SIEMENS

SIPROTEC 5
Communication Protocols

V8.03 and higher

Manual

C53000-L1840-C055-7

NOTE

For your own safety, observe the warnings and safety instructions contained in this document, if available.

Disclaimer of Liability

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Document version: C53000-L1840-C055-7.02

Edition: 02.2020

Version of the product described: V8.03 and higher

Preface

Purpose of the Manual

This manual contains information about:

- Communication within the SIPROTEC 5 family of devices and to higher-level control centers
- Installation of the modules
- Setting parameters in DIGSI 5
- Information on commissioning

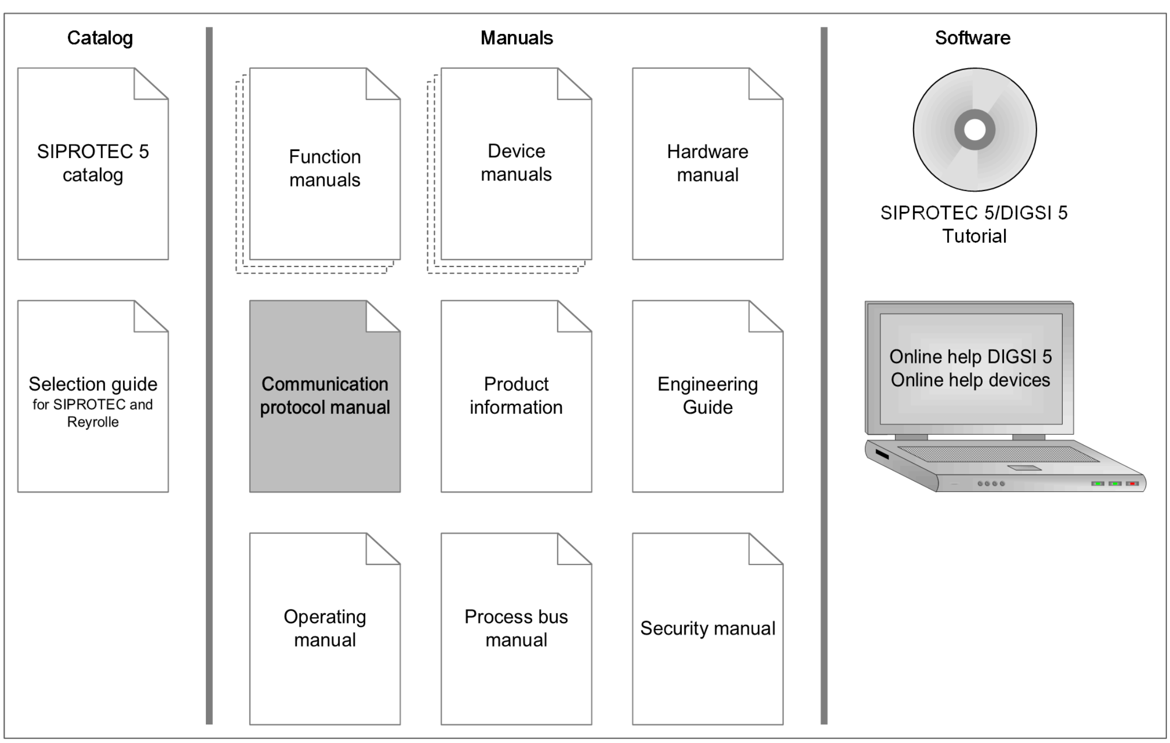
Target Audience

Protection system engineers, commissioning engineers, persons entrusted with the setting, testing and maintenance of automation, selective protection and control equipment, and operational crew in electrical installations and power plants.

Scope

This manual applies to the SIPROTEC 5 device family.

Further Documentation



[dwprecom-221012-01.tif, 4, en_US]

- Device manuals

  Each Device manual describes the functions and applications of a specific SIPROTEC 5 device. The printed manual and the online help for the device have the same informational structure.

- Hardware manual

  The Hardware manual describes the hardware building blocks and device combinations of the SIPROTEC 5 device family.

- Operating manual

  The Operating manual describes the basic principles and procedures for operating and assembling the devices of the SIPROTEC 5 range.

- Communication protocol manual

  The Communication protocol manual contains a description of the protocols for communication within the SIPROTEC 5 device family and to higher-level network control centers.

- Product information

  The Product information includes general information about device installation, technical data, limiting values for input and output modules, and conditions when preparing for operation. This document is provided with each SIPROTEC 5 device.

- Engineering Guide

  The Engineering Guide describes the essential steps when engineering with DIGSI 5. In addition, the Engineering Guide shows you how to load a planned configuration to a SIPROTEC 5 device and update the functionality of the SIPROTEC 5 device.

- DIGSI 5 online help

  The DIGSI 5 online help contains a help package for DIGSI 5 and CFC.

  The help package for DIGSI 5 includes a description of the basic operation of software, the DIGSI principles and editors. The help package for CFC includes an introduction to CFC programming, basic examples of working with CFC, and a reference chapter with all the CFC blocks available for the SIPROTEC 5 range.

- SIPROTEC 5/DIGSI 5 Tutorial

  The tutorial on the DVD contains brief information about important product features, more detailed information about the individual technical areas, as well as operating sequences with tasks based on practical operation and a brief explanation.

- SIPROTEC 5 catalog

  The SIPROTEC 5 catalog describes the system features and the devices of SIPROTEC 5.

- Selection guide for SIPROTEC and Reyrolle

  The selection guide offers an overview of the device series of the Siemens protection devices, and a device selection table.

Angaben zur Konformität

This product complies with the directive of the Council of the European Communities on harmonization of the laws of the Member States concerning electromagnetic compatibility (EMC Directive 2014/30/EU), restriction on usage of hazardous substances in electrical and electronic equipment (RoHS Directive 2011/65/EU), and electrical equipment for use within specified voltage limits (Low Voltage Directive 2014/35/EU).

This conformity has been proved by tests performed according to the Council Directive in accordance with the product standard EN 60255-26 (for EMC directive), the standard EN 50581 (for RoHS directive), and with the product standard EN 60255-27 (for Low Voltage Directive) by Siemens.

The device is designed and manufactured for application in an industrial environment.

The product conforms with the international standards of IEC 60255 and the German standard VDE 0435.

Standards

IEEE Std C 37.90

The technical data of the product is approved in accordance with UL.

For more information about the UL database, see *ul.com*

You can find the product with the **UL File Number E194016**.

IND. CONT. EQ.
69CA

Additional Support

For questions about the system, contact your Siemens sales partner.

Customer Support Center

Our Customer Support Center provides a 24-hour service.

Siemens AG
Customer Support Center
Humboldtstrasse 59
90459 Nuremberg
Germany
E-mail: *support.energy@siemens.com*

Training Courses

Inquiries regarding individual training courses should be addressed to our Training Center:

Siemens AG	Phone:	+49 (911) 433-7415
Siemens Power Academy TD	Fax:	+49 (911) 433-7929
Humboldtstrasse 59	E-mail:	*poweracademy@siemens.com*
90459 Nuremberg	Internet:	*www.siemens.com/poweracademy*
Germany		

Notes on Safety

This document is not a complete index of all safety measures required for operation of the equipment (module or device). However, it comprises important information that must be followed for personal safety, as well as to avoid material damage. Information is highlighted and illustrated as follows according to the degree of danger:

DANGER

DANGER means that death or severe injury **will** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

WARNING

WARNING means that death or severe injury **may** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

CAUTION

CAUTION means that medium-severe or slight injuries **can** occur if the specified measures are not taken.

✧ Comply with all instructions, in order to avoid moderate or minor injuries.

NOTICE

NOTICE means that property damage **can** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid property damage.

NOTE

Important information about the product, product handling or a certain section of the documentation which must be given attention.

Table of Contents

1 Communication Modules

1.1 Overview

SIPROTEC devices can be ordered with factory-installed communication modules. The communication modules can also be installed and replaced in the SIPROTEC devices afterwards. You do not have to open the device for this.

NOTE

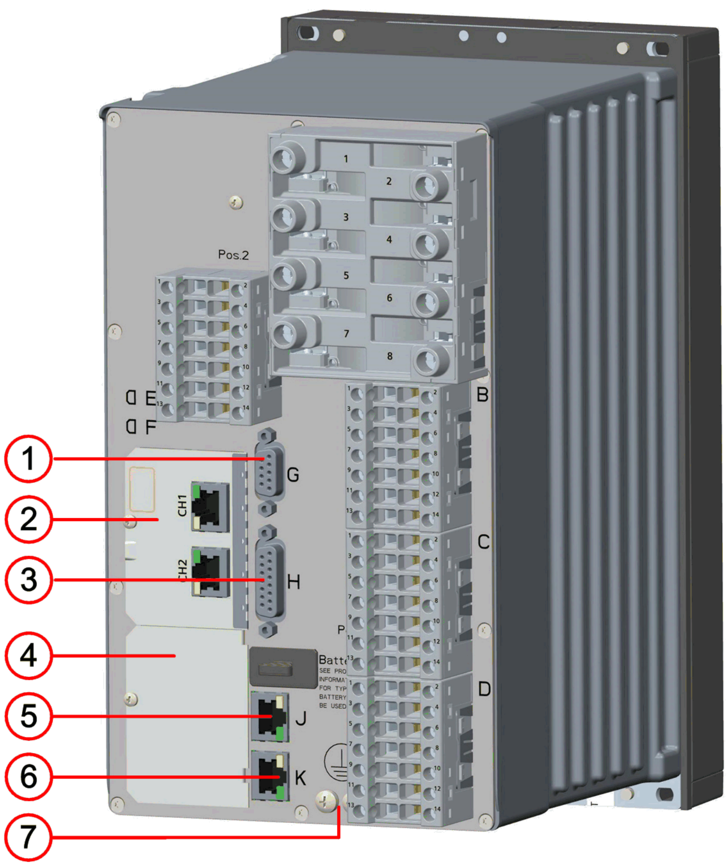
The communication modules available for reordering are not preconfigured. Use DIGSI 5 to carry out the functional adjustment to the required protocol application.

The communication modules can be installed in the base module or the 1/3 module and in the expansion module with the plug-in module assembly CB202. A maximum of 2 communication modules each can be installed. You can use only one CB202 in the device.

The plug-in module assembly CB202 is a printed circuit board assembly with an integrated power supply.

The plug-in module assembly CB202 communicates with the base module via a special connecting cable. This connecting cable (CAT 5 FTP patch cable) is always included in the scope of delivery of the plug-in module assembly CB202 or the devices containing the plug-in module assembly CB202 and needs not be ordered separately.

Ensure that you route the communication lines separately from network circuits.

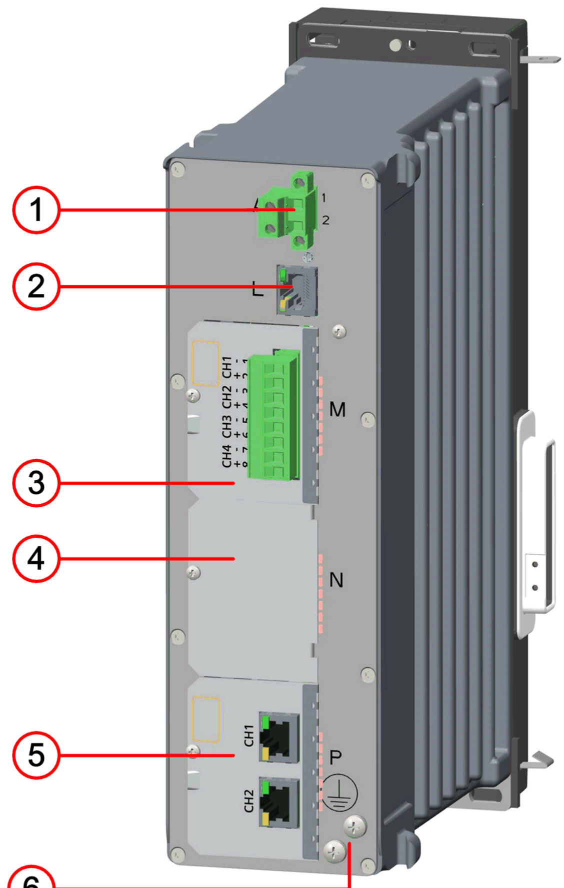


[le_cm201p, 1, --_--]

Figure 1-1 Plug-In Module Positions and Communication Terminals in the Base Module, with Modular Devices

(1)	Time synchronization G
(2)	Plug-in module position E
(3)	Terminal for detached on-site operation panel H

(4) Plug-in module position F
(5) Integrated Ethernet interface J
(6) Connection to expansion module with plug-in module assembly CB202
(7) Protective grounding terminals



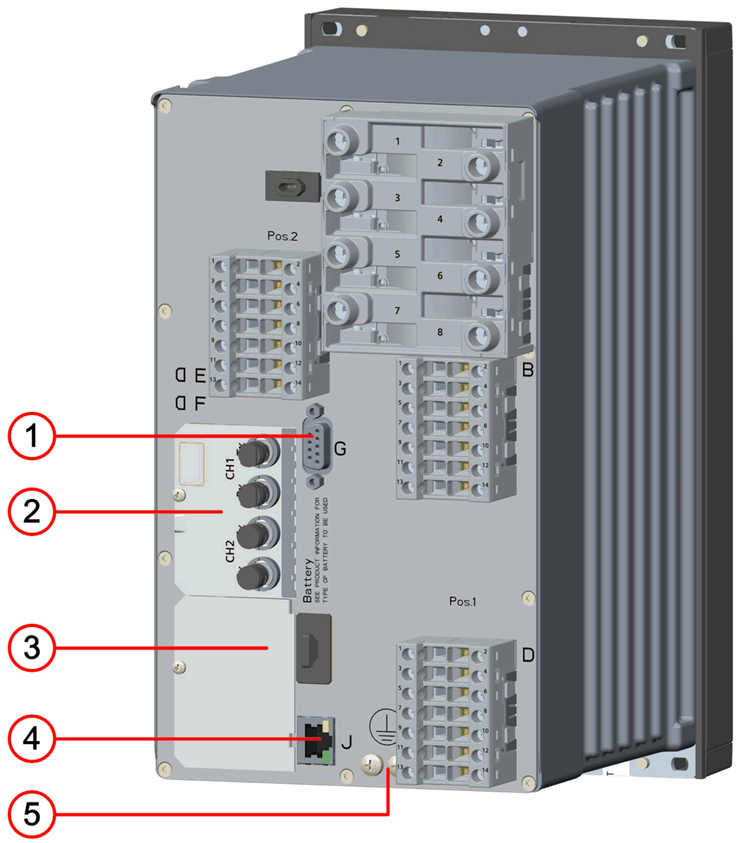
[le_lmnppo, 2, --_--]

Figure 1-2 Plug-In Module Positions and Communication Terminals in the Expansion Module with CB202

(1) 2-pole terminal to connect power supply
(2) COM link L (connection to interface K of the base unit)
(3) Plug-in module position M
(4) Plug-in module position N
(5) Plug-in module position P
(6) Protective grounding terminals

NOTE

You cannot insert any communication module at plug-in module position M. The plug-in module position M is intended for a measuring-transducer module only.



[le_slots and communication terminals, 2, --_--]

Figure 1-3 Plug-In Module Positions and Communication Terminals on the 1/3 Module, for Non-Modular Devices (7xx81, 7xx82)

(1) Time synchronization G
(2) Plug-in module position E
(3) Plug-in module position F (not applicable to 7xx81)
(4) Integrated Ethernet interface J
(5) Protective grounding terminals

The following communication modules can be used for SIPROTEC 5:

- Serial modules

  Application: Communication to the substation automation technology via substation-control protocols

  Protection interface (only optical serial modules) for interfacing to external communication converters for short direct connections.

  2 different communication protocols or 2 different applications can be operated on serial modules with 2 connections. The IEC 60870-5-103 protocol for the substation automation technology as well as a protection interface, for example, can be operated on a serial optical module for close range with 2 connections.

  Assign the protocol application to the corresponding channel of the communication module with DIGSI 5.

- Ethernet Modules
  Application: Ethernet-based communication to the substation automation technology via substation-control protocols (for example, IEC 61850 and DNP3)
  – Secure communication to DIGSI 5
  – Communication between the devices (IEC 61850-GOOSE)
  – Synchrophasor protocol

  The modules can be operated with or without an integrated switch.
- Long-distance modules
  Application: Direct protection interface communication over long distances using multimode or single-mode optical fibers.

The designation of the modules corresponds to the following scheme, which is typically explained with the module USART-AB-1EL. The module designation consists of 3 blocks.

1st block	Type of module
	USART = Serial module for short or long distance
	ETH = Ethernet module
2nd block	Unique code for the module in the product code of the device
	The code consists of 2 letters.
3rd block	Number and physical design of the connections
	1 = 1 connection (1 channel)
	2 = 2 connections (2 channels)
	EL = Electrical connection
	FO = Fiber-optic connection
	LDFO = Long-distance transmission via optical fibers

1.2 Communication Applications of the Plug-In Modules

You can find information on communication applications for the plug-in modules in the following tables.

Plug-In Modules for the Communication

Table 1-1 Communication Applications and Plug-In Modules

Port or Plug-In Module	Front Interface	Port G: Time Synchronization	Port J: Integrated Ethernet	Module Type: USART-AB-1EL	Module Type: USART-AC-2EL	Module Type: Plug-In Module USART-AD-1FO	Module Type: USART-AE-2FO	Module Type: ETH-BA-2EL	Module Type: ETH-BB-2FO	Module Type: ETH-BD-2FO[1]
Physical Connection										
USB	■									
9-pin D-sub socket		■								
1 x electrical Ethernet 10/100 Mbit/s, RJ45			■							
1 x electrical serial RS485, RJ45				■						
2 x electrical serial RS485, RJ45					■					
1 x optical serial, 820 nm, ST connector, 2 km via 62.5/125 µm multimode optical fiber						■				
2 x optical serial, 820 nm, ST connector, 2 km via 62.5/125 µm multimode optical fiber							■			
2 x electrical Ethernet 10/100 Mbit/s, RJ45, 20 m								■		■[2]
2 x optical Ethernet 100 Mbit/s, 1300 nm, LC connector, 24 km via 9/125 µm singlemode optical fiber										■[2]
2 x optical Ethernet 100 Mbit/s, 1300 nm, LC connector, 2 km via 50/125 µm or 62.5/125 µm multimode optical fiber									■	■
Applications										
DIGSI 5 protocol	■		■					■	■	■
IRIG-B, DCF77, PPS		■								
IEC 61850-8-1 server (including GOOSE, reporting to 6 clients)			■					■	■	■
IEC 61850-9-2 Merging Unit										■
IEC 61850-9-2 Process-Bus Client										■
IEC 60870-5-103				■	■	■	■			
IEC 60870-5-104								■	■	■
DNP3 serial				■	■	■	■			
DNP3 TCP								■	■	
Modbus TCP								■	■	
Synchrophasor (IEEE C37.118 – IP)								■	■	

1 For modular devices only (not for 7ST85 and 6MD89)

2 For the **2 x electrical Ethernet and 2 x optical Ethernet over 24 km** function, separate SFPs are necessary. These can be ordered as accessories.

Port or Plug-In Module	**Front Interface**	**Port G: Time Synchronization**	**Port J: Integrated Ethernet**	**Module Type: USART-AB-1EL**	**Module Type: USART-AC-2EL**	**Module Type: Plug-In Module USART-AD-1FO**	**Module Type: USART-AE-2FO**	**Module Type: ETH-BA-2EL**	**Module Type: ETH-BB-2FO**	**Module Type: ETH-BD-2FO[1]**
Protection interface (Sync. HDLC, IEEE C37.94)						■	■			
PROFINET IO								■	■	■[3]
SUP Serial (Slave Unit Protocol) for connecting external temperature- or 20-mA measuring devices				■	■	■				
SUP Ethernet SUP (Slave Unit Protocol) for connecting external temperature- or 20-mA measuring devices			■					■	■	
Diagnostic homepage			■					■	■	■
Additional Ethernet protocols and services										
DHCP, DCP (automatic IP configuration)			■					■	■	■
Line Mode								■	■	■
PRP (Ethernet ring redundancy)								■	■	■
HSR (Ethernet ring redundancy)[4]								■	■	
RSTP (Ethernet ring redundancy)								■	■	■
SNTP (time synchronization via Ethernet)			■					■	■	■
SNMP V3 (network management protocol)								■	■	■[5]
IEEE 1588v2 (PTP protocol via Ethernet – ms accuracy)								■	■	
IEEE 1588v2 (PTP protocol via Ethernet – µs accuracy)[6]										■

NOTE

The USART and ETH plug-in module types can be used in slots E and F in the base module as well as in slots N and P in the CB202 expansion module. They are not intended for use in slot M in the CB202 expansion module.

1 For modular devices only (not for 7ST85 and 6MD89)
3 Available for V8.20 and higher
4 In preparation for ETH-BD-2FO
5 Available for V8.20 and higher
6 With optional RJ45, the SFP accuracy is 1 ms.

1.3 Network Topology

1.3.1 Network Structures

The Ethernet communication modules and interface are available in both electrical and optical versions. Both module types are provided with an integrated switch functionality. This makes it possible to integrate the devices into almost all network structures together with third-party components.

The network structures are independent of the communication protocol (IEC 61850, DNP3, IEC 60870-5-104, ...).

The interfaces on the devices can be used in different operating modes. A distinction is drawn between the operating modes **Line** and **Switch**.

NOTE

In DIGSI, the **Dual Homing** operating mode is known as **Line**.

Superordinate Network Structures

SIPROTEC devices are always incorporated into superordinate network structures. This is not the case for connections with only a single partner.

The basic element of superordinate structures is always a so-called switch. Switches have several ports. The connections between these ports and the ports of other network switches form the superordinate network.

Today, superordinate network structures are formed from structures based on switches that operate using RSTP (Rapid Spanning Tree Protocol). This always means that the higher level network forms a ring or a network of such network switches. This results in a variety of possible circuits. A superordinate network is always included in the following figures of structures.

It can be seen that a network structure always consists of a higher level network structure and the connection to a device.

NOTE

With RSTP, you must recall that, in the event of an error, this structure and the superordinate network structure determine the time behavior. With Dual Homing, only the device-connection line that switches very quickly is protected. Errors in the higher level network are always subject to the time behavior of the network.

In the following explanations, the superordinate network structure is always shown as a simple ring. Such a ring can conceal a structure with several superimposed rings.

Dual Homing Interface Operating Mode

If you have not set a redundancy protocol, the **Dual Homing** operating mode will be active. In this operating mode, both ports of the SIPROTEC device behave like one independent port. The 1st port that detects a connection with another network component accepts it as active and handles the entire data transmission via that connection.

The 2nd port on the device operates on standby, that is, only the link status is monitored. If the active port fails, the device switches to the 2nd port within a few milliseconds.

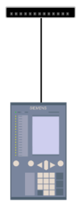
NOTE

Keep in mind that the device or the network connection has only one MAC address, that is, only one of the connected lines is active at any moment.

In the **Dual Homing** operating mode, redundant star structures (as viewed from the device) can be formed if both device ports are connected with different ports of a network switch or with one port on each of the 2 different network switches.

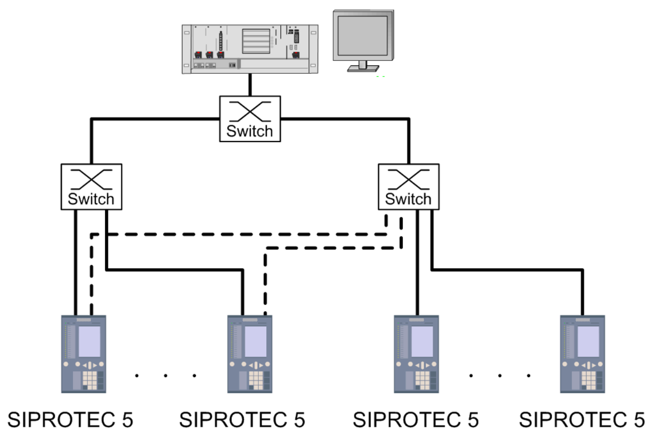
If only one port is connected with a network port, then this connection has no redundancy and has only a single connection, just like the network connection on a PC.

The following connections are possible:



[dwdhansc-170311-01.tif, 2, --_--]

Figure 1-4 Single Connection



[dw_SIP5-0031, 3, en_US]

Figure 1-5 Dual Homing with 2 Switches

Redundancy Protocol Interface Operating Mode

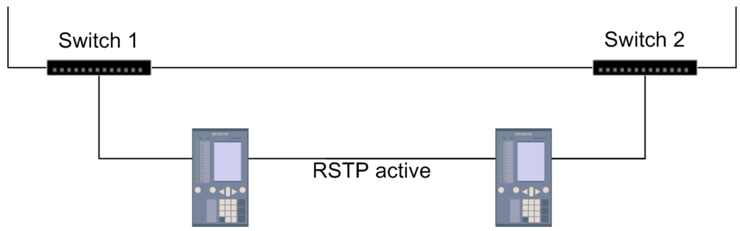
Currently, RSTP is available as a redundancy protocol. In accordance with IEEE 802.1D-2004, RSTP is then set as the redundancy protocol.

The Switch function in the device itself establishes interconnection of the components to one another as a ring and to the superordinate switches. This ensures that all telegrams intended for the device reach it. Telegrams sent from the device are incorporated into the data stream on the ring.

The **Redundancy Protocol** interface operating mode uses both ports on the device, which must be connected with 2 ports of a network switch or with one port each on 2 different network switches. The actual connection is similar to that of **Dual Homing**. In any case, the ports of the network switches support RSTP and are linked in the network. Only activation of RSTP at the device interfaces permits incorporation of SIPROTEC devices into ring or mesh structures.

Switch Function (Internal Switch)

The Switch function in the device itself establishes interconnection of components to one another as a ring and to the superordinate switches. This ensures that only telegrams intended for the device reach it. Telegrams sent from the device are incorporated into the data stream on the ring. The following figures show the connections. The connections of the 2 network switches show their location in the network.



[dwzwswpo-150113-01.tif, 2, en_US]

Figure 1-6 Redundant Connection with Different Network Switches

This figure shows the general use of the Switch function and the possibilities for connecting a device. The redundant connection ensures connection in the event of failure of the link or of a switch. Usually, several devices are arranged in a ring.

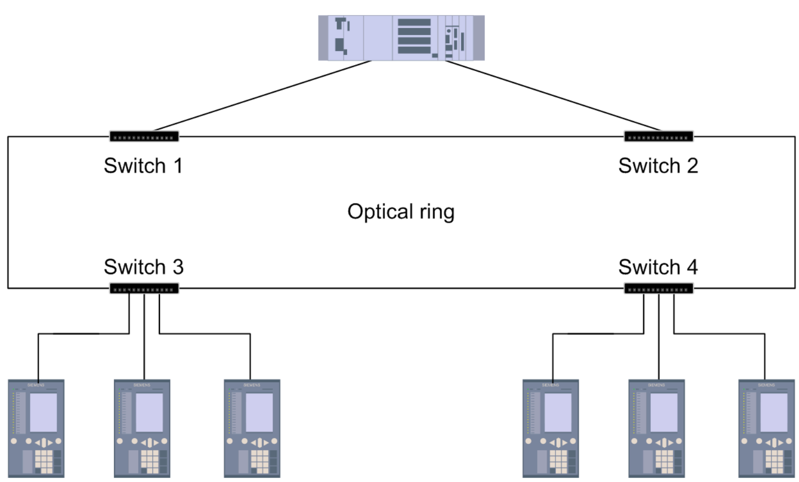
Interface Versions on the Modules

The interfaces of the Ethernet modules in the devices come in different versions for optical or electrical connections. Siemens recommends using an optical fiber for longer connections (> 20 m (787.4 in)). For physical reasons, the length of the connection between 2 switches or between a device and a switch is always limited. The length can be increased by using several switches. For shorter connections, you can also select electrical connections if the actual EMC is taken into account.

Single Structure

In a single structure, a ring consisting of network switches with electrical or optical connections forms the superordinate network structure. In this case, the SIPROTEC devices are connected to the ports of the network switch with a star connection. RSTP is not activated in the SIPROTEC devices.

The star-shaped arrangement of the connections yields a very simple structure which, however, provides no redundancy for the connection between the device and network switch.



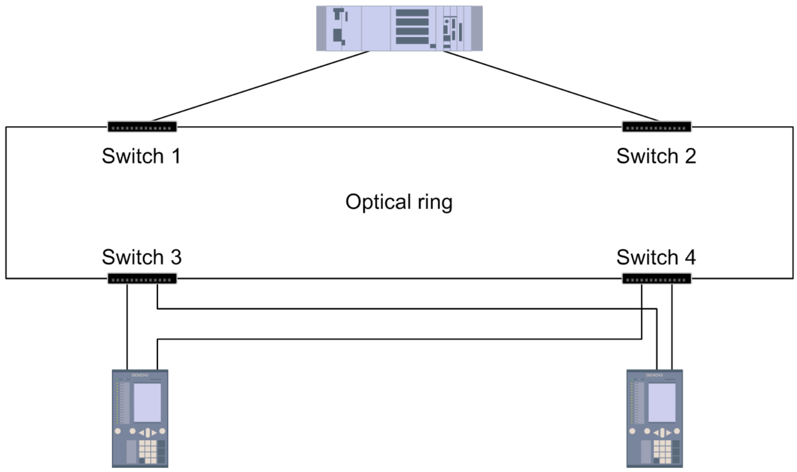
[dwopring-170311-01.tif, 2, en_US]

Figure 1-7 Single Optical Ring

Redundant Star Structure (Dual Homing)

In contrast to a single structure, the devices in a redundant star structure are connected with the network via both ports, in this case, with the ports of 2 different network switches.

In the **Dual Homing** operating mode, RSTP in the SIPROTEC devices is not activated/parameterized, but there is a redundant connection between network switches and the SIPROTEC device. The redundancy of the superordinate network is assured by the RSTP functionality there, but this does not affect the interface function of the devices. Another redundancy procedure can also be active in the superordinate network. The superordinate network can also be of a star shape.

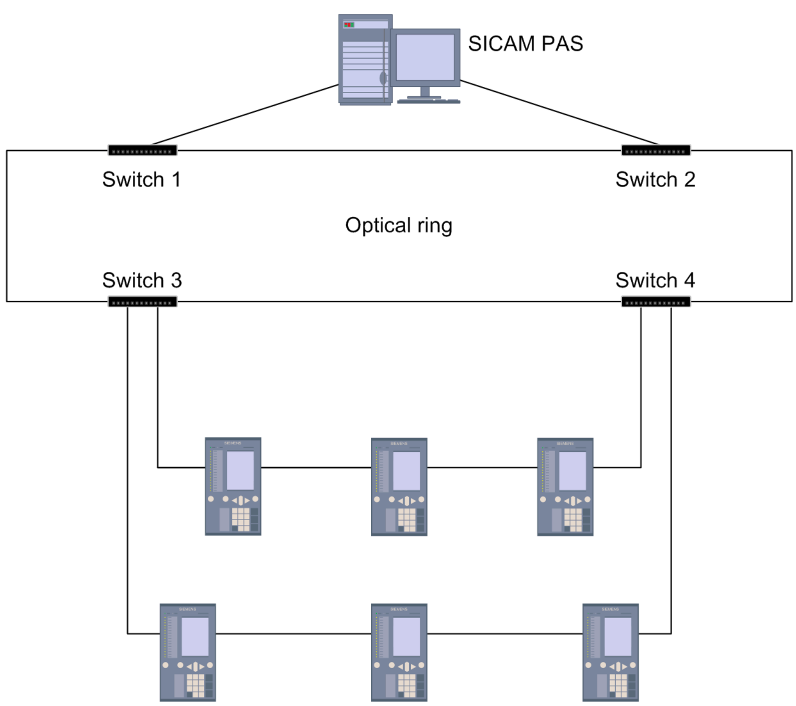


[dwduhome-170311-01.tif, 2, en_US]

Figure 1-8 Dual Homing Structure

Ring Structure

Ring structures are structures in which SIPROTEC devices are interconnected with devices from other manufacturers in a ring. The devices are incorporated into the ring structure via both ports. This yields rings consisting of devices and network switches 3 and 4. These network switches have at least 4 ports that support RSTP. Network switches 1 and 2 are connected with the SICAM PAS.



[dwdoprin-170311-01.tif, 2, en_US]

Figure 1-9 Ring Structure

Information is routed from participant to participant in the ring until it reaches its intended destination. If the ring structure shown is cut at a point, a line results. Communication continues to function almost without interruption, because network control with RSTP initiates a reconfiguration. A second fault in the line or in one of the participants, however, cannot be overcome. Depending on the structure, keeping additional faults under control is becoming less secure.

You must set the RSTP parameter **Bridge Priority**. This requires that you set one of the 2 switches connected with the Substation Automation System to priority 0. As a result, the switch with priority 0 is then specified as the root switch. You must set the other switch connected with the Substation Automation System to a lower priority. A higher numerical value means a lower priority. Siemens recommends setting this switch to 4096. This switch serves as the backup root switch in the event that the root switch fails.

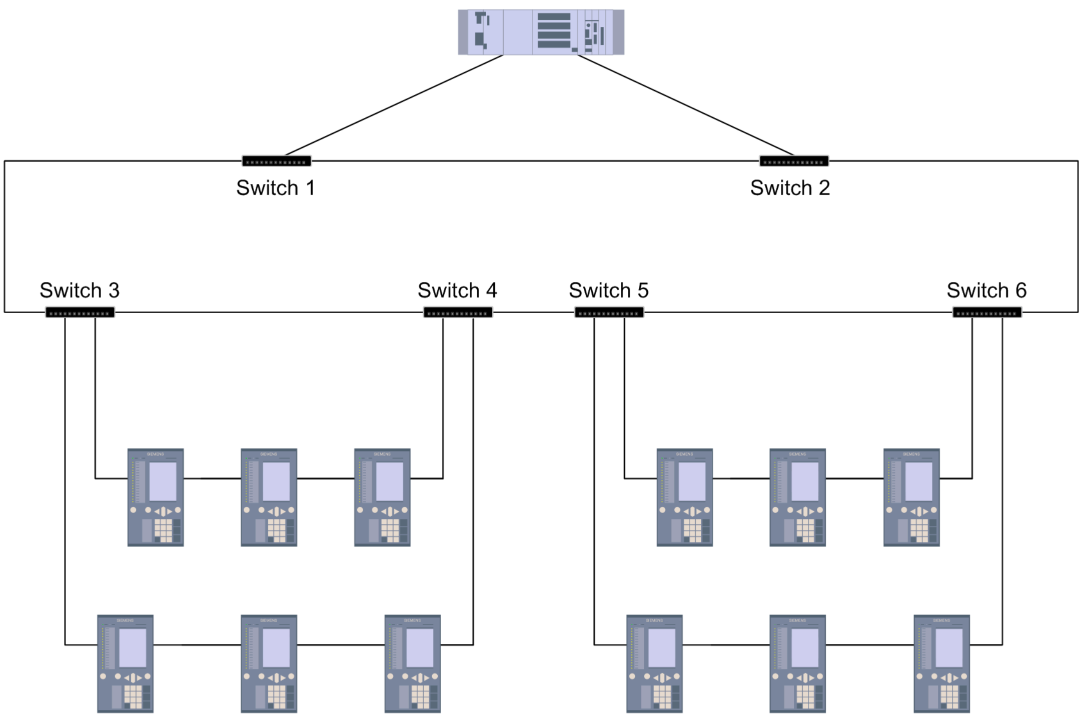
Network switches 3 and 4 always have the next-lowest priority, that is, the priority value must be set higher. The priority for both can be the same, however.

Siemens recommends using this topology for compact systems.

Multiple-Ring Structure

Multiple-ring structures can occur in succession in larger systems.

To create a multiple-ring structure, activate and set the settings for RSTP in the devices.



[dw2ringe-170311-01.tif, 2, en_US]

Figure 1-10 Dual-Ring Structure

The figure shows the possible arrangement in such a structure. Each ring can contain several switches. Even the SICAM PAS is incorporated via its own switches.

The structure shown represents a **Garland structure**: The SIPROTEC devices are connected in a line. At its ends, this line is connected with the switches. The line of devices is called a garland. The garland structure occurs several times in succession here.

Detailed information on the special aspects of setting the parameters for such a structure can be found in the following chapter.

Optical and Electrical Module Interfaces

In contrast to SIPROTEC 4 devices, there is no difference between modules with an optical interface and modules with an electrical interface in SIPROTEC 5 devices.

NOTE

When setting parameters, note the following:

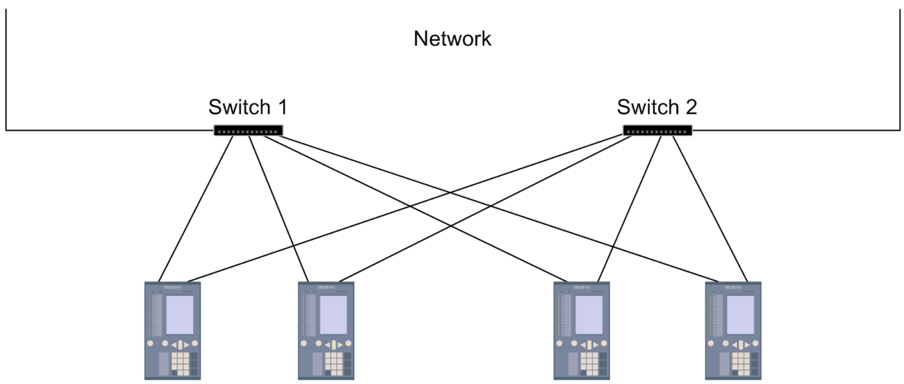
You can select between the Line, RSTP, PRP, and HSR structures.

The PRP and HSR protocols have no additional setting values.

The PRP and HSR protocols are supported by devices of version V3.00 and higher and by DIGSI 5. If your devices, Ethernet modules, and DIGSI 5 use an earlier version, upgrade the components.

PRP Structure

The PRP structure (Parallel Redundancy Protocol according to IEC 62439-3:2012) provides communication over 2 independent networks (LAN A and LAN B) simultaneously. As shown in the following figure, the 2 networks may not be connected to one another. Siemens recommends building both networks identically. Connect LAN A to channel 1 and LAN B to channel 2.



[dwprpstr-150113-01.tif, 2, en_US]

Figure 1-11 SIPROTEC Devices Connected via 2 Independent Networks (LAN A and LAN B)

If there is an interruption in communication on network A or network B, the data exchange continues without problems on the other network. This means that there is no interruption.

Updating the Device Configuration via Communication Modules in the PRP Structure

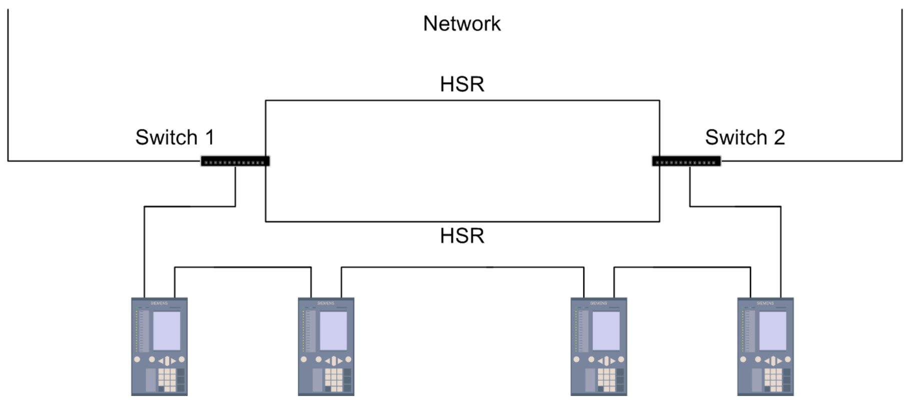
If the device configuration contains IEC 61850 as communication protocol, then the device is set to the **Fall-back** mode during the update process. The module is switched to the **Line Mode** communication. If the DIGSI PC is inserted to the PRP network via a RedBox (Redundancy Box), the communication to the terminal device continues to function in the PRP structure with the **Line Mode** network redundancy protocol.

NOTE

Communication problems can occur if you insert a DIGSI PC as SAN (Single Attached Node) into a PRP structure and a SIPROTEC 5 device goes into **Fallback** mode, for example, by loading the configuration when using IEC 61850. In the **Fallback** mode, the devices switch over internally to **Line Mode**. Therefore, Siemens recommends using a DIGSI PC in a PRP network with a RedBox (Redundancy Box).

HSR Structure

The devices are arranged in rings in the HSR structure (High Availability Seamless Redundancy Protocol according to IEC 62439-3:2012) shown in the following figure. The procedure does not have its own parameters.



[dwhsrstr-150113-01.tif, 2, en_US]

Figure 1-12 SIPROTEC Devices Arranged in Rings

If an interruption in communication occurs in a network, a seamless switchover takes place. All components in the HSR rings must support HSR.

If you want to connect non-HSR-capable devices, apply HSR RedBoxes or HSR-capable switches. For example, if communication via Ethernet with a PC with devices in the HSR ring is to take place, the connection must be established using a RedBox.

1.3.2 Network Structure-Dependent Parameters

RSTP needs the settings that are listed and described in the table under *9.8.2 Parameter Settings for Networks* in order to operate.

Detection of the Correct RSTP Settings

The RSTP diagnostic values can be displayed on the HMI (Human-Machine Interface) of the device and with DIGSI 5.

Also check the role of the ports.

For further information on the diagnostic values, refer to chapter *9.13.4.9 Application Diagnostic – RSTP* .

Determining the Location of the Alternate Port

There must always be an alternate port in a ring, since such a port in a ring forms a logical cut that is necessary to prevent continually circulating telegrams.

If the alternate port does not exist, it may still be possible to reach all devices, but there will no longer be any redundancy. That means a line break has occurred that was already handled prior by RSTP. A break in the line always leads to a reconfiguration and loss of the alternate port, since the alternate port must switch through in order to bridge the break caused by an error.

The alternate port in a configuration can always be determined by querying the port roles. This is possible with the aid of SNMP (Simple Network Management Protocol) or, with more effort, by means of the display of the device. Establishing the location of the alternate port depends on the number of switches in the range.

In the simple ring structure in *Figure 1-9*, the situation is as follows:

- If Switch 1 is the root switch, then there are 3 rings:
  - One ring consisting of Switches 1 to 4
  - Two 3-device lines of SIPROTEC devices
- If Switch 1 is the root switch, the ring consisting of 4 network switches contains the ring from Switch 1 to Switch 3 and Switch 2 and from there to Switch 4. If the priority of Switch 2 is lower than that of Switch 3, then the alternate port is set to the right port of Switch 4.
- If Switch 1 is the root switch, you obtain a 2nd ring: Switch 1 – Switch 3/Switch 2 – S11/Switch 4 – S12/S13. This establishes the alternate port on the tie line S12/S13. If S13 has a lower priority, then the alternate port is set to the right port of S12.
- The same holds for the 2nd ring of. SIPROTEC devices.

NOTE

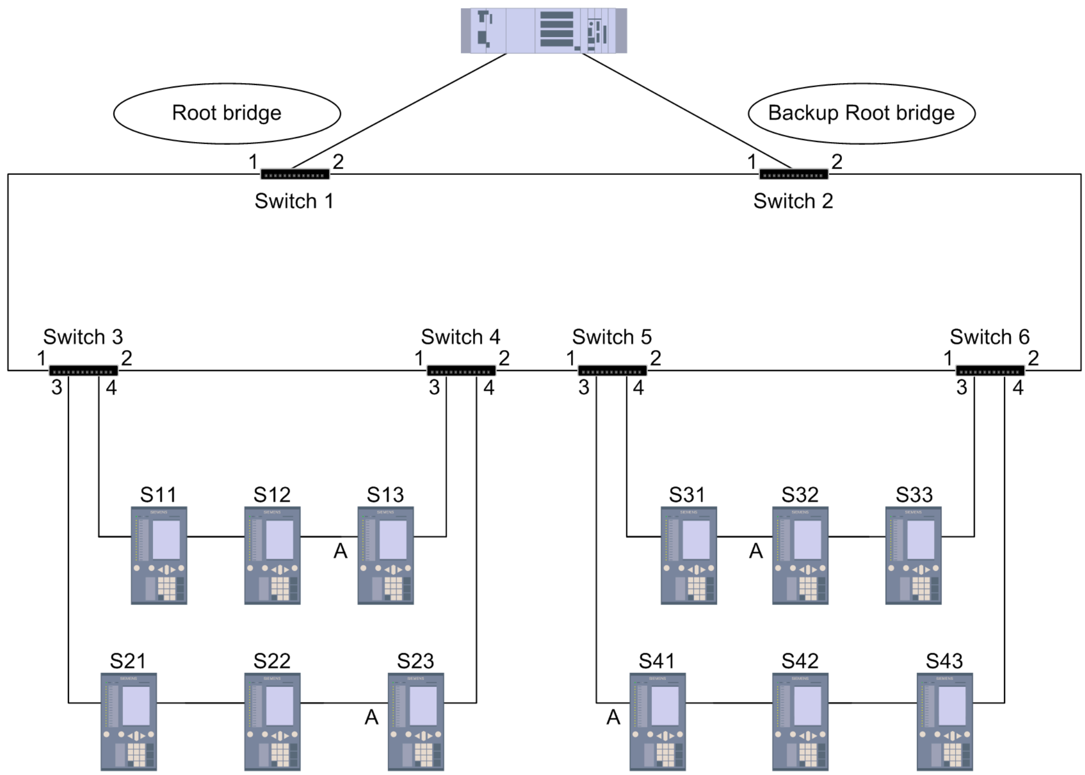
Keep in mind that the MAC address is linked to the priority. If the switches are set to the same priorities, then the MAC address is the determining factor.

In the dual-ring structure and when the alternate port is stationary, the situation is somewhat more complex:

- The primary ring is now Switch 1 – Switch 3/Switch 2 – Switch 4/Switch 6 – Switch 5/Switch 5. If Switch 4 has a lower priority than Switch 6, then the alternate port is set to the left port on Switch 5.
- The ring with the S1x switches is slightly different. The root switch (Switch 1) has a connection to Switch 3. This is where the subring Switch 3 – S11/Switch 4 – S12/S13 begins. In this case, the alternate port is set to one port of the connection between S12/S13. If S13 has a lower priority[7] than S12, then the left port on S13 is established as the alternate port.
- The ring with S4x is an additional example. The left port on Switch 5 is the alternate port in the primary ring. As a result, the connection to the root bridge runs through the right port on Switch 6, yielding: Switch 6 – Switch 5/S43 – S41/S42. The alternate port is established on the ports used for the connection S41-S42. If S41 has a lower valence than S42, then the right port on S41 is established as the alternate port.

Using this procedure, it is possible to determine the alternate ports for all structures and check them in the real system.
These settings are shown in the following figure.

[7] The priority consists of several components including, among others, the MAC address.



[dwstatap-170311-01.tif, 2, en_US]

Figure 1-13 Structure with Alternate Ports

Setting the MaxAge Parameter

The **MaxAge** parameter is preset to 20. This setting is listed as the default setting in the Standard IEEE Std 802.1D™ – 2004 and can be increased up to 40. The primary function of this parameter is to discard telegrams with a greater or identical age. Aging itself is established by the number of switches passed.

The **MaxAge** parameter must be defined such that all switches can reach the root switch when taking this definition into account, particularly in the case of a break in the line or device failure.

The alternate ports indicate the break points. If you consider the connections to the root switch, for example, S23 – S22 – S21 – Switch 3 – Switch 1, then a setting of 4 suffices for the **MaxAge** parameter.

NOTE

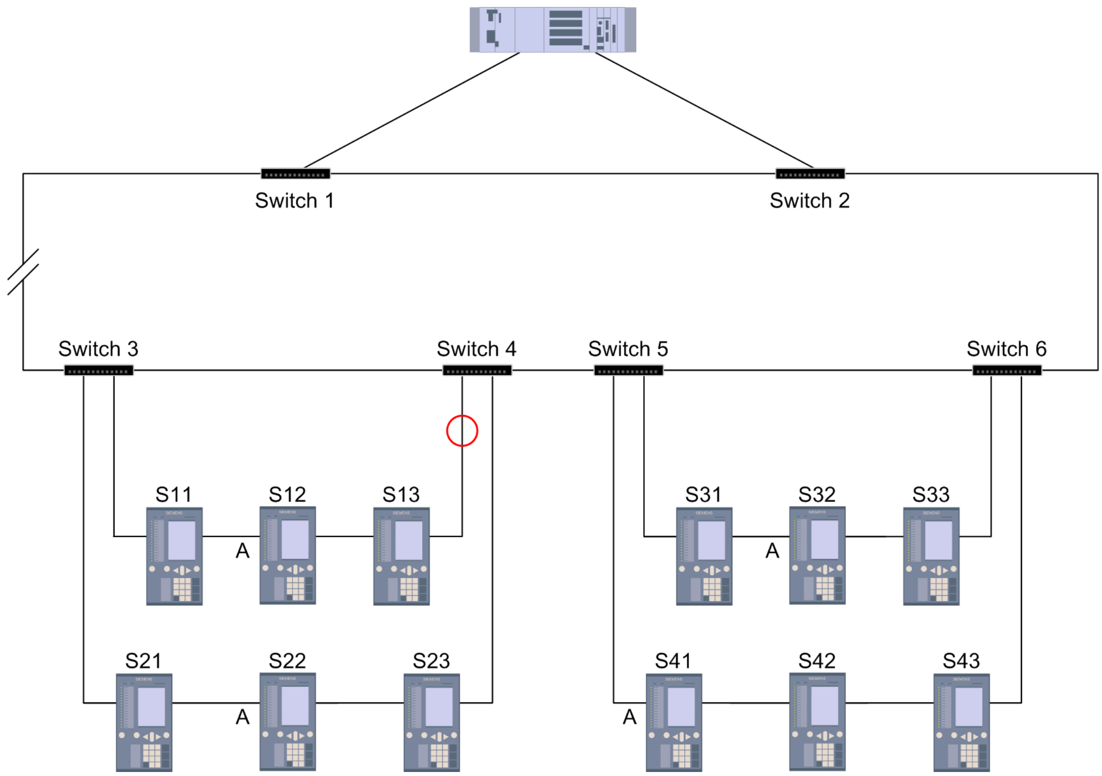
The alternate port is included in the count!

If the entire network is considered, then you must set the **MaxAge** parameter to 5 (Switch 1 – Switch 2 – Switch 6 – S43 – S42 – S41). This, however, represents the steady state.

Such a state must first be established. It must be possible to reach the root switch in all interruption scenarios. If the line from the left port on Switch 1 to the left port on Switch 2 breaks, then the alternate ports shift.

NOTE

Switching on a device can also cause such reconfiguration effects, for example, the shifting of alternate ports.



[dwubport-170311-01.tif, 2, en_US]

Figure 1-14 Broken Connection with Shifting of the Alternate Ports

The worst case is when the connection from the right port on S13 to Switch 4 breaks as well. In this case, the maximum setting is 8 (Switch 1 – Switch 2 – Switch 6 – Switch 5 – Switch 4 – Switch 3 – S11 – S12 – S13).

NOTE

The telegram age that results is 7, but since it must always be less than the **MaxAge** parameter, a setting of 8 is mandatory.

You can find more information on telegram age in chapter *9.8.2 Parameter Settings for Networks*.

The optimum situation is thus a setting of 8.

NOTE

It is also possible to set 20, but in the event of a root failure, RSTP telegrams can remain in the network until they disappear because of their age. These telegrams can cause temporary interruptions.

For this reason, you should not set the **MaxAge** parameter any higher than necessary.

Setting the HelloTime Parameter

You can set the **HelloTime** parameter to 1 s or 2 s. This value sets the interval between cyclically sent RSTP telegrams.

If you wish to achieve a fast response, set 1 s. In this way, root failure is handled quickly.

Setting Priorities

Priority settings in a network establish the location of the root bridge. Establish the location of the root bridge such that all switches, including the SIPROTEC devices, can reach the root bridge over almost identically long paths. Using this approach, you also achieve a minimum setting of the **MaxAge** parameter, as described in the section that discusses setting the **MaxAge** parameter. Normally, SIPROTEC devices should not form the root bridge.

Once the root bridge has been established, also specify a 2nd bridge as a backup root bridge in the event of failure of the primary root bridge when the network is similar to that shown in *Figure 1-13*. For the **MaxAge** parameter setting not to be increased unnecessarily, the backup root bridge should be in the immediate vicinity of the primary root bridge. This results in the following: for Switch 1, a priority setting of 0; Switch 2 is set to 4096; Switches 3 to 6 are higher, and the devices are all set to 32 768.

NOTE

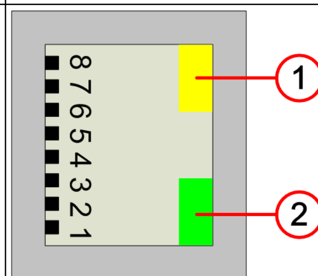
The port priorities are changed only in special cases.

1.4 Ethernet Modules

1.4.1 Ethernet Interface

Integrated Ethernet Interface (Port J)

This terminal is used to load the device with DIGSI 5 using Ethernet. This terminal also enables IEC 61850 Ethernet communication or communication with another protocol via Ethernet, for example, for connecting an external RTD unit.

Interface	Integrated Ethernet interface
Connection	 (1) LED 1: Yellow (2) LED 2: Green
Connector type	1 x RJ45
Baud rate	100 Mbit/s
Max. line length	20 m with Ethernet patch cable CAT 6 S/FTP, F/FTP, or SF/FTP
Insulation class	SELV (acc. to IEC 60255-27)
Interface design	Corresponds to IEEE 802.3, 100Base-TX

NOTE

The IEC 61850 protocol is an option that can be ordered for Port J (integrated Ethernet interface). This protocol is displayed only if the corresponding product feature has been purchased.

NOTE

A client-server communication can take place via Port J (integrated Ethernet interface), for example, reports can be transmitted.

In non-modular devices (CP100) and modular devices with CP300, this interface can also support GOOSE communication as an order option.

1.4.2 Operation of Ethernet Modules

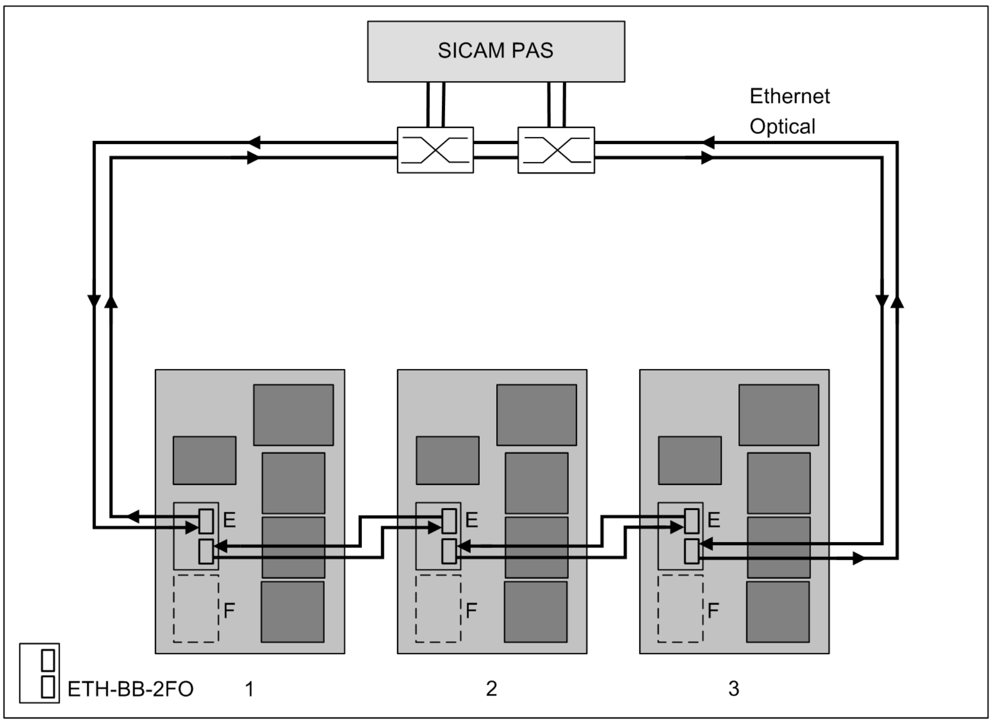
The Ethernet modules of the SIPROTEC 5 series can be operated optionally with or without integrated switch function. This applies for the electrical as well as the optical module. This function can be selected via the parameterization. It is not necessary to make any indication in the order. The optical Ethernet modules are compatible with the EN100 modules of the SIPROTEC 4 series. If the RSTP protocol or the HSR protocol is active, the optical modules of the SIPROTEC 4 series and the SIPROTEC 5 series can be operated in a ring.

When using SIPROTEC 4 devices with module firmware ≤ V4.06 and SIPROTEC 5 devices, the maximum allowable number of participants is 30 devices. When using SIPROTEC 4 devices with module firmware ≥ V4.07 and SIPROTEC 5 devices, the maximum allowable number of participants is 40 devices. When using SIPROTEC 5 devices, the maximum allowable number of participants is 40 devices.

Figure 1-15 shows operation of the Ethernet modules with integrated switch function. All devices of a station are shown which are connected to one another by means of optical fibers. The devices form optical rings. In addition, 2 switches are used on the substation controller for the SICAM PAS. The 2 switches take the requirements for the redundancy into account.

Additional participants with electrical interfaces can also be connected to the SICAM PAS (for example, the DIGSI 5 control PC). An external switch is sufficient. Optical communication modules are primarily used for this topology, as there can be substantial distances between the devices.

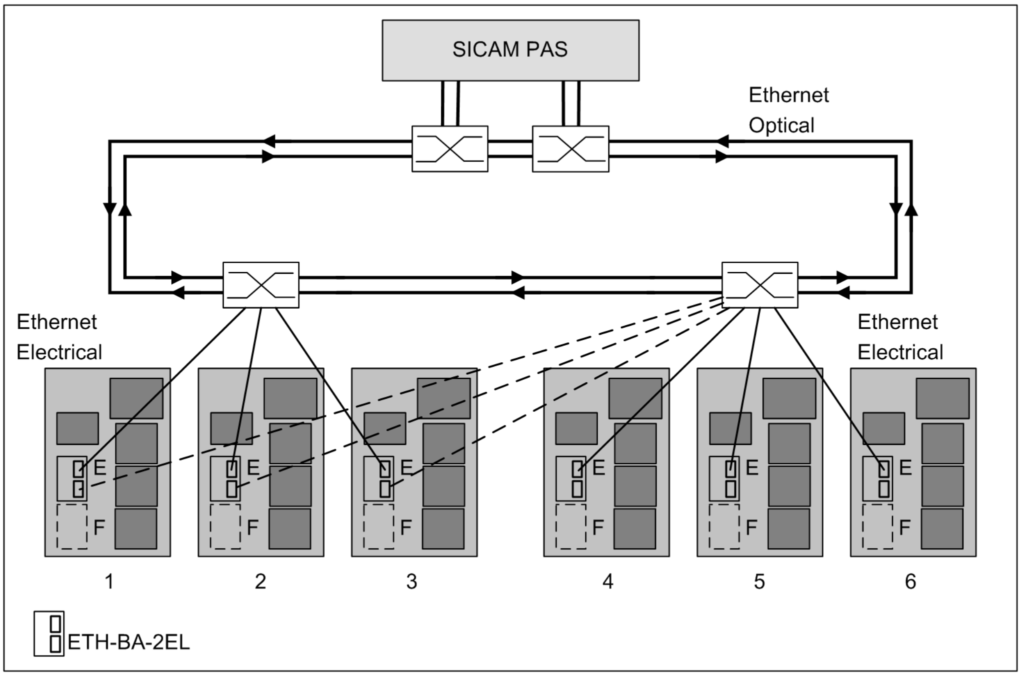
If the Ethernet modules are installed in expansion modules with a CB202 PCB assembly, the power supply can be provided with an independent battery. The integrated switch can maintain its function when the device is switched off. The data are transmitted in optical and electric rings. This prevents opening of the ring. The ring continues to operate when 1 or more devices are switched off.



[dweth1sw-030211-01.tif, 2, en_US]

Figure 1-15 Operation of Ethernet Modules with an Integrated Switch Function

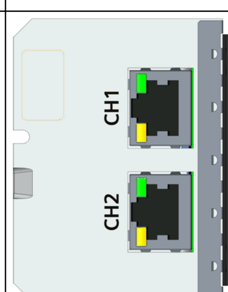
Figure 1-16 shows the operating mode without integrated switch function. Optionally, the 2nd connection can be connected to the 2nd switch. This connection is shown with a dashed line in *Figure 1-16*. The IP communication is established using the 1st connection here. If this connection fails, the system changes over to the 2nd connection within a few milliseconds. The IP connection is retained practically without interruption using the 2nd switch. This hot-standby connection redundancy increases the availability in such configurations, as shown in the following figure. The information on failure of the protection connection is transmitted to the substation automation technology.



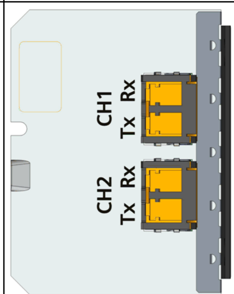
[dwethsw3-090713-01.tif, 2, en_US]

Figure 1-16 Operation of Ethernet Modules Without Integrated Switch Function with Single or Redundant Connection to the Switch

1.4.3 ETH-BA-2EL

Description	Communication module for the transmission of Ethernet protocols via 2 electrical interfaces
Product code	P1Zxxxxxxxxxx
Figure	
Connector type	2 x RJ45
Baud rate	100 Mbit/s
Protocol	DIGSI 5 protocol (secure Web service protocol) IEC 61850 (MMS and GOOSE) DNP3 Modbus IEC 60870-5-104 PROFINET IO Synchrophasor protocol You can switch other network services like SNMP, RSTP, PRP, HSR, SNTP and SUP Ethernet on and off.
Max. line length	20 m with Ethernet patch cable CAT 6 S/FTP, F/FTP, or SF/FTP
Interface design	Corresponds to IEEE 802.3, 100Base-TX

1.4.4 ETH-BB-2FO

Description	Communication module for the transmission of Ethernet protocols via 2 optical interfaces
Product code	P1Zxxxxxxxxxx
Figure	
Connector type	2 x duplex LC
Wavelength	λ = 1300 nm
Baud rate	100 Mbit/s
Protocol	DIGSI 5 protocol (secure Web service protocol) IEC 61850 (MMS and GOOSE) DNP3 Modbus TCP IEC 60870-5-104 PROFINET IO Synchrophasor protocol You can switch other network services like SNMP, RSTP, PRP, HSR, SNTP, and SUP Ethernet on and off.
Max. line length	2 km for 62.5 μm/125 μm optical fibers

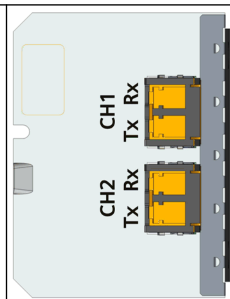
Transmitter Power	**Minimum**	**Typical**	**Maximum**
50 μm/125 μm, NA[8] = 0.2	-24.0 dBm	-21.0 dBm	-17.0 dBm
62.5 μm/125 μm, NA[8] = 0.275	-20.0 dBm	-17.0 dBm	-14.0 dBm

Receiver sensitivity	Maximum -12.0 dBm Minimum -31.0 dBm
Optical budget	Minimum 7.0 dB for 50 μm/125 μm, NA[8] = 0.2 Minimum 11.0 dB for 62.5 μm/125 μm, NA[8] = 0.275
Interface design	Corresponds to IEEE 802.3, 100Base-FX
Laser class 1 as per EN 60825-1/-2	With the use of 62.5 μm/125 μm and 50 μm/125 μm optical fibers

1.4.5 ETH-BD-2FO

Description	Communication module for the transmission of Ethernet protocols via 2 optical interfaces, suitable for Process-bus client, Merging Unit, and ultrafast GOOSE
Product code	P1Zxxxxxxxxxx

8 Numerical Aperture (NA = sin θ [launch angle])

Figure	
Connector type	2 x duplex LC
Wavelength	λ = 1300 nm
Baud rate	100 Mbit/s
Protocol	DIGSI 5 protocol (secure Web service protocol) IEC 61850 (MMS and GOOSE) IEC 61850-8-1 (9-2 Client and 9-2 Merging Unit) IEC 60870-5-104 You can switch other network services such as RSTP, PRP, SNTP, and IEEE 1588v2/PTP on and off.
Max. line length	2 km for 62.5 μm/125 μm optical fibers

Transmitter Power	Minimum	Typical	Maximum
50 μm/125 μm, NA[9] = 0.2	-24.0 dBm	-21.0 dBm	-17.0 dBm
62.5 μm/125 μm, NA[9] = 0.275	-20.0 dBm	-17.0 dBm	-14.0 dBm

Receiver sensitivity	Maximum -12.0 dBm Minimum -31.0 dBm
Optical budget	Minimum 7.0 dB for 50 μm/125 μm, NA[9] = 0.2 Minimum 11.0 dB for 62.5 μm/125 μm, NA[9] = 0.275
Interface design	Corresponds to IEEE 802.3, 100Base-FX
Laser class 1 as per EN 60825-1/-2	With the use of 62.5 μm/125 μm and 50 μm/125 μm optical fibers

NOTE

The firmware must be updated to version ≥ V7.90 if using the ETH-BD-2FO module. If the module is connected to a device with a previous version, a hardware failure is reported that disappears with an FW update to V7.90. As this is not an actual hardware failure, there is no need to send in the device.

The ETH-BD-2FO module offers the possibility of replacing the SFPs (Small Form-Factor Pluggable) delivered by default for a communication route of up to 2 km by SFPs that can be ordered separately in order to adapt the interface to different transmission media and longer routes.

SFP with Optical Interface for 24 km, Single Mode

Description	SFP for distances up to 24 km when using singlemode optical fibers
Product code	P1Zxxxxxxxxxx
Connector type	Duplex LC
Wavelength	λ = 1300 nm
Baud rate	100 Mbit/s
Protocol	See information for the module ETH-BD-2FO
Max. line length	24 km for 9 μm/125 μm optical fibers

9 Numerical Aperture (NA = sin θ [launch angle])

Distance 24 km	
Laser class 1 as per EN 60825-1/-2	With the use of 9 µm/125 µm optical fibers

Transmitter Power	**Minimum**	**Maximum**
Transmitter power coupled in singlemode optical fibers	-15 dBm	-8 dBm
Receiver sensitivity	-8 dBm	-31dBm
Optical budget	16 dB	–

SFP with Electrical Interface

Description	SFP with RJ45 connector, for Ethernet protocols via an electrical interface
Product code	P1Zxxxxxxxxxx
Connector type	RJ45
Baud rate	100 Mbit/s
Protocol	See information for the module ETH-BD-2FO
Max. line length	20 m with Ethernet patch cable CAT 6 S/FTP, F/FTP, or SF/FTP
Interface design	Corresponds to IEEE 802.3, 100Base-TX

Removing SFP Pluggable Transceivers

CAUTION

Risk of burns due to high temperatures of the SFP pluggable transceivers

Noncompliance with the safety notes may result in medium or light injuries.

- ✧ The SFP pluggable transceivers can be disconnected and plugged in while in operation. Siemens recommends switching off the device.
- ✧ Allow the SFP pluggable transceiver to cool as much as possible.

- ✧ Remove the connecting cables or the dust protection cap that was plugged on in the delivery state from the SFP pluggable transceiver.
- ✧ In order to release the interlocking, open the bracket on the SFP pluggable transceiver.
- ✧ Pull on the bracket in order to pull the SFP pluggable transceiver out of the slot. The removal must be possible with free movement and without great exertion of force.
- ✧ Provide the SFP pluggable transceiver with the dust protection cap so that the optics are protected from contamination.

Mounting SFP Pluggable Transceivers

- ✧ Check whether the bracket on the SFP pluggable transceiver is closed.
  The bracket must be closed.
- ✧ Insert the pluggable transceiver into the slot until it audibly locks in place.
  The SFP is securely fixed in the slot.

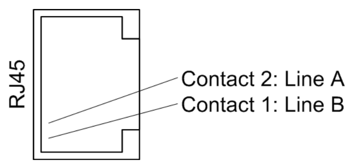
NOTE

Check for secure positioning of the transceiver in the slot and whether it is locked in place in order to avoid unintentional removal by pulling on the connection line.

1.5 Serial Modules for Short Distances

1.5.1 Special Features of Serial Electrical Modules

The serial electrical modules are equipped with RJ45 connections. These are not Ethernet connections. The serial signals of the RS485 interface are routed to the RJ45 connections (see following figure).



[dwrj45pb-030211-01.tif, 1, en_US]

Figure 1-17 RJ45 Terminals for the Serial Signals of the RS485 Interface

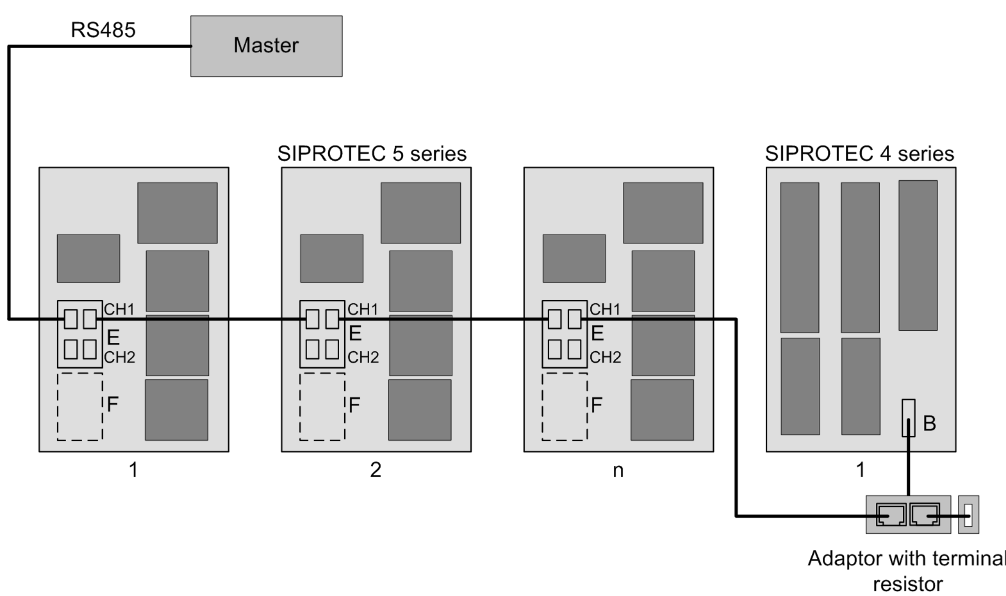
Cabling Examples of Devices with Serial Electrical Modules

Serial electrical RS485 connections of devices in the SIPROTEC 5 series can be cabled with low-cost Ethernet patch cables. Special bus cables and adaptors are not needed. Pay attention to the following note if you include devices from the SIPROTEC 4 series in the connection.

NOTE

The RS485 interface in devices of the SIPROTEC 4 series is a D-Sub 9 connection with a connected terminal resistor.

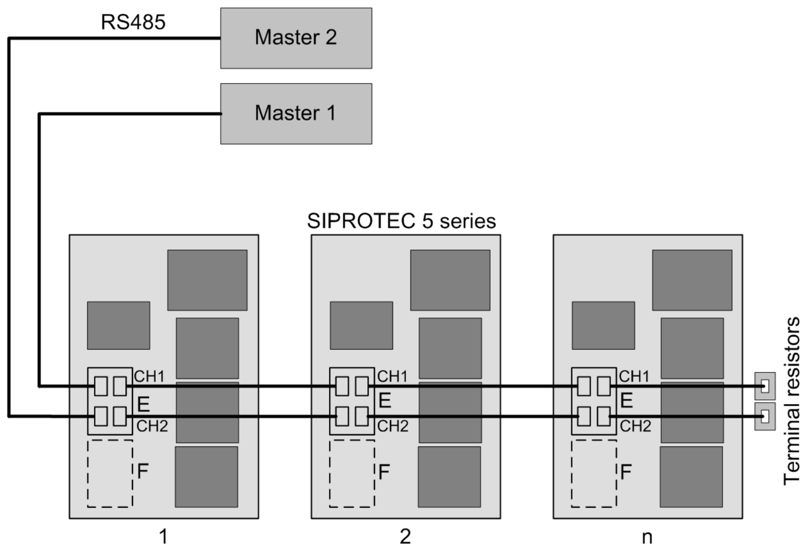
If you connect devices from the SIPROTEC 5 series with devices from the SIPROTEC 4 series, then use a Y adaptor with the order designation 7XV5103-2BA00. Complete the connection on the last device with a terminal resistor. For the SIPROTEC 5 device, use a terminal resistor with the order designation RS485-Terminator 7XV5103-5BA00.



[dwserma1-030211-04.tif, 1, en_US]

Figure 1-18 Communication with a Single Master Using an RS485 Bus

The preceding figure shows the cabling using the new RJ45 sockets in a simplified format. The serial RS485 bus can be extended by simply connecting Ethernet patch cables from device to device.



[dwserma2-030211-05.tif, 1, en_US]

Figure 1-19 Redundant Communication with 2 Masters Using RS485 Bus (for Example, Redundant IEC 60870-5-103 Protocol)

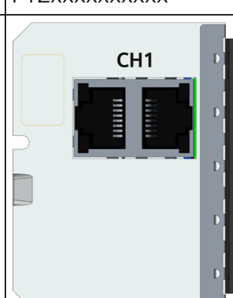
The preceding figure shows the use of both connections on one module for connecting the devices to 2 independent masters following the same principle as with a single master.

Reorders

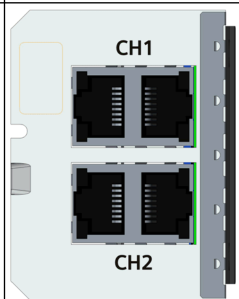
When reordering serial communication modules, specify the product code for the physical version of the module. The order configurator (IPC configurator) shows you which applications are capable of running on the module:

- Serial
- 1-channel or 2-channel
- Electrical or optical

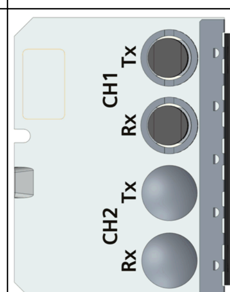
1.5.2 USART-AB-1EL

Description	Serial asynchronous communication module with one electrical interface
Product code	P1Zxxxxxxxxxx
Figure	
Connector type	2 x RJ45
Baud rate	1.2 kbit/s to 115.2 kbit/s
Protocol	IEC 60870-5-103 DNP3 SUP serial

1.5.3 USART-AC-2EL

Description	Serial asynchronous communication module with 2 independent electrical interfaces
Product code	P1Zxxxxxxxxxx
Figure	
Connector type	4 x RJ45
Baud rate	1.2 kbit/s to 115.2 kbit/s
For 1 or 2 protocols or applications (1 application per connection)	IEC 60870-5-103 DNP3 SUP serial

1.5.4 USART-AD-1FO

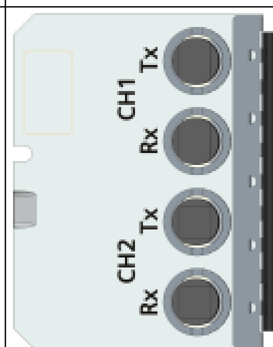
Description	Serial asynchronous or synchronous communication module with 1 independent optical interface
Product code	P1Zxxxxxxxxxx
Figure	
Connector type	2 x ST
Wavelength	λ = 820 nm
Baud rate	Asynchronous: 1.2 kbit/s to 115.2 kbit/s Synchronous: 64 kbit/s to 2 Mbit/s
For 1 protocol or application	IEC 60870-5-103 DNP3 SUP serial Protection-interface communication
Max. distance	2 km when using an optical fiber 62.5 µm/125 µm

Transmitter Power	Minimum	Typical	Maximum
50 µm/125 µm, NA[10] = 0.2	-19.8 dBm	-15.8 dBm	-12.8 dBm
62.5 µm/125 µm, NA[10] = 0.275	-16.0 dBm	-12.0 dBm	-9.0 dBm

10 Numerical Aperture (NA = sin θ [launch angle])

Receiver sensitivity	Maximum +1 dBm Minimum -32 dBm
Optical budget	Minimum 4.2 dB for 50 µm/125 µm, NA[10] = 0.2 Minimum 8.0 dB for 62.5 µm/125 µm, NA[10] = 0.275
Laser class 1 as per EN 60825-1/-2	With the use of 62.5 µm/125 µm and 50 µm/125 µm optical fibers

1.5.5 USART-AE-2FO

Description	Serial asynchronous or synchronous communication module with 2 independent optical interfaces
Product code	P1Zxxxxxxxxxx
Figure	
Connector type	4 x ST
Wavelength	λ = 820 nm
Baud rate	Asynchronous: both connections 1.2 kbit/s to 115.2 kbit/s Synchronous: both connections 64 kbit/s to 2 Mbit/s Asynchronous/Synchronous: 1 connection 1.2 kbit/s to 115.2 kbit/s and 1 connection 64 kbit/s to 2 Mbit/s
For 1 or 2 protocols or applications (1 application per optical connection)	IEC 60870-5-103 DNP3 SUP serial Protection-interface communication
Max. distance	2 km when using an optical fiber 62.5 µm/125 µm

Transmitter Power	**Minimum**	**Typical**	**Maximum**
50 µm/125 µm, NA[11] = 0.2	-19.8 dBm	-15.8 dBm	-12.8 dBm
62.5 µm/125 µm, NA[11] = 0.275	-16.0 dBm	-12.0 dBm	-9.0 dBm

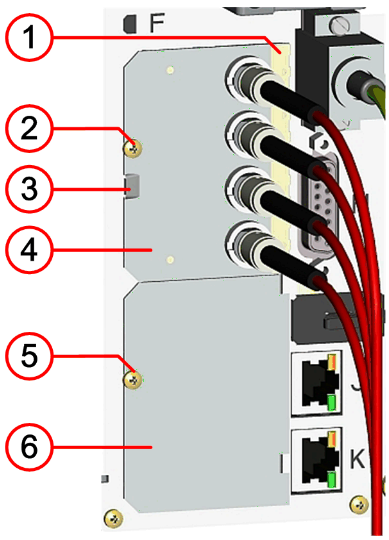
Receiver sensitivity	Maximum +1 dBm Minimum -32 dBm
Optical budget	Minimum 4.2 dB for 50 µm/125 µm, NA[11] = 0.2 Minimum 8.0 dB for 62.5 µm/125 µm, NA[11] = 0.275
Laser class 1 as per EN 60825-1/-2	With the use of 62.5 µm/125 µm and 50 µm/125 µm optical fibers

11 Numerical Aperture (NA = sin θ [launch angle])

1.6 Installation, Replacement

1.6.1 Fasteners

The fasteners of the plug-in modules are shown in the following figure regarding the example of an installed module and an empty, covered slot.



[le_fxing_elements, 1, --_--]

Figure 1-20 Fasteners

(1)	EMC spring contact
(2)	Fastening screw
(3)	Cut-out for prying out the modules
(4)	Plug-in module
(5)	Fastening screw
(6)	Cover plate

1.6.2 Installation

NOTE

Reordered modules are not contained in the original device configuration. Use DIGSI to perform the corresponding extension in the **Hardware and Protocols** Editor.

