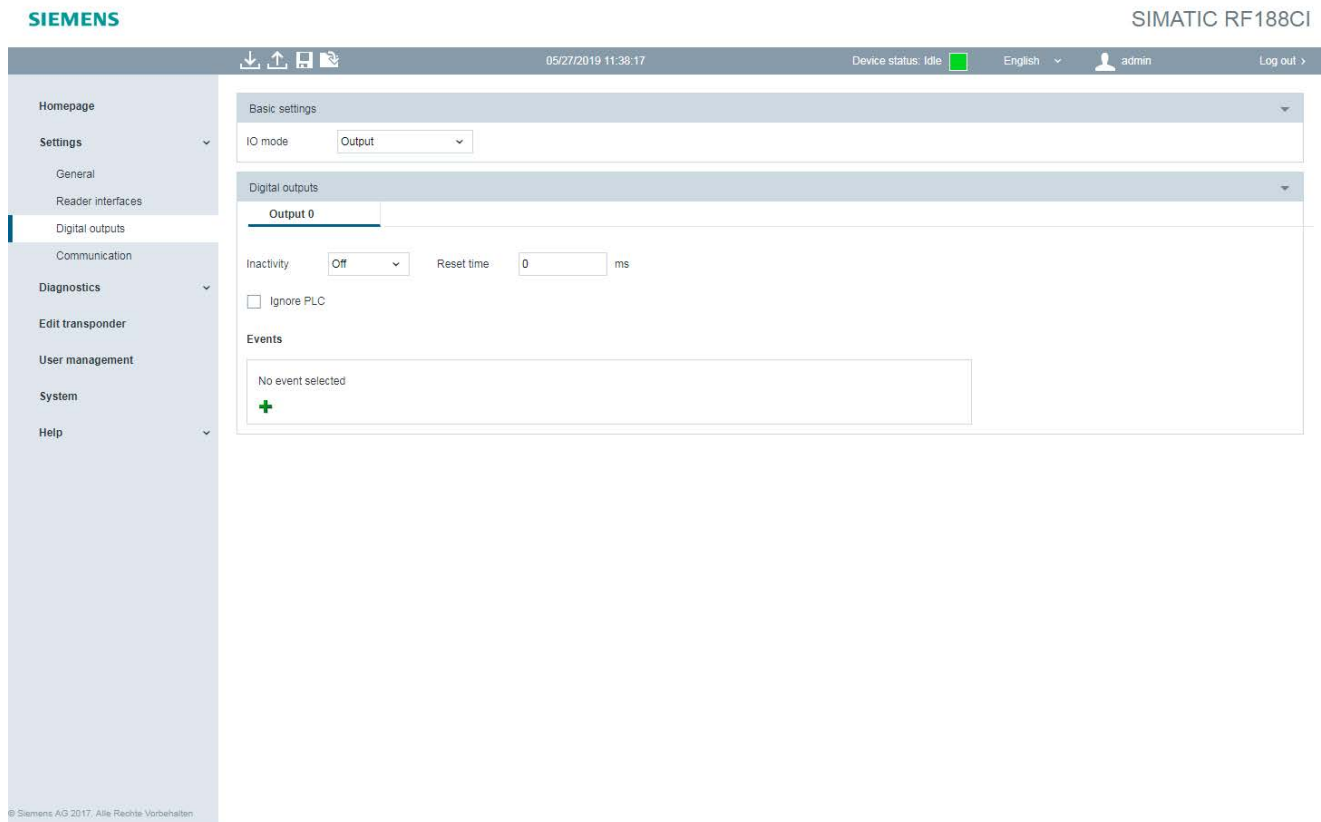


Figure 7-7 The "Settings - Digital outputs" menu item

Basic settings

In this area, you can select how the I/O interface is to be operated. Depending on your selection, the corresponding parameters are displayed in the following area.

The following options are available for the I/O interface:

- Input:
Single digital input
- Output:
Single digital output
- IO-Link:
Mode for connection of an IO-Link device with digital inputs/outputs.

Digital outputs

In the "Digital outputs" area, you can make the following settings for each output:

Table 7- 8 Description of the status properties

Boxes	Description	
Inactivity	Status that the output adopts following device startup.	
Reset time	If the reset time is set to a value $\neq 0$, the output automatically returns to the inactivity status when the reset time has elapsed. A value of 0 means that the status of the output is not influenced by this automatic function.	
	Value range	0 ... 65535 ms
	Increment	1 ms

Select the check box "Ignore PLC" to ensure that changes of the output bit via the controller do not have an effect on the physical outputs of the communication module. Changes at the digital outputs of the communication module are still being transferred to the controller.

Events

In the "Events" area, you can define events/conditions that cause a digital output to change to one of the following statuses:

- On
The output is turned on.
- Off
The output is turned off.
- Inverted
The output changes its status starting from the status that is active at the moment the event occurs.



Click the button  to add new events. Click the button  to remove already specified events.

Table 7- 9 Description of the events

Event	Description
Transponder processed	If a transponder was successfully processed by the selected read point, the output is changed to the state specified here.
Input change	If the state at the selected digital input changes, the output is set to the state specified here.
Output change	If the state at the selected digital output changes, the output is set to the state specified here.

Note

Reaction time of the digital outputs

Note that the reaction time of the digital outputs (and inputs) depends on the CM load and is 50 - 100 ms on average.

Note the following properties of the digital outputs:

- The outputs are only changed once when the event occurs.
The outputs remain set unchanged even when the event is no longer pending.
- Pending events have no effect on the output.

7.3.5 The "Settings - Communication" menu item

The "Settings - Communication" menu item is divided into the following tabs.

- Network interfaces
- PLC
- XML
- OPC UA

In the "Network interfaces" tab, you can enable/disable the network ports, SNMP and NTP protocols. You can disable STEP 7 access in the "PLC" tab. In the "OPC UA" tab, you can enable and edit the OPC UA server function of the communication module.

The "Network interfaces" tab



The "Network interfaces" tab is divided into the following areas:

- Network ports
- SNMP
- NTP
- Syslog messages

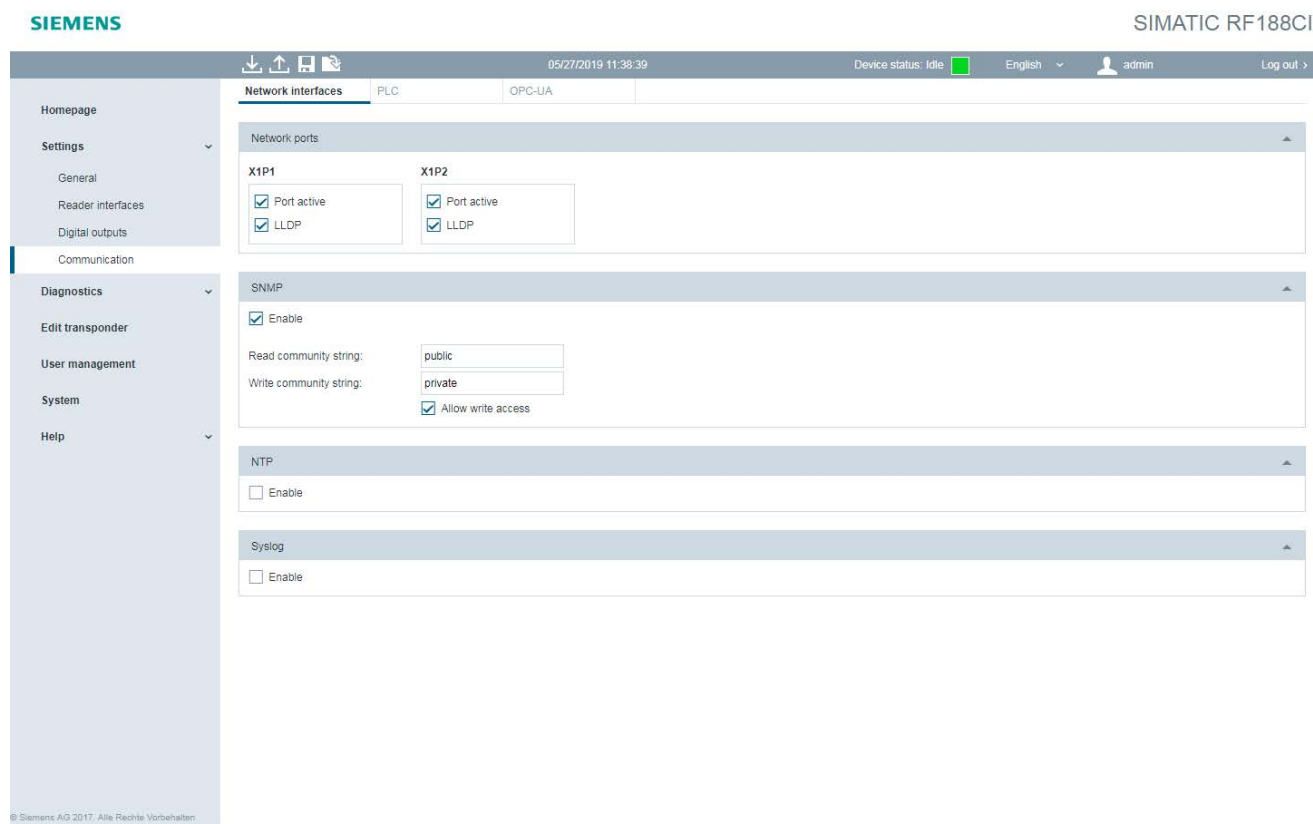


Figure 7-8 The "Settings -- Communication" menu item, "Network interfaces" tab

Network ports

In the "Network ports" area, you can enable/disable the network ports of the communication module. Click on the check box of the required network port to enable or disable it.

Note

Disabling the network ports

Make sure that you do not disable the port via which you are currently communicating with the device.

Note**Requirement for port statistics**

You can read out port statistics using PROFINET diagnostics and via SNMP.

Enable the "LLDP" check box to activate the communication log. "LLDP" is a protocol for monitoring the neighborhood.

Select the "DCP read only" check box if you want to ensure that no access to the communication module takes place via DCP. This setting prevents that the parameters of the communication module can be changed using SINEC PNI, for example.

SNMP

In the "SNMP" area, you can enable/disable the network protocol. "SNMP" is a protocol for monitoring network components.

This setting is activated at the factory. If you do not use the protocol, we recommend that you disable the setting for security reasons.

Table 7- 10 Description of the SNMP properties

Property	Description
Community string (reading)	Input box for specifying the user name for read access to SNMP variables.
Community string (writing)	Input box for specifying the user name for write access to SNMP variables. In this box, changes can only be made if write access was permitted. Write access is only possible for the SNMP variables "sysName", "sys-Location" and "sysContact" of the "system" group of MIB-2.
Allow write access	Check box to enable/disable write protection for SNMP variables.

NTP

In the "NTP" area, you can enable the network protocol. "NTP" is a protocol for synchronizing the time in network systems.

When supplied from the factory this setting is disabled and it needs to be enabled here before using NTP for the first time.

Table 7- 11 Description of the NTP properties

Property	Description
IP address of the NTP server x	Text box for entering the address of the NTP server from which the connected communication module synchronizes its time. Up to four NTP servers can be specified to compensate possible server failures.
Update interval in seconds	Input box for specifying the intervals at which the communication module automatically synchronizes its time.
Accept time from unsynchronized NTP server	Check box to ensure that the communication module also accepts the time from unsynchronized NTP servers.

Syslog messages

In the "Syslog messages" area, you can activate the Syslog messages. When the Syslog function is activated, the module generates Syslog messages at the preset UDP port according to RFC 5426. Syslog messages log information during access to the module as well as configuration changes. By default, these are saved in a log file and output in the "The "Diagnostics - Syslog logbook" menu item (Page 101)" menu. The log file is set up as a circulating buffer. If all the entries in the log file are occupied, the next new entry deletes the oldest entry.

When supplied from the factory this setting is disabled and it may have to be enabled here.

Table 7- 12 Description of the Syslog properties

Property	Description
IP address of the Syslog server	Text box for entering the address of the Syslog server to which the Syslog messages are transferred.
Default port	Text box for entering the default port of the Syslog server via which the Syslog messages are transferred.

The "PLC" tab

The "PLC" tab is divided into the following area:

- Basic settings

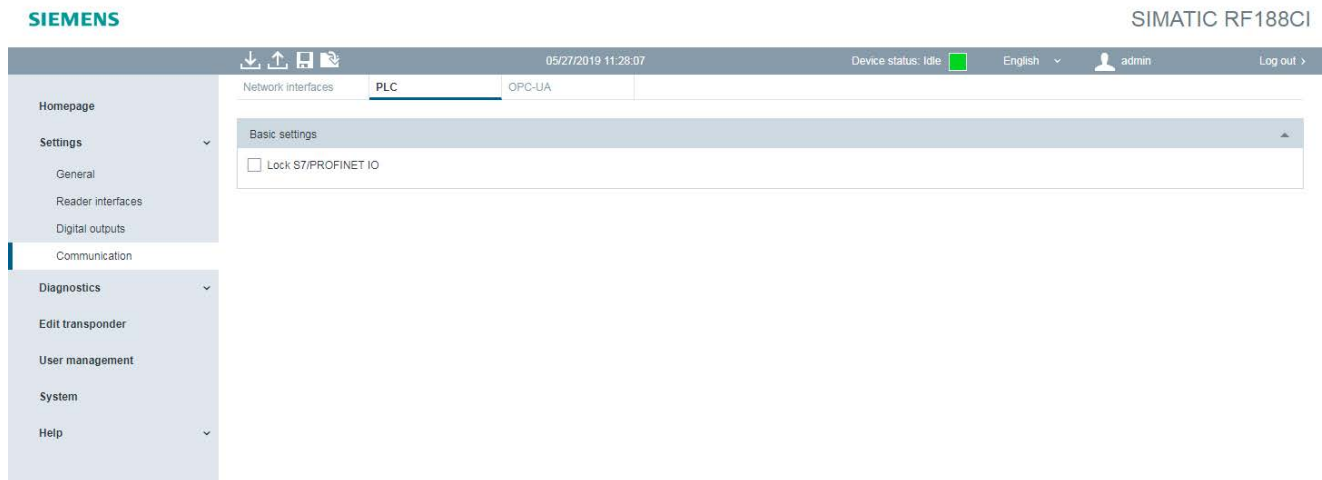


Figure 7-9 The "Settings - Communication" menu item, "PLC" tab

Basic settings

Select the check box "Disable S7/PNIO" if you want to ensure that no access to the communication module takes place via the controller (STEP 7). With this setting, the Ethernet interface is closed for communication with the controller.

Select the check box "Disable EtherNet/IP" if you want to ensure that no access to the communication module takes place via EtherNet/IP. With this setting, the Ethernet interface is closed for EtherNet/IP communication with the controller.

The "XML" tab



The "XML" tab is divided into the following areas:

- Basic settings
- XML channel

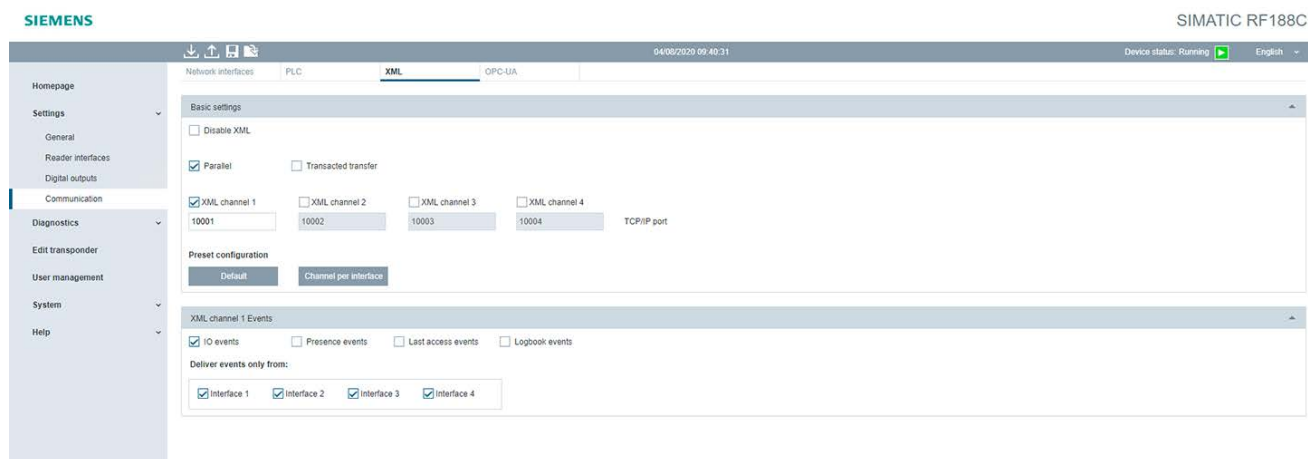


Figure 7-10 The "Settings - Communication" menu item, "XML" tab

Basic settings

You can the XML communication of the communication module in the "Basic settings" area. Click on the check box to enable or disable it.

Table 7- 13 Description of the parameters

Parameter	Description
Parallel	In addition to an existing connection, e.g. to a controller (PLC), parallel diagnostics access via the XML channel is enabled. In the case of parallel access, note that the XML application only has read access to the communication module.
Reliable transfer	<p>If the check box is selected, each frame (XML report) received from the user application of the communication module is confirmed with a response frame. If no response frame is received by the communication module within 10 seconds, it sends the report to the application again. Reports that are not transferred are buffered on the communication module.</p> <p>With this function, you can make sure that no frames from the communication module are lost even if the connection is unstable (e.g. WLAN connection aborts occasionally). This function also allows batch operation of the communication module when there is a connection to the user application at certain times. The communication module collects the frames; these can be called up using a PC application, if necessary.</p>
XML channel (1-4)	<p>Specifies which XML channels are used for communication.</p> <p>Below the check boxes, you can define the Ethernet ports of the respective XML channels in the text boxes.</p>

Parameter	Description
Channel per interface	Click on the button to activate communication via all XML channels. This function automatically presets the interface parameters in the "XML channel" areas. With this function, communication to the interfaces is performed via different XML channels.
Single channel	Click the button to enable communication via one XML channel. This function automatically presets the interface parameters in the "XML channel" area. With this function, communication for both interfaces is performed via one XML channel.

XML channel

In the "XML channel" area, you can define which events are transmitted via the selected XML channel.

Table 7- 14 Description of the parameters

Parameter	Description
Presence events	Information on the presence of connected readers or changes made to them
Tag data events	Transponder data of all registered transponders
Log events	Log entries
Interface (1-4)	Definition of which interfaces are used to transmit the selected events to the controller.

The "OPC UA" tab



The "OPC UA" tab is divided into the following areas:

- Basic settings
- Diagnostic settings
- Security settings
- OPC UA certificates

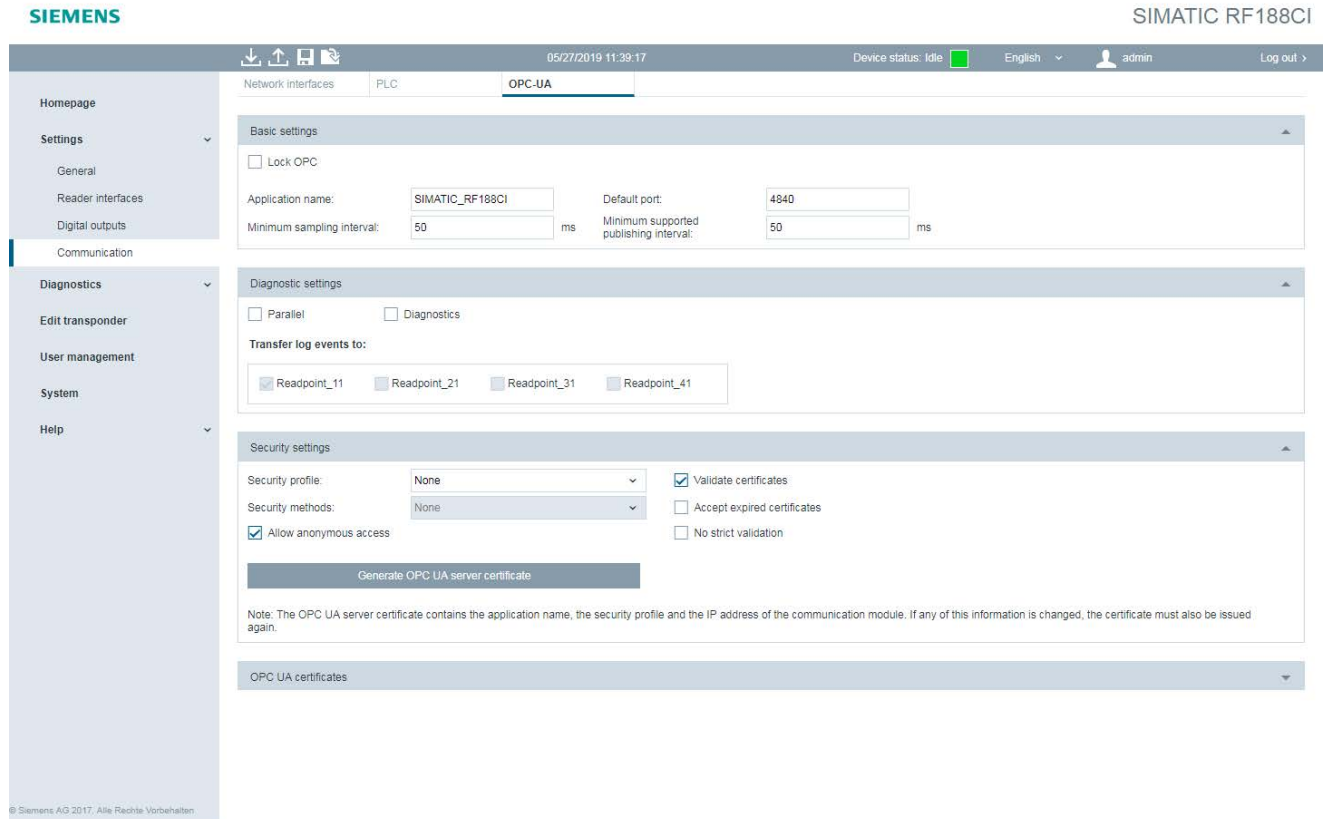


Figure 7-11 The "Settings - Communication" menu item, "OPC UA" tab

Basic settings

You can make the basic settings for the OPC UA communication in the "Basic settings" area. Select the "Disable OPC" check box to disable the OPC UA communication.

Table 7- 15 Description of the parameters

Parameter	Description
Application name	Name of the OPC UA application of the server. The application name is required to identify the OPC UA namespace of the communication module and should be unique for each communication module within the project. The application name is part of the URL of the OPC UA server of the communication module.
Minimum sampling interval	Minimum sampling interval at which the communication module samples the process data. Range of values: 10 .. 50 ms Default setting: 50 ms
Default port	Here you can change the port number of the application. As default, port number 4840 is used, the standard TCP port for the OPC UA binary protocol.
Minimum supported publishing interval	Minimum publishing interval supported by the server application at which the process data is published for logged on OPC UA clients. Lower values set by an OPC UA client are not taken into account. Range of values: 10 .. 65535 ms Default setting: 50 ms

Diagnostic settings

In the "Diagnostic settings" area, you can define which diagnostic information can be called up via specific channels.

Table 7- 16 Description of the parameters

Parameter	Description
Parallel	In addition to an existing connection, e.g. to a controller (PLC), parallel diagnostics access via the OPC UA channel can be enabled. In the case of parallel access, please note that the OPC UA client only has read access to the communication module. If the function is disabled, access to the communication module can take place either via the controller or via the OPC UA channel. If a connection is already established, an additional connection attempt from the other communication channel is rejected.
Diagnostics	Diagnostic information is transmitted to the OPC UA client. The diagnostic information includes: <ul style="list-style-type: none"> • Information about remote reader commands • Information on presence of reader • Information on presence of transponders • Transmission of log entries
Read point (1-4)	Definition of the read point via which the log entries are transmitted. The displayed names depend on the interface names specified in the "Reader interface" menu.

Security settings

In the "Security settings" area, you can make security settings for the OPC UA interface.