Preparing Installation

DANGER

Danger due to live voltage when installing the plug-in modules.

Noncompliance with the safety notes will result in death or severe injuries.

✧ Install plug-in modules on the electrically deactivated device only.

CAUTION

Exercise caution with laser beams of the optical plug-in modules.

Noncompliance with the safety notes can result in medium-severe or slight injuries.

✧ Do not look directly into the optical fiber terminals of the active optical plug-in modules, not even with optical devices. The laser beams can damage the eyes.

✧ De-energize the device.

NOTE

When using optical communication modules, Laser class 1 is maintained in compliance with EN 60825-1 and EN 60825-2 when using optical fibers ≤ 62.5 µm/125 µm.

✧ In the case of a surface-mounted device with integrated on-site operation panel, remove the entire on-site operation panel.

✧ Undo the fastening screw and remove the cover plate from the plug-in module position.

Installing the Plug-In Module

✧ Push in the plug-in module on the inner guide as far as it will go.

✧ Ensure that the EMC contact spring is seated correctly.

✧ Bolt down the plug-in module on the assembly frame to a torque of 0.4 Nm.

✧ Connect the lines to the terminals.

✧ Then check for secure attachment of the plugs.

✧ If necessary, fit the on-site operation panel again.

Completing Installation

✧ Resume operation of the device.

1.6.3 Replacement

Preparing for Replacement

DANGER

Danger due to live voltage when replacing the plug-in modules.

Noncompliance with the safety notes will result in death or severe injuries.

✧ Install plug-in modules on the electrically deactivated device only.

CAUTION

Exercise caution with laser beams of the optical plug-in modules.

Noncompliance with the safety notes can result in medium-severe or slight injuries.

- ✧ Do not look directly into the optical fiber terminals of the active optical plug-in modules, not even with optical devices. The laser beams can damage the eyes.

- ✧ De-energize the device.

NOTE

Laser class 1 is adhered to in compliance with EN 60825-1 and EN 60825-2, in the case of ≤ 62.5 μm/ 125 μm optical fibers.

When using the ARC-CD-3FO module, Laser class 1 is maintained in compliance with EN 60825-1 and EN 60825-2 when using 1-mm plastic optical fibers.

- ✧ In the case of a surface-mounted device with integrated on-site operation panel, remove the on-site operation panel before the base module.
- ✧ Remove all communication lines.
- ✧ Undo the fastening screw with which the plug-in module is fixed on the device.
- ✧ Insert a screwdriver (DIN 4 x 0.8) in the cut-out underneath the elongated hole in the assembly frame and disengage the plug-in module.
- ✧ Carefully pull out the plug-in module.

Fastening the Plug-In Module

- ✧ Push in the new plug-in module on the inner guide of the plug-in module position until it moves no further.
- ✧ Bolt down the plug-in module on the assembly frame to a torque of 0.4 Nm.
- ✧ Connect the lines to the terminals.
- ✧ Then check for secure attachment of the connectors.
- ✧ If necessary, fit the on-site operation panel again.

Completing Replacement

- ✧ Place the device is service again and perform a firmware update of the communication modules.

NOTE

If you have not cabled the optical fiber plug-in modules, then seal the terminals with protective covers. This prevents soiling of the terminals.

1.7 Basic Parameterization in DIGSI 5

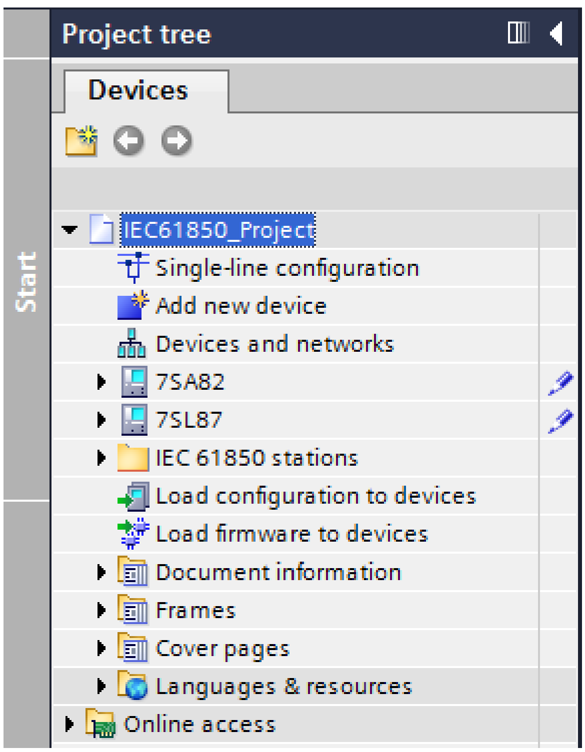
1.7.1 Selecting the Communication Module

If a product code was used to select the devices, they will be delivered with assembled communication modules. You can install and replace additional communication modules afterwards.

NOTE

When doing so, you must ensure that both the protocol firmware as well as the parameterization of the protocol are first transferred by DIGSI.

✧ In the **Project tree**, select the **Devices and networks** section.



[scprojtr-140113-01.tif, 2, en_US]

Figure 1-21 Selection in the Project Tree

✧ Select the communication modules from the library in the **Hardware Editor** working area in DIGSI.

NOTE

The type of communication protocols to be used is the deciding factor when selecting the communication module.

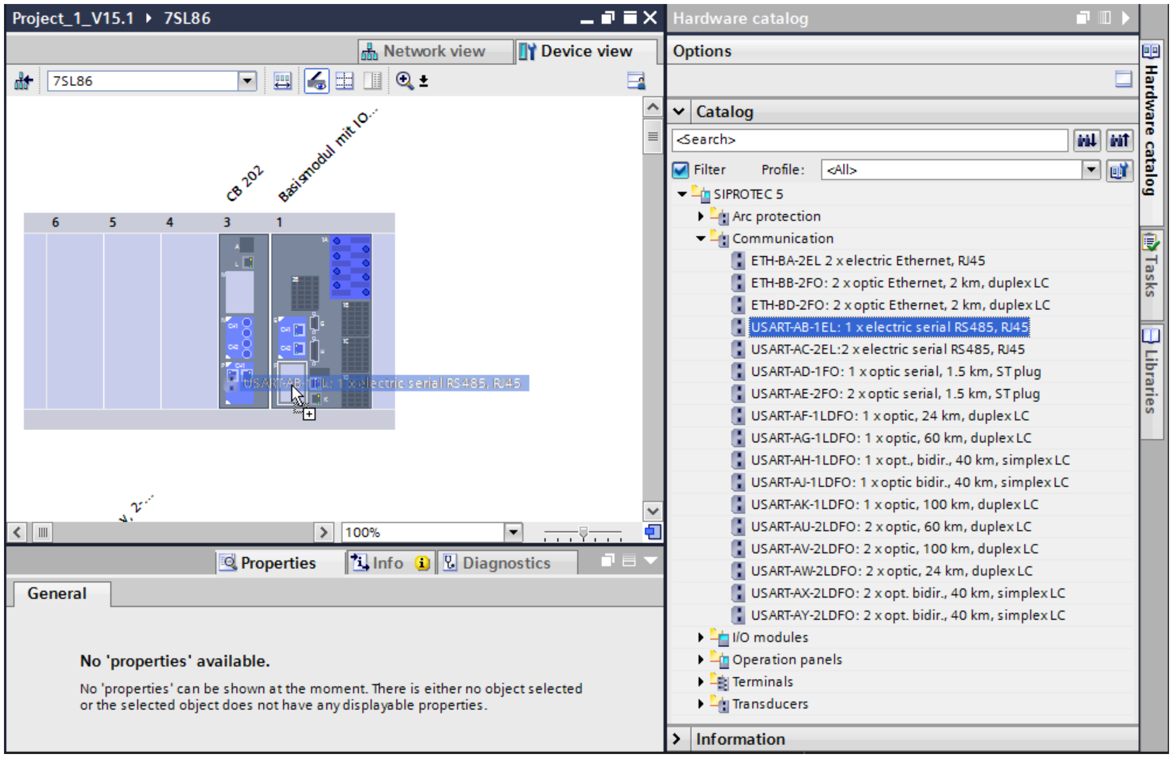
The protocols require a certain interface (serial or Ethernet). You can find more information on which protocol runs with which module in chapter *1.2 Communication Applications of the Plug-In Modules* .

You have 2 possibilities to select the communication module and drag it to the plug-in module position:

✧ Move the communication module using drag and drop from the hardware catalog to the plug-in module position of the device.

- or -

✧ Open the communication module by double-clicking in the hardware catalog.



[scmodsel-280113-01.tif, 3, en_US]

Figure 1-22 Select Communication Module from the Hardware Catalog and Drag it to the Module Slot, for Example, for a Serial Communication Module

1.7.2 Configuring Communication Interfaces

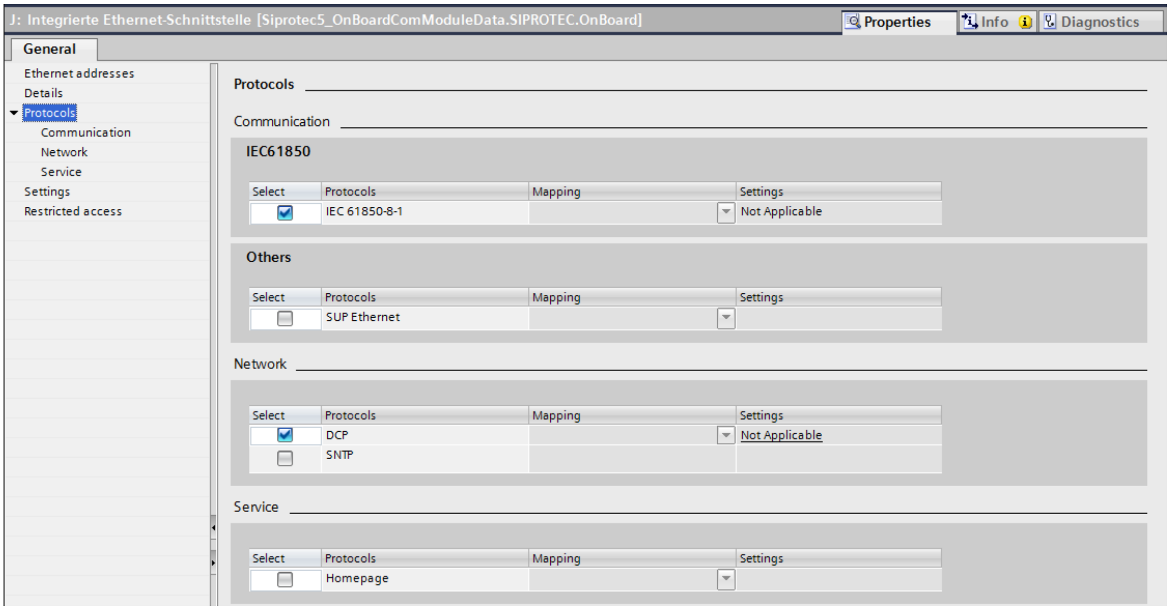
The communication interfaces are configured in the **Hardware Editor** working area in DIGSI 5.

✧ Select the communication module or the integrated Ethernet interface (Port J).

✧ Select the **Properties** tab.

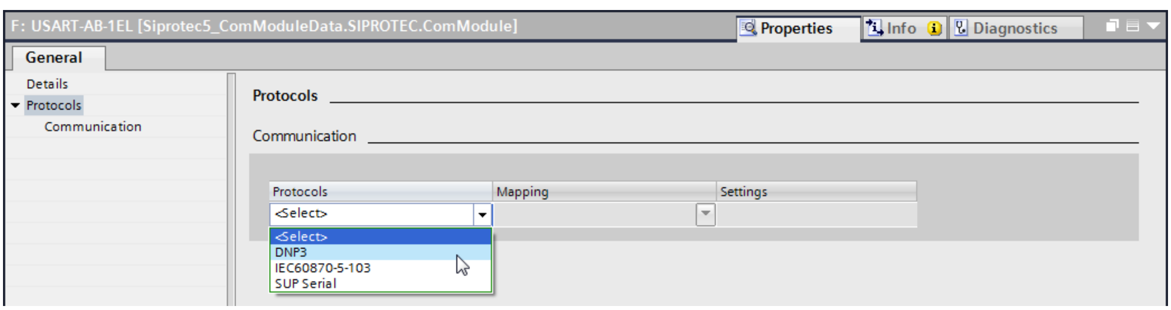
✧ In the lower Editor section, under **General**, select the **Protocols** entry.

✧ Select the desired protocol in the respective sections.



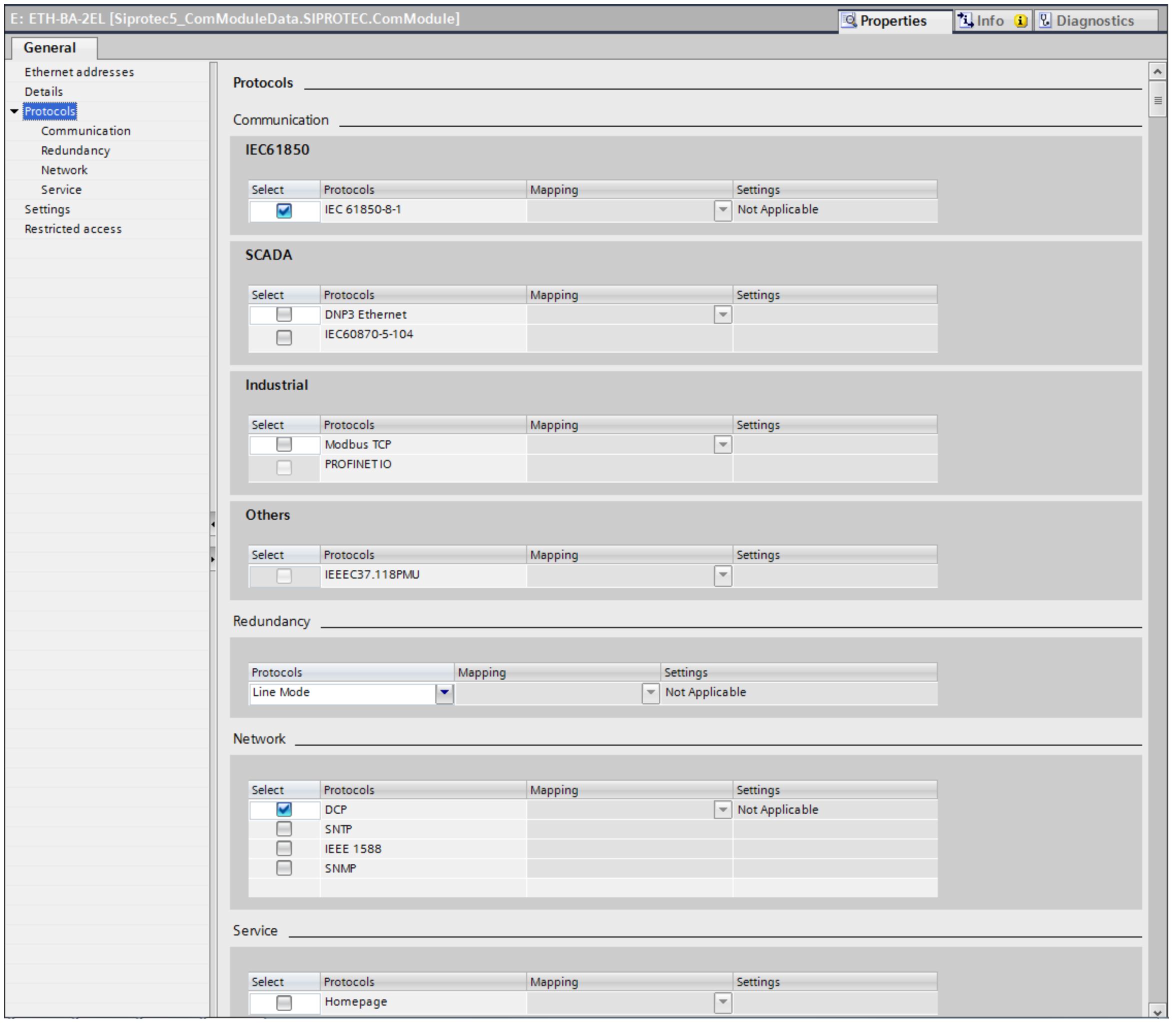
[scparptj-140113-01.tif, 3, en_US]

Figure 1-23 Protocol Selection – Integrated Ethernet Interface (Port J)



[sc_select_protocol_serial, 3, en_US]

Figure 1-24 Protocol Selection – Serial Communication Module



[sc_select_protocol_Ethernet, 2, en_US]

Figure 1-25 Protocol Selection – Ethernet Module

There are modules with 1 or 2 serial interfaces. You must configure all communication channels of the communication module individually.

Channel 1 is displayed for Ethernet modules. The selection applies to the communication module, however, regardless of which redundancy protocol you have selected.

For some protocols, you can parameterize the redundancy on the 2nd channel. For serial protocols, you must activate the redundancy for each channel.

You can route 1 or several network protocols for each channel.

You can also set the IEC 61850 protocol together with other communication protocols, for example with DNP3, IEC 60870-5-104, and Modbus TCP. You can find more information in chapter *1.7.4 Parallel Running with IEC 61850*.

The following table shows for each protocol whether multiple instantiation is possible within a single device:

Table 1-2 Possibility of Multiple Instantiation

Communication Protocol	Multiple Instantiation Possible Yes/No
IEC 61850	Yes
DNP3	Yes
IEC 60870-5-104	No
Modbus TCP	No

Communication Protocol	Multiple Instantiation Possible Yes/No
IEC 60870-5-103	Yes
PROFINET IO	No

With the selection of the communication channel, the parameters required for the protocol are shown. You can find the description of the parameters in the following chapters:

- DNP3:
  3.2.1 Settings for the Serial Connection and *3.2.2 Settings for Communication through Ethernet*
- IEC 60870-5-104:
  4.2.1 Settings
- Modbus TCP:
  5.3.1 Settings
- IEC 60870-5-103:
  6.2.1 Settings
- PROFINET IO:
  7.2.1 Settings

Setting the Network Protocols and the Network Redundancy Protocol

Except for DCP, all network protocols are deactivated in the default setting for safety reasons.

You can find more information on the network protocol and the network redundancy protocols in chapter *9.1 Activation and Ability to Deactivate the Services*.

✧ You can select one or more of these network protocols.

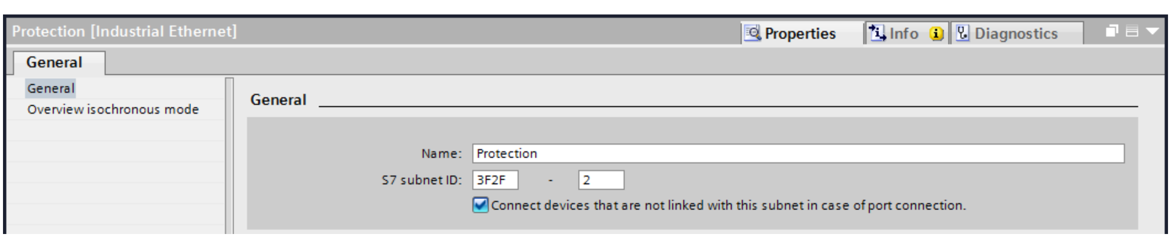
Creating a Subnetwork

✧ If no subnetwork exists, click the **Add new subnetwork** button under **Interface connected with** in the **General** section of the **Properties** tab.

- or -

✧ Highlight the communication module of a device in the **Network view**.

✧ While holding the left mouse button down, drag the cursor to the desired communication module of another device.



[scsubnet-140113-01.tif, 2, en_US]

Figure 1-26 Creating a Subnetwork

NOTE

When using SIPROTEC 5 devices with the IEC 61850 protocol, 2 communication modules configured with IEC 61850 must not be placed in the same subnetwork.

To establish an IEC 61850-GOOSE connection, modules must be in the same subnetwork.

1.7.3 VLAN

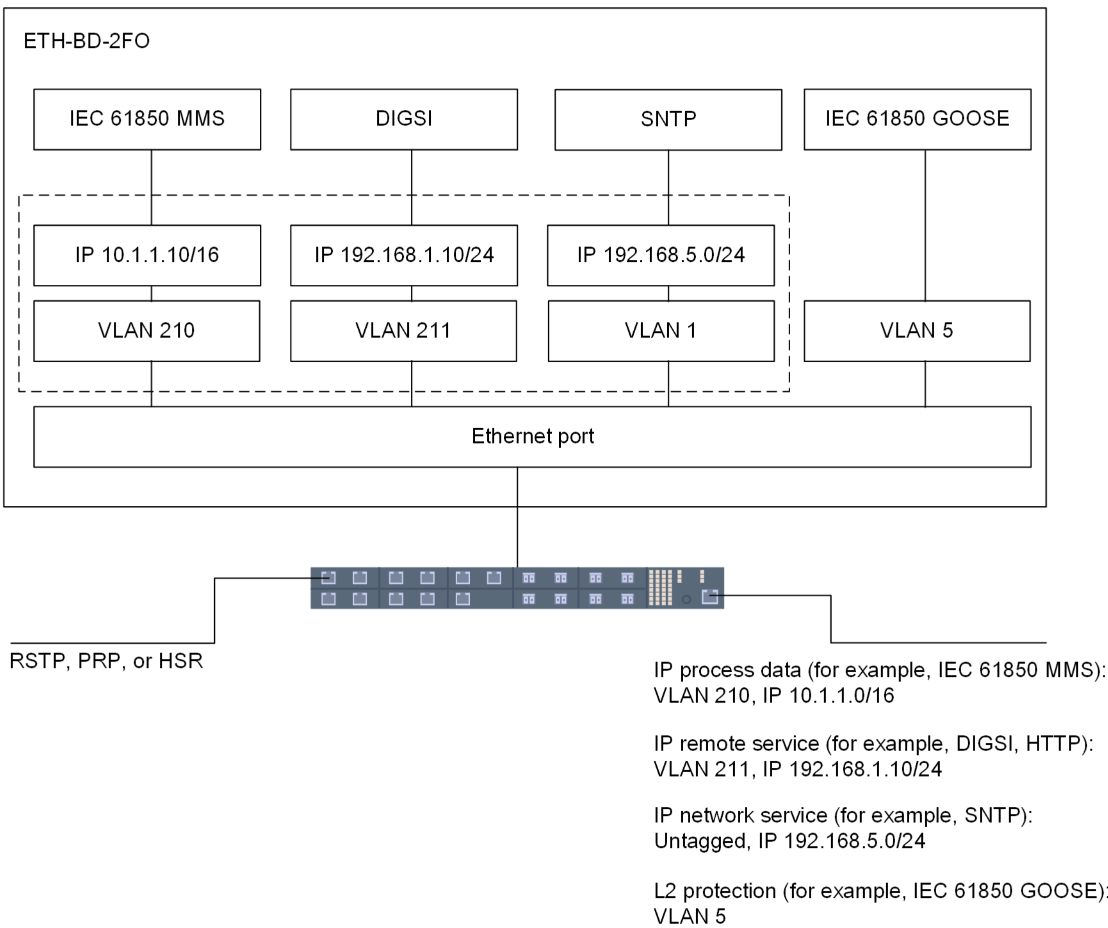
1.7.3.1 Overview

The Virtual Local Area Network (VLAN) is a data-link layer technology and standardized in IEEE 802.1Q. VLAN allows separation of different communication traffic types (for example, process data, engineering or management, voice calls, and video surveillance) sharing the physical links of the Ethernet network.

Regarding VLAN, SIPROTEC 5 supports the following protocols and technologies:

- Pure layer 2 protocols, for example, GOOSE and SMV.
- IP-based protocols, for example, IEC 61850 MMS, DIGSI 5.

The following figure shows an example of the VLAN solution:



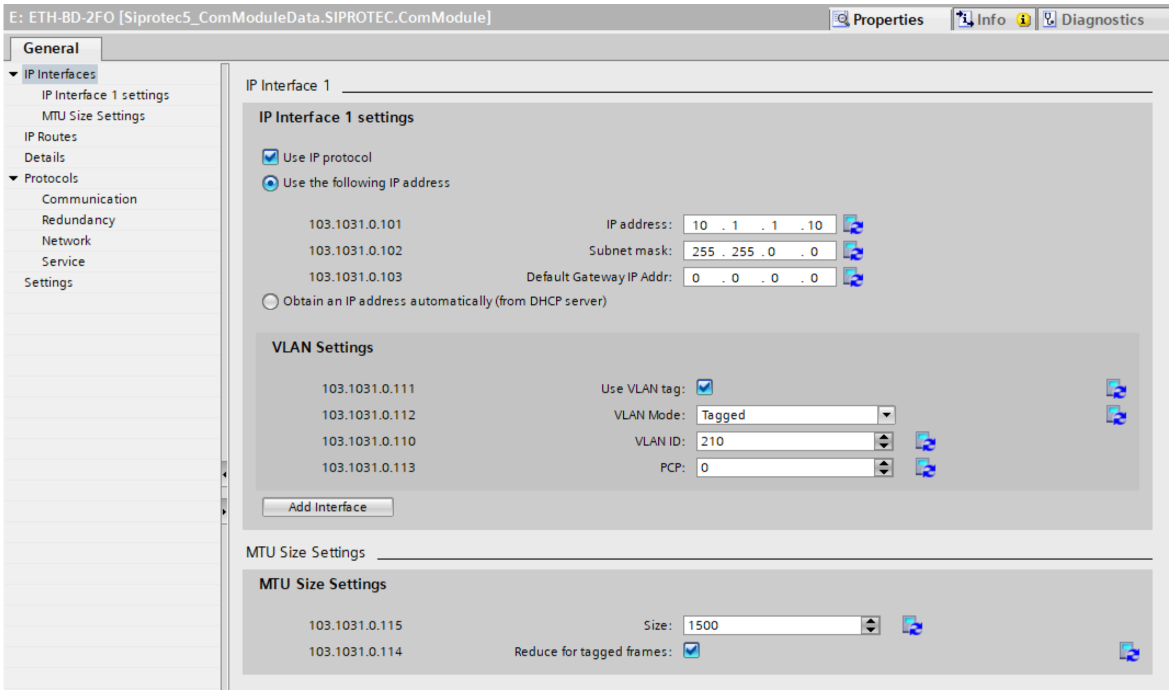
[dw_VLANSolutionExample, 2, en_US]

Figure 1-27 VLAN Solution Example

1.7.3.2 Settings in DIGSI

IP-Interface Settings

In DIGSI 5, you can configure the Ethernet communication module ETH-BD-2FO with IP-interface settings under the **General** section of the **Properties** tab.



[sc_VLANSettings, 1, en_US]

Figure 1-28 IP-Interface Settings

You can assign the IP address of the IP interface manually or by DHCP.

If **Use the following IP address** is marked, you have to assign the IP address of the IP interface manually.

Table 1-3 Setting Notes for IP address of IP interface

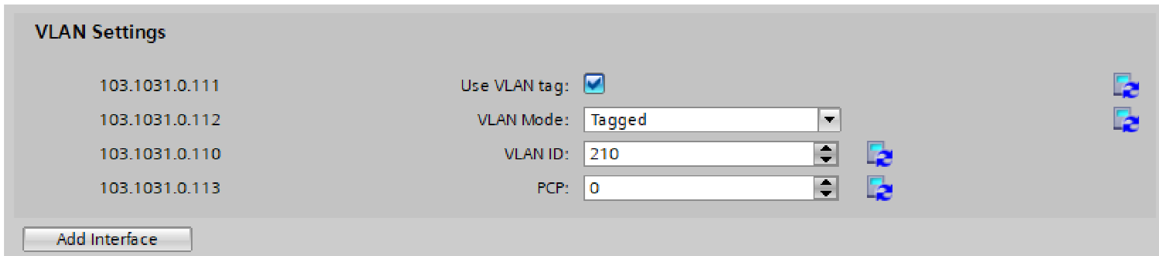
Parameter Name	Description	Settings
IP address	With the parameter **IP address**, you set the IP address of the IP interface.	The IP addresses have the format **x.y.y.x** (x: 1 to 254, y: 0 to 254). Not every possible combination is permissible within the range of value. Impermissible combinations are indicated automatically.
Subnet mask	Subnet mask is a 32-bit value that enables the recipient of IP packets to distinguish the network ID and host ID portions of the IP address.	Typically, the subnet masks use the format 255.x.x.x.
Default Gateway IP Addr	With the parameter **IP address**, you set the IP address of the default gateway. Each communication module only has 1 default gateway IP address. You can configure this parameter only in IP interface 1.	The IP addresses have the format **x.y.y.x** (x: 1 to 254, y: 0 to 254). Not every possible combination is permissible within the range of value. Impermissible combinations are indicated automatically.

If the **Obtain an IP address automatically (from DHCP server)** is marked, the IP address and default gateway IP address, the Subnet mask, are assigned by the DHCP (Dynamic Host Configuration Protocol) server.

NOTE

Make sure that each module is only assigned to 1 default gateway IP address.

VLAN settings are deactivated by default. You can activate the VLAN settings by marking the **Use VLAN tag** check box.



[sc_VLANSettingsEnabled, 1, en_US]

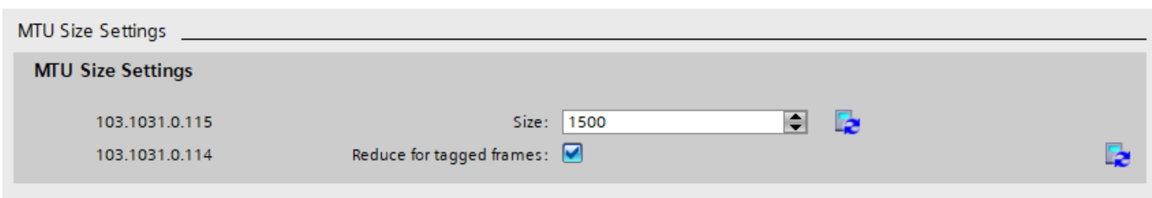
Figure 1-29 Activated VLAN Settings

Table 1-4 Setting Notes for VLAN

Parameter Name	Description	Settings
`Use VLAN tag`	With the parameter **`Use VLAN tag`**, you determine to activate the VLAN settings in DIGSI 5. The VLAN settings are deactivated by default. If the VLAN settings are deactivated, the untagged frames are sent by the IP interface. Received untagged and priority-tagged frames are accepted by the IP interface. If the VLAN settings are activated, the following values are set: • VLAN Mode = Tagged by default • VLAN ID = 2 by default • PCP = 0 by default	Check box unmarked (default setting) Check box marked
`VLAN Mode`	With the parameter **`VLAN Mode`**, you define whether tagged or priority-tagged frames are sent by this IP interface: • If you set the parameter to ***`Tagged`***, VLAN-tagged frames with the configured VLAN ID and PCP are sent via the IP interface. Received tagged frames with the configured VLAN ID are accepted by the IP interface. • If you set the parameter to ***`Priority-tagged`***, priority-tagged frames (**`VLAN ID`** = 0) are sent via the IP interface. Received untagged and priority-tagged frames are accepted by the IP interface.	Tagged (default setting) Priority-tagged

Parameter Name	Description	Settings
VLAN ID	The identifier of a VLAN. The parameter **VLAN ID** identifies which particular VLAN the frame belongs to. • If you have set the parameter **VLAN Mode** to ***Priority-tagged***, the parameter **VLAN ID** is *0* by definition. **VLAN ID** = 0 means that the frame does not belong to any VLAN. • If you have set the parameter **VLAN Mode** to ***Tagged***, you can set the parameter **VLAN ID** from ***2*** to ***4094***. **VLAN ID** = 1 is used internally as Port-VLAN ID (PVID) which will not be configured. **VLAN ID** = 1 cannot be used for user traffic.	Setting range = 2 to 4094 Default setting = 2
PCP	Priority Code Point for frame prioritization according to IEEE 802.1Q.	Setting range = 0 to 7 Default setting = 0

You can configure the size of the maximum transmission unit (MTU) on each Ethernet communication module ETH-BD-2FO.



[sc_MTUSizeSettings, 1, en_US]

Figure 1-30 MTU Size Settings

Table 1-5 Setting Notes for MTU Size

Parameter Name	Description	Settings
Size	With the parameter **Size**, you determine the size of MTU.	Setting range = 576 to 1500 Default setting = 1500
Reduce for tagged frames	If the parameter **Reduce for tagged frames** is marked, the MTU size can be different from the configured MTU size value: • For IP packets sent via VLAN-tagged and priority-tagged IP interfaces, the MTU size is reduced by 4 bytes compared to the configured value. • For IP packets sent via the untagged IP interface, the configured MTU size applies without reduction. If the parameter **Reduce for tagged frame** is unmarked, the configured MTU size value applies to VLAN-tagged, priority-tagged, and untagged IP interfaces.	Check box unmarked Check box marked (default setting)

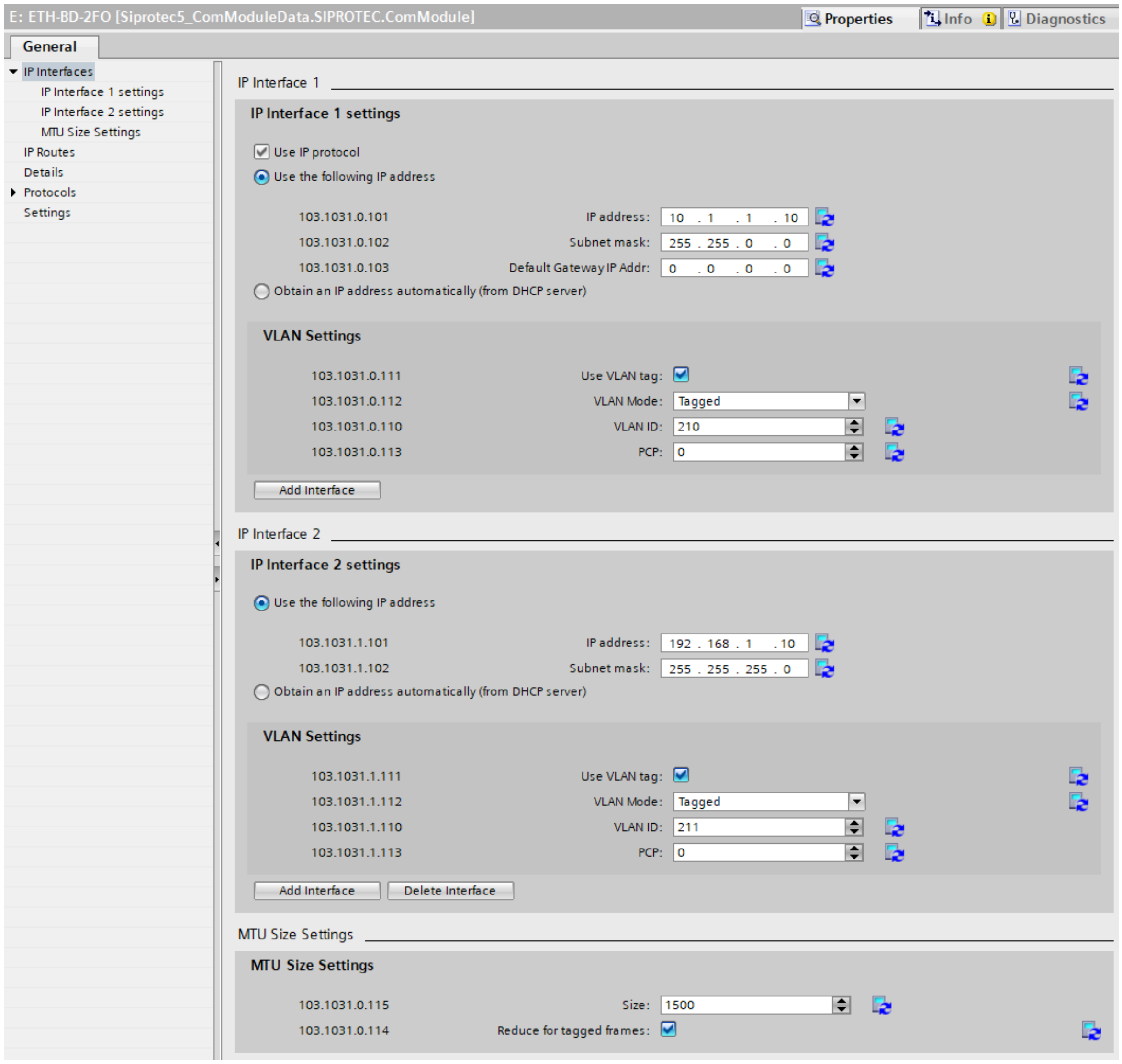
Multiple IP Interfaces with Multiple VLANs

You can add or delete IP interfaces in DIGSI 5 by clicking the button **Add Interface** or the button **Delete Interface**.

The IP interface 1 cannot be deleted. The maximum number of IP interfaces is 3.

Each IP interface can be configured independently. The IP interfaces must belong to separate, non-overlapping IP subnetworks (determined by the IP address and subnet mask). If you have set the parameter **VLAN Mode** to ***Tagged***, each IP interface must have a separate VLAN ID.

Either 1 and only 1 IP interface can have the **Use VLAN tag** parameter unchecked or 1 and only 1 IP interface can have the **VLAN Mode** parameter set to ***Priority-tagged***.



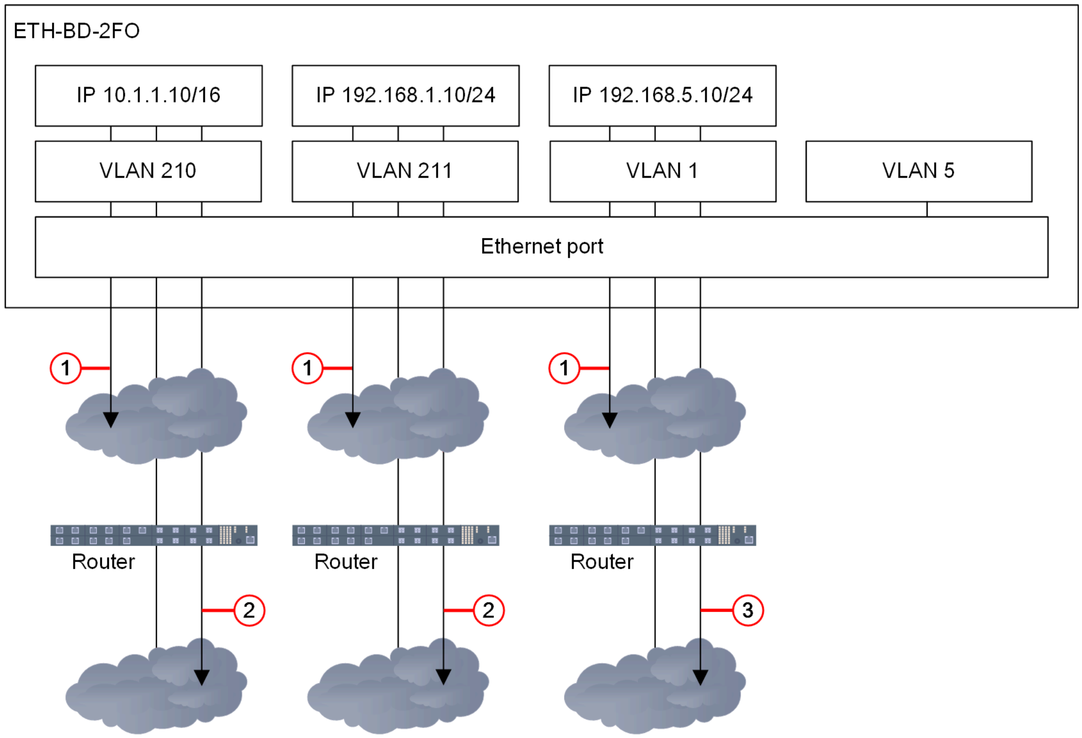
[sc_IPInterfacesSettings, 1, en_US]

Figure 1-31 Multiple IP-Interfaces Settings

Static IP Route Settings

The Ethernet communication module ETH-BD-2FO can communicate with different remote networks via multiple next-hop routers with the help of static IP routes.

The following figure shows an example of the IP route application:



[dw_IPRouteApplication, 1, en_US]

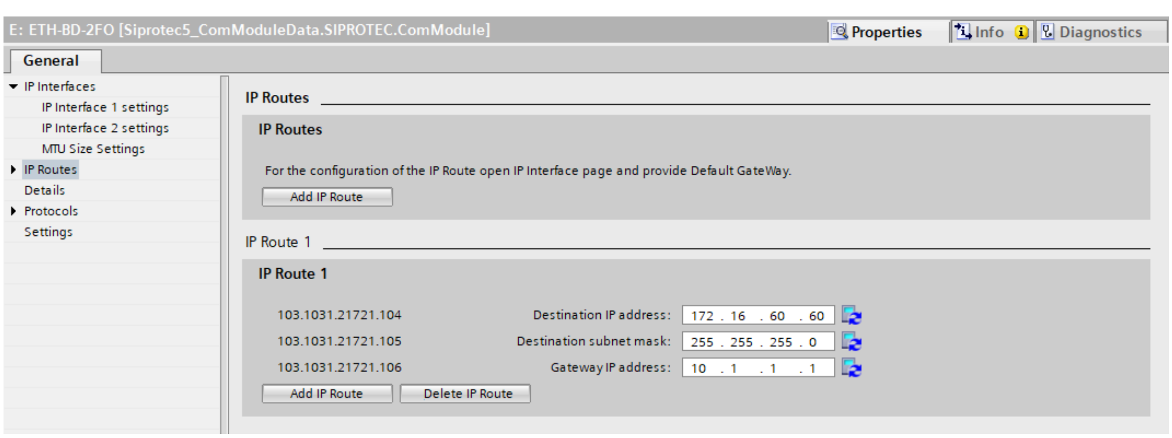
Figure 1-32 IP Route Application

(1) Traffic to the connected network: No IP route is needed.
(2) Traffic to the remote network: Static IP route is needed.
(3) Traffic to the remote network: Using the default route.

In DIGSI 5, you can configure the static IP route settings under the **General** section of the **Properties** tab.

After the default gateway IP address in the IP interface section is assigned by the gateway configuration or DHCP, you can configure the static IP routes.

You can configure up to 10 static IP routes besides the default route set in the gateway address of the interface.



[sc_IPRouteSettings, 1, en_US]

Figure 1-33 Static IP Route Settings

Table 1-6 Setting Notes for Static IP Route

Parameter Name	Description	Settings
`Destination IP address`	The combination of the parameters `Destination IP address` and `Destination subnet mask` determines the destination subnetwork that the static IP route is related to.	The IP addresses have the format **x.y.y.x** (x: 1 to 254, y: 0 to 254). Not every possible combination is permissible within the range of value. Impermissible combinations are indicated automatically.
`Destination subnet mask`		
`Gateway IP address`	With the parameter `Gateway IP address`, you set the IP address of the next-hop router (gateway). The IP route is used for sending IP packets to the destination subnetwork via the next-hop router.	

1.7.3.3 Configuring VLAN

The IP settings and VLAN settings are configured in the **Hardware and protocols** Editor in DIGSI 5.

You can configure the Ethernet communication modules ETH-BD-2FO with IP settings and VLAN settings in DIGSI 5.

Configuring 1 IP Address and VLAN per Module

✧ Select the communication module ETH-BD-2FO in the Device view.

✧ Select the **Properties** tab.

✧ In the lower Editor section, under **General**, double-click the **IP Interface** entry.

✧ Select the **IP Interface 1** entry.

✧ If DHCP is not used, insert IP address, subnet mask, and gateway address.

✧ In the **VLAN Settings** section, check the **Use VLAN tag** check box.

3 settings appear in the **VLAN Settings** section.

✧ Set the desired values for the respective settings.

Configuring Multiple IP Addresses and VLANs per Module

✧ Select the communication module ETH-BD-2FO in the Device view.

✧ Select the **Properties** tab.

✧ In the lower Editor section, under **General**, select the **IP Interface** entry.

✧ Under the **VLAN Settings** section, click the **Add Interface** button.

A new section named **IP interface 2 settings** and its related **VLAN Settings** section appears.

✧ Set the desired values for the respective settings.

IP-Interface Assignment

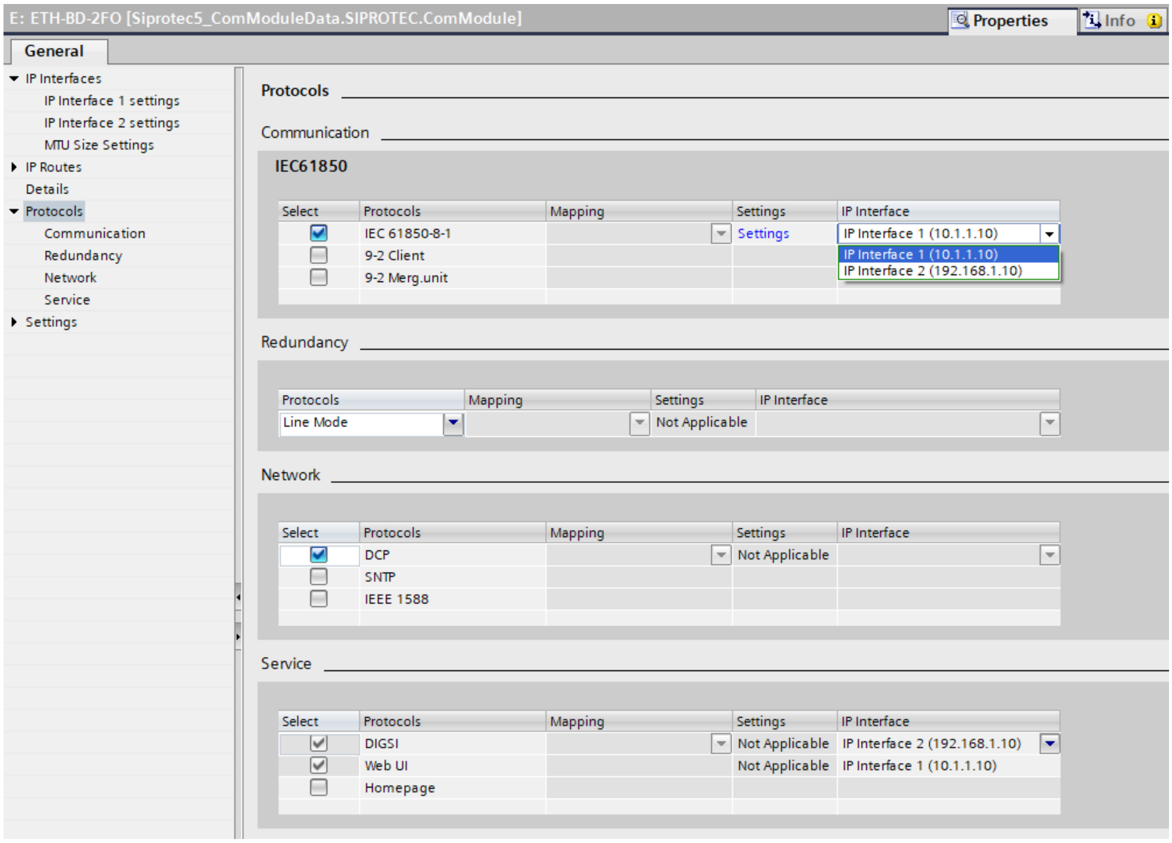
If you have defined multiple IP interfaces on the communication module ETH-BD-2FO, you can assign the IP interface to one or several server protocols. It is not necessary to assign the IP interface to client protocols. The IP interface is selected automatically by the module for client protocols (for example, SNTP, Syslog, RADIUS, MQTT).

✧ Select the communication module ETH-BD-2FO in the Device view.

✧ Select the **Properties** tab.

✧ In the lower Editor section, under **General**, select the **Protocols** entry.

The following figure shows the assignment using the IEC 61850-8-1 as an example.



[sc_IPInterfaceAssignment, 1, en_US]

Figure 1-34 IP-Interface Assignment

✧ Under the **Communication** section, check the **IEC 61850-8-1** check box.

✧ Select the desired IP Interface for the IEC 61850-8-1 protocol.

Configuring Static IP Routes

NOTE

You can configure static IP routes only when the default gateway address has been configured at IP interface 1 or any IP interface has been configured with DHCP.

✧ Select the communication module ETH-BD-2FO in the Device view.

✧ Select the **Properties** tab.

✧ In the lower Editor section, under **General**, select the **IP Routes** entry.

✧ Click the **Add IP Route** button.

A new section named **IP Route 1** appears.

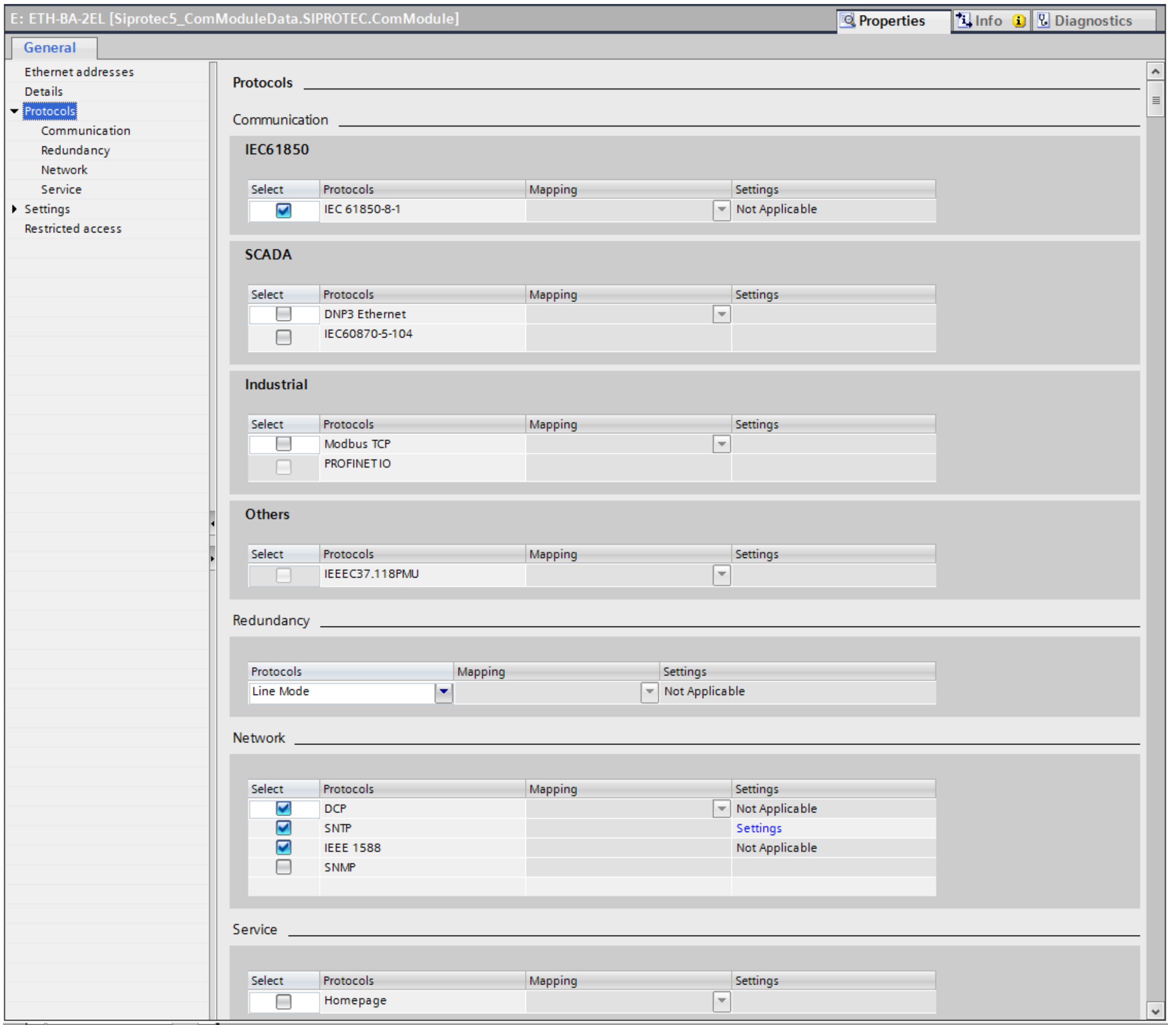
✧ Set the desired values for the respective settings.

NOTE

If destination networks must be reached via multiple next-hop routers (and not only via the single default gateway), the static IP routes are needed.

1.7.4 Parallel Running with IEC 61850

The SIPROTEC 5 device supports the protocols DNP3, Modbus, and IEC 60870-5-104 running in parallel with IEC 61850 on the same communication module.



[sc_IEC61850_other_protocols, 2, en_US]

Figure 1-35 Setting the IEC 61850 Protocol in the Ethernet Communication Module with Other Communication Protocols

Restrictions for DNP3, IEC 60870-5-104, and Modbus TCP

The following restrictions are recommended for DNP3, IEC 60870-5-104, and Modbus TCP:

- IEC 61850 clients: A maximum of 2 clients communicate with the SIPROTEC 5 device at one time.
- GOOSE (Generic Object Oriented Substation Event): A maximum of 5 GOOSE applications/datasets per device, with 50 data objects in total. Set the **`Minimum monitoring time`** to ≥ *10 ms* and use the standard settings of the communication profile **`PriorityLow`** in the GOOSE parameters of the IEC 61850 GOOSE application.

These recommendations are not binding. For example, you can configure more GOOSE applications with more data objects as source and destination and download them into the device. A higher GOOSE load can lead to a delayed transmission.

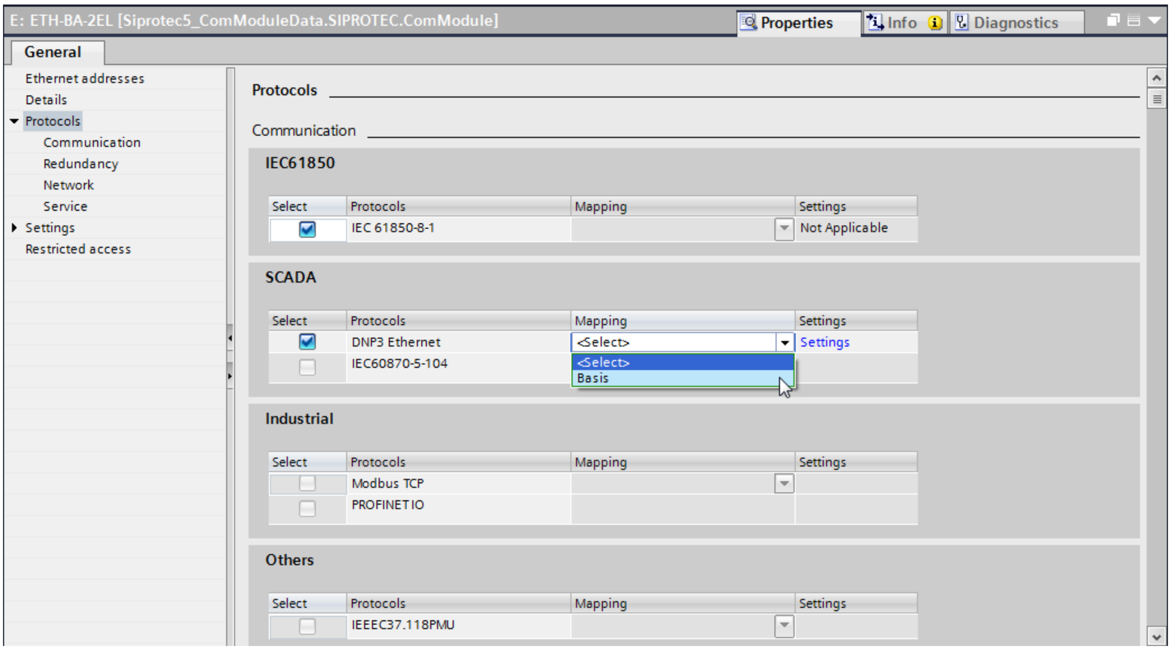
1.7.5 Mapping Selection

A mapping file contains prioritized indications, measured values, and commands.

At least one standard mapping is supplied for the protocol.

Selecting the protocols defines which mappings are available. You can select the mapping separately. The routings defined in the mapping are displayed in the **Communication Mapping** working area for each channel.

Routings in the communication matrix are also possible without selecting an existing mapping file.



[sc mapping selection 050314.tif, 2, en_US]

Figure 1-36 Selecting Mapping – Example for DNP3

NOTE

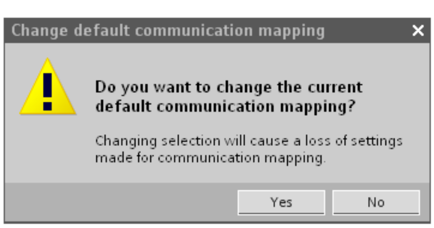
After instantiating the protection functions, assign the standard mapping as the second to last step. After this, you must set parameters for the time synchronization.

Data objects created later on are not automatically included in an existing mapping.

Changing Mappings

NOTE

If you change a standard mapping, all existing mapping information will be lost. DIGSI shows a message to this effect.



[scchgmap-060511-01.tif, 1, en_US]

Figure 1-37 Message in DIGSI

1.8 Adapting Mappings

1.8.1 Description

You can copy mappings within a device to other channels.

The prerouted signals are displayed in the **Communication Mapping** working area.

You can change the mapping on a channel with the following options:

- Routing additional signals by highlighting in the **Receive** or **Transmit** column and entering the protocol parameters
- Deleting existing mapping entries
- Changing the protocol addressing

You can route all information which is not dimmed in the operating range **Communication Mapping** to the protocol. The routing of some typical data types is explained in more detail below:

All data types can be routed to the protocols.

1.8.2 Mapping of Data Types

Indications

The indications are routed by highlighting the object in the **Transmit** column. Indications are information transmitted to a master. After this, you must enter the parameters required for the protocol.

You can route the following IEC 61850 data types to indications (binary inputs):

Data Type	DNP3	IEC 60870-5-104	Modbus	IEC 60870-5-103	PROFINET IO
SPS (Single-point status – single-point indication)	X	X	X	X	X
DPS (Double point status – double-point indication)	X	X	X	X	X
ACD (Directional protection activation information)	X	X	X	X	X
ACT (Protection-activation information)	X	X	X	X	X
ENS (Enumerated Status, for example, mode)	X	X	X	X	X
BSC (Binary controlled step position information)	–	X	X	–	X
INS (Integer status value)	–	X	–	–	–

You can map data types ACD, ACT, and ENS to SPS indications only via conversions. Conversions are used to map individual information contained in the data types. This partial information is automatically provided by the system; you do not have to convert it yourself.

Commands

You route the commands by highlighting in the **Receive** column.

You can route the following IEC 61850 data types to commands (binary outputs):

Data Type	DNP3	IEC 60870-5-104	Modbus	IEC 60870-5-103	PROFINET IO
SPC (Single Point Control)	X	X	X	X	X
DPC (Double Point Control)	X	X	X	X	X
BSC (Binary controlled step position information)	–	X	X	–	–
APC (Controllable analog set point information)	–	X	X	–	–
ENC (Controllable enumerated status)	–	–	–	X	–
INC (Controllable integer status)	–	–	–	–	–

If a command status signal should be mapped or if it is preset through the control model, the status signal from the command will be parameterized in the same line under the **Transmit** column.

Supported Control Models

The SIPROTEC 5 device supports the control models (according to IEC 61850):

- Direct with normal security
- SBO (Select before operate) with normal security
- Direct with enhanced security
- SBO with enhanced security

NOTE

In the case of commands, the IEC 60870-5-103 protocol and PROFINET IO allow only direct switching. Selection is not possible before switching. However, the protocol firmware simulates this cycle (select – operate) internally.

In the case of negative acknowledgment of a command, the reason for the negative acknowledgment cannot be distinguished. The possible reasons are listed in the following:

- Select negative
- Operate negative
- Other interlocking conditions in effect

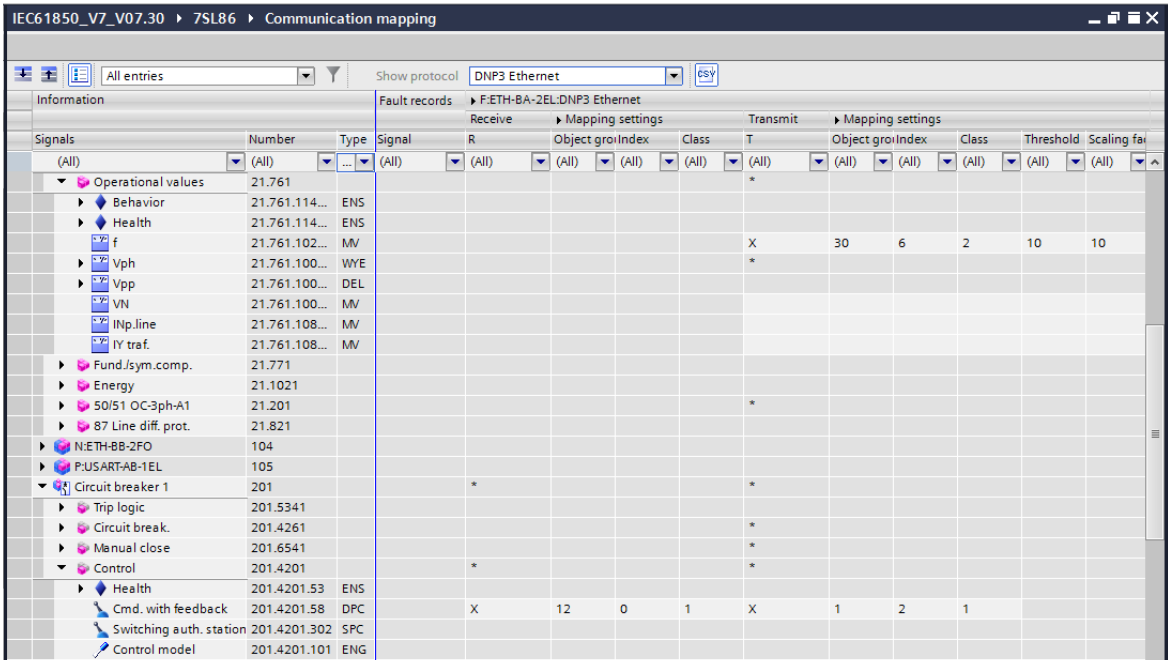
Measured Values

The measured values are routed by highlighting the object in the **Transmit** column. After this, you must enter the parameters required for the protocol.

You can route the following IEC 61850 data types to measured values:

Data Type	DNP3	IEC 60870-5-104	Modbus TCP	IEC 60870-5-103	PROFINET IO
DEL (phase-to-phase related measured values of a 3-phase system)	X	X	X	X	X
MV (measured value)	X	X	X	X	X
WYE (phase-to-ground related measured values of a 3-phase system)	X	X	X	X	X

You can map data types DEL and WYE to MV measured values only via conversions.



[sc_Mapping_all, 1, en_US]

Figure 1-38 Mapping of Indications, Commands, and Measured Values

Setting the Measured-Value Threshold

When processing measured values via the protocol, there are measured-value thresholds that you can set. The measured-value threshold for the individual measured values is not set in the communication matrix but centrally in the routing matrix. The following thresholds are preset:

Measured-Value Threshold	Setting Value
Deadband for values of the type **frequencies**: (Neutral zone for values of the type **frequencies**)	0.1 %
Deadband for values of the type **voltages**: (Neutral zone for values of the type **voltages**)	2 %
Deadband for values of the type **currents**: (Neutral zone for values of the type **currents**)	10 %
Deadband for values of the type **power**: (Neutral zone for values of the type **power**)	10 %
Deadband for values of the type **all others**: (Neutral zone for values of the type **all others**)	10 %
Deadband angle (dbAng) for values of all types: (Neutral zone angle (dbAng) for values of all types)	1 %

This setting value applies to the current measured value. If, for instance, the measured value is 110 kV and the default setting is 2 %, then the measured value will be transmitted in the event that the measured values changes by 2.2 kV.

Changes in the current value are compared with the value most recently transmitted and entered in an absolute summation, that is, regardless of whether the changes are positive or negative. If this sum violates a set threshold value that is value-dependent, the current measured value at that time is transmitted.

NOTE

All measured values are primary values. The unit for current is A or kA, the unit for voltage is kV, and the unit for apparent power is MVA or kVA, depending on the transformer values or rated values.

Counter Values

The counter values are routed by highlighting the object in the **Send** transmit column.

Data Type	DNP3	IEC 60870-5-104	Modbus	IEC 60870-5-103	PROFINET IO
BCR (Binary Counter Reading)	X	X	X	X	–

NOTE

For pulse counters, only the generated pulses are transmitted. The multiplier that can be set in DIGSI is not taken into account. This can lead to deviations between the transmitted value and the value displayed in the device.

Exemplary Calculations

The scaling of a power meter is defined by the following values:

60 000 pulses per hour correspond to $V = V_{prim}$ and $I = I_{prim}$.

V_{prim} = Rated voltage

I_{prim} = Rated current

The measured performance value is calculated based on the following formula:

$$V_{rated} \cdot I_{rated} \cdot \sqrt{3} = 2078.46\ \text{kW} = 2.078\ \text{MW}$$

[foleismw-121109-01.tif, 1, en_US]

In the SIPROTEC 5 device, this measured performance value is stated from 0.00 MW to 9.99 MW, that is with 2 relevant decimal places.

Siemens recommends a scaling factor of 100 for the transmission as an integer measured value through DNP3. With this, a value from 0 to 999 is transferred to the master.

If the scaling factor is less than 100, then important information about the decimal places is lost during the transmission. A scaling factor larger than 100 does not create any precise information. The accuracy is only simulated, but really non-existent. Thus, with a scaling factor of 100, there is an interpretation of the integer measured value (measured value $_{Integer}$) through DNP3 with: ±32 768. This corresponds to a value of ± 327.68 MW.

IEC 60870-5-103

Counter values, for example, kWh, are not defined in the IEC 60870-5-103 standard; consequently, there is no compatible data unit for transmission of the metered values. However, some SIPROTEC devices offer the ability to transmit metered values on the basis of IEC 60870-5-103. Private data unit 205 has been defined for this purpose. Metered values are transmitted as spontaneous indications. Each telegram contains a metered value with its own function type and information number.

IEC 60870-5-104

You can use counter interrogation commands to interrogate the integrated total. SIPROTEC 5 supports TI <101> with the functionality **Reset**. You can interrogate the integrated total with interrogation group 1 to interrogation group 4 and the general interrogation counter. You can reset the counter values with general interrogation counters as well as the interrogation group 1 to interrogation group 4. The interrogated integrated total is transmitted with Cause of Transmission <37> to <41>.

You can find additional information on Cause of Transmission in the standard IEC 60870-5-101, chapter 7.2.3.

1.8.3 Transmission Buffer

The protocols IEC 60870-5-103, DNP3, IEC 60870-5-104, and Modbus TCP support the transmission-buffer feature with the following characteristics:

- The transmission buffer is a ring buffer.
- If the buffer overflows, the current entry overwrites the earliest entry.
- If all the supported event types for the indication (for example, SPS, DPS, ACD, ACT, ENS, or BSC) are mapped to the communication protocol, they are used in the transmission buffer.
- When the object value changes, it is stored in the transmission buffer with a time stamp.
- After the device initialization or reboot, the transmission buffer is empty and then the startup values of the objects are entered in the transmission buffer.
- If the communication fails, the transmission buffer is not erased. Once the communication connection is re-established, entries are still saved and the protocol master reads the entries. If necessary, the buffer overflow is indicated.
- Once the buffer has been transmitted to the master, the transmitted transmission-buffer entries are deleted from the transmission buffer.

NOTE

You can find more information on the SOE properties for the Modbus TCP protocol in chapter *5.2.2 Properties of the Sequence of Event*.

1.8.4 Columns in the Communication Mapping Matrix

All protocols, except IEC 61850, have a communication address you can configure in the Communication mapping.
In the following table, you can find information concerning the columns that are only available for the protocols **IEC 60870-5-103 , IEC 60870-5-104 , Modbus TCP**, **DNP3**, and **PROFINET IO**. The columns are not available if none of these protocols is configured.

Element	Explanation
Toolbar	The Toolbar of the communication mapping matrix allows fast access to actions and settings.
Columns that are Always Present These columns are always present regardless of whether a protocol is configured or not, or which protocol is selected.	
Signals	This column contains the names of the signals. All signals are structured in a hierarchical manner according to function groups and functions. The structure is an image of the signal list. Click on the arrows to the left of the element names to show or hide individual elements of the structure.
Number	This column contains the unique number for each signal. If this column is not visible, click in the toolbar of the **Communication mapping** matrix on the following button:  The column is shown.
Type	This column contains the type for each signal, for example, **MV, INS**.
Fault record	This column indicates whether a signal is routed to the fault record. If a signal is routed to the fault record, the cell pertaining to the signal has an **X**. The cell is empty if a signal is not routed.

Element	Explanation
Columns Present for All Protocols These columns are available only for the **IEC 60870-5-103**, **IEC 60870-5-104**, **Modbus TCP**, **PROFINET IO**, and **DNP3** protocols as well as for the protection-data communication protocol. The columns are not available if none of these protocols is configured.	
Receive	You can route the input indications and commands in the receive direction in this column.
Transmit	You can route the output indications and measured values in the transmit direction in this column.
IEC 60870-5-103 These columns are available only for the **IEC 60870-5-103** protocol. The columns are not available if this protocol is not configured.	
Function type	Enter the number of a function type for a signal that has been routed in this column. The function type identifies the functionality of a device. Certain numbers are not used. You can use these numbers as you like, without affecting the IEC 60870-5-103 compatibility.
Information number	Enter an information number for a signal that has been routed in this column. The information number describes the signal category (Indication, metered value or command).
Data unit	Enter the number of a data unit (DU) for a signal that has been routed in this column. Depending on the signal type, you can select from different data units.
General interrogation	Specify in this column for an indication that has been routed, whether it is subject to general interrogation or not. You can select between **Yes** or **No**. If you select **Yes**, the indication is additionally transmitted only within the scope of a general interrogation.
Position	Specify in this column the position in the measured value telegram for a measured value that has been routed. In a 3-frame DU, you can route up to 4 measured values. In a 9-frame DU, you can route up to 16 measured values. In total, you can route one 3-frame DU and two 9-frame DU.
Fault channel	In this column, you can route a measured value that has been routed to the analog channel of a fault record. Enter the number of the fault-record channel for this purpose.
IEC 60870-5-104 These columns are available only for the **IEC 60870-5-104** protocol. The columns are not available if this protocol is not configured.	
IOA	With this column, you can specify the Information object address (IOA).
IOA 1	With this column, you can specify the 1st byte of the Information object address (IOA) with low byte.
IOA 2	With this column, you can specify the 2nd byte of the Information object address (IOA).
IOA 3	With this column, you can specify the 3rd byte of the Information object address (IOA) with high byte.
TI	This column indicates the **Type identification**.
GI group	Specify in this column for an indication that has been routed, whether it is subject to General Interrogation group (GI group) or not.
Threshold	Enter a measured-value threshold in percent for a measured value that has been routed in this column.
ScaledFactor	This column indicates the scaled factor for the measured values.
NormalizedMaxValue	This column indicates the maximum percentage value for the measured values.

Element	Explanation
Modbus TCP These columns are available only for the **Modbus TCP** protocol. The columns are not available if this protocol is not configured.	
Register type	In this column, you can specify the Register type. It describes the function code to retrieve the data of the signal.
Register address	Enter a register address for a signal that has been routed in this column. The register address has a certain range for different signal categories.
Event of Protection	You can specify in this column whether an indication that has been routed is subject to an Event of Protection or not.
PROFINET IO These columns are available only for the **PROFINET IO** protocol. The columns are not available if this protocol is not configured.	
Value	In this column, you can specify the address for a signal that has been routed. The address has a certain range for different signal categories.
DNP3 These columns are available only for the **DNP3** protocol. The columns are not available if this protocol is not configured.	
Index	Enter an index number ranging from 1 to 1,000 for a signal that has been routed in this column.
Class	Assign one of 3 classes to a signal that has been routed in this column. The class 1 is reserved for critical events. You can assign the class 2 or 3 to the less critical events.
Threshold	Enter a measured-value threshold in percent for a measured value that has been routed in this column. The measured-value threshold determines the transmission frequency of measured values. If you select the value zero for the measured-value threshold, each measured value is transmitted to the superordinate station. A value of 1 is used to avoid a communication overload. A measured-value threshold other than zero causes all changes of new measured values compared to the measured value transmitted last to be added. If the sum of the changes reaches the percent value set, a new measured value is transmitted at the next possible point in time. This measure prevents loading the communication path too much.
Protection-Data Communication Protocol These columns are available only for the protection-data communication protocol. The columns are not available if this protocol is not configured.	
Priority level	Select one of 3 priority levels for a signal that has been routed in this column. The priority level decides on how often it is transmitted.
Bit position	Set a bit position in the data bar for each signal that has been routed in this column. Note that some signal types need more than one bit. Also take care to ensure that a bit position is not already assigned to a signal of another device.
Fallback value	Select a fallback value for a received signal in this column. The fallback value decides what passes with the value of a signal if the connection is interrupted. Depending on the signal type, various fallback values can be selected. For example, the signal value can be set to a secure status or the last value received is retained.
IEC 60870-5-103 and DNP3 These columns are available only for the **IEC 60870-5-103** and **DNP3** protocols. The columns are not available if none of these protocols is configured.	
Object group	Enter the number of an object group for a parameter that has been routed in this column.
Scaling factor	Enter a value for the measured scaling for a measured value that has been routed in this column.

Element	Explanation
Busbar-Protection Protocol This column is only available for the busbar-protection bay units with busbar-protection protocol.	
Transmit	This column shows the fixed default settings for the routings for current measured values and switch positions that are necessary for the busbar protection.

Columns for IEC 60870-5-104

NOTE

The **Event of Protection** column in the communication mapping only affects the types **SPS** and **DPS**:

- 0: SPS mapped to TI <30>, DPS is mapped to TI <31>.
- 1: SPS and DPS are mapped to TI <38>.

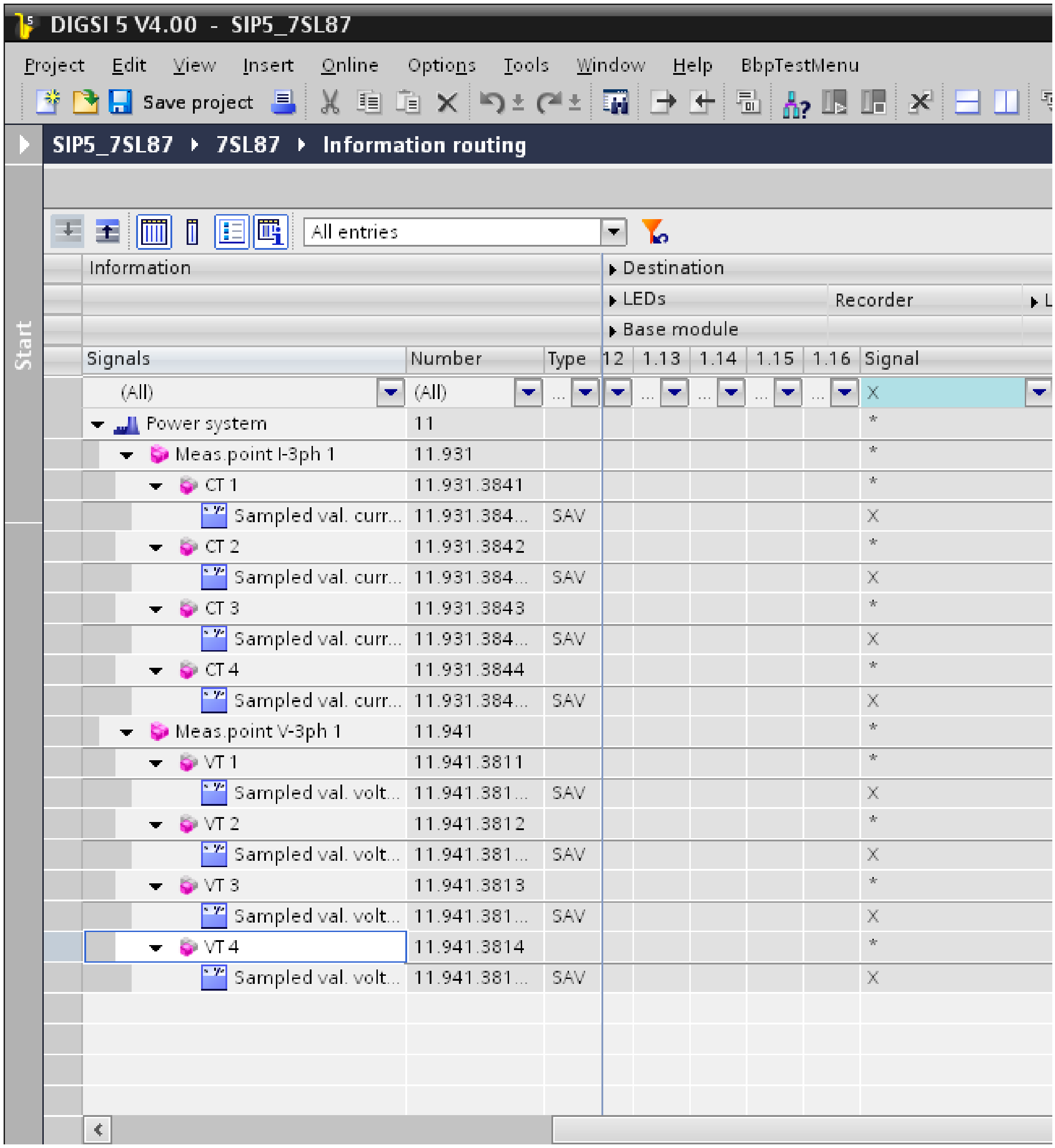
Columns for IEC 60870-5-103

NOTE

The range 242 to 253 in the function types may not be used. This range is used for device-internal information, for example, if the indication for the trigger event of the fault record has the function type **FunctionType:242/InfoNumber1 RcdTrg**. Other information from this internal range cannot be transferred.

1.8.5 Parameterization of Fault Records

Fault records are routed in the **information routing**. The analog and binary signals routed there are displayed in the communication matrix.
Highlight the **Signal** object in the information routing matrix.



[ScFltRecParT104_270813, 1, en_US]

Figure 1-39 Parameterization of Fault Records

NOTE

If the fault record for the serial protocol is selected, Siemens recommends 5 seconds as the setting for the maximum length of a fault (default setting in device). If the fault record is longer, the connection to the device could be broken because large data volumes have to be transferred serially. This constraint does not apply for Ethernet protocols.

IEC 60870-5-103

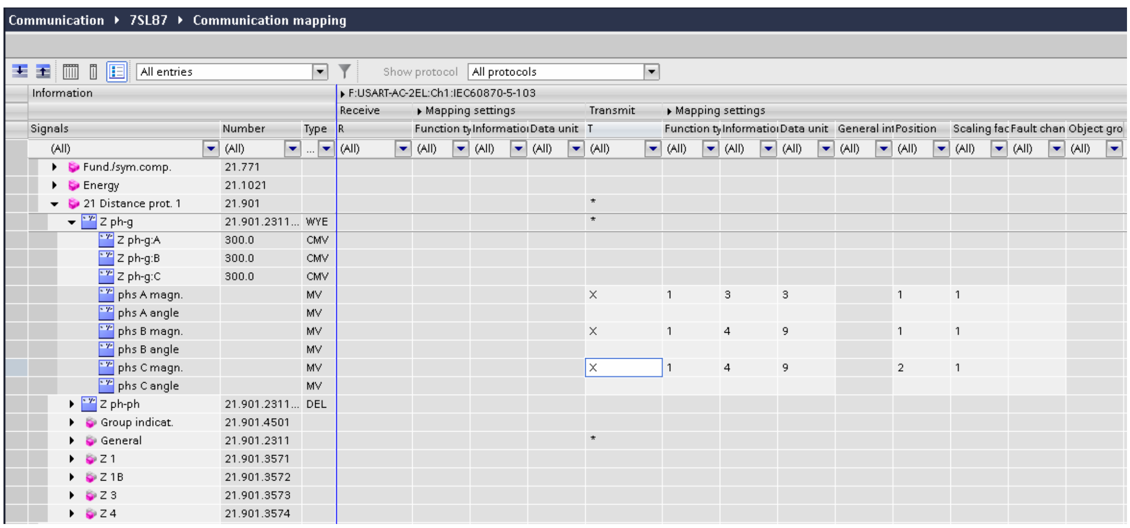
You make a selection for IEC 60870-5-103 from the analog signals by entering the channel numbers for the individual signals in the communication matrix. Using this channel number in a compatible range or in a Siemens-specific extension, the fault record is transmitted to a substation control unit. The sampling rate is 1 kHz.

The protocol requires additional settings. Sampled values as well as measured values can be routed and transmitted. For binary signals, the function type and information number must be entered in the communication matrix as well. All routed information is identified in the communication matrix by an **X** in the **Recorder** column. If this information is also to be transmitted via the IEC 60870-5-103 protocol for fault records, then you must specify the fault channel for the analog channels (**Enter values** column in DIGSI 5).

NOTE

With connection to SICAM PAS, the channel number 108 is reserved and must not be assigned here.

A maximum of 8 fault records can be prepared in the device for the IEC 60870-5-103 protocol. Since a larger number is stored internally in the device, only the most recent fault records are prepared for the IEC 60870-5-103 protocol in the device.



[scfltrec-280113-01.tif, 1, en_US]

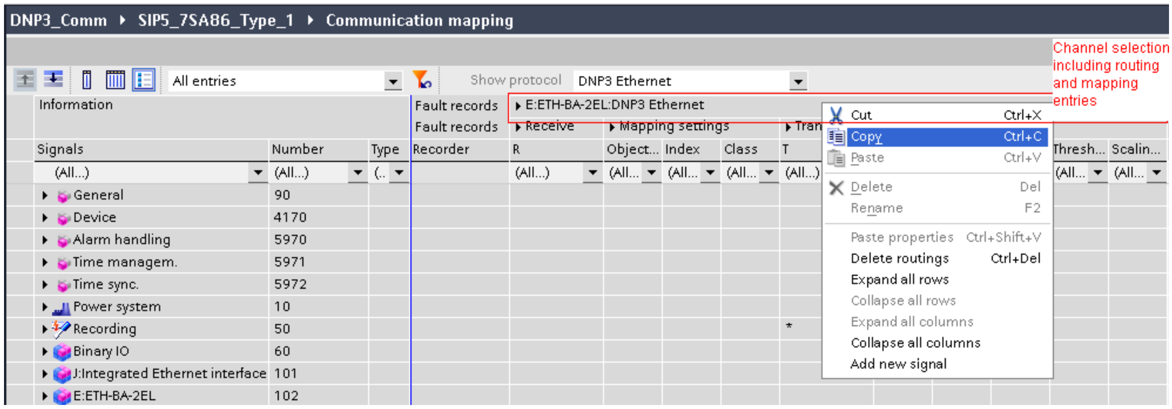
Figure 1-40 Parameterization of Fault Records

IEC 60870-5-104

For the IEC 60870-5-104 protocol, the most recent 8 fault records are prepared in the communication module.

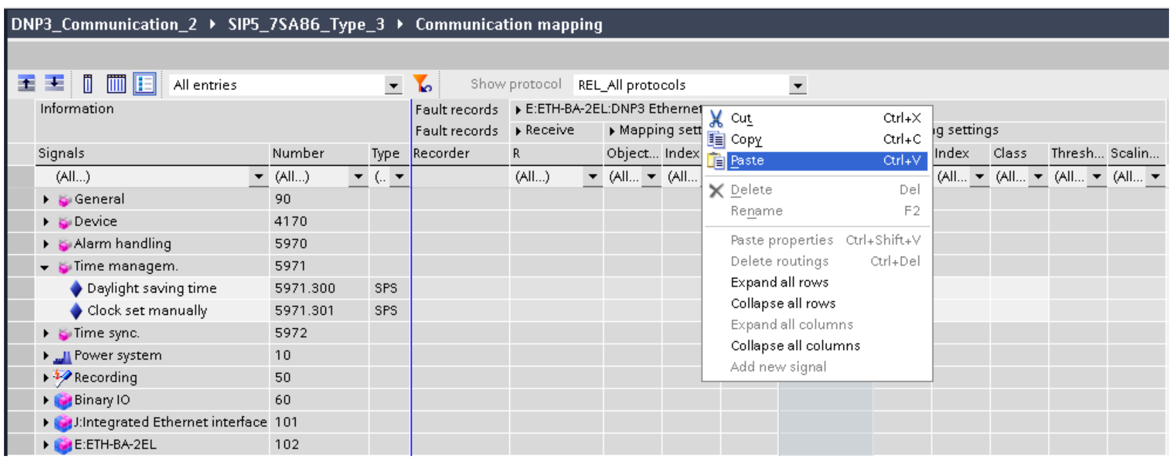
1.8.6 Copying Mappings

Once created, mappings can be copied to another channel on which the protocol also runs and also transferred to another device.



[sccopchn-240111-01.tif, 1, en_US]

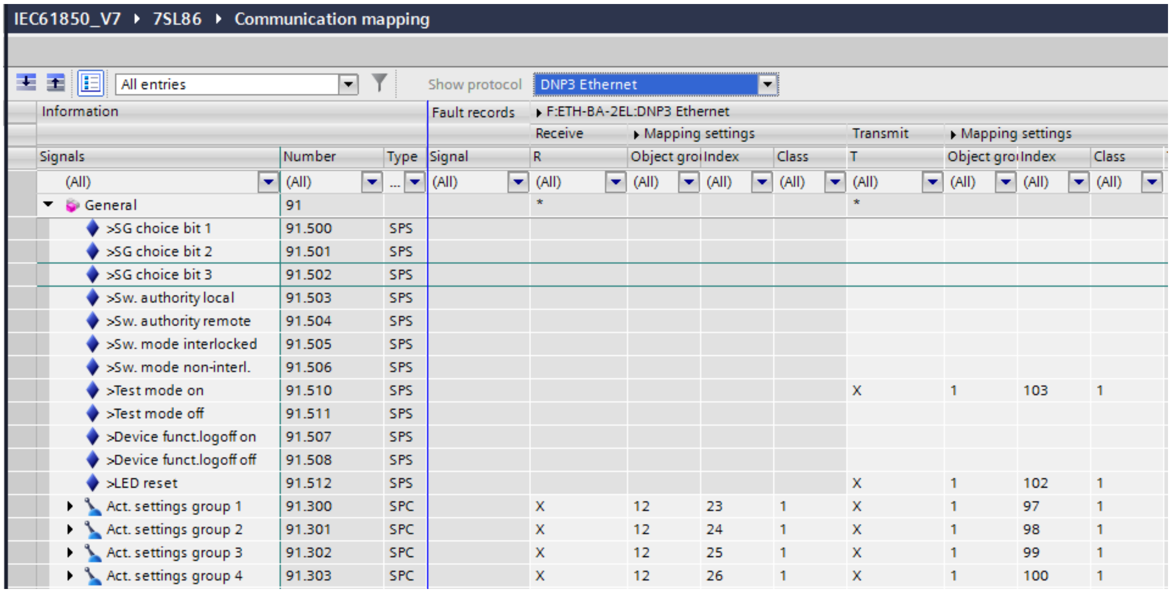
Figure 1-41 Copying Mapping Settings from a Channel



[scpaschn-250111-01.tif, 1, en_US]

Figure 1-42 Pasting Mapping Settings from a Channel

You can select a predefined mapping for a channel. You can then change the mapping and save it for this channel.



[sc_Mapping_overview, 1, en_US]

Figure 1-43 Changed Mapping

You can also copy the changed mappings between the channels, but you cannot save a changed mapping in the DIGSI 5 library again and then select it for another channel.

NOTE

When copying to a different device, only the mappings are copied for which the same function groups/functions/function blocks exist in the source and target device.

The mapping must match the application template of the device when copying to another device. The devices must be of the same type.

1.8.7 Exporting Mappings

Once created, mappings can be exported to a data file. The master/client configuration software can be configured using this export.

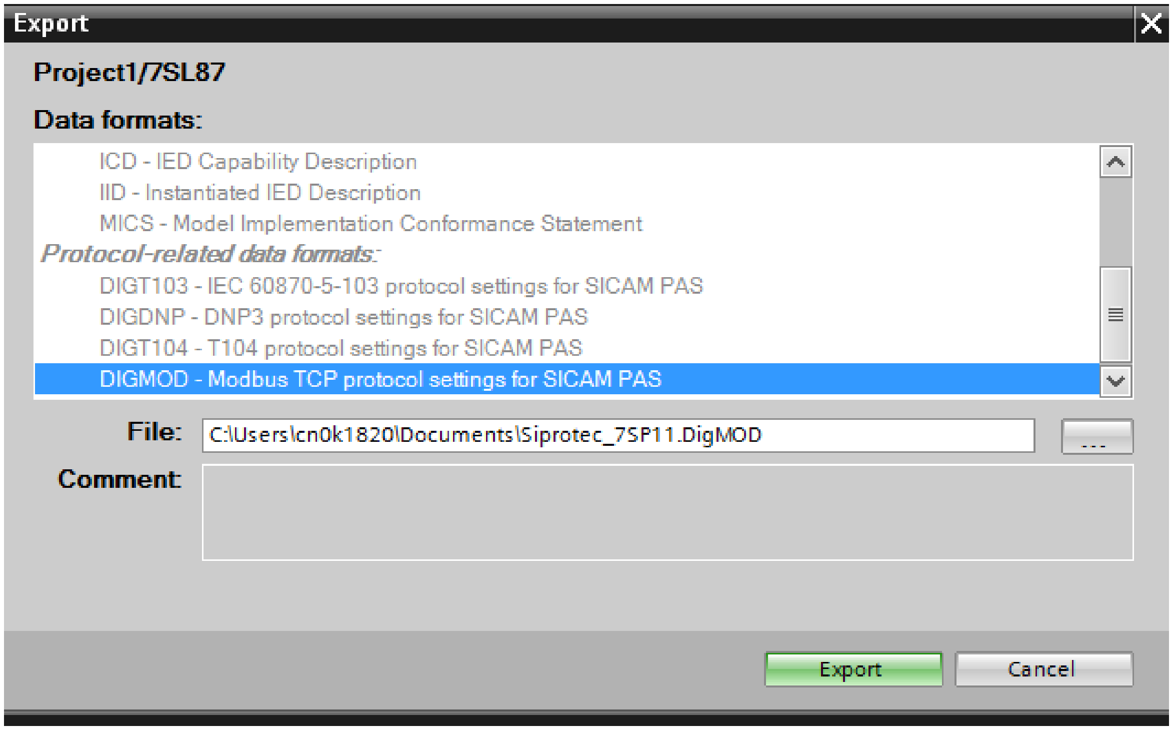
The Siemens parameterization software for SICAM PAS systems control can import this file directly.

To export a device mapping file, select the device and click the **Project** menu. Then select the menu item **Export**. The **Export** dialog appears.

You can select from the following data formats for the export:

- Device-dependent data formats, for example, TEAX, DEX5
- Protocol-dependent data formats
  For every protocol for which parameters are set, there is an own XML format with the appropriate file extension DigT103, DigDNP, DigT104, and DigMod.

Finally, click **Export**.



[Sc_MapExp_Modbus, 1, en_US]

Figure 1-44 Exporting Mapping

NOTE

SICAM PAS does not support the import of the file with all function codes configured in DIGSI 5.

You can find more information in the SICAM PAS manual and in the DIGSI 5 Online Help.

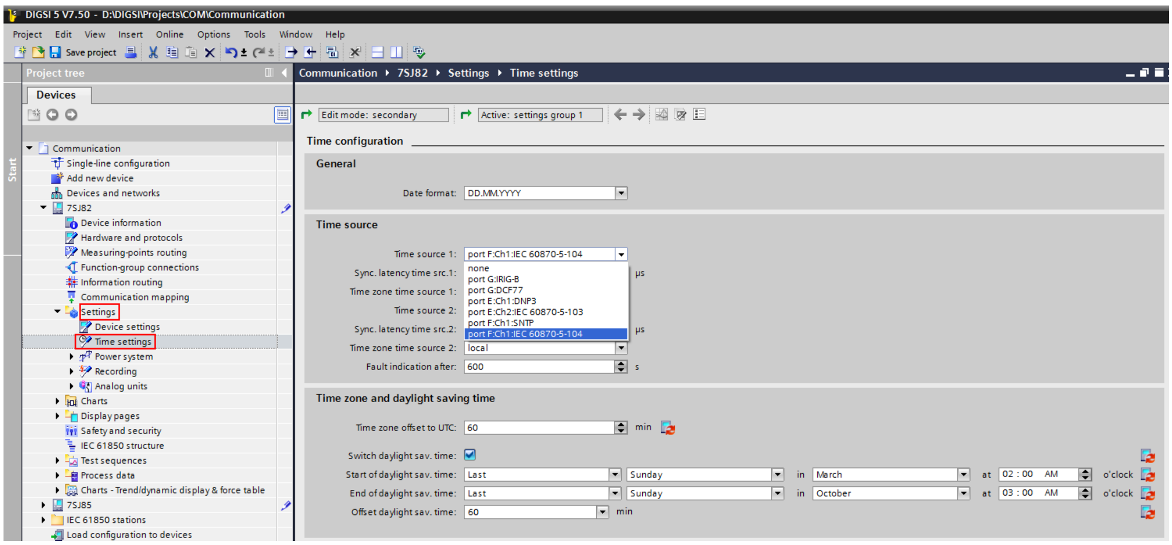
1.9 Time Synchronization

In order to allow the correct time recording of events synchronously, SIPROTEC 5 devices need a time synchronization.

Setting the Time Source

Parameters for 2 main clocks can be set in a SIPROTEC 5 device. If a communication protocol with time synchronization possibilities is available in a device, then the time sources can be configured as desired.

Make the time synchronization settings in DIGSI 5 in the **Time Settings** section in the **Parameters** category.



[sc_time_synchronization_sources, 2, en_US]

Figure 1-45 Setting Possibilities for the Time Sources

Set the time sources in the **Time Source 1** and **Time Source 2** fields. If the protocol is parameterized for a number of channels in the device, you can select this protocol for both sources.

Time source 1 is preferred over **Time source 2**. If **Time source 1** is synchronized for a time longer than specified in the setting **Failure indication after**, this time source remains the active synchronization source.

You can select 2 time sources independent of each other for each SIPROTEC 5 device in the time settings. Depending on the device and communication configuration, you have the following selection options:

Time Source	Description
None	An external time source is not configured. The time component inside the device takes on the time synchronization.
IRIG-B	An external IRIG-B receiver connected to port G takes on the time synchronization. This time source is always available for selection, independent of the device and communication configuration. SIPROTEC 5 devices support several protocol variants of the IRIG-B standards: • **IRIG-B 002(003)** The control function bits of the signal are not occupied. The missing year is formed from the current device time. In this case, it is possible to set the year via the online access in DIGSI 5. • **IRIG-B 006(007)** The bits for the calendar year are not equal to 00. The calendar year is set automatically by the time protocol. • **IRIG-B 005(004) with extension according to IEEE C37.118-2005** If in the time signal, other control function bits are occupied in addition to the calendar year, then the SIPROTEC 5 device takes the additional information into consideration for leap seconds, daylight saving time, time offset (zone, daylight saving time), and time accuracy.
DCF77	An external DCF 77 receiver connected to port G takes on the time synchronization. DCF 77 is only available in central Europe.
PI	Inside a protection topology, one of the devices involved can take on time synchronization as a timing master. The time synchronization is done via the protection connections and the configured protection interfaces of the SIPROTEC 5 devices. Signal runtimes of the protection communication are calculated automatically. This time source is only available for selection under the following prerequisites: • In the SIPROTEC 5 device, at least 1 communication channel is configured as a protection interface. • The SIPROTEC 5 device is not the timing master. This prerequisite is met if the parameter **Local device is device** in the group **Device Combination Settings** has a value that is not 1 (value 1 is the index of the timing master).
SNTP	The time synchronization is done via the Ethernet-based SNTP (Simple Network Time Protocol), for example with IEC 61850 stations. You can address 2 timers independent of each other in the group **SNTP Settings**, which feed their time signals into the Ethernet network. SIPROTEC 5 devices support both Edition 1 and Edition 2 in accordance with IEC 61850-7-2. In Edition 2, the logical attributes **LeapSecondsKnown**, **ClockFailure**, **ClockNotSynchronized**, and the value **TimeAccuracy** are maintained in each time stamp. In Edition 1, these signals contain default values. Thus, the interoperability for station-control technologies is ensured for both editions. The SNTP service must be activated in the configuration of the Ethernet interface in the group **Ethernet Module – Channel x Settings**, so that this service can be selected as a time source.

Time Source	Description
IEEE 1588	For time synchronization via Ethernet systems, you can use the protocol IEEE 1588. In this case, besides the clocks, all other power-system components must also support IEEE 1588, for example, switches as transparent clock (TC) or boundary clock (BC). There must be a timing master in the system. If there are several timing masters in the system, the actual master is set according to the IEEE 1588 best-master-clock algorithm (BMC). The actual timing master transmits the time to the receivers using Ethernet multicast. The SIPROTEC 5 device is such a receiver and subscribes to the multicast address while the IEEE 1588 option is activated. The transmission can be done with or with-out VLAN tag.
IEC 60870-5-103	The time is synchronized via telegram with an appropriately configured communication interface in accordance with the **IEC 60870-5-103** protocol.
IEC 60870-5-104	The time is synchronized via telegram with an appropriately configured communication interface in accordance with the **IEC 60870-5-104** protocol.
Modbus TCP	For time synchronization via SNTP, you can use the **Modbus TCP** protocol. The **Modbus TCP** protocol does not support the time synchronization.
DNP3	The time is synchronized via telegram with the appropriately configured communication interface in accordance with the **DNP 3** protocol. SIPROTEC 5 devices support 2 instances: • **Time synchronization via UTC** • **Time synchronization with local time** The daylight saving time status is not transmitted. The device assumes that the DNP3 master follows the same rules for the start and end of the daylight saving time as those that were set for the device.

Time sync. error Indication

If both timing masters (Time Source 1 and Time Source 2) are not available or receivable anymore, the synchronization does not take place anymore. After expiration of a set supervision time (parameter **Fault indication after**), the device indicates a time-synchronization failure (**Clock not synchronized indication**). From this point in time, the status **Clock failure** is set in the time stamp of all indications. The bit **Clock not synchronized** in the Standard IEC 61850-7-2 is set in the time stamp of the data object.

You can also set the time source on the device using **Device Function** → **Date and Time**.

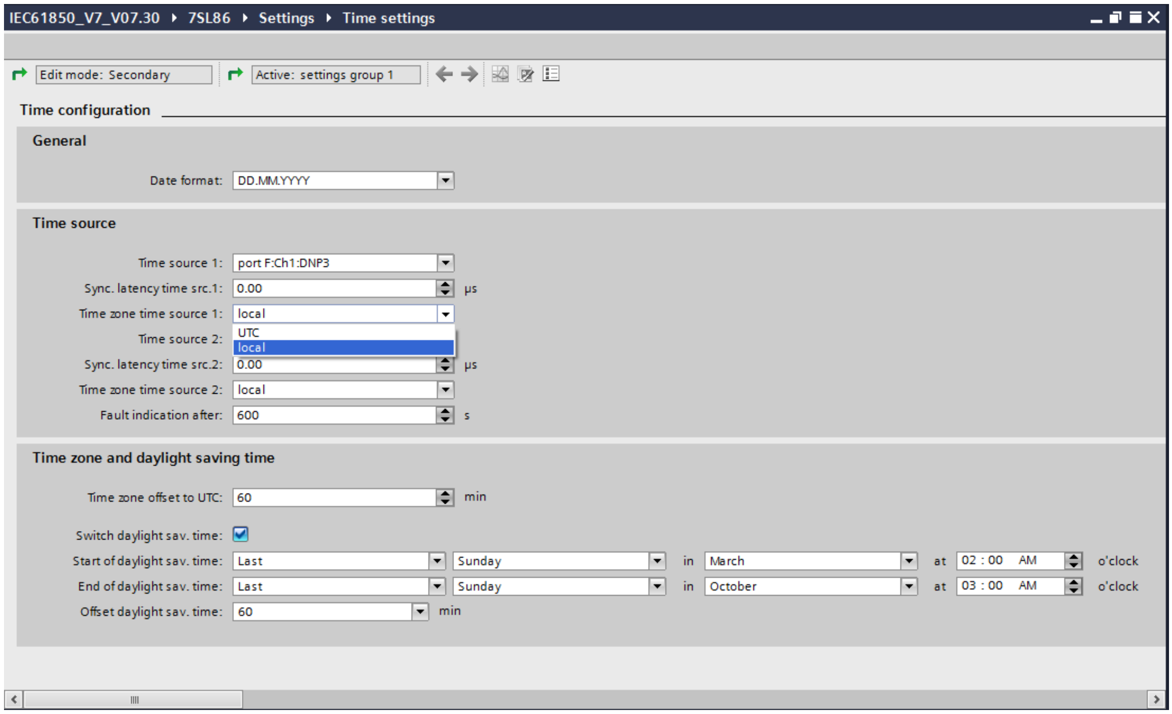
To compare signal runtimes you can define a delay for each time source, which is added to the times received.

Setting the Time Zone

In the protocol, there is the possibility of executing time synchronization with local time or with UTC. The selection occurs in DIGSI 5 with the parameters designated for this.

NOTE

If a time zone for time synchronization is already preset for the communication protocol, for example, DNP3 or IEC 60870-5-104, the time zone of the time source must be identical.



[sc_timezone, 1, en_US]

Figure 1-46 Setting the Time Zone

You can specify separately for each time source, whether their time zone corresponds to universal time (UTC) or to the time zone of the device.

The internal device time is maintained in universal time (UTC). To display time stamps, you can define the local time zone of the SIPROTEC 5 device including the applicable rules for the daylight saving time. This allows the display of the local time.

NOTE

During parameterization, the time in the parameter **Failure indication after** must be greater than the synchronization interval of the master. If the interval is set to 1 minute, the device switches to **Time source 2** if no synchronization telegram has been received from **Time source 1** for more than 1 minute. If **Time source 2** is not set or the last telegram from **Time source 2** was received longer ago than the time set under **Failure indication after**, the indication *Time sync. error* is issued. In addition, all time stamps are marked with the flag **Clock not synchronized**.

Accuracy

The accuracy of the time synchronization of the communication protocols (IEC 60870-5-103, IEC 60870-5-104, Modbus, DNP) is less than 5 ms. The achieved accuracy depends on the master station.

NOTE

If you require a more accurate time synchronization, perform the time synchronization via DCF/IRIG-B or SNTP (Simple Network Time Protocol) and IEEE 1588. A higher accuracy of 1 ms to 2 ms can be reached by using another network-time server.

Indication Synchronization Error

A time master must be present in the network. If a time master is no longer present or cannot be received anymore, the time is no longer synchronized. With the parameter **Failure indication after**, you set the monitoring time. When this monitoring time has elapsed, the device reports a failure of time synchronization (**Time sync. error**). From this moment on, the status **Clock not synchronized** is set in the time stamp of all indications.

This time fault remains until a new time-synchronization telegram is received.

You can find more information in chapter *2.6.8 Device Time*.

1.10 Operating Modes

The behavior of the protocol does not depend on the operating mode of the device. The protocol runs in the **Process** and **Simulation** operating modes of the device. The protocol is not activated in the operating modes **Fallback**, **Boot system**, and **Hardware test**.

2 IEC 61850

2.1 Introduction

2.1.1 Use in SIPROTEC 5 Devices

The IEC 61850 protocol is implemented on an Ethernet module. This Ethernet module can be inserted into module slots E, F, N, and P. In contrast to SIPROTEC 4, several Ethernet modules can be accommodated in one SIPROTEC 5 device. This permits communication between the client and the server for substation automation via the IEC 61850 MMS protocol (MMS – Manufacturing Message Specification) in one module. Cross communication between devices takes place on a second module via GOOSE messages (GOOSE – Generic Object-Oriented Substation Event). As an option, different networks can be used for communication.

NOTE

You can also use a network like for SIPROTEC 4.

The Ethernet modules come with 2 RJ45 connectors or with 2 duplex-LC interfaces for a 1300-nm fiber-optic connection. The physical interface is always duplicated to permit redundant networks. The Ethernet modules each have 1 IP address.

You can find more detailed information on ring structures in chapter *1.3.1 Network Structures* .

You can use DIGSI 5 to set the IEC 61850 protocol for the Ethernet module. DIGSI 5 is also used to make all necessary network settings. Various editors are available for the different protocol services listed in the IEC 61850 Standard. The IEC 61850 object image of a device can be configured flexibly to meet your requirements.

SIPROTEC 5 devices support the Editions 1 and 2 of IEC 61850. To provide complete compatibility with existing Edition 1 devices, you can use DIGSI 5 to switch the IEC 61850 server of the device to the Edition 1 mode. The IEC 61850 server then operates together with Edition 1 clients and exchanges GOOSE messages with Edition 1 devices.

Edition 2 offers the following benefits, among others:

- Correction and clarity in the event of misunderstandings and interoperability problems that are documented in the **Tissue** database.
- Functional extensions in the engineering process, especially when exchanging configuration data between system configuration tools
- Stronger test of SCL files during import
  This test is implemented using another special SCL scheme.
- Extension of test equipment capabilities (data tracking and monitoring functions), device models, character strings
- Extension of the data model in terms of statistics data, power quality, conditional monitoring, hydropower, distributed energy resources, wind power, and communication between substations
- More standardized data classes (logical-node classes, CDC)
  These data classes may not be used in an Edition 1 project in this manner.
- Support of several access points per device:
  Several communication modules are possible with IEC 61850
- Usage of GOOSE later binding, that is, export of instantiated input signals for GOOSE application

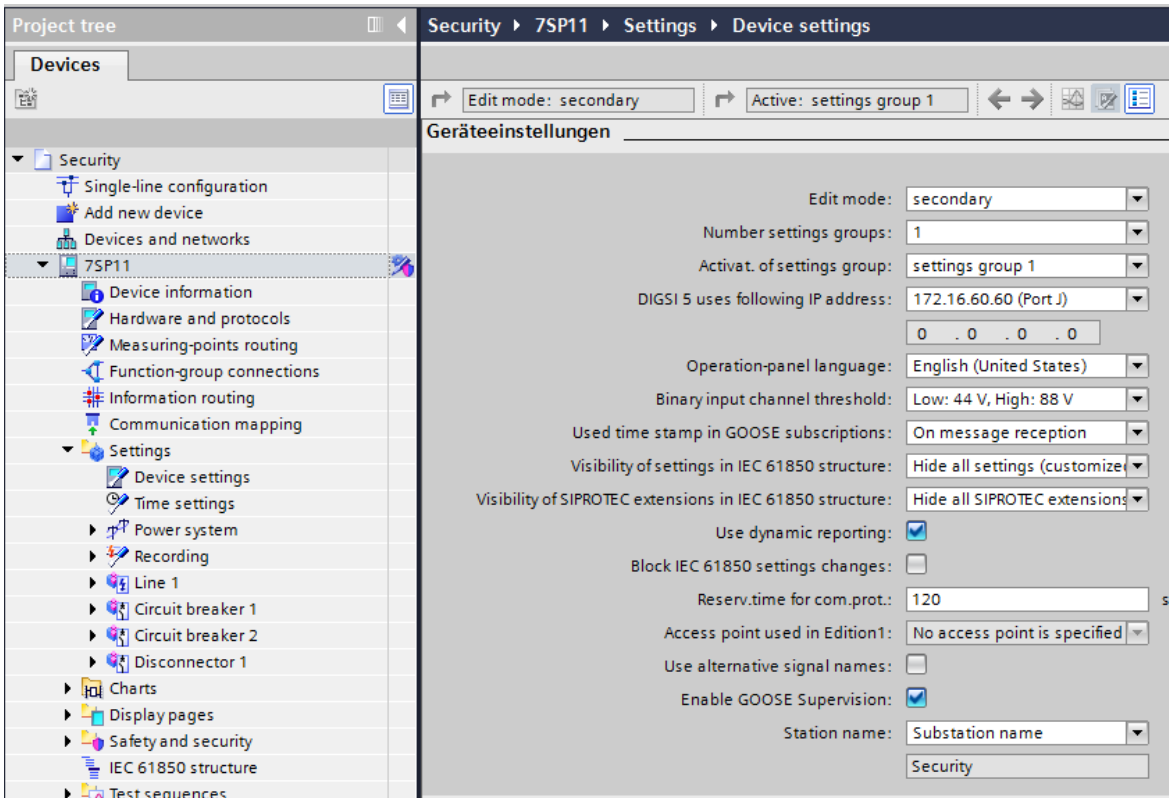
If you would like to use the benefits of Edition 2, the devices can be operated in the Edition 2 mode.

Additional Ethernet-based protocols such as DNP3, IEC 60870-5-104, or Modbus TCP can be activated on the same or on a different Ethernet module.

2.2 Protocol Characteristics in DIGSI 5

2.2.1 Device Setting for IEC 61850

For IEC 61850, you can make the follow settings for IEC 61850 in DIGSI under **Settings > Device settings**:



[sc_IEC61850_device_settings, 4, en_US]

Figure 2-1 Device Settings for IEC 61850

Parameters	Meaning
Used time stamp in GOOSE subscriptions	If a time stamp is sent via GOOSE, the receiver can use the signal without having to provide it with a time stamp when received. The following settings are possible: • On message reception • Provided by GOOSE publisher This parameter is only applicable if IEC 61850 is active. To receive the time stamp, you must activate the data attribute **t** during the parameterization of the GOOSE communication in the IEC 61850 System Configurator. If you do not activate the data attribute, then no time stamp will be received. You can activate individual data attributes or the whole functional constraint. You can find more information on this in the IEC 61850 System Configurator Manual.
Visibility of settings in IEC 61850 structure	With this option, you save storage capacity and time. You have the following setting options: • Show all settings • Show all settings (customized) • Hide all settings • Hide all settings (customized) If settings are to be read or changed via IEC 61850, set this parameter to ***Show all settings***. The data model is then expanded with all settings.
Visibility of SIPROTEC extensions in IEC 61850 structure	With this option, you save storage capacity and time. The following setting options are possible: • Show all SIPROTEC extensions • Show all SIPROTEC extensions (customized) • Hide all SIPROTEC extensions • Hide all SIPROTEC extensions (customized) If the Siemens protection indications are to be exchanged, set this parameter to ***Show all SIPROTEC extensions***. The data model is then expanded with all signals that are not defined in the standard IEC 61850-7-4.
Use dynamic reporting	With this option, you save storage capacity for buffer events in case of an interruption of the communication connection. If static reporting used and no IEC 61850 dynamic reporting is needed, no empty Report Control Blocks remains.
Block IEC 61850 settings changes	When settings are displayed in the IEC 61850 structure, you can read and change these settings via IEC 61850. To block these changes, activate this parameter.
Access point used in Edition 1	With this option, you define the access point required for communication if the IEC 61850 protocol is used in more than one module of the Edition 1 device.
Enable GOOSE Supervision	With this option, you can switch on or off the functionality of the GOOSE connection supervision function.

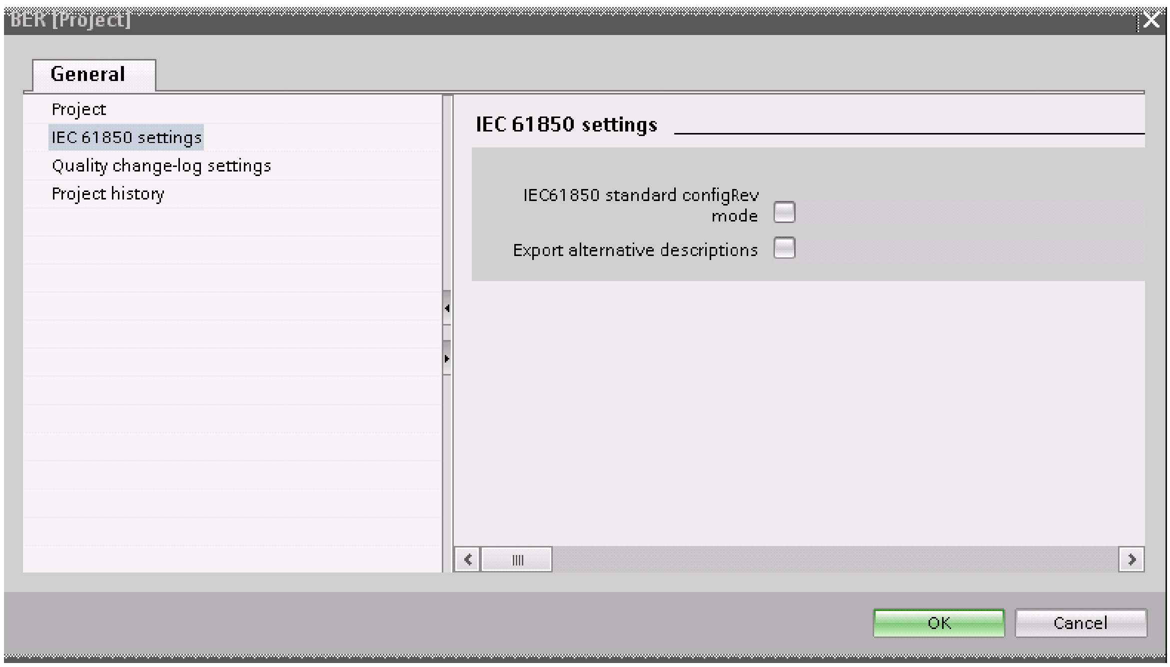
NOTE

The parameters **`Visibility of settings in IEC 61850 structure`** and **`Visibility of SIPROTEC extensions in IEC 61850 structure`** have no influence on:

- User-defined logical nodes
- User-defined signals
- Parameters in logical nodes, which begin with **L**, for example LTMS, LLN0

2.2.2 Project Settings for IEC 61850

For IEC 61850, you can set parameters for the project in DIGSI. To do this, right-click the project in the **Project tree** and select the context menu **Properties**:



[sc_project_settings, 2, en_US]

Figure 2-2 Project Settings for IEC 61850

Parameters	Meaning
IEC61850 standard configRev mode	The current time stamp is used as value for the configRev. If the option **Use standards-compliant mode** is selected, additive changes, for example, adding a data object to a logical node, lead to a change of the configRev.
Export alternative descriptions	Some IEC 61850 Clients support description texts of any language (so-called Unicode, incl. special characters). Other IEC 61850 Clients only support ASCII characters that are used, for example, in the English language. For IEC 61850 Clients with this limitation to ASCII characters, you have the possibility to export SCL files in English. You must activate the parameter in the project properties. To open the project properties, right-click the project and select the context menu **Properties...**. Then select the section **IEC 61850 settings**.

2.2.3 Selecting the IEC 61850 Edition

To begin the project engineering of SIPROTEC 5 systems with IEC 61850, create a project and specify the IEC 61850 edition individually for each device.

NOTE

Edition 1 is the default setting.

You can set the edition for each device individually.

If you have selected Edition 1, you can upgrade to Edition 2. Switching from Edition 2 to Edition 1 is not possible however, because functionality would be lost.

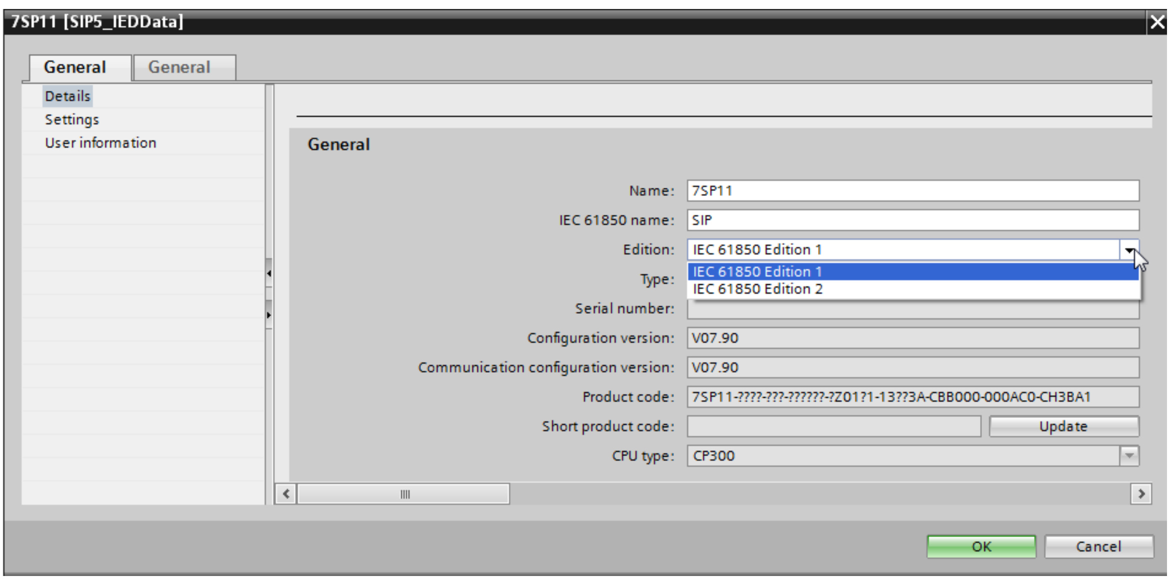
If you export project or device configuration data, they are exported in the established edition.

✧ Create a project in DIGSI.
Additional information can be found in DIGSI Online Help in the **Creating a project** chapter.

✧ Right-click the device in the **Project tree**.

✧ Select the **Properties...** context menu.

✧ Select the **Details** section.
In this section, specify the IEC 61850 Edition in the **Edition** list box.



[sciecedt-150113-01.tif, 3, en_US]

Figure 2-3 Setting the IEC 61850 Edition

Adding an IEC Station

✧ Open the project tree.

✧ Double-click the **IEC 61850 stations** folder in the project tree.

The element **Add new station** is displayed.

✧ Double-click **Add new station**.

The new station (for example, **IEC station 1**) is created.

NOTE

You can create a maximum of 1 IEC station. You cannot cut, copy, or paste IEC stations.

Assigning a Device to an IEC Station

In the **IEC station** Editor, the list of devices that can be assigned to an IEC station is displayed in the **Device name** column under the **Available devices** group.

NOTE

The following devices can be displayed in the **Available devices** group:

- Devices with activated IEC capability.
- Devices that do not yet belong to the IEC station.
- For an IEC station with Edition 1, only devices with Edition 1 are displayed.
- For an IEC station with Edition 2, devices with Edition 1 and Edition 2 are displayed.

✧ Select one or more of the devices displayed under **Available devices**.

✧ With the **>** button, you can assign an individual device.

- or -

✧ With the **>>** button, you can assign all devices to an **IEC station**.

IEC 61850 objects are validated (the compatibility of the device configuration is checked) and the selected device or devices are added and displayed in the **IEC station** Editor in the **Assigned devices** group.

Upgrade of the IEC 61850 Edition of the IEC Station and the Contained Devices

You can upgrade the IEC 61850 Edition of the devices within the IEC station from Edition 1 to Edition 2. A change of the IEC 61850 Edition from Edition 2 to Edition 1 is not possible.

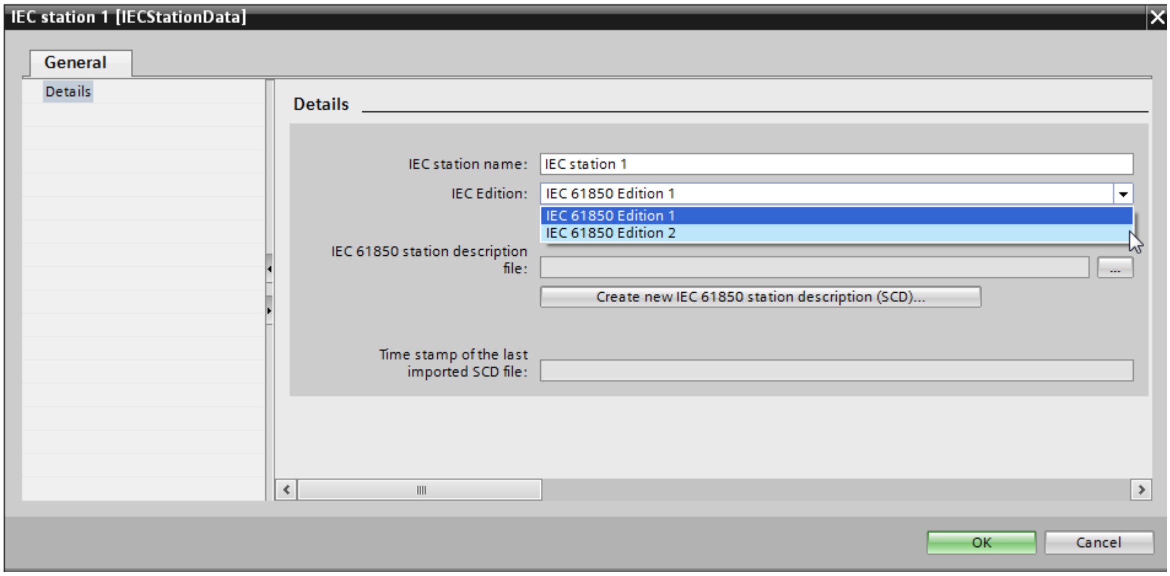
NOTE

In devices that are not yet assigned to the IEC station, the Edition of the devices remains set as in the devices. In this case, only devices that have the same Edition as the IEC station can later be assigned to this IEC station.

To carry out an upgrade of the IEC 61850 Edition, proceed as follows:

✧ In the **IEC 61850 stations** section, click the desired IEC station and select the context menu **Properties**.

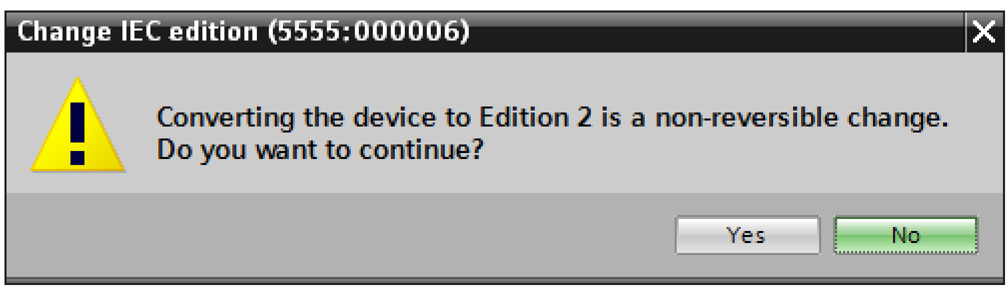
✧ In the dialog, under **IEC Edition**, select **IEC 61850 Edition 2** and click **OK**.



[sc_Update_IEC_Edition_Station, 2, en_US]

Figure 2-4 Change of the IEC 61850 Edition in the IEC Station

A warning indication appears.



[sc_Update_IEC_Edition_Station_Warning, 2, en_US]

Figure 2-5 Warning in Case of a Change of the IEC 61850 Edition in the IEC Station

✧ Click **Yes**. If you click **No** your change is discarded.

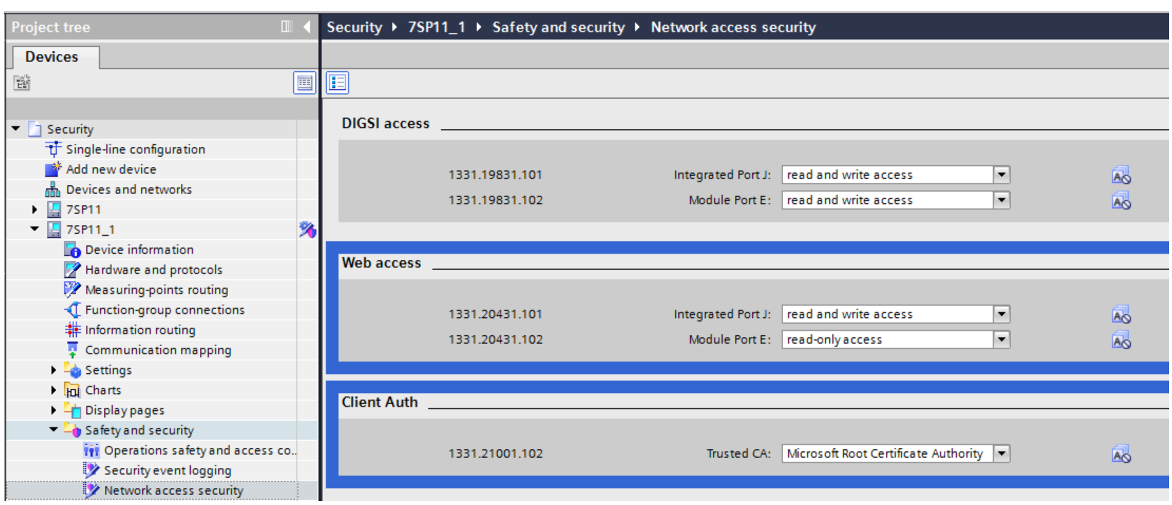
2.2.4 Security Settings

The security settings allow you to restrict the access rights for each Ethernet interface (Port J and Ethernet communication module).

You define the security settings in DIGSI 5 in the project tree under **Safety and security** → **Restricted access**.

You can assign the following access rights:

- Read-only access:
  This interface only allows read access to the device.
  The following services are not available in this state:
  - **Control model**
  - Select
  - SelectWithValue
  - Cancel
  - Operate
  - **GenDataObjectClass model**
  - SetDataValues
  - **Generic substation event model**
  - SetGoCBValues
  - **SETTING-GROUP-CONTROL-BLOCK model**
  - SelectActiveSG
  - SetEditSGValue
- Read and write access:
  This interface allows read and write access to the device.



[sc_restricted_access, 2, en_US]

Figure 2-6 Security Settings in DIGSI 5

2.3 IEC 61850 Structure

2.3.1 Overview

The IEC 61850 structure indicates the hierarchical arrangement of the IEC 61850 elements in an application. This process is also called **Flexible Engineering**.

Application Structure and IEC 61850 Structure

The following table illustrates the assignment between the application structure and the IEC 61850 structure:

Application Structure	IEC 61850 Structure
Communication interface	Access point
Function group FG	Logical device(s) (LD)
Function FN	Logical device(s) (LD)
Function block FB	Logical node(s) LN
Data object DO	Data object DO

An application in SIPROTEC 5 devices is organized into function groups and functions. The functions are arranged within a function group. Functions can consist of one or more function blocks.

The IEC 61850 structure is created by generically converting the application structure:

- The function group and function form the logical device. From a function group **Line1** with the function **87 Line diff.prot.**, the logical device becomes **Ln1_87LineDiffProt** in the IEC 61850 structure.
- The function blocks of the function are mapped as logical nodes. In the example above, these are the logical nodes **I_PDIF1** and **IF_PDIF2**. The prefix and suffix of a logical node are predefined. However, the prefix and suffix can be changed.
- The settings and supervisory indications, for example, group indications, are contained in logical nodes **GAPC1** and **PDIF_PTRC1**.

This IEC 61850 structure corresponds to the SIPROTEC 5 view. The SIPROTEC 5 view is the preset view for the Edition mode of IEC 61850.

Another view is the SIPROTEC 4 similar view. In the SIPROTEC 4 similar view, the IEC 61850 structure is arranged similar as in the SIPROTEC 4 devices. The logical devices **PROT**, **CTRL**, **MEAS**, and **DR** are predefined as fixed values. In the logical devices the function blocks are logical nodes. A generic assignment of function groups and functions to the IEC 61850 structure is no longer available in this view. Logical nodes and the superordinate controlling nodes are, however, displayed in the correct sequence (Logical device, Logical node, Data object and Data attributes).

Options

NOTE

These settings should be done at the beginning of the configuration, directly after activation of the IEC 61850 protocol.

The following tasks can be performed with the IEC 61850 structure editor:

- Switch between the SIPROTEC 5 view and the SIPROTEC 4 similar view.
- Adding logical nodes.
- Renaming logical devices and logical nodes.
- Adding signals.
- Transmitting and deleting structure elements.
- Showing or hiding the logical devices, logical nodes, and signals on the IEC 61850 interface.

Applications

The following describes 3 example applications for working with the IEC 61850 structure editor:

- To avoid a high flexible engineering effort when using a specification with few Logical Devices, you can switch from the SIPROTEC 5 structure to the SIPROTEC 4 structure using the IEC 61850 structure editor.
- If you want to adapt the structure and designations of the elements and devices regardless of the manufacturer, this can be done using the IEC 61850 structure editor. You can, for example, name a device according to its location or intended use. In the process, and also for all other elements, you can adapt the name to comply with the terminology used within your company. This type of structural adaptation is also called *2.3.2 Functional Naming and Flexible Product Naming*.
- If you are familiar with IEC 61850, you can make allowed changes to the functionality in the IEC 61850 structure editor. Instead of adding a function to a single-line configuration, you can add a user-defined logical node or user-defined signals directly to the IEC 61850 structure.

Advantages

The variability of the IEC 61850 structure provides advantages including the following:

- Exchangeability of devices at communication level
- Typification of the device configuration independent of the device manufacturer
- Reduction of lifecycle engineering costs
- Longevity of the configuration data generated

2.3.2 Functional Naming and Flexible Product Naming

The engineering concept **Functional naming and flexible product naming** allows the device replacements at the communication level. The configuration of the device communication interfaces ensures, that scope of information to be transferred and the naming between devices of different versions and manufacturers appears the same.

Definitions

- **Functional naming**
  A data model with functional structure based on SCL is manufacturer-independent and standardized. In IEC 61850, this function-oriented naming is called **Functional Naming** (function-related addressing). A system model according to IEC 61850 is formed by the modeling of the primary system structure with the following elements:
  - Logical nodes for the equipment
  - Distributed functions
  - Type classes of the logical nodes, data objects, and attributes
- **Flexible product naming**
  The data models of the devices reflect the implemented functions of bay and protection devices of the individual manufacturers. The product naming describes the actual configuration of the IEC 61850 naming, that means the object tree structure of the IEC 61850 data model. According to this naming, telegrams are formed and sent via the communication interface configured for IEC 61850.
  It means that IEC 61850 address is vendor-dependent:
  - Logical Devices
  - Function allocation between IEDs

Product Naming

With flexible product naming, you can change the object tree structure. You have the following possibilities:

- **Flexibility of the implemented device data models**
  You can define the structures of logical devices by adding user-defined logical devices.
- **Adding logical nodes**
  You can add user-defined logical nodes and completely use all data classes in IEC 61850.
- **Custom naming**
  The attribute **LDname** is used instead of the combination of the attributes **IEDname** and **LDinst** as part of the address in a GOOSE or report communication only in Edition 2 and the standard solution for functional naming.
  You can define the IED name, the instance name of the logical device, the prefix, and the suffix.

2.3.3 Adjusting a Data Model

In order to adjust a data model of the device to a desired interface configuration, you may implement the following modifications:

- You can rename the existing Logical Devices, for example, CB1 to QA1.
- You can rename IEDnames, for example SIP to E1Q4FP1.
- You can add LDs by creating function groups.
- You can remove existing LDs from the visible data model.
- You can add an ldName (Logical Device name). This LDname will then be used in the communication address instead of the IEDname (device name) and the Logical Instance ID (LDinst).

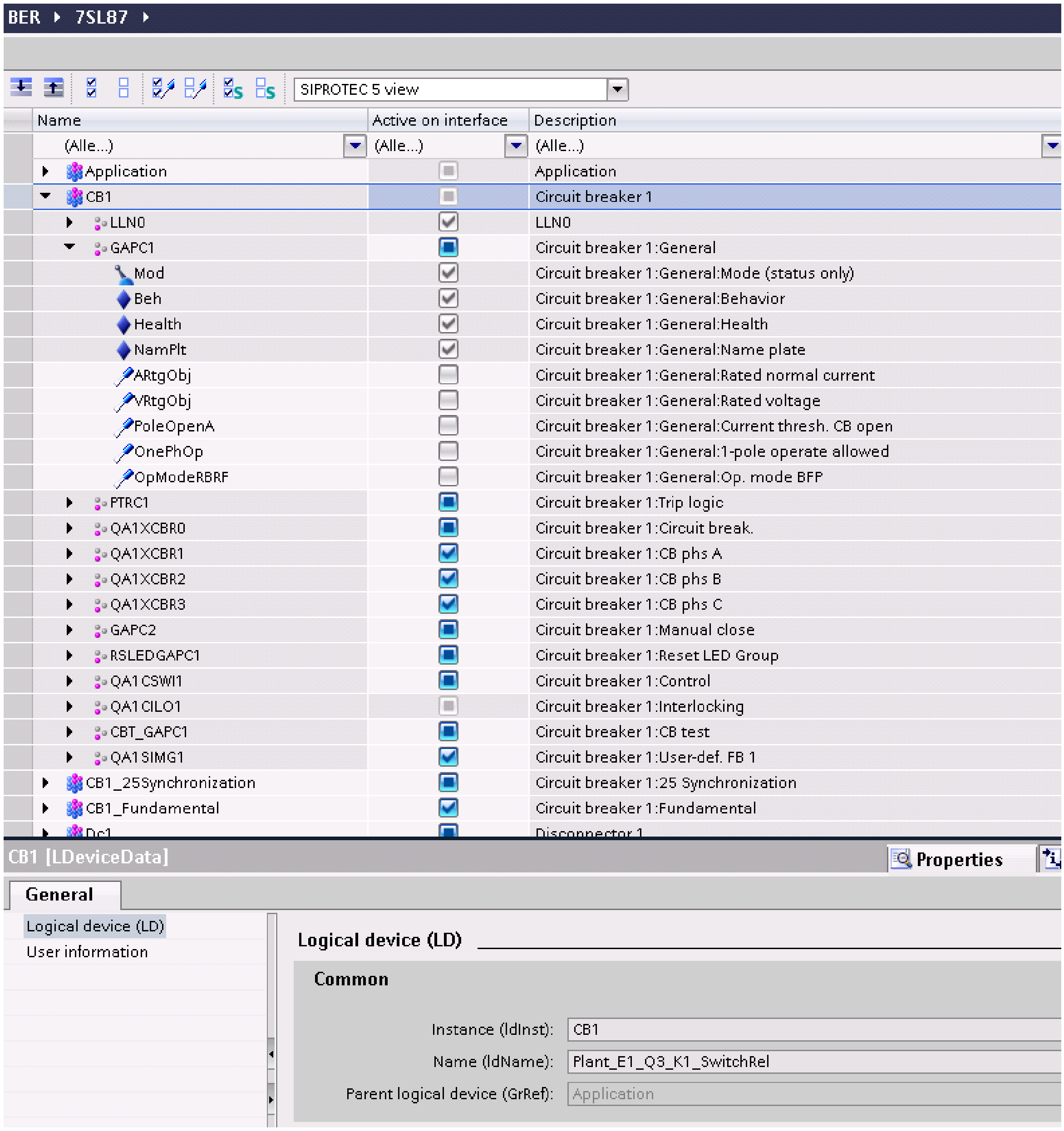
NOTE

You may not use the LDname twice within the entire Ethernet subnetwork. It exists only with Edition 2 of the IEC 61850 protocol.

- You can configure an LN Prefix and the LN Instance number.
- You can create new Logical Nodes, your LN Prefixes, and your LN Instance number.
  A newly added logical node is assigned the class **USER**.
- You can create data objects (DO).
- You can add data objects to new LNs.
- You can expand the data volume of a LN by one or several DOs.
- You can move one LN from one LD into another LD.
- You can remove existing LNs from the visible data model.
- You can remove existing DOs from the visible data model.
- You can adjust the namespace of LN and DO in order to clone new standard data models.

NOTE

The same data model is available via all communications models with IEC 61850.



[sciecstr-140113-02, 1, en_US]

Figure 2-7 IEC 61850 Structure

Examples of How to Adjust a Data Model

In a function-related system specification according to IEC 61346, you have assigned a group of LNs with DOs to an equipment circuit breaker.

These data objects are to be transmitted during the communication with the following function-related addresses:

- Switchgear (Station): Sample system
- Voltage level: E1
- Bay name: Q3
- Equipment circuit breakers: QA1
- Phase (Subequipment): A

- Logical Nodes:
  - XCBR
  - CSWI
  - CILO
  - RSYN

In order to illustrate this address structure in a product-related address scheme, configure a logical device with the following LDname:

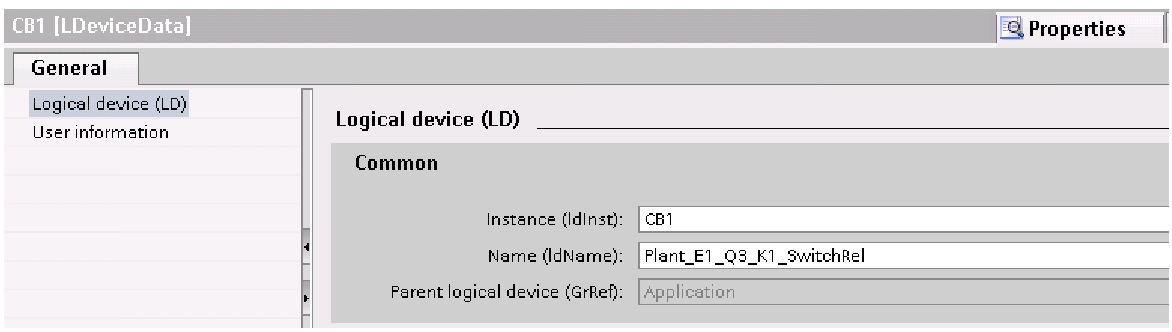
Sample system_E1_Q3_K1_SwitchRel

K1 means electronic control unit 1 and **SwitchRel-** refers to information related to the switching device.

LN instances are set with the prefix **QA1A**.

Implement the following changes in the IEC 61850 structure:

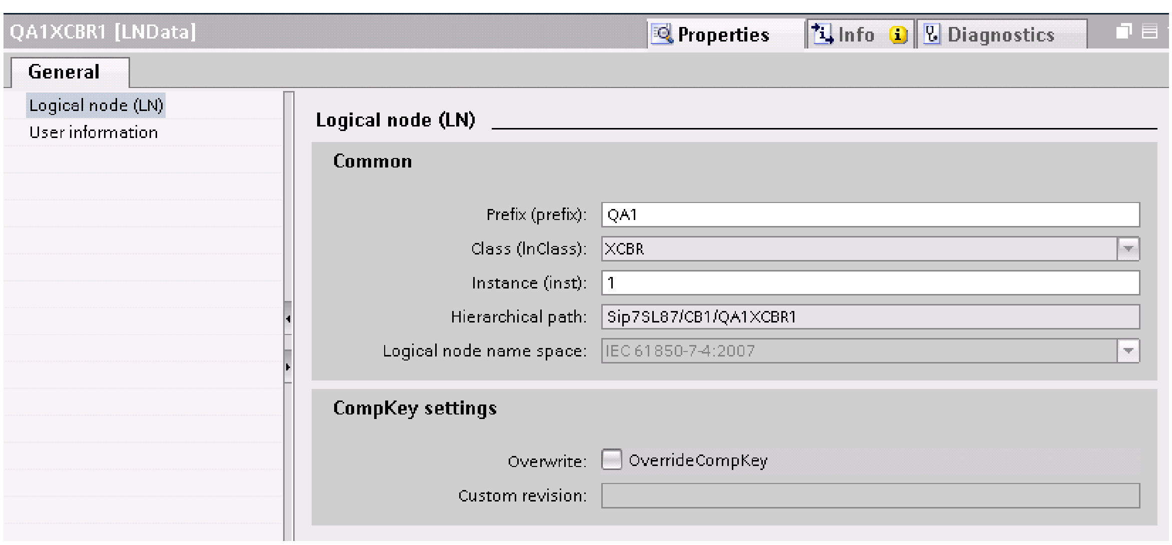
✧ Enter **Sample system_E1_Q3_K1_SwitchRel** into the **Name(ldName)** field.



[sciecst2-150113-02, 1, en_US]

Figure 2-8 Changing the LD Name

✧ Enter **QA1** into the field **prefix** LN XCBR0, XCBR1, XCBR2, XCBR3, CSWI0, CILO0.

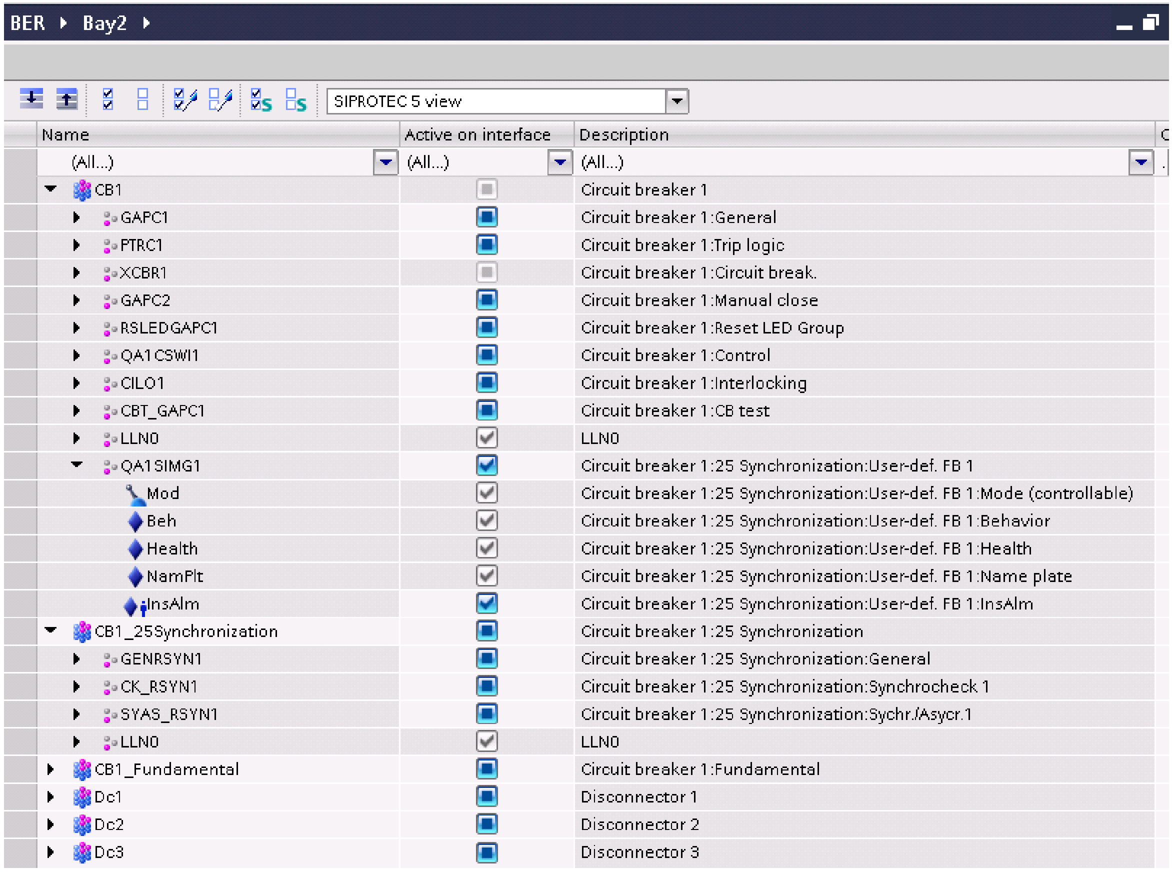


[sciecst3-150113-02, 1, en_US]

Figure 2-9 Entering the Prefix

✧ Move the LN from the LD CB1_Synchronization into LD CB1.

If data objects are missing from the standard content of the IED, you can simply copy the user-defined function (LN) and a user-defined signal (DO) from the library into the respective device.

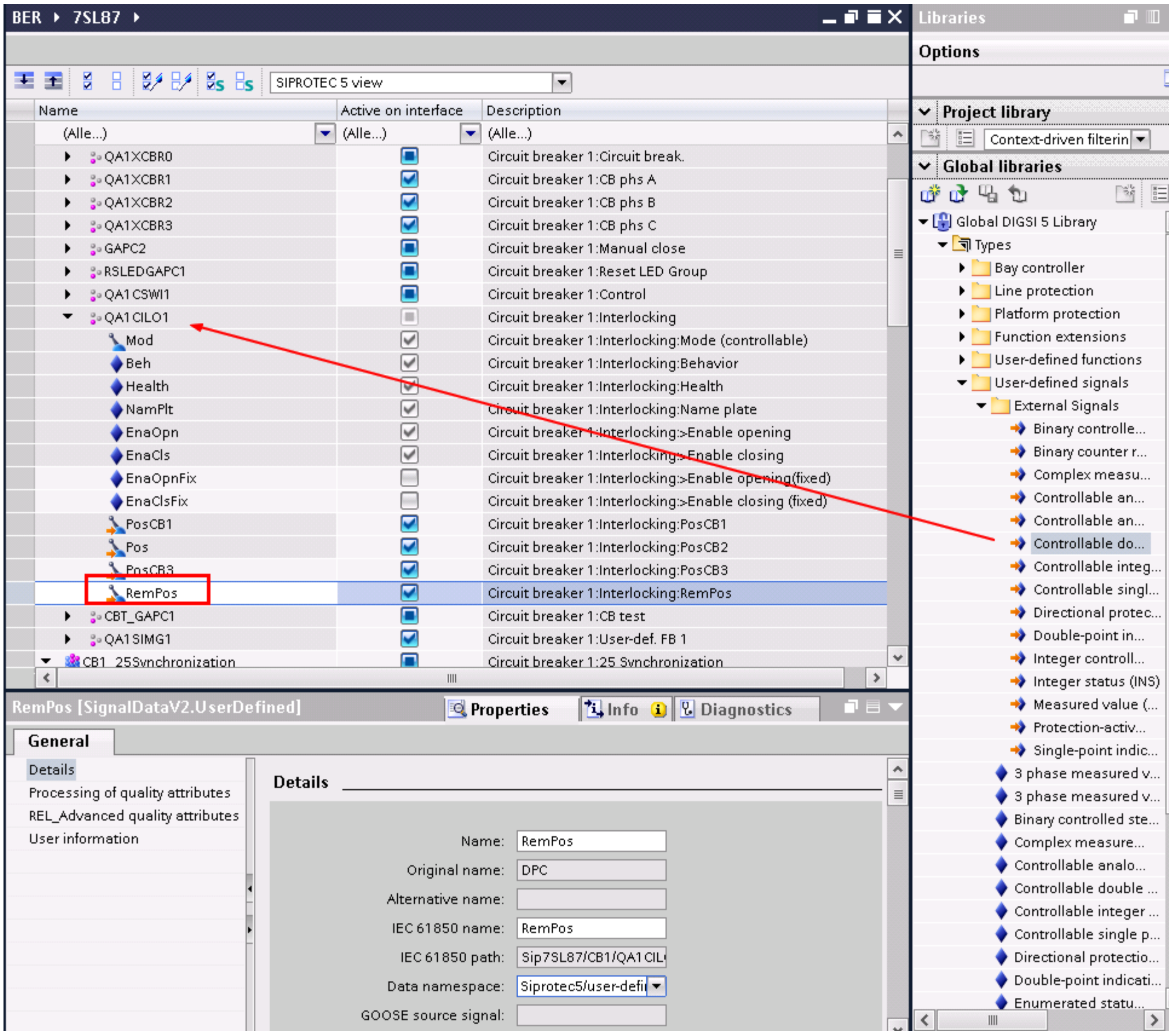


[sccoplns-140113-02, 1, en_US]

Figure 2-10 Adding a User-Defined Object to LN

✧ Create an input signal for GOOSE Later Binding.

If you need data objects for GOOSE Later Binding, you can copy signals from the **External Signals** folder to the corresponding logical device via Drag & Drop.



[sccopIns-140717, 1, en_US]

Figure 2-11 Creating an Input Signal for GOOSE Later Binding

2.3.4 Opening and Adjusting the IEC 61850 Structure Editor

A separate IEC 61850 structure editor is available for each offline configuration within a project.

Opening the IEC 61850 Structure Editor

In the project, open the folder of the affected offline configuration and double-click **IEC 61850 structure**. The IEC 61850 structure editor is displayed in the working area.

2.4 Exporting

2.4.1 Export Formats in DIGSI 5

Export files permit interoperable data exchange of IEC 61850 data between the configuration tools of various manufacturers. They can be used for documentation purposes or in other IEC 61850 configurators.

Export of IEC 61850-compliant SCL files is possible with DIGSI 5.

The following export formats are available at the device level to export device-specific IEC 61850 data:

Data Format	Meaning	Export Source		Import Target	
TEA-X	Data exchange format containing information of single or multiple devices (XML-based)	Device	Project	Device	Project
DEX5	Device archive with complete information about an individual SIPROTEC 5 device	Device	—	—	Project
DSP5	Display pages for an individual SIPROTEC 5 device	Device	—	Device	—
RIO	Protection settings for an individual SIPROTEC 5 device for use in test equipment	Device	—	—	—
ELCAD	Topology information from CAD diagrams	—	—	—	Project
SEQ5	Test sequences for an individual SIPROTEC 5 device	Device	—	Device	—
ST	DIGSI 4 function charts	—	—	Device	—
ICD	IED Capability Description	Device	—	Device	—
IID	Instantiated IED Description	Device	—	—	—
SCD	Substation Configuration Description	—	—	—	IEC Station
SSD	System-Specification Description	—	—	—	Project
MICS	Model Implementation Conformance Statement	Device	—	—	—
DIGT103	IEC 60870-5-103 protocol settings for SICAM PAS	Device	—	—	—
DIGT104	IEC 60870-5-104 protocol settings for SICAM PAS	Device	—	—	—
DIGMOD	Modbus TCP protocol settings for SICAM PAS	Device	—	—	—
DIGDNP	DNP3 protocol settings for SICAM PAS	Device	—	—	—
SIM	Simulation data format for single/ multiple devices	Device	Project	—	—
UAT	User-defined application template	Device	—	Device	Project Group folder

MICS

This file is the XML description of the device data model.

With this export format 3 files are exported: 1 XML description and 2 formatting files.

Both formatting files must be in the same directory as the XML file so that the XML files can be displayed correctly in the browser. If this is not the case, the XML file is displayed in an unformatted way.

If you have selected an unchanged application template, for example, **DIFF/DIS Overhead Line, 1.5 CB**, the MICS file of the application template corresponds to the functions preconfigured by Siemens. If you have added functions and data objects in DIGSI 5, these values are imported 1:1 into the MICS file.

NOTE

Exporting data with the MICS format is only available if you have parameterized an Ethernet interface (integrated Ethernet interface or an Ethernet communication module) with the IEC 61850 protocol.

SCL files are exported according to Edition 1 (SCL Scheme V1.7) or Edition 2 (SCL Scheme 2007 Revision B) of the IEC 61850 protocol. The edition is set in the device properties.

You can find more information on the export of CID, SCD, and SED files in the IEC 61850 System Configurator manual.

2.4.2 Exporting IEC 61850 Description Files

IEC 61850 description files include, for example, ICD and IID. They include descriptions of the performance properties of an IED.

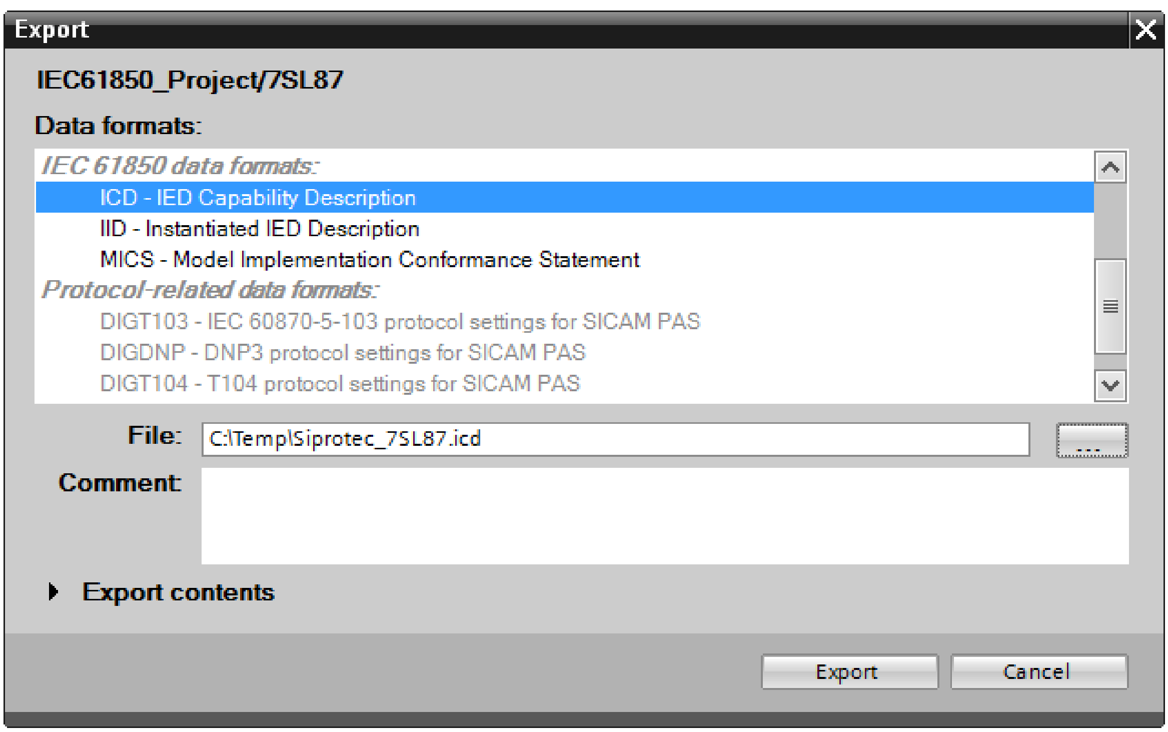
✧ In order to export IEC 61850 description files, highlight the device in the project tree.

✧ Select the **Export** function from the **Project** menu.

- or -

✧ In the context menu, select the **Export** function.

The export dialog appears. You can select from among various data formats.



[sc_Export_IEC61850, 1, en_US]

Figure 2-12 Export Content

Exporting MICS

✧ Select the **MICS – Model Implementation Conformance Statement** data format.

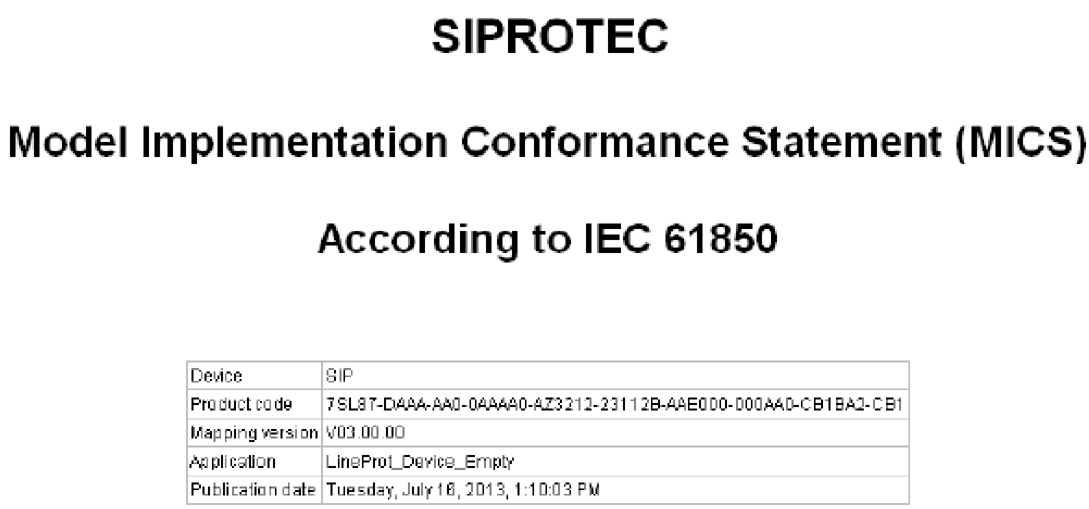
The MICS file is an XML file. 2 other files are exported. These files enable formatting the MICS XML file for visualization and for printing with a browser or for using an XML editor. Siemens recommends exporting these files into a separate directory, for example, c:/Temp/MICS.

✧ Open the Internet Explorer, click **File** → **Open** and navigate to the directory in which you have stored the MICS file.

✧ Select the **All Files** file type in order to display all file types, and click **Open**.

The homepage of the MICS file is displayed in the browser.

The subsequent pages show all IEC 61850 logical devices and logical nodes of the device. From there, you can navigate via hyperlinks to the further details. You can navigate through the entire IEC 61850 data structure of the device and find all the definitions of data objects in the chapters of the data types. The configured GOOSE connections are also displayed. You can print out the HTML pages as a PDF document, for example, but the browser view is more comfortable.



SIPROTEC

Model Implementation Conformance Statement (MICS)

According to IEC 61850

Device	SIP
Product code	7SL87-DAAA-AA0-0AAAA0-AZ3212-23112B-AAE000-000AA0-CB1BA2-CB1
Mapping version	V03.00.00
Application	LineProt_Device_Empty
Publication date	Tuesday, July 16, 2013, 1:10:03 PM

[sc_MICS, 1, --_--]

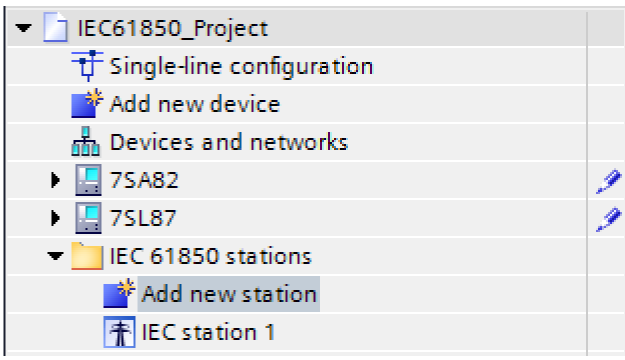
Figure 2-13 Homepage of the MICS File

2.5 IEC 61850 System Configurator

2.5.1 Integration with the IEC 61850 System Configurator

✧ Create a new IEC 61850 station by clicking **Add New Station** under **IEC 61850 Stations** in the **Project tree**.

A new IEC 61850 station **IEC station 1** is created.



[sc_new IEC station, 1, en_US]

✧ Right-click the IEC 61850 station **IEC station 1** and select the IEC Edition in the properties.

✧ In the properties, specify the path for the IEC 61850 Substation Configuration Description file.