Table 7- 17 Description of the parameters

Parameter	Description
Security profile	<p>Specification of the security profile and the access options for the UA server of the communication module</p> <ul style="list-style-type: none"> None The "None" security profile is used. This profile does not offer any security mechanisms (encryptions). Basic 128 ¹⁾ This profile corresponds to the security profile "Basic 128" of the OPC UA specification. The communication module uses signing and, if configured, 128-bit encryption. Basic 256 ¹⁾ This profile corresponds to the security profile "Basic 256" of the OPC UA specification. The communication module uses signing and, if configured, 256-bit encryption. Basic 256 / SHA 256 This profile corresponds to the security profile "Basic 256 / SHA 256" of the OPC UA specification. The communication module uses signing and, if configured, 256-bit encryption using the hash algorithm SHA-256. It is recommended that you use the highest security level (Basic 256 / SHA 256). ¹⁾ The security levels "Basic 128" and "Basic 256" should only be used if no other security profile can be used due to compatibility reasons.
Security method	<p>Specifying the security method of the server</p> <ul style="list-style-type: none"> Sign or sign and encrypt Depending on the settings on the communication partner (client), the communication module selects the method with the highest possible security. Sign The communication module only allows communication with signed frames. Sign and encrypt The communication module only allows communication with signed and encrypted frames.
Allow anonymous access	<p>If the check box is selected, the communication module allows anonymous users access to the data of its OPC UA server.</p> <p>Anonymous users do not need to specify a user name/password when establishing a connection. If anonymous access is not allowed, an OPC UA client or a user must provide a valid user name/password combination of a user with OPC UA rights. A user with OPC UA rights can be created via the WBM. The user profile preinstalled in the factory (user name: "admin", password "admin") also has OPC UA rights.</p>

Parameter	Description
Validate certificates	If the check box is selected, the communication module generally checks the certificate of the communication partner. If the partner certificate is invalid or not trustworthy, communication is aborted.
Accept expired certificates	The communication module generally checks the period of validity of the communication partner certificate. When the check box is selected, certificates are accepted and communication is set up even if the current internal communication module time is outside the period of validity of the partner certificate.
No strict validation	<p>If the check box is selected, the communication module also allows communication in the following situations:</p> <ul style="list-style-type: none"> • If the IP address of the communication partner is not identical to the IP address in its certificate. <p>Note: The OPC UA server does not check the IP address of its communication partner (client).</p> <ul style="list-style-type: none"> • If no blacklist is stored on the communication module for the CA of the partner certificate. <p>Regardless of these exceptions, to establish a connection at least the following requirements must be met:</p> <ul style="list-style-type: none"> • If the partner certificate is not trustworthy, the communication module must at least have stored a self-signed certificate of the partner. • If the partner certificate was issued by several CAs (Certification Authorities), all CA root certificates must be stored in the certificate store of the reader.
Generate OPC UA server certificate	<p>Button for creating an OPC UA server certificate.</p> <p>Among other things, the server certificate serves to identify the OPC UA server to the OPC UA client.</p> <p>The OPC UA server certificate contains the application name, the security profile and the IP address of the communication module. If any part of this information is changed, the server certificate needs to be recreated.</p> <p>Note: Note that the procedure can take several minutes.</p>

OPC UA certificates

In the "OPC UA certificates" area you can view existing certificates, import new certificates, accept client certificates that have not been accepted yet, and create certificate signing requests.

All certificates must meet the requirements of the standard "X.509" and contain the extensions required by OPC UA (e.g. "Alternative applicant"). For detailed information, see the OPC UA specifications.

Table 7- 18 Description of the parameters

Parameter	Description
Certificate type	<p>Selection of the certificate type</p> <p>Select the required certificate type from the drop-down list and click on the "Update" button to display the certificates matching the selected certificate type.</p> <ul style="list-style-type: none"> Server certificates <p>OPC UA server certificate of the communication module</p> Client certificates <p>OPC UA client certificates of the communication partner of the communication module.</p> CA certificates <p>Root certificates from certification authorities. Certification authorities are organizations that issue signed certificates that were derived from their certificates for network participants. This means the CA certificates are root certificates for the client certificates. Client certificates for which a valid CA certificate exists are automatically accepted during connection setup.</p> Issuer certificates <p>Root certificates from certification authorities. Unlike CA certificates, client certificates derived from issuer certificates must still be accepted and permitted by an administrator with the "Accept" button.</p> <p>Note that the selection of the certificate type has an effect on the display of the subsequent parameters.</p>
Certificates	<p>List of all existing certificates</p> <p>The certificates included in this list with a black background are considered as trustworthy by the communication module. To display details of a certificate, select the required certificate in the list. The selected certificate field is highlighted in color.</p> <p>Certificates displayed in red are not classified as trustworthy. A client using such a certificate cannot establish a connection to the OPC UA partner. These certificates must still be accepted and permitted by an administrator with the "Accept" button. Certificates displayed in black have already been accepted and are classified as trustworthy.</p> <p>Depending on the selected certificate type, you can delete existing certificates. To do so, select the desired certificate in the list and click on the "Delete" button.</p>

Parameter	Description
Certificate details	<p>List with detail information on the selected certificate</p> <p>Detailed information about the certificate details is available in the X.509 specifications.</p>
Blacklists	<p>List of all blacklists</p> <p>This area is only displayed when the certificate types "CA certificates" or "Issuer certificates" were selected. A blacklist is issued by a certificate authority. A blacklist must be stored for each CA certificate and issuer certificate. Blacklists give certification authorities the option to lock client certificates again that they have issued and signed.</p> <p>The certificates listed in a blacklist are locked for communication with the communication module. To display the details of a blacklist, select the required blacklist in the list. The selected blacklist is highlighted in color.</p> <p>To delete blacklists from the list again, select the desired blacklist in the list and click on the "Delete" button.</p>
Blacklist details	<p>List with detail information on the selected blacklist</p> <p>Detailed information about the blacklist details is available in the X.509 specifications.</p>
Import OPC UA certificate	<p>In this area you can transfer the OPC UA certificate files to the communication module.</p> <p>Valid formats:</p> <ul style="list-style-type: none"> • *.p12, *.pfx <p>Binary file format, in which the certificate file and the certificate key file are stored in a single file. This file is usually protected by a password. Enter the password in the text box at the bottom. Note that this format can only be used for server certificates.</p> <ul style="list-style-type: none"> • *.cer, *.crt, *.der, *.pem <p>Binary or text coded file format, in which the certificate file and the certificate key file are stored in separate files. Note that the server certificates necessarily require a separate certificate key file. For client certificates, CA certificates and issuer certificates, only the certificate file is specified. The certificate file and the certificate key file can be either binary or text coded.</p> <ul style="list-style-type: none"> • *.crl <p>Binary or text coded file format for blacklist files. These blacklists are necessarily required for CA certificates and issuer certificates. In this case, select the certificate file and the blacklist file before you click on the "Import" button. If a matching blacklist has already been stored on the communication module, a CA certificate or issuer certificate can be transferred by itself.</p> <p>Note that only files with the file extension *.crl can be used for blacklists. Once you have imported a server certificate, you still need to activate it.</p>
Certificate signing request (CSR)	<p>Button to create a certificate signing request.</p> <p>This area is only displayed when the certificate types "Server certificates" is selected.</p> <p>Click the "Create CSR" button to create a certificate signing request (CSR). The CSR file contains all relevant information of the installed server certificate. A CA (Certificate Authority) can create a signed, module-specific server certificate using this file that you can then import into this module.</p>

Note

Recommendations for secure use of OPC UA

It is recommended that you use the highest security level (Basic 256 / SHA 256) and disable anonymous access.

7.3.6 The menu command "Diagnostics - Hardware diagnostics"

In "Diagnostics - Hardware diagnostics", you can display the status parameters of the selected reader and of the transponder currently in the antenna field.

The menu item "Diagnostics - Hardware diagnostics" is divided into the following sections:

- Basic settings
- Monitoring status
- Status
- Error counter

Basic settings

Reader interfaces: Interface 1 RF310R Gen2 FW: V 1.6

Read point: Readpoint_11

Monitoring status

Update parameter Reset error counter ☐ Automatic cyclic updating

Last acknowledgment: 11/07/2019 14:10:00

Status

Reader status		Transponder status	
Parameter	Value	Parameter	Value
Hardware type	RF310R Gen2 (0x41)	UID	00 00 00 00 00 00 00 00
Hardware version	RF300 Gen2 and RF280R AS3911 (0x0029)	Transponder type	Unknown (0x00)
Bootloader version	V1.6 (0x0106)	Version	0
Firmware version	V 1.6 (0x560106)	Lock status of the OTP area	0
Driver type	3964R (0x31)	Size of the user memory	0
Driver version	V1.2 (0x0102)	Size of a memory block	0
Interface	RS 422 (0x01)	Number of memory blocks	0
Transmission speed	115.2 kBd (0x05)	Power-flux density measured value	0
Distance limiting	0	Passive error counter	0
Max. number of transponders	1	Active error counter	0
field_on_time	0x00	Usage counter	0
Antenna status	Antenna ON (0x01)		
Presence monitoring	Presence check ON (0x01)		

Figure 7-12 The menu item "Diagnostics - Hardware diagnostics"

Basic settings

In this area, you can use the "Reader interfaces" parameter to specify the reader for which a firmware update is to be performed or which read point should undergo diagnostics.

Monitoring status

In this area you can update the reader and transponder parameters and reset error counters of the reader.

Select the "Automatic cyclic update" check box to have the parameter values updated automatically and cyclically.

Status

The following parameters are read and displayed:

Table 7- 19 Displayed parameters of the "Reader status" area

Displayed parameters	Description	
Hardware type	Hardware type of the reader	
Hardware version	Hardware version of the reader	
Bootloader version	Bootloader version of the reader	
Firmware version	Firmware version of the reader	
Driver type	Driver type of the serial interface of the reader	
Driver version	Driver version of the serial interface of the reader	
Interface	Used serial interface of the reader Possible values: RS232, RS422	
Transmission speed	Used transmission speed of the reader Possible values: 19.2; 57.6; 115.2; 921.6 Kbaud	
Distance limiting	Set transmit power of the reader (RF380R) The following values are possible:	
	Value	Meaning
	02	0.5 W
	03	0.75 W
	04	1.0 W
	05	1.25 W
	06	1.5 W
	07	1.75 W
	08	2.0 W
Max. number of transponders	Maximum number of transponders to be expected that may be located in the antenna field at the same time.	

Displayed parameters	Description
Transponder type	Set transponder type profile The following values are possible:
	Value Meaning
	00 RF300 (RF3xxT)
	01 ISO 15693 general
	03 MDS D3xx, Infineon
	04 MDS D4xx, Fujitsu - 2 KB
	05 MDS D1xx, NXP
	06 MDS D2xx, TI
	07 MDS D261, ISTM
	08 MDS D5xx, Fujitsu - 8 KB
	10 RF300 (RF3xxT)
	20 ISO 14443 (MOBY E, E6xx)
	31 General Mode
	40 P2P master
	41 P2P master & combined mode with ISO transponder (MDS Dxxx)
	50 P2P master & combined mode with RF300 transponder
	4F P2P slave
Antenna status	Status of the antenna
Presence check	Set presence check profile

Table 7- 20 Displayed parameters of the "Transponder status" area

Displayed parameters	Description
UID	Unique identifier of the transponder
Transponder type	Transponder type (vendor, identification)
Version	Version of the transponder chip
Lock status of the OTP area	Disabled blocks of the OTP area on the chip
Size of the user memory	Memory size of the user memory in bytes
Size of a memory block	Size of the memory blocks of the transponder chip
Number of memory blocks	Number of memory blocks of the transponder chip
Measured value power flux density	Radiant power that arrives at the transponder. The lower the value, the more power the transponder receives.
Passive error counter	Number of passive errors which occurred
Active error counter	Number of errors which occurred Sum of the signature and CRC errors
Presence counter	Time in [ms] that the transponder spent in the antenna field.

Error counter

The following error types are read and displayed:

Table 7- 21 Error types displayed in the "Error counter" area

Displayed error types	Description
FZP	Passive error counter This error counter is an indicator of a disturbed environment (interferences).
ABZ	Abort counter Counter for protocol errors on the air interface for which the transponder aborted communication.
CFZ	Code error counter Counter for disruptions or collisions on the air interface that caused communication to be disturbed.
SFZ	Signature error counter Counter for failed signature encryptions of written blocks of data. Only relevant for the transponder type "RF300".
CRCFZ	CRC error counter Counter for failed CRC checks
ASMFZ	Error counter for problems on the interface to the host (CM/PC) Counter for errors on the serial interface
Signal strength	
AMLI	AM power indicator Received signal strength [dB] for which amplitude modulation with the transponder was detected.
PMLI	PM power indicator Received signal strength [dB] for which phase modulation with the transponder was detected.

Note**Error counter readings**

The displayed error counter readings are counted from the last restart of the reader or the last manual reset of the error counter readings.

7.3.7 The "Diagnostics - Log" menu item

The log of the communication module is displayed in the "Diagnostics - Log" menu item.

The screenshot shows the SIMATIC RF188CI web interface. The left sidebar contains navigation links: Homepage, Settings, Diagnostics, Log, Service log, Syslog logbook, Edit transponder, User management, System, and Help. The 'Log' menu item is selected. The main content area displays a table of log entries. The table has three columns: Date / time, Type, and Entry. The entries include configuration successful messages, reader found messages, and error messages. At the bottom of the table, there are four buttons: Update, Total history, Save, and Reset.

Date / time	Type	Entry
05/27/2019 11:38:04.236	COMMON	Configuration successful. (Device: CM Command: setConfiguration)
05/27/2019 11:37:34.692	COMMON	Configuration successful. (Device: CM Command: setConfiguration)
05/27/2019 11:34:17.245	COMMON	Reader found at Port X22: Class MOBY FW version 3 1.7 HW type: 2 HW subtype: 0x0043 HW version 1.0 Loader version 1.0 Driver type 1 Driver version 1.2 MLFB
05/27/2019 11:34:16.644	COMMON	Configuration successful. (Device: CM Command: setParameter Parameter name: TagDeliveredEvents Parameter value: false)
05/27/2019 11:34:16.640	COMMON	Configuration successful. (Device: CM Command: setParameter Parameter name: FilterEvents Parameter value: false)
05/27/2019 11:34:16.635	COMMON	Configuration successful. (Device: CM Command: setParameter Parameter name: EventFilters Parameter value: NONE)
05/27/2019 11:34:16.629	COMMON	Configuration successful. (Device: CM Command: setParameter Parameter name: RssiEvents Parameter value: false)
05/27/2019 11:34:16.598	COMMON	Reader found at Port X23: Class MOBY FW version 3 1.7 HW type: 2 HW subtype: 0x0043 HW version 1.0 Loader version 1.0 Driver type 1 Driver version 1.2 MLFB
05/27/2019 11:34:16.583	COMMON	Reader found at Port X21: Class MOBY FW version 3 1.7 HW type: 2 HW subtype: 0x0043 HW version 1.0 Loader version 1.0 Driver type 1 Driver version 1.2 MLFB
05/27/2019 11:34:15.526	COMMON	Reader software (build: T01.01.00.00_01.11.06) started with configuration: Configuration ID = 5BB24B88, Data Version = V1.1.0
05/27/2019 11:34:14.839	ERRORS	start: Could not load user defined configuration! Seems it has an invalid data version. Delete it and use default configuration instead.
05/27/2019 11:34:14.836	ERRORS	checkVersions: Invalid CM model. Current CM model is SIMATIC_RF188CI
05/27/2019 11:19:26.654	COMMON	Configuration successful. (Device: CM Command: setConfiguration)
05/27/2019 11:15:24.863	COMMON	Reader found at Port X22: Class MOBY FW version 3 1.7 HW type: 2 HW subtype: 0x0043 HW version 1.0 Loader version 1.0 Driver type 1 Driver version 1.2 MLFB
05/27/2019 11:15:24.856	COMMON	Reader found at Port X23: Class MOBY FW version 3 1.7 HW type: 2 HW subtype: 0x0043 HW version 1.0 Loader version 1.0 Driver type 1 Driver version 1.2 MLFB
05/27/2019 11:15:24.719	COMMON	Configuration successful. (Device: CM Command: setParameter Parameter name: TagDeliveredEvents Parameter value: false)
05/27/2019 11:15:24.714	COMMON	Configuration successful. (Device: CM Command: setParameter Parameter name: FilterEvents Parameter value: false)
05/27/2019 11:15:24.709	COMMON	Configuration successful. (Device: CM Command: setParameter Parameter name: EventFilters Parameter value: NONE)
05/27/2019 11:15:24.703	COMMON	Configuration successful. (Device: CM Command: setParameter Parameter name: RssiEvents Parameter value: false)
05/27/2019 11:15:24.677	COMMON	Reader found at Port X21: Class MOBY FW version 3 1.7 HW type: 2 HW subtype: 0x0043 HW version 1.0 Loader version 1.0 Driver type 1 Driver version 1.2 MLFB
05/27/2019 11:15:23.490	COMMON	Reader software (build: T01.01.00.00_01.11.06) started with configuration: Configuration ID = 5BB24B88, Data Version = V1.1.0
05/27/2019 11:15:22.925	ERRORS	start: Could not load user defined configuration! Seems it has an invalid data version. Delete it and use default configuration instead.
05/27/2019 11:15:22.923	ERRORS	checkVersions: Invalid CM model. Current CM model is SIMATIC_RF188C
05/27/2019 10:46:52.961	COMMON	Configuration successful. (Device: CM Command: setConfiguration)
05/27/2019 10:45:24.359	COMMON	Configuration successful. (Device: CM Command: setConfiguration)

Figure 7-13 The "Diagnostics - Log" menu item

The menu item "Log" shows all message types that were selected in the menu item "Settings - General" in the "Log settings" area. This menu item documents the actions performed by the communication module.

The entries contain the following properties:

Table 7- 22 Displayed properties of the log messages

Property	Description
Date/time	Time stamp when the entry was made by the communication module. Note that the time stamp is generated by the device clock (UTC time). This time is compared with the time zone set on the PC and displayed accordingly.
Type	Type of message Which message types are signaled depends on the check boxes enabled in the menu item "Settings - General" in the "Log settings" area.
Entry	Text of the message

With the "Update", "Save as" and "Reset" buttons, you can control the entries:

- Update

The log is read in again by the communication module and the list is updated. The log entries displayed include the most current data (200 KB).

- Total history

The complete stored log of the communication module is read in. The log entries displayed include all saved data (10 MB).

- Save

The log read by the communication module is saved as a *.csv file on the PC.

- Reset

The log is deleted in the communication module.

With a large number of log entries in the history, it may take several minutes before these are displayed.

7.3.8 The "Diagnostics - Service Log" menu item

The service log of the communication module is displayed in the "Diagnostics - Service Log" menu item. The log records internal processes of the communication module and is required for service support by SIEMENS specialists. Only make settings on this page if you are instructed to do so by SIEMENS personnel. The log entries are also evaluated by SIEMENS personnel.

The "Diagnostics - Service Log" menu item is divided into the following areas:

- Log settings for service
- Service log

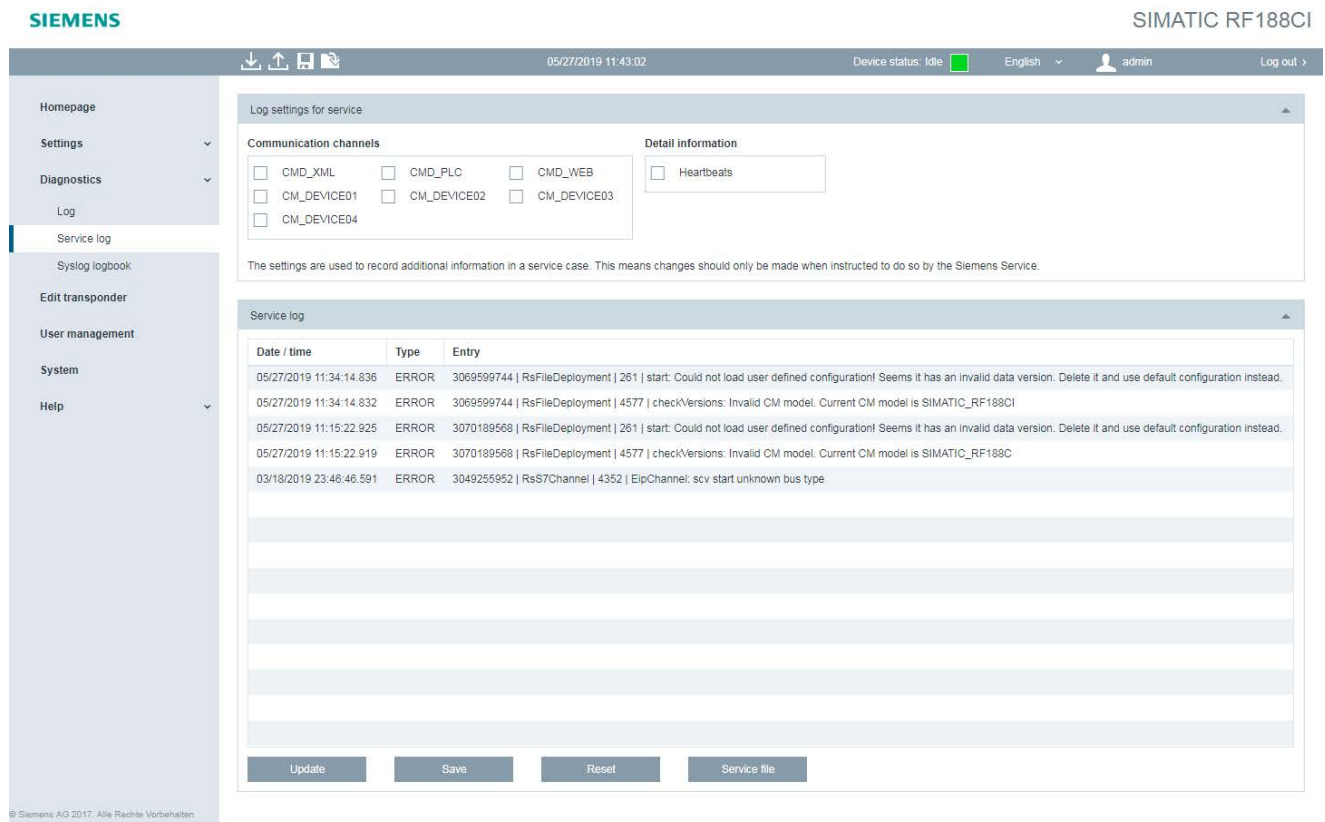


Figure 7-14 The "Diagnostics - Service Log" menu item

Log settings for service

In the "Log settings for service" area, you can define the message types that should be entered in the log.

Table 7- 23 Description of service log parameters

Parameter	Description
Communication channels	
CMD_XML	Frames on the XML interface
CMD_PLC	Internal frames on the PLC interface
CMD_WEB	Internal frames between Web server and reader
CM_DEVICE01	Frames on reader interface 1 (X21)
CM_DEVICE02	Frames on reader interface 2 (X22)
CM_DEVICE03	Frames on reader interface 3 (X23)
CM_DEVICE04	Frames on reader interface 4 (X24)
Detailed information	
Performance monitoring	Recording heartbeat telegrams in the service information. In this way, the log is kept free for user data.

Service log

The "Service log" area shows all the message types that were selected in the "Log settings for service" area.

The entries contain the following properties:

Table 7- 24 Displayed properties of the log messages

Property	Description
Date/time	Time stamp when the entry was made by the communication module. Note that the time stamp is generated by the device clock (UTC time). This time is compared with the time zone set on the PC and displayed accordingly.
Type	Type of message Which message types are signaled depends on the check boxes enabled in the menu item "Settings - General" in the "Log settings" area.
Entry	Text of the message

With the "Update", "Save as" and "Reset" buttons, you can control the entries:

- Update

The log is read in again by the communication module and the list is updated. The log entries displayed include the most current data (200 KB).

- Save

The log read out by the communication module is saved as a *.csv file.

- Reset

The log is deleted in the communication module.

- Service file

The log read out by the communication module is saved as an *.slf file. The service file contains additional information relevant to Siemens service personnel.

With a large number of log entries in the history, it may take several minutes before these are displayed.

7.3.9 The "Diagnostics - Syslog logbook" menu item

The menu item "Diagnostics - Syslog logbook" displays the logbook of the Syslog messages when the Syslog function is enabled. This page can only be called by users with administrator rights.

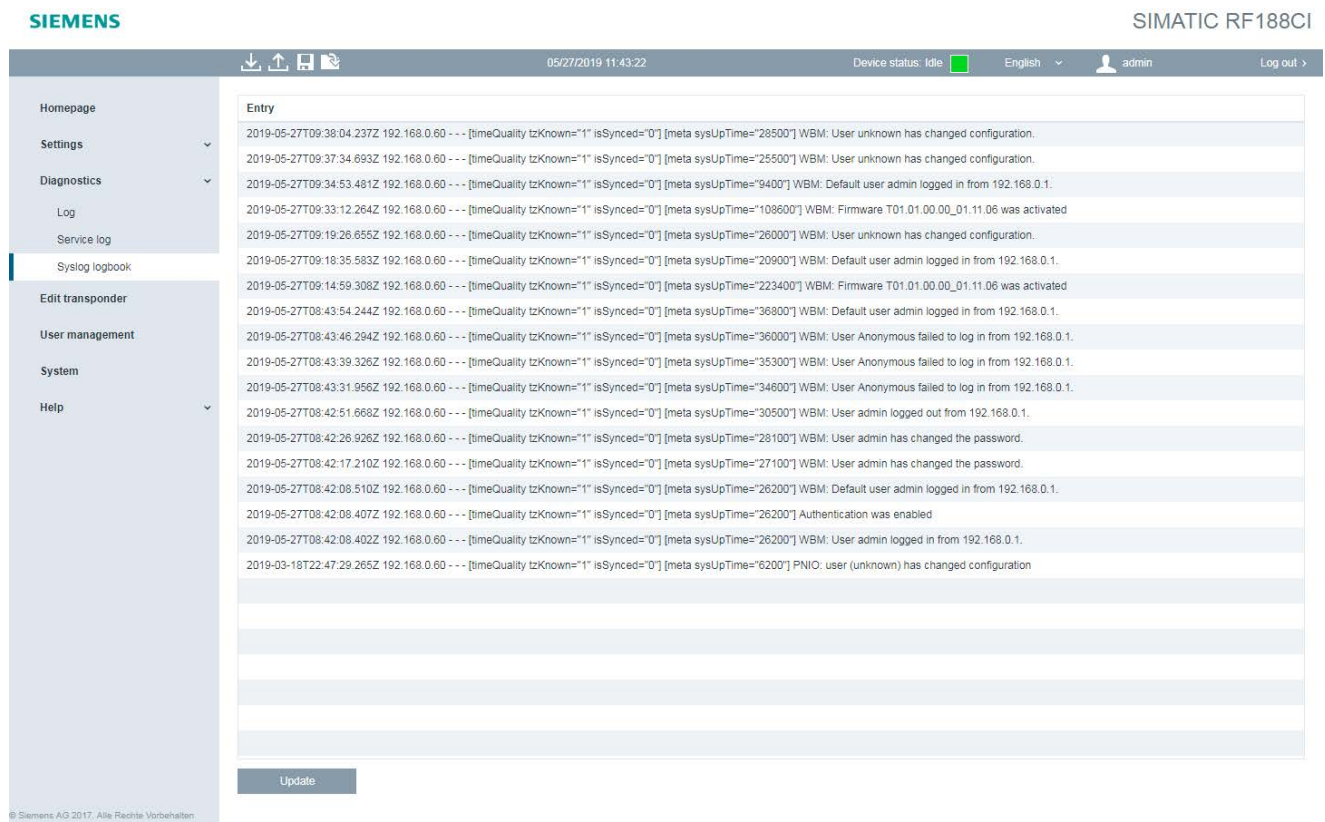


Figure 7-15 The "Diagnostics - Syslog logbook" menu item

All Syslog messages are displayed in the "Syslog logbook" menu item. This menu item documents all safety-related accesses to the communication module and actions performed. You can find detailed information on the Syslog messages, their structure and contents in the section "Syslog messages (Page 201)".