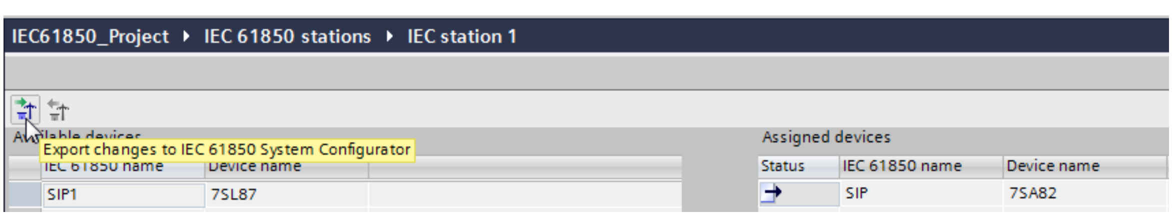
✧ Double-click the IEC 61850 station **IEC station 1** and assign the devices. To do this, select the device in the **Available devices** section and click the **>>** button.

IEC 61850 objects are validated (the compatibility of the device configuration is checked) and the selected device or devices are added and displayed in the **IEC station** Editor in the **Assigned devices** group.

NOTE

If you attempt to assign a device that has an IEC 61850 Edition other than the Edition of the IEC station, you will receive a warning. If the device has the IEC 61850 Edition 1, but the station has IEC 61850 Edition 2, the IEC 61850 Edition of the device is irrevocably switched over. A change from IEC 61850 Edition 2 to IEC 61850 Edition 1 is not possible.

✧ Export the device changes to the IEC 61850 System Configurator.



[sc_export to IEC Syscon, 1, en_US]

✧ Changed devices are marked in the **Assigned devices** section with an arrow symbol.
All IDs are exported automatically.

2.5.2 IEC 61850 System Configurator

You can find more information on the following topics in the IEC 61850-System Configurator manual:

- GOOSE applications:
  - GOOSE communication
  - Creating a GOOSE application
- Report applications:
  - Creating a report application
  - Configuring the dataset
  - Report control blocks
- Export of SCD/SED files
- VLAN priority for fast GOOSE tripping (see also chapter *2.6.6 VLAN Priority for Fast GOOSE Tripping*)

2.5.3 Importing an SCD into DIGSI

✧ Double-click the IEC 61850 station **IEC station 1**.

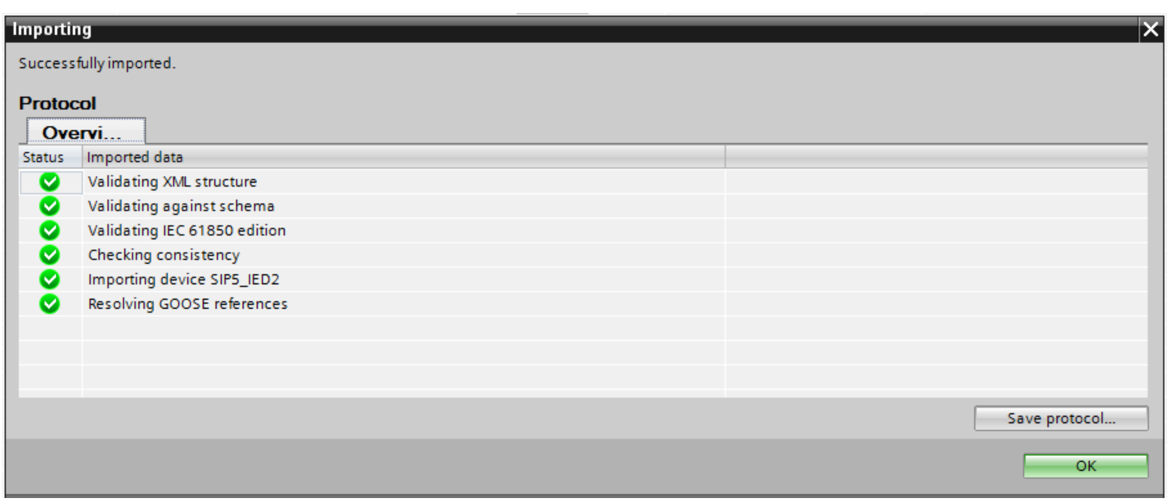
✧ Click the icon .

- or -

✧ Right-click the IEC 61850 station **IEC station 1**.

✧ In the context menu, select **Import changes from IEC 61850 System Configurator**.

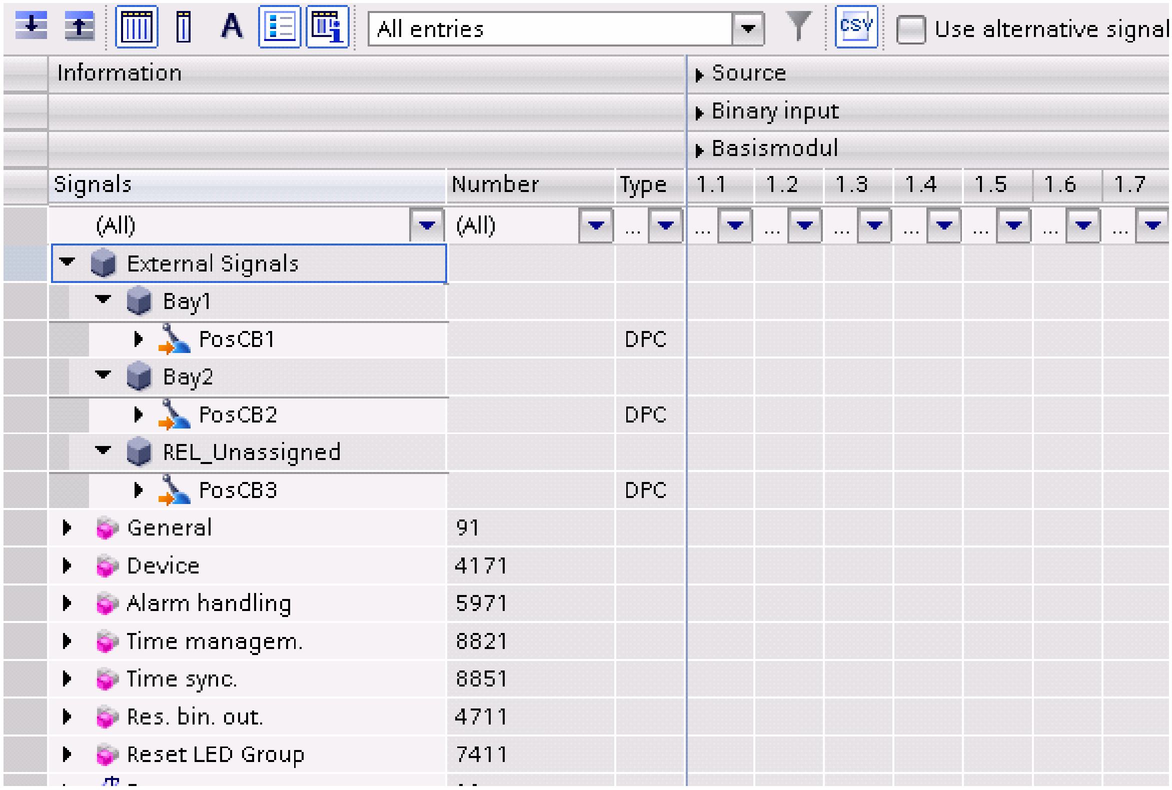
The **Importing** dialog appears. The report window only displays devices that have changed. Click **OK** to confirm the dialog.



[sc_IEC61850_Station_Import, 1, en_US]

Figure 2-14 Import from the IEC 61850 System Configurator

The **Import device...** entries show that the corresponding device has changed.
The GOOSE indications are created automatically in an **External Signals** node in the **Information routing**.



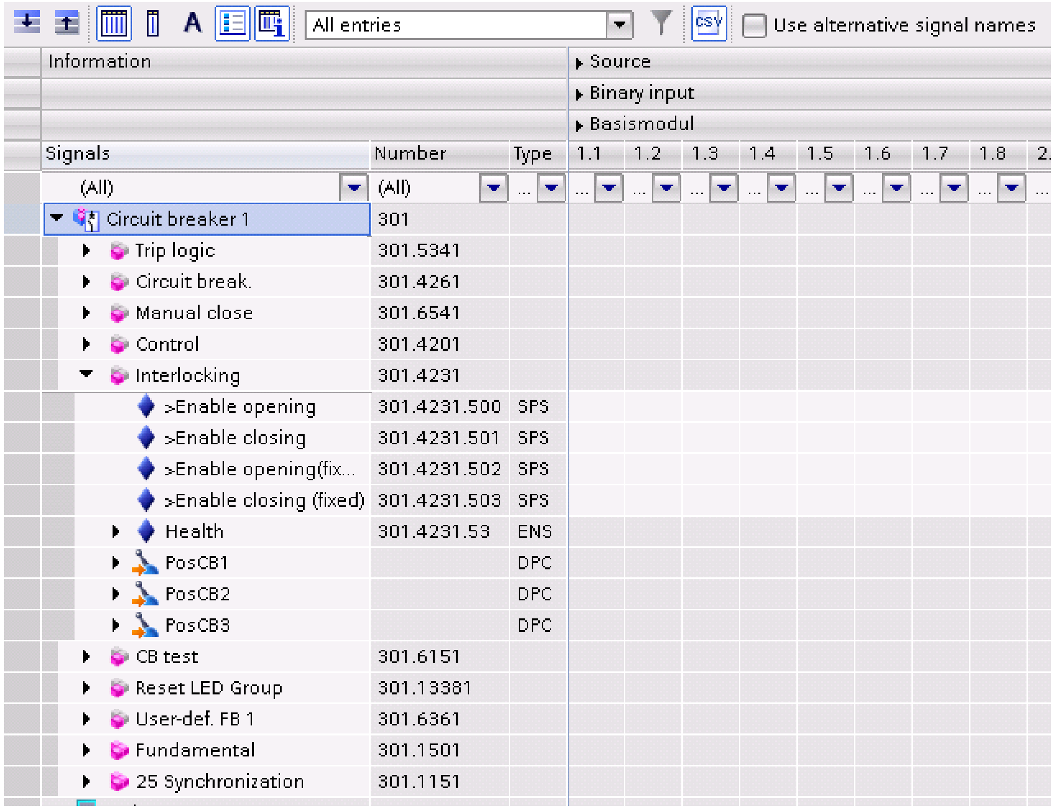
[sc_GOOSE_signal_after_SCD_import, 2, en_US]

Figure 2-15 GOOSE Indication after Import

NOTE

Consider that signals that are not connected are displayed under *Unassigned*. If you do not want to use these signals, you must delete them actively. Connected signals are sorted and displayed under the source device.

You can find the same GOOSE indication under the logical node you have selected in the System Configurator for the target of the related GOOSE indication, for example, in the **Interlocking** logical node:



[sc_GOOSE_signal_logical_node, 2, en_US]

Figure 2-16 GOOSE Indication in the Logical Node

2.6 Protocol Properties and Implementation

2.6.1 IEC 61850 Structure of a SIPROTEC 5 Device

There are 2 possible structures:

- SIPROTEC 5 view
- SIPROTEC 4 similar view

NOTE

Select the basic structure at the beginning. If you subsequently change the structure, all report and GOOSE configurations are lost.

SIPROTEC 5 View

A SIPROTEC 5 device is organized into function groups and functions. The protection functions are located in a function group, for example, Line. Breaker, for instance, is an additional function group that contains breaker-related functions.

The SIPROTEC 5 view contains the following components:

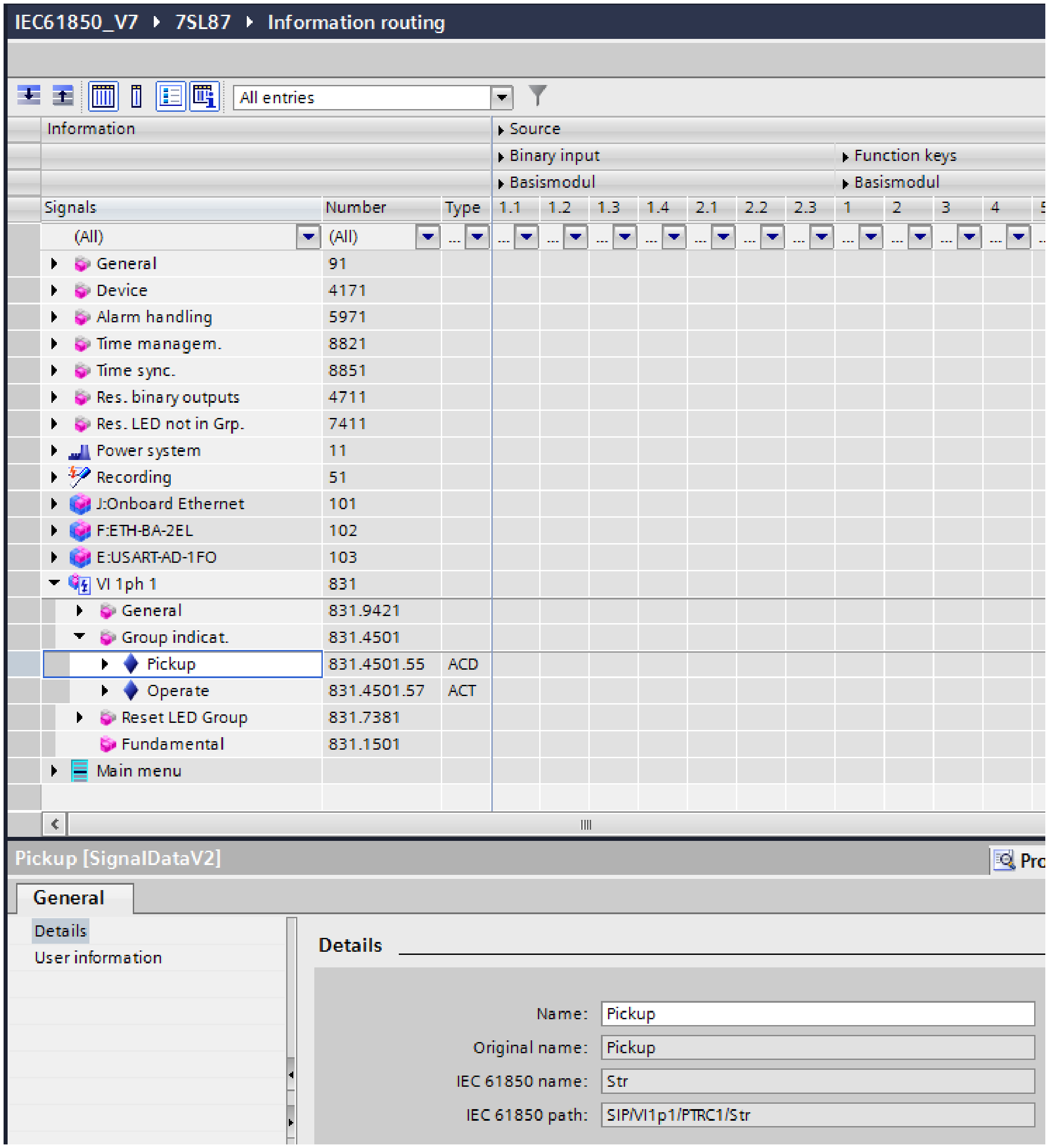
- Protection functions/functions

  The protection functions/functions consist of one or several tripping stages and a superordinate stage that controls the stages below it. In DIGSI 5, this view corresponds to, for example, information routing. A generic conversion into the IEC 61850 protocol structure takes place.

- Logical device

  The function group and function form the logical device. The following figure shows this, using the differential-protection function as an example. Ln1 Is the function group Line1 that contains the **87 Line diff.prot.** protection function and additional protection functions.

  The text of the logical device **Ln1_87LineDiffProt** consists of an abbreviation for the function group Line1 and the protection function. In the column at the right in the following figure, you can see the corresponding DIGSI 5 text that is used, for instance, in information routing. In information routing, the IEC 61850 descriptions and the DIGSI 5 texts will always be displayed in table format. This will enable you to always find the IEC 61850 object assigned to the DIGSI 5 objects.



[sc_SIP5 view, 2, en_US]

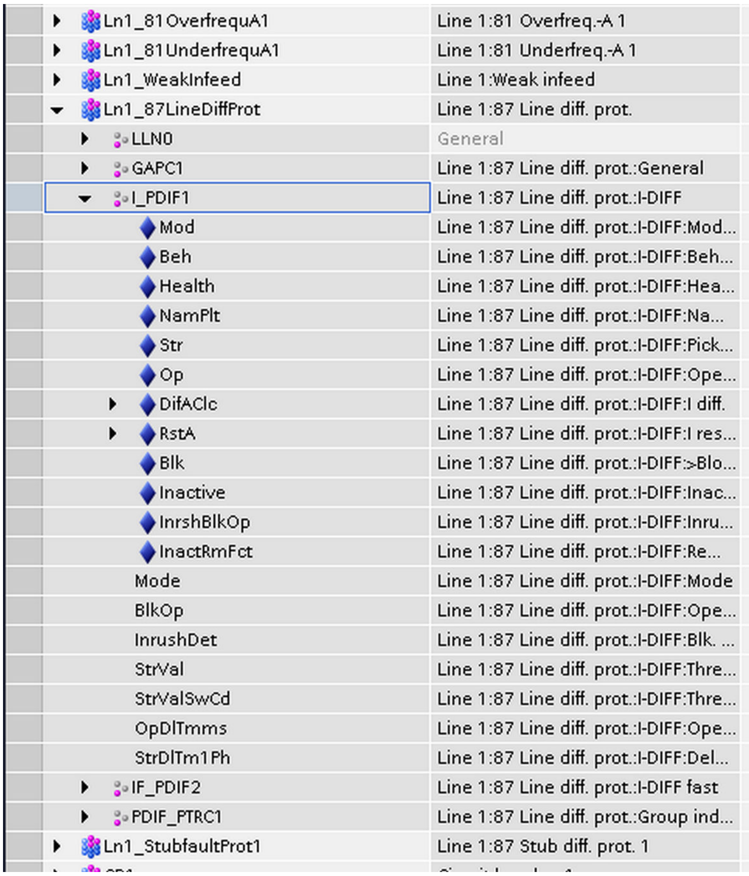
Figure 2-17 Information Routing in DIGSI

- Logical nodes

  The differential-protection stages appear as logical nodes (called PDIF per the Standard). These are the logical nodes **I_PDIF1** and **IF_PDIF2**. The prefix and suffix of the logical node are specified by Siemens. However, you can change them at any time.

  The logical nodes **GAPC1** and **PDIF_PTRC1** contain parameters that control the tripping stages as well as superordinate indications, for example, group indications. If you open up the logical nodes, you will see the information objects and settings contained therein.

This IEC 61850 structure is valid if you select the **SIPROTEC 5 view** structure in the IEC 61850 structure editor.



[sciec5st-280113-01.tif, 1, en_US]

Figure 2-18 IEC 61850 Structure of a SIPROTEC 5 Device (SIPROTEC 5 View), Using the First Tripping Stage of Differential Protection as an Example

The SIPROTEC 5 view offers the following advantages:

- Uniform display with information routing
- Improved granularity of the functions for monitoring (**Health** indication) or for the test (mod).

SIPROTEC 4 Similar View

The **SIPROTEC 4 similar view** is an additional IEC 61850 structure. It is preferred in Edition 1 because the LD texts are shorter.

The logical devices are given with the following designations, for instance:

- PROT
- CTRL
- MEAS
- DR

NOTE

If you switch to the SIPROTEC 4 similar view, all user-defined function groups are moved into the logical device CTRL.

If you add new function groups to the information routing, new logical devices are created. If you switch to the SIPROTEC 5 view and then switch back to the SIPROTEC 4 similar view, all user-defined function groups are moved back into the logical device CTRL.

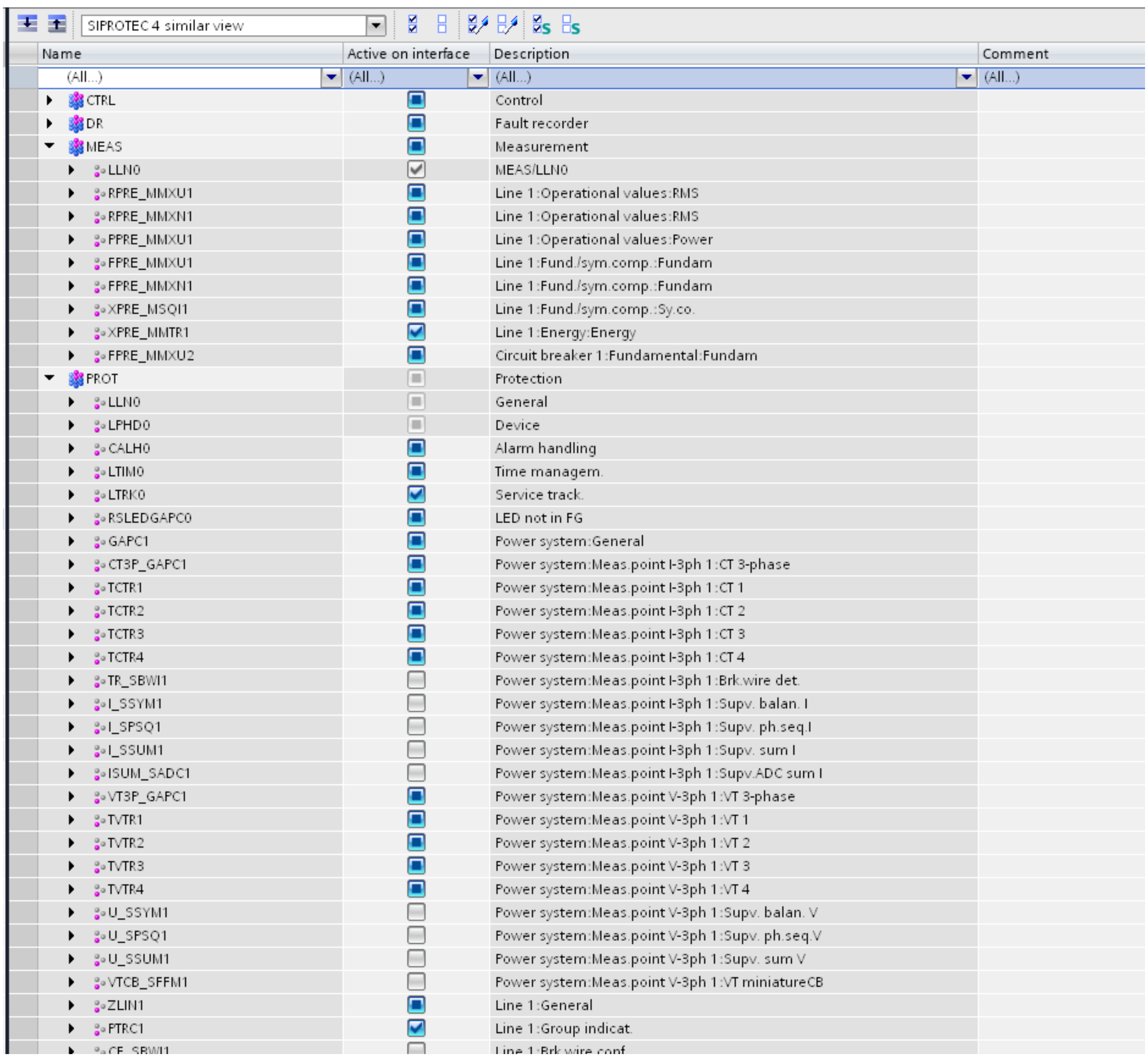
NOTE

The logical device EXT (Extended) is not available as default. However, you may create your own logical devices by way of user-defined function groups in the Information routing.

The logical devices exhibit a great deal of similarity to the LD structure of SIPROTEC 4 devices.

The logical devices contain the tripping stages, for example, protection function stages, and the superordinate stages that control them as logical nodes.

A generic assignment of function groups and functions to the IEC 61850 structure is no longer available in this view. Logical nodes and the superordinate controlling nodes are, however, displayed in the correct sequence. In addition, the DIGSI 5 text for an object or a parameter is always visible. You can also change this view in the Structure Editor at any time.



SIPROTEC 4 similar view

Name	Active on interface	Description	Comment
(All...)	(All...)	(All...)	(All...)
CTRL		Control	
DR		Fault recorder	
MEAS		Measurement	
LLN0		MEAS/LLN0	
RPRE_MMXU1		Line 1:Operational values:RMS	
RPRE_MMXN1		Line 1:Operational values:RMS	
PPRE_MMXU1		Line 1:Operational values:Power	
FPRE_MMXU1		Line 1:Fund./sym.comp.:Fundam.	
FPRE_MMXN1		Line 1:Fund./sym.comp.:Fundam.	
XPRE_MSQI1		Line 1:Fund./sym.comp.:Sy.co.	
XPRE_MMTR1		Line 1:Energy:Energy	
FPRE_MMXU2		Circuit breaker 1:Fundamental:Fundam.	
PROT		Protection	
LLN0		General	
LPHD0		Device	
CALH0		Alarm handling	
LTIM0		Time managem.	
LTRK0		Service track.	
RSLEDGAPC0		LED not in FG	
GAPC1		Power system:General	
CT3P_GAPC1		Power system:Meas.point I-3ph 1:CT 3-phase	
TCTR1		Power system:Meas.point I-3ph 1:CT 1	
TCTR2		Power system:Meas.point I-3ph 1:CT 2	
TCTR3		Power system:Meas.point I-3ph 1:CT 3	
TCTR4		Power system:Meas.point I-3ph 1:CT 4	
TR_SBWI1		Power system:Meas.point I-3ph 1:Brk.wire det.	
I_SSYM1		Power system:Meas.point I-3ph 1:Supv. balan. I	
I_SPSQ1		Power system:Meas.point I-3ph 1:Supv. ph.seq.I	
I_SSUM1		Power system:Meas.point I-3ph 1:Supv. sum I	
ISUM_SADC1		Power system:Meas.point I-3ph 1:Supv.ADC sum I	
VT3P_GAPC1		Power system:Meas.point V-3ph 1:VT 3-phase	
TVTR1		Power system:Meas.point V-3ph 1:VT 1	
TVTR2		Power system:Meas.point V-3ph 1:VT 2	
TVTR3		Power system:Meas.point V-3ph 1:VT 3	
TVTR4		Power system:Meas.point V-3ph 1:VT 4	
U_SSYM1		Power system:Meas.point V-3ph 1:Supv. balan. V	
U_SPSQ1		Power system:Meas.point V-3ph 1:Supv. ph.seq.V	
U_SSUM1		Power system:Meas.point V-3ph 1:Supv. sum V	
VTCB_SFFM1		Power system:Meas.point V-3ph 1:VT miniatureCB	
ZLIN1		Line 1:General	
PTRC1		Line 1:Group indicat.	
CF_SBWI1		Line 1:Brk.wire conf.	

[sciec4st-280113-01.tif, 2, en_US]

Figure 2-19 IEC 61850 Structure of a SIPROTEC 5 Device (SIPROTEC 4 Similar View)

The SIPROTEC 4 view offers the following advantage:

- SIPROTEC 4 devices can be modeled faster in SIPROTEC 5 flexible engineering.

NOTE

If you wish to change the IEC 61850 structure, you can begin with the SIPROTEC 5 view or the SIPROTEC 4 similar view and incorporate your changes via the IEC 61850 structure editor.

2.6.2 IEC 61850 Services

You can find details in PICS (Protocol Implementation Conformance Statement).

SIPROTEC 5 devices support the following IEC 61850 services:

GOOSE Messages

Datasets are created in the device by GOOSE applications. This takes place in the logical node **LLN0** of a logical device. You can specify where these datasets are created.

The first object configured in a GOOSE message from a logical device creates a dataset for a GOOSE message in LLN0. Further objects are configured in this dataset and added to this dataset, even if they originated in other LDs. Alternatively, if you wish to send objects in different datasets, you can also create a new GOOSE application and thus a new dataset.

NOTE

Sending objects in different datasets generates unnecessary data traffic, since each dataset created is transmitted via its own GOOSE message.

The dataset is sent as a GOOSE message and distributed to all network participants in the form of multicast telegrams. If participants wish to receive specific objects in a GOOSE message, the user can select these objects via the system configuration and receive them later online.

GOOSE messages are transmitted with high priority and repeated at an interval of a few milliseconds in the event of a spontaneous change of the data object. You set the repetition time in the IEC 61850 System Configurator.

You can find more information on GOOSE parameterization and on creating a GOOSE application in the System Configurator manual.

Control Commands

You can control an object in a device with control commands. By using the control model **Select Before Operate**, you can actuate a circuit breaker reliably, for instance. Commands without feedback can be executed in the device as well, for example, resetting the LEDs (LED Reset) by the client.

You can find more information on the configuration and control of switching objects in chapter *2.6.5 Control via IEC 61850*.

Settings can be changed by using the Setting Services function.

You can find more information in chapter *10.1.15.1 IEC 61850 Browser*.

2.6.3 Reporting

2.6.3.1 What Is a Report?

When using IEC 61850 in switchgear as well, you must test communication between protection devices and the substation automation technology just as you do with the previous protocols. This requires, among other things, the knowledge of the power system protection technician who selects and generates the signals sent to the systems control. Testing these connections is a basic part of commissioning.

The IEC 61850 Standard defines various types of communication. For time-critical data such as tripping events and transformer values initiated by a different IED, real-time transmission via GOOSE or sampled values is employed.

For **classic** communication, for example, between the systems control and a bay unit, the Standard describes various services based on the data model:

- **Control** for controlling
- **Log** for event lists
- **Report** for transmission of indications and measured values

There are static and dynamic reports. You can find more detailed information on this in chapter *2.6.3.3 Static Reporting*.

The following sections describe reports involving data exchange between a protection or bay unit (server) and the substation automation technology (client) and its tests. Reports are transmitted over Ethernet connections via TCP/IP (Transmission Control Protocol/Internet Protocol).

Data objects (indications) of a device are summarized as a list in a report. For instance, indication changes, caused for example, by a raising and cleared protection tripping event, are transmitted spontaneously from server to client. Therefore, the client does not have to query the server cyclically, as is the case with serial protocols, but automatically receives a notification of the event, for example, an indication change or a change of the measured value.

If the server permits, it is also possible to have cyclic transmission of data and general interrogation. The event control of data transmission is a property that is contained in the attributes of each report. You can affect these properties by using the IEC 61850 System Configurator.

Buffered and Unbuffered Reports

The Standard distinguishes between **Buffered Reports** and **Unbuffered Reports**. The **Buffered Report** is used most frequently today.

- **Buffered Report**
  In the case of an Buffered Report Control Block (BRCB), internal events trigger immediate transmission of reports. If the connection between the server and client is interrupted, indication changes in the protection device are stored. As soon as the connection has been reestablished, these indications are transmitted to the systems control with a time stamp and the attribute **Historic**. To enable saving to a practicable limit – as recommended in the standard – the server must have adequate storage capacity. If an uninterrupted connection exists between the client and server, for example, in the case of controlled operation in a switchgear, then the behavior of both procedures appear identical from the user view of the systems control.
- **Unbuffered report**
  In the case of an **Unbuffered Report Control Block** (URCB), internal events trigger immediate transmission of reports. If there is no connection or if the transport data flow is not fast enough, events can be lost.

Datasets are needed for reports.

Client LNs can be set. ICD files from the client are imported. Here, you will find the IP address. With this, you can assign the report to the client. This ensures that only this client will receive the report. You can do these settings in the System Configurator.

You can find information on subscribing to reports in the IEC 61850 Browser in chapter *10.1.15.3 Activating the Reports*.

2.6.3.2 Datasets

Static and Dynamic Datasets

Every IEC 61850 service relies on data from the data model. This requires **Datasets** that reference actual values in the model.

There are report datasets with data for this report, for example, indication of the positions of the disconnector switch and circuit breaker in the feeder. These datasets can be created statically or dynamically.

Static Datasets

In the case of a static dataset, the number of indications and measured values is specified in the Report Editor. Once these configuration data are loaded into the server, the client can no longer change the contents of the configuration data. A fixed report that the client can retrieve is stored in the server. Changing the number/scope of the indications requires new parameterization followed by loading to the server.

The benefit is that the data provided by a server are stored in an SCD configuration file (Station Configuration Description). The drawback is that the settings in the server must be changed if the number/scope of indications is changed for the substation automation technology.

Dynamic Datasets

In the case of dynamic datasets, the settings in the server do not need to be changed when the number/scope of indications changes. The client has 2 opportunities to read all data points that the server can potentially make available:

- Offline with a configuration file (ICD or SCD file), for example, in a SICAM substation automation technology.
- Online by connection establishment to the server, for example, in the IEC Browser Testtool.

The client specifies the information that a report from a device should contain. Thus, the content of a report is not fixed, but rather can be changed while the system is operating. The parameters set in the server do not have to be changed.

In this way, the client can be set to watch for special indications or measured values, for instance, for only a specific period. It can then create a report in the server, retrieve this report in order to obtain the information and then delete the report. No classic protocol offers this flexibility.

NOTE

Siemens supports the concept of dynamic datasets.

You can find additional information on the creation of datasets in the System configurator manual.

You can find information on creating and checking datasets in the IEC 61850 Browser in chapter *10.1.15.2 Dynamic Datasets*.

2.6.3.3 Static Reporting

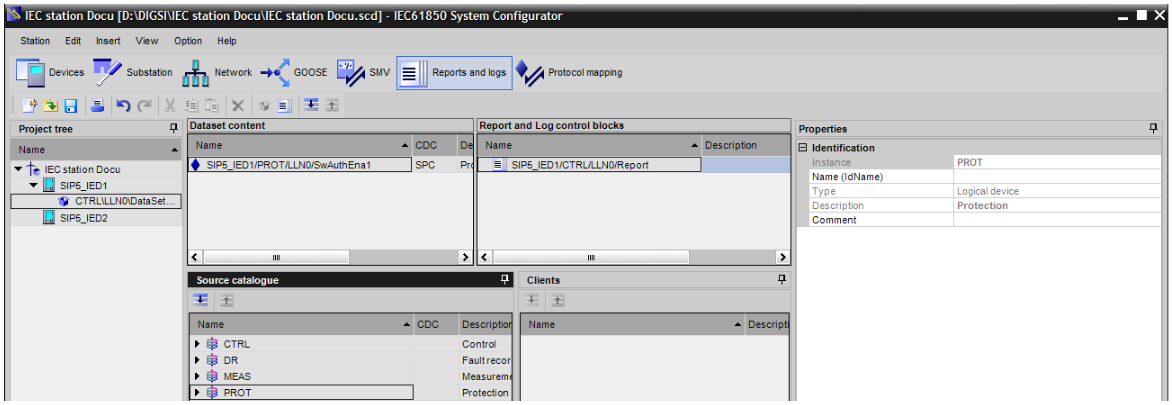
What Is a Static Report?

In a static report, the datasets are generated by the configuration in the IEC 61850 System Configurator. Such a dataset contains the data objects that are to be transmitted to an IEC 61850 client. You specify the content of the dataset with the configuration setup in DIGSI 5. This dataset is associated with a report. There are numerous possible configurations for a report.

IEC 61850 View in the System Configurator

The protection devices and bay units (server) provide a system configurator with all of the information that can be transmitted to a client (systems control) or between servers in the form of an ICD or IID file. In the case of protection functions, the manufacturer specifies the number/scope of the indications. For control functions, you establish the number/scope of indications with the configuration tool of the server (for SIPROTEC devices from Siemens, by means of DIGSI 5). The IEC 61850 Standard defines how this information is displayed in a separate XML scheme called SCL (Substation Configuration Language).

The system configurator displays the indication texts (**Description** column) together with the IEC 61850 texts (**Name** column).



[sc_syscon_reports_structure, 1, en_US]

Figure 2-20 Structure in the System Configurator

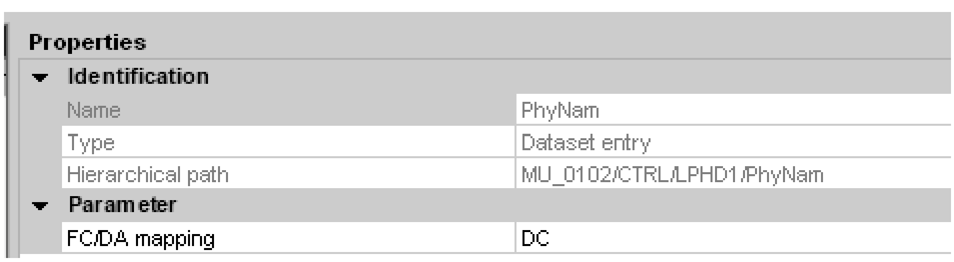
Only names (designations) from the data model (**IEC texts**) are transmitted between client and server. In this way, only the IEC texts can be seen in the case of eavesdropping of the Ethernet by a network sniffer.

Indications and measured values from the server of an IEC 61850 station are configured in a static report. For this purpose, the devices are displayed as information sources in terms of their IEC 61850 structure.

Configuration of a Static Report in the System Configurator

Device View

Select only information from the Device view that you wish to configure in the report. For this, create datasets. Describe the datasets using the properties dialog in the IEC 61850 System Configurator.



[sc_syscon_dataset_properties, 2, en_US]

Figure 2-21 Properties of the Dataset

Drag elements from the **Source catalog** into the dataset.

Right-click the dataset and select **Insert report** to add a ReportControlBlock (in this case: Protection) to this dataset. You also select between a **Buffered report** and an **Unbuffered report**.

Properties	
Identification	
Name	Report
Type	Report-Control
Hierarchical path	SIP/Application/LLN0/DataSet
Parameter	
Integrity	0
Supported clients	1
Buffer time	100
Buffer indications	No
Config revision	0
Report ID	SIP/Application/LLN0RPReport
Trigger options	
dchg	Yes
qchg	Yes
dupd	Yes
Period	Yes
Optional fields	
Sequence numbering	Yes
Time stamp	Yes
Dataset	Yes
Reason for inclusion	Yes
Data references	No
EntryID	Yes
Config references	Yes
Buffer Overflow	Yes

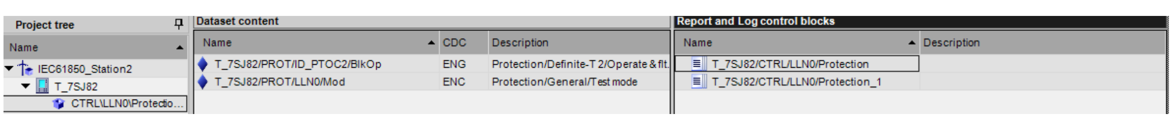
[scpropdl-140113-01.tif, 2, en_US]

Figure 2-22 Properties of a Static Report

You can find more detailed information on the **Optional fields** and the **Trigger options** in the chapter on Report Control Blocks in the **System Configurator** manual.

The server specifies these properties for the report and they cannot be changed. Under **Report number**, you can see the report ID (rptID). You can find the dataset under this ID to review.

All protection indications that are to be transmitted to the client are added to the dataset with the name **Protection**.



[scrpptin-280113-01.tif, 2, en_US]

Figure 2-23 Static Report with Protection Device Indications from the Overcurrent Protection

NOTE

You can create additional reports for information regarding command control or for measured values. A SIPROTEC device has a maximum of 11 buffered reports.

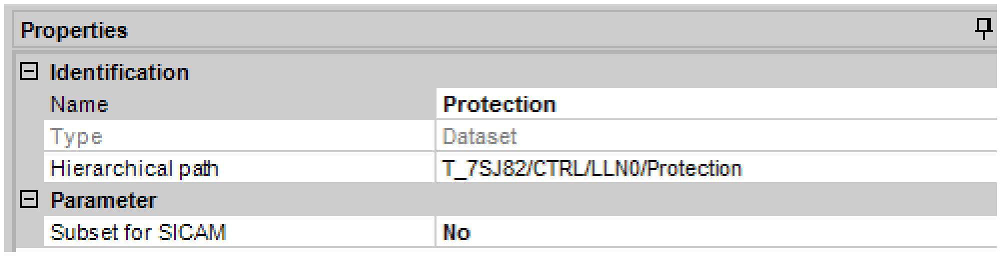
Server

The buffers in which the indications are located in the device are specified in the server on a manufacturer-specific basis.

The properties of the report (dataset, trigger conditions...) are saved in so-called **Report Control Blocks (RCB)**.

You can also change the dataset names that the system suggests (dataset + number) in the properties dialog of the dataset.

To make it easier to find the data during the subsequent review, Siemens recommends that you change the dataset name. In the example, the name of the dataset is changed to **Protection**.



[scprdset-140113-01.tif, 2, en_US]

Figure 2-24 Properties Dialog for a Dataset with Protection Device Indications

Test Mode

All data objects can be identified with a test flag. If the function block to which the data object belongs is in **Test** mode, then the test flag for a date object has been set. However, not all objects that are received via communication are marked with the test flag by the test mode of the function block. Input proxy objects, for example, contain the test flag that was received via communication.

The **Test** mode of a function block can be simulated by the following actions:

- The function block has been placed in test mode by the parameter `Mode` or by the controllable **Mod**.
- The entire device has been placed in the application test mode (HMI: Device functions/Operating modes/test).

If the reports have been configured, the data are written to an SCD file (Substation Configuration Description File) after the export. This file is important for loading the data in the device that is simultaneously the IEC 61850 server. For SIPROTEC devices, the file is loaded with DIGSI 5. To import indication lists into the client, use the SCD file. In this way, the client knows the scope of the reports and the datasets that contain the information. This standardized data exchange is a great benefit compared to previous substation automation protocols in which manufacturer-specific indication lists are exchanged in proprietary file formats or manually. The SCD file can be exported from the IEC 61850 System Configurator and is available as an input to the test program.

2.6.3.4 Testing Protection Indications

Using Reports to Test Protection Indications

✧ Create a report for the protection indication and connect the dynamic dataset with the control block.

✧ Pick up the protection indication by using a tool that can change the signal inside the device, for example, DIGSI 5 Test Editor.
You can find more information on the DIGSI 5 Test Editor in chapter *10.1.13 Test Editor*.

- or -

✧ Use binary inputs that trigger the protection application in order to pick up the protection indication.

Protection Indication on the IEC Browser

✧ Select the **Reporting** field.

- or -

✧ Click the **Auto Refresh** button in the IEC client.

✧ Pick up the protection indication.

This will enable you to detect changes on the device via the client.

2.6.4 Setting Parameters via IEC 61850

Settings in the device can be read and changed via the IEC 61850 protocol. This requires an IEC 61850 client, for example, the IEC Browser provided on the DIGSI 5 DVD. All settings displayed in logical nodes can be read and edited using the protocol.

The following stages are available:

- No parameters available
- Only reading order
- All

Consequently, an IEC 61850 client can change settings in the device independently of DIGSI 5 or the HMI (Human-Machine Interface).

The IEC 61850 Standard defines a SETTING-GROUP-CONTROL-BLOCK model (SGCB). This model allows an instance to have several values that can be used individually. It provides mechanisms for switching between several values of one or more data objects. Related values form the settings group.

The device supports up to 8 different settings groups that can be configured with DIGSI 5.

The only SGCB of a SIPROTEC 5 device is found in the logical node LLN0 of the logical device (LD) **PROT** in the **SIPROTEC 4 similar view** or the logical device **Application** in the **SIPROTEC 5 view**. All parameters of other logical devices are also addressed via hierarchical references (GrRef) of this SCGB.

The following structure is defined for the SGCB model:

SGCB Class			
Attribute Name	**Attribute Type**	**Read and Write Access** **(Read (r)/Write (w))**	**Description**
NumOfSG	INT8U	r	The attribute **NumOfSG** identifies the total number of available settings groups. n = NumOfSG
ActSG	INT8U	w (if the parameter **Active settings group** is set in DIGSI to **via control**)	The attribute **ActSG** identifies the values of the settings group that are in the active buffer. Admissible range: 1 to n
EditSG	INT8U	w	In order to edit a setting in a specific settings group, the attribute **EditSG** must be set to the appropriate value. Admissible range: 0 to n
CnfEdit	BOOLEAN	w	Siemens recommends using the attribute **CnfEdit** to confirm the edit process.
LactTm	TimeStamp	r	The attribute **LActTm** designates the time at which the **SelectActiveSG** service was edited.
ResvTms	INT16U	r	The attribute **ResvTms** defines the time interval in seconds during which the reservation of an SGCB is granted to a client.
Services SelectActiveSG SelectEditSG SetSGValue ConfirmEditSGValue GetSGValue GetSGCBValue			

The following settings are supported and can be changed:

- Single-point setting (SPG)
- Integer status setting (ING)
- CDC ENS setting (ENG)
- Time settings group (TSG)
- Analog setting (ASG)

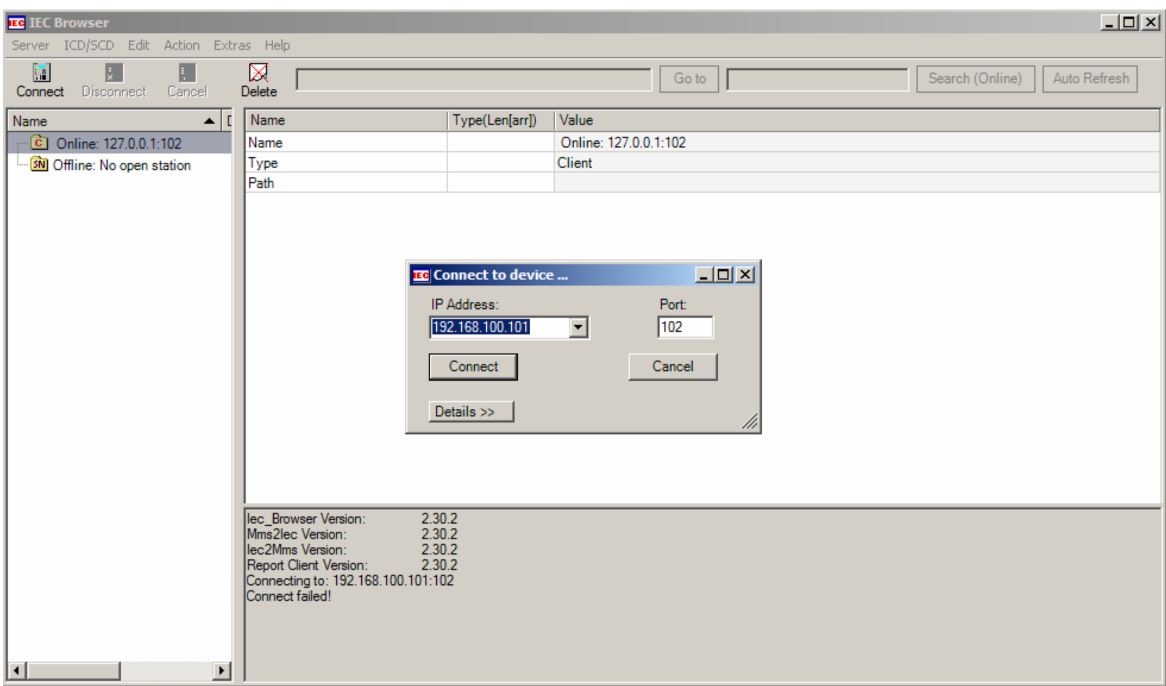
Example

The following example shows you how to change the tripping delay **OpDlTmms** of the overvoltage-protection function (PTOV) with the aid of the IEC Browser.

In this example, the logical node PTOV 7 contains the parameters (BlkOp, DrpoutRat, etc.). The data object (DO) **OpDlTmms** is an integer status setting (ING) and defines the time delay in milliseconds prior to tripping as soon as the tripping condition exists.

Establishing a Connection via the IEC Browser

✧ Use the IEC Browser to establish a connection to the device and make sure that the write function is activated.



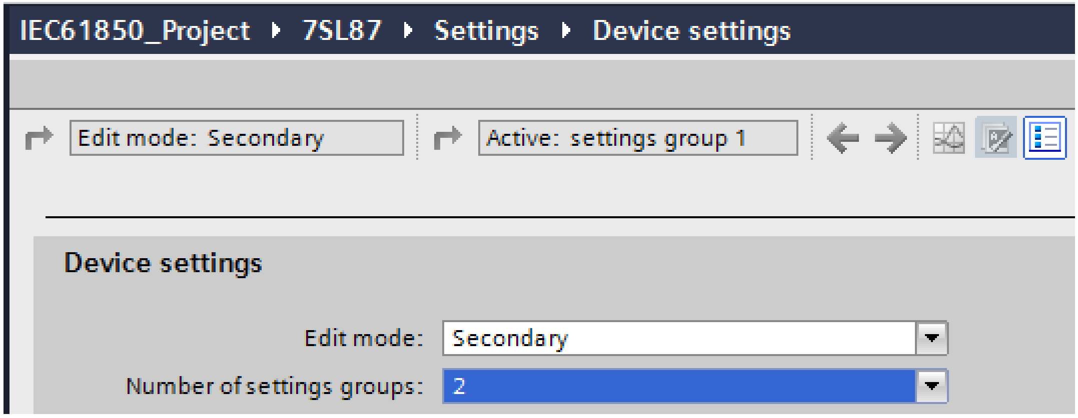
[sciecvbg-270111-01.tif, 2, --_--]

Figure 2-25 Connection via the IEC Browser

Call up the GetSGCBValue Service

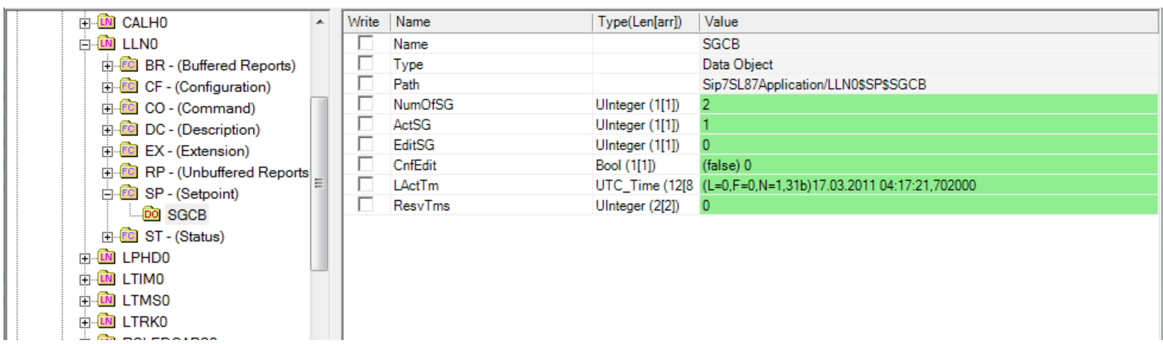
Use the GetSGCBValue service to read all attribute values from the SGCB.

✧ Set the number of settings groups in DIGSI using **Settings** > **Device settings**.



[sc_nb settings groups, 1, en_US]

✧ Navigate to the SGCB, which can be found under LD **PROT**, LN **LLN0**, and FC **SP**.



[scgtsgcb-270111-02, 1, --_--]

Figure 2-26 GetSGCBValue Service

In this example, 2 different settings groups are defined (NumOfSG=2). The currently active settings group (SETTING GROUP) is SG 1 (ActSG=1).

Call up the SelectEditSG Service

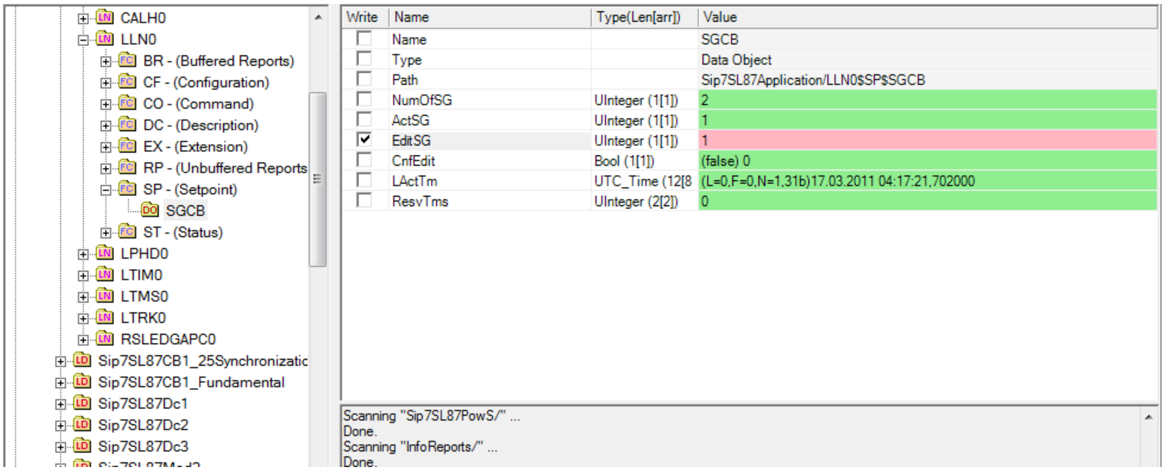
Use the SelectEditSG service to select the settings group SG, which can then be edited after selection.

✧ To edit a parameter in the currently active settings group, write **1** in the **Value** field of the attribute **EditSG**.

✧ Activate the check box next to the value.

✧ Right-click.

✧ Select **Write tagged Lines**.



[scseedsg-270111-02, 1, --_--]

Figure 2-27 SelectEditSG Service

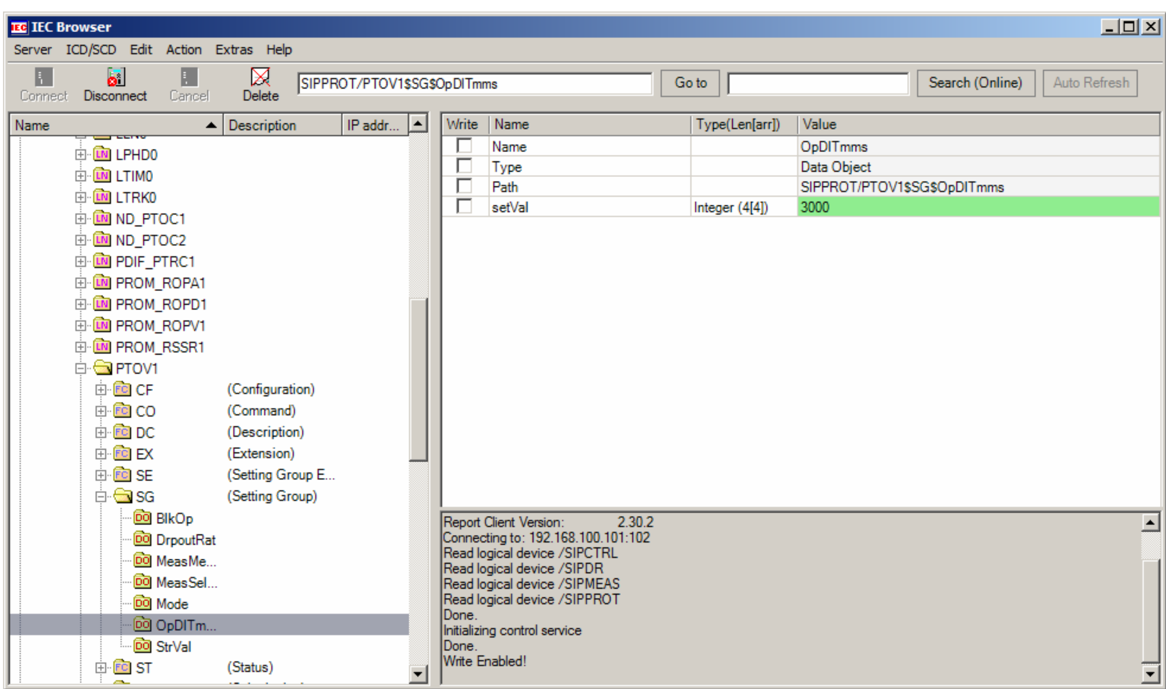
Now you can edit the parameters in SETTING GROUP 1.

Call up the GetSGValue Service

Use the GetSGValue service to read the value of the settings group SG (FC = SE) that was selected to be edited or the active settings group SG (FC = SG).

✧ To read the value of the currently active parameter, navigate to LD **PROT** LN **PTOV1** FC **SG** DO **OpDITmms** in the object-model project tree.

In this example, the parameter is to 3000 ms.



[scgetsgv-270111-01.tif, 2, --_--]

Figure 2-28 GetSGValue Service

Call up the SetSGValue Service

Use the SetSGValue service to write the value into the settings group SG selected to be edited.

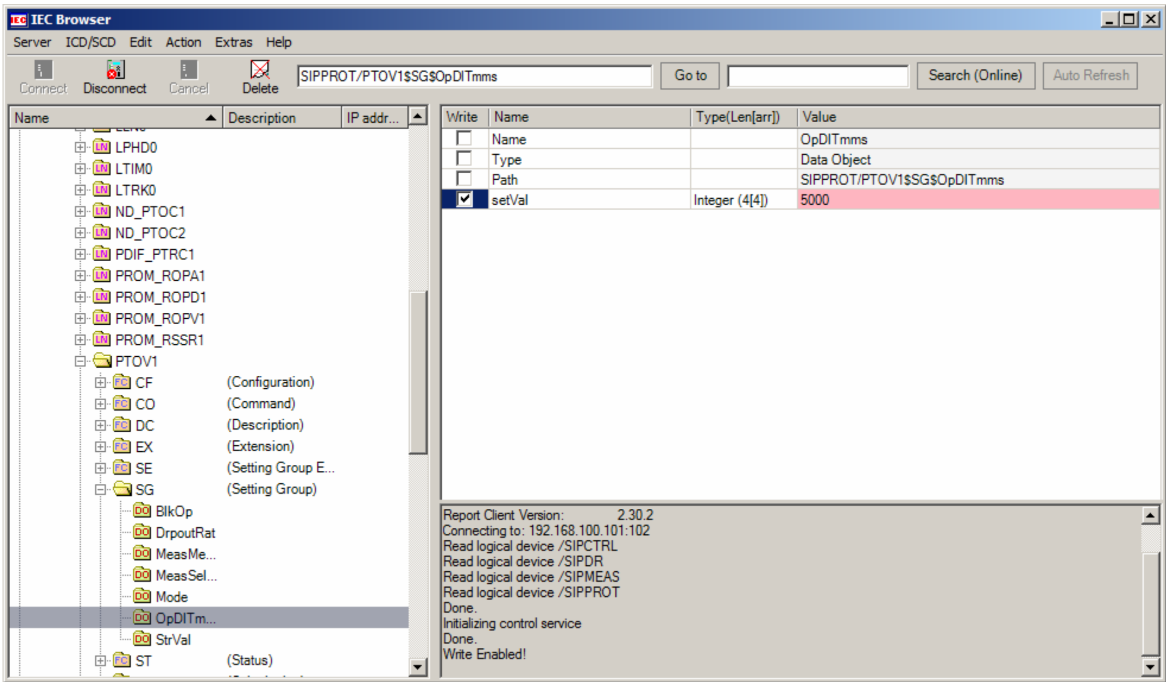
✧ Navigate to LD **PROT** LN **PTOV1** FC **SG** DO **OpDITmms** in the object-model project tree.

✧ Change the value, for example, to **5000**.

✧ Activate the check box next to the value.

✧ Right-click.

✧ Select **Write tagged Lines**.



[scsetsgv-270111-01.tif, 2, --_--]

Figure 2-29 SetSGValue Service

✧ As soon as the new value for the parameter has been written, confirm this value.

The current values in the settings group SG remain unchanged until the client has confirmed overwriting of the values with the new values from the editing buffer.

Call up the ConfirmEditSGValue Service

Use the ConfirmEditSGValue service to confirm that the new value in the settings group SG that was selected to be edited has changed to the value in the settings group SG.

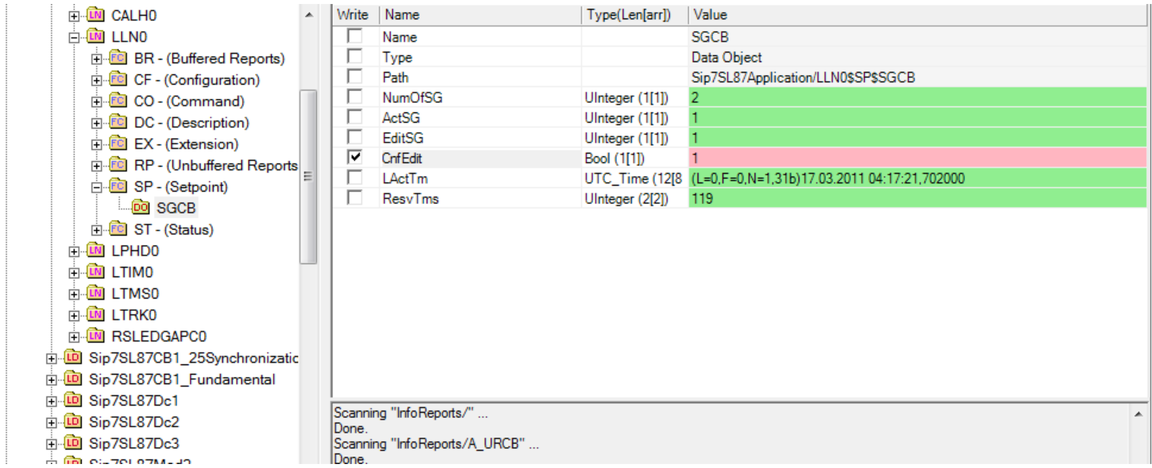
✧ Navigate to the SGCB, which can be found under LD **PROT**, LN **LLN0**, and FC **SP**.

✧ Change the value of the attribute **CnfEdit** to **1**.

✧ Activate the check box next to the value.

✧ Right-click.

✧ Select **Write tagged Lines**.



[sccfsgva-270111-02, 1, --_--]

Figure 2-30 ConfirmEditSGValue Service

The new value is now transferred from the editing buffer to the active buffer.

✧ If you read the current value of **OpDITmms** as described in the step **Call up GetSGValue service**, you will see the new active value, that is, 5000 ms.

NOTE

For some settings, **Restart required** is marked. These settings are marked in DIGSI with the  icon.

For these settings, the device executes a restart after the confirmation.

Call up the SelectActiveSG Service

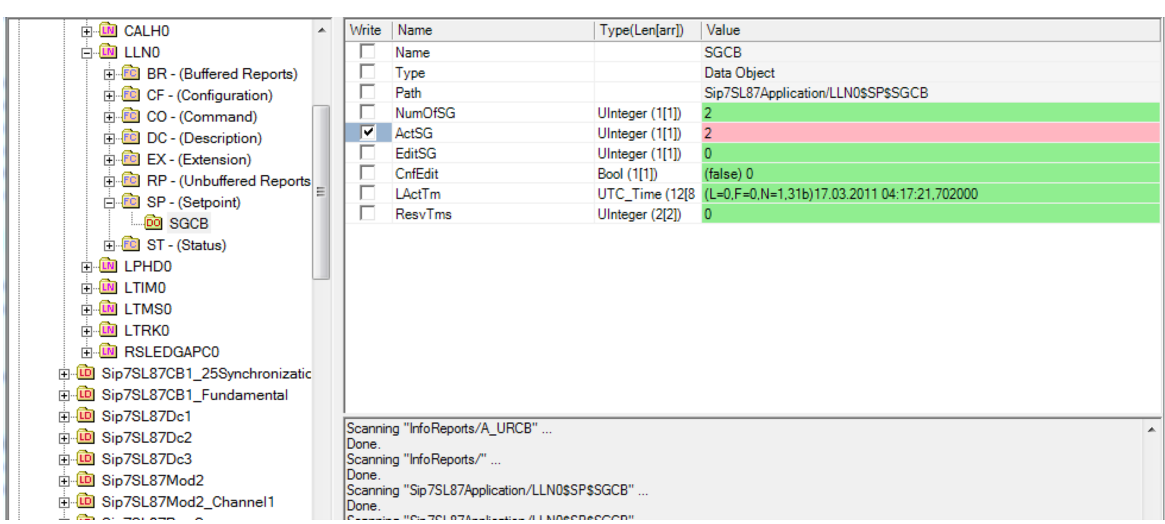
Use the SelectActiveSG service to select which settings group SG should be the active settings group.

✧ To switch to the 2nd settings group SG, change the value of the attribute **ActSG** to **2**.

✧ Activate the check box next to the value.

✧ Right-click.

✧ Select **Write tagged Lines**.



[scselact-270111-02, 1, --_--]

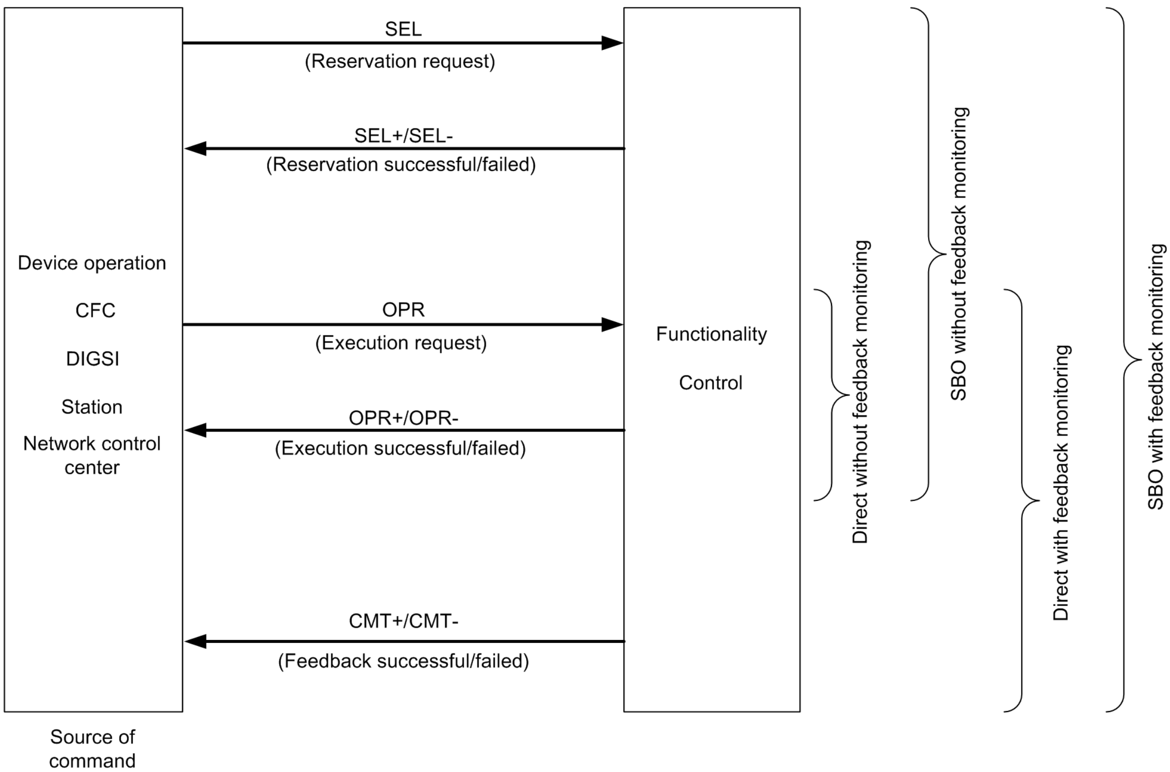
Figure 2-31 SelectActiveSG Service

2.6.5 Control via IEC 61850

SIPROTEC 5 devices support all 4 control models defined in the standard:

- Direct without feedback monitoring
- With reservation (SBO - Select Before Operate) without feedback monitoring
- Direct with feedback monitoring
- With SBO with feedback monitoring

The next figure shows the command sources, command types, and control models.

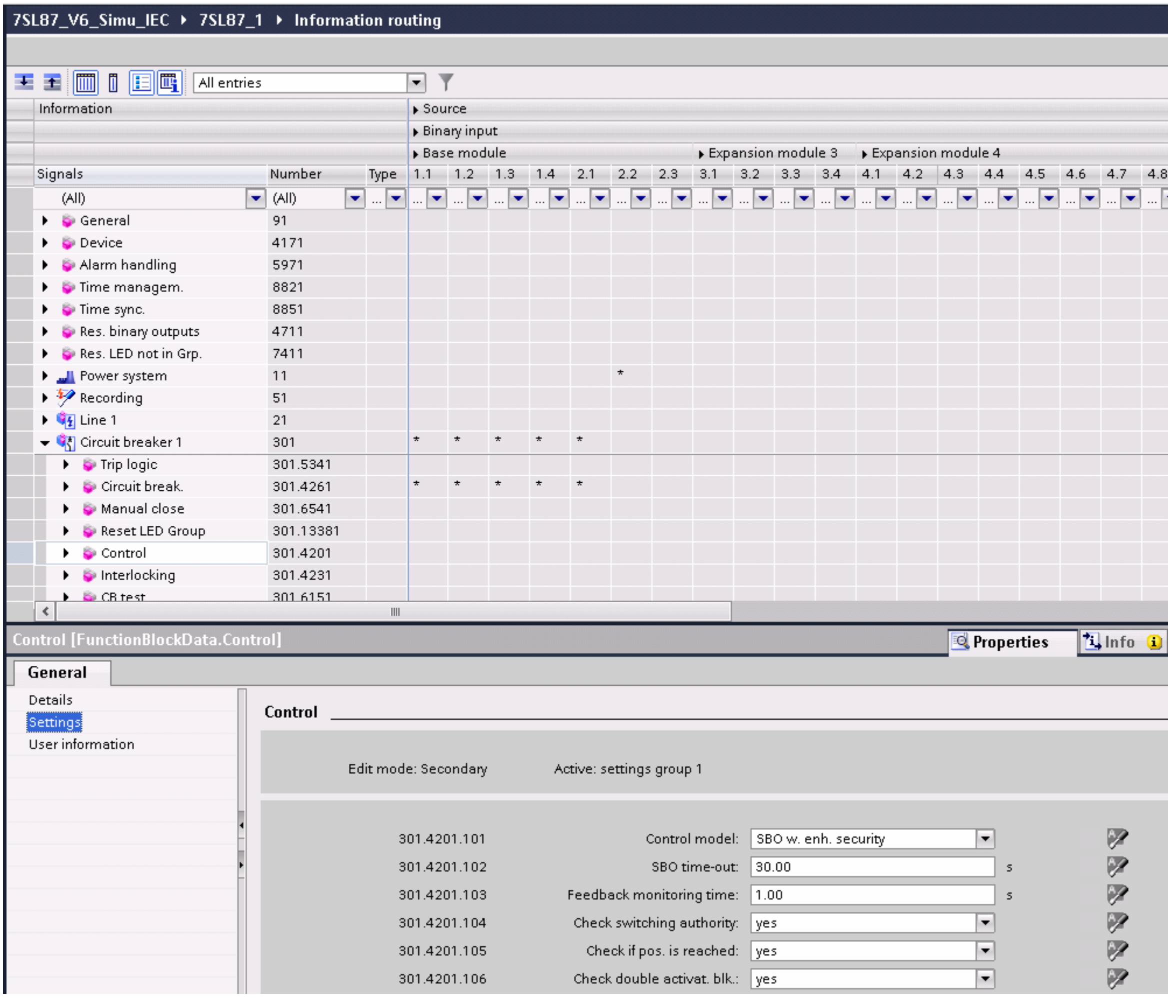


[dwsteuer-190912-01.tif, 1, en_US]

Figure 2-32 Command Sources, Command Types and Control Models

SBO control models support the **operate-once** variant. The command may only be interrupted if it conforms with the standard.

A control model is preset for all objects, taking into consideration the necessary safety aspects (implementation of the command, reaching the limit position, and safety relevance). For this reason, Siemens recommends retaining the preset control model. However, under certain circumstances it may be necessary to modify this control model.



[sc_control model, 1, en_US]

Figure 2-33 Control Model in DIGSI (Editable on Function-Block Level)

A function block **User-defined function block [control]** is available for the bay controller 6MD. If you use this function block, all added commands inherit the properties of this function block.

For controllable objects that are coupled to the process, Siemens and the standard recommend always selecting the control models **with expanded safety** (feedback monitoring).

According to the standard, commands with test state indicator are supported. This implies that a test command can be only implemented if the object **Beh** of the associated LNs has the value **test**.

The IEC 61850 protocol permits testing the switching commands for their operability prior to implementation. Test bits allow the interlocking devices to be switched on and off. The interlocking check bit affects which command checks are to be performed.

SIPROTEC 5 devices use test bits as follows:

- If the synchrocheck is not switched on for a circuit breaker and a switching command with the respective test bit is transmitted via IEC 61850 to the device, this switching command will be rejected with a negative acknowledgment **OPR-**. If the synchronization function is not a part of the **Circuit-breaker** function group, the test bit will be ignored and the switching command will be executed if all other command checks prove to be successful. More detailed command-check information can be found in the respective chapter of the Device manual.

- If the test bit is not set, it will be treated like the **non-interlocked** switching mode. If the **Interlocking** function block is not available in the **Circuit-breaker** function group, the interlocking conditions will not be tested and the switching command will be executed if all other command checks prove to be successful. More detailed command-check information can be found in the respective chapter of the Device manual.

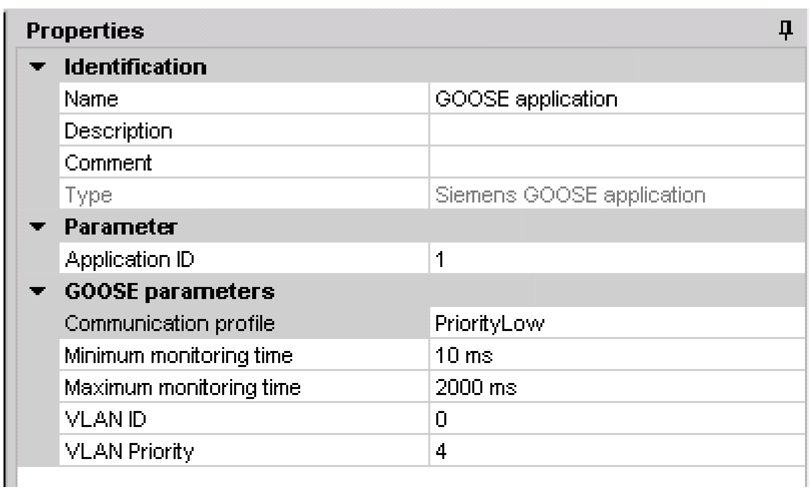
NOTE

For SICAM PAS/SCC parameterization, there are several SICAM SCC objects for each switching object, for example, switching with interlock or switching with synchrocheck. For this reason, it is mandatory to consider the specific treatment of the test bits during engineering of the system.

You can find more information on the switching authority in the manual SIPROTEC 5 High-Voltage Bay Controller 6MD85/86.

2.6.6 VLAN Priority for Fast GOOSE Tripping

You can set the VLAN priority for each GOOSE control block. To enable the function to work efficiently, a subscriber should receive only 1 GOOSE control block with the highest VLAN priority **7**. In some cases, more than 1 GOOSE control block with this priority value (**7**) can result in a high number of repetitions and thus to a slow-down in the processing of GOOSE events.



[sc_SysCon_VLANPrio, 1, en_US]

Figure 2-34 VLAN Priority

2.6.7 Measured Values and Measured-Value Description

In order to detect the measured values in the buffer or transmission via reports, the application of the dead-band is important.

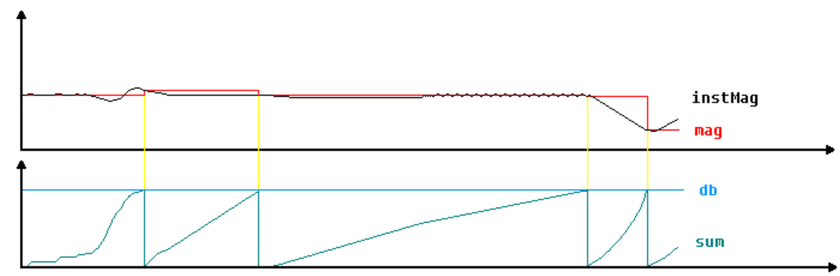
Measured values **instMag** are only forwarded with the deadband mechanism if they change outside of an adjustable window. The window is defined as an upper and lower limit, a percentage of the actual measured value.

NOTE

The summation takes place every 500 ms.

If the measured value **instMag** deviates from the deadband value **mag**, then the amount of the difference of these 2 values will be added. If over time the accumulated sum exceeds the upper limit **db** (deadband value), the deadband value **mag** will be set to the current value of **instMag**, and the sum will be reset to 0.

By using the trigger option **TrgOp=dchg**, the deadband value **mag** can be saved in the buffer or can be reported. After setting the trigger option **TrgOp=dchg**, the device may wait several milliseconds before the report is sent.



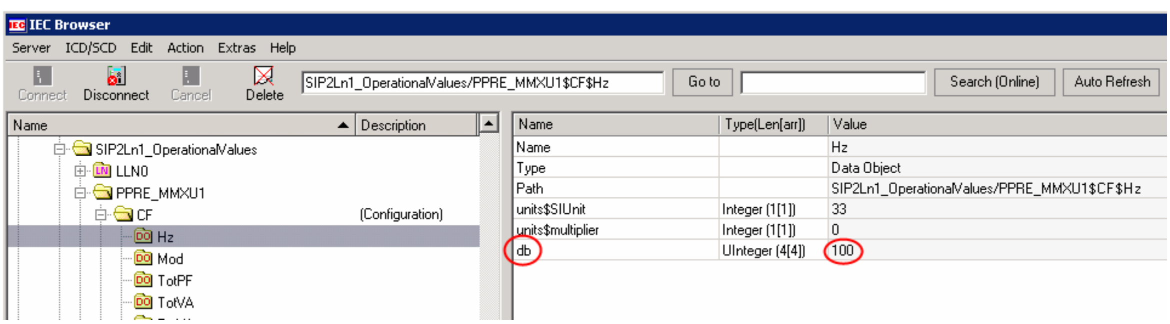
[scdiaiec-230211-01.tif, 1, --_--]

Figure 2-35 Diagram on the Behavior of Values

The diagram illustrates the relationship between the following values:

- Measured value **instMag**
- Deadband value **mag**
- Upper limit **db** (deadband value)
  The upper limit **db** is used as a unit of 0.001 % and refers as a percentage to the currently measured value
- Accumulated sum, referred to simply as **sum**

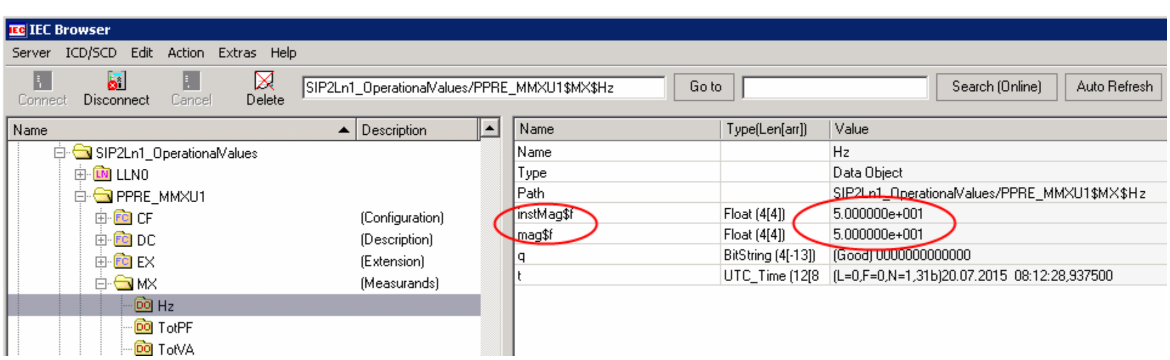
The deadband value **mag** changes significantly slower than the measured value **instMag**.



[sc_db_IECBrowser, 1, --_--]

Figure 2-36 Example of db Value

The figure shows the **db** value in the IEC Browser.



[sc_IECBrowser_instmag_and_mag, 1, --_--]

Figure 2-37 instMag and mag Values

Large differences between **instMag** and **mag** lead to the repeated updating of **mag**.
Small differences between **instMag**and **mag** lead to an infrequent change of **mag**.

NOTE

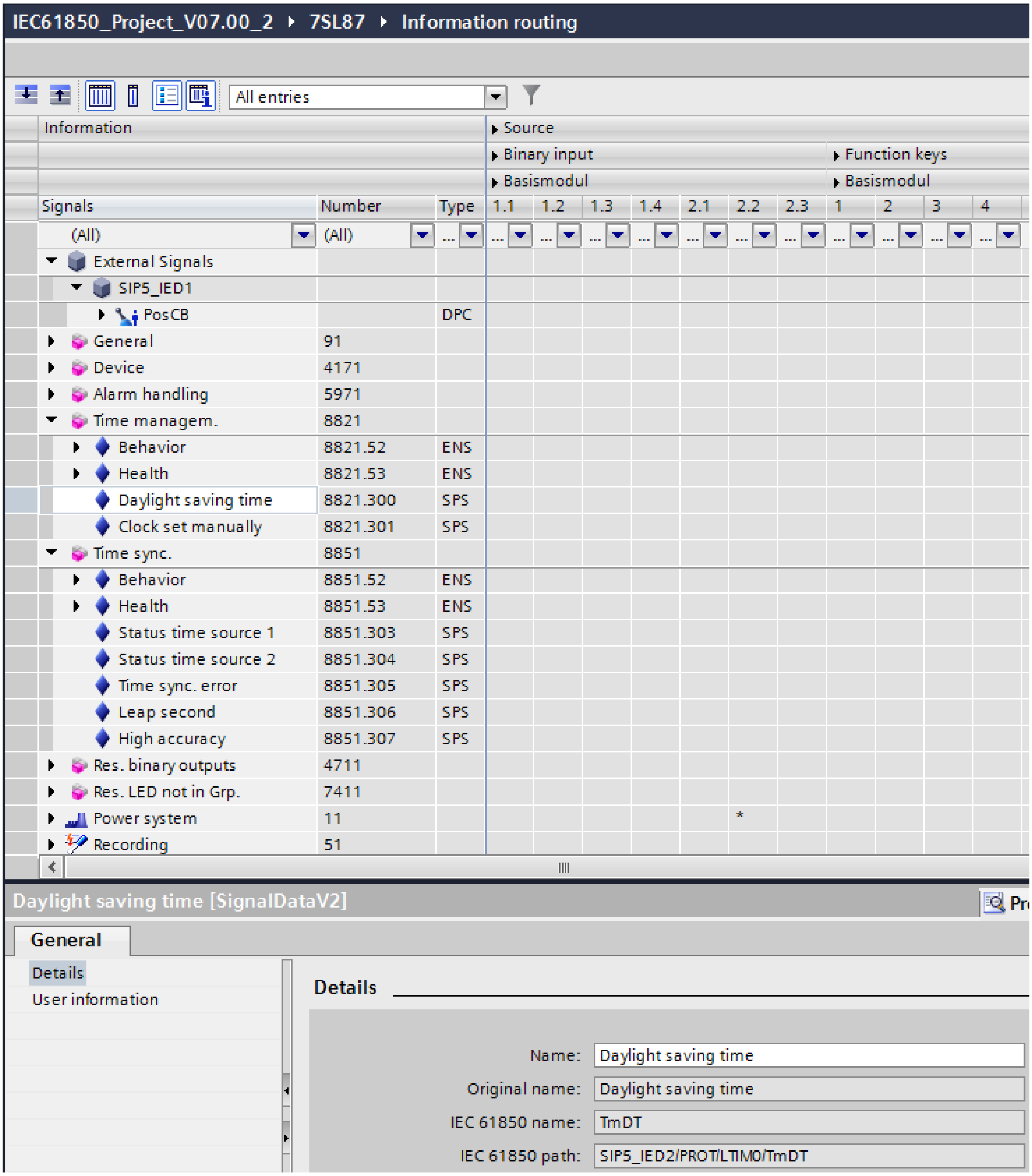
Since **db** is a percentage of the measured value, very small measured values and increased noise may cause a flood of **mag** indications. An additional threshold in the device prevents a flood of indications.

If spontaneous changes do not need to be sent quickly, reports with measured values can also be transmitted cyclically.

2.6.8 Device Time

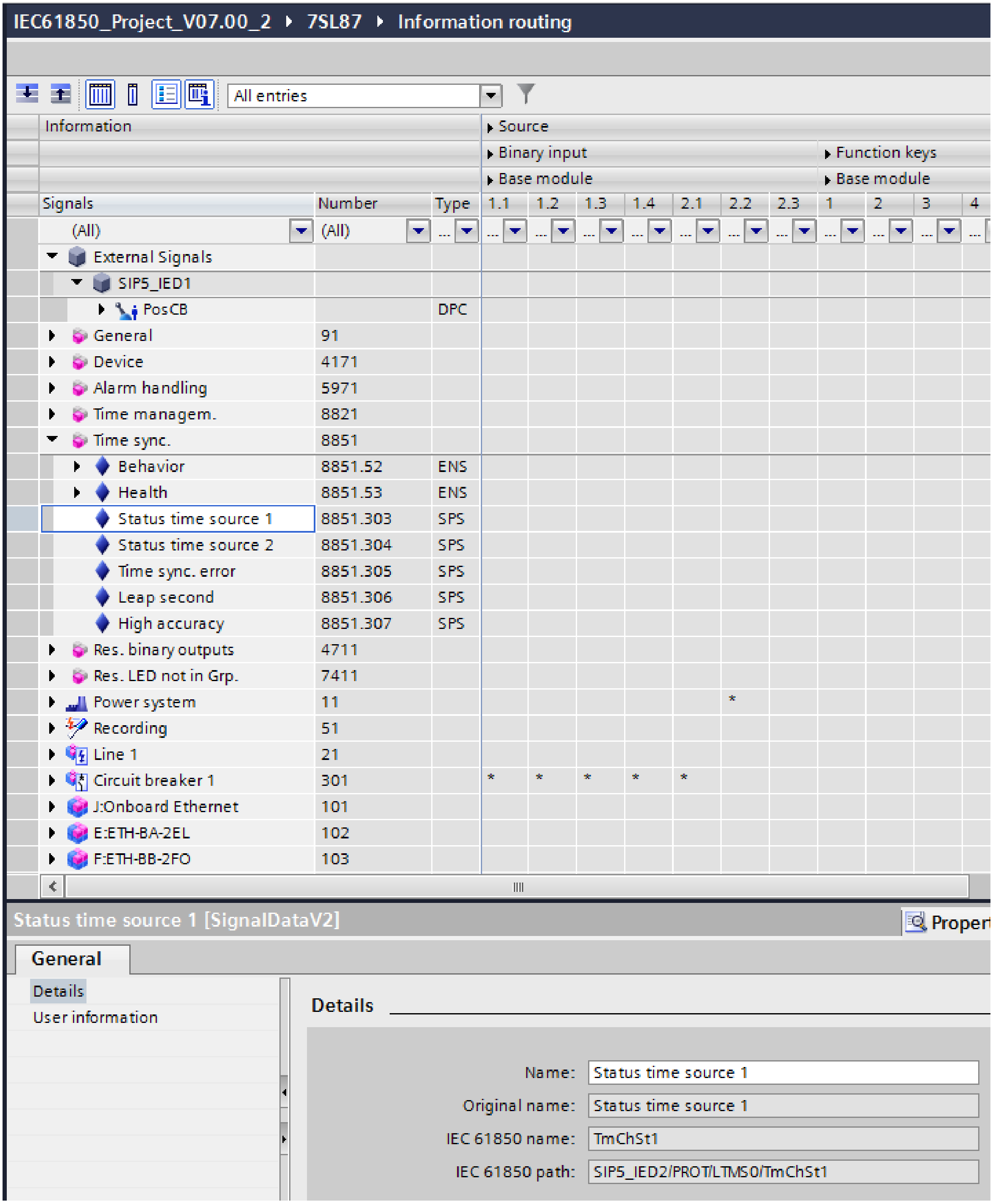
2.6.8.1 Description

The SNTP protocol or the IEEE 1588 protocol can be used for time synchronization via Ethernet networks.



[sc_Device_time_LTIM, 1, en_US]

Figure 2-38 Device-Time Messages – Example LN/LTIM



[sc_Device_time_LTMS, 1, en_US]

Figure 2-39 Device-Time Messages – Example LN/LTMS

SIPROTEC 5 devices support both Edition 1 and Edition 2 according to IEC 61850-7-2. In Edition 2, the logical attributes **LeapSecondsKnown**, **ClockFailure**, **ClockNotSynchronized**, and the value **TimeAccuracy** are maintained in each time stamp. In Edition1, these signals contain default values. Thus, the interoperability for substation automation technologies is ensured for both editions.

In the best case (highest quality), the following values are set:

- TimeAccuracy = 24 (2^{-24} s = 59.6 ns)
- ClockNotSynchronized = false
- ClockFailure = false

If the time quality decreases, first only the **TimeAccuracy** changes, for example, to**TimeAccuracy** = 10 (2^{-10} s = 0.98 ms). The worst value that is possible for **TimeAccuracy** is 0 (2^{-0} s = 1 s). If the time quality becomes even worse, this is indicated with the special value **TimeAccuracy** = **31 (unspecified)**.

With an unsynchronized device, the following values are displayed for all indications:

- TimeAccuracy = 31 (unspecified)
- ClockNotSynchronized = true

2.6.8.2 Determining the TimeAccuracy Value

The accuracy of a received time stamp can be identified by the received telegram (see *IRIG-B, Expanded Protocol, Page 127*). If this is not the case, the source is supposed to have a perfect accuracy (deviation = 0).

The measured deviation between the received time and device time (for a precise receive time) is added to this value. As long as no other time telegram is received, the indicated accuracy of the SIPROTEC device continually decreases at 0.2 ppm (0.2 µs/s). This accuracy has internal fine resolution. The accuracy is represented in the time stamps approximately as exponential in form (2^{-24} s to 2^{-0} s) as **TimeAccuracy**. This representation is specified by the IEC.

If the value **ClockNotSynchronized** is set to **true**, **TimeAccuracy** is set to **31 (unspecified)** (typically after a time value according to the setting **Fault indication after** after the last synchronization telegram).

IRIG-B, Expanded Protocol

An accuracy value (expansion acc. to IEEE C37.118-2005) contained in IRIG-B 005(004) is added to the measured deviation between the received time and the device time.

If the special value **locked** is received, then only the deviation between the received time and the device time is taken as the accuracy value.

SNTP

SNTP contains an accuracy value with the aid of the stratum value. However, since this value cannot be converted into a concrete deviation, it is ignored by the SIPROTEC 5 device. The receiving offset is taken into account as with all sources.

IEEE 1588

The accuracy values from the **Announce message** (**grandmasterClockQuality**, **TimeInaccuracy** in profile-specific IEEE_C37_238 TLV) are not evaluated.

Other Time Formats

These sources are considered as perfect – apart from a measured offset to device time.

2.6.8.3 Determining the ClockNotSynchronized Value

After device startup, this value is first set to **true**. Through a 1st synchronization using one of the set sources, it changes to **false**.

However, if no more synchronization telegrams are received for the set time **Fault indication after** (default: 600 s), then the value is set to **ClockNotSynchronized** = **true**.

If the value **ClockFailure** is set, then also **ClockNotSynchronized** is always set.

The status of **ClockNotSynchronized** corresponds to the state of the message **Time sync. error** right up to startup. However, the message status at startup is **off**. If no synchronization takes place, for parameterized sources, this status changes to **on** after **Fault indication after**.

2.6.8.4 Determining the ClockFailure Value

If hardware errors occur on the time components, the logical value **ClockFailure** is set to **true**.

This value is set at startup until a valid time can be read from the clock module buffered with the button cell or until the time can be set manually (HMI, DIGSI) or by a parameterized synchronization source.

If **ClockFailure** is set, **ClockNotSynchronized** = **true** and **TimeAccuracy** = **31 (unspecified)** are also set.

The status of the message **Clock fail** corresponds to the status of the value.

2.6.9 Asset Management

You can monitor firmware and configuration statuses across the entire plant. Attributes of the devices are used for this purpose.

The following versions and information are made available for asset management via the IEC 61850 interface.

Asset	IEC 61850 Name	Note
Mainboard Firmware Version	LPHD.PhyNam.swRev	Version 7.40 is displayed by **V07.40**, version 7.50 by **V07.50** and so forth.
Communication Module Firmware Version	LCCH.NamPlt.swRev	Version 7.40 is displayed by **V07.40**, version 7.50 by **V07.50** and so forth.
Mainboard Configuration Version	Every LN.NamPlt.swRev, except LLN0 and LCCH	Version 7.40 is displayed by **V07.40**, version 7.50 by **V07.50** and so forth. Single elements that have not been changed in version V7.40 can have an older version.
Vendor	LPHD.PhyName.vendor	
BM Number	LPHD.PhyName.serNum	
Product Code	LPHD.PhyName.hwRev	
Device Type	LPHD.PhyNam.model	

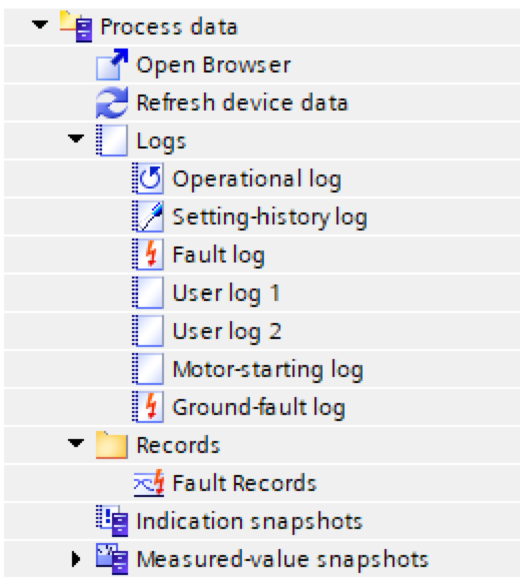
2.7 File Transmission

2.7.1 Retrieving Fault Records and Logs

The MMS (Manufacturing Message Specification) file transfer can be used for the transmission of COMTRADE fault records and COMFEDE event logs.

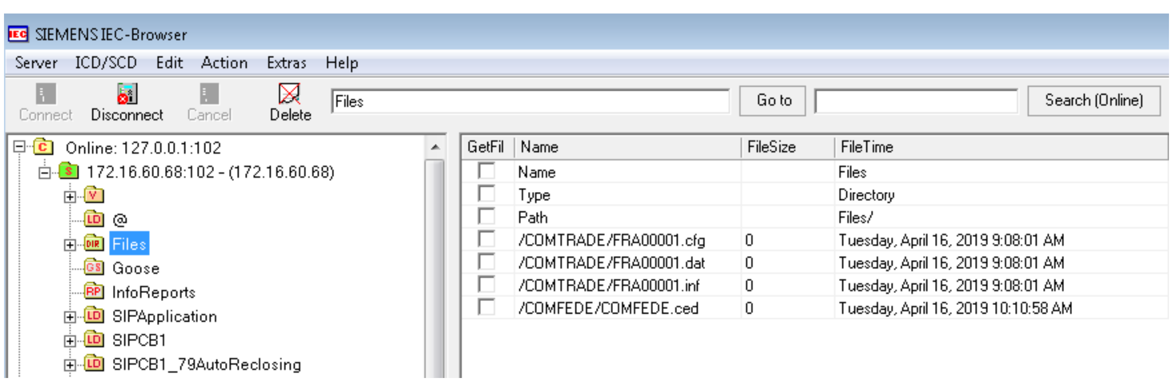
Therefore, the MMS file transfer provides a standard and automated way to retrieve all SIPROTEC 5 process data without using DIGSI 5.

You can find 2 different methods of retrieving fault records and logs in the following figures.



[sc_ProcessData, 1, en_US]

Figure 2-40 Retrieving Fault Records and Logs via DIGSI 5



[sc_LogsviaMMS, 1, --_--]

Figure 2-41 Retrieving Fault Records and Logs via MMS File Transfer

2.7.2 Fault Records

File transfer is used to transmit fault records from a server to a client. The fault records, such as intended in the COMTRADE standard, are stored in the server together with a configuration file (.cfg) and a binary data file (.dat). When COMTRADE 2013 is used, the content comprises an information file (.inf) and a header file (.hdr). A client reads both files and can then display the fault record with analog and binary traces. This requires special analysis software, for example, SIGRA.

The configuration file contains, among other information:

- All analog and binary traces of the fault record
- Names of the traces
- Sampling rate

The raw data for these traces are contained in the data file, which is stored as a binary COMTRADE in the device.

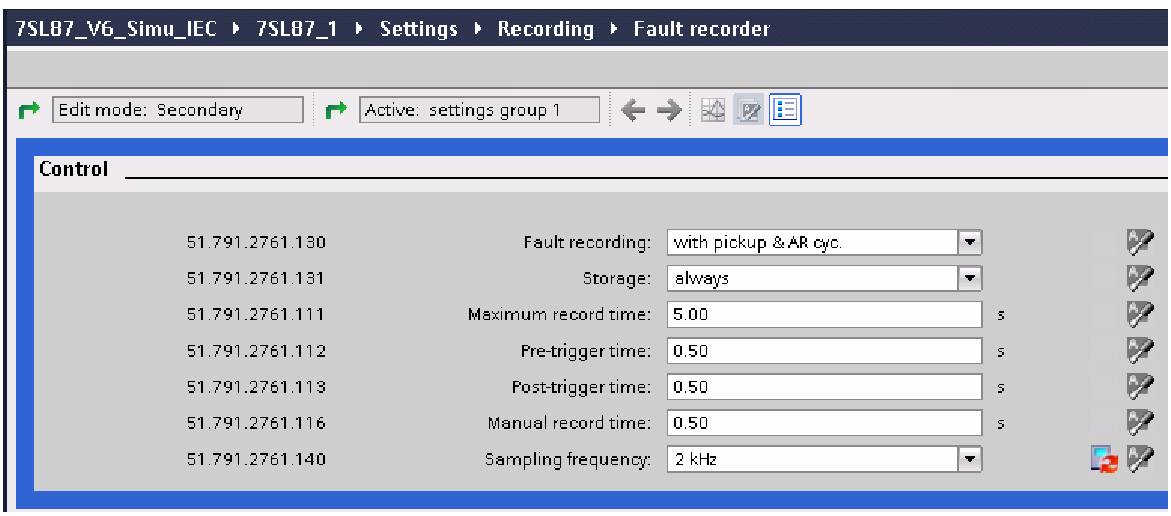
Binary traces must be configured in the **Recorder** column in the DIGSI 5 Information routing.

Fault records are transmitted with a resolution of 8 kHz via the IEC 61850 protocol, except for 7KE85. 7KE85 can transmit fault records via the IEC 61850 protocol with a resolution of 16 kHz.

NOTE

Fault records can also be read from the device by DIGSI 5. They are available there at a maximum sampling rate of 8 kHz. You can configure the sampling rate differently for DIGSI 5 and IEC 61850. The DIGSI 5 sampling rate is always identical to or greater than the IEC 61850 sampling rate. Transmission to DIGSI 5 does not use the IEC 61850 protocol, but instead uses a compressed and encrypted protocol.

Configure the sampling rate in DIGSI 5 as follows:



[sc_fault record, 1, en_US]

Figure 2-42 Configuring the Sampling Rate in DIGSI

An IEC 61850 Client can retrieve a directory of the fault record from the device. It can later transmit the records from the device with MMS file transfer. You can find more information in the manual about PIXIT, PICS, TICS IEC 61850.

NOTE

The COMTRADE file must be generated internally before transmission. Thus the file size is initially unknown and is reported as 0 in accordance with the IEC 61850 standard.

2.7.3 COMFEDE

2.7.3.1 Overview

The SIPROTEC 5 device has the following operational logs that can be retrieved as a standard COMFEDE file over MMS file transfer.

- Operational logs
- Fault logs
- Ground-fault logs
- User-defined logs
- Setting-history logs
- Motor-starting logs
- Sequence-of-events log
- Communication-supervision log

You can find more information about the content of the logs in chapter 8.5.1 General in the Operation Manual.

NOTE

For security reasons, the security logs are not accessible via COMFEDE. The security logs are accessible via syslog.

NOTE

The troubleshooting logs (device-diagnosis logs, communication log) are available only for the maintenance personnel via DIGSI.

2.7.3.2 Description COMFEDE

The IEEE C37.239-2010 defines the Common Format for Event Data Exchange (COMFEDE) for power systems. COMFEDE is the format for file transfer in protection devices with the following main characteristics:

- COMFEDE consists of a XML file with the extension *.CED, following a defined XSD schema.
- The format of COMFEDE is able to at least hold the information related to the following log and reports:
  - Sequence-of-events (SOE) log
  - Fault-summary reports
- Additionally, a COMFEDE file contains the following device information data:
  - Device name
  - Product code
  - Serial number
  - Firmware version
  - Configuration version

Downloading the COMFEDE File

IEC 61850 clients can download the COMFEDE file from the device.
If one of the following events occurs, an active download will be interrupted:

- New fault logs are created.
- New ground-fault logs are created.
- New operational logs are created.
- New user-defined logs are created.
- New setting-history logs are created.
- New motor-starting logs are created.

- New sequence-of-events log is created.
- The repeated download request is sent.
- The IEC 61850 client is disconnected from the device.

If there is an interruption, the IEC 61850 client must restart the downloading.

After the download is finished, you can save the COMFEDE.ced on a local PC.

NOTE

When the device has many process data, the COMFEDE file download can take several minutes.

Interaction with the COMTRADE Download

If a communication module is downloading a COMFEDE file, an additional download request of a COMTRADE file on the same module will be rejected.

If a communication module is downloading a COMTRADE file, an additional download request of a COMFEDE file on the same module will be rejected.

NOTE

In either case, the device with MMS file transfer replies the error FILE_BUSY (02).

A new download request for COMFEDE or COMTRADE files is only possible once the current download is completed.

NOTE

Each communication module can process the COMFEDE or COMTRADE file download independently from each other. For example, a COMTRADE download on Port E and a COMFEDE download on Port J can be processed at the same time.

2.7.3.3 COMFEDE Display

Opening the COMFEDE File

To display the downloaded COMFEDE file on a local PC, proceed as follows:

✧ Download **COMFEDE.css** and **COMFEDE.xslt** from the Internet page.

✧ Rename the **COMFEDE.ced** to **COMFEDE.xml**.

✧ Put **COMFEDE.css**, **COMFEDE.xslt**, and **COMFEDE.xml** together in one folder.

✧ Open the **COMFEDE.xml**with the Web browser, for example, Internet Explorer.

The following Internet page is displayed:

SIPROTEC 5

Common Format for Event Data Exchange (COMFEDE)

Company Name	Siemens
Station name	Station
Device	7SP82
Product code	7SP82-DAAA-AA0-0AAAA0-A90411-12113B-AAC000-000AB0-HB2BD4-JA0
Serial number	BMDDDD123456_BF1807023681
Vendor	Siemens
Firmware version	V07.90
Configuration version	V07.90

Attention: This document is automatically generated!

Liability exclusion We have checked the compliance of this brochure with the hard and software described. However, since deviations cannot be ruled out entirely, we do no accept liability for any error or omission. The information in this manual is checked periodically, and necessary corrections will be included in future editions. We appreciate suggestions for improvements. Technical modifications, even without notice, remain reserved.

Table of contents

[sc_COMFEDEDisplay, 1, en_US]

Figure 2-43 COMFEDE Display

You can navigate to the more detailed information using the hyperlinks under **Table of contents**.

Display of Fault Logs and Fault Records

To display the fault log and fault record, proceed as follows:

✧ Click **Fault log** under **Table of contents**.

The fault-log table is displayed.
You can find the fault logs as hyperlinks in the table.
If there is a file name in the **COMTRADE** column, you can also find the fault record via the file name.

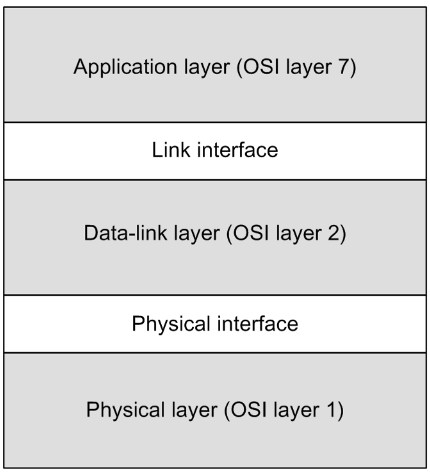
3 DNP3

3.1 Protocol Characteristics

3.1.1 Protocol Structure

3.1.1.1 Description

DNP3 has a graded architecture. Instead of the OSI model, however, a simplified 3-layer model suggested by the IEC is used. This model was named **Enhanced Performance Architecture** (EPA) by the IEC. However, DNP3 adds a 4th layer, a pseudo transport layer, with which messages can be segmented. The graphics were taken from the DNP3-Spec-V1-Introduction-20071215.pdf standard.



[dw_epadia, 1, en_US]

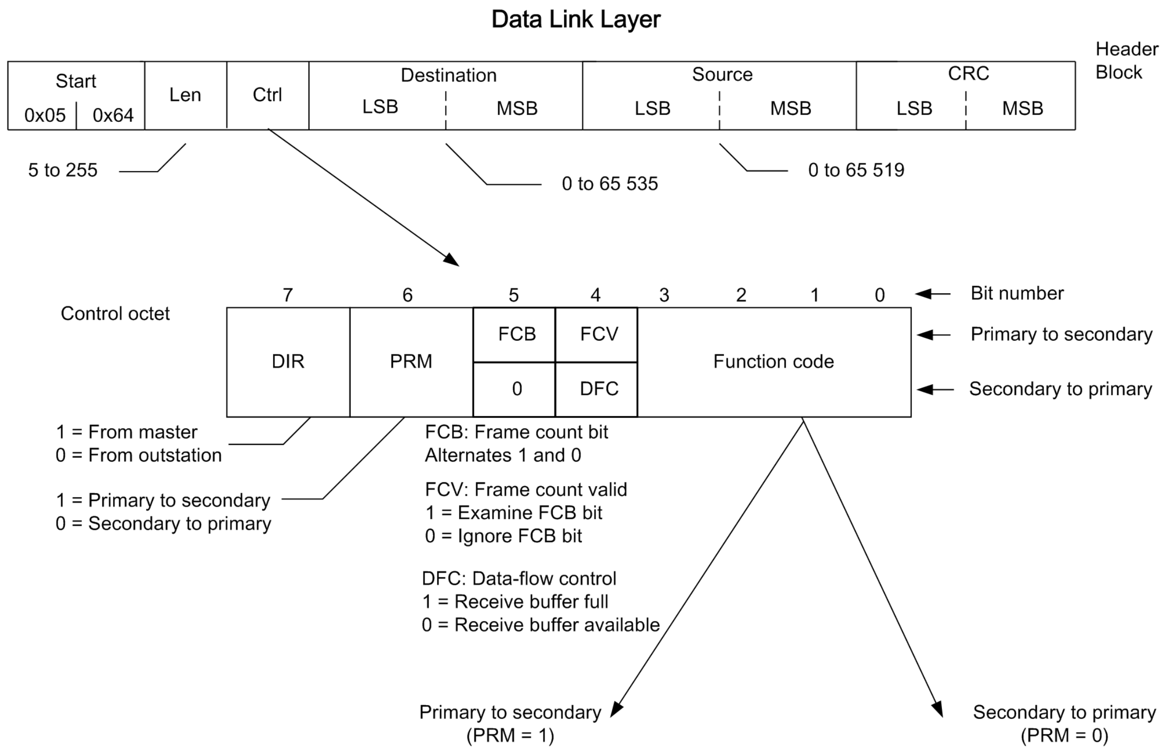
Figure 3-1 EPA Diagram

The SIPROTEC 5 device supports the DNP3, level 2 version.
You can find additional information in the standard IEEE 1815 at *http://standards.ieee.org/*.

3.1.1.2 Physical Layer

The physical layer mainly deals with the physical media through which the protocol is transferred. The physical layer deals with, for example, the condition of the media (free or occupied) and the synchronization through the media (start and stop).

DNP3 most frequently uses a simple, asynchronous serial transmission like RS232 or RS485 with physical media like pilot wires and optical fiber. Moreover, the transmission can take place through Ethernet.



Primary function code	Function-code name	FCV bit
0	RESET_LINK_STATES	0
1	-	-
2	TEST_LINK_STATES	1
3	CONFIRMED_USER_DATA	1
4	UNCONFIRMED_USER_DATA	0
5	-	-
6	-	-
7	-	-
8	-	-
9	REQUEST_LINK_STATUS	0
A	-	-
B	-	-
C	-	-
D	-	-
E	-	-
F	-	-

Secondary function code	Function-code name
0	ACK
1	NACK
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
A	-
B	LINK_STATUS
C	-
D	-
E	-
F	NOT_SUPPORTED

[dw_dalila, 1, --_--]

Figure 3-2 Physical Layer

3.1.1.3 Data-Link Layer

The data link layer manages the logical connection between the transmitter and the receiver of the information and improves the fault tolerance of the physical line. This is achieved with DNP3 by starting every data transmission package with a data head, and a 16 bit CRC (cyclic redundancy check) is executed for every 16 bytes of the package.

A package is a part of the complete message transferred through the physical layer. The maximum size of a data package is 256 bytes. Each package has a 16-bit source address and a 16-bit target address, which can also be a general address (0xFFFF).

The 10-byte data link layer head contains:

- Address information
- 16-bit start code

- Frame length
- Data link control byte

The data link control byte displays the cause of the data transmission and the status of the logical connection. The data link control byte can have the following values:

- ACK (data link confirmation)
- NACK (negative confirmation)
- Connection needs to be reset
- Connection is reset
- Data link confirmation from the package required

If a data link confirmation is needed, the receiver must respond with an ACK data package if the package was received and the CRC checks were successful. If no data link confirmation is requested, no response is required.

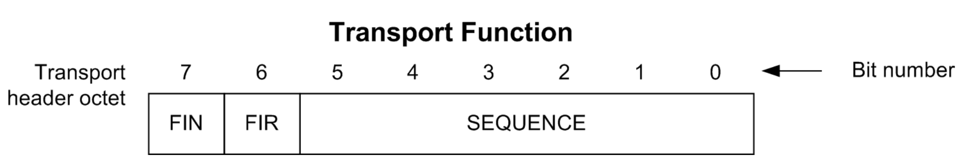
3.1.1.4 Pseudo Transport Layer

The pseudo transport layer segments application messages in multiple data transmission packages.

The pseudo transport layer implements an individual byte function code for every package. The byte function code displays what the data transmission package is:

- The 1st package of a message
- The last package of a message
- Both (for individual message packages)

The function code delivers a running package number. This subsequent package number is increased with each package and allows the receiver's transport layer to analyze the package.



[dw_trfnct, 1, --_--]

Figure 3-3 Pseudo Transport Layer

3.1.1.5 Application Layer

The application layer responds to received messages and creates messages based on the necessity and availability of the user data. As soon as messages are available, they are sent to the pseudo transport layer. The messages are segmented here, sent to the data link layer and transferred through the physical layer.

If the data that is to be sent is too large for an individual application message, a number of application messages can be created and sent in a sequential manner. Each message is an independent application message. Their only connection with each other is the label in all messages that says that more messages will follow. Only the last message does not contain this label. Each application message refers to a fragment due to the fact that the user data may be fragmented. A message can thus be a single fragment message or a multi-fragment message.

Application packages from DNP3 slaves are normally responses to queries. A DNP3 slave can also send a message without a request, thus, an unsolicited response.

As in the data link layer, application fragments can be sent with a confirmation request. An application confirmation indicates that a message was not only received, but rather it was also syntactically analyzed without any errors. A data transmission confirmation or an ACK indicate only that the transmission package was received and that the CRC checks were error-free.

Each application package begins with an application layer header, followed by one or more object heads/object data. The application layer header contains an application control code and an application function code.

If one of the following conditions is fulfilled, then the application control code contains labels:

- The package is a multi-package message.
- An application layer acknowledgment is requested for the package.
- The package is not requested.

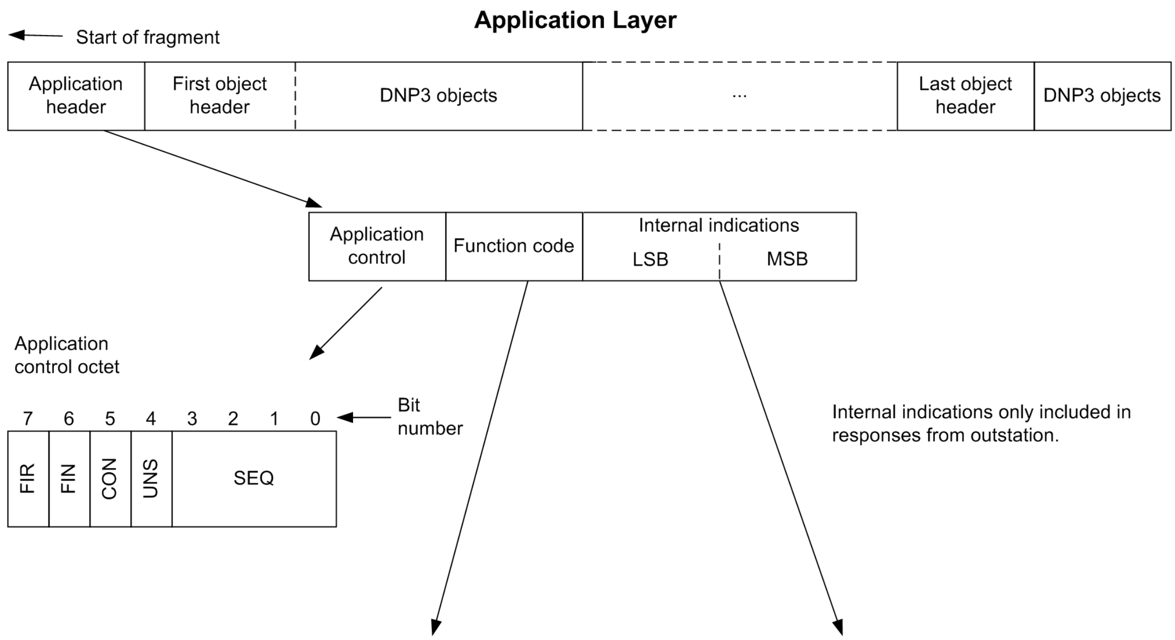
The application control code contains a continual application layer number. With this application layer number, the receiving application layer can recognize alien packages or lost packages.

The application function code in the header of the application layer indicates the cause or the requested function in the message. While DNP3 allows a number of data types in a single message, it also allows only an individual query for a data type within the message.

Examples for application function codes include:

- Acknowledgments for confirmation on the application layer
- Read and write
- Select and execute (SBO (select before operate), controls)
- Direct control (for switching objects without SBO)
- Save and delete (for counters)
- Restart (both cold and warm)
- Enable and disable non-requested messages
- Selection of the classes

The application function code in the header of the application layer applies for all object headers. Thus, the application function code applies for all data within the message package.



Function code

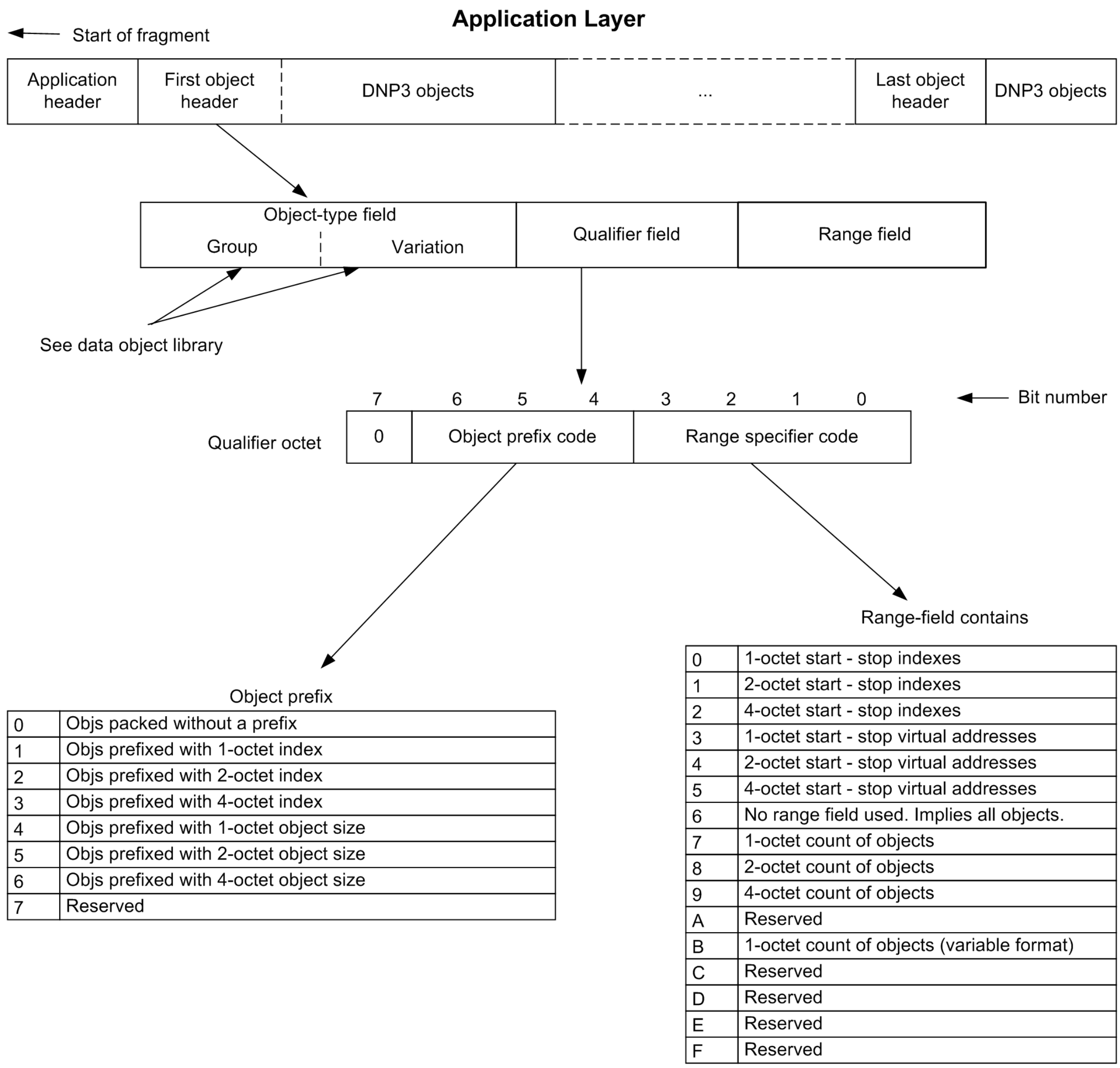
Requests (Hex)			
0	Confirm	10	Initialize application
1	Read	11	Start application
2	Write	12	Stop application
3	Select	14	Enable unsolicited
4	Operate	15	Disable unsolicited
5	Dir operate	16	Assign class
6	Dir operate - No resp	19	Open file
		1A	Close file
		1C	Get file information
D	Cold restart	1D	Authenticate file
E	Warm restart	1E	Cancel file
F	Initialize data		
Responses (Hex)			
81	Response		
82	Unsolicited response		

Internal indications

LSB	
IIN1.0	All stations
IIN1.1	Class 1 events
IIN1.2	Class 2 events
IIN1.3	Class 3 events
IIN1.4	Need time
IIN1.5	Local control
IIN1.6	Device trouble
IIN1.7	Device restart
MSB	
IIN2.0	Function code not supported
IIN2.1	Object unknown
IIN2.2	Parameter error
IIN2.3	Event buffer overflow
IIN2.4	Already executing
IIN2.5	Configuration corrupt
IIN2.6	Reserved 1
IIN2.7	Reserved 2

[dw_aplay_1, 1, --_--]

Figure 3-4 Application Layer – Part 1



[dw_aplay_2, 1, --_--]

Figure 3-5 Application Layer – Part 2

3.1.2 Transfer through Ethernet

3.1.2.1 Requirements for the Physical, Transport, and Application Layers

The transmission through Ethernet takes place according to the same specifications as transmission through serial connections. Only the method for the time synchronization through the network must be changed. All requirements in the other protocol layers can be applied. Connection packages are transported in an unchanged manner through the Ethernet protocol suite under the control of the data link layer.

3.1.2.2 Acknowledgments

If the SIPROTEC devices communicate through Ethernet, they must not work with confirmations from the physical layer (CONFIRMED_USER_DATE). If necessary, the confirmations must be used by the application layer. For confirmations of the application layer, there is no difference between IP networks (IP = Internet protocol) and serial channels.

3.1.2.3 Message Transmission

As soon as the data-link layer has established a TCP connection (TCP = Transmission Control Protocol), the physical layer of DNP3 can transmit packages as needed. The type of query (requested or not requested) does not depend on the type of connection.

The SIPROTEC 5 devices support dual DNP3 Ethernet masters on the same Ethernet module.

A typical case for each DNP3 master is as follows:

- TCP connection is established with a device
- Class 1, 2, 3, 0 request is executed once
  The data integrity is checked.
- Non-requested transmission is made possible
- Work is continued in this mode.

3.1.3 Functional Scope

The DNP3 interface of the SIPROTEC 5 device supports the following functions:

Function	Description
Binary inputs with status	Remote Terminal Unit (RTU) Object 01 and variation 02 describe the state of a digital input channel or internal software information. They are also used during the general interrogation by an RTU to synchronize the database. The general interrogations are conducted after the run or cyclically during the runtime.
Binary inputs with changed time	Object 02 and variation 02 describe the changes of a digital input channel or of internal software information with the associated change time. The binary inputs are used for spontaneous process events.
Binary outputs with status	Object 10 and variation 02 describe the current status of a binary output channel. The control relay output block controls the binary output channels. See also object 12.
Control relay output block	Object 12 and variation 01 are used for commands for the process or for the setting-up of internal functions.
32-bit binary meter with marking	Object 20 and variation 01 are used for the display of metered values for active and reactive power.
32-bit binary change meter without time	Object 22 and variation 01 are used for the display of changed meter data for active and reactive power.
32 bit analog inputs (measured values)	Object 30 and variation 01 describe signed 32-bit values for the digitalized analog signals or their calculated values.
16 bit analog inputs (measured values)	Object 30 and variation 02 describe signed 16-bit values for the digitalized analog signals or their calculated values. They are used for the general interrogation during start-up. A measured value snapshot is also possible.
32-bit analog change values without time	Object 32 and variation 01 are used for the display of a changed analog value.
16-bit analog change values without time	Object 32 and variation 02 are used for the display of a changed analog value.
Time and date Write function	Object 50, variation 01 The time and date object are used for time synchronization.
Time and date Read function	Read the system time of the device. Date and time are displayed in milliseconds. Here midnight on January 1, 1970 is 00:00 hours, 00:00 minutes, 00:00 seconds and 00:00 milliseconds.

Function	Description
Data class	Object 60, variation 01, 02, 03, 04 These objects indicate different classes of information elements: • Class 0 contains all information objects that are not distinguished in terms of class 1 to 3 • Classes 1 to 3 contain groups of events from information elements • The data from class 1 has the highest priority, followed by class 2, class 3, and the static data • Class 1 always means class 0 + 1, class 2 means class 0 + 2
File transfer	Object 70, variation 01, 02, 03, 04, 05, 06, 07 Transfer of a fault record possible
Internal displays	Object 80, variation 01 Writing the value 00 on index 7 leads to reset of the bit **Restart** in the flag byte for all data objects. Writing to Index 4 resets the **Need Time** Bit.

NOTE

These variations are set. You cannot change the variations in DIGSI.

3.1.4 Fault Record Transfer

The file transfer can be used to transfer a fault record (Object 70). The **Rcd Made** message is used to query the availability of the fault record. When the message is mapped and there is a new fault in the device the message is transferred. Cyclical reading of the directory is also possible. If there are files in the directory then there are also fault records. Specifically, the transfer takes place as follows:

The following steps are required to read the directory:

- Reading of the directory with File Transport Object (obj 70 var 7)
- Waiting for the response
- If the read operation was successful, the master station increases the block number and reads the next block.
- If the status indicator **Last** is set in the response, the master station closes the file with **File Operation Status Object** (obj 70 var 4).

Every fault record is identified by an existing file. The following information is transferred for this:

- File Name Offset
- File Name Size
- File Type
- File Size
- Time Of Creation
- Permissions
- Request ID
- File Name

The master station can now select the required fault. The transfer takes place in the same manner as with reading the directory.

3.1.5 Amount of Mappable Information

The following information can be mapped:

Information	Maximum Mappable Amount
Indications + Controllables at Tx	500
Controllables at Rx	50
Settings at Tx	Not supported
Measurements at Tx	100
Counters at Tx	20

3.1.6 Additional Information

The mapping of the commands occurs like the mapping of messages. Here, object group 12 is preset.

Scaling Measured Values

The measured values between the SIPROTEC 5 device and the DNP3 master are transferred as integer values in 16-bit or 32-bit format. 16 bits correspond with a range from 0 to 65 535; 32 bits correspond with a range from 0 to 4 294 967 295.

You can find more detailed information on this in chapter *1.7.5 Mapping Selection*.

The measured values are available in the SIPROTEC 5 device in floating-point format, related to the parameterized rated variables of the primary system in percentage.

Converting Measured Values

Before the transfer of a measured value through DNP3, the measured values must be converted in the SIPROTEC 5 device. The measured values are scaled.

The scaling of a measured value determines the form of transmission. These forms of transmission are:

- Value type
- Scaling factor

Scaling Factor

The measured value is multiplied in the SIPROTEC 5 device by the scaling factor. The measured values are then changed into integer measured values (for DNP3) in the floating-point procedure.

Through multiplication with a multiple of 10, decimal places can also be transferred into integer measured values.

Calculation Formula for Integer Measured Values

The following conditions must be met for the calculation:

- The floating-point number (measured value $_{\text{Float}}$) is available in the corresponding value type (primary or secondary value).
- The floating-point number (measured value $_{\text{Float}}$) is available as a percent value.

The integer measured value (measured value $_{\text{Integer}}$) for the transmission through DNP3 is calculated according to the following formula:

$$\text{Measured value}_{\text{Integer}} = \text{Measured value}_{\text{Float}} \cdot \text{Scaling factor}$$

[fomwintr-230310-01.tif, 2, en_US]

Mapping on the Object Status

The following table shows mapping on the object status.

Table 3-1 Mapping on the Object Status

IEC 61850 Implementation				Preferred DNP3 Implementation		
Attribute Name		**Attribute Type**	**Value/Value Range**	**Point Type**	**Point Count or Note**	**Comment**
		PACKED LIST	–	–	–	–
validity		CODED ENUM	Good	–	ONLINE set if **good**	–
			Questionable	–	COMM_LOST	–
detailQual		PACKED LIST	–	–	–	–
	overflow	BOOLEAN	DEFAULT FALSE	–	ROLLOVER	–
	outOfRange	BOOLEAN	DEFAULT FALSE	–	OVER_RANGE	–
	badReference	BOOLEAN	DEFAULT FALSE	–	REFERENCE_ERR	–
	oscillatory	BOOLEAN	DEFAULT FALSE	–	CHATTER_FILTER	–
	failure	BOOLEAN	DEFAULT FALSE	–	OFFLINE	–
	oldData	BOOLEAN	DEFAULT FALSE	–	COMM_LOST	–
	inconsistent	BOOLEAN	DEFAULT FALSE	–	DISCONTINUITY	–
	inaccurate	BOOLEAN	DEFAULT FALSE	–	–	–
source		CODED ENUM	Process	–	–	–
			Substituted	–	LOCAL_FORCED	–
test		BOOLEAN	DEFAULT FALSE	–	LOCAL_FORCED	–
operatorBlocked		BOOLEAN	DEFAULT FALSE	–	LOCAL_FORCED	–

Number Representation Depending on the Parameterization

If you determine the scaling of a measured value, then you first set the number format and the unit. The number format contains the number of relevant decimal places.

Percent Values

For percent values, Siemens recommends a scaling factor of 100. This results in an interpretation of the integer measured value (measured value$_{\text{Integer}}$) through DNP3 with a measured value from ± 32 767. This corresponds with a percentage value of ± 327.67%.

Secondary Values

If, for example, the values from the transducer inputs are specified in mA, then the transmission of a measured value as a secondary value makes sense.
The number of significant decimal points depends on the system and transducer data.

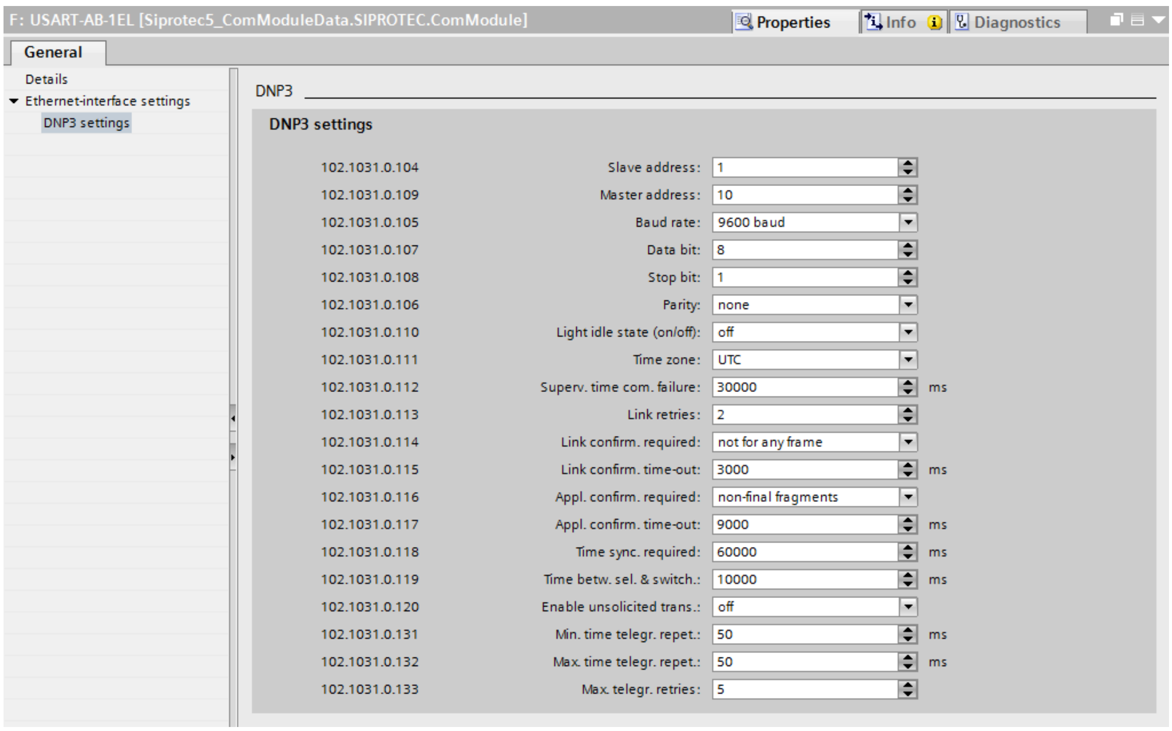
Primary Values

The position of the decimal point and the respective unit are determined for primary values based on the parameterized rated variables of the primary system.

3.2 Settings and Properties

3.2.1 Settings for the Serial Connection

During the parameterization, make the following settings for the serial communication between the DNP3 master and the SIPROTEC 5 device via DNP3:



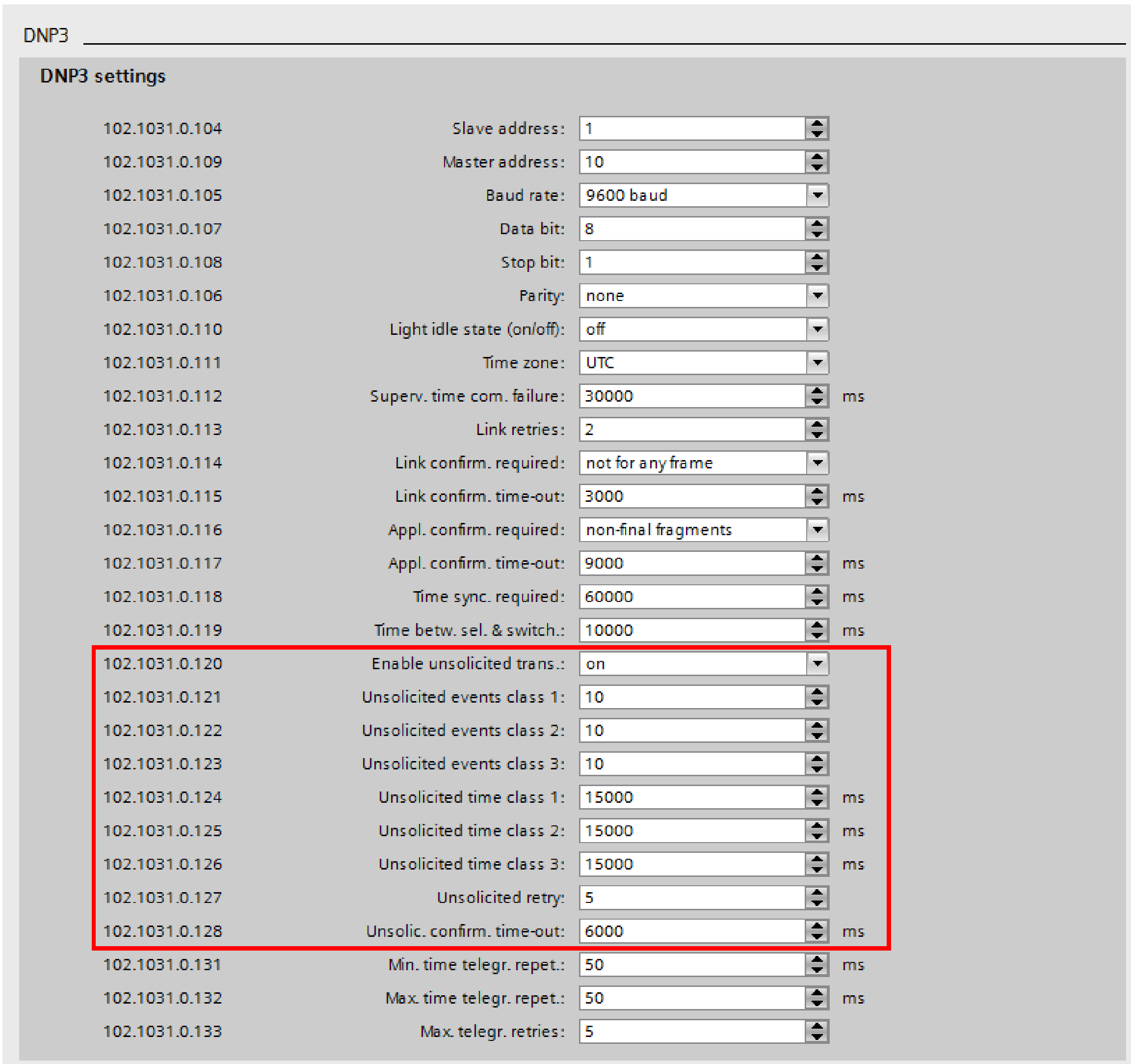
[sc_DNP3 serial communication, 1, en_US]

Figure 3-6 DNP3 Serial Connection Settings – When the Setting **Enable unsolicited trans.** Is off

Parameter Name	Description	Settings
Slave address	Link address of the SIPROTEC 5 device	Setting range = 1 to 61 439 Default setting = 1
Master address	Address of the DNP3 master	Setting range = 1 to 61 439 Default setting = 10
Baud rate	The DNP3 communication module supports baud rates in the range from 2400 Bd to 57 600 Bd.	Default setting = 9600 Bd
Data bit	7 data bits or 8 data bits can be set on the communication module.	8 data bits must be set for the DNP3 protocol.
Stop bit	The DNP3 communication module supports 1 stop bit and 2 stop bits.	Default setting = 1 stop bit
Parity	You set the parity with this parameter.	No parity (default setting) Even parity Odd parity
Light idle state (on/off)	You determine the communication medium with this parameter. If the communication takes place via an optical fiber, the rest position is specified at the same time. The light idle state is relevant only for optical modules.	Not active: Communication via RS485 On: Communication via optical fiber; rest position light on Off: Communication via optical fiber; rest position light off (default setting)

Parameter Name	Description	Settings
Time zone	Time zone of the DNP3 device (must be the same as the time zone of the SIPROTEC 5 device)	UTC (default setting) Local
Superv.time com.failure	If no communication with a master occurs in the parameterized time, an error message is issued.	Setting range = 0 ms to 3 600 000 ms Default setting = 30 000 ms
Link retries	The number of transmission attempts (LinkRetries) If the receiver did not send a confirmation, a data package is transmitted again.	Setting: Sending with confirmation Default setting = 2
Link confirm. required	The receiver is asked to send a confirmation of the required packages.	Not for any frame (default setting) Multiframe fragment All frames
Link confirm. time-out	The parameter **Link confirm. time-out** specifies a time interval. During this time interval (in ms), the receiver waits for a confirmation from the opposite end until the last telegram is repeated. This only happens, if the information has been sent with confirmation. The time starts after the last byte has been sent.	Default setting = 3000 ms
Appl. confirm. required	This parameter specifies when a confirmation of the application layer is required.	Event-data messages: If messages contain event data, then a confirmation of the application layer is required. Non-final fragments: If telegrams are divided into different fragments, a confirmation of the application layer is required except for the last fragment, then a confirmation of the application layer is required (default setting).
Appl. confirm. time-out	The receiver waits during a desired period of time (in ms) until the previous response is confirmed. If the confirmation of the application layer is used together with the link confirmation, then make sure that the time-out of the application layer (AppCon-Time-out) is long enough to end all transmissions. The following formula describes this requirement: AppConTime-out > LinkConTime-out * (Link retries + 1)	Default setting = 9000 ms
Time sync. required	Time interval (in ms) until the internal display **Time required** is set. This time interval is included in every response message. The time interval signals to the master to start a new time synchronization with the device.	0 = The internal display is never set. Default setting = 60 000 ms
Time betw. sel. & switch.	A command must be selected and executed in this time (in ms).	Default setting = 10 000 ms
Enable unsolicited trans.	With this parameter, you determine whether unsolicited transmission is configured.	Off = The unsolicited transmission is not configured and can never be switched on from a connected master (default setting). On = The unsolicited transmission is configured and must be made possible after the 1st unsolicited response from the master.
Min. time telegr. repet.	Minimum time of the telegram repetition following a collision	Setting range = 0 ms to 100 ms Default setting = 50 ms

Parameter Name	Description	Settings
`Max. time telegr. repet.`	Maximum time of the telegram repetition following a collision	Setting range = 0 ms to 50 ms Default setting = 50 ms
`Max. telegr. retries`	Maximum number of the telegram repetitions following a collision	Setting range = 1 to 200 Default setting = 5



[sc_DNP3SerialConectionSettings_On, 1, en_US]

Figure 3-7 DNP3 Serial Connection Settings – When the Setting **`Enable unsolicited trans.`** Is on

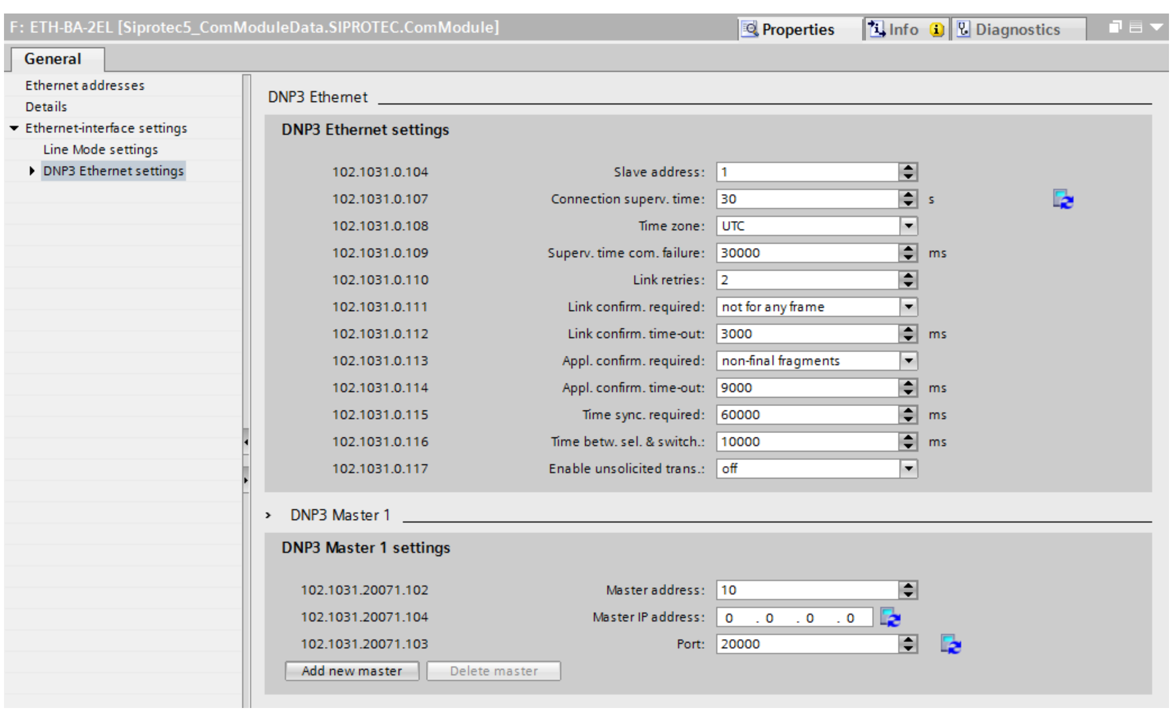
The following parameters only make sense if the parameter **`Enable unsolicited trans.`** is set to ***on***:

Parameter Name	Description	Settings
`Unsolicited events class 1/2/3`	This parameter regulates a condition of the non-requested transmission for every class of changed events (class 1, class 2, and class 3). If the number of events per class equals or exceeds this value, then an unsolicited response is sent.	Default setting = 10
`Unsolicited time class 1/2/3`	This parameter regulates a condition of the non-requested transmission for every class of changed events (class 1, class 2, and class 3). If the time (in ms) after an event equals or exceeds this value, an unsolicited response is transmitted. The unsolicited message is also sent if only 1 event occurred.	Default setting = 15 000 ms
`Unsolicited retry`	If no unsolicited response was sent within the time set under the **`Unsolicited confirm. time-out`** parameter, then this parameter regulates how many times a different unsolicited response is sent.	Default setting = 5
`Unsolic. confirm. time-out`	Time (in ms) for waiting for the receiver to confirm the non-requested response. If a query to read is received in the meantime, the read query is answered first, and then the unsolicited response is not transmitted.	Default setting = 6000 ms

3.2.2 Settings for Communication through Ethernet

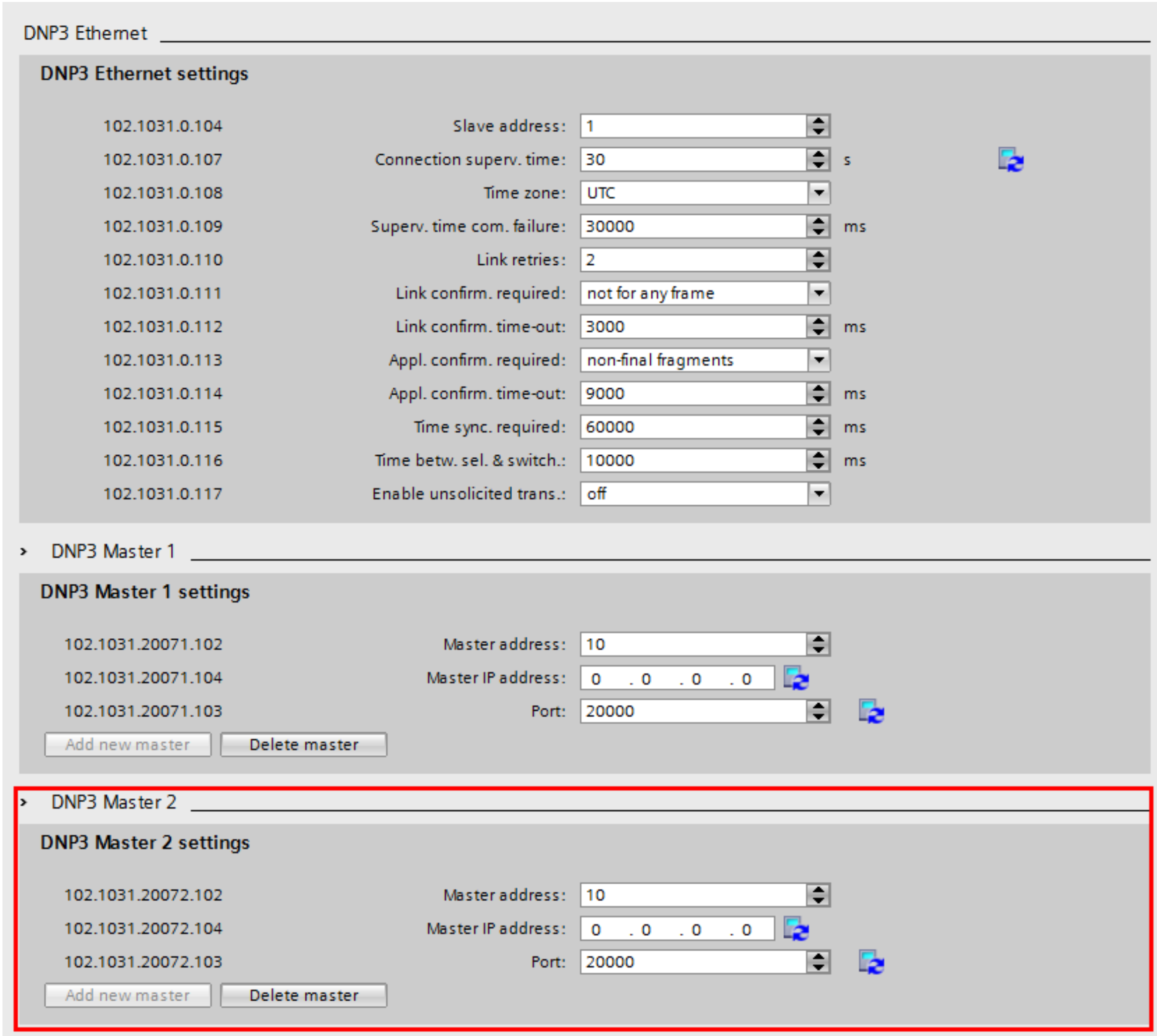
During parameterization, make the following settings for the Ethernet communication on the Ethernet module between the DNP3 master and the SIPROTEC 5 device via DNP3.

The SIPROTEC 5 device supports 2 DNP3 Ethernet masters on the same Ethernet module. You can click **Add new master** to add a new master in DIGSI.



[sc_DNP3EthernetSettings, 1, en_US]

Figure 3-8 DNP3 Ethernet Settings

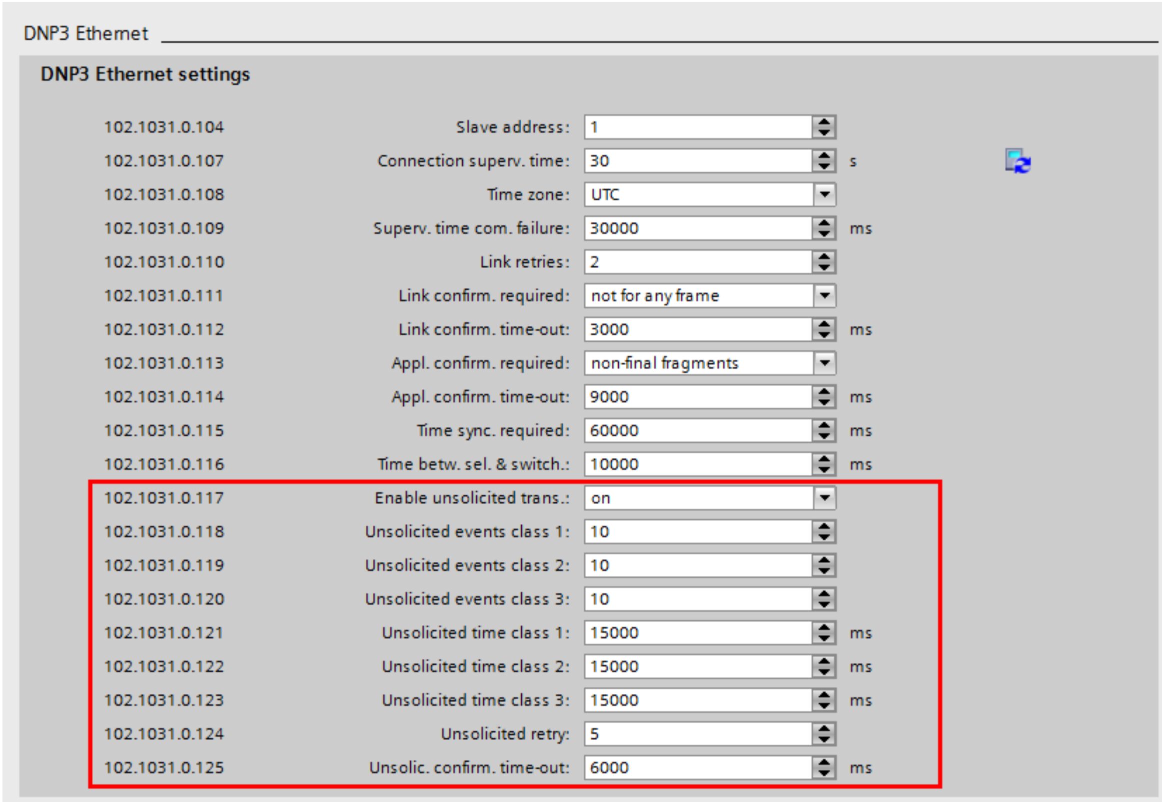


[sc_DNP3EthernetSettingsMaster2Added, 1, en_US]

Figure 3-9 DNP3 Ethernet Settings with 2nd Master

Parameter Name	Description	Settings
Slave address	Link address of the SIPROTEC 5 device	Setting range = 1 to 61 439 Default setting = 1
Connection superv. time	Time monitoring setting	Setting range: 0 s to 61 439 s Default setting = 30 s
Time zone	Time zone of the DNP3 device (must be the same as the time zone of the SIPROTEC 5 device)	UTC (default setting) Local
Superv. time com.failure	If no communication with a master occurs in the parameterized time, an error message is issued.	Setting range = 0 ms to 3 600 000 ms Default setting = 30 000 ms
Link retries	The number of transmission attempts (LinkRetries) If the receiver did not send a confirmation, a data package is transmitted again.	Setting: Sending with confirmation Default setting = 2
Link confirm. required	The receiver is asked to send a confirmation of the required packages.	Not for any frame (default setting) Multiframe fragment All frames

Parameter Name	Description	Settings
Link confirm. time-out	The parameter **Link confirm. time-out** specifies a time interval. During this time interval (in ms), the receiver waits for a confirmation from the opposite end until the last telegram is repeated. This only happens, if the information has been sent with confirmation. The time starts after the last byte has been sent.	Default setting = 3000 ms
Appl. confirm. required	This parameter specifies when a confirmation of the application layer is required.	Event-data messages: If messages contain event data, then a confirmation of the application layer is required. Non-final fragments: If telegrams are divided into different fragments, a confirmation of the application layer is required except for the last fragment, then a confirmation of the application layer is required (default setting).
Appl. confirm. time-out	The receiver waits during a desired period of time (in ms) until the previous response is confirmed. If the confirmation of the application layer is used together with the link confirmation, then make sure that the time-out of the application layer (AppConTime-out) is long enough to end all transmissions. The following formula describes this requirement: AppConTime-out > LinkConTime-out * (Link retries + 1)	Default setting = 9000 ms
Time sync. required	Time interval (in ms) until the internal display **Time required** is set. This time interval is included in every response message. The time interval signals to the master to start a new time synchronization with the device.	0 = The internal display is never set. Default setting = 60 000 ms
Time betw. sel. & switch.	A command must be selected and executed in this time (in ms).	Default setting = 10 000 ms
Enable unsolicited trans.	With this parameter, you specify whether unsolicited transmission is configured.	Off = The unsolicited transmission is not configured and can never be switched on from a connected master (default setting). On = The unsolicited transmission is configured and must be made possible after the 1st unsolicited response from the master.
Master address	Address of the DNP3 master	Setting range = 1 to 61 439 Default setting = 10
Master IP address	IP address of the DNP3 master IPv4 address 0.0.0.0 means that the slave can listen to and contact every IP address.	Setting range = 0.0.0.0 to 255.255.255.255 Default setting = 0.0.0.0
Port	Port number in the range of 1 to 61 439	Default setting = 20 000



[sc_DNP3EthernetSettings_On, 1, en_US]

Figure 3-10 DNP3 Ethernet Settings - When the Setting **Enable unsolicited trans.** Is on

NOTE

The **Master address** of each DNP3 master must be unique.

The combination of **Port** and **Master address** must be unique.

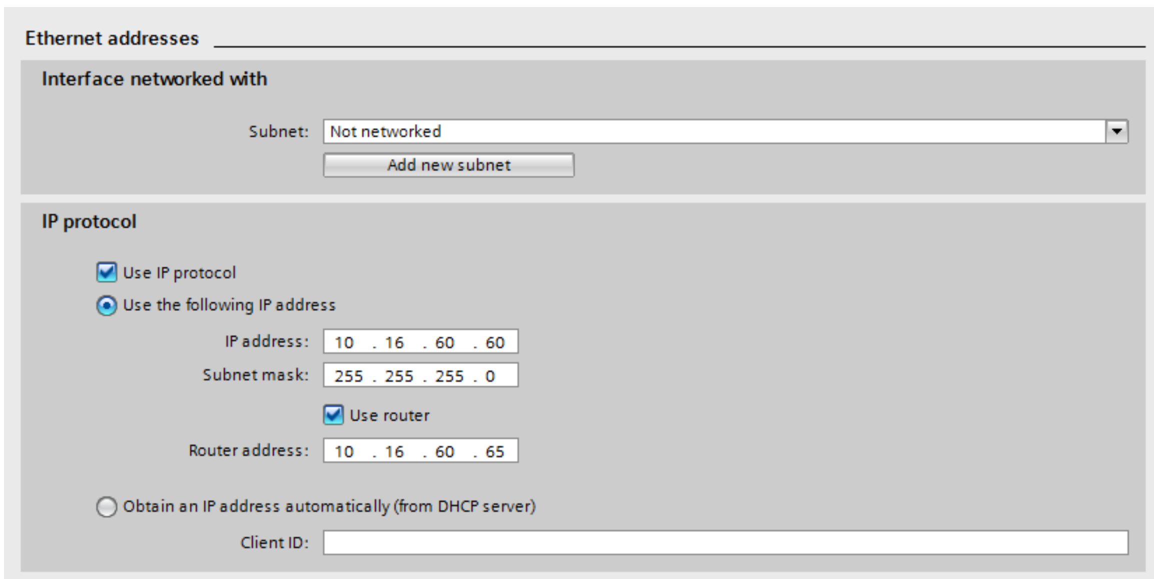
When either of the DNP3 master IP addresses is 0.0.0.0, the **Port** must be unique.

The following parameters only make sense if the parameter **Enable unsolicited trans.** is set to *on*:

Parameter Name	Description	Settings
Unsolicited events class 1/2/3	This parameter regulates a condition of the non-requested transmission for every class of changed events (class 1, class 2, and class 3). If the number of events per class equals or exceeds this value, then an unsolicited response is sent.	Default setting = 10
Unsolicited time class 1/2/3	This parameter regulates a condition of the non-requested transmission for every class of changed events (class 1, class 2, and class 3). If the time (in ms) after an event equals or exceeds this value, an unsolicited response is transmitted. The unsolicited message is also sent if only 1 event occurred.	Default setting = 15 000 ms

Parameter Name	Description	Settings
Unsolicited retry	If no unsolicited response was sent within the **Unsolicited confirm. time-out** parameter, then this parameter regulates how many times a different unsolicited response should be sent.	Default setting = 5
Unsolic. confirm. time-out	Time (in ms) for waiting for the receiver to confirm the non-requested response. If a query to read is received in the meantime, the read query is answered first, and then the unsolicited response is not transmitted.	Default setting = 6000 ms

The other required IP settings are taken from the module setting.



[sc_ethset, 1, en_US]

Figure 3-11 IP Settings in the Module Setting

4 IEC 60870-5-104

4.1 Protocol Characteristics

4.1.1 Description

The protocol IEC 60870-5-104 is structured as shown in the following *Table 4-1*.

Table 4-1 Protocol Structure

Selection of application functions of IEC 60870-5-5 according to IEC 60870-5-101	Initialization	User process
Selection of ASDUs (Application Service Data Unit) from IEC 60870-5-101 and IEC 60870-5-104		Application layer (layer 7)
APCI (Application Protocol Control Information) Transport interface		
Selection of TCP/IP protocol suite (RFC 2200)		Transport layer (layer 4)
		Network layer (layer 3)
		Data-link layer (layer 2)
		Physical layer (layer 1)
NOTE: Layer 5 and 6 are not used		

4.1.2 Selection of the TCP/IP Protocol Suite

As you know, IEC 60870-5-104 is a protocol based on TCP/IP (Transfer Control Protocol / Internet Protocol). *Table 4-2* shows the recommended selection of the TCP/IP protocol suite (RFC 2200) used in this standard. The relevant RFCs (Request For Comments) are available at the Internet address http://www.ietf.org.

Table 4-2 Selected Standard Provisions of the TCP/IP Protocol Suite RFC 2200

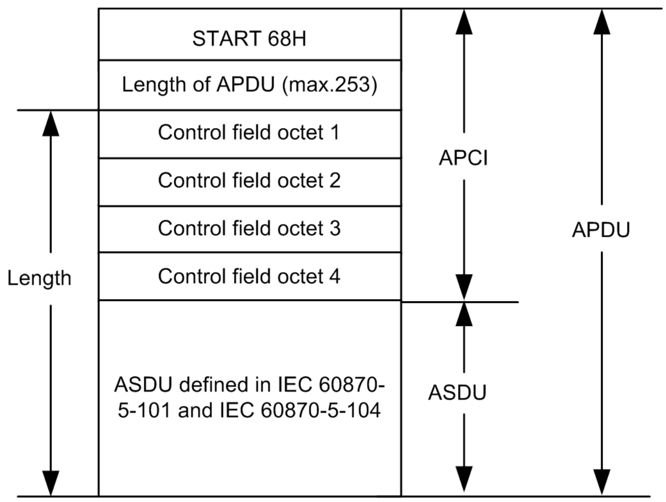
RFC 793 (Transmission control protocol)		Transport layer (layer 4)
RFC 791 (Internet protocol)		Network layer (layer 3)
RFC 1661 (Peer-Peer Protocol)	RFC 894 (Transmission of IP datagrams over Ethernet networks)	Data-link layer (layer 2)
RFC 1662 (Peer-Peer Protocol in high-level data link control-like framing)		
X.21	IEEE (Institute of Electrical and Electronics Engineers) 802.3	Physical layer (layer 1)
Serial line	Ethernet	

4.1.3 Definition of Application Protocol Control Information

The transport interface is a stream-oriented interface which does not define any start or stop mechanism for the ASDUs of IEC 60870-5-101. In order to detect the start and end of the ASDUs, each APCI includes the following delimiting elements, see *Figure 4-1*.