With the "Update" button you can read in the entries from the communication module again and update the list. The displayed log entries contain 128 KB of data.

7.3.10 The "Edit transponder" menu item

You can read out and write transponder data with the "Edit transponder" menu item. This page is divided into 2 areas:

- Basic settings
- Read/write

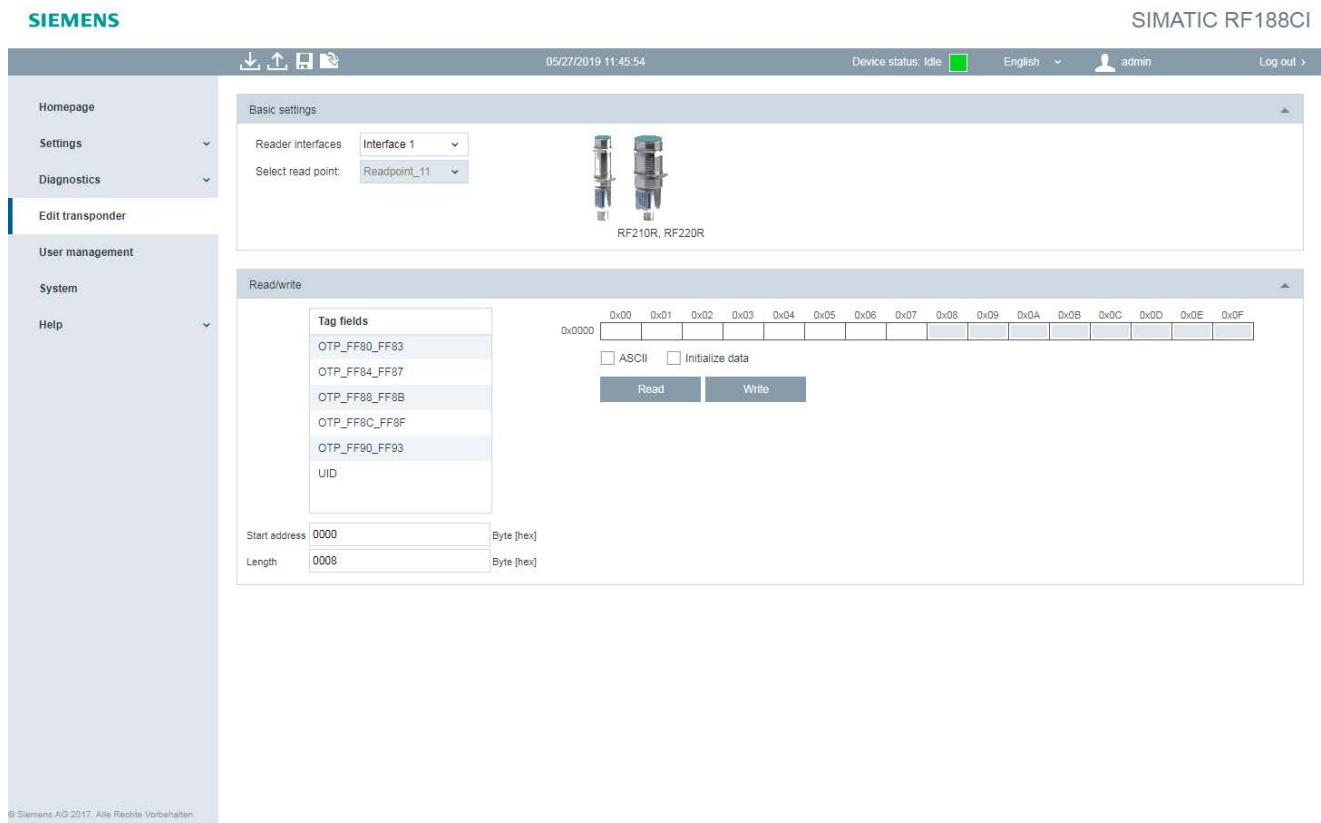


Figure 7-16 The "Edit transponder" menu item

Basic settings

This area enables you to select the reader or reader interface with which transponders are to be processed.

Read/write

In the "Read/write" area, you can read out and overwrite the memory areas. You can access pre-defined addresses (tag fields). Using the parameters, you can adapt the memory area manually.

Table 7- 25 Description of the parameters of the tag fields

Parameter	Description
Start address	Value of the start address of the data to be read/written.
	Value range 0 ... 65535 bytes
Length	Number of bytes to be read/written starting at the start address.
	Value range 1 ... 1024 bytes
Data	Input boxes for the values (HEX format).
	Possible characters 0 ... 9, A ... F
ASCII	Showing/hiding the ASCII view. When the ASCII view is active, the data is shown additionally in ASCII notation. You can edit the data both in the HEX format or in the ASCII format. You can choose between the two input modes "Overwrite" and "Insert".
Initialize data	Show/hide the view for initializing the data. Using the initialization function, you can preset the data fields.

Next to the list of tag fields, the data of the selected memory area is displayed in HEX view.

With the "Read" button, the data is read from the transponder. The data read from the transponder is highlighted in red to distinguish it from the data entered manually. If no values are displayed, this means that no values have yet been read from the transponder.

Click the "Write" button to transfer the changed data to the transponder.

NOTICE
Reading/writing transponder data with an established connection to the controller <p>Note that, if a connection to the controller is established, the configuration of the readers is performed via the controller. To enable transponder data to be read/written via the WBM, the connected readers must have been initialized via the S7 controller beforehand.</p>

7.3.11 The "User management" menu item

To be able to work with the user management function you first need to enable it. To do this, click the "Enable user management" button and confirm with "OK". The user management requires a secure connection using HTTPS. Change the connection and log in with an administrator login.

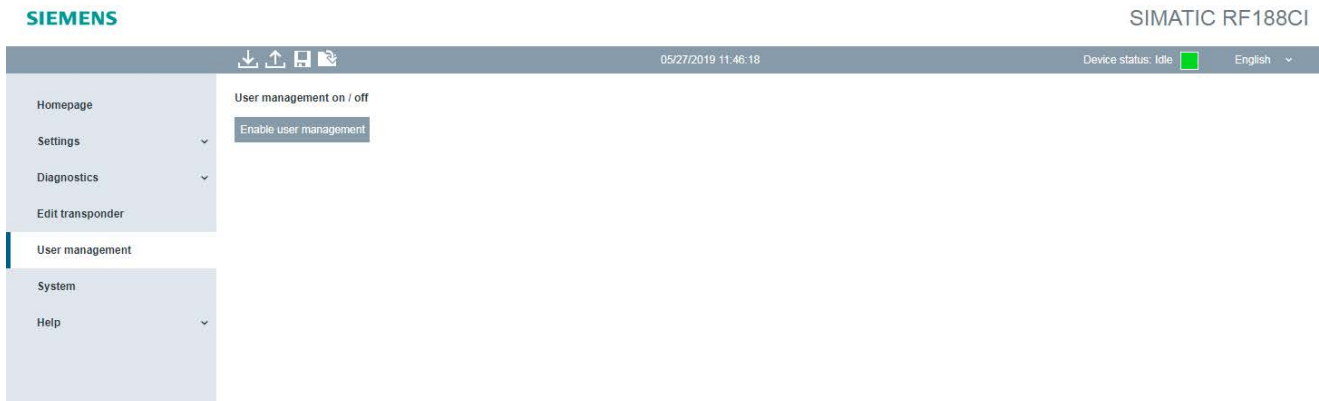


Figure 7-17 The "User management" menu item; "User management on / off"

Note

First login to WBM via HTTPS

Note that user administration can only be enabled by an administrator. During the first login as administrator, you must change the password for security reasons.

The communication modules are delivered with the following user profile pre-installed at the factory:

- User name: admin
- Password: admin

Using the "admin" user profile, you can create new user profiles and delete existing profiles.

NOTICE

Security recommendation: Enable user management

After starting the WBM the first time, no user management is enabled. To make sure that no unauthorized persons can access the CM settings, we recommend that you enable the user management and create new user profiles after the first login and delete the pre-installed profile.

Procedure

Proceed as follows to log in to the WBM:

1. Enter your user name in the "User" input box.
2. Enter your password in the "Password" input box.
3. Click the "Log in" button.

Result: You are logged onto the WBM and can now set communication module parameters.

The "User management" menu item

In the "User management" menu item, you can create, delete and edit user profiles and change passwords. This page is divided into the following areas:

- User profiles
- User properties
- Password
- Roles
- User management on / off

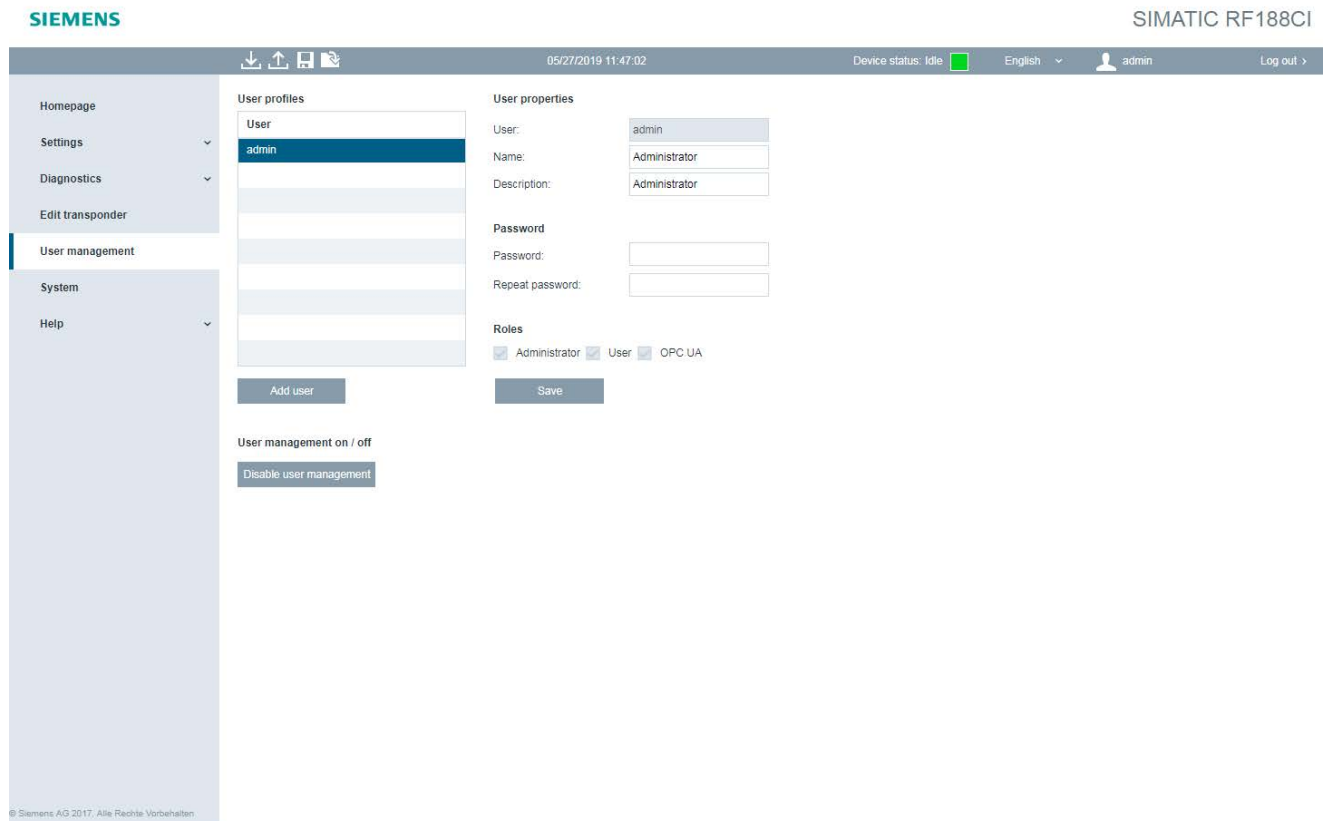


Figure 7-18 The "User management" menu item

User profiles

The "User profiles" area contains a list of all existing user profiles. Up to a maximum of 32 user profiles can be created. To edit a user profile, select the required user name in the list. The selected user name is highlighted in color.

Click the "Add new users" button to create a new user. Click the "Delete" button to delete a selected user profile.

User properties

In the "User" text box, enter the name of the newly created user profile. You require the user name and the password to log in to the WBM. The user name cannot be edited later.

In the "Name" input box, you can enter the name of the person or the name of the group that works with the user profile. In the "Description" input box, you can enter further information about the user profile.

Password

Enter the password of the user profile in the "Password" and "Repeat password" input boxes. You require the user name and the password to log in to the WBM. User passwords can be changed by the users themselves or an administrator. The strength of your password is indicated by color and text.

If you lose your administrator password, you must reset the communication module to the factory settings as described in the section "Restoring the factory settings manually (Page 173)".

Roles

In the "Roles" area, you can assign roles to the user profile. Click the relevant check box to assign the required roles to the user profile. The "Administrator" role has all read/write rights

- Users

Restricted user profile with read/write rights. As "User", you cannot create new user profiles or edit other user profiles. In addition to this, as the "user", you cannot write to the reader in the "Run" reader status.

- Administrator

User profile with all read/write rights

- OPC UA

Restricted user profile with OPC UA rights. As an "OPC UA" user, you can only log onto the OPC UA connection. This role has no rights whatsoever in the WBM and it cannot be used to log on to the WBM.

Click the "Save" button to save the changes and to create the new user profile.

Note

Restrictions when transferring the configuration

Note that you as "User" can only transfer changes when the device status of the communication module is "Idle". As an "administrator", you can also transfer changes even when the device status is "Run".

The following table provides you with an overview of the menu items that are restricted for the "User" role:

Table 7- 26 Restrictions for the "User" role

Menu items		Restrictions
Start page		<ul style="list-style-type: none"> • Restricted: Input boxes cannot be filled. • No operator control is possible in the "Run" device status.
Diagnostics		
	Hardware diagnostics	No operator control is possible in the "Run" device status.
	Log	Restricted: The log cannot be reset.
	Syslog log	The page is not displayed.
Edit transponder		No operator control is possible in the "Run" device status.
User management		Restricted: Only the user's own password can be changed.
System		No operator control is possible in the "Run" device status.

In addition, changes cannot be transferred to the communication module using the "Transfer configuration to communication module" button as long as an active communication connection exists.

User management on / off

Click the "Disable user management" button if you want to disable user management again. Note that any user has all read/write privileges (administrator rights) when user administration is disabled.

7.3.12 The menu item "System - System settings"

In the "System - System Settings" menu item, you can update firmware, reset the communication module to the factory settings, change the IP address of the communication module, load certificates on the communication module and transfer control files to the PC. This page is divided into the following areas:

- Firmware update
- Reset
- IP address
- HTTPS certificate
- Device description files

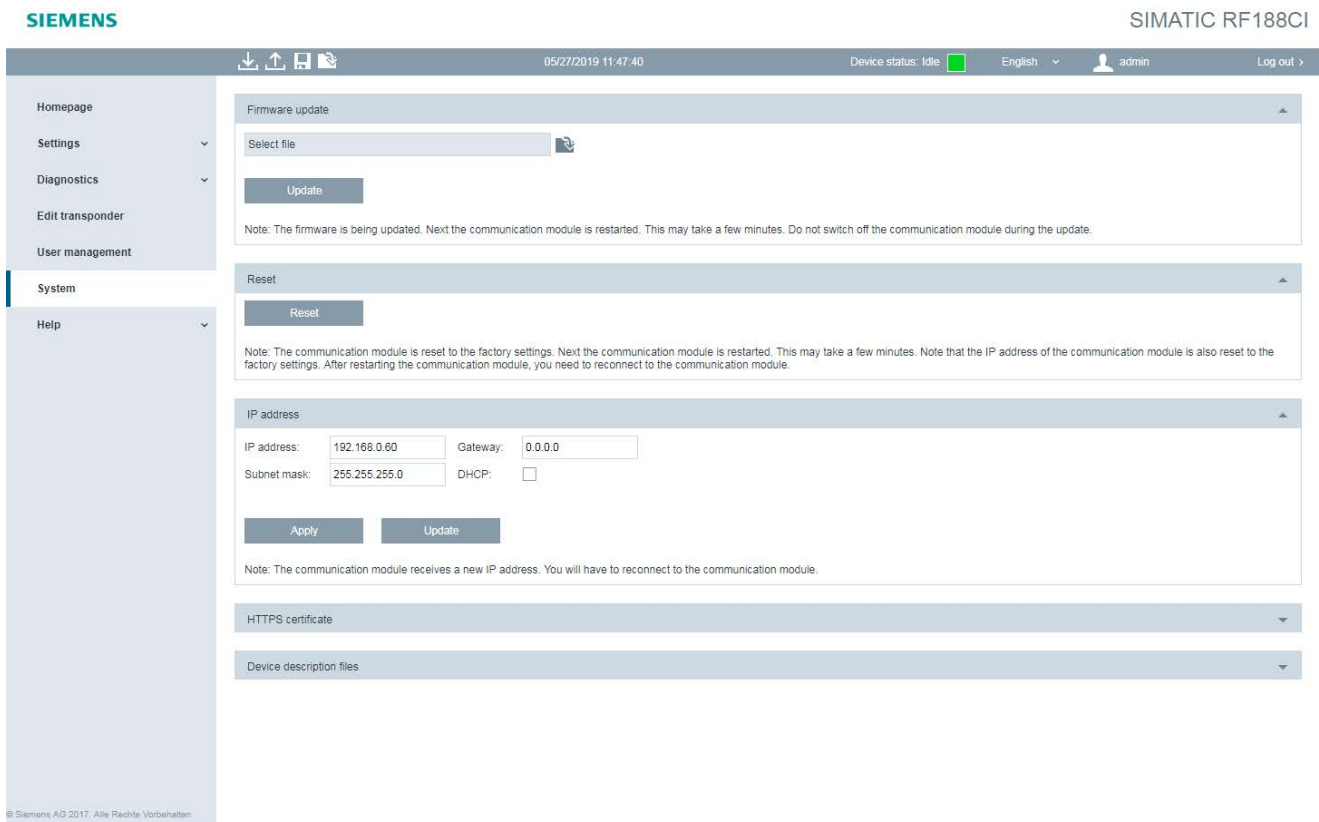


Figure 7-19 The menu item "System - System settings"

Firmware update

In the "Firmware update" area, you can update the firmware of the communication module. For a detailed description of firmware updates, refer to the section Firmware update (Page 166).

Reset

In the "Reset" area, you can reset the communication module to the factory settings. When you reset the communication module, all set configuration data, settings of the user management and address information are lost.

To reset the communication module to the factory settings, click the "Reset" button. After the reset, the communication module is automatically restarted. Note that, after this, you need to assign a new IP address to the communication module.

If you lose your administrator password, you must reset the communication module to the factory settings as described in the section "Restoring the factory settings manually (Page 173)".

IP address

In the "IP address" area, you can change the IP address, subnet mask, and gateway of the communication module. As an alternative, the IP address can be obtained from a DHCP server.

Note

Support of option "12"

When the address is assigned via DHCP, the option "12" (hostname) is also supported. The host name can be taken from the SNMP variable "sysName".

The variable can be written using SNMP tools.

HTTPS certificate

In the "HTTPS certificate" area, you can transfer certificate files and certificate key files to the communication module. Remember that you first need to import the data into the communication module before you can activate it.

Using the certificates, you can integrate the communication module in your specific security infrastructure. Certificates are used to check the identity of a person or a device, to authenticate a service or to encrypt files. You can create your own certificates or use official certificates created by a certification authority. You can import certificates that contain a certificate as well as a private key (PKCS#12). When you import certificates and the associated private keys in separate files, then both files must be coded either in "ASN.1" or "Base64".

You can use the "Create CSR" button to create a certificate signing request (CSR). The CSR file contains all relevant information of the installed server certificate. A CA (Certificate Authority) can create a signed, module-specific server certificate using this file that you can then import into this module.

Contact your administrative IT department for further information on the topic of certificates.

Device description files

The GSDML and ESD files current at the time of delivery as well as the OPC UA device description file are stored on the communication module. Click the "Save on PC" button to transfer device description files to the connected PC. You can use these files to integrate the communication modules into the configuration software of your S7 and Rockwell controllers.

7.3.13 The menu command "System - Reader firmware"

In the "System - Reader Firmware" menu item, you can update the firmware of the readers connected to the communication module.

- Basic settings
- Firmware update

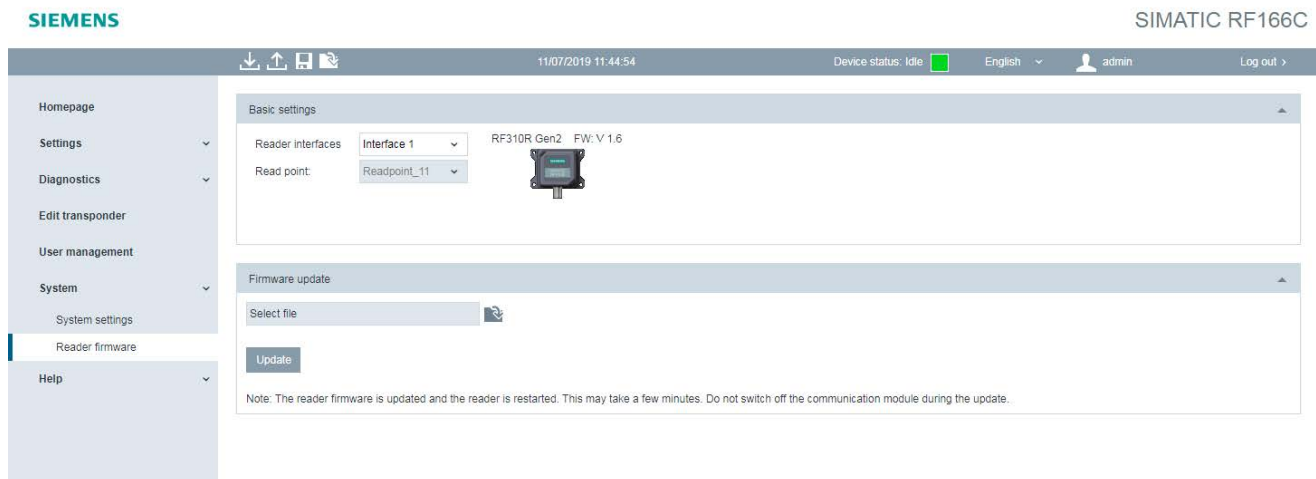


Figure 7-20 The menu command "System - Reader firmware"

Basic settings

In this area, you can use the "Reader interfaces" parameter to specify the reader for which a firmware update is to be performed. Depending on the connected reader, you can select the desired reading point.

Firmware update

In the "Firmware update" area, you can update the firmware of the selected reader. For a detailed description of firmware updates, refer to the section "Firmware update (Page 166)".

7.3.14 The "Help" menu item

Service and Support

The "Help - Service and Support" menu item includes information on the RF18xC und RF18xCi communication modules, the WBM as well as links to the relevant documents and the Siemens Industry Online Support.

Operating Instructions

With the "Help" menu item, you can find the manual for the corresponding communication module, "SIMATIC RF185C, RF186C RF188C, RF186CI, RF188CI".

Programming via SIMATIC controller



This section is intended only for S7 users.

You can program and configure the SIMATIC RF185C, RF186C, RF188C as well as the RF186CI and RF188CI communication modules using Ident instructions via a SIMATIC controller.

To configure Ident systems using STEP 7 Basic / Professional (TIA Portal), you need appropriate Ident instructions. The Ident profile and the Ident blocks are integrated in STEP 7 as of version V13.1.

You can find a detailed description of the Ident profile and the Ident blocks in the "Ident profile and Ident blocks, standard function for Ident systems (<https://support.industry.siemens.com/cs/ww/en/view/109762333>)" function manual.

8.1 Digital inputs/outputs

The RF18xCI communication modules have configurable digital inputs/outputs that you can configure using the WBM. You will find more information on this in the section "The "Settings - Digital outputs" menu item (Page 78)".

You can operate the interface as a single input (DI 0) or a single output (DO 0 and PI 0), as needed, or you can connect an IO-Link module. IO-Link modules with up to 8 inputs and/or 8 outputs are supported.

The inputs/outputs are mapped in a data word each in the process image of the controller. Because the physical output value of the CM can deviate from the process image value of the controller through internal linking, each physical output value is also mapped as additional input in the controller.

Table 8- 1 Assignment of the digital inputs/outputs

Byte 1								
Bit	7	6	5	4	3	2	1	0
Input	PI 7	PI 6	PI 5	PI 4	PI 3	PI 2	PI 1	PI 0
Output	--	--	--	--	--	--	--	--
Byte 0								
Bit	7	6	5	4	3	2	1	0
Input	DI 7	DI 6	DI 5	DI 4	DI 3	DI 2	DI 1	DI 0
Output	DO 7	DO 6	DO 5	DO 4	DO 3	DO 2	DO 1	DO 0

PI: Physical output value

DI: Digital input value

DO: Digital output value

Programming via XML



This section is intended only for XML users.

You can program the communication modules via the XML interface using XML commands. You can find detailed information on the XML diagnostic functions in the "XML programming for SIMATIC Ident (<https://support.industry.siemens.com/cs/ww/en/ps/14971/man>)" manual.

Programming via OPC UA



This section is intended only for OPC UA users.

OPC UA basics

OPC UA is a standardized communication protocol. It allows data exchange between all types of industrial devices that support OPC UA and that are integrated in the same network. In this context, devices that provide or publish data, information and command calls are known as OPC UA servers. Devices that use this data, information and these command calls are known as OPC UA clients.

Using OPC UA, you can also integrate the communication modules into cloud systems or communicate with them.

Knowledge of fundamental OPC mechanisms as well as programming know-how is indispensable for understanding the following section and implementing your own OPC UA client for use with the communication modules. The OPC UA standard specifications will help you here.

The standard "OPC Unified Architecture for AutoID Companion Specification" was defined by the organizations "AIM Germany" and "OPC Foundation". This describes the connection of identification devices via OPC UA. The identification devices can be subdivided as follows:

- Text recognition devices (OCR)
- Optical readers (e.g. barcode)
- RFID reader and
- Devices for localization (RTLS).

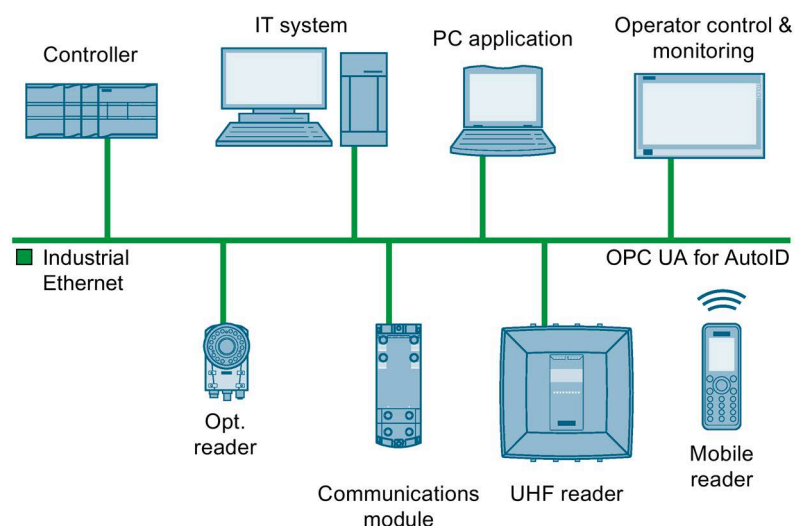


Figure 10-1 Ident devices in an OPC UA network

You will find more information on OPC UA on the pages of the "OPC Foundation (<https://opcfoundation.org/>)". The "OPC Unified Architecture for AutoID Companion Specification" can be obtained via the "AIM Germany (www.aim-d.de)".

All SIMATIC communication modules have implemented OPC UA servers with the range of functions for RFID devices defined by "OPC Unified Architecture for AutoID" (Release 1.00). For this, "OPC Unified Architecture for AutoID" defines the "AutoIDDevice" and, derived from this, the "RfidReaderDevice". With the communication modules, each reader interface stands for a read point and thus for an independent "AutoIDDevice" or "RfidReaderDevice".

Note that depending on the connected terminal device, not all methods/functions defined in the "AutoIDDevice" can be used in a sensible manner (e.g. antenna power).

An XML device description file, for connection of the communication module via OPC UA, is stored on the communication module and can be downloaded via the WBM ("System > Device description file").

10.1 Supported methods/functions

Parallel to regular operation via PC or SIMATIC controller, you can read out the results of the SIMATIC commands and diagnostic information via the Ethernet interface using OPC UA and make them available to another application. Note that only read-only accesses are supported during the parallel operation of the communication modules via OPC UA. In this case, all control or write accesses, as well as calls of methods and setting of variables described in the following, are not supported.

Requirements

- The maximum five permitted OPC UA client connections are not dependent on the read points. Note that multiple clients can also work with one read point.
- An OPC UA client that wishes to use the full RFID functionality of the readers connected to a communication module needs to support the following fundamental OPC UA access mechanisms:
 - Data Access (DA)
 - Events
 - Methods

OPC UA basic methods/basic functions

The integrated OPC UA servers of the communication modules support the following OPC UA basic methods/basic functions:

- OPC UA server basic functions according to the "Micro Embedded Device Server Profile" of the OPC Foundation.

As an extension of the "Micro Embedded Device Server Profile":

- "Standard Event Subscription Server Facet"
- "SecurityPolicy - Basic256"
- "SecurityPolicy - Basic 256Sha256"
- Maximum 5 OPC UA client connections
- "Full AutoID Server Facet" according to the specification "OPC Unified Architecture for AutoID" (Release 1.00). Each reader interface stands for a read point and thus for an independent "AutoIDDevice" or "RfidReaderDevice". This means that each communication module supports as many read points as the number of devices that can be connected.
- On a communication module, an OPC UA client can be connected as a main application or as a second application connected in parallel to a PROFINET, PROFIBUS, EtherNet/IP or XML main application.

For an OPC UA client to also be able to connect in case of a PROFINET, PROFIBUS, EtherNet/IP or XML main application, the "Parallel" parameter must be selected in the WBM in the "Communication > OPC UA" menu. This case is intended purely for diagnostics purposes, so write access is no longer possible here for OPC UA clients.

The assignment of the OPC UA read points to the connected devices is derived from the read point names. You can find these in the read point attributes.

Table 10- 1 Assignment of read points; example based on an RF188C

Reader interface	BrowseName	DisplayName ¹⁾
1	Read_point_1	Readpoint_11
2	Read_point_2	Readpoint_21
3	Read_point_3	Readpoint_31
4	Read_point_4	Readpoint_41

¹⁾ The DisplayName can be adapted.

Each OPC UA server publishes to the OPC UA clients its OPC UA functionalities via nodes in its address area. You can find the read points or "RfidReaderDevices" under the node "Objects > DeviceSet" in the address area of the OPC UA server of the communication modules.

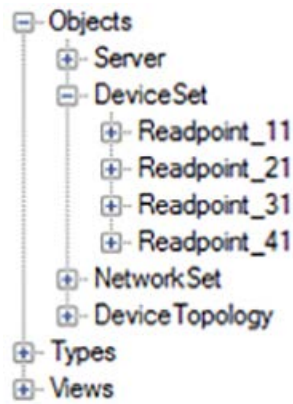


Figure 10-2 Node "Objects > DeviceSet"

You will find the methods/functions listed below under the following path in the address area of a read point "Objects > DeviceSet > Readpoint_x1".

RFID-specific methods / functions

The integrated OPC UA servers of the communication modules support the following RFID-specific methods/functions according to the "OPC Unified Architecture for AutoID" for each read point:

Table 10- 2 RFID-specific methods / functions

OPC UA methods		
	Scan	Synchronous execution of inventories The detected transponders are directly returned.
	ScanStart, ScanStop	Trigger the read points to start inventories. The detected transponders are delivered by means of events (Rfid-ScanEventType).
	KillTag	Destroy transponders. This function is only supported by UHF readers.
	LockTag	Lock areas on the transponder. This function is only supported by UHF readers.
	SetTagPassword	Set transponder-specific passwords. This function is only supported by UHF readers.
	ReadTag	Read out transponder data.
	WriteTag	Write transponder data.

OPC UA events		
	RfidScanEventType	Receive "TagEvents".
OPC UA variables (read only)		
	AntennaNames	Antennas of read point
	AutoldModelVersion	Version of the supported AutoID model
	DeviceInfo	Information on the communication module (e.g. information on the device)
	DeviceLocationName	Information on the communication module (e.g. information on the location)
	DeviceManual	URL to the manual for the communication module
	DeviceName	DisplayName of the read point
	DeviceRevision	Reserved
	DeviceStatus	Device status of read point
	HardwareRevision	Hardware version of the communication module
	LastScanData	Most recently scanned transponder of the read point (Scan, ScanStart).
	Manufacturer	Manufacturer (always "Siemens AG")
	Model	Variant of the communication module
	RevisionCounter	Always "-1"
	SerialNumber	Serial number of the communication module
	SoftwareRevision	Software version of the communication module

Refer to the "OPC Unified Architecture for AutoID" specification for a more detailed description of the methods/functions.

You can refer to the XML device description file "SimaticIdent.RFxxxx.xml" supplied with each communication module for the IDs of the nodes described here. An XML device description file is stored on the communication module and can be downloaded via the WBM ("System > Device description file"). Alternatively, you can also find the node IDs through browsers by means of a generic OPC UA client through the address area of the server.

Additional functions

The integrated OPC UA servers of the communication modules offer additional functions and diagnostic options as a supplement to the AutoID standard. The following table provides an overview of the additional functions. The individual elements are described in greater detail below the table.

Table 10- 3 Additional functions

OPC UA events		
	AutoldDiagnosisEvent	Diagnostic events for the communication module
	RfidLastAccessEvent	Event for the last transponder access
	AutoldLastLogEntryEvent	Event for the last log entry
	AutoldPresenceEvent	Event for the presence of transponders
OPC UA variables		
	ExecuteScan	Read point scans for transponders.
	SimaticIdentModelVersion	Version information of the supported SIMATIC Ident OPC UA model
	CommonSettings	General settings
	CodeTypes	Definition of the data type for all AutoID identifiers with methods or events. <ul style="list-style-type: none"> Variable "LastScanData" Diagnostics variable "Identifier" Union "ScanData"
	CodeTypesRWDData	Definition of the data type of the "RWDData" diagnostics variable
	DeviceClock	Device clock of the communication module
	RfidSettings	RFID-specific settings
	MinRssi	Lowest accepted RSSI value of the antenna This function is only supported by UHF readers.
	RfPower	Radiated power of the antenna
	Diagnosis	Diagnostics information
	Presence	Presence of transponders

	Diagnosis - LastAccess	Various information on the last successful transponder access or command
	Client	Client interface via which the last transponder access took place.
	Command	Command that was executed during the last transponder access operation.
	Identifier	Transponder which was accessed with the last command.
	Timestamp	Time of the last transponder access
	RWData	Read/written data of the last command. Only possible with commands for reading/writing the transponder memory.
	Antenna	Antenna via which the transponder was accessed with the last command.
	CurrentPowerLevel	Power with which the last command was executed on the transponder. This function is only supported by UHF readers.
	PC	Protocol Control Word of the transponder that was accessed last. This function is only supported by UHF readers.
	Polarization	Polarization with which the last command was executed on the transponder. This function is only supported by UHF readers.
	Strength	RSSI value with which the last command was executed on the transponder. This function is only supported by UHF readers.
	Diagnosis - Logbook	Various log information.
	LastLogEntry	The last entry in the log.
	LogColumns	The headers column of the log as formatted string
	DigitalIOPorts	Digital IO ports
	DigitalInputs	Digital inputs of the communication module This function is only supported by the CI variants of the communication modules.
	DigitalOutputs	Digital outputs of the communication module This function is only supported by the CI variants of the communication modules.

You can find the specified functions under the following path in the address area of a read point:

- DeviceSet > Readpoint_x1 > IOData
- DeviceSet > Readpoint_x1 > RuntimeParameters

10.2 OPC UA variables

10.2.1 Description of the variables

OPC UA variables represent a simple way to query information from the communication modules or make settings on the communication modules. Almost all OPC UA clients support variables. However, you need to observe the following points when using variables:

The restriction of the update rate by the "Sampling" interval and by the "Publishing" interval is common to all OPC UA variables. These are fundamental OPC mechanisms that can define the intervals at which the values can be updated or queried via OPC UA. If the intervals at which the values for a variable are updated from a process should be shorter than the defined intervals, values can be overwritten before the query by an OPC UA client.

This problem is worsened by the use of logically related variables. If it is not possible to determine in time that related variables can be queried completely by the client before variables are written with new values again from the process, usage is not possible. If a client supports events, make sure that these are used. The effects described above cannot occur with events.

10.2.2 ExecuteScan

Table 10- 4 ExecuteScan

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/ExecuteScan
Data type	Boolean
Access	R/W
Description	Indicates whether the read point is currently scanning for transponders or allows the scan process to be activated/deactivated.
Possible values	<p>Query of the current status:</p> <ul style="list-style-type: none"> • TRUE: Read point scans for transponders. • FALSE: Read point does not scan for transponders. <p>Set:</p> <ul style="list-style-type: none"> • TRUE: The scan process of the read point for transponders is activated. • FALSE: The scan process of the read point for transponders is deactivated.

10.2.3 SimaticIdentModelVersion

Table 10- 5 SimaticIdentModelVersion

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/SimaticIdentModelVersion
Data type	String
Access	R
Description	Indicates the version of the OPC UA module.
Possible values	Example: V1.1.0

10.2.4 CommonSettings

You can make basic settings on the communication module using these variables.

Table 10- 6 CodeTypes

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/CommonSettings/CodeTypes
Data type	UInt32
Access	R/W
Description	<p>Definition of the data type for all AutoID identifiers in "AutoID Standard".</p> <p>The setting has an effect specifically on the data type of the "LastScanData", variable, the "Identifier" diagnostics variable and the "ScanData" union used for the "Identifier" in methods or events.</p> <p>The types "String", "ByteString" and "ScanDataEpc" are supported. The type definition of "CodeTypes" is "MultiStateDiscreteType". This means that the variable has an "Enum" that indicates the supported data types as "Property".</p>
Possible values	<ul style="list-style-type: none"> • 0: ByteString • 1: String • 2: ScanDataEpc

Table 10- 7 CodeTypesRWData

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/CommonSettings/CodeTypesRWData
Data type	UInt32
Access	R/W
Description	<p>Definition of the data type for the "RWData" diagnostics variable and the "ScanData" union used for "RWData" in the "RfidLastAccessEvent".</p> <p>The types "String", "ByteString" and "ScanDataEpc" are supported. The type definition of "CodeTypesRWData" is "MultiStateDiscreteType". This means that the variable has an "Enum" that indicates the supported data types as "Property".</p>
Possible values	<ul style="list-style-type: none"> • 0: ByteString • 1: String • 2: ScanDataEpc

Table 10- 8 DeviceClock

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/CommonSettings/DeviceClock
Data type	UtcTime
Access	R/W
Description	<p>The internal device clock of the communication module</p> <p>The communication module loses the time when it is switched off. The time can be applied after switch-on by this variable via the application.</p>
Possible values	<p>Example:</p> <p>2018-05-29T08:29:15.812Z</p>

10.2.5 RfidSettings

You can make the RFID settings on the communication module using these variables.

Table 10- 9 MinRssi

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/RfidSettings/Antennaxx/MinRssi
Data type	Int32
Access	R/W
Description	<p>Lowest accepted RSSI value of an antenna</p> <p>Transponders which are detected with a lower RSSI value are counted as not detected. This is a value without a unit and without direct reference to the power strength.</p> <p>This variable is only supported by UHF readers.</p>
Possible values	0 ... 255

Table 10- 10 RfPower

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/RfidSettings/Antennaxx/RfPower
Data type	SByte
Access	R/W
Description	Radiated power of the antenna
Possible values	<p>0 ... 127</p> <p>The special features of the different reader types are described below:</p> <p>With RF380R:</p> <ul style="list-style-type: none"> • 2: 0.5 W • 3: 0.75 W • 4: 1.0 W • 5: 1.25 W • 6: 1.5 W • 7: 1.75 W • 8: 2.0 W <p>Settings outside the specified values mean that the default value of 1.25 W is used.</p> <p>For UHF readers:</p> <p>Radiated power of the antenna in [dB]</p> <ul style="list-style-type: none"> • 0 • 5 ... 33 <p>Settings outside of the specified values are set to the respective area limits (1-4 → 5; 34-127 → 33).</p>

10.2.6 Diagnosis

These variables serve diagnostics and tracking purposes of the plant via OPC UA. You can use these variables both with an OPC UA application and with a PROFINET application as main application.

Requirements

- OPC UA application

For the diagnostics values to be available also in the case of an OPC UA application as main application, the "Diagnostics" option needs to be set in WBM.

- PROFINET, PROFIBUS, EtherNet/IP or XML application

For an OPC UA client to be able to connect in addition in case of a PROFINET, PROFIBUS, EtherNet/IP or XML application as the main application, the "Parallel" option needs to be enabled in the WBM. In this case, the Diagnostics option is automatically enabled as well. Please note that write access is no longer possible for OPC UA clients as soon as the "Parallel" option is set.

Diagnostics - Presence

Table 10- 11 Presence

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/Presence
Data type	UInt16
Access	R
Description	Shows the presence of transponders. The prerequisite is that the reader supports "Presence" mode and is operated in this mode, and that the option "Parallel" or "Diagnostics" is set in the WBM.
Possible values	<ul style="list-style-type: none"> • 0: There is no transponder in the antenna field • 1: There is at least one transponder in the antenna field • >1: Exact number of transponders (if supported by the reader)

Diagnostics - LastAccess

These variables supply various information on the last successful transponder access or command.

Please note that these variables supply logically related information. With successful transponder access, the contents of the "Time stamp" will be written last; all other supported "LastAccess" variables are filled first. These variables can thus serve as a trigger for an OPC UA client in order to query the other variable values.

If it is not possible to determine in time that variables can be queried completely by the client before the next transponder access takes place and variables are written with new values again from the process, usage is not possible. If this is not possible, use the "AutoldLastAccessEvent" events, which are also supported by the communication modules.

Table 10- 12 Client

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/LastAccess/Client
Data type	String
Access	R
Description	<p>Diagnostics on the last transponder access</p> <p>Indicates the client interface via which the last transponder access to this read point took place.</p> <p>The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.</p>
Possible values	<ul style="list-style-type: none"> • PNIO: Access via PROFINET • OPCUA: Access via OPC UA • WBM: Access via WBM • XML1: Access via the XML channel 1 • XML2: Access via the XML channel 2 • XML3: Access via the XML channel 3 • XML4: Access via the XML channel 4 • EIP: Access via EtherNet/IP • PB: Access via PROFIBUS • READPOINT: internal access via the read point <p>The read points of the device can scan for transponders independently. This is the case, for example, when at least one user application has started an asynchronous scan command or when a configured trigger was started with RF600. These events can also overlap in which case they can no longer be clearly assigned. In this case, the value "READPOINT" is always used instead.</p>

Table 10- 13 Command

Path	/Root/Objects/DeviceSet/Readpoint_x/RuntimeParameters/Diagnosis/LastAccess/Command	
Data type	String	
Access	R	
Description	<p>Diagnostics on the last transponder access</p> <p>Outputs the command executed during the last transponder access operation.</p> <p>The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.</p>	
Possible values	Depending on the client interface used:	
	PNIO, PB, EIB (Ident profile): <ul style="list-style-type: none"> • INVENTORY • WRITE-ID • KILL-TAG • LOCK-TAG-BANK • PHYSICAL-READ • PHYSICAL-WRITE • FORMAT • TAG-STATUS • GET • PUT • NEXT 	PNIO, PB (FB 45): <ul style="list-style-type: none"> • WRITE • READ • INIT • MDS-STATUS
	OPC UA: <ul style="list-style-type: none"> • Scan • ReadTag • WriteTag • KillTag • LockTag • SetTagPassword • Read • Write 	WBM, XML: <ul style="list-style-type: none"> • readTagIDs • writeTagID • readTagMemory • writeTagMemory • killTag • lockTagBank • getTagStatus
	READPOINT: <ul style="list-style-type: none"> • Observed 	--

Table 10- 14 Identifier

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/LastAccess/Identifier
Data type	Defined as "BaseDataType" The actual data type is defined during runtime by the "Code-Types" variable. The types "String", "ByteString" and "ScanDataEpc" are supported.
Access	R
Description	Diagnostics on the last transponder access Outputs the UID or EPC of the transponder that was accessed with the last command. The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.
Possible values	Example (RF300 reader, data type string): 000000005575B67D

Table 10- 15 Timestamp

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/LastAccess/Timestamp
Data type	UtcTime
Access	R
Description	Diagnostics on the last transponder access Outputs the time of the last transponder access. The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.
Possible values	Example: 2018-05-29T08:29:15.812Z

Table 10- 16 RWDATA

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/LastAccess/Rfid/RWData
Data type	Defined as "BaseDataType" The actual data type is defined during runtime by the "Code-TypesRWData" variable. The types "String", "ByteString" and "ScanDataEpc" are supported.
Access	R
Description	Diagnostics on the last transponder access Outputs the read/written data of the last command. Only possible with commands for reading/writing the transponder memory. The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.
Possible values	Example (RF300 reader, data type string): 0011223344556677

Table 10- 17 Antenna

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/LastAccess/Rfid/Antenna
Data type	Int32
Access	R
Description	<p>Diagnostics on the last transponder access</p> <p>Indicates the antenna via which the transponder was accessed with the last command.</p> <p>The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.</p>
Possible values	<p>Two-digit number</p> <p>The first digit stands for the read point index, the second digit for the antenna index within the read point.</p> <p>Example:</p> <ul style="list-style-type: none"> • Read point 1, antenna 1: 11 • Read point 2, antenna 1: 21

Table 10- 18 CurrentPowerLevel

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/LastAccess/Rfid/CurrentPowerLevel
Data type	Int32
Access	R
Description	<p>Diagnostics on the last transponder access</p> <p>Outputs the power with which the last command was executed on the transponder. This variable is only supported by UHF readers.</p> <p>The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.</p>
Possible values	<p>Decimal number for the power in [dB]</p> <p>Increment: 0.25 dB</p> <ul style="list-style-type: none"> • 0 • 5.00 ... 33.00

Table 10- 19 PC

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/LastAccess/Rfid/PC
Data type	UInt16
Access	R
Description	<p>Diagnostics on the last transponder access</p> <p>Outputs the protocol control word of the transponder that was accessed last. This variable is only supported by UHF readers. The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.</p>
Possible values	<p>Example:</p> <p>3000</p>

Table 10- 20 Polarization

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/LastAccess/Rfid/Polarization
Data type	String
Access	R
Description	<p>Diagnostics on the last transponder access</p> <p>Outputs the polarization with which the last command was executed on the transponder. This variable is only supported by UHF readers. The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.</p>
Possible values	<ul style="list-style-type: none"> • Default • Circular • Linear_vertical • Linear_horizontal

Table 10- 21 Strength

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/LastAccess/Rfid/Strength
Data type	Int32
Access	R
Description	<p>Diagnostics on the last transponder access</p> <p>Outputs the RSSI value with which the last command was executed on the transponder. This variable is only supported by UHF readers. The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.</p>
Possible values	0 ... 255

Diagnostics - Log

These variables supply various log information of the communication module.

Table 10- 22 LastLogEntry

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/Logbook/LastLogEntry
Data type	String
Access	R
Description	Log diagnostics The last entry in the log is output. The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.
Possible values	Example: 2018-05-30T13:14:43.546+00:00 COMMANDS readTagIDs CMD 0 Readpoint_11 000000005575B67D PC=0000 RSSI=0 Pwr=0

Table 10- 23 LogColumns

Path	Root/Objects/DeviceSet/Read_point_x/RuntimeParameters/Diagnosis/Logbook/LogColumns
Data type	String
Access	R
Description	Log diagnostics The headers column of the communication modules log is output as formatted string. The individual fields are separated by semi-colons. The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.
Possible values	Date_Time ; Type ; Entry ; Command_Type; Sequence_Number ; Readpoint ; EPCID_UID ; PC ; RSSI ; Power

10.2.7 DigitalIOPorts

These variables are used to query and set the digital inputs and outputs of the RF18xCi communication module. The information for all digital inputs/outputs is always transferred regardless of whether these are physically occupied or not.

Table 10- 24 DigitalInputs

Path	Root/Objects/DeviceSet/Read_point_x/IOData/DigitalIOPorts/DigitalInputs
Data type	String
Access	R
Description	<p>Supplies the states of the digital inputs of the communication module.</p> <p>The number of actually existing physical digital inputs depends on the communication module version being used, the operating mode of the digital inputs/outputs and on the connected IO-Link module.</p>
Possible values	<p>00000000 ... 11111111</p> <p>Binary characters (0, 1) per input</p> <p>Each position stands for an input of the communication module:</p> <ul style="list-style-type: none"> • Inport00: 1st position (least significant bit right) • Inport01: 2nd position • Inport02: 3rd position • Inport03: 4th position • Inport04: 5th position • Inport05: 6th position • Inport06: 7th position • Inport07: 8th position <p>Depending on the value of the particular position, the corresponding input is at "ON" (1) or "OFF" (0).</p>

Table 10- 25 DigitalOutputs

Path	Root/Objects/DeviceSet/Read_point_x/IOData/DigitalIOPorts/DigitalOutputs
Data type	String
Access	R/W
Description	<p>Supplies the states of the digital outputs of the communication module and allows the states of the output to be set.</p> <p>The number of actually existing physical digital outputs depends on the communication module version being used, the operating mode of the digital inputs/outputs and on the connected IO-Link module.</p>
Possible values	<p>00000000 ... 11111111</p> <p>Binary characters (0, 1) per output, also "x" on setting for masking out</p> <p>Each position stands for an output of the communication module:</p> <ul style="list-style-type: none"> • Output00: 1st position (least significant bit right) • Output01: 2nd position • Output02: 3rd position • Output03: 4th position • Output04: 5th position • Output05: 6th position • Output06: 7th position • Output07: 8th position <p>Read: Depending on the value of the particular position, the corresponding output is at "ON" (1) or "OFF" (0).</p> <p>Write: Depending on the value of the particular position, the corresponding output is set to "ON" (1) or "OFF" (0). Outputs whose state is to remain unchanged can be masked out with "x".</p> <p>Example: xxxxxx01</p> <p>Output01 is switched off, Output00 is switched on, the other outputs remain unchanged.</p>

10.3 OPC UA events

10.3.1 Description of the events

OPC UA variables represent a simple way to query or accept information from the communication modules.