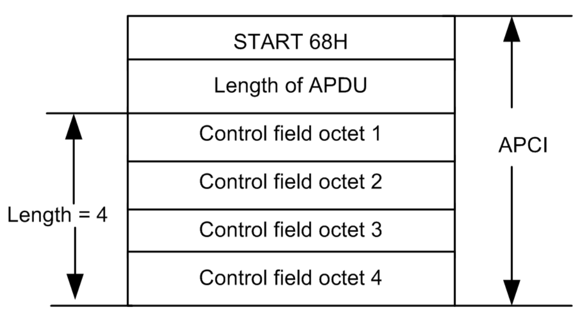
- A start character
- The specification of the length of the ASDU
- The control field

Either only the APCI field for control purpose or a complete APDU can be transferred, see *Figure 4-2*.



[sc_APDU-defined-telecontrol-comp-standard, 1, --_--]

Figure 4-1 APDU Definition



[sc_APCI-defined-telecontrol-comp-standard, 1, --_--]

Figure 4-2 APCI Definition

For more detailed information, refer to chapter 5 of the standard of Part 5-104:
Transmission protocols – Network access for IEC 60870-5-101 using standard transport profiles.

4.1.4 Selection of ASDUs

The ASDUs defined in IEC 60870-5-101 and in chapter 8 of the standard of IEC 60870-5-104 (Ed_2_57_812e_FDIS) are valid. Refer to the standards for detailed information. For the ASDUs supported in SIPROTEC 5, refer to the following tables.

Table 4-3 Process Information in Monitoring Direction

Type Identification (TI) :=	UIB[1..8]<0..38>	Abbreviation
<1> :=	Single-point indication	M_SP_NA_1
<3> :=	Double-point indication	M_DP_NA_1
<5> :=	Step-position indication	M_ST_NA_1
<7> :=	Bit string of 32 bits	M_BO_NA_1
<13> :=	Measured-value, short floating-point number	M_ME_NC_1
<15> :=	Integrated totals	M_IT_NA_1
<30> :=	Single-point information with time stamp CP56Time2a	M_SP_TB_1
<31> :=	Double-point information with time stamp CP56Time2a	M_DP_TB_1

<32> :=	Step-position information with time stamp CP56Time2a	M_ST_TB_1
<36> :=	Measured-value, short floating-point number with time stamp CP56Time2a	M_ME_TF_1
<37> :=	Integrated totals with time stamp CP56Time2a	M_IT_TB_1
<38> :=	Event of protection equipment with time stamp CP56Time2a	M_EP_TD_1

Table 4-4 Process Information in Control Direction

Type Identification (TI) :=	UI8[1..8]<45..47,50>	Abbreviation
<45> :=	Single command	C_SC_NA_1
<46> :=	Double command	C_DC_NA_1
<47> :=	Regulating step command	C_RC_NA_1
<50> :=	Set point command, short floating-point number	C_SE_NC_1

Table 4-5 System Information in Control Direction

Type Identification :=	UIB[1..8]<100..105>	Abbreviation
<100> :=	Interrogation command	C_IC_NA_1
<101> :=	Counter interrogation command	C_CI_NA_1
<102> :=	Read command	C_RD_NA_1
<103> :=	Time-synchronization command	C_CS_NA_1

Table 4-6 File Transfer

Type Identification (TI) :=	UIB[1..8]<120..126>	Abbreviation
<120> :=	File ready	F_FR_NA_1
<121> :=	Section ready	F_SR_NA_1
<122> :=	Call directory, select file, call file, call section	F_SC_NA_1
<123> :=	Last section, last segment	F_LS_NA_1
<124> :=	Acknowledge file, acknowledge section	F_AF_NA_1
<125> :=	Segment	F_SG_NA_1
<126> :=	Directory	F_DR_TA_1

4.1.5 Redundancy

4.1.5.1 General

SIPROTEC 5 supports multiple master groups. Multiple master groups can increase the availability of the communications system. Only 1 communication module supports the IEC 60870-5-104 protocol in the device at one time.

Each master group can be an independent redundancy group as follows:

- Only 1 active main master and 1 backup master connected to the slave (SIPROTEC 5 device)
- Only test telegrams between the backup master and the slave

If a communication network implements redundancy, the selected redundant bus topology is always a combination of the following redundancies:

- Master redundancy
- Media redundancy

The 2 redundancies can be combined flexibly with each other. Therefore, there can be different bus and redundancy topologies.

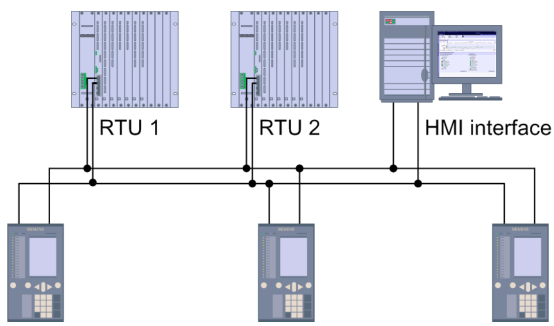
A communications system which includes both master and media redundancies is designated as a redundant system. If there is an interruption of the cables or disconnection of the main master, the redundant system can take over the work of the interrupted component.

4.1.5.2 Parameterization of a Redundant Communication

Media Redundancy

Media redundancy is the redundancy of the electrical or fiber-optic cable bus media and can be implemented, for example, with the PRP protocol.

The following figure shows that an RTU communicates with a SIPROTEC 5 device via 2 cables. If the RTU or SIPROTEC 5 device identifies an interruption in one cable, it can automatically switch to the other cable.



[dw_T104MediaRedundancy, 1, en_US]

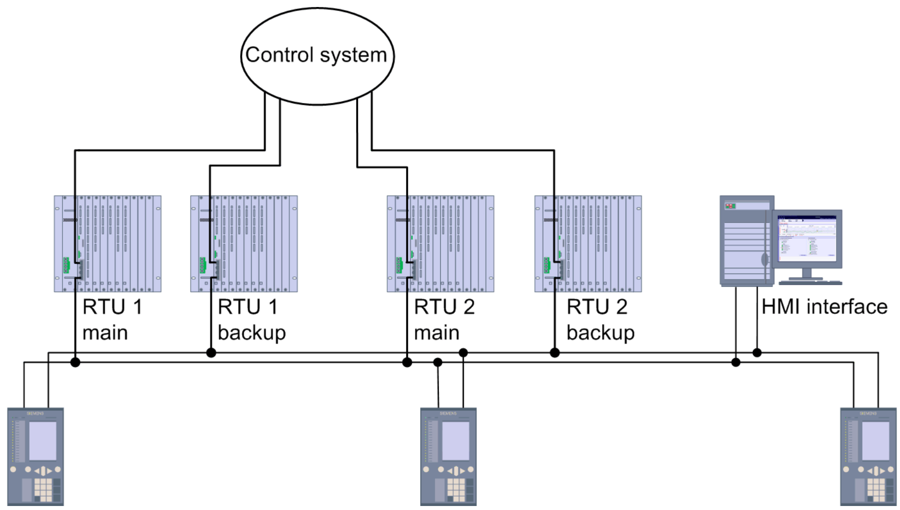
Figure 4-3 Media Redundancy

Master Redundancy

Master redundancy protects against a disconnection of the main master.

If the parameter **Redundancy** is on, a master redundancy is enabled. One master becomes the main master while the other master is the backup master. You can find detailed configuration information in chapter *4.2.1 Settings*. Both of the masters communicate with the SIPROTEC 5 device. The main master transmits the process data, and the backup master only transmits the test telegram.

If a disconnection of the main master occurs during ongoing operation, the backup master becomes the main master. The action can also be executed with an IEC 60870-5-104 command.



[dw_T104MasterRedundancy, 1, en_US]

Figure 4-4 Master Redundancy

You must set several parameters for a redundant communication in SIPROTEC 5. You can find more information on the settings in chapter *4.2.1 Settings*.

4.1.5.3 Redundancy in SIPROTEC 5

The following table shows several scenarios of master IP configuration when there is only 1 master.

Table 4-7 Scenarios of Master IP Configuration for 1 Master

Redundancy Disable/Enable	IP-Address Setting		Action
Redundancy is disabled (Port number is 2404)	Main master IP	0.0.0.0 (by default)	Any IEC 60870-5-104 master can communicate with the device.
	Main master IP	192.168.0.12 (for example)	Only the main master with the fixed IP can communicate with the device.
Redundancy is enabled (Port number is 2404)	Main master IP	192.168.0.11 (for example)	Only the main master and the backup master can communicate with the device. The main master and the backup master can only communicate with the device via port 2404. The IP address 0.0.0.0 is invalid.
	Backup master IP	192.168.0.12 (for example)	

The following table shows the scenarios of master IP configuration when there are more than 1 master.

Table 4-8 Scenarios of Master IP Configuration for More Than 1 Master

Redundancy Disable/Enable	IP-Address Setting		Action
Redundancy is disabled (Port number is 2404)	Main master IP	192.168.0.11 (for example)	Only the main master and the backup master can communicate with the device. The main master and the backup master can only communicate with the device via port 2404. The IP address 0.0.0.0 is invalid.
	Backup master IP	192.168.0.12 (for example)	
Redundancy is enabled (Port number is 2404)	Main master IP	192.168.0.11 (for example)	
	Backup master IP	192.168.0.12 (for example)	

4.1.6 File Operation for Fault Record

In IEC 60870-5-104, the disturbance data are transferred as a COMTRADE file via file transfer.

The SIPROTEC 5 device supports COMTRADE 1999 and COMTRADE 2013. You can change the COMTRADE revision with the parameter **`COMTRADE revision year`**.

- For COMTRADE 1999, a maximum of 8 pairs of the latest COMTRADE files (8 *.cfg and 8 *.dat files, 16 files in total) is available in the communication module.
- For COMTRADE 2013, a maximum of 8 pairs of the latest COMTRADE files (8 *.cfg, 8 *.dat, 8 *.inf, and 8 *.hdr files, 32 files in total) is available in the communication module.

NOTE

The maximum size of the fault record file is 4.8 MB. If the maximum size is exceeded, the file transfer via IEC 60870-5-104 does not succeed.

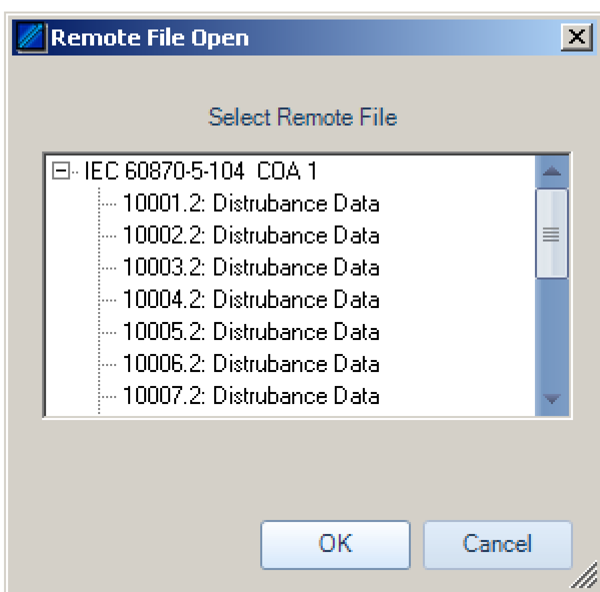
The .dat file is the largest of the COMTRADE files. You can calculate the file size of the .dat file with the following formula:

FileSize = [10 bytes + (NumberOfAnalogChannels) · 2 bytes + (NumberOfBinaryChannels/8) · 1 byte] · SamplingFrequency · RecordingTime

You can read the fault-record directory via IOA = 10000.

For file operation, proceed as follows:

- The IEC 60870-5-104 master sends a call directory command. The slave responds to this command and shows all the disturbance-data files.
- The IEC 60870-5-104 master confirms the selected file. The transmission proceeds.



[File List, 1, --_--]

Figure 4-5 File List for COMTRADE 1999

NOTE

COMTRADE 1999 supports at maximum 16 files (8 *.cfg and 8 *.dat files). The files start from 10001 to 10032. The latest file overwrites the eldest one.

The following example is based on COMTRADE 1999:

- 10001, 10005, ..., and 10029 are saved as *.cfg files (configuration file).
- 10004, 10008, ..., and 10032 are saved as *.dat files (data file).
- 10029 and 10032 are always the latest files.
- 10001 and 10004, 10005 and 10008, ..., 10029 and 10032 are combined as 1 complete COMTRADE file.
- 10001 to 10032 are reserved for file transfer, which is not configured to IEC 60870-5-104 for other purposes.

NOTE

COMTRADE 2013 supports at maximum 32 files (8 *.cfg, 8 *.dat, 8 *.inf, and 8 *.hdr files). The files start from 10001 to 10032. The latest file overwrites the eldest one.

The following example is based on COMTRADE 2013:

- 10001, 10005, ..., and 10029 are saved as *.cfg files (configuration file).
- 10002, 10006, ..., and 10030 are saved as *.dat files (data file).
- 10003, 10007, ..., and 10031 are saved as *.inf files (information file).
- 10004, 10008, ..., and 10032 are saved as *.hdr files (header file).
- 10029, 10030, 10031, and 10032 are always the latest files.
- 10001, 10002, 10003, and 10004, ..., 10029, 10030, 10031, and 10032 are combined as 1 complete COMTRADE file.
- 10001 to 10032 are reserved for file transfer, which is not configured to IEC 60870-5-104 for other purposes.

After the transmission is finished, the IEC 60870-5-104 master sends an acknowledgment request to the device.

4.1.7 Amount of Mappable Information

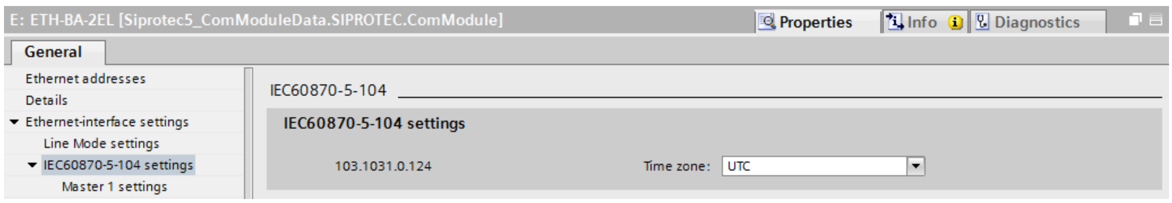
The following information may be mapped:

Information	**Maximum Mappable Amount**
Indication + Controllable at Tx(Tx: transfer direction)	500
Controllable at Rx (Rx: receive direction)	50
Settings at Tx	Settings via IEC 60870-5-104 is not supported
Measurements at Tx	100
Counters at Tx	20

4.2 Settings and Properties

4.2.1 Settings

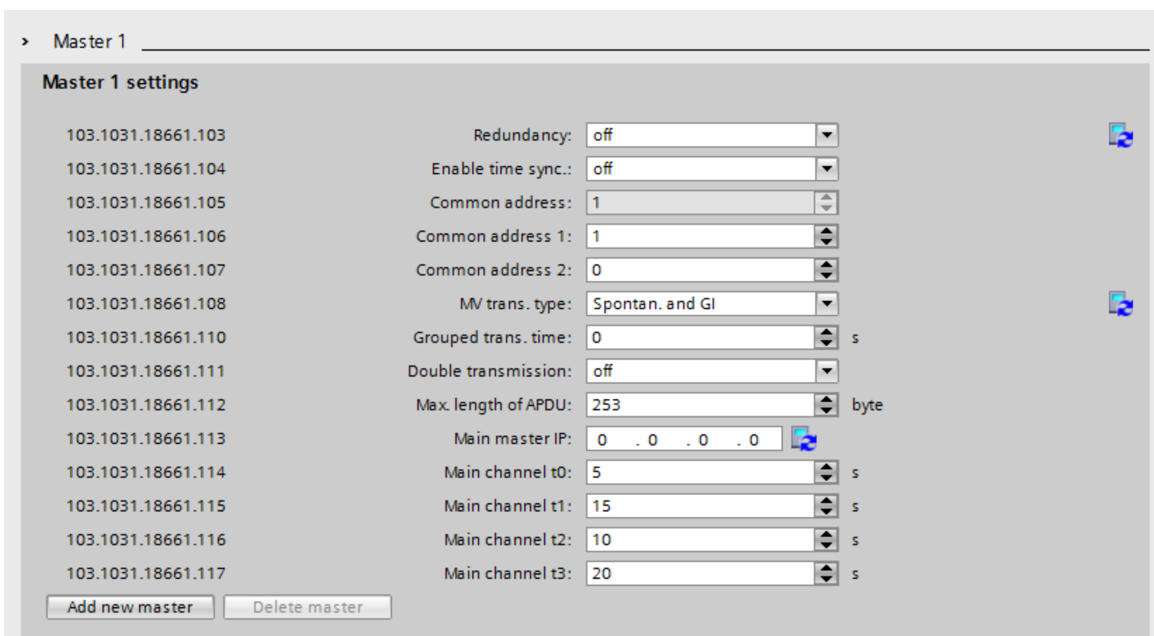
During the parameterization, make the following settings for the communication between the controlling station and the SIPROTEC 5 device via IEC 60870-5-104.



[sc_T104 general setting, 1, en_US]

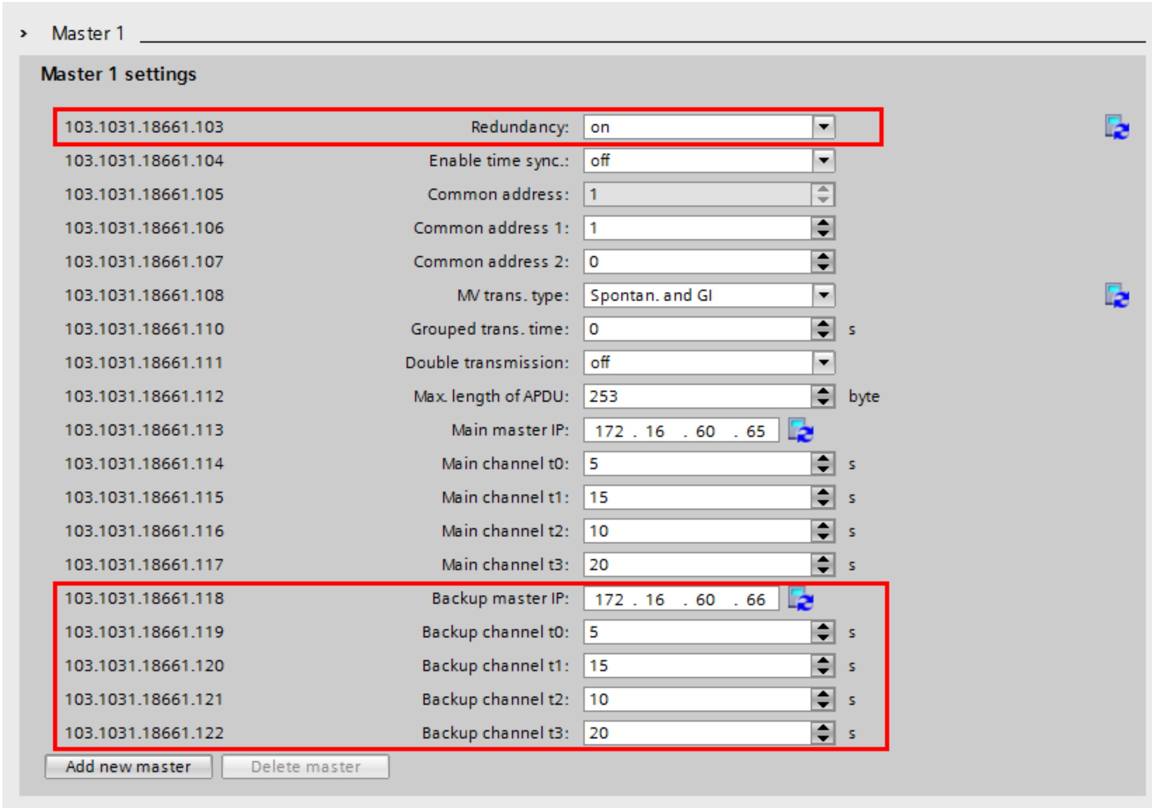
Figure 4-6 IEC 60870-5-104 General Setting

IEC 60870-5-104 supports a maximum of 3 masters with redundancy. The 3 masters have the same mapping and setting configurations. The following screenshots show the master 1 as an example. You can add a maximum of 3 masters in DIGSI 5.



[sc_T104 master setting default, 1, en_US]

Figure 4-7 IEC 60870-5-104 Master Settings – the Parameter **Redundancy** Is off



[sc_T104 master settings redundancy, 1, en_US]

Figure 4-8 IEC 60870-5-104 Master Settings – the Parameter **Redundancy** Is on

The following table shows the setting notes of master 1 as an example.

Parameter Name	Type	Description	Settings
Time zone	UTC/Local	Time zone of IEC 60870-5-104. The time zone has to be the same as the time zone of the SIPROTEC 5 device.	Standard setting = UTC
Redundancy	On/Off	When redundancy is off, all settings for the backup master are ignored.	Standard setting = Off
Enable time sync.	On/Off	Determines whether the SIPROTEC 5 device expects and evaluates time synchronization from the IEC 60870-5-104 master.	Standard setting = Off
Common address	Uint16	IEC 60870-5-104 station address of the SIPROTEC 5 device	Permitted range: 1 to 65 535 Standard setting = 1
Common address 1	Int8	IEC 60870-5-104 station address of the SIPROTEC 5 device	Permitted range: 0 to 255 Standard setting = 1
Common address 2	Int8	IEC 60870-5-104 station address of the SIPROTEC 5 device	Permitted range: 0 to 255 Standard setting = 0
MV trans. type	Enum	Selection of the measured-values transmission type	• Spontan.only • Cyclic only • Spontan. and GI (standard setting) • Spontan. and cyclic • All

Parameter Name	Type	Description	Settings
Cycle time	Int16	Time for sending cyclic data. Relevant if **Cyclic only**.	Permitted range: 1 s to 65 535 s Standard setting = 60 s
Grouped trans. time	Int16	The time for measurement transmission as a group. Single changes of measurements are stored and commonly sent out after this time. Reduce of required bandwidth. 0 = deactivate group transmission	Permitted range: 0 s to 10 s Standard setting = 0 s
Double transmisson	On/Off	Sends indications with or without time stamp. If double transmission is switched *On*, the indication is sent twice to the Master. Once with the time stamp and once without time stamp.	Standard setting = Off
Max. length of APDU	Int16	Maximum length of APDU (application protocol data unit) per master in the monitoring direction	Permitted range: 25 to 253 bytes Standard setting = 253 bytes
Main master IP	Int32	• When redundancy is disabled and there is only 1 master: Ipv4 address 0.0.0.0 means that the slave can listen and contact every IP address. • When redundancy is disabled and there are 2 or 3 masters: Ipv4 address cannot be 0.0.0.0 or cannot be the same as the backup master IP. • When redundancy is enabled: Ipv4 address cannot be 0.0.0.0 or cannot be the same as the backup master IP.	Permitted range: 0.0.0.0 to 255.255.255.255 Standard setting = 0.0.0.0
Main channel t0	Int16	Connection establishment time-out	Permitted range: 1 s to 255 s Standard setting = 30 s
Main channel t1	Int16	ASDU reply time-out	Permitted range: 1 s to 255 s Standard setting = 15 s
Main channel t2	Int16	Wait next information transmission frame (I frame) time-out. t2 < t1	Permitted range: 1 s to 255 s Standard setting = 10 s
Main channel t3	Int16	Idle time-out	Permitted range: 1 s to 255 s Standard setting = 20 s
Backup master IP	Int32	Ipv4 address cannot be 0.0.0.0 or be the same as the main master IP.	Permitted range: 0.0.0.0 to 255.255.255.255 Standard setting = 0.0.0.0
Backup channel t0	Int16	Connection establishment time-out	Permitted range: 1 s to 255 s Standard setting = 5 s
Backup channel t1	Int16	ASDU reply time-out	Permitted range: 1 s to 255 s Standard setting = 15 s
Backup channel t2	Int16	Wait next information transmission frame (I frame) time-out. t2 < t1	Permitted range: 1 s to 255 s Standard setting = 10 s
Backup channel t3	Int16	Idle time-out	Permitted range: 1 s to 255 s Standard setting = 20 s

4.3 Interoperability

4.3.1 Overview

This chapter is for IEC 60870-5-104 experts and is not translated to other languages. It contains an interoperability list for the functions supported by IEC 60870-5-104.

This companion standard presents sets of parameters and alternatives from which subsets must be selected to implement particular telecontrol systems. Certain parameter values, such as the choice of “structured“ or “unstructured“ fields of the INFORMATION OBJECT ADDRESS of ASDUs represent mutually exclusive alternatives. This means that only one value of the defined parameters is admitted per system. Other parameters, such as the listed set of different process information in command and in monitor direction allow the specification of the complete set or subsets, as appropriate for given applications. This clause summarizes the parameters of the previous clauses to facilitate a suitable selection for a specific application. If a system is composed of equipment stemming from different manufacturers, it is necessary that all partners agree on the selected parameters.

The interoperability list is defined as in IEC 60870-5-101 and extended with parameters used in this standard. The text descriptions of parameters which are not applicable to this companion standard are strike-through (corresponding check box is marked black).

Note: In addition, the full specification of a system may require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

☐ Function or ASDU is not used

[X] Function or ASDU is used as standardized (default)

[R] Function or ASDU is used in reverse mode

[B] Function or ASDU is used in standard and reverse mode

The possible selection (blank, X, R, or B) is specified for each specific clause or parameter.

A black check box indicates that the option cannot be selected in this companion standard.

4.3.2 System or Device

(System parameter, indicate the station function by marking one of the following with **X**)

[X] Controlled station definition (Slave)

☐ System definition

☐ Controlling station definition (Master)

4.3.3 Network Configuration

4.3.3.1 Not Realized Features

(Network-specific parameter, all configurations that are used are to be marked **X**)

■	Point-to-point	■	Multipoint
■	Multiple point-to-point	■	Multipoint-star

4.3.4 Physical Layer

4.3.4.1 Not Realized Features

Transmission Speed (Control Direction)

Unbalanced interchange **Circuit V.24/V.28** **Standard**	**Unbalanced interchange** **Circuit V.24/V.28** **Recommended if >1 200bit/s**	**Balanced interchange** **Circuit X.24/X.27**
■ 100 bit/s	■ 2 400 bit/s	■ 2 400 bit/s
■ 200 bit/s	■ 4 800 bit/s	■ 4 800 bit/s
■ 300 bit/s	■ 9 600 bit/s	■ 9 600 bit/s
■ 600 bit/s		■ 19 200 bit/s
■ 1200 bit/s		■ 38 400 bit/s
		■ 56 000 bit/s
		■ 64 000 bit/s

Transmission Speed (Monitor Direction)

Unbalanced interchange **Circuit V.24/V.28** **Standard**	**Unbalanced interchange** **Circuit V.24/V.28** **Recommended if >1 200bit/s**	**Balanced interchange** **Circuit X.24/X.27**
■ 100 bit/s	■ 2 400 bit/s	■ 400 bit/s
■ 200 bit/s	■ 4 800 bit/s	■ 4 800 bit/s
■ 300 bit/s	■ 9 600 bit/s	■ 9 600 bit/s
■ 600 bit/s		■ 19 200 bit/s
■ 1 200 bit/s		■ 38 400 bit/s
		■ 56 000 bit/s
		■ 64 000 bit/s

4.3.5 Link Layer

4.3.5.1 Not Realized Features

(Network-specific parameter, all options that are used are marked **X**. Specify the maximum frame length. If a non-standard assignment of class 2 messages is implemented for unbalanced transmission, indicate the Type ID and COT of all messages assigned to class 2.)

Frame format FT 1.2, single character 1 and the fixed time-out interval are used exclusively in this companion standard.

Link Transmission Procedure	**Address Field of the Link**	**Frame Length**
■ Balanced transmission	■ Not present (balanced transmission only)	■ Maximum length L (number of octets)
■ Unbalanced transmission	■ One octet	
	■ Two octets	

Link Transmission Procedure	Address Field of the Link	Frame Length
	■ Structured	
	■ Unstructured	

When using an unbalanced link layer, the following ASDU types are returned in class 2 messages (low priority) with the indicated causes of transmission:

■ The standard assignment of ASDUs to class 2 messages is used as follows:

Type Identification	Cause of Transmission
9, 11, 13, 21	<1>

■ A special assignment of ASDUs to class 2 messages is used as follows:

Type Identification	Cause of Transmission
N.A.	N.A.

Note: (In response to a class 2 poll, a controlled station may respond with class 1 data when there is no class 2 data available).

4.3.6 Application Layer

Transmission Mode for Application Data

Mode 1 (Least significant octet first), as defined in clause 4.10 of IEC 60870-5-4, is used exclusively in this companion standard.

Common Address of ASDU

(System-specific parameter, all configurations that are used are to be marked **X**)

■ 1 octect (not supported)

☒ 2 octets

Information Object Address

(System-specific parameter, all configurations that are used are to be marked **X**)

■ 1 octet (not supported)

■ 2 octets (not supported)

☐ Structured

☐ Unstructured

☒ 3 octets

Cause of Transmission

(System-specific parameter, all configurations that are used are to be marked **X**)

■ 1 octet (not supported)

☒ 2 octets (with originator address) Originator address is set to 0 if not used

Length of APDU

(System-specific parameter, specify the maximum length of the APDU per system)

The maximum length of APDU for both directions is 253. It is a fixed system parameter

■ Maximum length of APDU per system in control direction (not supported)

■ Maximum length of APDU per system in monitor direction (not supported)

Selection of Standard ASDUs

Process Information in Monitor Direction

(Station-specific parameter, mark each Type ID **X** if it is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

[x]	<1> = Single-point information	M_SP_NA_1
■	<2> = Single-point information with time tag (not supported)	M_SP_TA_1
[x]	<3> = Double-point information	M_DP_NA_1
■	<4> = Double-point information with time tag (not supported)	M_DP_TA_1
[x]	<5> = Step position information	M_ST_NA_1
■	<6> = Step position information with time tag (not supported)	M_ST_TA_1
[ ]	<7> = Bitstring of 32 bit	M_BO_NA_1
■	<8> = Bitstring of 32 bit with time tag (not supported)	M_BO_TA_1
[x]	<9> = Measured value, normalized value	M_ME_NA_1
■	<10> = Measured value, normalized value with time tag (not supported)	M_ME_TA_1
[x]	<11> = Measured value, scaled value	M_ME_NB_1
■	<12> = Measured value, scaled value with time tag (not supported)	M_ME_TB_1
[x]	<13> = Measured value, short floating-point value	M_ME_NC_1
■	<14> = Measured value, short floating-point value with time tag (not supported)	M_ME_TC_1
[x]	<15> = Integrated totals	M_IT_NA_1
■	<16> = Integrated totals with time tag (not supported)	M_IT_TA_1
■	<17> = Event of protection equipment with time tag (not supported)	M_EP_TA_1
■	<18> = Packed start events of protection equipment with time tag (not supported)	M_EP_TB_1
■	<19> = Packed output circuit information of protection equipment with time tag (not supported)	M_EP_TC_1
[ ]	<20> = Packed single-point information with status change detection	M_SP_NA_1
[ ]	<21> = Measured value, normalized value without quality descriptor	M_ME_ND_1
[x]	<30> = Single-point information with time tag CP56Time2a	M_SP_TB_1
[x]	<31> = Double-point information with time tag CP56Time2a	M_DP_TB_1
[x]	<32> = Step position information with time tag CP56Time2a	M_ST_TB_1
[ ]	<33> = Bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
[x]	<34> = Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
[x]	<35> = Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
[x]	<36> = Measured value, short floating-point value with time tag CP56Time2a	M_ME_TF_1
[x]	<37> = Integrated totals with time tag CP56Time2a	M_IT_TB_1
[x]	<38> = Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
[ ]	<39> = Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
[ ]	<40> = Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

The ASDUs of the set from <30> to <40> are used.

Process Information in Control Direction

(Station-specific parameter, mark each Type ID **X** if it is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

☒	<45> = Single command	C_SC_NA_1
☒	<46> = Double command	C_DC_NA_1
☒	<47> = Regulating step command	C_RC_NA_1
☐	<48> = Set point command, normalized value	C_SE_NA_1
☒	<49> = Set point command, scaled value	C_SE_NB_1
☒	<50> = Set point command, short floating-point value	C_SE_NC_1
☐	<51> = Bitstring of 32 bit	C_BO_NA_1
☒	<58> = Single command with time tag CP56Time2a	C_SC_TA_1
☒	<59> = Double command with time tag CP56Time2a	C_DC_TA_1
☒	<60> = Incremental command with time tag CP56Time2a	C_RC_TA_1
☐	<61> = Set point command, normalized value with time tag CP56Time2a	C_SE_TA_1
☒	<62> = Set point command, scaled value with time tag CP56Time2a	C_SE_TB_1
☒	<63> = Set point command, short floating-point value with time tag CP56Time2a	C_SE_TC_1
☐	<64> = Bitstring of 32 bit with time tag CP56Time2a	C_BO_TA_1

Either the ASDUs of the set from <45> to <51> or of the set from <58> to <64> are used.

System Information in Monitor Direction

(Station-specific parameter, mark **X** if it is only used in the standard direction, **R** if only used in the reverse direction and **B** if used in both directions)

☒	<70> = End of initialization	M_EI_NA_1

System Information in Control Direction

(Station-specific parameter, mark each Type ID **X** if it is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

☒	<100> = Interrogation command	C_IC_NA_1
☒	<101> = Counter interrogation command	C_CI_NA_1
☒	<102> = Read command	C_RD_NA_1
☒	<103> = Clock synchronization command	C_CS_NA_1
■	<104> = Test command (not supported)	C_SE_NB_1
☐	<105> = Reset process command	C_RP_NA_1
■	<106> = Delay acquisition command (not supported)	C_CD_NA_1
☒	<107> = Test command with time tag CP56time2a	C_TS_TA_1

Parameter in Control Direction

(Station-specific parameter, mark each Type ID **X** if it is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

☐	<110> = Parameter of measured value, normalized value	P_ME_NA_1
☐	<111> = Parameter of measured value, scaled value	P_ME_NB_1

☐ <112> = Parameter of measured value, short floating-point value P_ME_NC_1

☐ <113> = Parameter activation P_AC_NA_1

File Transfer

(Station-specific parameter, mark each Type ID **X** if it is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

X	<120> = File ready	F_FR_NA_1
X	<121> = Section ready	F_SR_NA_1
X	<122> = Call directory, select file, call file, call section	F_SC_NA_1
X	<123> = Last section, last segment	F_LS_NA_1
X	<124> = Ack file, ack section	F_AF_NA_1
X	<125> = Segment	F_SG_NA_1
X	<126> = Directory {blank or X, only available in monitor (standard) direction}.	F_DR_TA_1

Type Identifier and Cause of Transmission Assignments

(Station-specific parameters)
Shaded boxes are not required.
Blank: functions or ASDU not used.
Mark Type Identification/Cause of transmission combinations:
X if only used in the standard direction
R if only used in the reverse direction
B if used in both directions

Type Identification		Cause of Transmission																			
		Periodic, cyclic	Background scan	Spontaneous	Initialized	Request or requested	Activation	Activation confirmation	Deactivation	Deactivation confirmation	Activation termination	Return info caused by a remote cmd	Return info caused by a local cmd	File transfer	Interrogated by group <number>	Request by group <n> counter request	Unknown type identification	Unknown cause of transmission	Unknown common address of ASDU	Unknown information object address
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47
<1>	M_SP_NA_1			X		X						X	X		X					
<3>	M_DP_NA_1			X		X						X	X		X					
<5>	M_ST_NA_1			X		X						X	X		X					
<7>	M_BO_NA_1																			
<9>	M_ME_NA_1	X		X		X									X					
<11>	M_ME_NB_1	X		X		X									X					
<13>	M_ME_NC_1	X		X		X									X					
<15>	M_IT_NA_1			X												X				
<20>	M_PS_NA_1																			
<21>	M_ME_ND_1																			
<30>	M_SP_TB_1			X								X	X							
<31>	M_DP_TB_1			X								X	X							
<32>	M_ST_TB_1			X								X	X							
<33>	M_BO_TB_1																			
<34>	M_ME_TD_1			X																
<35>	M_ME_TE_1			X																
<36>	M_ME_TF_1			X																
<37>	M_IT_TB_1			X																
<38>	M_EP_TD_1			X																
<39>	M_EP_TE_1																			
<40>	M_EP_TF_1																			
<45>	C_SC_NA_1						X	X	X	X	X						X	X	X	X
<46>	C_DC_NA_1						X	X	X	X	X						X	X	X	X
<47>	C_RC_NA_1						X	X	X	X	X						X	X	X	X
<48>	C_SE_NA_1																			
<49>	C_SE_NB_1						X	X	X	X	X						X	X	X	X
<50>	C_SE_NC_1						X	X	X	X	X						X	X	X	X
<58>	C_SC_TA_1						X	X	X	X	X						X	X	X	X
<59>	C_DC_TA_1						X	X	X	X	X						X	X	X	X
<60>	C_RC_TA_1						X	X	X	X	X						X	X	X	X
<61>	C_SE_TA_1																			
<62>	C_SE_TB_1						X	X	X	X	X						X	X	X	X
<63>	C_SE_TC_1						X	X	X	X	X						X	X	X	X
<70>	M_EI_NA_1*)				X															
<100>	C_IC_NA_1						X	X	X	X	X						X	X	X	
<101>	C_CI_NA_1						X	X			X						X	X	X	
<102>	C_RD_NA_1					X											X	X	X	
<103>	C_CS_NA_1			X			X	X									X	X	X	
<105>	C_RP_NA_1																			
<107>	C_TS_TA_1						X	X									X	X	X	X
<110>	P_ME_NA_1																			
<111>	P_ME_NB_1																			
<112>	P_ME_NC_1																			
<113>	P_AC_NA_1																			
<120>	F_FR_NA_1													X						
<121>	F_SR_NA_1													X						
<122>	F_SC_NA_1					X								X			X	X	X	
<123>	F_LS_NA_1													X						
<124>	F_AF_NA_1													X			X	X	X	
<125>	F_SG_NA_1													X			X	X	X	
<126>	F_DR_TA_1*)						X													

* Blank or X only

[sc_104 interoperbility table, 1, --_--]

Figure 4-9 Interoperability Table

4.3.7 Basic Application Functions

Station Initialization

(Station-specific parameter, mark **X** if function is used)

☒ Remote initialization

Cyclic Data Transmission

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

[x] Cyclic data transmission

Read Procedure

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

[x] Read procedure

Spontaneous Transmission

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

[x] Spontaneous transmission

Double Transmission of Information Objects With Cause of Transmission Spontaneous

(Station-specific parameter, mark each information type **X** where both a Type ID without time and corresponding Type ID with time are issued in response to a single spontaneous change of a monitored object)

The following type identifications may be transmitted in succession caused by a single status change of an information object. The particular information object addresses for which double transmission is enabled are defined in a project-specific list.

[ ] Single-point information M_SP_NA_1, M_SP_TA_1, M_SP_TB_1 and M_PS_NA_1

[ ] Double-point information M_DP_NA_1, M_DP_TA_1 and M_DP_TB_1

[ ] Step position information M_ST_NA_1, M_ST_TA_1 and M_ST_TB_1

[ ] Bitstring of 32 bit M_BO_NA_1, M_BO_TA_1 and M_BO_TB_1 (if defined for a specific project)

[ ] Measured value, normalized value M_ME_NA_1, M_ME_TA_1, M_ME_ND_1 and M_ME_TD_1

[ ] Measured value, scaled value M_ME_NB_1, M_ME_TB_1 and M_ME_TE_1

[ ] Measured value, short floating point number M_ME_NC_1, M_ME_TC_1 and M_ME_TF_1

Station Interrogation

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

Global:

[x] Global

Group:

(Information Object Addresses assigned to each group must be shown in a separate table)

[x] Group 1	[x] Group 7	[x] Group 13
[x] Group 2	[x] Group 8	[x] Group 14
[x] Group 3	[x] Group 9	[x] Group 15
[x] Group 4	[x] Group 10	[x] Group 16
[x] Group 5	[x] Group 11	
[x] Group 6	[x] Group 12	

Clock Synchronization

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

- [x] Clock synchronisation
- [ ] Day of week used
- [ ] RES1, GEN (time tag substituted/ not substituted) used
- [x] SU-bit (summertime) used

Command Transmission

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

- [x] Direct command transmission
- [ ] Direct set point command transmission
- [x] Select and execute command
- [ ] Select and execute set point command
- [ ] C_SE ACTTERM used
- [x] No additional definition
- [x] Short pulse duration (duration determined by a system parameter in the outstation)
- [x] Long pulse duration (duration determined by a system parameter in the outstation)
- [x] Persistent output
- [x] Supervision of maximum delay in command direction of commands and set point commands
- [Configurable] Maximum allowable delay of commands and set point commands

Transmission of Integrated Totals

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

- [ ] Mode A: Local freeze with spontaneous transmission
- [ ] Mode B: Local freeze with counter interrogation
- [ ] Mode C: Freeze and transmit by counter-interrogation commands
- [ ] Mode D: Freeze by counter-interrogation command, frozen values reported spontaneously

- [x] Counter read
- [ ] Counter freeze without reset
- [ ] Counter freeze with reset
- [x] Counter reset

- [x] General request counter
- [x] Request counter group 1
- [x] Request counter group 2
- [x] Request counter group 3
- [x] Request counter group 4

Parameter Loading

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

☐ Threshold value
☐ Smoothing factor
☐ Low limit for transmission of measured values
☐ High limit for transmission of measured values

Parameter Activation

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

☐ Act/deact of persistent cyclic or periodic transmission of the addressed object

Test Procedure

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

☐ Test procedure

File Transfer

(Station-specific parameter, mark **X** if function is used)

File transfer in monitor direction

☐ Transparent file
☒ Transmission of disturbance data of protection equipment
☐ Transmission of sequences of events
☐ Transmission of sequences of recorded analog

File transfer in control direction

☐ Transparent file

Background Scan

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

☐ Background scan

Acquisition of Transmission Delay

(Station-specific parameter, mark **X** if function is only used in the standard direction, **R** if only used in the reverse direction, and **B** if used in both directions)

■ Acquisition of transmission delay (not supported)

Definition of Time Outs

Parameter	Default Value	Remarks	Selected Value
t_0	30 s	Time-out of connection establishment	Fixed
t_1	15 s	Time-out of send or test APDUs	Configurable

Parameter	Default Value	Remarks	Selected Value
t_2	10 s	Time-out for acknowledges in case of no data messages $t_2<t_1$	Configurable
t_3	20 s	Time-out for sending test frames in case of a long idle state	Configurable

Maximum range of values for all time outs: 1 s to 255 s, accuracy 1 s

Maximum Number of Outstanding I Format APDUs K And Latest Acknowledge APDUs (w)

Parameter	Default Value	Remarks	Selected Value
k	12 APDUs	Maximum difference receive sequence number to send state variable	Fixed
w	8 APDUs	Latest acknowledge after receiving w I-format APDUs	Fixed

Maximum range of values k: 1 to 32767 (2^{15}-1) APDUs, accuracy 1 APDU

Maximum range of values w: 1 to 32767 APDUs, accuracy 1 APDU (Recommendation: w should not exceed two-thirds of k).

Portnumber

Parameter	Value	Remarks
Port number	2404	Fixed

Redundant Connections

1 Number N of redundancy group connections used

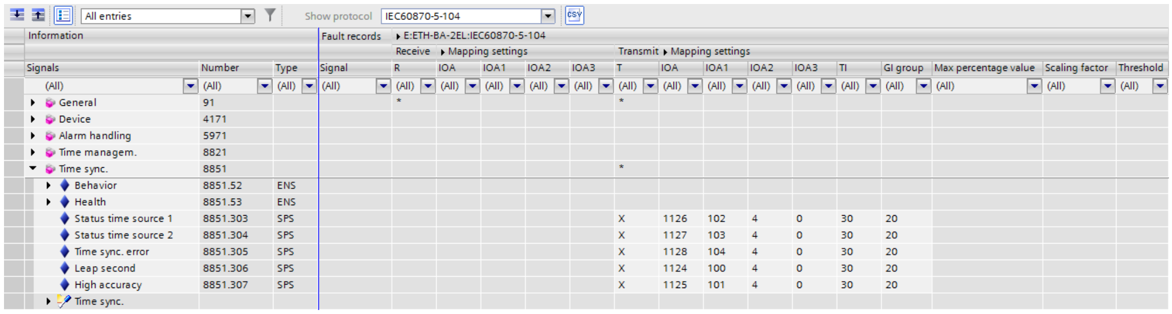
RFC 2200 Suite

RFC 2200 is an official Internet Standard which describes the state of standardization of protocols used in the Internet as determined by the Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used in the Internet. The suitable selection of documents from RFC 2200 defined in this standard for given projects has to be chosen by the user of this standard.

- [x] Ethernet 802.3
- [ ] Serial X.21 interface
- [ ] Other selection from RFC 2200

4.4 Communication Mapping

The following figure shows the IEC 60870-5-104 communication mapping of the 6MD device as an example.



[sc_T104 communication mapping, 1, en_US]

Figure 4-10   IEC 60870-5-104 Communication Mapping

The following table shows the details of the IEC 60870-5-104 communication mapping.

Table 4-9   IEC 60870-5-104 Communication Mapping

Mapping Settings	Type	Description	Permitted Ranges and Values
IOA	Uint24	Information Object Address of the information	Permitted range: 1 to 16 777 215
IOA 1	Uint8	The first byte of IOA, low byte	Permitted range: 0 to 255
IOA 2	Uint8	The second byte of IOA	Permitted range: 0 to 255
IOA 3	Uint8	The third byte of IOA, high byte	Permitted range: 0 to 255
TI	Uint8	Type identification	Permitted range: 1 to 126
GI group	Uint8	Data objects of general interrogation	Permitted range: 1 to 5; 20 to 36
MaxPercentageValue	Uint32	Maximum percentage value for measured values	Permitted value: 120 or 240
ScalingFactor	Uint8	Scaled factor for measured values	Permitted value: 1, 10, 100, or 1000
Threshold	Uint8	Threshold value of a measurement in %	Permitted range: 0 to 100

NOTE

You must configure the MV signals under WYE and DEL to the same TI. Otherwise, the measured value is not an expected value.

5 Modbus TCP

5.1 Protocol Characteristics

5.1.1 Exception Response of Modbus Slave

If the Modbus slave receives a command from the Modbus master which cannot be processed (for example, a request to read a non-existent register), then the slave answers with an exception-response message. The following table shows the exception codes that are signaled in an exception-response message to the Modbus master by the Modbus slave of the SIPROTEC device.

Table 5-1 Exception Response

Exception Code	Exception Response Message	Description
01	ILLEGAL_FUNCTION	The Modbus slave of the SIPROTEC device does not support the function code used in the query by the Modbus master.
02	ILLEGAL_DATA_ADDRESS	The register address is not configured in the Modbus slave.
03	ILLEGAL_DATA_VALUE	The Modbus master tries to write to a register with illegal data.

5.1.2 Supported Modbus Functions

The Modbus slave of the SIPROTEC 5 device supports the following Modbus functions:

Function Code	Function Name	Description	Broadcast Supported
1	Read Coil Status	Reading one or several coil-status registers of the Modbus slave. The coil-status registers reflect the ON/OFF status of discrete outputs of the SIPROTEC device.	no
2	Read Input Status	Reading one or several input-status registers of the Modbus slave. The input-status registers reflect the ON/OFF status of discrete inputs and the status of the protection function of the SIPROTEC device.	no
3	Read Holding Registers	Reading one or several holding registers of the Modbus slave. The holding registers contain device-status indications, measured values, mean values and metered measurand.	no
4	Read Input Registers	Reading one or several input registers of the Modbus slave. The input registers contain recorded measured values.	no
5	Force Single Coil	Writing (force to ON or OFF) one coil-status register.	no
15	Force Multiple Coils	Writing (force to ON or OFF) multiple coil-status registers	no
16	Preset Multiple Registers	Writing holding registers for APC (Controllable analog set point information).	no

5.1.3 Data Type Definition

5.1.3.1 Single-Point Indications: SPS, ACT, ACD, ENS

You can read single point indications by function code 1, 2, 3, or 4 via Modbus TCP. All these single point indications are CDC (Common Data Class) types defined in IEC 61850-7-3.

Different data structures are used with different function codes.

For more information, refer to the following tables:

Table 5-2 Reading SPS by Read Coil Status (FC1) or Read Input Status (FC2)

Bit x
Value

Table 5-3 Reading SPS by Read Holding Register (FC3) or Read Input Register (FC4)

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Validity	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Value

Values and **validity** in the preceding tables are described as follows:

Validity:	0 = Valid
	1 = Invalid
Range of values:	0 = Off
	1 = On

5.1.3.2 DPS

You can read double point indications, such as DPS (Double-point status), by function code 1, 2, 3, or 4 via Modbus TCP.

Different data structures are used with different function codes.

For more information, refer to the following tables:

Table 5-4 Reading DPS by Read Coil Status (FC1) or Read Input Status (FC2)

Bit x+1	Bit x
Value	

Table 5-5 Reading DPS by Read Holding Register (FC3) or Read Input Register (FC4)

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Validity	0	0	0	0	0	0	0	0	0	0	0	0	0	Value	

Values and **validity** in the preceding tables are described as follows:

Validity:	0 = Valid
	1 = Invalid
Range of values:	0 = Intermediate position
	1 = Off
	2 = On
	3 = Bad state

5.1.3.3 BSC (Monitoring Direction)

You can read BSC (Binary controlled step position information) by function code 3 or 4.

For more information, refer to the following tables:

Table 5-6 Valid BSC Value by Read Holding Register (FC3) or Input Register (FC4)

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	0	0	0	0	0	0	0	0	0	Value					

Range of values: 1 to 63 (normal operation value)

If the transformer-tap signals are not mapped to binary inputs in DIGSI, the BSC value is invalid (see *Table 5-7*). The value is -64 (0xFFC0).

Table 5-7 Invalid BSC Value

Bit 15	Bit 14	Bit 13	Bit 12	Bit 11	Bit 10	Bit 9	Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0

5.1.3.4 SPC

You can send Single Point Control (SPC) by function code 5.

Table 5-8 Sending SPC by Force Single Coil (FC5)

Bit x
Value

Range of values: 0 = Off
1 = On

5.1.3.5 BSC (Command Direction)

You can send BSC (Binary controlled step position information) by function code 5.

Table 5-9 Sending BSC by Force Single Coil (FC5)

Bit x
Value

Range of values: 0 = Lower
1 = Higher

5.1.3.6 DPC

You can send Double Point Control (DPC) by function code 15.

Table 5-10 Sending DPC by Force Multiple Coils (FC15)

Bit x+1	Bit x
Value	

Range of values: 0 = Not allowed
1 = Off
2 = On
3 = Not allowed

NOTE

Siemens recommends using 2 registers in the command from the master controlling. It means the quantity should be 2. All the other quantities are responded with exception code 02 (ILLEGAL_DATA_ADDRESS).

5.1.3.7 APC (Command Direction)

You can send APC (Controllable analog set point information) by function code 16.

Table 5-11 Sending APC by Preset Multiple Registers (FC16)

Holding Register x+1		Holding Register x	
Byte 3 (MSB:Most Significant Bit)	Byte 2	Byte 1	Byte 0 (LSB:Least Significant Bit)
Value			

Range of values (Integer 32): -2 147 483 648 to 2 147 483 647

NOTE

Siemens recommends using 2 registers in the command from the master controlling. It means the quantity should be 2. All the other quantities are responded with exception code 02 (ILLEGAL_DATA_ADDRESS).

5.1.3.8 MV, CMV, DEL, WYE

You can read measured values, such as MV (Measured Value), CMV (Complex Measured Value), DEL (Phase to phase related measured values of a three-phase system) and WYE (Phase to ground related measured values of a three-phase system), by function code 3 or 4.

Table 5-12 Reading MV by Read Holding Register (FC3) or Read Input Register (FC4)

Holding Register x+1		Holding Register x	
Byte 3 (MSB)	Byte 2	Byte 1	Byte 0 (LSB)
Value			

Range of values (Float 32): $-3.4 * 10^{38}$ to $3.4 * 10^{38}$
0 x 7F8000001 = NaN (Not a Number)

5.1.3.9 BCR

You can read counter values, such as Binary Counter Reading (BCR), by function code 3 or 4.

Table 5-13 Reading BCR by Read Holding Register (FC3) or Read Input Register (FC4)

Holding Register x+1		Holding Register x	
Byte 3 (MSB)	Byte 2	Byte 1	Byte 0 (LSB)
Value			

Range of values: -2 147 483 648[12] to 2 147 483 647

5.1.3.10 SOE

The complex data type **Message block** defines an entry in the event recorder. For further information regarding the properties and the retrieval methods of the event recorder, refer to chapter *5.2.1 Overview*.

Holding register xxxx	Register type	Bit offset
	Byte 1	Byte 2

Holding register xxxx+ 1	Register address	
	Byte 3 (MSB)	Byte 4 (LSB)

12 The minimum value -2 147 483 648 indicates that the value is not valid.

Holding register xxxx+ 2	Message cause	Indication type
	Byte 5	Byte 6

Holding register xxxx+ 3	Value	
	Byte 7 (MSB)	Byte 8 (LSB)

Holding register xxxx+ 4	Milliseconds (0 to 59999)	
	Byte 9 (MSB)	Byte 10 (LSB)

Holding register xxxx+ 5	Hours (0 to 23)	Minutes (0 to 59)
	Byte 11	Byte 12

Holding register xxxx+ 6	Month (1 = January to 12 = December)	Day (1 to 31)
	Byte 13	Byte 14

Holding register xxxx+ 7	Clock status	Year (0 = 1900)
	Byte 15	Byte 6

Byte 1 to 4: Identification

The first 4 bytes identify an indication and correspond to the parameters **`Register type`** and **`Register address`** selected in DIGSI 5.

Byte No.	Name	Values
Byte 1	Register Type	0 = Coil status register
		1 = Input status register
		4 = Holding register
Byte 2	Bit Offset	0
Byte 3	Register Address	Indication of the register address configured in DIGSI 5
Byte 4	Register Address	

Byte 5: Message Cause

Byte No.	Name	Values
Byte 5	Message Cause	0

Byte 6: Indication Type

Byte 6 describes the type of the information.

Table 5-14 Indication Type

	Indication Type							
Bit position	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Meaning	Reserved (= 0)				Information type (refer to *Table 5-15*)			

Table 5-15 Description of the Information Type (Bits 0 to 3)

$0001_{bin} = 1_{hex}$ for single-point indications
$0010_{bin} = 2_{hex}$ for double-point indications
$0011_{bin} = 3_{hex}$ for transformer-tap indications

5.1.3.11 Device Information

Modbus master can read the device information fixed in the SIPROTEC 5 device.

Item	Register Address	Description
IP address	4000 to 4001	Example: C0 A8 64 68 Means: 192.168.100.104
Net Mask	4002 to 4003	Example: FF FF FF 00 Means: 255.255.255.0
Gateway	4004 to 4005	Example: 00 00 00 00 Means: 0.0.0.0
MAC address	4006 to 4008	Example: 00 A0 1E A0 A0 11 Means: 00:A0:1E:A0:A0:11
Configuration Mode	4009 to 4010	Example: 02 00 00 00 Means: refer to *Table 5-16*
Configuration State	4011 to 4012	Example: 01 00 00 00 Means: refer to *Table 5-17*
DCP Enabled	4013	Example: 00 00 Means: DCP Disabled
BF Number	4014 to 4019	Example: 42 46 42 39 39 39 39 39 39 39 39 39 Means: BF999999999

Table 5-16 Description of the Configuration Mode

Value	Mode	Description
0	MODE_DISABLED	The interface is disabled for IP traffic, so it has no IP address.
1	MODE_UNKNOWN	If an error occurs, the mode is unknown.
2	MODE_STATIC	The interface is parameterized with a static IP address.
3	MODE_DHCP	The interface is parameterized via DHCP.

Table 5-17 Description of the Configuration State

Value	Mode	Description
0	STATE_IDLE	Until now, the interface is not parameterized.
1	STATE_CONFIGURED	The interface is configured with a reachable IP.
2	STATE_DISABLED	For IP communication, the interface is disabled.
3	STATE_PENDING	The interface is configured via DHCP, but the DHCP server is unreachable so far.
4	STATE_FAILED	For the IP interface, the IP configuration fails.
5	STATE_DUPLICATE	The interface is configured with a static IP, but the IP exists in the network.

5.1.3.12 Routing of the Data Types

The routing of some typical data types is explained in more detail below:

Table 5-18 Routing the Typical Data Types

Type	Address Range	Direction	CDC Type	Function Code	Register Quantity (RegisterAddr+1 Reservation)	Data Type in SICAM PAS
Indication	1 ~ 1000	Tx Monitor	SPS, ACT, ACD, ENS	1,2	1	SP_FC1 SP_FC2
				3,4	1	SP_INT16_FC3 SP_INT16_FC4
			DPS	1,2	2	DP_FC1 DP_FC2
				3,4	1	DP_ INT16_FC3 DP_ INT16_FC4
			BSC	3,4	1	ME_INT16_FC3 ME_INT16_FC4
Command	1001 ~ 1200	Rx Control	SPC	5	1	SC_FC5
			DPC	15	2	DC_FC15
			BSC	5	1	SC_FC5
			APC	16	2	SE_INT32_FC16
Measured value	2001 ~ 2200	Tx Monitor	MV, DEL, WYE	3,4	2	ME_F32_FC3 ME_F32_FC4
Metered value	3001 ~ 3020	Tx Monitor	BCR	3,4	2	IT_I32_FC3 IT_I32_FC4

NOTE

The measured and metered values in the preceding tables are saved in the Big Endian [13] format.

The SIPROTEC 5 device provides device information with the following parameters. The register addresses are specified. The Master can read all information with the function code 03.

You can find more information in chapter *5.1.3.11 Device Information*.

5.1.4 Amount of Mappable Information

The following information may be mapped:

Information	Maximum Mappable Amount
Indication + Controllable at Tx (Tx: transfer direction)	500
Controllable at Rx (Rx: receive direction)	50
Settings at Tx	Settings via Modbus TCP is not supported
Measurements at Tx	100
Counters at Tx	20

13 For Big-Endian systems, the greatest value byte of a word is saved at the lowest address. The byte with the least value is saved at the highest address.

5.1.5 Additional Information

NOTE

If the measured value or the metered value is 7F8000001, this means that the measured value is not a number (NaN - Not a Number).

If the measured value or the metered value is 7F800000, this means that an overflow of the measured value occurred.

If the measured value or the metered value is 80000000, this means that the measured value is invalid.

5.2 Sequence of Events

5.2.1 Overview

For SOE configuration in DIGSI 5, refer to chapter *Indications, Page 61*.

5.2.2 Properties of the Sequence of Event

The Modbus communication module has a sequence of event with entries of the type **Message block**. For more information, refer to chapter *5.1.3.10 SOE*.
A maximum number of 300 entries is allowed for SOE.

Characteristic

- The event recorder is a ring buffer.
- If buffer overflows, the current entry replaces the oldest entry.
  The Modbus master is informed about a buffer overflow with a bit in the handshake register **SOE_Control**. (refer to chapter *5.2.5 Handshake Mechanism*).
- Events of the type single-point indication, double-point indication, and the transformer-tap indications are accepted in the event recorder.
- When the object value changes, it is stored in the event record with a time stamp.
- After the device initiation or reboot, the event recorder is empty and then the startup values of the objects are entered in the event recorder.
- If the communication fails, the event buffer is not erased. Entries are still saved and the Modbus master reads the entries once the communication link is re-established (buffer overflow is indicated if necessary).
- The Modbus master reads the entries of the event recorder (Message blocks) via Holding registers. The entries must be acknowledged.
- After reading and acknowledging by the Modbus master, the transferred event recorder entries are deleted from the event buffer.

5.2.3 Structure Holding Registers for Event Recorder

5.2.3.1 Overview

This chapter describes the Holding registers for reading and acknowledging the event-recorder entries.
The range in the Holding registers for reading and acknowledging the event-recorder entries consists of the following:

- One register **No. of Event recorder entries** (read-only access)
- One handshake register **SOE_Control** (read/write access)
- 3 entries of the data type **Message block** (24 Holding registers in summary) for reading the event-recorder entries (read-only access).

Register Address	Designation	Comments
40601	No. of Event recorder entries	Number of event-recorder entries which are not read yet
40602	SOE_Control	Handshake register (read/write access)

Register Address	Designation	Comments
40603	Message block # 1	Register Type/Bit offset
40604		Register address
40605		Message cause/ Indication type
40606		Value
40607 to 406010		Time stamp
406011	Message block # 2	Register Type/ Bit offset
406012		Register address
406013		Message cause/ Indication type
406014		Value
406015 to 406018		Time stamp
406019	Message block # 3	Register Type/Bit offset
406020		Register address
406021		Message cause/Indication type
406022		Value
406023 to 406026		Time stamp

Detailed information about the **Time stamp** in the preceding table is defined in the following table.

Register 0		Register 1		Register 2		Register 3	
Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
Milliseconds		Hours	Minutes	Month	Day	Clock status	Year

NOTE

Only the following access to the event-recorders range in the Holding registers is permitted:

- **SOE_Control** (read/write)
- **SOE_Control** and **Message block # 1** (read-only)
- **SOE_Control**, **Message block # 1**, **Message block # 2**, and **Message block # 3** (read-only)

Additionally, the register **No. of Event recorder entries** can be read.

5.2.3.2 Register No. of Event Recorder Entries

The register **No. of Event recorder entries** contains the number of event-recorder entries in the event buffer and the Holding registers which are not read yet.

Range of values: 0 (no entry at present in the event recorder) to 300

If the 3 areas in the Holding registers for transmission of the message blocks contain message blocks for reading and if these were not given a receipt yet, these 3 areas count as event-recorder entries (in addition to the parameterized **No. of Event recorder entries**).

5.2.3.3 Handshake Register SOE_Control (Read Access)

The individual bits of the handshake register **SOE_Control** have for read access the meaning indicated in the following table. For detailed information about handshake mechanism, refer to chapter *5.2.5 Handshake Mechanism*

Table 5-19 Handshake Byte SOE_Control (Read Access)

	SOE_Control (Read Access / Out Direction)															
Bit Position	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Meaning	Buffer overflow	0	Reserved (= 0)				Number of Message blocks		Sequence number							

Sequence Number (Bits 0 to 7)

- With each transmission of **Message blocks** (entries from the event recorder, a maximum of 3 entries per query), the **Sequence number** increases sequentially by 1, starting with 1 (00000001_{bin}) up to 255 (11111111_{bin}) and thereafter starting with 1 again.
- Only during the initialization or reboot of the SIPROTEC device the **Sequence number** has the initial value 0. No entries are available in the event recorder yet. For transmission of the first entry, the **Sequence number** increases by 1 and then never assumes the value 0 again (unless another initialization start or reboot occurs).
- If no indication changes are to transmit during a number of master queries, the **Sequence number** remains unchanged during this time. The Modbus master then reads repeatedly the same last transmitted **Sequence number** until new entries in the event recorder come. The **Sequence number** increases by 1 when the new entry comes.

At the same time, the value of the **Sequence number** provides the acknowledgment that the Modbus master has evaluated the read entries by writing back the value of the Sequence number to the **SOE_Control** handshake register.

Number of Message Blocks (Bits 8 and 9)

There are 3 Message blocks for transmission of event-recorder entries available. The Number of **Message blocks** indicates how many of them contain valid entries.

If none or less than 3 events/entries are to transmit, then the Register type in the unused **Message blocks** has the value $FF_{hex} = 255_{dec}$.

Reserved (Bits 10 to 14)

The bits of the register **SOE_Control**in input direction indicated as *reserved* are not used now.

At these positions, the value = 0 is transmitted

Buffer Overflow (Bit 15)

A set bit indicates an overflow of the event buffer.

If no new buffer overflow occurs in the meantime, the bit **Buffer overflow** is reset after the acknowledgment of the current transmitted **Message blocks**.

5.2.3.4 Handshake Register SOE_Control (Write Access)

For write access, the individual bits of the handshake register **SOE_Control** have the meaning indicated in the following table. For detailed information about handshake mechanism, refer to chapter *5.2.5 Handshake Mechanism*.

Table 5-20 Handshake Byte SOE_Control (Write Access)

	SOE_Control (Write Access / Output Direction)															
Bit Position	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Meaning	Clear List	0	Reserved (= 0)				Number of Message blocks		Sequence number							

Sequence Number (Bits 0 to 7)

Acknowledgment of the reception is an evaluation of the read Message blocks.

The Modbus master reads **SOE_Control** and **Message block**. The master copies the **Sequence number** from the **SOE_Control** and writes it back into **SOE_Control** as a reception.

As long as the Modbus master mirrors back the **Sequence number** to the register**SOE_Control** in a faulty way, the contents (Message blocks) read in last time are given back in the following query.

If a **Sequence number** is given for a receipt, further write accesses (without a renewed read access) are only possible with the **Sequence number** read last or with Sequence number = 0.

The number of Message blocks is not evaluated at these write accesses.

An acknowledgment/write access with a faulty **Sequence number** (for example, unequal with the sequence number read) is answered with Modbus exception 03 (ILLEGAL_DATA_VALUE).

Write accesses with Sequence number = 0 are always possible.

Then only the command bit **Clear List** is evaluated. If the associated bit is set, the command is executed.

Number of Message Blocks (Bits 8 and 9)

Bit 8 and Bit 9 indicate the reception of the number of the read **Message blocks**.

Together with the valid Sequence number, the Modbus master tells the Modbus slave how many event-recorder entries, provided in the 3 Message blocks of the Holding registers, were read and evaluated.

Receipt Value in No. of Message Blocks	**Reaction**
Equal to 0	The present Message blocks are offered for reading. Furthermore, the Sequence number is incremented. If less than 3 Message blocks are offered when the Sequence number was read for the last time and further entries are entered in the Event recorder in the meantime, then a maximum of 3 Message blocks can be read.
Less than the value No. of Message blocks read from SOE_Control register	The number of message blocks in the receipt from the master indicates how many message blocks have been confirmed. The confirmed message blocks can be deleted in the event buffer. Not read Message blocks are moved up in the Holding registers range for Message blocks and the remaining Holding registers are filled with new entries from the event list for reading, if necessary. The Sequence number is incremented.

Receipt Value in No. of Message Blocks	Reaction
Equal to the value No. of Message blocks read from SOE_Control register	All read Message blocks are deleted from the event buffer. If there are further entries in the event recorder, then they are now offered for reading and the Sequence number is incremented.
Greater than the value No. of Message blocks read from SOE_Control register	The receipt value in No. of Message blocks is ignored. All read Message blocks are deleted from the event buffer. If there are further entries in the event recorder, then they are now offered for reading and the Sequence number is incremented.

Reserved (Bits 10 to 13)

The bits of the SOE_Control register in output direction indicated as *reserved* are not used now and are not evaluated by the Modbus slave. At these positions, the value = 0 is transferred.

Start GS (Bit 14)

Always 0

Clear List (Bit 15)

Setting the bit **Clear List** deletes the event recorder.

All entries in the event recorder are lost. The register **No. of Event recorder entries** is set to 0.

The Modbus master transfers the bit in 2 ways:

- Transfer the bit in the next receiption of read **Message block** to the Modbus slave
- Transfer the bit by writing **SOE_Control** with **Sequence number** = 0

Deleting the event recorder does not lead to a reset of the **Sequence number**. The next (incremented) **Sequence number** is used when the next **Message blocks** are to transmit.

The bit **Clear list** can be set to *1* by the Modbus master. That means, the Modbus slave can delete all the event recorders without reception from the Modbus master.

5.2.4 Message Blocks

The entries of the event recorder are transferred via the Holding registers (with a maximum of 3 **Message blocks** within one Modbus message).

The information in the handshake register **SOE_Control** shows how many **Message blocks** are offered for reading in the Holding registers.

The data type **Message block** is described in the chapter *5.1.3.1 Single-Point Indications: SPS, ACT, ACD, ENS* .

5.2.5 Handshake Mechanism

The Modbus master reads the register **SOE_Control** cyclically to determine, whether the event recorder contains entries.

An incremented **Sequence number** in the register **SOE_Control** indicates new entries which are ready for reading.

If new entries in the event recorder are recognized, the Modbus master reads the register **SOE_Control** again and with a maximum of 3 **Message blocks**.

The maximum number of **Message blocks** in the Holding registers is indicated in the **Number of Message blocks** of the previous read register **SOE_Control**. The Holding register contains valid data.

If **Message blocks** are already read during polling of **SOE_Control**, then they can be evaluated first.

After evaluation of the **Message blocks**, the Modbus master gives a receipt to the Modbus slave. The Modbus master gives the read **Sequence number** and the number of evaluated event-recorder entries back to the register **SOE_Control** .

If further entries have to be read, the Modbus slave deletes the read and evaluated entries from the event recorder and increments the **Sequence number**.

If a communication failure appears (for example, CRC error), then the master has to repeat the read access.

As long as no receipt is given with a write access to the register **SOE_Control** , event list data are not changed or deleted in the Holding registers .

The described mechanism of polling, reading, evaluating, and giving a receipt continues now .

If the register **No. of Event list entries** is read with the register **SOE_Control** simultaneously, then it can be estimated if and how many **Message blocks** are read with the next query to optimize read accesses.

5.2.6 Multi-Connection to Master via Modbus

5.2.6.1 General

SIPROTEC 5 supports multi-connection via Modbus as follows:

- Maximum 2 Modbus masters connect to the Modbus slave (SIPROTEC 5 device) simultaneoulsy.
- Only 1 communication module supports the Modbus protocol in the device.

5.2.6.2 Parameterization of the Multi-Communication

The following table shows several scenarios of the master IP configuration.

Configuration Scenario	IP-Address Setting		Action
1	Master IP address 1	0.0.0.0 (by default)	Any Modbus master can communicate with the SIPROTEC 5 device.
	Master IP address 2	0.0.0.0 (by default)	
2	Master IP address 1	0.0.0.0 (by default)	Only the Modbus master with the fixed IP address (for example, 192.168.0.12) can communicate with the SIPROTEC 5 device.
	Master IP address 2	192.168.0.12 (for example)	
3	Master IP address 1	192.168.0.11 (for example)	Only the Modbus master with the fixed IP address (for example, 192.168.0.11) can communicate with the SIPROTEC 5 device.
	Master IP address 2	0.0.0.0 (by default)	
4	Master IP address 1	192.168.0.11 (for example)	Only the Modbus master with the fixed IP address (for example, 192.168.0.11 or 192.168.0.12) can communicate with the SIPROTEC 5 device.
	Master IP address 2	192.168.0.12 (for example)	

NOTE

You can find a list of detailed settings in chapter *5.3.1 Settings*.

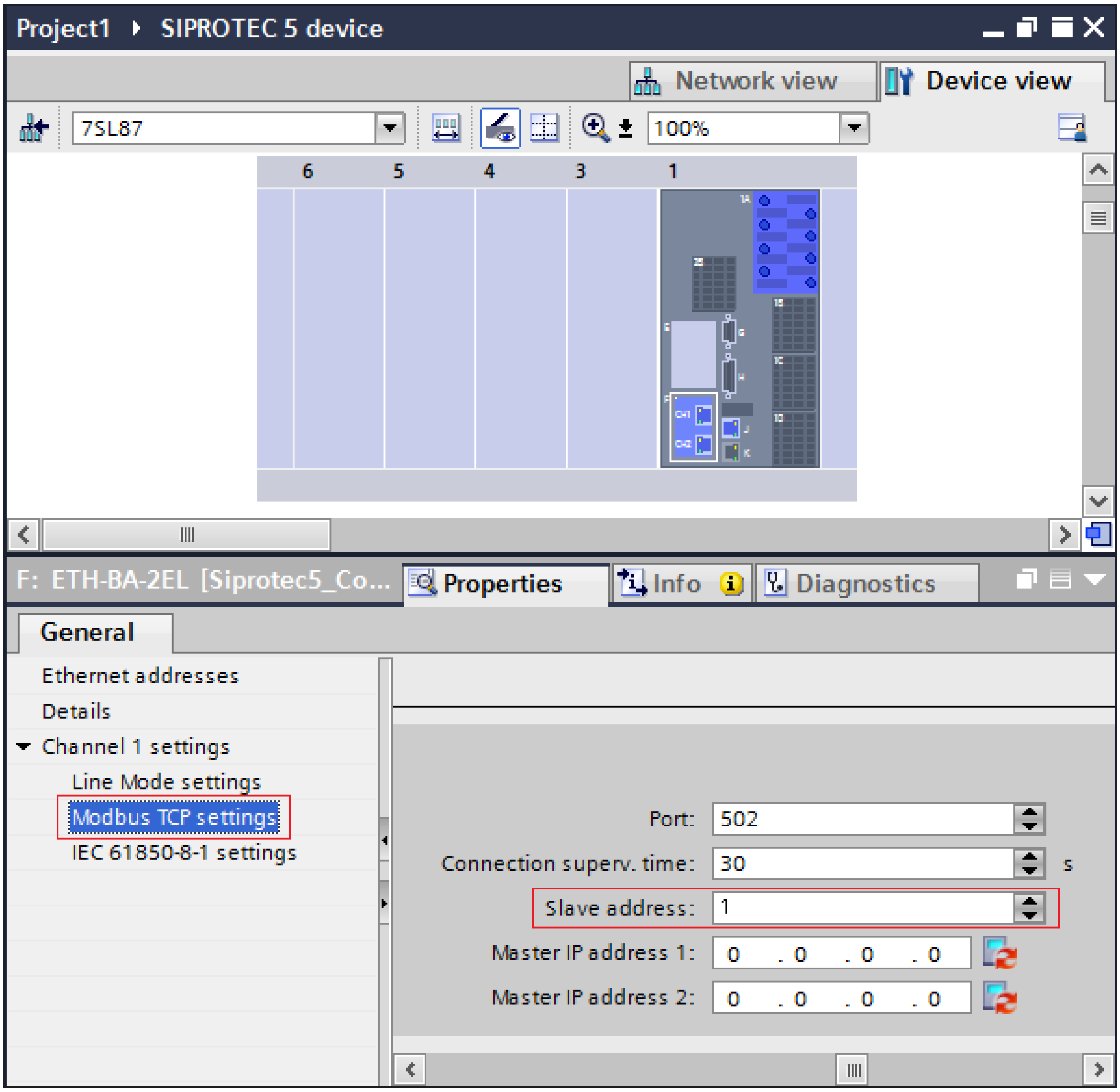
5.2.7 Operating Modes

The behavior of the protocol does not depend on the operating mode of the device. The protocol is running in the modes **process** and **simulation** of the device and the protocol is not activated in the operating modes **fallback** and **commissioning**.

5.3 Settings and Properties

5.3.1 Settings

During the parameterization, make the following settings for the communication between the Modbus master and the SIPROTEC 5 device.



[Sc_Set_Modbus, 1, en_US]

Figure 5-1 Modbus Settings

Parameter Name	Type	Description	Settings
Port	Int16	The TCP port to listen on.	Permitted range = 502 to 65 535 Standard setting = 502
Connection supervision time	Int16	If the connection time is expired, the SIPROTEC 5 device closes the TCP connection.	Permitted range = 30 s to 36000 s Standard setting = 30 s

Parameter Name	Type	Description	Settings
Slave address	Int16	Slave address of the SIPROTEC 5 device. If the address is 255, the device does not check the request address from the master.	Permitted range = 1 to 255 Standard setting = 1
Master IP address 1	Int32	IPv 4 (Internet Protocol Version 4) address 0.0.0.0 means that the slave can listen to and contact every IP address.	Permitted range = 0.0.0.0 to 255.255.255.255 Standard setting = 0.0.0.0
Master IP address 2	Int32	IPv 4 (Internet Protocol Version 4) address 0.0.0.0 means that the slave can listen to and contact with every IP address.	Permitted range = 0.0.0.0 to 255.255.255.255 Standard setting = 0.0.0.0

6 IEC 60870-5-103

6.1 Protocol Characteristics

6.1.1 Protocol Structure

6.1.1.1 Description

The protocol IEC 60870-5-103 is structured on the 3-layer model:

- Physical layer
- Data-link layer
- Application layer

6.1.1.2 Physical Layer

The physical layer specifies the transmission medium for the protocol.
Data transmission can be implemented as follows:

- Via optical fibers
- Via a wire-bound transmission system

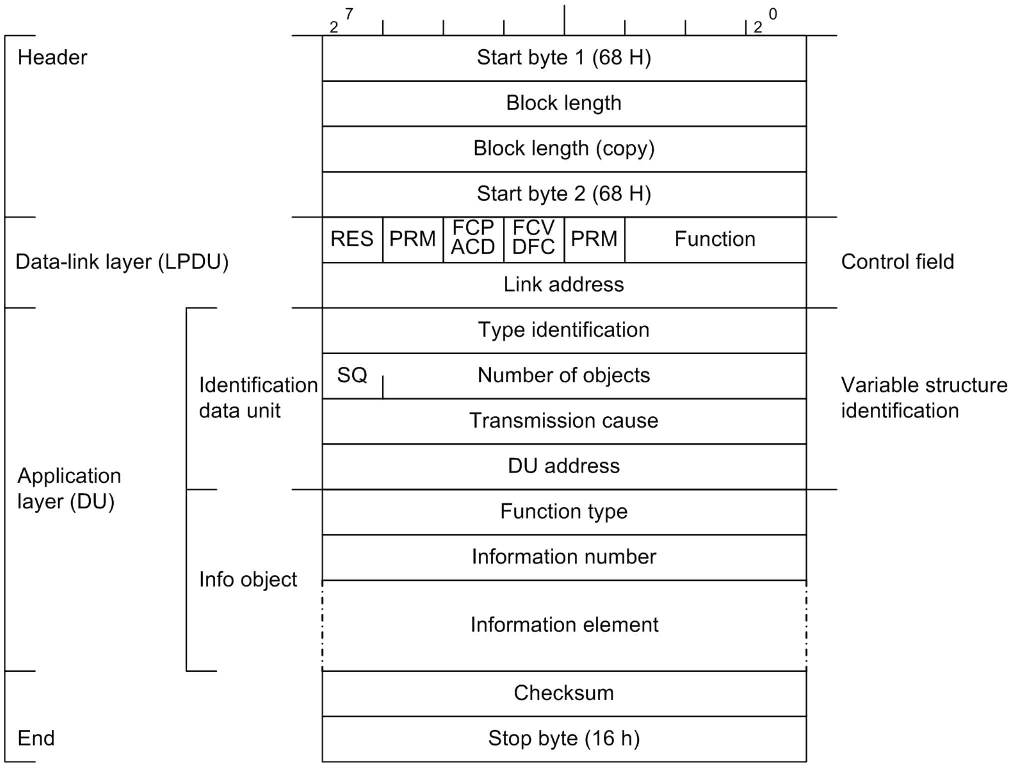
The SIPROTEC 5 device supports both communication media. The wire-bound transmission takes place via an RS485 interface.

6.1.1.3 Data-Link Layer

The connections between a substation automation and the protection device must be executed via an unbalanced link. This thereby prevents several protection devices from transmitting simultaneously.

The IEC 60870-5-103 protocol uses exclusively the format class FT 1.2 defined in IEC 60870-5-1 (transmission formats). At the same time, formats with fixed and variable length as well as the single character E5H are permissible.

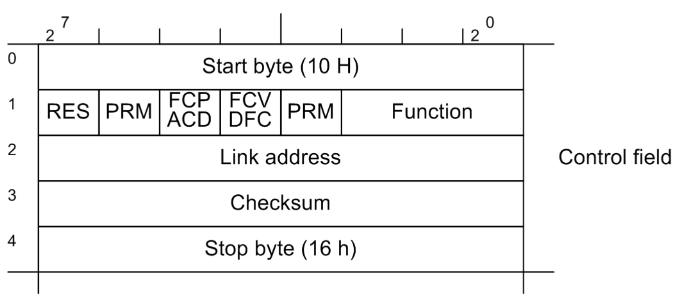
The telegram with variable length is used for transmission of the user data between the monitoring and monitored station and in the opposite direction.



[dw_tgrvlg, 2, en_US]

Figure 6-1 Telegram with Variable Length

The telegram with fixed length is intended for services of the data-link layer. In special cases, this format with fixed length is used as an acknowledgment instead of an individual character.



[dw_tgrflg, 2, en_US]

Figure 6-2 Telegram with Fixed Length

The individual character is used to acknowledge service data of the data-link layer and user data.

E5H = ACK: Positive acknowledgment

You can find more detailed information on the link address in chapter *6.2.1 Settings*.

6.1.2 Application Layer

6.1.2.1 Description

The application layer describes the Data Units (Data Units (DU)) for the transport telegrams. The SIPROTEC 5 device supports the following functions:

- Standard DUs in monitoring direction
- Standard DUs in control direction

6.1.2.2 Standard DUs in Monitoring Direction

Table 6-1 Standard DUs in Monitoring Direction

Data Unit (DU)	Meaning	Comments
DU 1	Indication with time stamp	–
DU 2	Indication with relative time	–
DU 3	Measured values I	See chapter *Measured Values, Page 62*
DU 4	Measured values with relative time	–
DU 5	Identification indication	Manufacturer (8 ASCII characters): **SIEMENS** Software version (4 ASCII characters): for example, **0102** = Version V01.02
DU 6	Time synchronization	–
DU 8	End of the general interrogation	–
DU 9	Measured values II	See chapter *Measured Values, Page 62*
DU 10	Generic data	See chapter *6.1.4.1 Description*
DU 23	Fault overview	–
DU 26	Ready for transmission of fault data	–
DU 27	Ready for transmission of a channel	–
DU 28	Ready for transmission of flags	–
DU 29	Transmission of flags	–
DU 30	Transmission of fault values	–
DU 31	End of transmission	–
DU 205	Metered values	–

6.1.2.3 Standard DUs in Control Direction

Table 6-2 Standard DUs in Control Direction

Data Unit (DU)	Meaning	Comments
DU 6	Time synchronization	–
DU 7	General interrogation command	–
DU 10	Generic data	See chapter *6.1.4.1 Description*
DU 20	General command	–
DU 21	Generic command	See chapter *6.1.4.1 Description*
DU 24	End of the general interrogation	–
DU 25	Acknowledgment of fault data transmission	–

6.1.3 Redundancy

6.1.3.1 Redundancy Aspects in a Communications System

If redundancy has to be implemented in a communication network, the selected redundant bus topology will always be a combination of the following redundancies:

- Master redundancy
- Media redundancy

These 2 redundancies can be combined independently of one another. As a result, several different bus and redundancy topologies can arise.

If a communications system includes both redundancies, this will be designated as a redundant system. The redundant system prevents an outage of the following components:

- Communication channel in the slave
- Power cable
- Communication master

The following table lists the functions of the primary channel as well as of the backup channel:

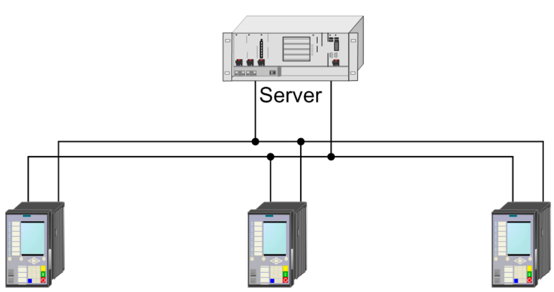
Service	Primary Channel	Backup Channel
Query class 1	X	X
Query class 2	X	X
General interrogation	X	X
Commands	X	–
Fault transmission	X	X
Time synchronization	X	X
Read parameters	X	X
Write parameters	X	–
GA[14] of Generic Services	X	X

6.1.3.2 Parametrization of a Redundant Communication

The SIPROTEC 5 device allows you to parameterize several communication channels via IEC 60870-5-103. In this way, you can also parameterize a redundant connection. This redundancy can also be implemented via various communication modules.

You can implement a master redundancy or a media redundancy. The selection is made via the parameter **Number of masters**.

The parameter **One master** denotes media redundancy. The SIPROTEC 5 device is passive here. The master communicates with the slave via a channel. If the master identifies an interruption in the communication channel, it can automatically change to the other channel. The parameter **Minimum duration of a channel connection** specifies the time until a new channel change by the master is possible.



[dw_medred, 1, en_US]

Figure 6-3 Media Redundancy

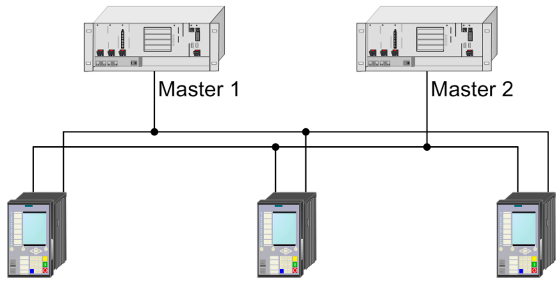
If 2 masters are parameterized, this represents a master redundancy. One master forms the primary master while the other master is the backup master. Both communicate simultaneously with the SIPROTEC 5 device. However, the following restrictions apply for the backup master:

- The time synchronization is possible via the backup master only if this channel is parameterized as the second time source.
- Control via the backup master is not possible.

The parameter **Primary channel after startup** specifies the channel on which the primary master is expected after the startup. In ongoing operation, the backup master can become the primary master. The

14 GA: General interrogation

changeover is executed with an IEC 60870-5-103 command. You must specify the parameters necessary for this (function type and information number) in the settings.



[dw_maredu, 1, en_US]

Figure 6-4 Master Redundancy

NOTE

At full redundancy there are 4 channels with IEC 60870-5-103. However, you can only set parameters for 2 time sources.

For this reason, at full redundancy Siemens recommends selecting IEC 60870-5-103 as the 1st timing master and a protocol-independent master, such as DCF, as the 2nd timing master.

6.1.4 Generic Services

6.1.4.1 Description

The generic services can be used to transmit data with different types and formats. At the same time, this data can be read and written as well.

In the SIPROTEC 5 device the generic services are used for reading and changing the setting parameters of the protection device.

The following services are supported in detail:

- General interrogation of generic data
- Reading an individual parameter
- Writing an individual parameter

The mapping description of the relevant device contains a list of changeable parameters.

The parameters refer to the active settings group.

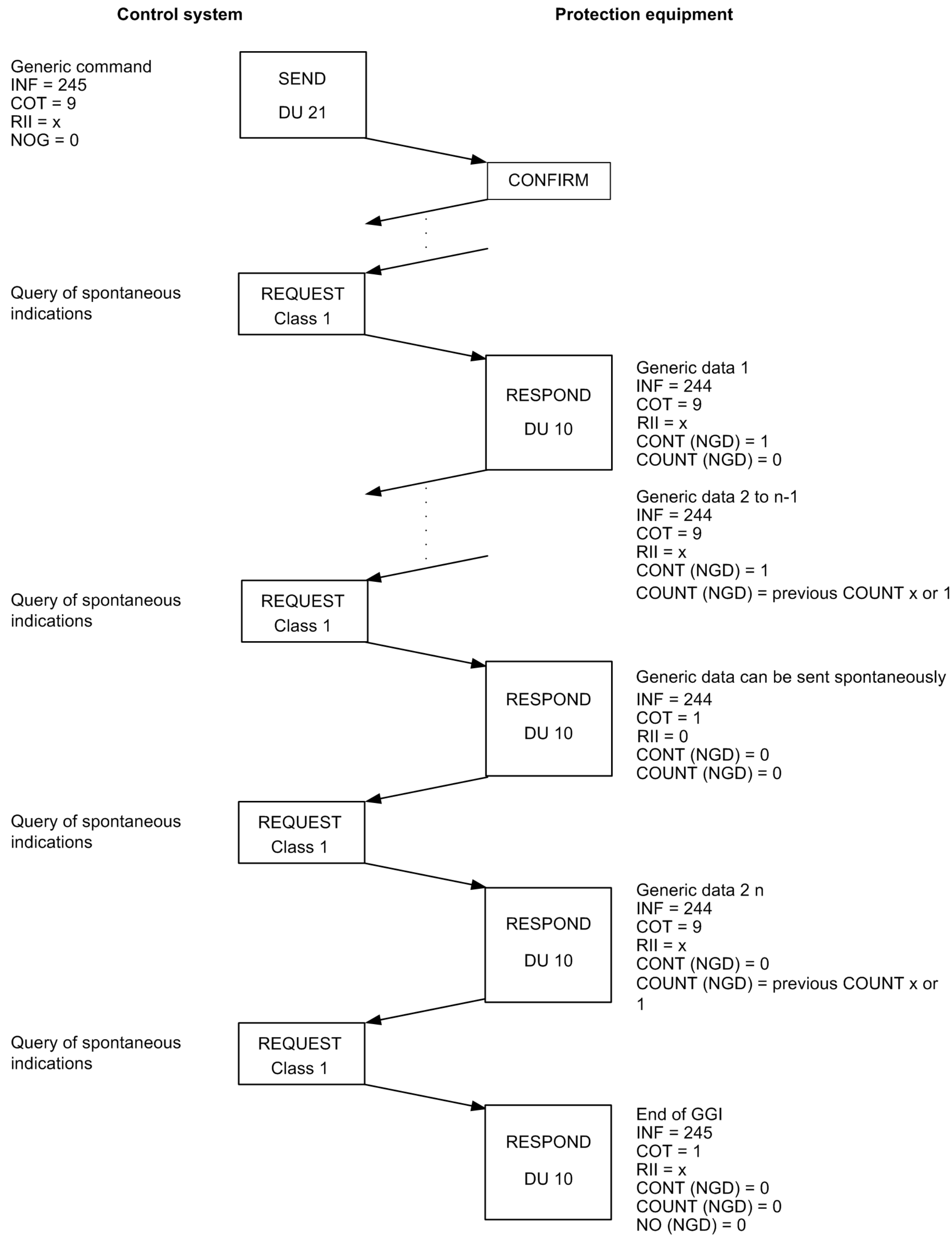
Reading and writing are possible only in the active settings group.

6.1.4.2 General Interrogation of Generic Data

The general interrogation of generic data provides a list of all parameters which you can change via the IEC 60870-5-103 protocol. The list also includes the current settings.

Siemens recommends that you carry out a general interrogation before any change to parameters.

The sequence is shown in the following figure.



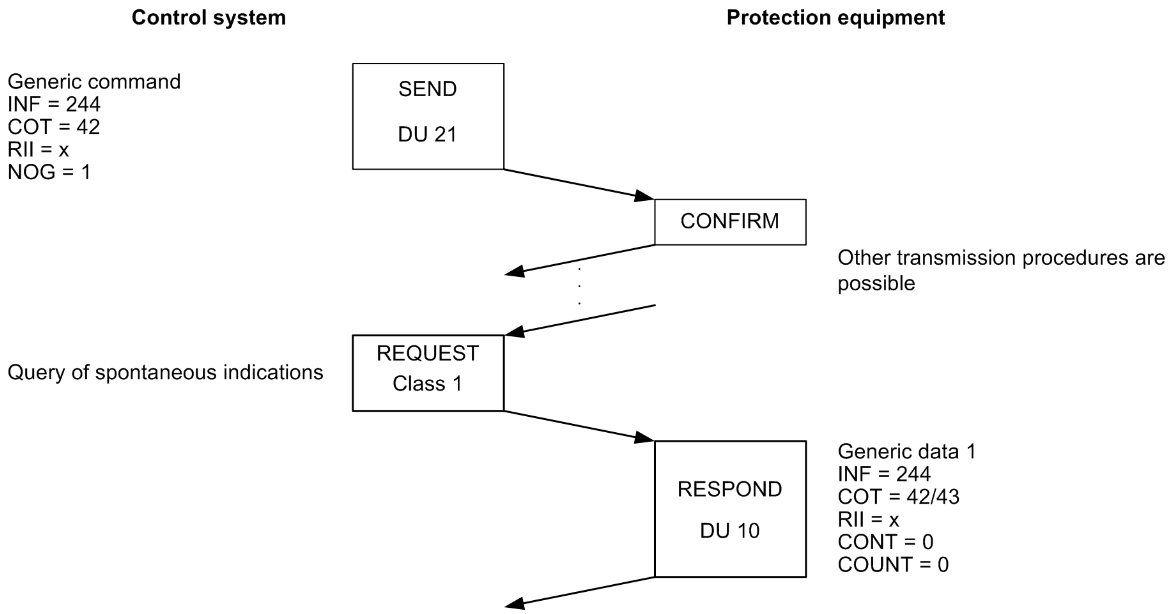
[dw_gagedt, 2, en_US]

Figure 6-5 General Interrogation of Generic Data

6.1.4.3 Reading an Individual Parameter

The function **`Reading an individual parameter`** prompts the protection device to read an individual attribute of an entry. The attribute is represented by its generic identification number.

The mapping description contains the assignment between the generic identification number and the parameter for the relevant device.



[dw_gendat, 2, en_US]

Figure 6-6 Reading an Individual Parameter

6.1.4.4 Writing an Individual Parameter

The function **`Writing an individual parameter`** prompts the protection device to record new values for individual entries. The attribute is represented by its generic identification number.

The mapping description contains the assignment between the generic identification number and the parameter for the relevant device.

NOTE

The SIPROTEC 5 device only writes one value in a telegram. Only a generic data description is supported here:

DATATYPE: 4 (integral value)

DATASIZE: 4

NUMBER: 1

DATATYPE: 7 (float value)

DATASIZE: 4

NUMBER: 1

The following figures show typical example telegrams for writing parameters. This involves a float parameter and a text parameter. The mapping data (GIN) are examples. The exact GIN can be found in the mapping description of the relevant device.

- Setting a float parameter:
  The setting values in the device are mapped via the protocol to the float values to be transmitted. The device's mapping file contains this mapping.

<10> Generic data									TYPE IDENTIFICATION	
1	0	0	0	0	0	0	1		VARIABLE STRUCTURE QUALIFIER	
<40> Generic write command									CAUSE OF TRANSMISSION	
									COMMON ADDRESS OF ASDU	
<254> Generic function type									FUNCTION TYPE:=GEN	
<250> Write entry with execution									INFORMATION NUMBER	
									RII	
{1,0,0}									NGD {NO, COUNT, CONT}	
0107H									GIN	
<1> ACTUAL VALUE									KOD	
<7>								DATATYPE	GDD	Data set
4								DATASIZE		
1								NUMBER		
1.5									GID	

[dw_wrdepa, 1, --_--]

Figure 6-7 Setting a Float Parameter

  As only integral values are possible for the value indication (GID), you must indicate the values without a comma.

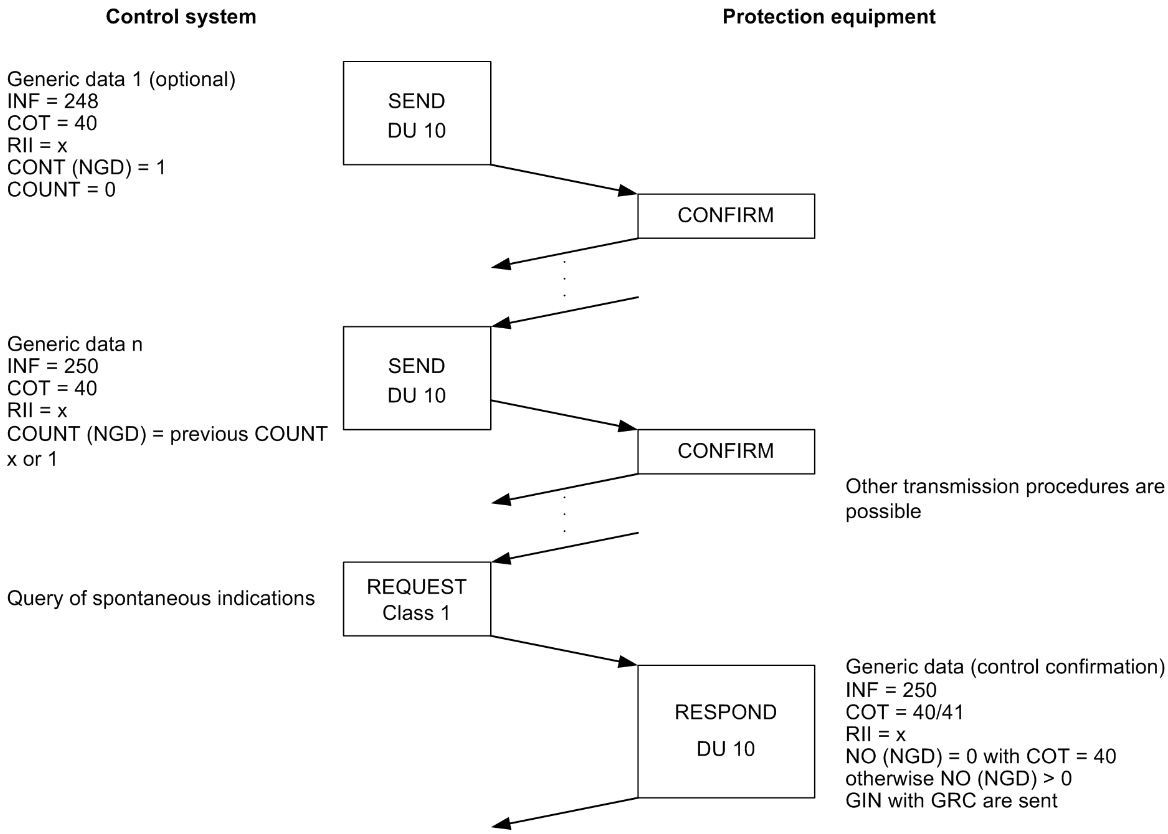
- Setting a text parameter (for example, 50, 51 Phase Time Overcurrent) to OFF:

<10> Generic data									TYPE IDENTIFICATION	
1	0	0	0	0	0	0	1		VARIABLE STRUCTURE QUALIFIER	
<40> Generic write command									CAUSE OF TRANSMISSION	
									COMMON ADDRESS OF ASDU	
<254> Generic function type									FUNCTION TYPE:=GEN	
<250> Write entry with execution									INFORMATION NUMBER	
									RII	
{1,0,0}									NGD {NO, COUNT, CONT}	
0100H									GIN	
<1> ACTUAL VALUE									KOD	
<4>								DATATYPE	GDD	Data set
4								DATASIZE		
1								NUMBER		
23									GID	

[dw_wrtxpa, 1, --_--]

Figure 6-8 Set Text Parameter

The assignment of the entry value to the relevant text can be found in the mapping description.



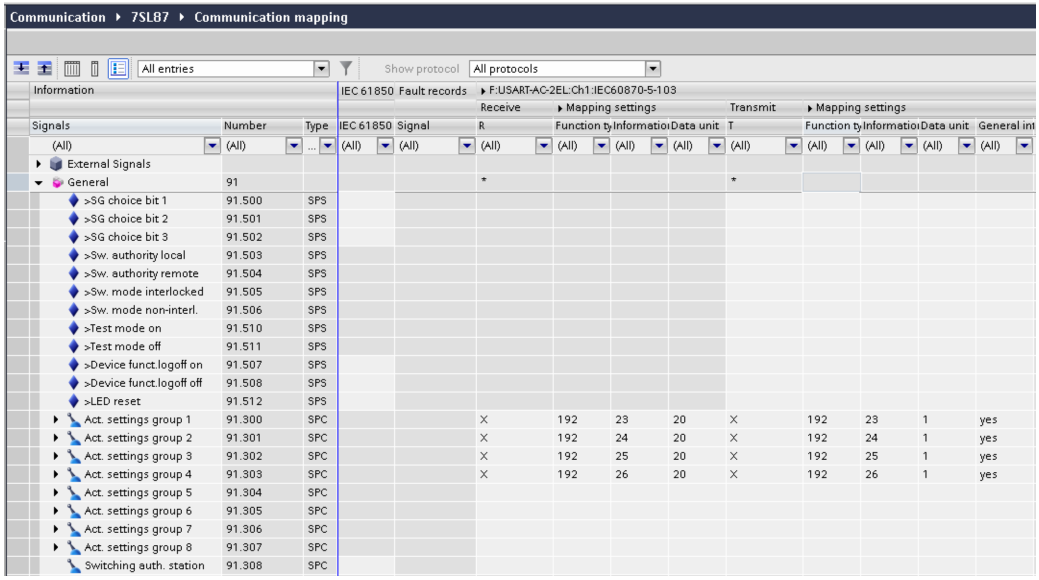
[dw_wrtpar, 2, en_US]

Figure 6-9 Writing an Individual Parameter

6.1.5 Settings Group Switching

In premapping of the protocol, 4 settings groups are premapped. You set the number of the parameterized settings groups in DIGSI under **Settings** → **Device Settings**. Depending on the number of parameterized settings groups, additional settings groups can be visible in the matrix. You use the private range of information numbers for this purpose.

If you want to use the telecontrol protocol to switch the parameter, then also map the command direction (Transmit) for the respective settings group in the communication matrix under the function block **General**.



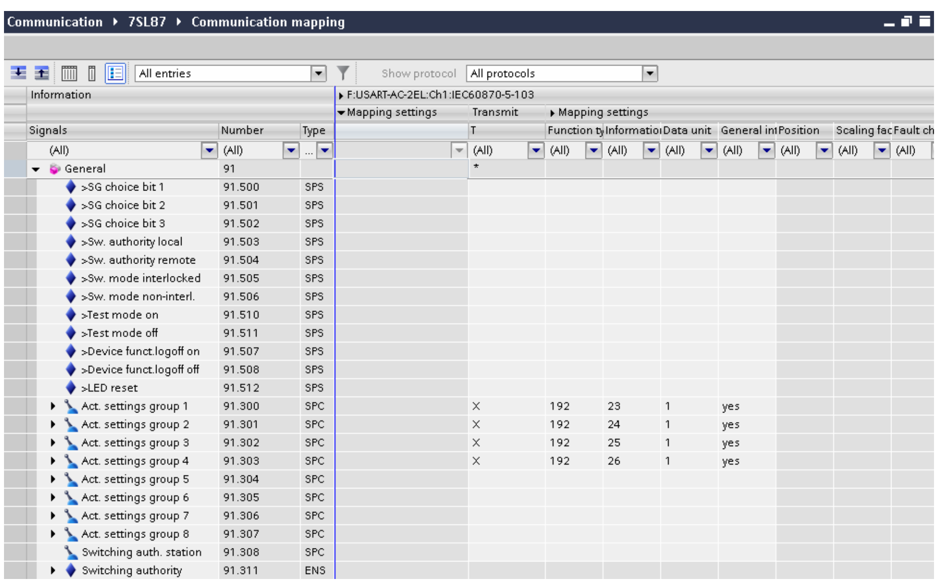
Communication ▸ 7SL87 ▸ Communication mapping

Signals	Number	Type	IEC 61850	Signal	R	Function ty	Informatio	Data unit	T	Function ty	Informatio	Data unit	General int
(All)	(All)	...	(All)	(All)	(All)	(All)	(All)	(All)	(All)	(All)	(All)	(All)	(All)
External Signals													
General	91				*				*				
>SG choice bit 1	91.500	SPS											
>SG choice bit 2	91.501	SPS											
>SG choice bit 3	91.502	SPS											
>Sw. authority local	91.503	SPS											
>Sw. authority remote	91.504	SPS											
>Sw. mode interlocked	91.505	SPS											
>Sw. mode non-interl.	91.506	SPS											
>Test mode on	91.510	SPS											
>Test mode off	91.511	SPS											
>Device funct.logoff on	91.507	SPS											
>Device funct.logoff off	91.508	SPS											
>LED reset	91.512	SPS											
Act. settings group 1	91.300	SPC			X	192	23	20	X	192	23	1	yes
Act. settings group 2	91.301	SPC			X	192	24	20	X	192	24	1	yes
Act. settings group 3	91.302	SPC			X	192	25	20	X	192	25	1	yes
Act. settings group 4	91.303	SPC			X	192	26	20	X	192	26	1	yes
Act. settings group 5	91.304	SPC											
Act. settings group 6	91.305	SPC											
Act. settings group 7	91.306	SPC											
Act. settings group 8	91.307	SPC											
Switching auth. station	91.308	SPC											

[sc_sgsocd, 1, en_US]

Figure 6-10 Mapping Commands for Settings Group Switching

The indications for an active settings group are mapped in the device in transmit direction.



Communication ▸ 7SL87 ▸ Communication mapping

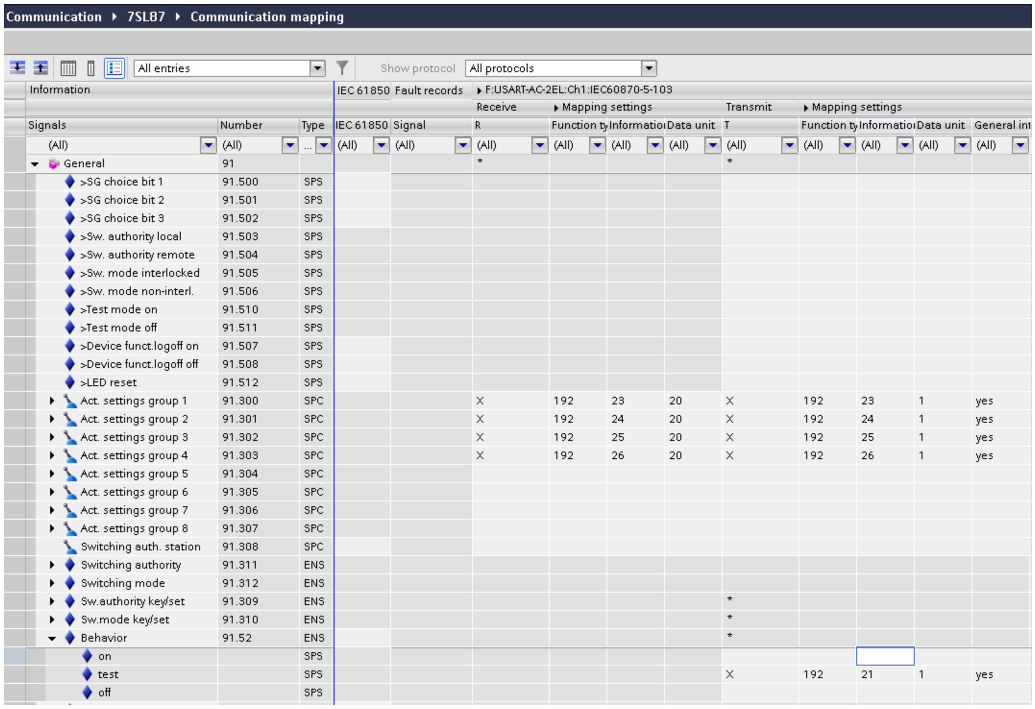
Signals	Number	Type		T	Function ty	Informatio	Data unit	General int	Position	Scaling fac	Fault ch
(All)	(All)	...		(All)	(All)	(All)	(All)	(All)	(All)	(All)	(All)
General	91			*							
>SG choice bit 1	91.500	SPS									
>SG choice bit 2	91.501	SPS									
>SG choice bit 3	91.502	SPS									
>Sw. authority local	91.503	SPS									
>Sw. authority remote	91.504	SPS									
>Sw. mode interlocked	91.505	SPS									
>Sw. mode non-interl.	91.506	SPS									
>Test mode on	91.510	SPS									
>Test mode off	91.511	SPS									
>Device funct.logoff on	91.507	SPS									
>Device funct.logoff off	91.508	SPS									
>LED reset	91.512	SPS									
Act. settings group 1	91.300	SPC		X	192	23	1	yes			
Act. settings group 2	91.301	SPC		X	192	24	1	yes			
Act. settings group 3	91.302	SPC		X	192	25	1	yes			
Act. settings group 4	91.303	SPC		X	192	26	1	yes			
Act. settings group 5	91.304	SPC									
Act. settings group 6	91.305	SPC									
Act. settings group 7	91.306	SPC									
Act. settings group 8	91.307	SPC									
Switching auth. station	91.308	SPC									
Switching authority	91.311	ENS									

[sc_indasg, 1, en_US]

Figure 6-11 Mapping Indications for a Settings Group

6.1.6 Test Mode

For functional reasons, map the standards-compatible information **Test mode on** under the function block **General → Behavior → Test**.



[sc_testmd, 1, en_US]

Figure 6-12 Mapping the Test Mode

6.1.7 Fault Recording

Individual information can be selected from the fault recordings in the device and transmitted in the fault record via IEC 60870-5-103.

The SIPROTEC 5 devices send the fault recording with function type No.253.

The following maximum number of items can be transmitted via IEC 60870-5-103:

- Analog signals: 40
- Binary signals: 100

Up to 8 latest fault records can be stored for IEC 60870-5-103. This number may decrease if very large fault records (long recording time) are stored.

NOTE

After the successful transmission, the fault records in the device are not deleted.

6.1.8 Amount of Mappable Information

The following information may be mapped:

Information	Maximum Mappable Amount
Indications + Controllables at Tx (Tx: transfer direction)	500
Controllables at Rx (Rx: receive direction)	50
Settings at Tx	500

Information	Maximum Mappable Amount
Measurements at Tx	100
Counters at Tx	20

6.1.9 Global Function Type

For every device, there is a global function type that is used for general functions such as general interrogation or time synchronization.

You can find explanations for the devices and function-type numbers in the following table.

Device	Function-Type Number
7UM8	70
7VK8	94
7SA8	128
6MD8	160
7SJ8	160
7SK8	160
7UT8	176
7SL8	192
7SD8	192
7SS8	194
7KE8	225
7ST8	230

6.1.10 Additional Information

NOTE

The information number 20 is reserved together with data unit (DU) 1 for transmission blocking. Routing to another information object is not permitted.

Select Mapping

The standard mapping for IEC 60870-5-103 contains both routings specified by the IEC 60870-5-103 protocol and Siemens-specific routings.

Commands

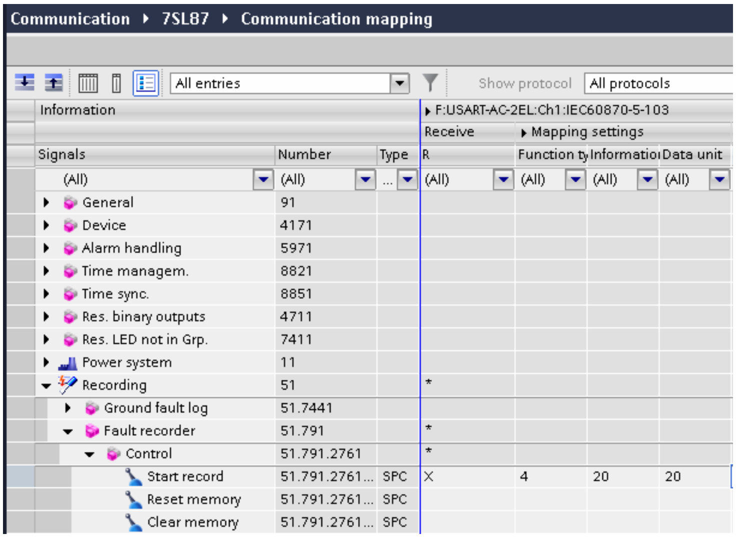
The commands are mapped in the same way as the indications. Only the parameter **`General interrogation`** is deleted.

NOTE

In the case of commands, the IEC 60870-5-103 protocol allows only direct switching. Selection is not possible before switching. However, the protocol firmware simulates this cycle (select – operate) internally.

In the case of negative acknowledgment of a command, the reason for the negative acknowledgment cannot be distinguished. The possible reasons are listed in the following:

- Select negative
- Operate negative
- Other interlocking conditions in effect



[scmapctr-280113-01.tif, 2, en_US]

Figure 6-13 Mapping Commands

Position in the Measured-Value Telegram

Up to 4 measured values can be routed in a DU 3 telegram.

Up to 16 measured values can be routed in a DU 9 telegram.

In total, you can route 1 DU 3 and 10 DU 9 telegrams. You can route a maximum 100 measured values.

When routing DU3 and DU9, the position must be successive and the routing starts from position 1.

Scaling Measured Values

The measured values are transferred as a percentage between the SIPROTEC 5 device and the IEC 60870-5-103 master.

A measured value is resolved with 13 bits in the IEC 60870-5-103 protocol. This is 2^{12} - 1 = 4096. This integer number is assigned to a measured value of 240 % (120 %) of the rated value. The maximum value (240 % or 120 %) can be set globally for all measured values.

The following example illustrates this situation: A current is to be transmitted. The rated current is 1000 A. A current of 2400 A (240 %) corresponds to 8191. Therefore, the 1000 A current is transmitted with the numerical value 1000/2400 * 4096 = 1707.

You can set parameters for the transmission threshold of every measured value independent of the protocol used.

A detailed description can be found in the Device Manual in the **Measured, Energy and Statistic Values** chapter and in the Operating Manual in the **Setting and Resetting Energy Values** chapter.

Converting Measured Values

The range of values of a measured value that can be transmitted is usually ±240 % or ±2.4 times the standardized value.

The value in data units 3 and 9 has 13 bits (one sign, 12 data bits). This means that ±4096 corresponds to ±240 % (or 120 %) of a measured value.

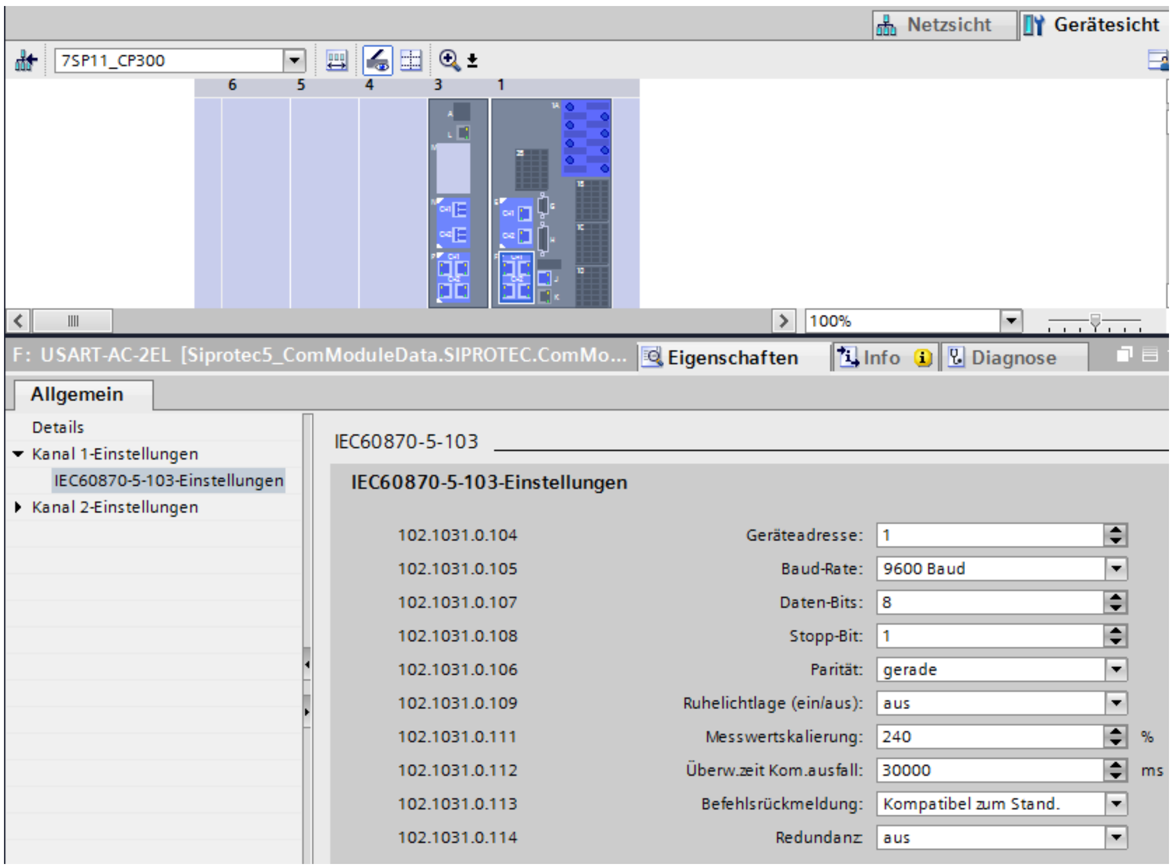
Some measured values, however, do not comply with this definition:

- cos phi: -4096 means cos phi = -1; +4096 means cos phi = +1
- Isens real, Isens reactive: -4096 corresponds to Isens = -800 mA; +4096 corresponds to Isens = +800 mA
- Frequency: The rated frequency (50 Hz or 60 Hz) is 100 % and thus corresponds to 1706 when 4096 = 240 % or 3413 when 4096 = 120 %.

6.2 Settings and Properties

6.2.1 Settings

During the parameterization, make the following settings for the serial communication between the systems control unit and the SIPROTEC 5 device via IEC 60870-5-103.



[sc_modpro, 4, en_US]

Figure 6-14 Settings for IEC 60870-5-103

Parameter	Description	Settings
`Slave address`	Link address of the SIPROTEC 5 device.	Permitted range = 1 to 254 Default setting = 1
`Baud rate`	The IEC 60870-5-103 communication module supports baud rates in the range from 2400 Bd to 57 600 Bd.	Default setting = 9600 Bd
`Parity`	You set the parity with this parameter.	The following parities can be set: • No parity • Even parity (default setting) • Odd parity
`Data bit`	7 data bits or 8 data bits can be set on the communication module.	8 data bits must be set for the IEC 60870-5-103 protocol.
`Stop bit`	The IEC 60870-5-103 communication module supports 1 stop bit and 2 stop bits.	Default setting = 1 stop bit

Parameter	Description	Settings
`Light idle state`	You determine the communication medium with this parameter. If the communication takes place via an optical fiber, the idle state is specified at the same time. The light idle state is relevant only for optical modules.	The following settings are possible: • On: Communication via optical fiber; light idle state on • Off (default setting): Communication via optical fiber; light idle state off
`Measure standardization`	You set the measured value scaling with this parameter.	You have the following setting options here: • 240 % (default setting) • 120 %
`Superv.time com.failure`	If no communication with a master occurs in the parameterized time, the indication **Fault communication channel** is then issued. The settable time is between 1000 ms and 3 600 000 ms.	Default setting = 10 000 ms
`Double command feedback`	With this parameter, you specify whether the intermediate position should also be transmitted for double-command feedback.	The following settings are possible: • Compatible with standard [15] (default setting) • V4 compatible[16]
`Redundancy`	The parameter specifies whether the device is to communicate via a redundant connection.	The following settings are possible: • On • Off (default setting)

The following parameters are only important for redundant communication. These parameters are not required for normal communication. This parameters are displayed only if you have set the parameter `Redundancy` to **On**.

`Redundant slot`	Slot location of the module on which the second (redundant) channel is parameterized.	Slot designation
`Redundant channel`	Module channel on which the second (redundant) protocol is parameterized.	Channel number
`Number of masters`	The IEC 60870-5-103 communication module supports connection to one master (media redundancy) and to 2 masters (master redundancy). The number of masters is specified here.	Default setting = 1 master
`Primary channel after startup`	This channel of the communication module receives the status **primary** after the module starts up. If this channel is set to **Yes**, the other channel must be set to **No**. The channel set to **Yes** is the primary channel; the other channel is the secondary channel. Only one channel can be the primary channel.	Yes No

[15] Without transmission of disturbed position

[16] With transmission of disturbed position and Cause of Transmission 13 in the case of negative command feedback

Function type for channel change	The parameter specifies the function type for the command (DU 20) with which the status (primary/backup) of the channel can be changed. After the change, an indication (DU 1) is sent. This indication also has this function type.	The range of values is 1 to 254. Default setting = 100
Information number for channel change	The parameter specifies the information number for the command (DU 20) with which the status (primary/backup) of the channel can be changed. After the change, an indication (DU 1) is sent. This indication also has this information number.	The range of values is 1 to 254. Default setting = 10

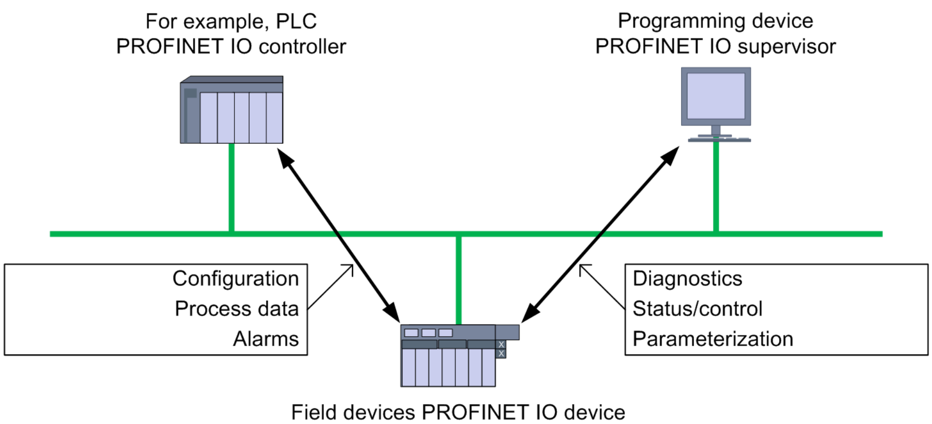
7 PROFINET IO

7.1 Protocol Characteristics

7.1.1 Description

PROFINET IO is an Ethernet-based communication protocol that can be used in all areas of communication automation.

The data exchange of PROFINET IO follows the Provider/Consumer model. A configured PROFINET IO system has the same look and feel as in PROFIBUS.



[dw_PRO_IO_Device_new, 2, en_US]

Figure 7-1 Communication Paths for PROFINET IO

The following device classes are defined for PROFINET IO:

- PROFINET IO controller
  A PROFINET IO controller is typically the programmable logic controller (PLC) on which the automation program runs. The PROFINET IO controller provides output data to the configured IO devices in its role as provider and is the consumer of input data of IO devices.
- PROFINET IO supervisor
  A PROFINET IO supervisor can be a Programming Device (PD), a personal computer (PC), or a human-machine interface (HMI). It serves for commissioning or diagnostic purposes and corresponds to a class-2 master in PROFIBUS.
- PROFINET IO device
  A PROFINET IO device is a distributed IO field device that is connected to one or more IO controllers via PROFINET IO. It is comparable to the function of a slave in PROFIBUS. The PROFINET IO device is the provider of input data and the consumer of output data. The SIPROTEC 5 device works as the IO device.

System-level redundancy (S2) can also be achieved with the new ETH-BD-2FO module with additional support of transfer of sequence of events to the IO controller.

NOTE

SIPROTEC 5 device is an IO device. Alarm is not supported in version V7.30. The SIPROTEC 5 device does not support an IP assignment from the IO controller in version V7.30.

A plant unit contains at least one IO controller and one or more IO devices. IO supervisors are integrated only temporarily for commissioning or troubleshooting purposes.

The device model in the PROFINET IO protocol is based on the principles of PROFIBUS. It consists of slots and groups of IO channels (subslots). The technical characteristics of the field devices are described in an XML-based GSD (General Station Description) file.

Data in PROFINET networks is highly varied. Cyclical PROFINET IO data can be transmitted with high priority.

Network topologies in PROFINET derive from the requirements of the system to be networked. The most common topologies are star, line, tree, and ring-shaped. In practice, the system is usually a mix of these topologies.

Device Model of an IO Device

The device model describes all field devices in terms of their possible technical and functional features. It is specified by the DAP (Device Access Point) and the defined modules for a particular device family. A DAP is the access point for communication with the Ethernet interface and the processing program. In order to manage the actual process-data traffic, a variety of IO modules can be assigned to it.

The following structures are standardized for an IO device:

- The slot designates the place where an IO module is inserted in a modular IO field device.

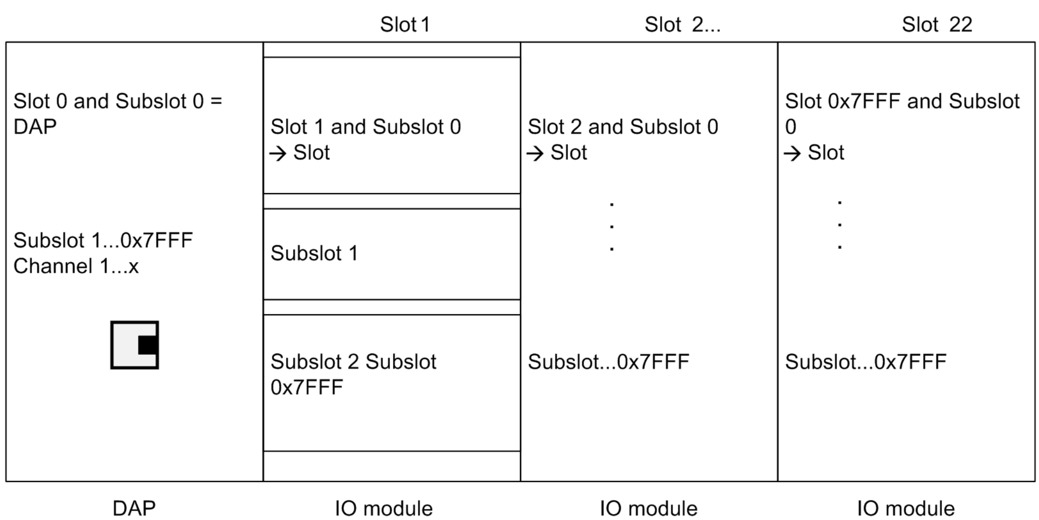
  The configured modules containing one or more subslots for data exchange are addressed based on the different slots.

- Within a slot, the subslots form the actual interface to the process (inputs/outputs). The granularity of a subslot (bitwise, bytewise, or wordwise division of IO data) is determined by the manufacturer.

  The data content of a subslot is always accompanied by status information, from which the validity of the data can be derived.

  The index specifies the data within a slot/subslot that can be read or written acyclically via read/write services. For example, parameters can be written to a module or manufacturer-specific module data can be read out based on an index. Certain indices are defined in the standard, and other indices can be freely defined by the manufacturer.

  Cyclic IO data are addressed by specifying the slot/subslot combination. These can be freely defined by the manufacturer. For acyclic data communication via read/write services, an application can specify the data to be addressed using slot, subslot, and index.



[dw_IO_module_slot, 1, en_US]

Figure 7-2 Addressing of IO Data in PROFINET Based on Slots and Subslots

7.1.2 Device Identification

Each PROFINET IO device requires a unique device identification. This device identification consists of the Vendor_ID and the Device_ID, with the Device_ID comprising the device class and device family.

The device identification for a PROFINET IO device in SIPROTEC 5 devices is:

0x002A0E02

and is composed as follows:

Table 7-1 Device Identification

Vendor_ID	Device_ID	
	Device class	Device family
0x002A (Siemens AG)	0E (Protection and PQ)	02 (SIPROTEC 5)

The device identification is stored, for example, in the GSDML file, see chapter *7.3.1 PROFINET IO Configuration*.

7.1.3 Data-Type Definitions for IO Data Exchange

7.1.3.1 Overview

The following data types and definitions are used to exchange data between the IO device and the IO controller via PROFINET IO:

- Single-point indication
- Single command
- Double-point indication
- Double command
- Measured value
- Metered value
- Controllable analog process value
- Binary controlled step position information

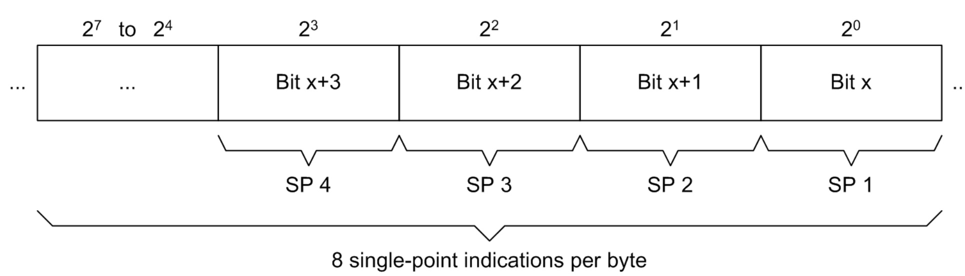
7.1.3.2 Data Type Single-Point Indication (SP, Input)

Number of byte values: 1/8 (1 bit)

Range of values:

0 = OFF

1 = ON



[dw_Data_type_single_point, 1, en_US]

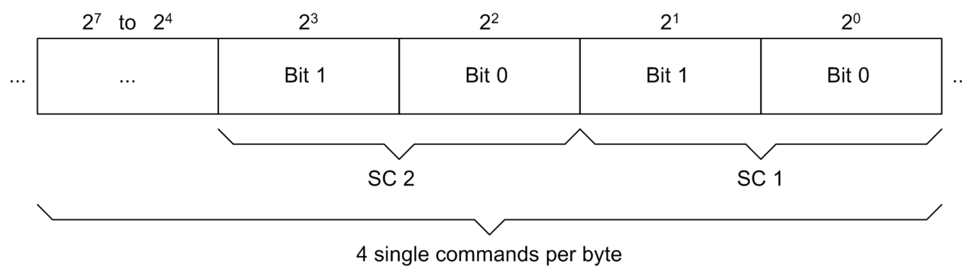
Figure 7-3 Data Type: Single-Point Indication

7.1.3.3 Data Type Single Command (SC, Output)

Number of byte values: 1/4 (2 bits)

Range of values:

0 = intermediate state	bit 1 = 0 and bit 0 = 0
1 = OFF	bit 1 = 0 and bit 0 = 1
2 = ON	bit 1 = 1 and bit 0 = 0
3 = disturbed state	bit 1 = 1 and bit 0 = 1



[dw_Data_type_single_command, 1, en_US]

Figure 7-4 Data Type: Single Command

NOTE

Single commands of the SIPROTEC 5 device are controlled via PROFINET IO using 2 bits (similar to double commands, see chapter *7.1.3.4 Data Type Double-Point Indication (DP, Input)*).

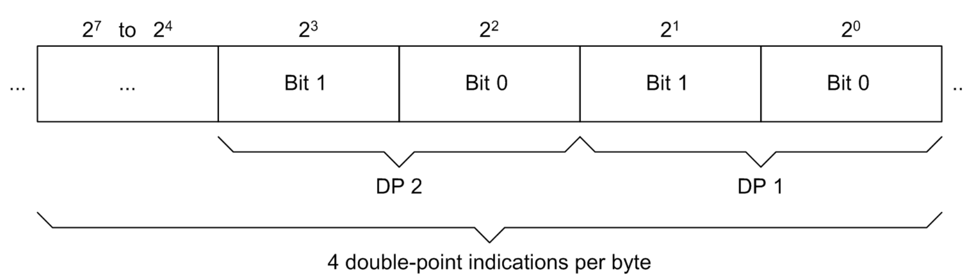
The switching direction OFF for single commands with pulse output is not permitted and is rejected in the SIPROTEC 5 device.

7.1.3.4 Data Type Double-Point Indication (DP, Input)

Number of byte values: 1/4 (2 bits)

Range of values:

0 = intermediate state	bit 1 = 0 and bit 0 = 0
1 = OFF	bit 1 = 0 and bit 0 = 1
2 = ON	bit 1 = 1 and bit 0 = 0
3 = disturbed state	bit 1 = 1 and bit 0 = 1



[dw_Data_type_double-point indic, 1, en_US]

Figure 7-5 Data Type: Double-Point Indication

7.1.3.5 Data Type Double Command (DC, Output)

Number of byte values: 1/4 (2 bits)

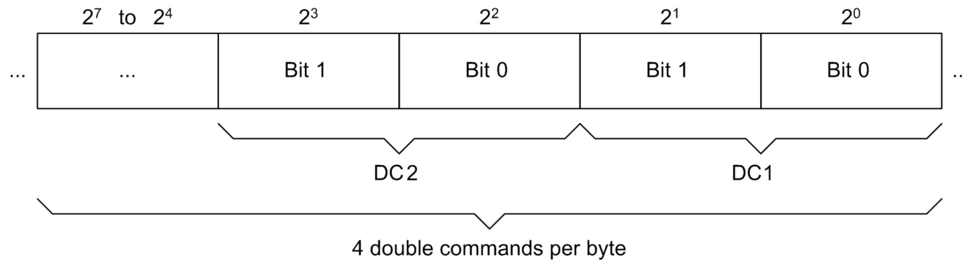
Range of values:

0 = intermediate state (not allowed to control with 0)

1 = OFF

2 = ON

3 = disturbed state (not allowed to control with 3)



[dw_Data_type_double-command, 1, en_US]

Figure 7-6 Data Type: Double Command

NOTE

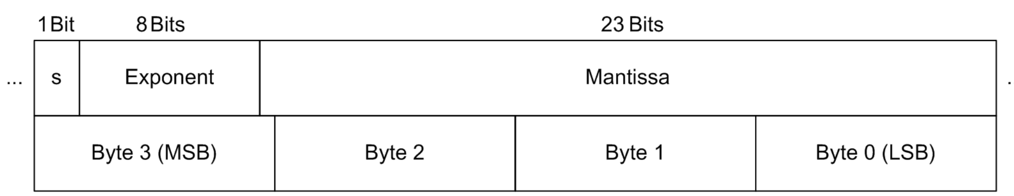
For the data type double command, you must parameterize the associated command feedback as double-point indication in DIGSI 5.

7.1.3.6 Measured Values

Number of byte values: 4 (32 bits)

Range of values: $\pm 1.7 \cdot 10^{38}$

Measured values are transmitted in 32-bit floating-point format. The format consists of a sign bit (S), exponent, and mantissa as shown in the following:



[dw_Data_type_measured_value, 1, en_US]

Figure 7-7 Data Type: Measured Value

Sign Bit (S)

If measured values are negative, the sign bit (S) is set.

Measured Values (Mantissa and Exponent)

The value of a measured value is obtained as follows:

0 < Exponent < 255	Resulting value = $(-1)^{<sign>} \cdot 2^{(<exponent> - 127)} \cdot 1,<mantissa>$
Exponent = 0	Resulting value = 0
Exponent = 255	Mantissa not equal to 0: invalid (Not a Number, NaN)

Quality Information

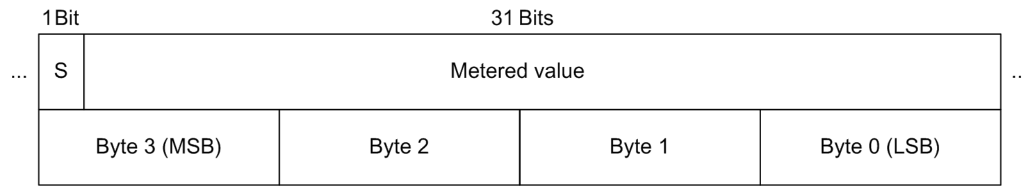
Table 7-2 Quality Information

Floating-Point Number (Hexadecimal)	Status	Remark
0x7F800000	Overflow	Overflow of the measured value
0x7F800001	Invalid	Measured value invalid or not computable, for example, frequency or cos ϕ when voltage or current is too low.

7.1.3.7 Metered Values (BCR, Input)

Number of byte values: 4 (32 bits)

Valid range of values: 0 to + 2 147 483 647



[dw_Data_type_metered_value, 1, en_US]

Figure 7-8 Data Type: Metered Value

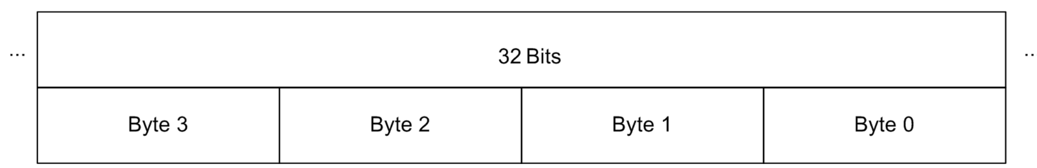
Sign Bit (S)

If the external error bit for the pulse metered values and the binary input is set, the metered value with the set sign bit is invalid.

7.1.3.8 Controllable Analog Process Values (APC, Output)

Number of byte values: 4 (32 bits)

Valid range of values: 0 to + 16 777 216



[dw_Data_type_APC, 1, en_US]

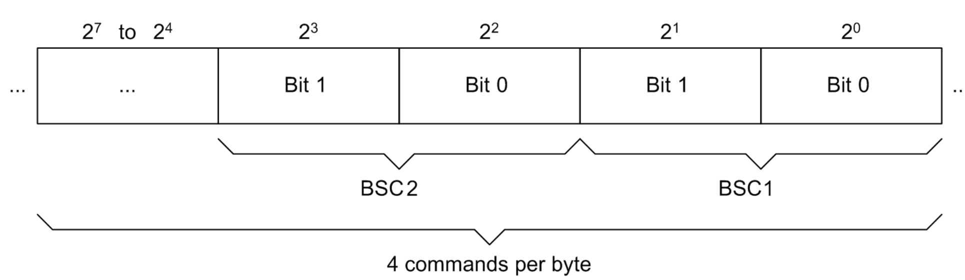
Figure 7-9 Data Type: Controllable Analog Process Value

7.1.3.9 Binary Controlled Step Position Information (BSC, Output)

Number of byte values: 1/4 (2 bits)

Range of values:

0 = Invalid command	bit 1 = 0 and bit 0 = 0
1 = Lower command	bit 1 = 0 and bit 0 = 1
2 = Higher command	bit 1 = 1 and bit 0 = 0
3 = Invalid command	bit 1 = 1 and bit 0 = 1



[dw_Data_type_BSC, 1, en_US]

Figure 7-10 Data Type: Binary Controlled Step Position Information

7.1.3.10 Unit IDs, Units, and Unit Multipliers

The following unit IDs are assigned to the units of the measured values:

Table 7-3 Units and Unit Multipliers

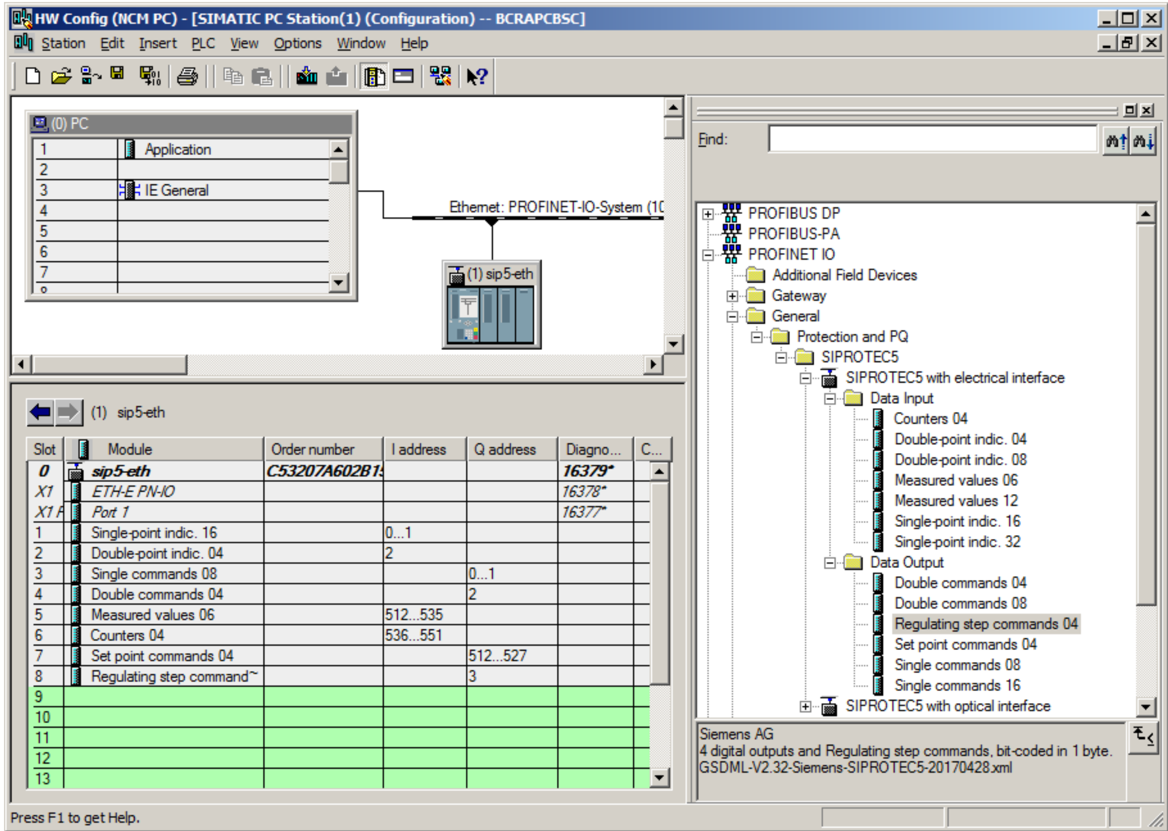
ID	Unit, Unit Multiplier	ID	Unit, Unit Multiplier	ID	Unit, Unit Multiplier
1	Dimensionless	33	kΩ	172	MWh
3	%	51	W	173	GWh
4	°	53	kW	174	kvar
5	°C	54	MW	175	Mvar
11	A	61	VA	176	Gvar
12	mA	63	kVA	177	kvarh
13	kA	64	MVA	178	Mvarh
17	h	71	Hz	179	Gvarh
21	V	92	km	184	GVA
22	mV	95	miles	185	°F
23	kV	170	GW	203	MΩ
31	Ω	171	kWh		

The unit IDs can be read via acyclic telegrams, see chapter *7.1.6.1 Reading Unit IDs of Measured Values and Metered Values*.

7.1.4 IO Modules

The IO modules described in the following tables are available for the PROFINET IO configuration of the SIPROTEC 5 devices in the IO controller. For this purpose, the GSDML file, which contains the description of the IO modules, is loaded into the parameterization software of the IO controller.

Figure 7-11 shows an example for selecting the IO module of the SIPROTEC 5 device with Ethernet interface. Siemens parameterization software Step7 is used as the IO controller configuration tool.



[sc_para_example, 2, --_--]

Figure 7-11 Parameterization Example

PROFINET IO Bus Interface DAP (Device Access Point)

The DAP module is always plugged in at slot 0 of the IO device and cannot be removed. The module describes the physical device data such as interface and port. In addition, it is possible to read or write device-related diagnoses and acyclic telegrams.

Cyclic data exchange	None
Acyclic reading/writing of data (standard PROFINET IO services)	• Reading of diagnostics data and I&M data[17] 0, 1, 2, 3, 4 • Writing of I&M data 1, 2, 3, 4
Acyclic reading/writing of data (SIPROTEC-specific)	None
Parameters	None

IO Module Single-Point Indications 16

Single-Point Indications 16	
Category in the hardware catalog	Input data
Data type	16 single-point indications, see chapter *7.1.3.2 Data Type Single-Point Indication (SP, Input)*
Data size	2 bytes
Acyclic reading/writing of data	None
Parameters	None

17 I&M data is data for device identification and maintenance.

IO Module Single-Point Indications 32

Single-Point Indications 32	
Category in the hardware catalog	Input data
Data type	32 single-point indications, see chapter *7.1.3.2 Data Type Single-Point Indication (SP, Input)*
Data size	4 bytes
Acyclic reading/writing of data	None
Parameters	None

IO Module Double-Point Indications 04

Double-Point Indications 04	
Category in the hardware catalog	Input data
Data type	4 double-point indications, see chapter *7.1.3.4 Data Type Double-Point Indication (DP, Input)*
Data size	1 byte
Acyclic reading/writing of data	None
Parameters	None

IO Module Double-Point Indications 08

Double-Point Indications 08	
Category in the hardware catalog	Input data
Data type	8 double-point indications, see chapter *7.1.3.4 Data Type Double-Point Indication (DP, Input)*
Data size	2 bytes
Acyclic reading/writing of data	None
Parameters	None

IO Module Measured Values 06

Measured Values 06	
Category in the hardware catalog	Input data
Data type	6 measured values as Float32 values (floating point), see chapter *7.1.3.6 Measured Values*
Data size	24 bytes
Acyclic reading of data	Reading of 6 unit IDs as unsigned 16-bit values, see chapter *7.1.6.1 Reading Unit IDs of Measured Values and Metered Values* Reading from: • Slot: slot number of the plugged module • Subslot: 1 • Index: 100
Acyclic writing of data	None
Parameters	None

IO Module Measured Values 12

Measured Values 12	
Category in the hardware catalog	Input data
Data type	12 measured values as Float32 values (floating point), see chapter *7.1.3.6 Measured Values*

Measured Values 12	
Data size	48 bytes
Acyclic reading of data	Reading of 12 unit IDs as unsigned 16-bit values, see chapter *7.1.6.1 Reading Unit IDs of Measured Values and Metered Values* Reading from: • Slot: slot number of the plugged module • Subslot: 1 • Index: 100
Acyclic writing of data	None
Parameters	None

IO Module Single Commands 08

Single Commands 08	
Category in the hardware catalog	Output data
Data type	8 single commands, see chapter *7.1.3.3 Data Type Single Command (SC, Output)*
Data size	2 bytes
Acyclic reading/writing of data	None
Parameters	None

IO Module Single Commands 16

Single Commands 16	
Category in the hardware catalog	Output data
Data type	16 single commands, see chapter *7.1.3.3 Data Type Single Command (SC, Output)*
Data size	4 bytes
Acyclic reading/writing of data	None
Parameters	None

IO Module Double Commands 04

Double Commands 04	
Category in the hardware catalog	Output data
Data type	4 double commands, see chapter *7.1.3.4 Data Type Double-Point Indication (DP, Input)*
Data size	1 byte
Acyclic reading/writing of data	None
Parameters	None

IO Module Double Commands 08

Double Commands 08	
Category in the hardware catalog	Output data
Data type	8 double commands, see chapter *7.1.3.4 Data Type Double-Point Indication (DP, Input)*
Data size	2 bytes
Acyclic reading/writing of data	None
Parameters	None

IO Module Binary Counters 04

Binary Counters 04	
Category in the hardware catalog	Input data
Data type	4 metered values as unsigned Integer 32 values, see chapter *7.1.3.7 Metered Values (BCR, Input)*
Acyclic reading of data	Reading of 4 unit IDs as unsigned 16-bit values, see chapter *7.1.6.1 Reading Unit IDs of Measured Values and Metered Values* Reading from: • Slot: slot number of the plugged module • Subslot: 1 • Index: 100
Data size	16 bytes
Acyclic reading/writing of data	None
Parameters	None

IO Module Set Point Commands 04

Set Point Commands 04	
Category in the hardware catalog	Output data
Data type	4 set point commands, see chapter *7.1.3.8 Controllable Analog Process Values (APC, Output)*
Data size	16 bytes
Acyclic reading/writing of data	None
Parameters	None

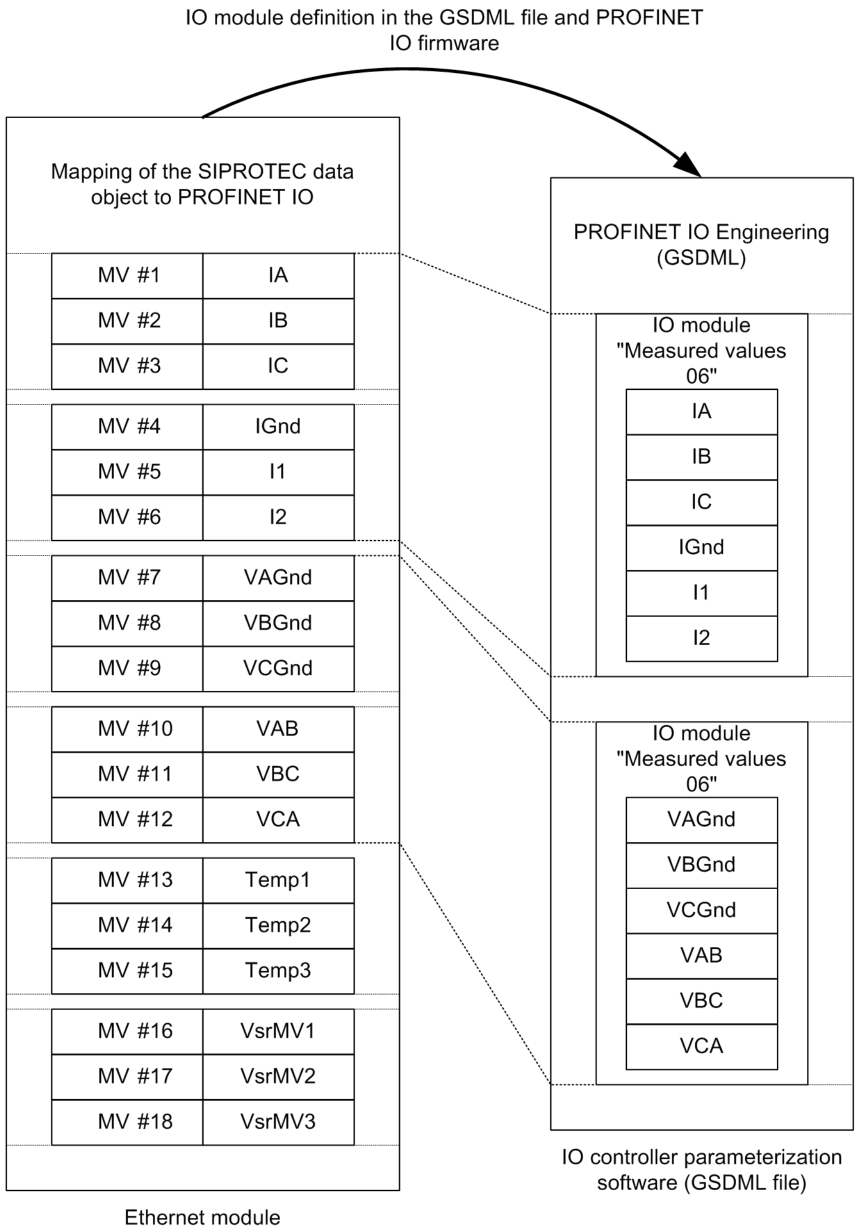
IO Module Regulating Step Commands 04

Regulating Step Commands 04	
Category in the hardware catalog	Output data
Data type	4 regulating step commands, see chapter *7.1.3.9 Binary Controlled Step Position Information (BSC, Output)*
Data size	1 byte
Acyclic reading/writing of data	None
Parameters	None

7.1.5 Assignment of IO Modules to SIPROTEC 5 Data Objects

The following components and dependencies are involved in an access to the device data via PROFINET IO:

- Mapping of SIPROTEC 5 data objects to PROFINET IO
- IO modules for PROFINET IO parameterization

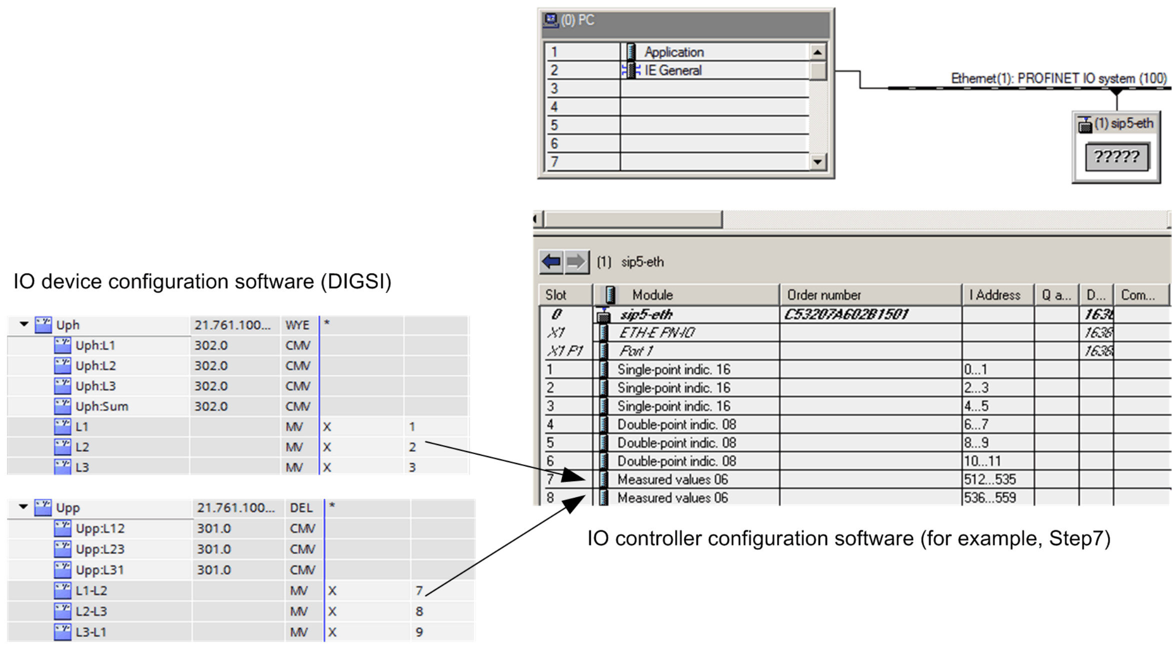


[dw_example_assign_IO_SIP, 1, en_US]

Figure 7-12 Example Assignment of the IO Modules to SIPROTEC 5 Data Objects (Measured Values)

For example, if the SIPROTEC 5 device provides 18 measured values (MV#1 to MV#18). However, only 12 measured values (current, voltage) can be transmitted and assigned to the PROFINET IO mapping in DIGSI 5 (MV#1 to MV#12). In this case, you have 2 choices as follows:

- 2 IO modules measured values 06 from the GSDML file of the SIPROTEC 5 device
- 1 IO modules measured values 12 from the GSDML file of the SIPROTEC 5 device



[sc_example_assign_IO_SIP, 1, en_US]

Figure 7-13 Parameterization Example of Assigning the IO Modules to SIPROTEC 5 Data Objects

Mapping of SIPROTEC 5 Data Objects to PROFINET IO

The mapping describes all SIPROTEC data objects which are sent or received via communication, and defines their position or identification in PROFINET IO.

Each PROFINET IO data object is assigned a PROFINET IO mapping data-object number, starting at 1 for each data type (for example, MV#1, see *Figure 7-12*).

IO Modules for PROFINET IO Parameterization

For information in the maximum data volume per data type for the data exchange, refer to chapter *7.1.9 Amount of Mappable Information*. The preset data-object assignments or the assignments entered during parameterization in DIGSI define the data at the individual mapping positions.

Only such data is transmitted via PROFINET IO which is represented by the respective IO modules.

The assignment of IO module data contents to the PROFINET IO mapping data-object numbers always starts at the smallest PROFINET IO mapping data-object number, see *Figure 7-12*.

The IO modules of one type do not have to follow directly one after another in the IO controller parameterization software.

IO modules which cannot be assigned to any PROFINET IO object are left unconsidered during the further data exchange.

7.1.6 Acyclic Reading of Data

7.1.6.1 Reading Unit IDs of Measured Values and Metered Values

An acyclic read telegram is defined for reading units. The order of the values in the telegram corresponds to the order of the values in the IO module.

Number of values	Byte offset = 0
Reserved = 0	Byte offset = 1
Unit ID #1 (Unit 16)	Start offset = 2
...	Start offset = 4
Unit ID #n (Unit 16)	Start offset = n * 2 Max. end offset = (n * 2) + 1

[dw_acyclic_data_telegram, 1, en_US]

Figure 7-14 Acyclic Data Telegram and Reading Unit IDs

Number of Values

There are 2 optional IO modules available for measured values: 6 or 12 measured values for each module.

There is only 1 IO module which is available for 4 metered values.

Unit ID #1 to Unit ID #n

The telegram always only contains as many unit IDs as entered in the byte **Number of values**. This also determines the length of the telegram.

The definition of the unit IDs is described in chapter *7.1.3.10 Unit IDs, Units, and Unit Multipliers*.

7.1.7 Executing Switching Operations via PROFINET IO

7.1.7.1 Command Output Types for Switchgear Control

The SIPROTEC 5 device supports Single command and Double command. They are controlled via PROFINET IO consistently using 2 bits of the PROFINET IO output telegram (see chapter *7.1.3.3 Data Type Single Command (SC, Output)* and chapter *7.1.3.4 Data Type Double-Point Indication (DP, Input)*).

A command can be issued in the SIPROTEC 5 device as persistent output or as pulse output.

Persistent Outputs

If a value transition (signal edge) from ***intermediate state*** or ***OFF*** to ***ON*** is detected via PROFINET IO for the associated bit pair, the commands are issued in the continuous output mode (controlled). The commands remain activated until a value transition occurs from ***intermediate state*** or ***ON*** to ***OFF*** via PROFINET IO.

You can find the definitions of the values for ***intermediate state***, ***ON***, and ***OFF*** in chapter *7.1.3.3 Data Type Single Command (SC, Output)* and chapter *7.1.3.4 Data Type Double-Point Indication (DP, Input)*.

Pulse Outputs

The SIPROTEC 5 device independently issues a control pulse for switching a switchgear, including the observation of the parameterized times.

The switching operation (pulse output via the assigned binary outputs of the SIPROTEC 5 device) is executed when a value change of the associated bit pair is transmitted in the PROFINET IO output telegram:

- For double commands from ***intermediate state*** or ***ON*** to ***OFF*** or from ***intermediate state*** or ***OFF*** to ***ON***
- For single commands from ***intermediate state*** to ***ON***

NOTE

The switching direction ***OFF*** for single commands with pulse output is not permitted and is rejected in the SIPROTEC 5 device.

7.1.7.2 Recommended Transmission of Commands via PROFINET IO

If a corresponding value change is detected at the associated bit positions of the IO module in the PROFINET IO output telegram, outputs are only set via PROFINET IO in the SIPROTEC 5 device. You can find more information in chapter *7.1.7.1 Command Output Types for Switchgear Control*.

NOTE

A value change at the associated bit position in the PROFINET IO telegram triggers a command processing operation in the SIPROTEC 5 device. However, this does not mean that the associated output actually takes the set point value. For example, the setting of an output caused by interlocking can be rejected. The feedback of a switching device should be read back for monitoring purposes.

If the bit combination for a command changes and the bit value for ***ON*** or ***OFF*** is still transmitted (statically) in the cyclic output telegram, this has no consequences in the SIPROTEC 5 device while communication is running.

A statically set bit combination for ***ON*** or ***OFF*** may cause undesirable command executions when communication is restored in the event of communication interruptions (see chapter *7.1.8 Behavior When Communication to IO Controller is Faulted*) or STOP of the PLC (see chapter *7.3.2.2 PLC in STOP during Communication with SIPROTEC 5 Device*) or when the PLC switches from STOP to RUN.

Siemens therefore recommends transmitting switching operations in SIPROTEC 5 devices via PROFINET IO by using a pulse over the bus:

- Intermediate state (**00**) → ON (**10**) → intermediate state (**00**) for switching on
- Intermediate state (**00**) → OFF (**01**) → intermediate state (**00**) for switching off

The pulse duration (period during which the bit combinations for ***ON*** or ***OFF*** apply) should be at least 3 times the set cycle time of the IO device (reference value at least approx. 100 ms).