The known difficulties in time-based synchronization between the query and update of the variable values during more complex process with OPC UA variables do not occur with events. If events are defined for specific actions, an independent event is generated for each action that has occurred and been completed. Overwriting the related information is excluded.

With events, in contrast to variables with their simple data types, OPC UA clients require the possibility to handle more complex data types such as structures and unions in addition.

The integrated OPC UA servers of the communication modules offer the following three additional events as a supplement to the Autold standard:

- AutoldPresenceEvent
- RfidLastAccessEvent
- AutoldLastLogEntryEvent

These three events are for diagnostics purposes. These events are derived directly or indirectly from the "AutoldDiagnosisEvent" event, which in turn is derived from "BaseEvent" with its properties as defined in the OPC UA standard.

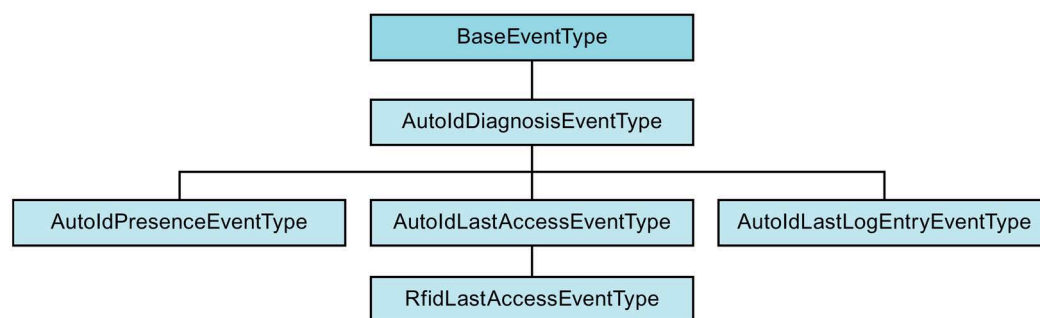


Figure 10-3 Derivations of the OPC UA events based on the "BaseEvent"

10.3.2 AutoldPresenceEvent

This is an event for the presence of transponders. A "PresenceEvent" is generated for each change in presence. The prerequisite is that the reader supports "Presence" mode and is operated in this mode, and that the option "Parallel" or "Diagnostics" is set in the WBM.

A "PresenceEvent" contains the following Properties in addition to the properties inherited from "BaseEvent":

- DeviceName
- Presence

Table 10- 26 DeviceName

Data type	String
Description	DisplayName of the read point from which the event comes. This Property is inherited from "AutoldDiagnosisEvent". The BrowseName of the read point is supplied via the standard property "SourceName" of "BaseEvent".
Possible values	Example: Readpoint_11

Table 10- 27 Presence

Data type	UInt16
Description	Shows the presence of transponders.
Possible values	<ul style="list-style-type: none"> • 0: There is no transponder in the antenna field • 1: There is at least one transponder in the antenna field • >1: Exact number of transponders (if supported by the reader)

10.3.3 RfidLastAccessEvent

This is an event for the last transponder access. An "RfidLastAccessEvent" is generated for every command that was successfully executed on a transponder. The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.

In addition to the inherited properties of "BaseEvent", an "RfidLastAccessEvent" also contains the following properties:

- DeviceName
- Client
- Command
- LastAccessResult

Table 10- 28 DeviceName

Data type	String
Description	DisplayName of the read point from which the event comes. This Property is inherited from "AutoldDiagnosisEvent". The BrowseName of the read point is supplied via the standard property "SourceName" of "BaseEvent".
Possible values	Example: Readpoint_11

Table 10- 29 Client

Data type	String
Description	Client interface via which the last transponder access or the last command on this read point took place.
Possible values	<ul style="list-style-type: none"> • PNIO: Access via PROFINET • OPCUA: Access via OPC UA • WBM: Access via WBM • XML1: Access via the XML channel 1 • XML2: Access via the XML channel 2 • XML3: Access via the XML channel 3 • XML4: Access via the XML channel 4 • EIP: Access via EtherNet/IP • PB: Access via PROFIBUS • READPOINT: internal access via the read point <p>The read points of the device can scan for transponders independently. This is the case, for example, when at least one user application has started an asynchronous scan command or when a configured trigger was started with RF600. These events can also overlap in which case they can no longer be clearly assigned. In this case, the value "READPOINT" is always used instead.</p>

Table 10- 30 Command

Data type	String	
Description	Command that was executed during the last transponder access operation.	
Possible values	Depending on the client interface used:	
	PNIO, PB, EIB (Ident profile): <ul style="list-style-type: none"> • INVENTORY • WRITE-ID • KILL-TAG • LOCK-TAG-BANK • PHYSICAL-READ • PHYSICAL-WRITE • FORMAT • TAG-STATUS • GET • PUT • NEXT 	PNIO, PB (FB 45): <ul style="list-style-type: none"> • WRITE • READ • INIT • MDS-STATUS
	OPC UA: <ul style="list-style-type: none"> • Scan • ReadTag • WriteTag • KillTag • LockTag • SetTagPassword • Read • Write 	WBM, XML: <ul style="list-style-type: none"> • readTagIDs • writeTagID • readTagMemory • writeTagMemory • killTag • lockTagBank • getTagStatus
	READPOINT: <ul style="list-style-type: none"> • Observed 	--

The property "LastAccessResult" is a field of "RfidLastAccessResult" structures. A field entry or a structure carries the information for a transponder that was accessed by the "Command". If multiple transponders were accessed by the command, the field has multiple entries.

RfidLastAccessResult

The "RfidLastAccessResult" structure is derived from the "LastAccessResult" structure and has the following components, including the derived elements:

- Identifier
- CodeType
- Timestamp
- RWData
- CodeTypeRWData
- Antenna
- CurrentPowerLevel
- PC
- Polarization
- Strength

Table 10- 31 Identifier

Data type	ScanData This is a union with the possible types for "Identifier". The types "String", "ByteString" and "ScanDataEpc" are supported. The used data type is defined or set via the "CommonSettings > CodeTypes" variable.
Description	UID or EPC of transponder which was accessed with the last command.
Possible values	Example (RF300 reader, data type string): 000000005575B67D

Table 10- 32 CodeType

Data type	CodeTypeDataType
Description	Shows the set format of the "Identifier" as String.
Possible values	<ul style="list-style-type: none"> • RAW:BYTES • RAW:STRING • EPC

Table 10- 33 Timestamp

Data type	UtcTime
Description	Time of the last transponder access
Possible values	Example: 2018-05-29T08:29:15.812Z

Table 10- 34 RWDData

Data type	ScanData This is a union with the possible types for "RWDData". The types "String", "ByteString" and "ScanDataEpc" are supported. The used data type is defined or set via the "CommonSettings > CodeTypesRWDData" variable.
Description	Read/written data of the last command Only possible with commands for reading/writing the transponder memory.
Possible values	Example (RF300 reader, data type string): 0011223344556677

Table 10- 35 CodeTypeRWDData

Data type	CodeTypeDataType
Description	Shows the set format of "RWDData" as String.
Possible values	<ul style="list-style-type: none"> • RAW:BYTES • RAW:STRING • EPC

Table 10- 36 Antenna

Data type	Int32
Description	The antenna via which the transponder was accessed with the last command.
Possible values	<p>Two-digit number</p> <p>The first digit stands for the read point index, the second digit for the antenna index within the read point.</p> <p>Example:</p> <ul style="list-style-type: none"> • Read point 1, antenna 1: 11 • Read point 2, antenna 1: 21

Table 10- 37 CurrentPowerLevel

Data type	Int32
Description	Power with which the last command was executed on the transponder. This variable is only supported by UHF readers.
Possible values	<p>Decimal number for the power in [dB]</p> <p>Increment: 0.25 dB</p> <ul style="list-style-type: none"> • 0 • 5.00 ... 33.00

Table 10- 38 PC

Data type	UInt16
Description	Protocol Control Word of the transponder that was accessed last. This variable is only supported by UHF readers.
Possible values	Example: 3000

Table 10- 39 Polarization

Data type	String
Description	Polarization with which the last command was executed on the transponder. This variable is only supported by UHF readers.
Possible values	<ul style="list-style-type: none"> • Default • Circular • Linear_vertical • Linear_horizontal

Table 10- 40 Strength

Data type	Int32
Description	RSSI value with which the last command was executed on the transponder. This variable is only supported by UHF readers.
Possible values	0 ... 255

10.3.4 AutoldLastLogEntryEvent

This is an event for the last log entry. A "LastLogEntryEvent" is generated for every event that was made in the log. The prerequisite is that the "Parallel" or "Diagnostics" option is set in the WBM.

Note that the log is assigned to the communications module and not to a read point. Even if entries for read points are made in the log, log entries are always made by the communications module. The associated "LastLogEntryEvents" are always generated by the communications module. The OPC UA read points only serve as transmitters of events to OPC UA clients. This has the consequence that every read point transmits all "LastLogEntryEvents", even those that relate to other read points. In the WBM, you can define the read points via which the "LastLogEntryEvents" should be transmitted.

In addition to the inherited properties of "BaseEvent", a "LastLogEntryEvent" also contains the following Property:

- DeviceName

Table 10- 41 DeviceName

Data type	String
Description	<p>Name of the communications module that made the log entry and generated the Event.</p> <p>This Property is inherited from "AutoldDiagnosisEvent". The inherited standard property "SourceName" of "BaseEvent" contains the BrowseName of the read point via which the event was transmitted.</p>
Possible values	<p>Example:</p> <p>SIMATIC_RF188C (192.168.0.254)</p>

The text of the log entry is in the "Message" Property inherited by the "BaseEvent".

Programming via Rockwell controller



This section is intended only for Rockwell users.

You can program the communication modules using add-on instructions via a Rockwell controller. With the described functions, you can read out and write transponder data via the connected readers. You can find a detailed description of the Ident profile and the add-on instructions in the "Ident profile and Ident blocks, standard function for Ident systems (<https://support.industry.siemens.com/cs/ww/en/view/109762333>)" function manual.

Service and maintenance

12.1 Diagnostics

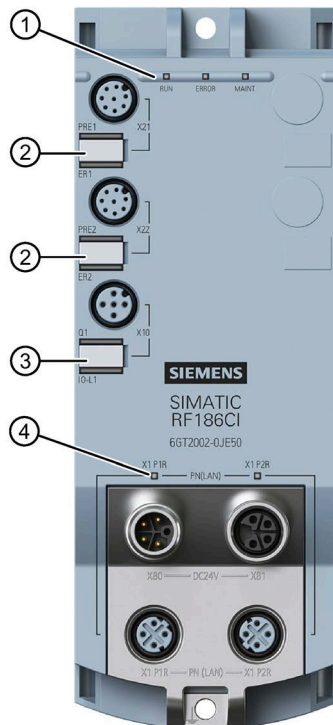
The following diagnostic options are available for the communication modules:

- Via the LED displays of the communication modules
- Via SNMP
- Using WBM
- Via the TIA Portal (STEP 7 Basic / Professional)
- Via XML
- Via OPC UA

These alternative methods are described below.

12.1.1 Diagnostics via the LED display

The following figure shows the LEDs of the RF18xC/RF18xCI in detail.



- | | | |
|---|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ① | Status LED display | |
| | <ul style="list-style-type: none"> • RUN/STOP (RUN) • ERROR (ERROR) • MAINTENANCE (MAINT) | <p>Indicates whether the CM is ready for operation.</p> <p>Indicates whether an error has occurred.</p> <p>Shows whether the communication module needs maintenance.</p> |
| ② | Reader LED display | |
| | <ul style="list-style-type: none"> • PRESENCE (PRE) • ERROR (ER) | <p>Indicates whether there are one or multiple transponders in the antenna field.</p> <p>Indicates whether communication with the reader is taking place and whether a reader error has occurred.</p> |
| ③ | IO LED display | |
| | <ul style="list-style-type: none"> • Channel status (Q1) • Channel fault (IO-L1) | <p>Indicates whether the output is switched on.</p> <p>Indicates whether an IO-Link device is connected and whether an error has occurred.</p> |
| ④ | PROFINET/Ethernet LED display | |
| | <ul style="list-style-type: none"> • LINK P1 (X1 P1R) • LINK P2 (X1 P2R) | <p>Indicates that there is a link via the Ethernet interface "1".</p> <p>Indicates that there is a link via Ethernet interface "2".</p> |

Figure 12-1 LED displays of the RF18xC/RF18xCI communication module

Status LED display




















The operating states of the communication module are displayed by the "RUN/STOP", "ERROR" and "MAINT" LEDs. The LEDs can adopt the colors green, red or yellow and the statuses off , on , flashing :

Table 12- 1 Shows the operating states via the status LED display

RUN	ERROR	MAINT	Meaning
			The CM is switched off.
			<ul style="list-style-type: none"> LED test while the CM is starting up. The CM is manually reset to factory settings. A connected cable or a connected reader is defective.
			<ul style="list-style-type: none"> No data exchange between the CM and user application takes place. The CM has not yet received a user command. The connection to the user application has been closed.
	--	--	Data exchange between the CM and user application takes place. The CM has received and executed a user command.
--	--		A firmware update is in progress.
--	--		The voltage at the CM is too low.
			<ul style="list-style-type: none"> The flash test is performed for reader identification. At the same time, the LEDs of the reader and PROFINET/Ethernet LED display also flash. The firmware is defective.
--		--	There is an error. You can find more information on error messages in the section "Error messages (Page 155)".

Reader LED display















The operating states of the reader are displayed by the LEDs "PRE" and "ER". The LEDs can adopt the colors green, red or yellow and the statuses off , on , flashing :

Table 12- 2 Shows the reader states via the reader LED display









PRE	ER	Meaning
		The CM is switched off.
	--	The reader is configured (reset telegram has been sent).
		LED test while the CM is starting up.
		The flash test is performed for reader identification. At the same time, the LEDs of the reader and PROFINET/Ethernet LED display also flash.
--		Communication takes place between CM and reader.
	--	The presence of a transponder is reported.

PRE	ER	Meaning
	--	The presence of several transponders is reported. Note: The number of transponders located in the antenna field cannot be read via the LED.
--		An error has occurred between CM and reader. Possible errors: <ul style="list-style-type: none"> • 1x: After the reader was started up, no "WriteConfig" command was sent to the reader. • 2x: Configuration error The specified configuration does not match the type of reader connected. • 3x: Transmission error • 4x: Group error You can find more information on error messages in the section "Error messages (Page 155)".

IO LED display

The operating states of the I/O interface are displayed by the LEDs "IO-L1" and "Q1". The LEDs can adopt the colors green, red or yellow and the states off, on, flashing:

Table 12- 3 Display of the reader states via the IO LED display

IO-L1	Q1	Meaning
		The interface is located in the "Input" or "Output" configuration and the input/output is switched off.
		The interface is located in the "Input" or "Output" configuration and the input/output is switched on.
	--	The interface is located in the "IO-Link" configuration. An IO-Link device is not connected or was not recognized.
	--	The interface is located in the "IO-Link" configuration. An IO-Link device is connected and was recognized.
	--	There may be an error at the input/output (e.g. short-circuit).
	--	The load voltage (2L+) is not connected.

PROFINET/Ethernet LED display







The states of the PROFINET/Ethernet connections are indicated by the "X1 P1R" and "X1 P2R" LEDs. The LEDs can adopt the colors green, red or yellow and the statuses off , on , flashing :

Table 12- 4 Shows the PROFINET/Ethernet states via the PROFINET/Ethernet LED display

X1 P*R	Meaning
	<ul style="list-style-type: none"> No connection is available. No cable has been connected.
	The flash test is performed for reader identification. At the same time, the LEDs of the status and reader LED display also flash.
	<ul style="list-style-type: none"> LED test while the CM is starting up. A connection is available.

12.1.2 Diagnostics via SNMP

Comprehensive diagnostic options of the network functions of the communication module are available via SNMP. The following diagnostic options (MIBs) are supported by the communication modules:

- automationSimaticNet.mib
- automationSnSystem.mib
- automationSystem.mib
- IEC-62439.mib
- IP.mib
- LLDP-EXT-DOT1.mib
- LLDP-EXT-DOT3.mib
- LLDP-EXT-PNO.mib
- LLDP.mib
- RFC1213.mib
- SNMPv2.mib
- SNMPv2Smi.mib

You can find the MIB files corresponding to the communication modules on the pages of Siemens Industry Online Support

(<https://support.industry.siemens.com/cs/ww/en/view/67637278>) (automation MIBs), information on the MIB files under "PROFINET user organization (<https://www.profibus.com/download/profinet-specification/>)".

The communication modules support the SNMPv1 protocol. SNMP is activated at the factory. You can find information on SNMP in the section "The "Settings - Communication" menu item (Page 80)".

You can find detailed information on using SNMP and, in particular, on the structure of the automation.mib in the diagnostics manual "Network management diagnostics and configuration with SNMP (<https://support.industry.siemens.com/cs/ww/en/view/103949062>)".

12.1.3 Diagnostics using the WBM

A wide variety of diagnostics options are available via the WBM. These are described below.

Logs

In the "Log" menu, you can find all the diagnostics messages of the communication module that have occurred. The "Service log" helps SIEMENS specialists to analyze errors. You can read out the syslog messages from the "Syslog log" and you can read out the "Status parameters" of the connected readers and transponders using the "Hardware diagnostics".

You will find further information on the "Log" in the section "The "Diagnostics - Log" menu item (Page 97)".

12.1.4 Diagnostics using the TIA Portal (STEP 7 Basic / Professional)



This section is intended only for S7 users.

Requirements

STEP 7 Basic / Professional is installed and started, and a project is open. The communication module is connected to the controller or PC via Industrial Ethernet or PROFINET and has been powered up.

Definition

If error states occur, e.g. termination of a connection, they are indicated in the online device view by a red tool symbol in front of the relevant module. Note that error states of the reader are only displayed if you have activated the diagnostic interrupt messages of the relevant reader.

To obtain more information on the error that has occurred, you can read out the diagnostic information of the respective module (communication module or reader).

Procedure

Reading out diagnostics information of the communication module

Proceed as follows to read the diagnostics information of the communication module using STEP 7 Basic / Professional (TIA Portal):

1. Change to the network view.
2. Right-click on the desired communication module and click on "Online & Diagnostics" in the shortcut menu.
3. Select the "Diagnostics" parameter group.

The diagnostics window provides you with the following options for diagnostics of the communication module:

- The identifier and the firmware version of the communication module are displayed under the "General" entry.
- Under the "Diagnostic status" entry, you can see the current status information of the communication module.
- Under the "PROFINET interface" entry, you can find status information and further information about the PROFINET interface.

Module	
Short designation:	RF186C V1.0
Article number:	6GT2 002-0JE20
Hardware:	1
Firmware:	T1.0.0
Firmware expansion:	---
Rack:	0
Slot:	0

Module information	
Module name:	IID device
Plant designation:	Text
Location ID:	Text
Installation date:	Tuesday, July 31, 2018 14:14
Additional information:	Info_2018

Manufacturer information	
Manufacturer description:	SIEMENS AG
Serial number:	VFE1821961
Copyright entry:	---
Profile:	16#0000
Profile details:	16#0003

Figure 12-2 Display of the diagnostics information of the communication module

Reading out diagnostics information of the connected readers

Requirement: The diagnostic interrupt messages of the reader have been activated.

Proceed as follows to read the diagnostics information of the readers connected to the communication module using STEP 7 Basic / Professional (TIA Portal):

1. Switch to the device view of the communication module.
2. In the device overview, right-click on the desired reader module and click on the "Online & Diagnostics" entry in the shortcut menu.
3. Select the "Diagnostics" parameter group.

In the diagnostics window, you have the following options for diagnosing the reader:

- General information, such as the identifier and the article number of the reader is displayed under the "General" entry.
- Under the "Diagnostic status" entry, you can see current status information and the diagnostic interrupt messages of the reader.

The error messages are stored in the CPU diagnostics buffer as plain text. You can further process these messages with the appropriate function blocks, e.g. so that they are forwarded to an HMI.

Diagnostics using the "TO_Ident" technology object

Alternatively, you can also diagnose the communication modules using the "TO_Ident" technology object. You can find detailed information on this in the TIA Portal help.

12.1.5 Diagnostics via XML



This section is intended only for XML users.

Comprehensive diagnostics options are available to you via XML. You can find detailed information on the diagnostic options that can be found in the "XML programming for SIMATIC Ident (<https://support.industry.siemens.com/cs/ww/en/ps/14971/man>)" manual.

12.1.6 Diagnostics over OPC UA



Comprehensive diagnostics options are available to you via OPC UA. The various diagnostics options are described below.

OPC UA variables and events

Using the OPC UA variables and events, you can read out diagnostic messages and query them in a targeted manner. You can find more information on this subject in the section "Programming via OPC UA (Page 115)".

12.1.7 Diagnostics using Studio 5000 Logix Designer



This section is intended only for users of Rockwell controllers.

You will find information on diagnostics using the Studio 5000 Logix Designer in the Studio 5000 Logix Designer manual.

12.1.8 Parameterization of the diagnostics



With STEP 7 Basic / Professional, you can select which diagnostic interrupt messages you wish to view. Follow the steps below to deactivate the diagnostic interrupt messages:

- Communication module:

Select communication module

"General > Module parameters > Diagnostic interrupt"

- Connected readers:

Select communication module

"Device view > Device overview > Reader module > General > Module parameters > Diagnostics messages"

Diagnostic interrupts/messages

Diagnostic interrupts (communication module diagnostics)

If the diagnostic interrupt has been activated ("On"), the following diagnostic interrupts are reported:

- Fault in power supply
- Hardware fault
- Firmware error

Diagnostic messages (reader diagnostics)

The following settings of the diagnostic messages are available to you:

- **None**

No further diagnostic data is reported.

- **Hard errors**

Critical hardware errors/faults are reported by the S7 diagnostics. Extended diagnostic messages are generated in the case of the following events.

- Hardware fault (memory test)
- Firmware error (checksum)
- Break in connection to reader
- Fault in power supply to the readers
- Short-circuit/break, if supported by hardware
- Firmware update (message at start/end)

- **Hard / soft errors**

Critical hardware errors and errors that occur during command processing are reported by the S7 diagnostics. In contrast to the hard errors, errors that arise during command processing are also reported in this case.

Please note that messages triggered by command processing are automatically taken back after 3 seconds.

Differentiation of diagnostic interrupt messages

With the diagnostic interrupt messages, a distinction is made between incoming and outgoing diagnostic interrupts.

- **Incoming diagnostic interrupt**

An event occurs and triggers an alarm.

- **Outgoing diagnostic interrupt**

The event is no longer current, a diagnostic message is output. For events that only exist momentarily, the reset is delayed by 3 seconds.

Further information

You can find detailed information on diagnostics on PROFINET IO in the manual "SIMATIC PROFINET system description

(<https://support.industry.siemens.com/cs/ww/en/view/19292127>)".

12.2 Error messages

You have the following options for error analysis of the modules:

- Via error messages of the communication module
- Via error messages of the WBM
- Via XML error messages
- Via OPC UA error messages

These alternative methods are described below.

12.2.1 Error messages of the communications module

Note that depending on the cause of the error, the "ERROR" status LED or the "ER" reader LED of the respective reader interface always flashes if error messages occur. You can read the error via the error codes or alternatively via the WBM log.

In the following table, you will find an overview of the error codes as well as the flashing patterns of the "ER" LED of the respective reader at which the error occurred.

Table 12- 5 Features of the communication modules

"ER" LED	Block (hex)	Error description
4x	0xE1FE0100	Cannot write to the memory of the transponder. Possible causes: <ul style="list-style-type: none"> • Transponder memory is defective. • EEPROM transponder was written too frequently and has reached the end of its service life.
4x	0xE1FE0200	Presence error The transponder is no longer within the transmission window of the reader. The command was not or only partially executed. Read command: There is no valid data in "IDENT_DATA". Write command: The transponder that has just left the antenna field contains an incomplete data record. Possible causes: <ul style="list-style-type: none"> • Operating distance between reader and transponder is not being maintained. • Configuration error: The data record to be processed is too large (in dynamic mode).
4x	0xE1FE0300	Address error The address range of the transponder has been exceeded. Possible causes: <ul style="list-style-type: none"> • Start address of the command start has been incorrectly set. • Wrong transponder type • The area to be written to is write-protected.

"ER" LED	Block (hex)	Error description
4x	0xE1FE0400	Initialization error Transponder is unable to execute the initialization command Possible causes: <ul style="list-style-type: none"> Transponder is defective.
4x	0xE1FE0500	The transponder memory is full.
4x	0xE1FE0600	Error in transponder memory The transponder has never been written to or has lost the contents of its memory due to battery failure. Possible causes / action to be taken: <ul style="list-style-type: none"> Replace the transponder (if the battery bit is set). Re-initialize the transponder.
4x	0xE1FE0700	ECC error
4x	0xE1FE0800	The transponder in the antenna field does not have the expected UID / EPC ID or has no UID / EPC ID.
4x	0xE1FE0900	The command is not supported by the transponder.
4x	0xE1FE0A00	The transponder is read/write-protected.
4x	0xE1FE8100	The transponder is not responding.
4x	0xE1FE8200	The transponder password is incorrect. Access is denied.
4x	0xE1FE8300	The verification of the written transponder data has failed. Possible causes: <ul style="list-style-type: none"> Transponder is defective. Transponder is in the limit area.
4x	0xE1FE8400	General transponder error
4x	0xE1FE8500	The transponder has too little power to execute the command. Possible causes: <ul style="list-style-type: none"> Transponder is in the limit area.

"ER" LED	Block (hex)	Error description
4x	0xE2FE0100	<p>Field disturbance on reader</p> <p>Possible causes:</p> <ul style="list-style-type: none"> • The reader is receiving interference pulses from the environment. <ul style="list-style-type: none"> – External interference field. The interference field can be detected with the "inductive field indicator" of the mobile reader. – The distance between two readers is too small and does not correspond to the configuration guidelines. – The connecting cable to the reader is defective or too long or does not comply with the specification. • Too many transmit errors <p>The transponder was unable to receive the command or write data from the communication module correctly even after several attempts.</p> <ul style="list-style-type: none"> – The transponder is positioned exactly in the limit area of the transmission window. – Data transmission to the transponder is being affected by external interference. <ul style="list-style-type: none"> • CRC sending error <ul style="list-style-type: none"> – The transponder reports CRC errors frequently (transponder is positioned in the limit area of the reader; transponder and/or reader has a hardware defect). • Only during initialization: CRC error on receipt of acknowledgment from transponder (cause as for field interference on the reader). • When formatting, the transponder must be in the transmission window of the reader, otherwise a timeout error will occur, in other words: <ul style="list-style-type: none"> – The transponder is located exactly in the limit range of the transmission window. – The transponder is defective and consumes too much power. – The EEPROM transponder was incorrectly configured by "FORMAT". • RF600: <ul style="list-style-type: none"> – No ETSI channel is available. – An incorrect communication standard was selected in the "INIT" command. – The expert parameter is incorrect. – The performance check of the ETSI radio profile is faulty.
4x	0xE2FE0200	More transponders are located in the transmission window than can be processed at the same time by the reader.
4x	0xE2FE8100	There is no transponder with the required EPC ID/UID in the transmission window or there is no transponder at all in the antenna field.
4x	0xE2FE8200	The requested data is not available.
4x	0xE2FE8300	CRC error in reader-transponder communication.
4x	0xE2FE8400	The selected antenna is not enabled.
4x	0xE2FE8500	The selected frequency is not enabled.
4x	0xE2FE8600	The carrier signal is not activated.
4x	0xE2FE8700	There is more than one transponder in the transmission window.
4x	0xE2FE8800	General radio protocol error
--	0xE3FE0100	The file name is not allowed.
--	0xE3FE0200	The file does not exist.

12.2 Error messages

"ER" LED	Block (hex)	Error description
3x	0xE4FE0100	Warning in the event of low power supply The power supply is very close to the low limit.
--	0xE4FE0200	Hardware fault
3x	0xE4FE0300	Connection problem with the reader Error in the connection to the reader; the reader is not answering. Possible causes / action to be taken: <ul style="list-style-type: none"> • The cable between the communication module and reader is wired incorrectly or there is a cable break. • The 24 V supply voltage is not connected or is not turned on or has failed briefly. • Automatic fuse on the communication module has blown. • The hardware is defective. • Perform an "init_run" once the error has been corrected.
4x	0xE4FE0400	The buffer on the communication module or reader is not adequate to store the command temporarily.
4x	0xE4FE0500	The buffer on the communication module or reader is not adequate to store the data temporarily.
4x	0xE4FE0600	The command is not permitted in this status or is not supported. Possible causes: <ul style="list-style-type: none"> • The "INIT" command has been concatenated. • Command repetition was started without "Presence mode".
1x	0xE4FE0700	Startup message from reader/communication module The reader or communication module was off and has not yet received a "Reset_Reader" ("WRITE-CONFIG") command. Possible causes / action to be taken: <ul style="list-style-type: none"> • Execute the "INIT" command. • The same physical address in the "IID_HW_CONNECT" parameter is being used more than once. Check your "IID_HW_CONNECT" parameter assignments. • Check the connection to the reader. • The device has not yet been restarted after the change to the transmission speed.
4x	0xE4FE8100	The specified tag field of the transponder is unknown.
4x	0xE4FE8A00	General error
2x	0xE4FE8B00	No or bad configuration data/parameters were transferred. Possible causes: <ul style="list-style-type: none"> • You are accessing a read point that is not configured.

"ER" LED	Block (hex)	Error description
4x	0xE4FE8C00	<ul style="list-style-type: none"> Communication error between Ident profile and communication module. Handshake error. Possible causes / action to be taken: <ul style="list-style-type: none"> The UDT of this communication module has been overwritten by other program sections. Check the parameter settings of the communication module in the UDT. Check the Ident profile command that causes this error. After eliminating the error, execute the "INIT" command. Backplane bus / PROFIBUS DP error occurred. This error is only indicated when access monitoring has been enabled in the PROFIBUS configuration. Possible causes / action to be taken: <ul style="list-style-type: none"> Backplane bus / PROFIBUS DP bus connection was interrupted (wire break on the bus; bus connector on the communication module was briefly unplugged) The backplane bus / PROFIBUS DP master no longer addresses the communication module Execute the "INIT" command. The communication module has detected a frame interruption on the bus. The backplane bus, PROFIBUS may have been re-configured (e.g. with HW Config or TIA Portal)
--	0xE4FE8D00	<ul style="list-style-type: none"> Firmware error Possible causes: The firmware update was not run completely. Internal communication error of the communication module/reader Possible causes / action to be taken: <ul style="list-style-type: none"> Connector contact problem on the communication module / reader Hardware of the communication module/reader has a defect; → Send in communication module/reader for repair. After eliminating the error, execute the "INIT" command. Internal monitoring error of the communication module/reader Possible causes / action to be taken: <ul style="list-style-type: none"> Program execution error on the communication module / reader Switch supply voltage to communication module/reader off and on again. After eliminating the error, execute the "INIT" command.
--	0xE4FE8E00	<p>The current command was aborted by the "WRITE-CONFIG" ("INIT" or "SRESET") command for the bus connector was pulled.</p> <p>Possible causes:</p> <ul style="list-style-type: none"> Communication with the transponder was aborted by "INIT". This error can only be reported if there is an "INIT" or "SRESET".
--	0xE5FE0100	Incorrect sequence number order (SN) on the reader/communication module
--	0xE5FE0200	Incorrect sequence number order (SN) in the Ident profile
--	0xE5FE0400	Invalid data block number (DBN) on the reader/communication module
--	0xE5FE0500	Invalid data block number (DBN) in the Ident profile

"ER" LED	Block (hex)	Error description
--	0xE5FE0600	Invalid data block length (DBL) on the reader/communication module
--	0xE5FE0700	Invalid data block length (DBL) in the Ident profile
--	0xE5FE0800	<p>The previous command is still active or the buffer is full.</p> <p>A new command was sent to the reader or communication module although the last command is still active.</p> <ul style="list-style-type: none"> • The active command can only be aborted with "INIT". • Before a new command can be started, "DONE bit = 1" must be set (exception "INIT"). • Two Ident profile calls were assigned the same "HW_ID", "CM_CHANNEL" and "LADDR" parameter settings. • Two Ident profile calls are using the same pointer. • After eliminating the error, execute the "INIT" command. • When working with command repetition (e.g., fixed code transponder), no data is being fetched from the transponder. The data buffer on the reader/communication module has overflowed. Transponder data has been lost.
--	0xE5FE0900	The reader or the communication module runs a hardware reset ("INIT_ACTIVE" set to "1"). The Ident profile expects an "INIT" (bit 15 in the cyclic control word).
--	0xE5FE0A00	The "CMD" command code and the relevant acknowledgment do not match. This can be a software error or synchronization error that cannot occur in normal operation.
--	0xE5FE0B00	Incorrect sequence of acknowledgment frames (TDB / DBN)
--	0xE5FE0C00	Synchronization error (incorrect increment of "AC_H / AC_L" and "CC_H / CC_L" in the cyclic control word). "INIT" had to be executed.
3x	0xE5FE8100	Communication error between reader and communication module Access denied
3x	0xE5FE8200	Communication error between reader and communication module Resource is occupied
3x	0xE5FE8300	Communication error between reader and communication module Functional error of the reader interface
3x	0xE5FE8400	Communication error between reader and communication module Other faults/errors
4x	0xE6FE0100	<p>Unknown command</p> <p>An uninterpretable XML command was sent to the reader or the Ident profile sends an uninterpretable command to the reader.</p> <p>Possible causes:</p> <ul style="list-style-type: none"> • The "AdvancedCmd" block was supplied with an incorrect "CMD". • The "CMD" input of the "AdvancedCmd" block was overwritten.
4x	0xE6FE0200	Invalid command index (CI)

"ER" LED	Block (hex)	Error description
4x	0xE6FE0300	<ul style="list-style-type: none"> A parameter of an XML command has an invalid value or the parameter assignment of the communication module or the reader was incorrect. <p>Possible causes / action to be taken:</p> <ul style="list-style-type: none"> Check the parameters in the Ident profile. Check the relevant XML command. Check the parameter assignment in HW Config / STEP 7 (TIA Portal). The "WRITE-CONFIG" command has incorrect parameter settings. After a startup, the reader or communication module has still not received an "INIT". <ul style="list-style-type: none"> The parameter assignment of the reader or communication module on PROFIBUS/PROFINET was incorrect and the command cannot be executed. <p>Possible causes / action to be taken:</p> <ul style="list-style-type: none"> Length of the input/output areas is too small for the cyclic I/O word. Check whether you have used the correct GSD file. Command (e.g. "READ") issued with excessively long user data. <ul style="list-style-type: none"> Error when processing the command. <p>Possible causes / action to be taken:</p> <ul style="list-style-type: none"> The data in "AdvancedCmd" or "IID_CMD_STRUCT" is incorrect (e.g. "WRITE" command with length = 0). Check "AdvancedCmd" or "IID_CMD_STRUCT" and execute an "INIT". The hardware of the reader/communication module is defective. The reader or communication module receives bad data with an "INIT". Inconsistent length specifications in the command <ul style="list-style-type: none"> The wrong reset block was selected. <p>Possible causes / action to be taken:</p> <ul style="list-style-type: none"> Regardless of the selected reader system, use the "Reset_Reader" function block.
4x	0xE6FE0400	<p>Presence error</p> <p>A transponder has passed through the transmission window of a reader without being processed.</p> <ul style="list-style-type: none"> This error message is not reported immediately. Instead, the reader or communication module waits for the next write / read command. This command is replied to immediately with this error and the write/read command is not executed. The next command is executed normally again by the reader/communication module. You can reset this error status using an "INIT". Bit 2 is set in the "OPT1" parameter and there is no transponder in the transmission window.
4x	0xE6FE0500	<p>An error has occurred that makes a Reset_Reader ("WRITE-CONFIG" with "Config = 3") necessary.</p> <p>Possible causes / action to be taken:</p> <ul style="list-style-type: none"> The "WRITE-CONFIG" command is incorrect. After eliminating the error, execute an "INIT". Check the parameter "IID_HW_CONNECT".
4x	0xE6FE8100	A parameter is missing.
4x	0xE6FE8200	The parameter has an invalid format.

12.2 Error messages

"ER" LED	Block (hex)	Error description
4x	0xE6FE8300	The parameter type is invalid.
4x	0xE6FE8400	Unknown parameter.
4x	0xE6FE8500	The command or the frame has an invalid format.
4x	0xE6FE8600	The inventory command failed.
4x	0xE6FE8700	Read access to the transponder has failed.
4x	0xE6FE8800	Write access to the transponder has failed.
4x	0xE6FE8900	Writing the EPC ID/UID on the transponder has failed.
4x	0xE6FE8A00	Enabling write protection on the transponder has failed.
4x	0xE6FE8B00	The "Kill" command failed.
--	0xE7FE0100	In this state, only the "Reset_Reader" command ("WRITE-CONFIG") is permitted.
--	0xE7FE0200	The "CMD" command code is not permitted.
--	0xE7FE0300	The "LEN_DATA" parameter of the command is too long and does not match the global data reserved within the send data buffer (TXBUF).
--	0xE7FE0400	<p>The receive data buffer (RXBUF) or the send data buffer (TXBUF) is too small, the buffer created at TXBUF/RXBUF does not have the correct data type or the parameter "LEN_DATA" has a negative value.</p> <p>Possible cause / action to be taken:</p> <ul style="list-style-type: none"> • Check whether the buffers TXBUF/RXBUF are at least as large as specified in "LEN_DATA". • With S7-1200/1500: <ul style="list-style-type: none"> – In the Ident profile, only an "Array of Byte" may be created for TXBUF and RXBUF. – In the "Reader_Status" block, only an "Array of Byte" or the corresponding data types ("IID_TAG_STATUS_XX_XXX" or "IID_READER_STATUS_XX_XXX") may be created
--	0xE7FE0500	Error message that informs you that only an "INIT" command is permitted as the next command. All other commands are rejected.
--	0xE7FE0600	<p>Wrong data record index of an acyclic data record</p> <p>Permitted index is in the ranges "101 ... 108" and "-20401 ... -20418".</p>
--	0xE7FE0700	<p>The reader or communication module does not respond to "INIT" ("INIT_ACTIVE" is expected in the cyclic status message).</p> <p>The next steps:</p> <ul style="list-style-type: none"> • Check the address parameter "LADDR".
--	0xE7FE0800	Timeout during "INIT" (60 seconds)
--	0xE7FE0900	Command repetition is not supported.
--	0xE7FE0A00	Error during the transfer of the PDU (Protocol Data Unit).

--" means that the error is not displayed by the LEDs.

12.2.2 Reading out error messages using the WBM

Reading out error messages using the WBM

All the diagnostics messages of the communication module are entered in the "Log" if a check mark was set for "ERRORS" in the WBM configuration in "Settings - General". You will find further information on the "Log" in the section "The "Diagnostics - Log" menu item (Page 97)".

12.2.3 XML error messages



A list of the possible XML error codes can be found in the "XML programming for SIMATIC Ident (<https://support.industry.siemens.com/cs/ww/en/ps/14971/man>)" manual.

12.2.4 OPC UA error messages



The following table lists the OPC UA-specific error codes.

Table 12- 6 OPC UA error messages of the communication module

Autold status	OPC UA status	Autold text	Error description
1	good	MISC_ERROR_TOTAL	General error
1	good	MISC_ERROR_TOTAL	<ul style="list-style-type: none"> Firmware error Possible cause: The firmware update was not run completely. Internal communication error of the communication module/reader <ul style="list-style-type: none"> Connector contact problem on the communication module / reader Hardware of the communication module/reader has a defect; → Send in communication module/reader for repair Start "INIT" after correcting the error Internal monitoring error of the communication module/reader <ul style="list-style-type: none"> Program execution error on the communication module / reader Turn the power supply of the communication module/reader off and on again Start "INIT" after correcting the error
1	good	MISC_ERROR_TOTAL	The inventory command failed.

12.2 Error messages

Autold status	OPC UA status	Autold text	Error description
1	good	MISC_ERROR_TOTAL	Enabling write protection on the transponder has failed.
1	good	MISC_ERROR_TOTAL	The "Kill" command failed.
3	good	PERMISSION_ERROR	The transponder is read/write-protected.
4	good	PASSWORD_ERROR	The transponder password is incorrect. Access is denied.
5	Bad Invalid Argument / good	REGION_NOT_FOUND_ERROR	All commands: A parameter of an OPC UA command has an invalid value. "ReadTag"/"WriteTag" command: The addressed memory area is not available in the current transponder.
7	good	OUT_OF_RANGE_ERROR	Address error The address range of the transponder has been exceeded. Possible causes: <ul style="list-style-type: none"> Start address of the command start has been incorrectly set. Wrong transponder type The area to be written to is write-protected.
7	good	OUT_OF_RANGE_ERROR	The requested data is not available.
8	good	NO_IDENTIFIER	There is no transponder with the required EPC ID/UID in the transmission window or there is no transponder at all in the antenna field.
9	good	MULTIPLE_IDENTIFIERS	More transponders are located in the transmission window than can be processed at the same time by the reader.
9	good	MULTIPLE_IDENTIFIERS	There is more than one transponder in the transmission window.
10	good	READ_ERROR	Read access to the transponder has failed.
14	good	WRITE_ERROR	Write access to the transponder has failed.
14	good	WRITE_ERROR	Writing the EPC ID/UID on the transponder has failed.
15	good	NOT_SUPPORTED_BY_DEVICE	Unknown command An uninterpretable XML command was sent to the reader or the Ident profile sends an uninterpretable command to the reader. Possible causes: <ul style="list-style-type: none"> The "AdvancedCmd" block was supplied with an incorrect "CMD". The "CMD" input of the "AdvancedCmd" block was overwritten.
17	good	DEVICE_NOT_READY	The specified read point is not active because no antenna was assigned to it.

Autold status	OPC UA status	Autold text	Error description
18	good	INVALID_CONFIGURATION	The specified tag field of the transponder is unknown.
19	good	RF_COMMUNICATION_ERROR	The transponder is not responding.
19	good	RF_COMMUNICATION_ERROR	The verification of the written transponder data has failed.
19	good	RF_COMMUNICATION_ERROR	General transponder error
19	good	RF_COMMUNICATION_ERROR	The transponder has too little power to execute the command.
19	good	RF_COMMUNICATION_ERROR	The transponder signals a CRC error.
19	good	RF_COMMUNICATION_ERROR	The selected frequency is not enabled.
19	good	RF_COMMUNICATION_ERROR	The carrier signal is not activated.
19	good	RF_COMMUNICATION_ERROR	General radio protocol error
20	good	DEVICE_FAULT	Fault in power supply The power supply is very close to the low limit.
20	good	DEVICE_FAULT	Antenna errors <ul style="list-style-type: none"> • The antenna or the antenna cable is defective. • Error in the connection to the reader; the reader is not answering (in PROFIBUS operation). <ul style="list-style-type: none"> – The cable between the communication module and reader is wired incorrectly or there is a cable break – The 24 V supply voltage is not connected or is turned off or has failed briefly – Automatic fuse on the communication module has blown – Hardware defective – Another reader is in the vicinity and is active – There is a reflecting metal surface in the vicinity that is disrupting the antenna field – Execute "init_run" after correcting the error
--	--	--	The selected antenna is not enabled.
--	OpcUa_BadInvalidState	--	The command is not permitted in this status or is not supported. Possible cause: <ul style="list-style-type: none"> • "INIT" was chained. • Command repetition was started without "Presence mode".

Autold status	OPC UA status	Autold text	Error description
--	OpcUa_BadOutOfRange / OpcUa_Bad Configuration Error	--	No or bad configuration data/parameters were transferred. Possible cause: <ul style="list-style-type: none"> You are accessing a read point that is not configured.
--	BadInvalidArgument	--	A parameter is missing.
--	BadInvalidArgument	--	The parameter has an invalid format.
--	BadInvalidArgument	--	The parameter type is invalid.
--	BadInvalidArgument	--	Unknown parameter.
--	Bad	--	The command or the frame has an invalid format.

12.3 Firmware update

The following options are available for updating the firmware of the communication modules and the readers connected to them:

- Using WBM
- Using the TIA Portal (STEP 7 Basic / Professional V15.1 or higher)

In addition, the firmware of the readers connected to the communication module can be updated. The firmware of the readers is updated using the TIA Portal (STEP 7 Basic / Professional V15.1 or higher).

These alternative methods are described below.

12.3.1 Updating the firmware via WBM

Requirements

- The communication module is connected to the PC via Industrial Ethernet or PROFINET.
- The communication module has been disconnected from active operation.
- All user applications are closed.
- The required update file is stored locally.

Procedure

Proceed as follows to run a firmware update using the WBM:

1. Start your Web browser.
2. Enter the IP address of the communication module in the address field of your browser.
3. If not logged in, log in to the WBM.

Note that you as "User" can only perform a firmware update if the communication module has the "Idle" status.

4. Click on the "System - System settings" menu item.
5. In the "Firmware update" area, click the "Select firmware file" icon.
6. Select the update file (*.sfw).
7. Click on the "Open" button.
8. Click the "Update" button.

Result: The firmware is updated. The update process is indicated in the information bar.

Once the update is completed, the communication module is restarted. The communication module is ready for operation when the "RUN" LED is lit/flashs green. Note that the startup process takes approx. 1 minute after a firmware update.

The updated firmware is active following the restart.

12.3.2 Update firmware via TIA Portal (STEP 7 Basic / Professional)



This section is intended only for S7 users.

Requirements

- The communication module is connected to the controller or PC via Industrial Ethernet.
- The IP address of the communication module is stored in the module parameters.
- The communication module has been separated from running operation.

Note that performing the update while the application is running can slow down both the update and command processing.

- The required update files were stored locally.

Procedure

Proceed as follows to perform a firmware update of the communication module via STEP 7 Basic / Professional (TIA Portal):

1. Start the TIA Portal.
2. Open your existing project and change to the project view.
3. Change to the network view.
4. Right-click on the desired communication module and click on "Online & Diagnostics" in the shortcut menu.
5. Select the entry "Functions > Firmware Update via Web Interface".
6. Click on the "Web Diagnostics" button.

Reaction: The WBM of the communication module opens in your Web browser.

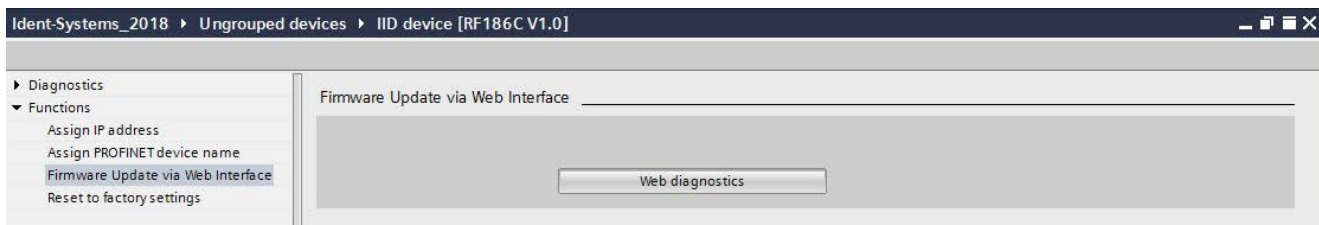


Figure 12-3 Firmware update of the communication module

7. Continue the firmware update as described in the section "Updating the firmware via WBM (Page 167)".

12.3.3 Updating firmware of the readers using the TIA Portal (STEP 7 Basic / Professional)



This section is intended only for S7 users.

Please note that updating the firmware of the readers is currently possible only for the RF200 and RF300 readers. The firmware version to be loaded determines whether the update can be performed.

Requirements

- The communication module is connected to the controller or PC via Industrial Ethernet or PROFINET.
- Readers are connected to the communication module.
- The communication module has been separated from running operation.

Note that performing the update while the application is running can slow down both the update and command processing.

- All user applications are closed.
- The required update file is stored locally.

Procedure

Proceed as follows to perform a firmware update of the reader via STEP 7 Basic / Professional (TIA Portal):

1. Start the TIA Portal.
2. Open your existing project and change to the project view.
3. Change to the network view.
4. Select the affected communication module and switch to the device view.
5. Establish an online connection.
6. Right-click on the desired communication module to which the respective reader is connected and click on "Online & Diagnostics" in the shortcut menu.

7. Select the entry "Functions > Firmware update".

Figure 12-4 Firmware update of the reader

8. In the "Firmware loader" area, click "Browse" and select the update file (*.upd).
9. Select the "Enable firmware after update" check box.
 - Note: If the check box is not selected, the new firmware is only activated on the next startup of the communication module.
10. Click the "Start upgrade" button.

Result: The firmware is updated. The update process is displayed.

12.4 Factory defaults

You can restore the configuration of the communication modules to the factory settings at any time. To reset to the factory settings, you have the following options available:

- Using WBM
- Via SINEC PNI
- Manually via the reader interface

These alternative methods are described below.

12.4.1 Restoring the factory settings via WBM

Requirement

The communication module is connected to the PC via Industrial Ethernet or PROFINET.

Note

IP address is required

Note that you always need the IP address to reset a communication module. If the IP address of a communication module is not known, you can assign a new IP address to the communication module using SINEC PNI. You can find information on assigning an IP address in the section "Assigning the IP address / device name with SINEC PNI (Page 50)".

Procedure

Proceed as follows to reset all settings to the factory settings using the WBM:

1. Start your Web browser.
2. Enter the IP address of the communication module in the address field of your browser.
3. If not logged in, log in to the WBM.
4. Click on the "System" menu item.
5. In the "Reset" area, click on the "Reset" button.

Result: The communication module is reset to its original factory settings. The restore process is indicated in the information bar.

Note that restoring to factory settings assigns the factory-set IP address to the communication module. Because the IP address is discarded, it is possible that the connection between the WBM and browser is lost. You can only recognize when the restore process is completed based on the "RUN" LED. After restoring, the communication module is restarted. The communication module is ready for operation when the "RUN" LED is lit/flashes green.

After restarting the communication module, you may have to assign a new IP address or a new device name to the communication module.

12.4.2 Reset the factory setting with SINEC PNI

Requirement

The reader is connected to the PC via Industrial Ethernet or PROFINET.

Procedure

Proceed as follows to reset all settings to the factory settings using SINEC PNI:

1. Start SINEC PNI.

2. Click on the "Start network scan" button on the toolbar.

Reaction: The network is scanned for connected devices and all recognized devices are displayed in the device list.

3. Select the desired reader in the device list.

4. Click on the "Reset device" button on the toolbar.

Result: The reader is reset to the original factory settings.

Note that restoring to factory settings assigns the factory-set IP address to the reader.

Because the IP address is discarded, it is possible that the connection between the WBM and browser is lost. You can only recognize when the restore process is completed based on the "RUN" LED. After restoring, the reader is restarted. The reader is ready for operation when the "RUN" LED is lit/flashes green.

After restarting the reader, you may need to assign a new IP address or a new device name to the reader.

12.4.3 Restoring the factory settings manually

Requirement

The communication module has been disconnected from the power supply.

Procedure

Proceed as follows to restore all settings to factory defaults using the reader interface:

1. Create a wire jumper (wire diameter ≤ 0.8 mm).
2. Use the jumper to connect pins 4 (RxD) and 7 (TxD) of the reader X21 interface with one another.

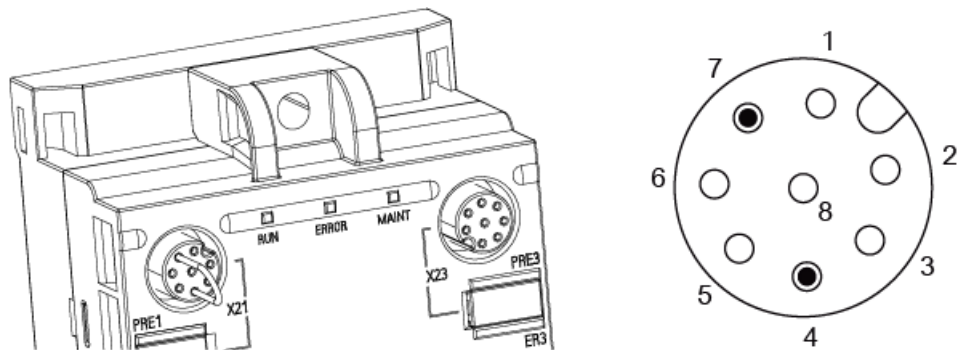


Figure 12-5 Pins of the X21 reader interface to be connected

3. Connect the communication module to the power supply.
4. Wait until all LEDs flash for a few seconds, briefly light up continuously, and then flash again.
5. Remove the jumpers.
6. Wait until the "RUN" LED is continuously lit in green.

Result: The communication module is reset to its original factory settings.

Note that restoring to factory settings assigns the factory-set IP address to the communication module. Because the IP address is discarded, it is possible that the connection between the WBM and browser is lost.

After restarting the communication module, you may have to assign a new IP address or a new device name to the communication module.

12.5 Module replacement

NOTICE

Backing up the configuration

Before replacing a module, save the configuration stored on the communications module so that you can transfer it to the newly connected communications module after replacing the module.

NOTICE

Loading a configuration

Note that you cannot use the configuration file to transfer user profiles and passwords to other communications modules. After loading the configuration file into a new communications module, you may need to enable user management and create new user profiles and passwords.

The following options are available for saving the current configuration of the communications module and restoring it to the newly connected communications module after module replacement:

- On the controller
- With the help of the TIA Portal (STEP 7 Basic / Professional from V15.1) in a STEP 7 project
- Using the WBM on your PC

These alternative methods are described below.

12.5.1 Backup configuration data

These alternative methods are described below.

Table 12- 7 Properties and requirements for the backup options

Backup options	Properties
Backup on the controller	<ul style="list-style-type: none"> Module replacement possible without PG Automatic sequence possible <p>⇒ The automatic sequence needs to be programmed by the user.</p>
Backup in the STEP 7 project	<ul style="list-style-type: none"> Download to the communication module only possible manually via STEP 7 No management of configuration versions <p>⇒ Only the last version is ever stored (no storage of older versions).</p> <p>⇒ You need to update the configuration version in the project yourself manually.</p>
Backup as an *.xml file on the PC	<ul style="list-style-type: none"> Configuration data is saved regardless of the project and controller <p>⇒ The download to the communication module can be performed manually using the WBM user application.</p> <ul style="list-style-type: none"> You can copy additional communication modules of the same type Older configuration versions can be saved (versioning) <p>⇒ The updating and versioning of the configuration versions needs to be started and managed manually by you yourself.</p>

Backup on the controller



Using the "Config_Upload" and "Config_Download" blocks, you can read ("Config_Upload") or write ("Config_Download") the configuration of the communication module ("CM_Configuration_1") via the control program. Since the configuration is stored permanently, you need to reserve a data block for this on the controller.

To ensure that the communication module was replaced correctly, you can read out the version ID (CONFIG_ID) of the communication module and compare this to the Config ID that was stored earlier in the controller with the "Config_Upload" command in the data block. You can also use the device status to check the serial number to see if the device has been replaced.

You can find additional information on programming the blocks and the structure of the configuration data in the section "Config_Upload/Download" of the manual "Ident Profile and Ident Blocks, Standard function for Ident systems".

Backup into a STEP 7 project



From the device view of the TIA Portal, you can access the "Properties" tab of the communication module. When configuring with HSP, in the "Configuration management" entry, you can save the configuration of the communication module in your project and also load this into the communication module again.

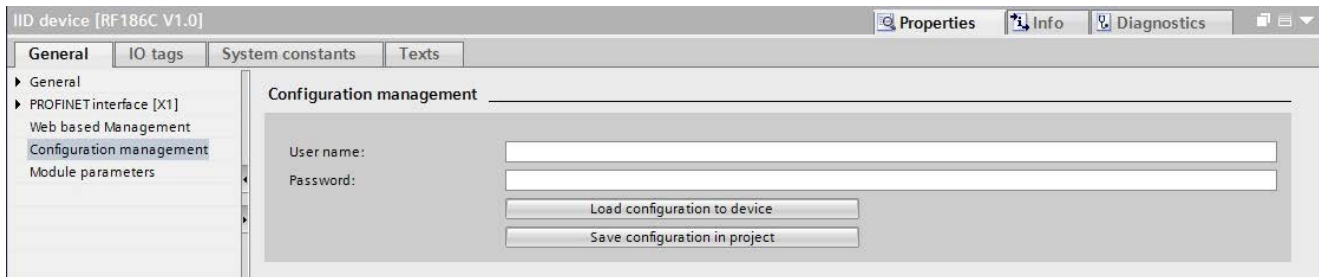


Figure 12-6 Backing up the configuration of the communication module

Requirement

- The "PROFINET interface [X1]" entry contains the correct IP address of the communication module.
- The user name and corresponding password have been entered correctly.
- The entered user has the required rights to run the download/upload (refer to the section "The "User management" menu item (Page 104)").

Note

User name and password only necessary if user management is enabled

The "User name" and "Password" text boxes only need to be completed if the user management of the WBM is enabled.

Following the upload/download, the status bar indicates whether the action was completed successfully.

Backup on your PC



On the upper toolbar of the WBM, there are two buttons for loading and saving configurations. These buttons enable you to save configurations, reload them and transfer them to other communication modules. You will find further information on saving and loading the configuration on or from the PC in the section "The WBM (Page 63)".

12.5.2 Replacing a module

Requirements

- The RF18xC/RF18xCI communication module is mounted. A new RF18xC/RF18xCI communication module of the same type is available.
- The communications module is connected and has started up.

Before replacing a module

 WARNING

Read the manual of the SIMATIC controller you using

Prior to installation, connecting up and commissioning, read the relevant sections in the manual of the SIMATIC controller you are using. When installing and connecting up, keep to the procedures described in the manual.

NOTICE

Backing up the configuration

Before replacing a module, save the configuration stored on the communications module so that you can transfer it to the newly connected communications module after replacing the module.

NOTICE

Installation/removal with the power off

Only wire the SIMATIC controller and the communications modules to be switched on when the voltage is switched off. Make sure that the power supply is turned off when installing/uninstalling the devices.

Procedure

Proceed as follows to replace a communications module (Ethernet/PROFINET connection):

1. Ensure that the communications module is disconnected from the power supply.

If you work via a SIMATIC controller, make sure that this is disconnected from the power supply.

2. Disconnect the cables from the communications module.
3. Remove the communications module.
4. Install the new communications module.
5. Connect the communications module to the PC or the SIMATIC controller using the available Ethernet cable.
6. If necessary, connect the communications module to one or more readers.
7. Connect the communications module to the power supply using the connecting cable.

Wait until the communications module has started up and is ready for operation ("RUN" LED is lit/flashing green).

8. If necessary, assign a unique IP address and a unique device name to the communications module.
9. Load the configuration onto the communications module.
10. Switch on user management if necessary and create new user profiles.

Module replacement with automatic device name assignment

When you replace a module, you have the option of assigning the device names automatically based on the configured PROFINET topology. This function is only possible when replacing a device.

Requirement

- The PROFINET topology has been configured.
- The "Device replacement without exchangeable medium" option is enabled in the PROFINET settings on the CPU.
- The new communications module is in the factory state, i.e. no device name and no IP address have been assigned.

If the communications module is not in the factory state, the factory settings of the module must be restored.

Technical data

13.1 Technical specifications RF185C, RF186C, RF188C

Table 13- 1 Technical specifications of RF18xC

6GT2002-0JEx0	
Product type designation	SIMATIC RF185C SIMATIC RF186C SIMATIC RF188C
Ethernet interface	
Connection type	PROFINET IO, EtherNet/IP, OPC UA, XML
Physical medium	Ethernet over 4-wire cable
Operating mode	100BaseX full duplex
Transmission speed	100 Mbps
Connector	2x M12 interface, 4-pin, D-coded
Max. cable length	100 m
Cable type	STP Cat 5
Autonegotiation	Yes
Autocrossing	Yes
Switch function	Yes, internal
PROFINET RT	Yes
Vendor ID	0x002A
Device ID	0x0C06
Reader interface	
Connector	M12 coupler plugs, 8-pin, A-coded
Connectable readers	<ul style="list-style-type: none"> • RF185C: 1 x reader • RF186C: 2 x reader • RF188C: 4x reader
Transmission speed	19.2 ... 921.6 Kbaud ¹⁾
Max. cable length	<ul style="list-style-type: none"> • 700 m at 115.2 Kbaud • < 100 m at 921.6 Kbaud dependent on reader (preassembled cables 2 ... 50 m; for other standard cables and custom assembled cables, refer to the section "Connecting cables to the reader")

6GT2002-0JEx0	
Electrical data	
Supply voltage ²⁾	
• Rated value	• 24 VDC
• Permitted range	• 20 to 30 VDC
Current consumption without reader	Typ. 130 mA
Current draw via reader interfaces	max. 800 mA each, at 24 V DC
Mechanical data	
Dimensions (W × H × D)	60 × 165 × 45 mm
Weight	Approx. 260 g
Environmental conditions	
Ambient temperature	
• During operation	• -25 ... +55 °C
• During transportation and storage	• -40 ... +70 °C
Degree of protection	IP67
Oscillation, vibration in operation (according to IEC 60068-2-27)	0.75 mm (10 ... 58 Hz) 4 g (58 ... 150 Hz)
Shock resistance, shock in operation (according to IEC 60068-2-6)	30 g
MTBF (at 40°C)	70 years
Approvals	<ul style="list-style-type: none"> • CE • cULus (file E85972) • FCC Code of Federal Regulations, CFR 47, Part 15, Sections 15.107 and 15.109 (Class A) • PNO-certified according to Conformance Class B

¹⁾ Depending on the connected reader.

²⁾ All supply and signal voltages must be safety extra low voltage (SELV/PELV according to IEC 61140) 24 V DC supply: Safety (electrical) isolation of low voltage (SELV/PELV acc. to IEC 61140)

13.2 Technical specifications for RF186CI, RF188CI

Table 13- 2 Technical specifications of RF18xCi

6GT2002-0JEx0	
Product type designation	SIMATIC RF186CI SIMATIC RF188CI
Ethernet interface	
Connection type	PROFINET IO, EtherNet/IP, OPC UA, XML
Physical medium	Ethernet over 4-wire cable
Operating mode	100BaseX full duplex
Transmission speed	100 Mbps
Connector	2x M12 interface, 4-pin, D-coded
Max. cable length	100 m
Cable type	STP Cat 5
Autonegotiation	Yes
Autocrossing	Yes
Switch function	Yes, internal
PROFINET RT	Yes
Vendor ID	0x002A
Device ID	0x0C06
Reader interface	
Connector	M12 coupler plugs, 8-pin, A-coded
Connectable readers	<ul style="list-style-type: none"> RF186CI: 2 x reader RF188CI: 4x reader
Transmission speed	19.2 ... 921.6 Kbaud ¹⁾
Max. cable length	<ul style="list-style-type: none"> 700 m at 115.2 Kbaud < 100 m at 921.6 Kbaud dependent on reader (preassembled cables 2 ... 50 m; for other standard cables and custom assembled cables, refer to the section "Connecting cables to the reader")
I/O interface	
Connector	M12 interface, 5-pin, A-coded
Max. cable length	20 m
Connectable I/O devices	<ul style="list-style-type: none"> Input Output IO-Link module (Input/Output module; Class A, B)

6GT2002-0JEx0	
Electrical data	
Supply voltage ²⁾	
• Rated value	• 24 VDC
• Permitted range	• 20 to 30 VDC
Current consumption without reader	Typ. 130 mA
Current draw via reader interfaces	max. 800 mA each, at 24 V DC
Current consumption via I/O interfaces	
• Class A	• max. 150 mA each, at 24 V DC
• Class B	• max. 500 mA each, at 24 V DC
Mechanical data	
Dimensions (W × H × D)	60 × 165 × 45 mm
Weight	Approx. 260 g
Environmental conditions	
Ambient temperature	
• During operation	-25 ... +55 °C
• During transportation and storage	-40 ... +70 °C
Degree of protection	IP67
Oscillation, vibration in operation (according to IEC 60068-2-27)	0.75 mm (10 ... 58 Hz) 4 g (58 ... 150 Hz)
Shock resistance, shock in operation (according to IEC 60068-2-6)	30 g
MTBF (at 40°C)	70 years
Approvals	<ul style="list-style-type: none"> • CE • cULus (file E85972) • FCC Code of Federal Regulations, CFR 47, Part 15, Sections 15.107 and 15.109 (Class A) • PNO-certified according to Conformance Class B

¹⁾ Depending on the connected reader.

²⁾ All supply and signal voltages must be safety extra low voltage (SELV/PELV according to IEC 61140) 24 V DC supply: Safety (electrical) isolation of low voltage (SELV/PELV acc. to IEC 61140)

Dimension drawings

All dimensions in [mm].

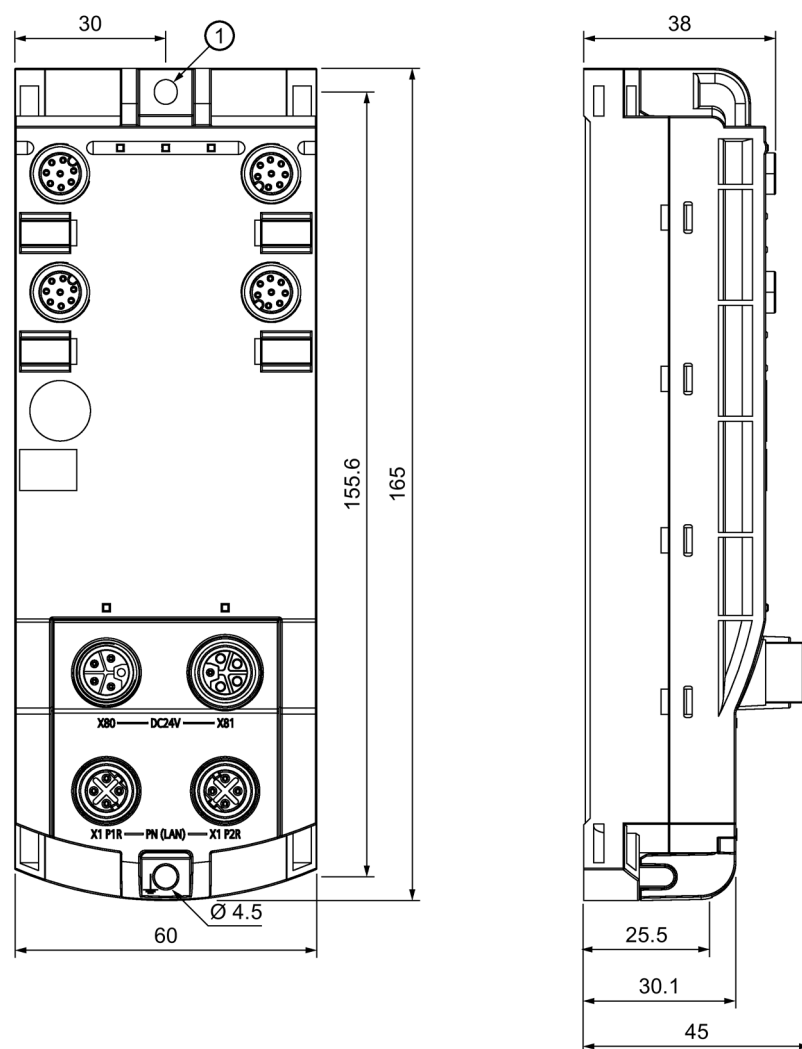


Figure 14-1 Dimension drawing of an RF18xC communication module

The figure shows an RF188C communication module.

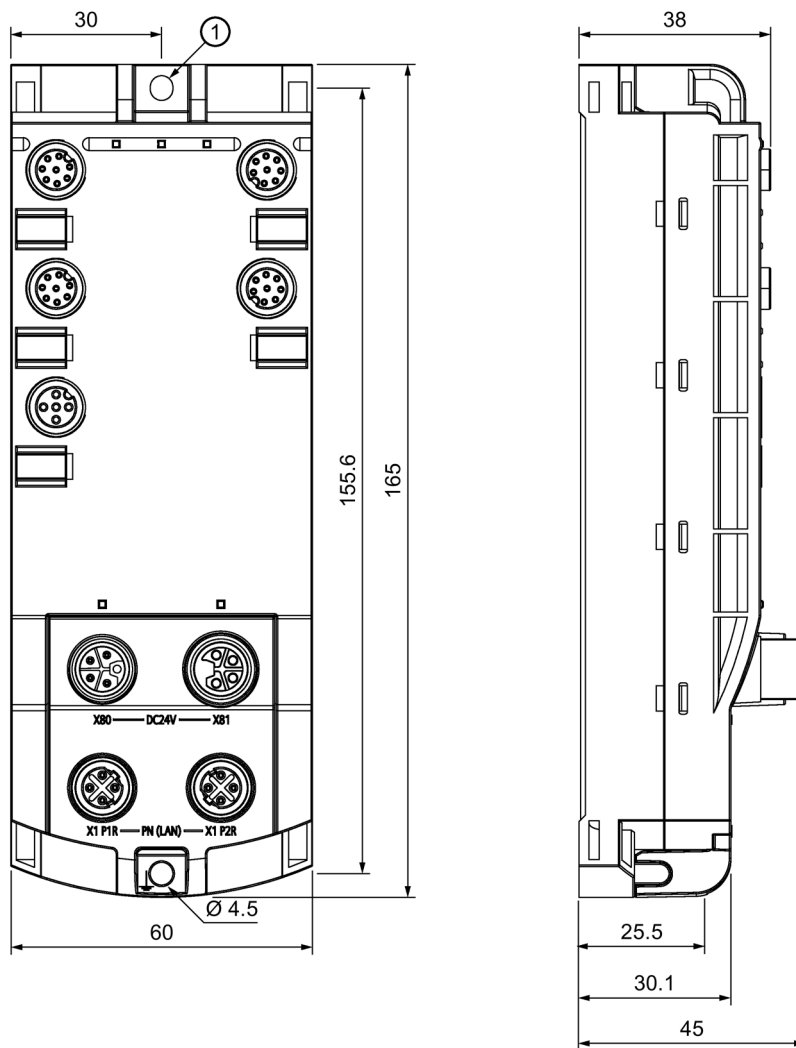


Figure 14-2 Dimension drawing of an RF18xCI communication module

The figure shows an RF188CI communication module.

Appendix

A.1 System planning

The SIMATIC RF18xC/RF18xCI communication module is only one of many devices in the SIMATIC Ident portfolio. In addition to the communications module, an industrial identification system also consists of a higher-level controller/PC, connecting cables, as well as readers and/or optical readers. The following tools support you in compiling and planning your Ident system with all relevant components:

- TIA Selection Tool (<http://www.siemens.com/tia-selection-tool>)
- SIMATIC Ident Configuration Guide (<https://support.industry.siemens.com/cs/ww/en/view/67384964>)

TIA Selection Tool

The TIA Selection Tool offers you a free configuration wizard with which you can easily and quickly assemble all relevant automation products into a complete system. The TIA Selection Tool can create a complete order list from your product selection or product configuration.

SIMATIC Ident Configuration Guide

The SIMATIC Ident Configuration Guide is an ID-specific guide that supports you in selecting the products relevant for your Ident system by clearly displaying all compatible devices and connecting cables.

A.2 Connecting cables

A.2.1 Standard cables

Available cables

- Connecting cable/extension cable M12 ↔ M12 for RF200, RF300, RF600, RF1000, MV400 and MV500

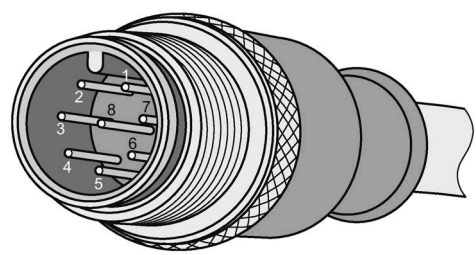
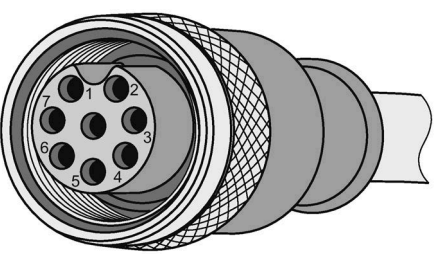
l = 2 m, 5 m, 10 m, 20 m, 50 m

Note: Please note the manuals of the connected systems/devices in this regard.

- Industrial Ethernet cable
- 24 V supply voltage
- IO-Link cable

Pin assignment

Table A- 1 Connecting cable/extension cable M12 ↔ M12

M12 connector (male)		M12 connector (female)	
	1	1	
	2	2	
	3	3	
	4	4	
	5	5	
	6	6	
	7	7	
	8	8	

A.2.2 Custom assembled connecting cables

As an alternative to the preassembled standard cables, you can assemble cables individually for many configurations. A reader connector with screw terminals is available for self-assembly (see the relevant system manual). Cables and reader connectors can be ordered using the TIA Selection Tool or the SIMATIC Ident Configuration Guide.

Maximum cable length of the connecting cables

The readers (RS232) connected to the communication module can be operated with a maximum cable length of 50 m. In some situations, longer connecting cables up to 1000 m are possible for connection via RS422. Please note that a transfer speed of 115.2 Kbaud can only be guaranteed for a max. cable length of 700 m and a transmission speed of 921.6 Kbaud only for a max. cable length of 100 m. The current consumption of the connected reader must, however, be taken into account. You will find further information in the relevant system manuals.

Joining more than two cables to form a long cable should be avoided due to the additional contact resistances.

Requirements for cables and connectors

You need cables of the following specifications for a custom assembled cable:

- 6 x 0.25 mm²
- L-YC11Y 6 x 1 x 0.25
50 m: 6GT2090-4AN50
120 m: 6GT2090-4AT12
800 m: 6GT2090-4AT80

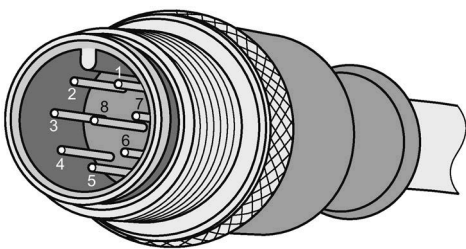
You can use the following connectors:

- CM-sided: M12/8-pin, male
6GT2090-0BE00
- Reader-sided: M12/8-pin, female
6GT2090-0BD00

Pin assignment

The pin assignment is listed in the following table.

Table A- 2 Pin assignment

M12 connector (male)	Pin	Assignment		Core color
		RS422	RS232	
	1	+24 V	+24 V	Note data sheet provided by cable manufacturer
	2	-RxD	--	
	3	0 V	0 V	
	4	+RxD	RxD	
	5	+TxD	+5 V	
	6	-TxD	--	
	7	--	TxD	
	8	Functional ground / shielding	Functional ground / shielding	

A.3 Operation of optical handheld readers, access control readers or serial devices

The manuals of the relevant devices contain information on the parameterization options for the devices stated in the following:

- SIMATIC MV320 (<https://support.industry.siemens.com/cs/ww/en/ps/15157/man>)
- SIMATIC RF1000 (<https://support.industry.siemens.com/cs/ww/en/ps/24223/man>)

You will find the parameter assignment options of other serial devices in the manuals of the respective device vendor.

A.3.1 Compatible Ident devices

The following Ident devices can be operated using the communication module via the Freeport protocol and the RS232 interface:

- SIMATIC MV320
- SIMATIC RF1040R/RF1070R

You can also connect any serial device to the communication module because the communication module can use the Freeport protocol to communicate with serial devices (e.g. bar code scanner, intelligent sensor or other automation components with serial connection). For communication modules with four serial interfaces, only two interfaces support RS232.

A.3.2 Connecting handheld readers / access control readers / serial devices

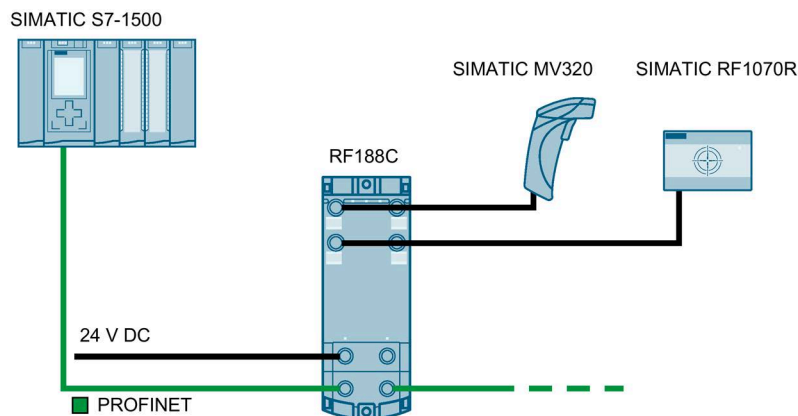


Figure A-1 Example of a cabling setup

The coiled connecting cable of the optical handheld readers SIMATIC MV320 has a length of 1.6 m. Due to its coiling, it can be extended to a length of 4 m during operation. A preassembled cable is also available for connection of the SIMATIC RF1040R/RF1070R readers.

When connecting general serial devices, you need to assemble the cable yourself for the specific device. You will find detailed information on this topic in section "Custom assembled connecting cables (Page 186)".

Power supply

The connected field device can be supplied with power via the communication module if the performance data of the communication module is not exceeded. Note the technical specifications of the RF18xC/RF18xCI in this respect: 24 V max. 0.8 A or 5 V max. 0.6 A.

A.3.3 Hardware configuration

The optical handheld readers and access control readers can be integrated into SIMATIC automation systems using STEP 7 Basic / Professional (TIA Portal) or STEP 7 Classic (SIMATIC Manager).

Note that the "Freeport" protocol can only be used for a connection via PROFINET and EtherNet/IP.

Below the configuration via the TIA Portal is described. Information on configuring other serial devices is available in the respective manuals.

Requirement

The optical handheld reader / the RF1040R/RF1070R is connected to the controller via the communication module and has started up. The TIA Portal has been started. You have created a project.

Procedure

Proceed as follows to configure the communication module:

1. Switch to the device view of the communication module and drag the "Freeport" submodule from the hardware catalog to the module of the communication module.
2. Select the user mode "FB 45" or "Ident profile".
3. Set all other parameters (see below) as required and download the configuration to the controller.

Configuring the optical handheld readers

To allow the operation of the optical handheld readers via the RS232 interface with the communication module you need to configure the handheld readers appropriately.

Note

Codes in the product information

The optical handheld readers and the connecting cables are supplied with product information with configuration codes.

For communication between the communication module and the reader, you must set the following identical parameters in both modules:

- Interface: RS-232
- Transmission speed: 115.2 kBd
- Data bits: 8
- Parity: None
- Stop bits: 1

Configuring the RF1040R/RF1070R reader

No further settings need to be made for the RF1040R/RF1070R reader. In its delivery state, the reader is set so that it can be operated both via USB as well as the R232 interface.

A.3.4 Functions and commands

Communication can be established using the ident blocks / the ident profile and the function block FB 45. The "Write" command handles the sending of data and the "Read" command the receipt of data.

Table A- 3 Compatible controllers/program blocks

Program blocks	Controllers		
	S7-300 / S7-400 and STEP 7 V5.5	S7-1200 and STEP 7 Basic/Professional	S7-1500 and STEP 7 Basic/Professional
FB 45	Yes	No	No
Ident profile/Ident blocks as of V2.0	Yes	Yes	Yes

The following table shows the block-specific commands that you can execute with serial field devices.

Table A- 4 Overview of the commands

Program blocks	Command	Description
FB 45	Init_run	Initialize the device The parameter value "option_1" can be set to "0" or "2". Further input is unnecessary.
	Read	Read data <ul style="list-style-type: none"> Address "0x0000" The length of the valid data is entered in the first 2 bytes of the result. The user data is entered starting at the third byte. Max. net data 231 bytes; no error message if the length is exceeded Address "0x0002" No length information in the result; max. net data 233 bytes
	Write	Sending data The address must be specified as "0xFFFF". Max. net data 233 bytes (without length information); no error message if the length is exceeded
Ident blocks ¹⁾	Read	Read data <ul style="list-style-type: none"> Address "0x0000" The length of the valid data is entered in the first 2 bytes of the result. The user data is entered starting at the third byte. Max. net data 227 bytes; no error message if the length is exceeded Address "0x0002" No length information in the result; max. net data 229 bytes
	Write	Sending data The address must be specified as "0xFFFF". Max. net data 194 bytes (without length information); no error message if the length is exceeded

Program blocks	Command	Description
	Reset_Univ	Reset the communication between CM and device and empty the buffer. The 11th byte ("option_1") of parameter "PARAM" can be occupied by "0x0" or "0x02". The value "0x04" must be entered in the first byte, and "0x0A" in the 6th byte. When using the technology object, the command "Reset_Reader" can be used as an alternative.
	Reset_Reder	As an alternative to the "Reset_Univ" command, this command can be used with using the technology object "SIMATIC Ident > TO_Ident".

1) When using Rockwell controllers, the commands are identical to those of the Ident blocks.

You will find more information on programming in the corresponding function manual.

You can find detailed information on the commands and error messages of the RF1040R/RF1070R in the "Programming" section of the "SIMATIC RF1000" manual. The system job frames displayed must be stored in the data area for the "Write" command. The answer message frames are output in the data block following a "Read" command.

Notes on the commands and functions

Init_run

Communication with the CM is initialized with the "Init_run" (RESET command). The RESET command does not have reader-specific parameters and triggers the deletion of the buffers.

After the "Init_run" the communication module is ready for operation.

Read

When the "Read" command is started, the data that the CM has already received is transferred to the controller.

If the "Read" command is started before the CM has received data, the command remains active until the CM has received data that is then transferred to the controller. An active "Read" command can be canceled with an "Init_run"/"Write_Config" command.

The presence bit ("TP" or "ANZ_MDS_present") indicates that the CM has received new data and that this data is available for fetching with a "Read" command. After data transmission to the controller, the presence bit is reset unless new data has already been received.

When doing this, note the buffer size and the buffer overflow. If the receive buffer of the CM is full, existing data is overwritten by newly received data.

A.3.5 Block-specific error messages

Table A- 5 Block-specific error messages

Block	Error ID	Meaning
FB 45	0x06	Negative acknowledgment or bad frame from the reader
	0x05	Unknown command, incorrect command parameters or forbidden command chaining (wrong length information)
	0x0D	Address error in the command (\neq "0x0000", "0x0002", "0xFFFF")
	0x12	Internal communication error
	0x13	New data was received before existing data was fetched. <ul style="list-style-type: none"> Scan operation: The newest data is lost. With the "Write" command the oldest acknowledgments are lost without an error message being generated.
	0x18	"Init_Run" necessary
	0x1F	Active command was canceled by "Reset" (init_run) or bus connector was unplugged
Ident profile	0xE2FE01	Negative acknowledgment or bad frame from the reader
	0xE6FE01	Unknown command, incorrect command parameters or forbidden command chaining (wrong length information)
	0xE1FE03	Address error in the command (\neq "0x0000", "0x0002", "0xFFFF")
	0xE4FE8D	Internal communication error
	0xE4FE04	New data was received before existing data was fetched. <ul style="list-style-type: none"> Scan operation: The newest data is lost. With the "Write" command the oldest acknowledgements are lost without an error message being generated.
	0xE6FE05	"Reset_Reader" necessary
	0xE5FE04	Invalid data block number (DBN) on the reader/communication module

A.4 Compatibility with SIMATIC RF180C

Some of the SIMATIC RF18xC/RF18xCI communication module features are different than those of the predecessor model SIMATIC RF180C. However, these can be migrated or replaced taking into account the following differences.

Differences in hardware

The differences in the module hardware are as follows:

- The width of the two modules RF180C and RF18xC/RF18xCI is the same for both with 60 mm. The two modules differ regarding the height, depth and position of the fixing screws. See the dimension drawings of the two modules.
- The RF18xC communication module has an L-coded M12 connector for power supply and forwarding. When replacing an RF180C with a M12 7/8" terminal block, for example, with an RF18xC, you need an adapter from M12 7/8" to M12 L-coded.

Differences in the configuration/parameter assignment

You must take the following differences into account during configuring:

- SIMATIC RF180C

The CM has one module in the hardware configuration for both channels.

- SIMATIC RF18xC

The CM has one module in the hardware configuration for each channel.

The channel differences have an effect on addressing in the "HW_Connect" variable or in the technology object.

Parameter assignment with the technology object:

- SIMATIC RF180C:

In the "Ident device" parameter, select the module "2x RS422 channel_1" of the RF180C for both channels. Depending on the channel in which the module is used, you must adapt the module name accordingly ("_2" for channel 2).

- SIMATIC RF18xC

In the "Ident device" parameter, select the module of the corresponding channel (e.g. "Reader_1" for "Channel1").

Parameter assignment with the "HW_Connect" variable:

- SIMATIC RF180C

When you establish the connection via an S7-1200/-1500 controller, enter the value "2x RS422 channel_1" in the "HW_ID" parameter of the module.

In the "CM_CHANNEL" parameter, enter the value "1" for channel 1 and the value "2" for channel 2.

In the "LADDR" parameter, enter the value "2x RS422 channel_1" in the start address of the module.

- SIMATIC RF18xC

When you establish the connection via an S7-1200/-1500 controller, enter the corresponding module in the "HW_ID" parameter.

Always enter the value "1" in the "CM_CHANNEL" parameter.

In the "LADDR" parameter, enter the start address of the corresponding module.

STEP 7 migration

To migrate an RF180C communication module to an RF18xC, proceed as follows:

1. Open your existing project.
2. Open the device configuration and replace the respective RF180C communication module with an RF18xC communication module in the "Devices & networks" folder.
3. Apply the module parameters of the RF180C for each reader module of the RF18xC.
4. Assign parameters to the RF18xC communication module.
 - Parameter assignment with the technology object:

In the technology objects, replace the RF180C modules with the corresponding reader modules of the RF18xC.
 - Parameter assignment with the "HW_Connect" variable:

Adapt the "CM_CHANNEL" and "LADDR" parameters in the "HW_CONNECT" variable. When you establish the connection via an S7-1200/-1500 controller, you must also adapt the "HW_ID" parameter.

A.5 Ordering data

Table A- 6 Ordering data

	Article number
Communication module RF185C for PROFINET IO; max. 1 reader can be connected	6GT2002-0JE10
Communication module RF186C for PROFINET IO; max. 2 readers can be connected	6GT2002-0JE20
Communication module RF188C for PROFINET IO; max. 4 readers can be connected	6GT2002-0JE40
Communication module RF186CI for PROFINET IO with I/O interface; max. 2 readers can be connected	6GT2002-0JE50
Communication module RF188CI for PROFINET IO with I/O interface; max. 4 readers can be connected	6GT2002-0JE60

Table A- 7 Ordering data - Accessories

	Article number
IO-Link module K20, 4 DI with 4 digital inputs	3RK5010-0BA10-0AA0
IO-Link module K20, 8 DI with 8 digital inputs	3RK5010-0CA00-0AA0
Connecting cable for RF200 / RF300 / RF600 / MV440 M12-180 / M12-180	2 m 6GT2891-4FH20
	5 m 6GT2891-4FH50
	10 m 6GT2891-4FN10
	20 m 6GT2891-4FN20
	50 m 6GT2891-4FN50
Connecting cable for RF200 / RF300 / RF600 / MV440 M12-180 / M12-90	2 m 6GT2891-4JH20
	5 m 6GT2891-4JH50
	10 m 6GT2891-4JN10
CM adapter cable for MV500	0.5 m 6GF3500-8BA11
	5 m 6GF3500-8BA12
CM connecting cable for MV320	1.6 m 6GT2191-0BH50
CM connecting cable for RF1000	2.0 m 6GT2891-4UH20

		Article number
Power supply cable L-coded, 4-pin M12-180	0.5 m	6XV1801-6DE50
	1.0 m	6XV1801-6DH10
	1.5 m	6XV1801-6DH15
	2.0 m	6XV1801-6DH20
	3.0 m	6XV1801-6DH30
	5.0 m	6XV1801-6DH50
	10 m	6XV1801-6DN10
	15 m	6XV1801-6DN15
Power supply cable L-coded, 4-pin M12-90	0.5 m	6XV1801-6GE50
	1.0 m	6XV1801-6GH10
	1.5 m	6XV1801-6GH15
	2.0 m	6XV1801-6GH20
	3.0 m	6XV1801-6GH30
	5.0 m	6XV1801-6GH50
	10 m	6XV1801-6GN10
	15 m	6XV1801-6GN15
Power supply cable sold by the meter 4 x 1.5 mm ²		6XV1801-2B
Field-fabricated connector for power supply cable socket (female)		6GK1906-0EB00
Field-fabricated connector for power supply cable connector (male)		6GK1906-0EA00
Industrial Ethernet cable D-coded M12-180 / M12-180	0.3 m	6XV1870-8AE30
	0.5 m	6XV1870-8AE50
	1.0 m	6XV1870-8AH10
	1.5 m	6XV1870-8AH15
	2.0 m	6XV1870-8AH20
	3.0 m	6XV1870-8AH30
	5.0 m	6XV1870-8AH50
	10 m	6XV1870-8AN10
	15 m	6XV1870-8AN15
Industrial Ethernet cable D-coded M12-90 / M12-90	0.3 m	6XV1870-8GE30
	0.5 m	6XV1870-8GE50
	1.0 m	6XV1870-8GH10
	1.5 m	6XV1870-8GH15
	2.0 m	6XV1870-8GH20
	3.0 m	6XV1870-8GH30
	5.0 m	6XV1870-8GH50
	10 m	6XV1870-8GN10
	15 m	6XV1870-8GN15

		Article number
Industrial Ethernet cable D-coded M12-180 / IE FC RJ45	2.0 m	6XV1871-5TH20
	3.0 m	6XV1871-5TH30
	5.0 m	6XV1871-5TH50
	10 m	6XV1871-5TN10
	15 m	6XV1871-5TN15
IO-Link cable (Class A) M12-180 / M12-180	1.5 m	3RK1902-4PB15-3AA0
	5.0 m	6GT2891-4MH50
	10 m	6GT2891-4MN10
IO-Link cable (Class B) A-coded, 5-pin M12-180 / M12-180	0.5 m	6XV1801-2CE50
	1.0 m	6XV1801-2CH10
	1.5 m	6XV1801-2CH15
	2.0 m	6XV1801-2CH20
	3.0 m	6XV1801-2CH30
	5.0 m	6XV1801-2CH50
	10 m	6XV1801-2CN10
	15 m	6XV1801-2CN15
Connection cable for wide-range power supply L-coded, 4-pin / A-coded, 4-pin M12-180 / M12-180	5 m	6GT2091-0PH50
M12 sealing caps for unused connections (10 units) Usable as of product version "02"		3RX9802-0AA00
DVD "RFID Systems Software & Documentation"		6GT2080-2AA20

A.6 Certificates & approvals

Note

Granted approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

Current approvals

SIMATIC NET/SIMATIC Ident products are regularly submitted to the authorities and approval centers for approvals relating to certain markets and applications.

Contact your Siemens representative if you need a list of the current approvals for the individual devices or check the Internet pages of Siemens Industry Online Support:

Current approvals (<https://support.industry.siemens.com/cs/ww/en/ps/15728/cert>)

Go to the relevant product there and select the "Certificates" entry type from the "Entry list" tab.

Overview of the approvals and standards

The RF185C/RF186C/RF188C/RF186CI/RF188CI communication modules have the following approvals and meet the following standards:

- EC directives and standards
 - EU directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive) according to the following standards:
EN 61000-6-1, EN 61000-6-2, EN 61000-6-3, EN 61000-6-4, EN 55032, EN 55024
 - EU Directive 2011/65/EU "Restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS)
- cULus LISTED IND. CONT. EQ.
- FCC

EU Declaration of Conformity



The RF185C/RF186C/RF188C/RF186CI/RF188CI communication modules meet the general and safety-related requirements of the following EU directives and conform to the harmonized European standards (EN) for programmable controllers published in the official gazettes of the European Union and here:

- EU directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive)
 - Immunity
EN 61000-6-2: Industrial area
 - Noise emission
EN 55032: Electromagnetic Compatibility of Multimedia Devices and Equipment - Requirements for emissions
- EU Directive 2011/65/EU "Restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS)

The CE Declaration of Conformity is available for the responsible authorities at the following address:

Siemens Aktiengesellschaft
Process Industries and Drives
Process Automation
D-76181 Karlsruhe
Germany


You will find the CE Declaration of Conformity for this product on the Internet at the following address:

CE declaration of conformity (<https://support.industry.siemens.com/cs/ww/en/ps/15105/cert>)

Country-specific approvals

Safety

If the device has one of the following markings, the corresponding approval has been obtained.

Marking	Description
	Underwriters Laboratories Inc. in accordance with <ul style="list-style-type: none"> • UL 61010-1, UL 61010-1-12 • UL 61010-2-201 • File E85972
	USA (FCC) This device complies with part 15 of the FCC rules.
	EAC (Eurasian Conformity) Eurasian Economic Union of Russia, Belarus, Armenia, Kazakhstan and Kyrgyzstan Declaration of conformity according to the technical regulations of the customs union (TR ZU)
	South Korea (KCC) Korea Communications Commission Certificate of Broadcasting and Communication Equipments

Syslog messages

B.1 Structure of the Syslog messages

The Syslog server collects all log information of the devices and informs you about specific events. The Syslog messages are received from the Syslog server over the configured UDP port (default: 514) and sent according to RFC 5424 or RFC 5426.

Syslog messages log information during access to the device. Information can be status information, such as the origin of the message or a time stamp. The Syslog protocol prescribes a specified order and structure of the possible parameters. Syslog messages are structured as follows in accordance with RFC 5424:

Table B- 1 Structure of the Syslog messages

Parameter	Explanation
HEADER	
PRI	Within PRI, the priority of the Syslog message is coded into Severity (severity of the message) and Facility (origin of the message).
VERSION	Version number of the Syslog specification.
TIMESTAMP	The device sends the time stamp in the format "2010-01-01T02:03:15.0003+02:00" as local time including time zone and adjustment for daylight saving time/standard time, if necessary.
HOSTNAME	References the source computer with its name or IP address. IPv4 address according to RFC1035: Bytes in decimal form: XXX.XXX.XXX.XXX If there is no information, "-" is output.
APP-NAME	Device or application from which the message originates. This parameter is not used by the device and "-" is always output.
PROCID	The process ID is used to clearly identify the individual processes, for example, during analysis and troubleshooting. This parameter is not used by the device and "-" is always output.
MSGID	ID for identification of the message. This parameter is not used by the device and "-" is always output.
STRUCTURED-DATA	
timeQuality	The structured data element "timeQuality" provides information on the system time. The "tzKnown" parameter specifies whether the sender knows its time zone (value "1" = known; value "0" = unknown). The "isSynced" parameter specifies whether the sender is synchronized with a reliable external time source, e.g. via NTP (value "1" = synchronized; value "0" = not synchronized).
sysUpTime	The "sysUpTime" parameter is metainformation about the message. It specifies the time (in hundredths of a second) since the last reinitialization of the network management part of the system.
MSG	
MESSAGE	Message as ASCII string (English)

Note**Additional information**

You can find additional information on the structure of Syslog messages and the meaning of the parameters in the RFC 5424.

<https://tools.ietf.org/html/rfc5424>

B.2 Variables in Syslog messages

The variables are displayed in the "Syslog messages" section in the "Message text" field with curly brackets {variable}.

The output messages can contain the following variables:

Table B- 2 Possible variables in Syslog messages

Variable	Description	Format	Possible values or example
{Ip address}	IPv4 address to RFC1035	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105
{Protocol}	Layer 4 protocol used or service that has generated the event.	%s	TCP WBM PNIO PB OPC EIP
{User name}	Character string (without spaces) that identifies the authenticated user based on the name.	%s	<name>
{Action user name} or {Destination user name}	Identifies the user based on his/her name This is not the authenticated user.	%s	<First name>.<Name>
{Role}	Symbolic name for the group role.	%s	Administrator User OPC UA
{Time second}	Number of seconds	%d	44
{Max sessions}	Maximum number of sessions	%d	10
{Url}	URL of the Web server that was accessed.	%s	/Engineering/Reset2Factory?r=0.685644556250803 3
{Config detail}	Character string (with spaces) for the configuration.	%s	Power

B.3 List of Syslog messages

This section describes the Syslog messages. The structure of the messages is based on IEC 62443-3-3.

Identification and authentication of human users

Message text	{protocol}: User {user name} logged in from {ip address}.
Example	WBM: User admin logged in from 192.168.0.1.
Explanation	Valid logon information that is provided during logon.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: User {user name} failed to log in from {ip address}.
Example	WBM: User admin failed to log in from 192.168.0.1.
Explanation	Incorrect user name or incorrect password specified during logon.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: User {user name} logged out from {ip address}.
Example	WBM: User admin logged out from 192.168.0.1.
Explanation	User session completed - logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: Default user {user name} logged in from {ip address}.
Example	PNIO: Default user admin logged in from 192.168.0.1.
Explanation	Default user is logged on via the IP address.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

User account management

Message text	Authentication was enabled.
Example	Authentication was enabled.
Explanation	Authentication was enabled.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

B.3 List of Syslog messages

Message text	Authentication was disabled.
Example	Authentication was disabled.
Explanation	Authentication was disabled.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} has changed the password.
Example	WBM: User admin has changed the password.
Explanation	User has changed the password.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} has changed the password of user {Destination user name}.
Example	WBM: User admin has changed the password of user user1.
Explanation	User has changed the password of another user.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} created user-account {Destination user name} with role {Role}.
Example	WBM: User admin created user-account admin2 with role Administrator.
Explanation	The administrator has created an account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Message text	{Protocol}: User {User name} deleted user-account {Destination user name}.
Example	WBM: User admin deleted user-account admin2.
Explanation	The administrator has deleted an existing account.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.3

Enforcement of authorization

Message text	{Protocol}: User {User}: Access to url {url} denied.
Example	WBM: User admin: Access to url /Engineering/Reset2Factory?r=0.6856445562508033 denied.
Explanation	Access to Web resource was denied.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.1

Unsuccessful logon attempts

Message text	{Protocol}: User {User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.
Example	WBM: User admin account is locked for 544 minutes after 2 unsuccessful login attempts.
Explanation	With too many failed logon attempts, the corresponding user account is locked for a specific time.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.11

Session lock

Message text	{Protocol}: The session of user {User name} was closed after {Time second} seconds of inactivity.
Example	WBM: The session of user admin was closed after 310 seconds of inactivity.
Explanation	The current session was locked due to inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

Limiting the number of simultaneous sessions

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Example	WBM: The maximum number of 10 concurrent login sessions exceeded.
Explanation	The maximum number of simultaneous sessions has been exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

Nonrepudiation

Message text	{Protocol}: User {User name} has changed configuration.
Example	OPC: User unknown has changed configuration.
Explanation	User has changed the entire configuration. User could not be found. The "unknown" user is always output.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	{Protocol}: User {User name} has changed {Config detail} configuration.
Example	OPC: User admin has changed Power configuration.
Explanation	User has changed specific configuration.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Message text	{Protocol}: User {User name} has initiated a reset to factory defaults.
Example	WBM: User admin has initiated a reset to factory defaults.
Explanation	User has initiated a reset to factory settings.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Software and information integrity

Message text	Configuration integrity verification failed.
Example	Configuration integrity verification failed.
Explanation	Configuration integrity verification failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

Session integrity

Message text	{Protocol}: Session ID verification failed.
Example	WBM: Session ID verification failed.
Explanation	Session ID is invalid.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.8

Restoration of the automation system

Message text	{Protocol}: Firmware {Version} was activated.
Example	WBM: Firmware V2 was activated.
Explanation	Firmware successfully activated.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Message text	{Protocol}: Firmware activation failed.
Example	WBM: Firmware activation failed.
Explanation	Firmware activation failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Service & Support

Industry Online Support

In addition to the product documentation, you are supported by the comprehensive online information platform of Siemens Industry Online Support at the following Internet address:

Link: (<https://support.industry.siemens.com/cs/de/en/>)

Apart from news, you will also find the following there:

- Project information: Manuals, FAQs, downloads, application examples etc.
- Contacts, Technical Forum
- The option to submit a support request:
Link: (<https://support.industry.siemens.com/My/ww/en/requests>)
- Our service offer:

Right across our products and systems, we provide numerous services that support you in every phase of the life of your machine or system - from planning and implementation to commissioning, through to maintenance and modernization.

You will find contact data on the Internet at the following address:

Link: (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en)

RFID homepage

For general information about our identification systems, visit Homepage (www.siemens.com/ident).

Online catalog and ordering system

The online catalog and the online ordering system can also be found on the Industry Mall home page (<https://mall.industry.siemens.com>).

SITRAIN - Training for Industry

The training offer includes more than 300 courses on basic topics, extended knowledge and special knowledge as well as advanced training for individual sectors - available at more than 130 locations. Courses can also be organized individually and held locally at your location.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address:

Link: (<https://new.siemens.com/global/en/products/services/industry/sitrain.html>)