7.1.7.3 Multiple Command Output

Command processing in the SIPROTEC 5 device operates in a 100-ms cycle. This includes:

- Command checking
- Command output
- Feedback monitoring
- Generating positive or negative command feedback

If a positive command feedback has been issued, which is also entered as a change of the value of the switchgear position in the cyclic input telegram via PROFINET IO, command processing remains active for one cycle maximum (100 ms).

As the SIPROTEC 5 device does not process several commands in parallel, an additional command, which is received within an active command processing, is rejected and is not executed.

If it is desired that the IO controller issues 2 or more commands directly one after another, a time delay of 100 ms must be observed after reception of the positive command feedback in the cyclic input data until issuing of the next command. This ensures that the subsequent command is executed in a reliable way.

7.1.7.4 Behavior During Special Operating Conditions

- The IO controller detects a change of the switchgear position not initiated by the IO controller (for example, circuit-breaker trip) by the change of the value of the switchgear position in the associated bit positions of the input telegram.
  If, for example, the IO controller wants to restart the switchgear that was switched off locally, it must first transmit the ACTUAL value (***OFF***) or ***intermediate state*** via PROFINET IO and can subsequently restart the switchgear by setting the TARGET value (***ON***).
- The IO controller detects when a switching operation requested via PROFINET IO cannot be executed, because the switching authority is set to ***LOCAL***, for example, or the associated bay interlocking is not satisfied. The IO controller recognizes this because the feedback of the double command/single command in the PROFINET IO input telegram is not updated according to the TARGET switch position (activate a feedback monitoring time in the IO controller if necessary).
  Before a new switching attempt, the ACTUAL switch position for switchgear must first be transmitted again according to the input telegram or ***intermediate state*** in the output telegram.
- You can find information on the behavior during communication interruptions in chapter *7.1.8 Behavior When Communication to IO Controller is Faulted*.

7.1.8 Behavior When Communication to IO Controller is Faulted

The following behavior is defined for SIPROTEC 5 devices when the communication to the IO controller is interrupted:

After Having Recognized that the Connection Is Interrupted

- The marking **Channel Live** in the SIPROTEC 5 device is set to ***OFF*** (logging in the operational log, processing in CFC possible).
- The state of the outputs or switchgear has not changed compared to the state before communication interruption.

After the Communication Has Been Restored

- The marking **Channel Live** in the SIPROTEC 5 device is set to ***ON*** (logging in the operational log, processing in CFC possible).
- The data from the telegrams again received by the IO controller is taken over (if permitted by the switching authority and the interlocking specifications).

If you do not want the switchgear positions of the SIPROTEC 5 devices to be affected after the connection between the IO controller and IO device has been restored, ***intermediate state*** (value **00**) must be issued in the associated bit positions in the output telegram, or the switching authority must be set to ***(LOCAL)***.

7.1.9 Amount of Mappable Information

The following information can be mapped:

Information	Maximum Mappable Amount
Indication + controllable at Tx (Tx: transfer direction)	500
Controllable at Rx (Rx: receive direction)	20
Settings at Tx	Not available
Measurements at Tx	40
Metered values	10

NOTE

Siemens recommends configuring the signals according to the table and the following suggestion.

If the addresses (**value** in DIGSI mapping matrix) of the same type signal are not continuous, the range should less than the maximum mappable amount in the preceding table.

NOTE

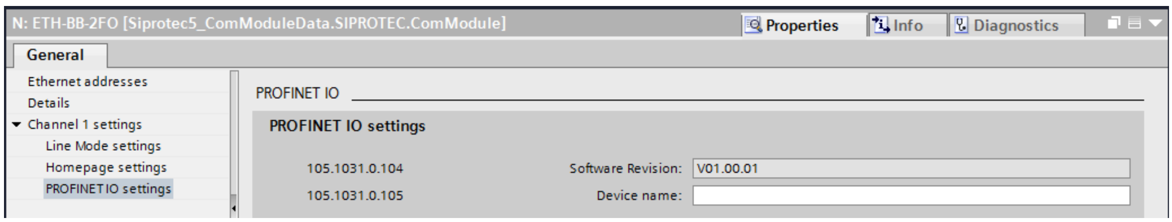
Avalanche scenarios with many process changes (for example, 100 per second) are supported.

7.2 Settings and Properties

7.2.1 Settings

IO Device Name

The device name of the PROFINET IO is assigned via DCP. You can find more information in chapter *9.4.2 Network Settings and Device Name*.



[sc_Pro_Settings, 1, en_US]

Figure 7-15 Protocol Settings

During the parameterization, make the following settings for the communication between the PROFINET IO controller and the SIPROTEC 5 device via PROFINET IO.

Parameter Name	Type	Description	Settings
Software Revision	Int16	Read only Software revision of the Ethernet module	V01.00.01
Device Name	String	Name of the IO device	-

NOTE

Siemens recommends configuring the device name without blank and underline characters. And **unassigned** is reserved word for internal using.

7.3 Parameterizing IO Controller

7.3.1 PROFINET IO Configuration

The SIPROTEC IO device is configured using the parameterization software of the IO controller. For this purpose, the GSDML file of the SIPROTEC IO device is loaded into the parameterization software of the IO controller. This file contains the description of the device properties and the configuration options of the electric Ethernet module and optical Ethernet module with PROFINET IO.

The GSDML file is named GSDML-V2.32-Siemens-SIPROTEC-<date>.xml, for example GSDML-V2.32-Siemens-SIPROTEC5-20160525 .xml, with <date> being the version date of the GSDML file.

7.3.2 Siemens S7 PLC and Step7

7.3.2.1 Overview

Observe the following information concerning the configuration when using the SIPROTEC 5 devices via PROFINET IO in combination with Siemens S7 PLC and the Step7 parameterization software.

You can find more information for Siemens S7 PLC and the Step7 parameterization software on the following Internet page: *https://support.automation.siemens.com/*.

7.3.2.2 PLC in STOP during Communication with SIPROTEC 5 Device

If the PLC is switched from RUN to STOP or switches to STOP due to an internal PLC program response during PROFINET IO communication with the SIPROTEC 5 device, the running PROFINET IO communication between the IO controller of the PLC and the IO device of the SIPROTEC 5 device remains active. Cyclic data exchange continues, that is, communication is not interrupted.

For all IO modules in output direction, however, the IOPS (IO Provider Status) from the PLC is set to **bad** and the data of these IO modules are transmitted with all values equaling zero.

When changing from RUN to STOP, the status of the outputs in the SIPROTEC 5 device remains in the status during RUN.

The tagging SysIntErr. in the SIPROTEC 5 device (see chapter *7.1.8 Behavior When Communication to IO Controller is Faulted*) is not set.

During transition from STOP to RUN, the data from the cyclic telegrams are accepted and output for the IO modules in output direction once the IO controller has restored the IOPS for these IO modules to **good**.

If you want the outputs of the SIPROTEC 5 device to remain unaffected during transition from STOP to RUN, the ***intermediate state*** (value **00**) is to be output at the associated bit positions in the output telegram. You can find more information on executing switching operations in chapter *7.1.7 Executing Switching Operations via PROFINET IO*).

7.3.2.3 Periphery Access Commands

The S7-CPUs can access data received by the connected devices via PROFINET IO or write data to these devices using periphery access commands in the CPU program.

To read a measured value (float value, 4 bytes, see chapter *7.1.3.6 Measured Values*) from the SIPROTEC 5 device, the command **L PID x** is used, for example, with x denoting the address of the measured value in the periphery address space of the S7-CPU.

To read, for example, 5 measured values, the preceding instruction must be executed 5 times with the associated addresses. After each reading operation, the values must be processed or copied in a data block for subsequent processing in the program, for example:

- L PID x
- T DB10.DBD y etc.

The measured value read from address x is written to element y of data block DB10 assuming that DB10 is a data block with inputs of the type REAL.

7.3.2.4 Reading and Writing Data with SFC14 and SFC15

The S7 system functions SFC14 (**DPRD_DAT**) and SFC15 (**DPWR_DAT**) in the CPU program can also be used to transmit data instead of periphery access commands. This is possible for data within an IO module.

To read, for example, all 12 measured values of an IO module **measured values 12** in one call and transmit them into a data block, proceed as follows:

✧ Create a data block to accommodate the data to be read (with 12 REAL values).

✧ Call SFC14:

CALL SFC14

LADDR: = W#16#200 // IO module address, for example, 512, hexadecimal

RET_VAL: = MW100 // for example, flag word 100 as return value

RECORD: = P#DB10.DBX0.0 BYTE 48 // 12 values = 48 bytes to DB10, for example

If the destination data block contains more information than only the 12 measured values and if these do not start at data-block byte 0, you can also start copying at this offset, for example with:

CALL **DPRD_DAT**

LADDR: = W#16#200

RET_VAL: = MW100

RECORD: = P#DB10.DBX24.0 BYTE 48 // 48 bytes to DB10, for example, starting from byte 24

7.3.2.5 Reading and Writing Acyclic Data with SFB52

The SIPROTEC IO device offers acyclic datasets (see chapter *7.1.6 Acyclic Reading of Data*) that can be read or written with the following system function blocks in the S7 SPS:

- Reading unit IDs → reading with SFB52 (**RDREC**)

Reading the unit IDs of an IO module **measured value 12** is illustrated using the following example.

The SFB52 operates asynchronously, that is, reading the acyclic data can last several PLC user cycles.

Define the structure of the dataset to be read in a data block, for example DB11:

SFB52 Call

The data block DB52 is required as instance DB for calling SFB52. If it does not exist yet, you are prompted automatically whether to generate DB52 when entering the example shown in the following section.

You can use other flags or data blocks instead of those used in the example (DB11, M10, MD21, MW25, and MW100).

CALL SFB52, DB52

REQ := M10.3 // Triggering the read job

ID := DW#16#200 // IO module address, for example, 512, hexadecimal

INDEX := 100 // Index of the acycl. data, see chapter *7.1.4 IO Modules*

MLEN := 26 // Length of the data to be read, see chapter *7.1.6.1 Reading Unit IDs of Measured Values and Metered Values*

VALID := M10.0 // SFB52 return value: TRUE = dataset was read

BUSY := M10.1 // SFB52 return value: TRUE = reading in process

ERROR := M10.2 // SFB52 return value: TRUE = read error

STATUS := MD21 // SFB52 return value: error code

LEN := MW25 // SFB52 return value: length of the read // Information in bytes

RECORD := P#DB11.DBX0.0 BYTE 26 // Destination for the read data

In the example, M10.3 = TRUE triggers reading of the unit IDs.

M10.1 and M10.2 are used to check in each subsequent PLC user cycle whether the reading process is still running or whether an error has occurred.

If the reading process has been completed, M10.0 indicates that the dataset has been read successfully and that the data are available in the destination data block.

Acyclic data (for example to preset metered values or statistical values) is accomplished with SFB53 in a similar way to the SFB52 example for reading:

- Define the structure of the dataset to be written in a data block
- Specify the data to be written in the data block

8 Protection Interface

8.1 Information on the Protection Interface, PMU, and Web User Interface

You can find a more detailed description of the protection interface and the Phasor Measurement Unit (PMU) in the following chapters of the device manual:

- Protection Interface and Protection Topology
- Phasor Measurement Unit (PMU)

You can find a more detailed description of the browser-based user interface in the SIPROTEC 5 Operation Manual in the chapter Operation with a Browser-Based User Interface.

9 Additional Ethernet Services

9.1 Activation and Ability to Deactivate the Services

The following additional Ethernet services are available for the integrated Ethernet interface (Port J) of the device:

- DIGSI 5 protocol (always available)
- DCP
  Activates the Discovery and Basic Configuration Protocol (DCP) for the Ethernet module
  This protocol allows DIGSI 5 to find a SIPROTEC 5 device in the local network without an IP address.
- SNTP
  Activates the Simple Network Time Protocol (SNTP) for the Ethernet module
  This protocol is needed for the time synchronization over an Ethernet network.
- SUP Ethernet (for connecting external analog units)
  Activates **SUP Ethernet** (Slave Unit Protocol via Ethernet) for the Ethernet module
  This protocol is used for the communication between the RTD unit and the SIPROTEC 5 device.

The following additional Ethernet services are available for the Ethernet communication module:

- DIGSI 5 protocol (always available)
- DCP
- SNMP
  Activates the Simple Network Management Protocol (SNMP). Provides monitoring information about the device to the network-management system.
- SNTP
- IEEE 1588
  Activates **IEEE 1588** for the module.
  This protocol is used for time synchronization via the network communication.
- SUP Ethernet (for connecting external analog units)
- Homepage
  Activates the homepage for the Ethernet module
  Ethernet communication modules provide a testing and diagnostic function. With the IP address/home, these values can be read with a browser. During operation, the Homepage can be switched off (safety function), and the http port disappears. Only read access is supported.

You can select the following network redundancy protocols:

- RSTP
  Activates the Rapid Spanning Tree Protocol (RSTP) for the Ethernet module
  This protocol will be needed for redundant ring structures in the Ethernet networks.
- PRP
  Activates the Parallel Redundancy Protocol (PRP) for the Ethernet module
  With the PRP structure, communication takes place simultaneously over 2 independent networks.
- HSR
  Activates the High Availability Seamless Redundancy Protocol (HSR) for the Ethernet module
  With the HSR structure, the devices are arranged in rings.
- Line Mode
  Activates the line structure

With the exception of the DIGSI 5 protocol, all additional Ethernet services can be switched on and off for each Ethernet interface on the device. As a result, you can decide for yourself under security aspects whether the device should react to SNMP access or not.

You can find more information on SUP Ethernet in the following manuals:

- SIPROTEC Transformer Differential Protection
- SIPROTEC Distance Protection, Line Differential Protection, and Overcurrent Protection for 3-pole Tripping
- SIPROTEC Distance Protection, Line Differential Protection, and Switch Management for 1-pole and 3-pole Tripping

Activating the Ethernet Service via DIGSI

✧ To switch on an Ethernet service in the device, activate the corresponding check box in the channel settings of the Ethernet communication module or for the integrated Ethernet interface.

Deactivating the Ethernet Service via DIGSI

✧ To switch off an Ethernet service in the device, deactivate the corresponding check box.
You will find additional information regarding network security in the Security Blueprint.

9.2 Ports of the SIPROTEC 5 Devices

The following list of all ports used in a SIPROTEC 5 device should help with the firewall settings for a network with SIPROTEC 5 devices.

Port	**Functionality**
TCP Port 443	DIGSI 5 protocol
TCP Port 102	IEC 61850-8-1 MMS protocol
Multicast	GOOSE
UDP Port 123[18]	SNTP
UDP Port 161	SNMP
Broadcast	DCP
Port 502[19]	SUP
HTTP	Homepage
TCP Port 2404 (configurable)	IEC 60870-5-104
TCP Port 20000 (configurable)	DNP3
TCP Port 8080 to 8083	Homepage See chapter *9.13.1 Content and Structure*.
TCP Port 4443	Web user interface

18 UDP – User Datagram Protocol
19 Can be modified via DIGSI

9.3 DIGSI 5 Protocol

There are 3 ways to connect from DIGSI to a device:

- Via USB
- Via the integrated Ethernet interface (Port J)
- Via an Ethernet communication module.

NOTE

Only a SIPROTEC 5 device can be connected with DIGSI via USB.
Use the Ethernet interfaces for connections to several SIPROTEC 5 devices.

An IP-based internal Siemens protocol is used for data transmission between DIGSI and a SIPROTEC 5 device.

DIGSI and the SIPROTEC 5 device are authenticated via SSL (Secure Sockets Layer). The necessary certificates are contained in the device or DIGSI upon delivery.

You can find more information on the diagnostic pages in DIGSI in chapter *10.1.5 Diagnostic Information for IEC 61850*.

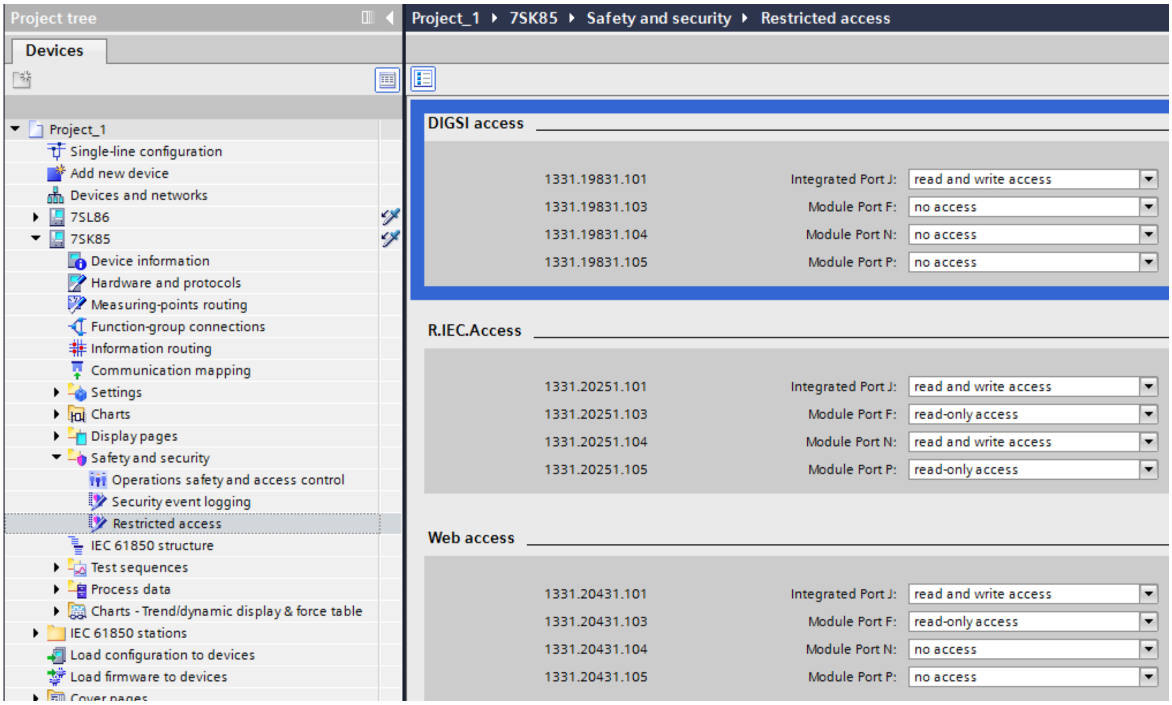
Security Settings

The security settings allow you to restrict the access rights for each Ethernet interface (Port J and Ethernet communication module).

You define the security settings in DIGSI in the **Project tree** under **Safety and Security** → **Restricted access**.

You can assign the following access rights:

- No access:
  This interface allows no DIGSI communication.
- Read-only access:
  This interface only allows read access to the device.
- Read and write access:
  This interface allows read and write access to the device.



[sc_security_settings, 1, en_US]

Figure 9-1 Security Settings in DIGSI

9.4 DCP Protocol

9.4.1 DCP

The Discovery and Basic Configuration Protocol (DCP) is used for automatic recognition of devices without a configured IP address. DIGSI 5 can find all SIPROTEC 5 devices in the network using DCP.

DCP is not required for the functionality of communication protocols. The protocol can however in parallel be configured for a DIGSI Life List functionality.

The DIGSI Life List shows the connected devices. You can monitor and process these devices via the DIGSI Life List.

If you also desire a DIGSI Life List functionality through the LAN, then you must activate DCP.

If you create a new device in DIGSI or add an Ethernet communication module to the device, DCP is activated. If you change this recommended default and want to switch off the DIGSI Life List functionality in the device, deactivate the DCP check box in the channel settings of the Ethernet communication module or for the integrated Ethernet interface.

NOTE

If you have deactivated the DIGSI access via the communication module and the integrated Ethernet interface in the security settings (see chapter *9.3 DIGSI 5 Protocol*), a DIGSI connection via DCP is also not possible.

9.4.2 Network Settings and Device Name

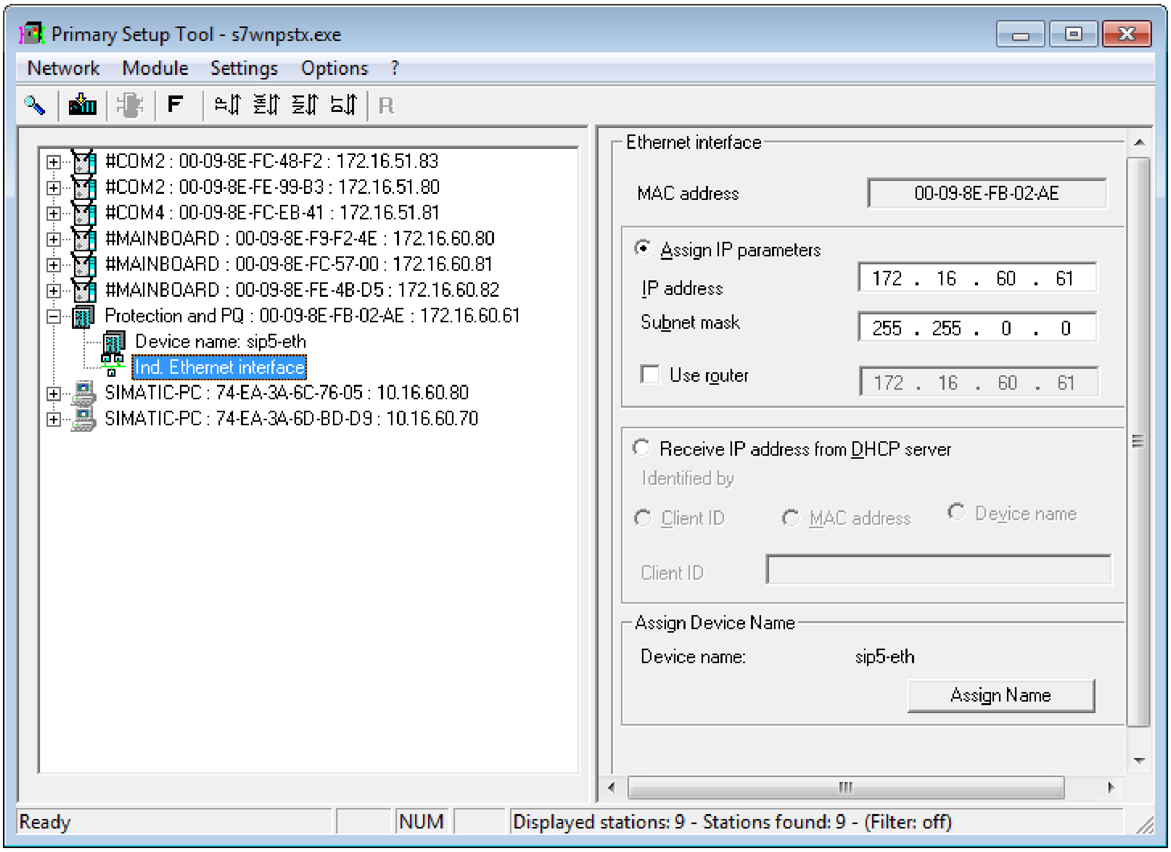
You can change the network settings of the Ethernet module and the name of the PROFINET IO device by using DCP. The DCP service is in conflict to the original one in DIGSI 5. If you configure the PROFINET IO protocol on the communication module in DIGSI 5, you must disable the original DCP. Use the Primary Setup Tool stated in *Figure 9-2* for this purpose.

NOTE

The Ethernet module with PROFINET IO does not support the DIGSI DCP service.

The Ethernet module with PROFINET IO does not support DHCP.

If no valid configuration exists for PROFINET IO, access to the device via DCP is also possible.



[sc_Pri_Setup_Tool, 1, en_US]

Figure 9-2 Primary Setup Tool: Main Window

9.4.3 Reset to Default Settings

After having restored the factory settings, the Ethernet module performs a **reset** and a restart with the following settings:

- IP address and subnet mask: IP address and subnet mask set in DIGSI
- Default gateway: 0.0.0.0
- No device name is assigned (empty device name) in **Homepage**, and **unassigned** in device HMI.

9.5 SNTP

9.5.1 Protocol Description

The Simple Network Time Protocol is used to synchronize clocks via the Internet. With SNTP, client computers can synchronize their clocks with a time server via the Internet.

SNTP enables a time resolution of 1 ms. When considering similar runtimes, SNTP can determine the average runtime of a synchronization telegram between the client and the server in the Ethernet network. This transmission time can be taken into account in the terminal device and improves synchronization of terminal devices.

SNTP is available for the integrated Ethernet interface (Port J) and in all Ethernet communication modules.

Version SNTPv4 is supported.

Time Server in the Network

For time synchronization via Ethernet according to SNTP, a time server must be present in the network. 1 or 2 time servers are supported. This time server must also be able to address the different time requirements of the devices as defined in SNTP. Time servers can be reached through an IP address.

The following SNTP settings can be configured:

Parameter Name	Settings	Default Setting
Time source 1	IP address of the SNTP server	10.16.60.1
Time source 2	IP address of the redundant SNTP server If no 2nd SNTP server is available, you can leave the default setting for the time source 2 unchanged.	10.16.60.2
Time interval	SNTP server inquiry time interval Time interval: 15 s to 60 s	15 s
Start time	Reference when the device queries the time. Time interval: 1 s to 3600 s	20 s

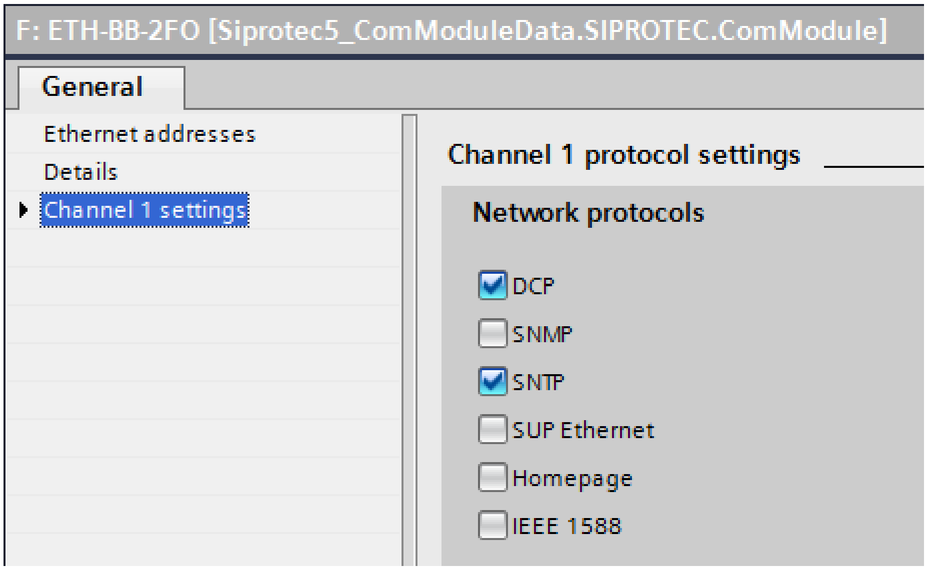
If the 1st SNTP time server configured in the network cannot be reached, the 2nd SNTP server is automatically queried. If the 2nd SNTP time server also cannot be reached, there is no synchronization via SNTP. The device reports a time-synchronization failure.

9.5.2 Setting the Parameters for Time Synchronization

For the purpose of time synchronization, activate SNTP on the Ethernet communication module or on the integrated Ethernet interface.

✧ To activate SNTP on the Ethernet module, select the Ethernet communication module in the Device view.

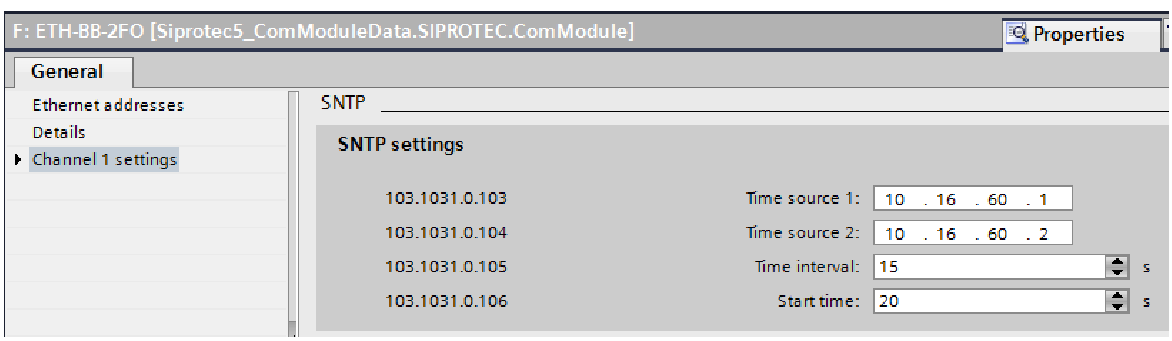
✧ Place a check mark at SNTP under **Channel 1 settings** in the **Network protocols** section.



[sc_tmsync SNTP, 1, en_US]

✧ If diagnostics is desired, place a check mark at **Homepage** and set the **Homepage Mode** to **on** in the **Homepage Settings**.

✧ To access the **SNTP settings** section, click **Channel 1 settings**.
You can make the SNTP settings in this section.



[sctmsync-140113-01.tif, 2, en_US]

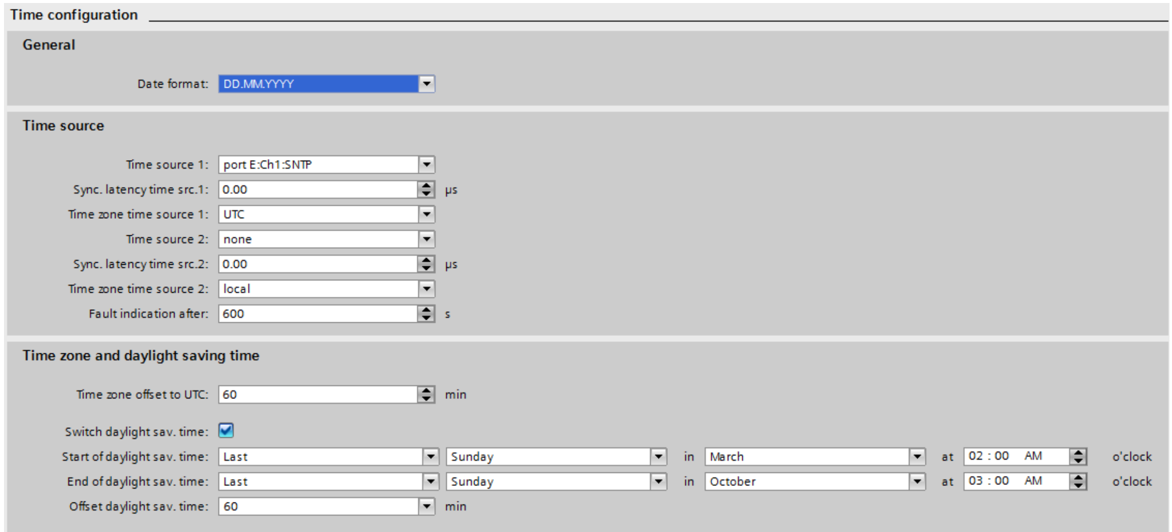
Figure 9-3 SNTP Settings

NOTE

Redundant SNTP time servers are supported. The device gets the time information from both time servers. If there is no 2nd SNTP server, set the value **0.0.0.0** for **Time source 2**. Setting another value can result in error messages.

✧ Select a device in the **Project tree**.

✧ Under **Settings**, select the **Time settings** section.
Here, you can select SNTP as the time source under **Time source 1**.



[sctmsyn2-140113-01.tif, 2, en_US]

Figure 9-4 Setting the Time Source

9.6 IEEE 1588

9.6.1 Protocol Description

The IEEE 1588 protocol is used for synchronization of clocks via the network communication. IEEE 1588 is available in all Ethernet communication modules as time receiver.

Runtimes and processing times in the components are also transmitted within the protocol. These correction times can be taken into account in the end device and improve synchronization of end devices.

The direct Ethernet transport via a Multicast Ethernet MAC address in compliance with Annex F of the IEEE 1588 standard is used (Annex F Transport of PTP over IEEE 802.3/Ethernet). Receiving telegrams with IEC 62439-3 (PRP) is supported.

9.6.2 Setting the Parameters for Time Synchronization

For time synchronization, activate IEEE 1588 on the Ethernet communication module ETH-BA-2EL, ETH-BB-2FO, or ETH-BD-2FO.

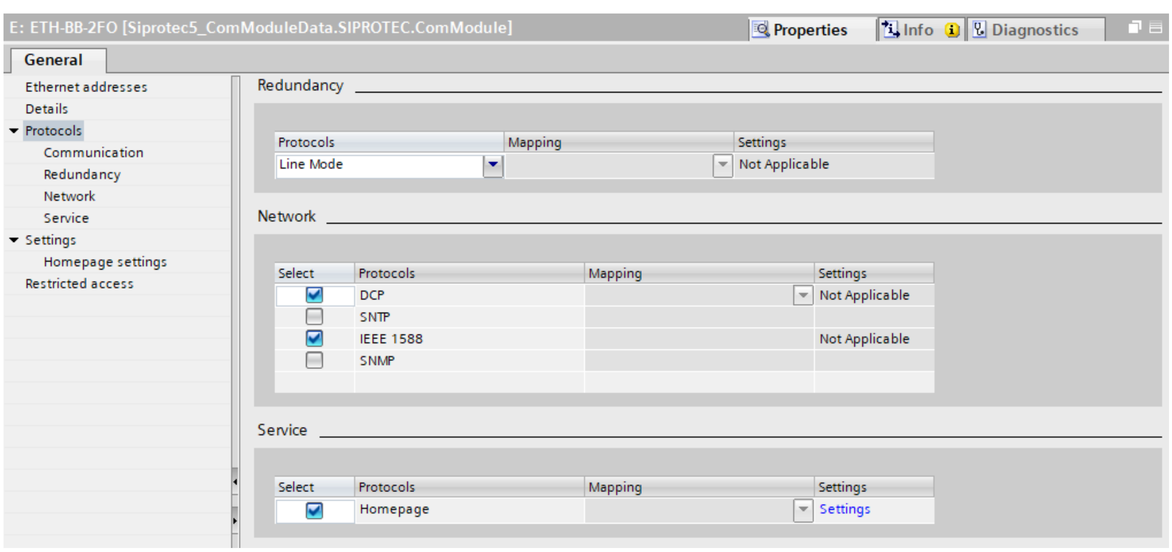
✧ To activate IEEE 1588 on the Ethernet module, select the Ethernet communication module under **Hardware and Protocols** in the Device view.

✧ Under **Protocols** in the **Network protocols** section, mark the check box **IEEE 1588**.

✧ If a diagnosis is required, mark the check box **Homepage** and set the **Homepage mode** to **On** in the **Homepage Settings**.

You can find more detailed information in the chapters *9.13.4.2 Network Protocols – IEEE 1588 for the Modules ETH-BA-2EL and ETH-BB-2FO* and *9.13.4.3 Network Protocols – IEEE 1588 on the Module ETH-BD-2FO*.

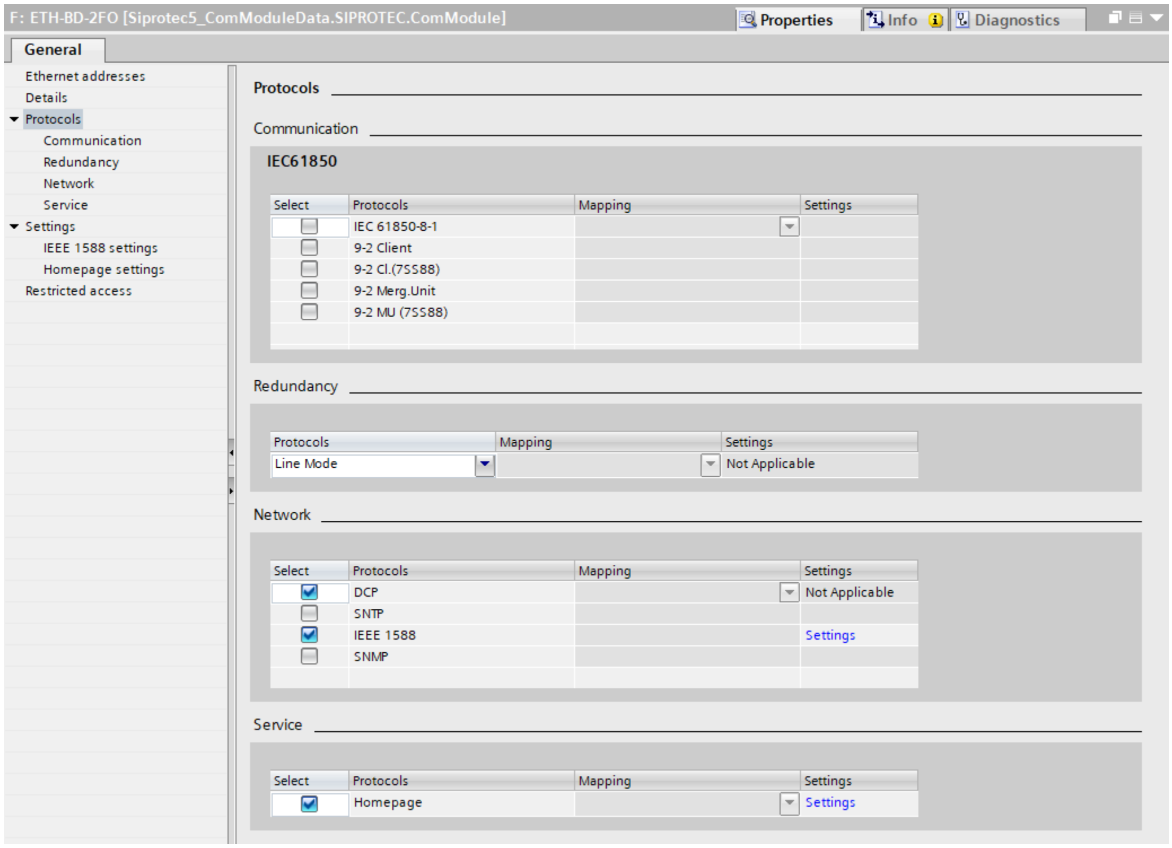
No further settings are required for the instantiation of the IEEE 1588 protocol on the ETH-BA-2EL or ETH-BB-2FO module. The following figure shows the activation of IEEE 1588 using the ETH-BB-2FO module as an example.



[sc_IEEE1588Activating_BB, 1, en_US]

Figure 9-5 IEEE 1588 Activation for ETH-BB-2FO

Further settings are required for the instantiation of the IEEE 1588 protocol on the ETH-BD-2FO module.



[sc_IEEE1588Activating_BD, 1, en_US]

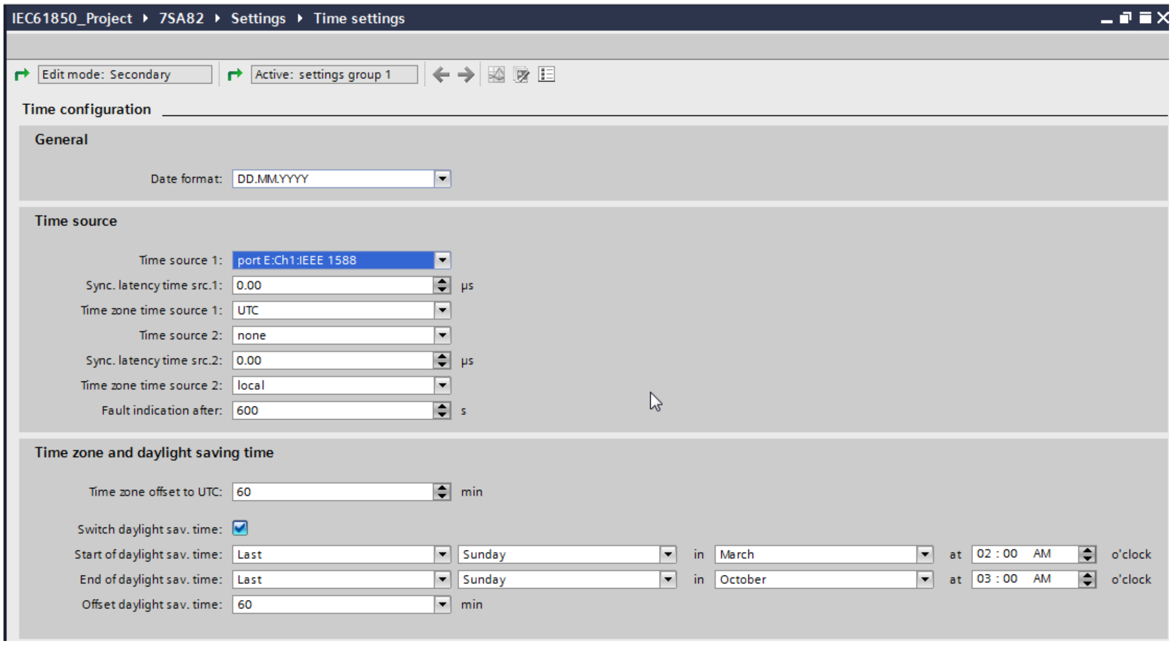
Figure 9-6 IEEE 1588 Activation for ETH-BD-2FO

Using IEEE 1588 as a Time Source

✧ Under **Settings**, select the **Time settings** section.
There, you can select IEEE 1588 as the time source under **Time source 1** as well as under **Time source 2**.

✧ If you have selected IEEE 1588 as the time source, set the respective **Time zone** to **UTC**.

✧ With **Fault indication after**, you can specify the time after which a time source is categorized as malfunctioning and after which a switchover to the redundant **Time source 2** takes place if **Time source 1** is faulty.

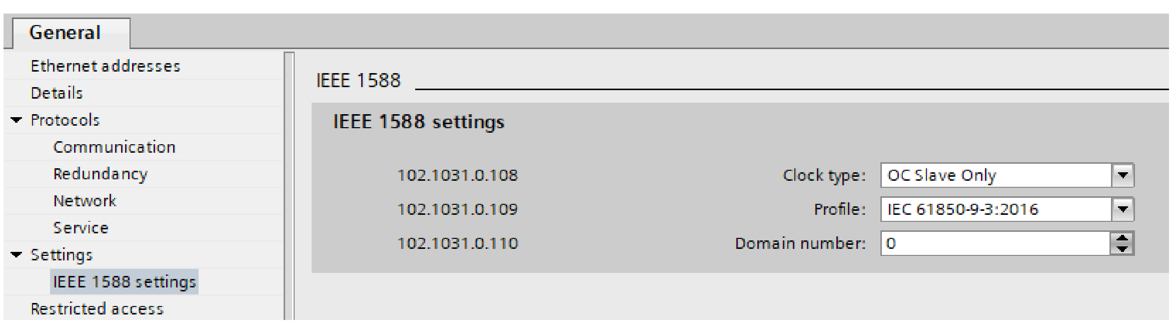


[sc_IEEE1588 time zone, 3, en_US]

Figure 9-7 Setting the IEEE 1588 Time Source

9.6.3 Settings and Properties

Compared to the modules ETH-BA-2EL and ETH-BB-2FO, the IEEE 1588 protocol instantiated on the module ETH-BD-2FO is more accurate in time synchronization. *Figure 9-8* shows the settings of the IEEE 1588 protocol on the module ETH-BD-2FO. In this module, the time stamp for IEEE 1588 is generated by hardware. With this scheme, the accuracy of IEEE 1588 time synchronization can reach the sub-microsecond range.



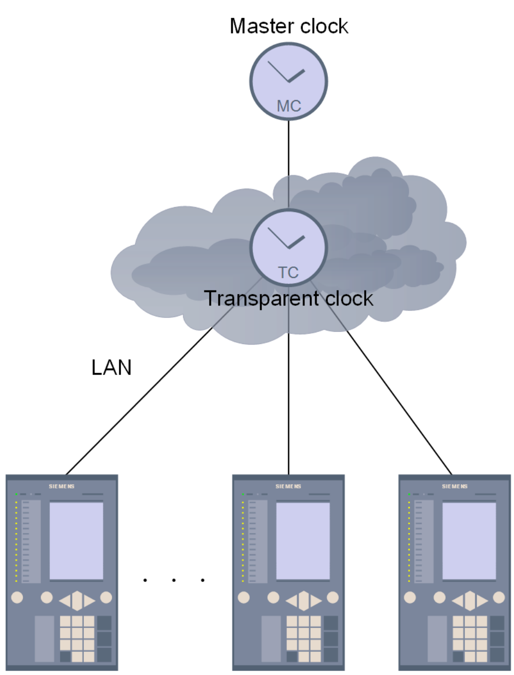
[sc_BDModuleSettings, 1, en_US]

Figure 9-8 IEEE 1588 Settings on the Module ETH-BD-2FO

Table 9-1 Setting Notes

Parameter Name	Description	Default Setting	Setting Range
Clock type	With the parameter **Clock type**, you select the PTP clock type.	OC Slave Only	–
Profile	With the parameter **Profile**, you select the PTP clock profile. The PTP clock profile represents a set of allowed PTP features applicable to the specific industry.	IEC 61850-9-3:2016	–
Domain number	With the parameter **Domain number**, you select the PTP domain number. A PTP domain is a logical grouping of PTP clocks. The clocks synchronize to each other using the IEEE 1588 protocol.	0	0 to 255

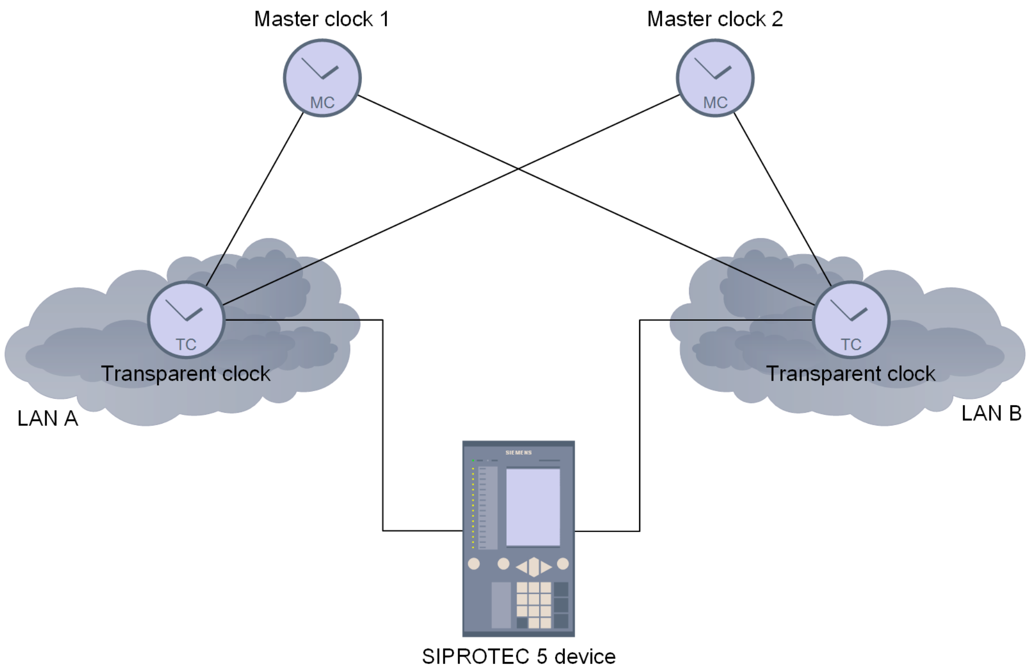
The following figure shows an example of the IEEE 1588 time synchronization via the non-redundancy connection.



[dw_Non-RedundancyExample, 2, en_US]

Figure 9-9 Example of a Star Topology

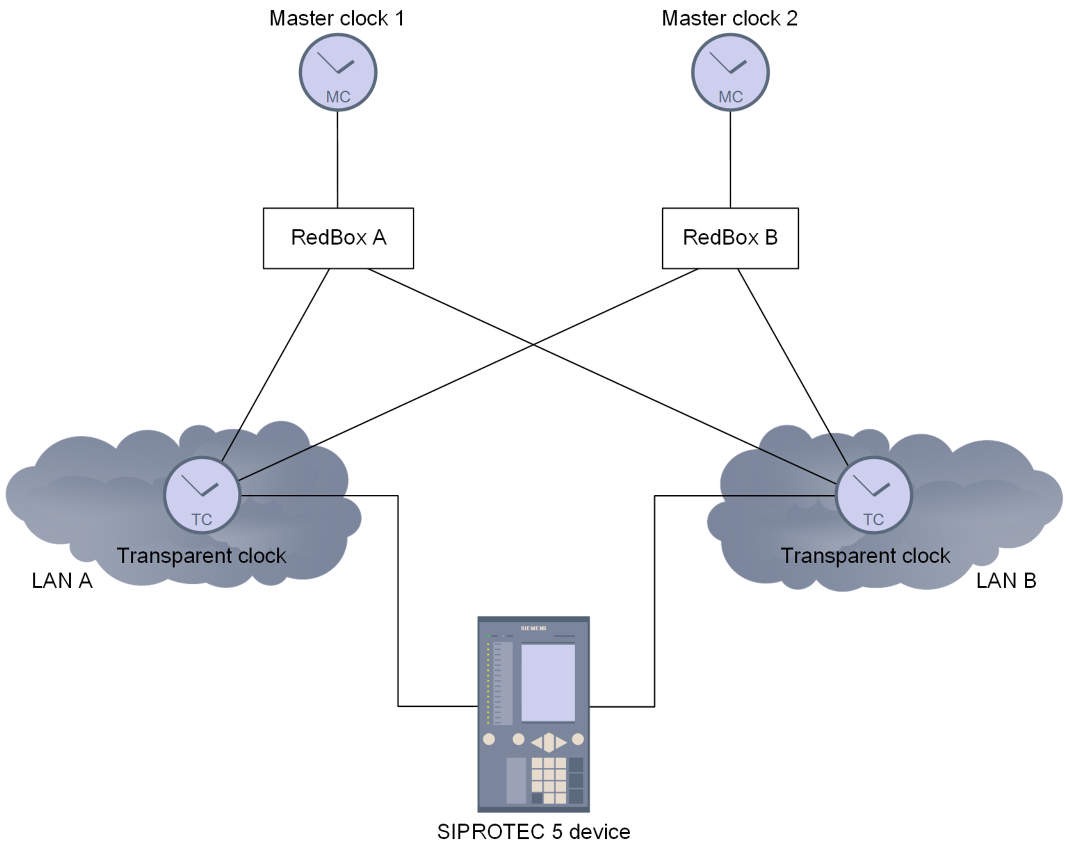
The following figure shows an example of the IEEE 1588 time synchronization via a PRP network.



[dw_PRPExample, 3, en_US]

Figure 9-10 Example of a PRP Network

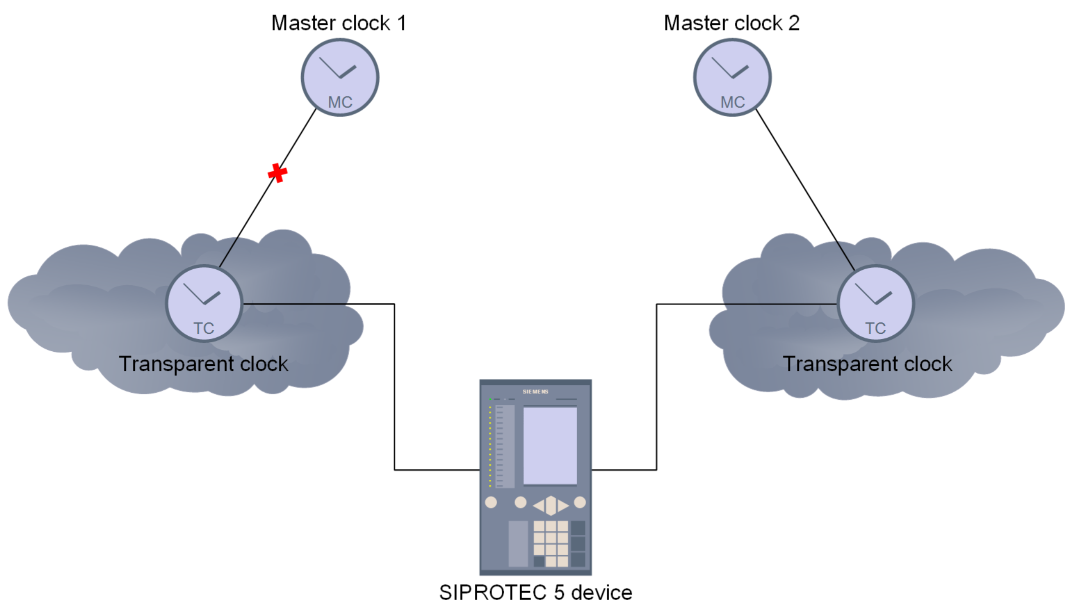
If the master clock cannot support the native PRP function, use a RedBox.



[dw_PRPExtendedExample, 2, en_US]

Figure 9-11 Example of a PRP Network with 2 RedBoxes

The following figure shows an example of the IEEE 1588 time synchronization via a redundant network. If the module ETH-BD-2FO is configured in the **Dual Homing** operating mode, only one of the connected lines is active at any moment. Therefore, if the active master clock, for example, master clock 1, is down, the SIPROTEC 5 device in this topology cannot be synchronized via IEEE 1588.



[dw_PRP_dualHoming_Example, 1, en_US]

Figure 9-12 Example of an Improper Network Configuration

9.6.4 Signals

There are 2 signals for the IEEE 1588 protocol:

- *Health*
  The signal indicates the state of the protocol. The following 3 states can occur in this case:
  - ***OK***
    The state indicates that the protocol is working.
  - ***Warning***
    The state indicates the failed parameterization[20].
  - ***Alarm***
    The state indicates the failure of the protocol.
- *Channel Live*
  The signal indicates the state of the IEEE 1588 traffic during the IEEE 1588 running phase:
  - ***Off***
    When the state of *Channel Live* is ***Off***, no packet exchange with other IEEE 1588 clocks is active.
  - ***On***
    When the state of *Channel Live* is ***On***, the packet exchange with other IEEE 1588 clocks is active.

9.6.5 Technical Data

IEEE 1588 Protocol Properties (via Module ETH-BD-2FO)

Clock type	Ordinary clock
1-step or 2-step operation	2-step on egress
End-to-end, peer-to-peer, or manual-delay calculation	Only peer-to-peer

20 If the IEEE 1588 protocol did not get the correct settings from the mainboard and then started with default settings, a failed parameterization occurs.

Transport type	Layer 2 (Ethernet) transport
Slave-only mode	Yes
Supported profiles	IEC 61850-9-3: 2016 Power Utility Profile
Priority 1	255
Priority 2	255

Accuracy Data (via Module ETH-BD-2FO)

The accuracy data is acquired via a test. The test is proceeded by using RuggedCOM RSG2488 (with GPS input) as the grandmaster clock and using RuggedCOM RST2228 as the transparent clock.

Max. number of TCs (transparent clocks) crossed to keep 1 μs accuracy in a steady state	6
Accuracy over time after the time synchronization is lost	Less than 15 ms/24 hours
Hold over time	5 s

NOTE

The prerequisite for the accuracy data is that the grandmaster clock, transparent clocks, and ETH-BD-2FO are interconnected with optical media.

If the electrical media is used and a copper SFP transceiver is inserted in ETH-BD-2FO, the time accuracy of IEEE 1588 can be degraded due to the uncertain latency introduced by the built-in PHY. This accuracy data can vary with SFP transceivers from different vendors. Siemens recommends using only optical SFP transceiver models approved by Siemens for IEEE 1588.

9.6.6 IEEE 1588 Protocol Implementation Conformance Statement (PICS)

NOTE

This PICS only applies to the IEEE 1588 protocol instantiated on the module ETH-BD-2FO.

Conventions

The **Base** column shows the definitions and specifications in the base standard. Each entry in this column is selected from the following list:

- Mandatory (m): The base standard mandates this capability and it is implemented.
- Optional (o): The base standard leaves this capability optional, but it is implemented.

The **Condition** column shows the condition for the capability. Each entry in this column is selected from the following list:

- Conditionally supported (c): This capability is supported under the conditions specified in the corresponding index in the PICS table.
- Unconditionally supported (–): This capability is not constrained.

PICS

Table 9-2 Precision Time Protocol Profile for Power-Utility Automation

PICS Proforma Reference	Capability	Range of Values	Base	Condition	Support
CLOCK_TYPE_OC	Clock is OC according to this base.	True, False	m	c.1	True
CLOCK_TYPE_TC	Clock is TC according to this base.	True, False	m	c.1	False
CLOCK_TYPE_BC	Clock is BC according to this base.	True, False	m	c.1	False

PICS Proforma Reference	Capability	Range of Values	Base	Condition	Support
NR_PORTS	Number of clock ports (total)	Integer > 0	m	-	1, 2
PORTS_STEP	1: All ports support 1-step on egress. 2: All ports support 2-step on egress. 3: All ports support both 1-step and 2-step.	1, 2, 3	m	-	{2}
SLAVE_ONLY	All ports of the clock are slave-only	True, False	m	c.2	True
TIME_TRACEABLE	Connectable to a time reference outside of PTP (for example, GPS)	True, False	m	c.3	False
FREQ_TRACEABLE	Connectable to a frequency reference outside of PTP (for example, GPS)	True, False	m	c.3	False
DAC	Doubly attached OC	True, False	o	-	True
PORTS_PAIRED	Paired clock ports for redundancy (for example, {3-4})	Identifier pair	o	c.4	{1, 2}
REDBOX_DATC	Redbox as TC	True, False	o	c.5	N/A
REDBOX_SLTC	Redbox as Stateless TC	True, False	o	c.5	N/A
REDBOX_TWBC	Redbox as 3-way BC	True, False	o	c.6	N/A
REDBOX_DABC	Redbox as DAC BC	True, False	o	c.6	N/A
MIB_SNMP	Supports MIB of IEC 62439-3:2016, Annex E	True, False	m	c.7	False
MIB_61850	Supports IEC TR 61850-90-4 Clock Objects	True, False	m	c.7	False
MIB_OTHER	Clock supports fixed values or a mechanism defined by the manufacturer (if True, this list is appended to this PICS)	True, False	m	c.7	True[21]
ATOI	Supports ATOI TLV as specified in IEC 61588:2009 | IEEE Std 1588–2008, 16.3	True, False	o	-	False
PPS	Clock has a 1 PPS output	True, False	o	-	False
ACCURACY	Design value of clock accuracy	Nanoseconds	o	-	1000 ns
DEVIATION	Design value of Allan deviation	Nanoseconds	o	-	4 ns
HOLDOVER	If it is the grandmaster and no longer synchronized to its time reference signal, the time length of the clock is expected to stay in clock class 7.	Seconds	o	-	N/A
c.1: At least one is supported (CLOCK_TYPE_OC and CLOCK_TYPE_TC can both be True). c.2: Only if CLOCK_TYPE_OC = True c.3: Only if SLAVE_ONLY = False c.4: Is "m" (>1) if DAC = True c.5: Support is only declared if CLOCK_TYPE_TC = True and DAC = True c.6: Support is only declared if CLOCK_TYPE_BC = True and DAC = True c.7: At least one is supported					

[21] You can enable or disable parameters and configure the domain number via DIGSI 5. The state values are displayed via the Homepage.

9.7 DHCP

9.7.1 DHCP

The Dynamic Host Configuration Protocol (DHCP) enables a client, in this case the Ethernet interface, to access IP address and configuration data from a DHCP server. In this case, a DHCP server has to be available in the network. If DHCP is activated, you do not have to configure the Ethernet interface network settings yourself.

9.7.2 Activating DHCP

✧ Select the Ethernet communication module.

✧ Navigate to the **Ethernet Addresses** section.

✧ In the **IP Protocol** section, activate the **Automatically an IP Address (from the DHCP Server)** check box.

- or -

✧ Set the **IP Address** to **0.0.0.0**.
The device then acts on the assumption that a DHCP server is available, and receives the addresses from this server.

9.8 RSTP

9.8.1 Description

The Rapid Spanning Tree Protocol (RSTP) serves for the reorganization of the network structure in the event of an error. In other words, RSTP reroutes the data to another path after the failure of a network path.

9.8.2 Parameter Settings for Networks

NOTE

In this document, bridge and switch mean the same thing.

Parameter name	Settings
HelloTime bridge	This time determines at what intervals the HelloTime telegrams are transmitted. 1 s or 2 s Standard setting = 2 sec
MaxAge bridge	The extent of a network is relevant when setting the value. MaxAge is a meter that counts down with each pass through a bridge. Each switch must be able to reach the root switch. For this reason, the MaxAge has to be set such that the value on all paths to the root bridge can never be 0. If this condition is not met, then the network will break down and will not regenerate on its own. This results in constant topology changes. 6 to 40 Standard setting = 40
Bridge Forward Delay Time	The Forward Delay Time setting is only relevant if an STP switch is active in the network. In such a case, the Forward Delay Time determines the reconfiguration time of the network after an interruption. Siemens recommends not changing the Forward Delay Time setting. 4 s to 30 s Standard setting = 21 sec
Transmit Hold Count	Transmit Hold Count is a meter that applies to all ports of the bridge. It limits the number of RSTP telegrams per port transmitted in sequence and without delay. When this telegram is transmitted, only one more telegram per second is transmitted. For a highly meshed system, a Transmit Hold Count that is set low will result in a significant slowing of the reconfiguration when the root switch fails. Siemens recommends not changing the Transmit Hold Count setting. 1 to 10 Standard setting = 10

Parameter name	Settings
Bridge Priority	Bridge priority establishes the position of the bridge in the network. The lower the value, the higher the priority. The bridge with the highest priority is the root bridge. Siemens recommends setting the priority of the root bridge to 0. Siemens recommends setting the priority of the replacement root bridge, which should be located right next to the root bridge, to 4096. The replacement root bridge should replace the root bridge in case of a failure. Siemens recommends setting the priority of all other devices and bridges to 32 768. 0 to 61 440, in increments of 4096 Standard setting = 32 768
Bridge Identifier	The priority value of a bridge consists of the bridge priority and bridge identifier. The bridge identifier therefore provides a finer gradation of the switches. This enables you to set the location of the alternate switches in the network. Siemens recommends not changing the default setting of 2048. 0 to 4095 Standard setting = 2048
Auto Edge Port 1	The Auto Edge Port 1 value can be set individually for each port and enables the automatic transition of a port into edge port state if no RSTP telegrams are received. Then after the fixed migration time of 3 seconds, the ports go into the forwarding state. The enabling of this value harbors the danger of circulating telegrams. Siemens recommends keeping this set to **off**. on/off Standard setting = off
Port Priority Port 1	The Port Priority Port 1 value can be set for each port. The port priority goes into the valence of vectors on the recipient side and is taken into account by the port identifier. The port identifier consists of the port priority and the port number. Siemens recommends leaving the port priority set to the standard value. 0 to 240, in increments of 16 Standard setting = 128
Port Path Costs Port 1	The path costs indicate the quality of a line. The higher the value, the worse the line. In IEEE Std 802.1D™ - 2004, this value is established depending on the velocity. For example, for 100 Mbit, path costs of 200 000 are defined. The setting is included in the valence calculation of the vector. Siemens recommends not changing this setting. 0 to 200 000 000 Standard setting = 200 000
Auto Edge Port 2	See the Auto Edge Port 1 parameter
Port Priority Port 2	See the Port Priority Port 1 parameter
Port Path Costs Port 2	See the Port Path Costs Port 1 parameter

9.9 PRP

PRP (Parallel Redundancy Protocol) is a redundancy protocol for Ethernet networks. This protocol is specified in the norm IEC 62439-3. In comparison to conventional redundancy procedures, for example, RSTP (Rapid Spanning Tree Protocol, IEEE 802.1D-2004), PRP offers a switchover without interruptions. This avoids a dead time in the event of a fault, and thus the highest availability.

Previous redundancy methods are based on mechanisms where the power-system components (switches and bridges) agree with each other and find the best communication path for normal operation.

In the event of a fault, for example, in a cable, an optical fiber, or in case of a switch failure, the interruption is detected and alternative paths are found in the network and connected. No communication can take place during this switching procedure. Depending on the size and on the configuration of the Ethernet network, this state can last for 10 ms up to around 1 s. A protocol extension in the end device is not necessary in this case because the protocol is implemented in the switches.

PRP adopts a different approach.

The redundancy procedure is generated in the end device itself. The procedure is simple: The redundant end device has 2 Ethernet interfaces with the same address (DAN, Double Attached Node). Then, the same indication is sent twice, with PRP (parallel) via 2 separated networks. Both indications are unambiguously identified with a sequence number.

The receiver takes the information that arrives first, stores the ID of the information in a duplicate filter using the source address and the sequence number of the information. Thereby, the receiver recognizes the 2nd redundant information and discards it. This redundant information is then discarded.

If the 1st indication is missing, the 2nd indication with the same information arrives via the other network. This redundancy avoids a switchover of the network and is therefore a redundancy without interruption.

The end device does not forward any indication to the other network.

Since this procedure is realized in the Ethernet layer (same MAC address), it is transparent and can be used by all Ethernet informative data protocols (IEC 61850, DNP, other TCP/IP based protocols).

In addition, it is possible to use one of the 2 networks for the transmission of not redundant indications. To do so, connect a SAN (Single Attached Node) device to a network. In this way, a PRP end device can communicate with a SAN end device (in a not redundant way). If you wish to connect a SAN end device in a redundant way to a PRP system, use a REDBOX (redundancy box). This REDBOX provides PRP functionality externally as an in-line device. However, the PRP procedure also presents a disadvantage: You are buying the increased redundancy function at the cost of a duplicate network (2x switches, cables).

NOTE

Both networks must not be connected as this causes Ethernet double addressing and this can result in malfunctions!

There are 2 versions of PRP: PRP-0 and the successor PRP-1. Siemens implements PRP-1.

9.10 HSR

Like PRP, HSR (High Availability Seamless Redundancy Protocol) is specified in the norm IEC 62439-3. Both protocols provide a redundancy without switchover.

The basic function can be found in the definition of PRP. With PRP, the same indication is sent via 2 separated networks. In contrast to that, with HSR, the indication is sent twice in the both directions of the ring. The receiver gets the indication via 2 ways in the ring, takes the 1st indication, and discards the 2nd (see PRP).

Whereas a PRP end device does not forward any indication, an HSR node has a switch function. Thus, the HSR node forwards indications in the ring that are not addressed.

In order to avoid circling indications in the ring, special measures are defined in the case of HSR. SAN (Single Attached Node) end devices can only be connected with a REDBOX in the case of HSR.

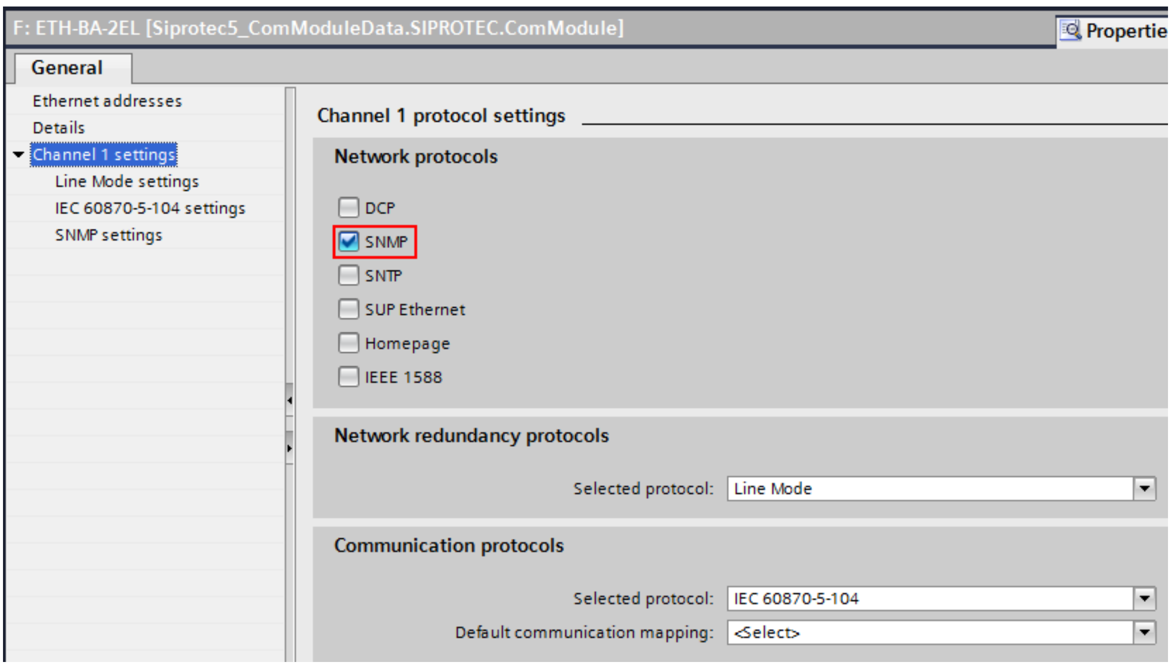
PRP systems and HSR systems can be coupled in a redundant way with 2 REDBOXES.

9.11 SNMP

9.11.1 Settings for SNMP

SNMPv3 (SNMP – Simple Network Management Protocol) is available in all Ethernet communication modules. The SIPROTEC 5 device supports the reception of IEC 60870-5-104 parameters and real-time information via SNMP version 3 (Network Management Protocol). You can find more information on this topic in chapter *4.2.1 Settings*.

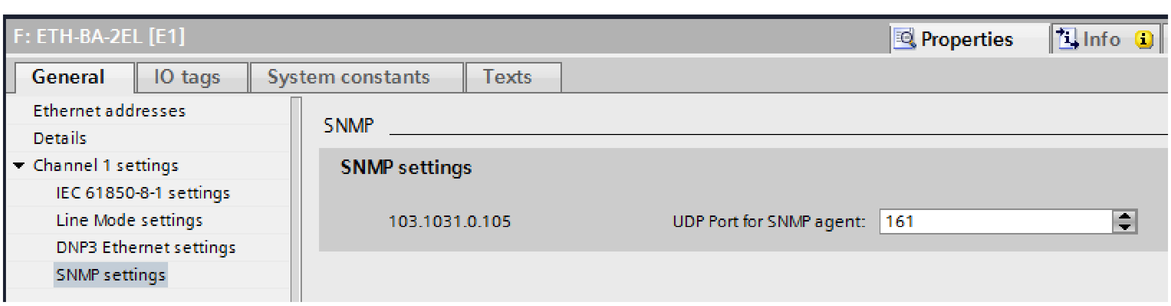
As default, SNMP is deactivated. If you want to switch on SNMP in the device, activate the SNMP check box in the channel settings of the Ethernet communication module.



[sc_Enable SNMP, 1, en_US]

Figure 9-13 Selecting SNMP as the Network Protocol

Then, if necessary, you can set the UDP port where the SNMP agent (Ethernet communication module) receives the queries. The default setting for the UDP port normally should not be changed.



[sc_SNMP_settings, 1, en_US]

Figure 9-14 SNMP Settings, UDP Port

SNMP allows the state query of these modules. For the display of MIB information (MIB – Management Information Base), an MIB browser and the description files are required.

9.11.2 SNMP Standard MIBs

The following standard MIBs are supported:

- MIB-II (RFC 1213)
- Interfaces MIB (RFC 2863)
- IP Forwarding MIB (RFC 4292)
- IP- & ICMP-MIB (RFC 2011)
- TCP-MIB (RFC 4022, formerly RFC 2012)
- UDP-MIB (RFC 4113, formerly RFC 2013)
- SNMPv2-MIB (RFC 3418)
- Framework MIB (RFC 2571)
- MPD-MIB (RFC 2572)
- USM-MIB (RFC 2574)
- Target & Notification MIB (RFC 2573)

You can find additional information under *http://www.snmplink.org/OnLineMIB/Standards/*.

9.11.3 SNMP SIPROTEC 5 Enterprise MIB

In addition to standard MIBs, a SIEMENS SIPROTEC 5 Enterprise-MIB (1.3.6.1.4.1.22638.2) is supported. The Siprotec5.mib file describes the information objects available there.
You can find the MIB file on the Internet under *http://www.siprotec.de* or *http://www.siprotec.com*.

sip5Identity

Sip5Identity (1.3.6.1.4.1.22638.2.2) contains the ID of the Ethernet communication module. The information does not change at runtime.

- identityBMNumber:
  Serial number of the Ethernet communication module
- identityProdCode:
  Siemens item number of the Ethernet communication module

sip5Optical

The sip5Optical (1.3.6.1.4.1.22638.2.3) information is relevant only for an optical Ethernet communication module.

- OpticalTransceiverRxPwr:
  Current transceiver receiver power in 0.1 μW increments
- OpticalTransceiverTxPwr:
  Current transceiver transmission power in 0.1 μW increments
- OpticalTransceiverTemp:
  Current transceiver temperature in °C

sip5Rstp

The sip5Rstp (1.3.6.1.4.1.22638.2.4) information is relevant only if RSTP was activated for the Ethernet communication module.
Explanations regarding the RSTP information can be found below in the chapter on RSTP.

sip5Sntp

The sip5Sntp (1.3.6.1.4.1.22638.2.5) information is relevant only if SNTP was activated for the Ethernet communication module.

- sntpPrimarySvr:
  Parameterized IP address of the primary NTP server
- sntpSecondarySvr:
  Parameterized IP address of the secondary NTP server
- sntpClockMaster:
  Current NTP master clock (primary or secondary NTP server)

sip5Goose

The sip5Goose (1.3.6.1.4.1.22638.2.6) information is relevant only if IEC 61850-8-1 was parameterized for the Ethernet communication module and a GOOSE application was activated.

- gooseTxConnConfig:
  Number of parameterized GOOSE connections (Tx only)
- gooseTxConnActive:
  Current number of active GOOSE connections (Tx only)
- gooseRxMismatchTel:
  Current number of faulty GOOSE telegrams received
- gooseRxLostTel:
  Current number of lost GOOSE telegrams (receive direction)

sip5PortStatus

The sip5PortStatus (1.3.6.1.4.1.22638.2.7) information is independent of the module and protocol parameterization.

- portStatusCH1:
  Link status for Channel 1 (Up/Down)
- portStatusCH2:
  Link status for Channel 2 (Up/Down)

9.11.4 SNMP V3 Features

Security is a weak aspect in SNMP versions 1 through 2c. These versions of SNMP do not support logon with password and user names; instead, communities were used. The disadvantage being that every user in the network with a suitable program can read data and even change values.

SNMP Version 3 offers encryption and improved authentication. For additional security, for SIPROTEC 5 devices, you cannot change any settings or values of the device via SNMP, except for settings affecting SNMP.

As default, 3 users are created in an **initial** group, with read and write access:

User	Authentication	Password	Encryption	Password
initial	No	No	No	No
templateMD5	MD5	12345678	DES	12345678
templateSHA	SHA	12345678	DES	12345678

The manner in which you create groups and users as well as change passwords depends on the MIB browser used. Refer to the corresponding MIB browser documentation.

NOTE

For safety reasons, Siemens recommends removing these initial standard users, creating your own users, and assigning passwords.

The corresponding SNMP tree structures and tables for user management are readable and writable (USM-MIB).

You can find more information in the RFC documentation: USM-MIB (RFC 3414, 2574) and VACM-MIB (RFC 3415, 2575).

NOTE

If the parameterization for SNMP is removed and loaded in the device, all previous settings made for SNMP on the Ethernet communication module are deleted. This means that the initial state applies when parameterizing the SNMP again.

NOTE

If you load the Config and switch off SNMP and then load SNMP, the initial status is again applicable.

If you modify the Config without modifying SNMP, then SNMP remains just as before.

9.12 SUP

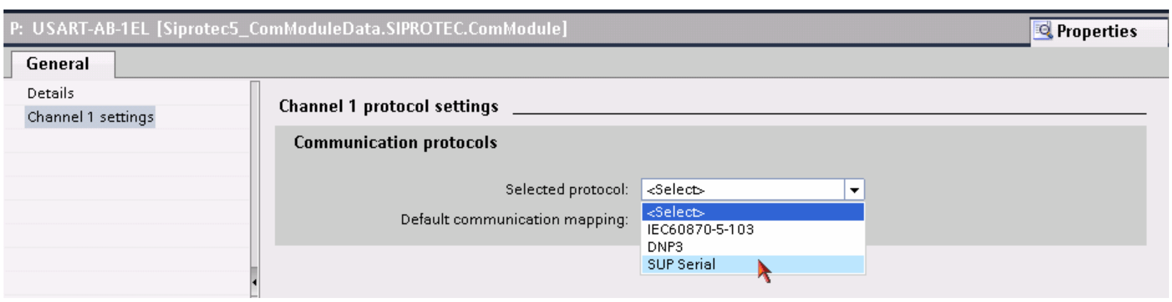
9.12.1 SUP

The Slave Unit Protocol (SUP) network protocol is used for communication between the RTD unit (temperature relays that measure the temperature of up to 12 sensors and provide the data to an RS485 interface for external evaluation) and the SIPROTEC 5 device.

9.12.2 Activating SUP

Activating SUP Serial

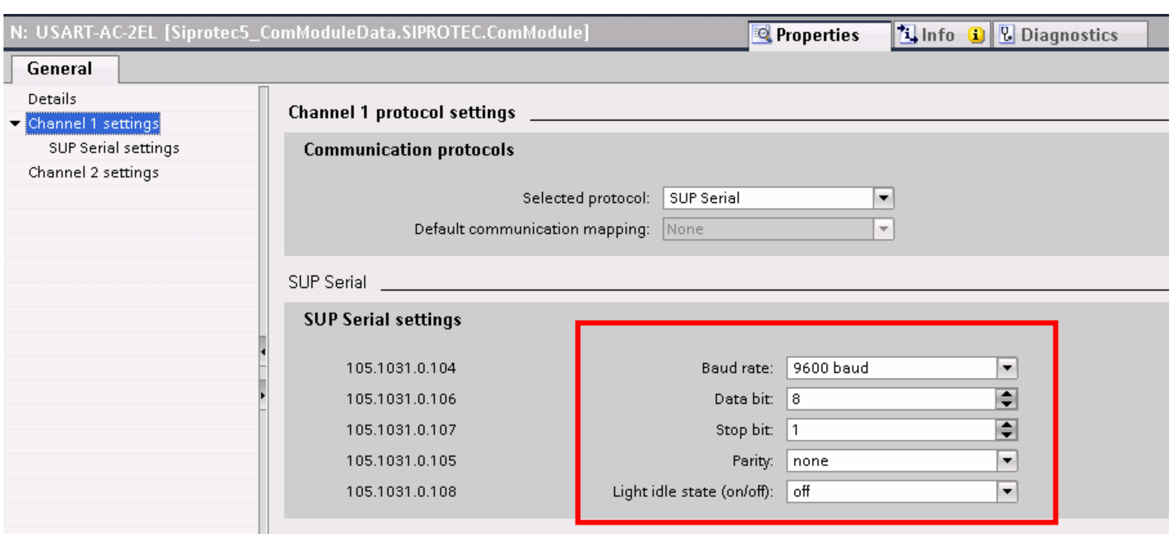
- ✧ Select the communication module.
- ✧ Navigate to the **Channel 1 Settings** section.
- ✧ In the list box **Selected Protocol**, select the **SUP Serial** protocol.



[sc_auser4, 2, en_US]

Figure 9-15 Selecting the SUP Protocol

- ✧ Make the communications settings for the relevant serial channels.



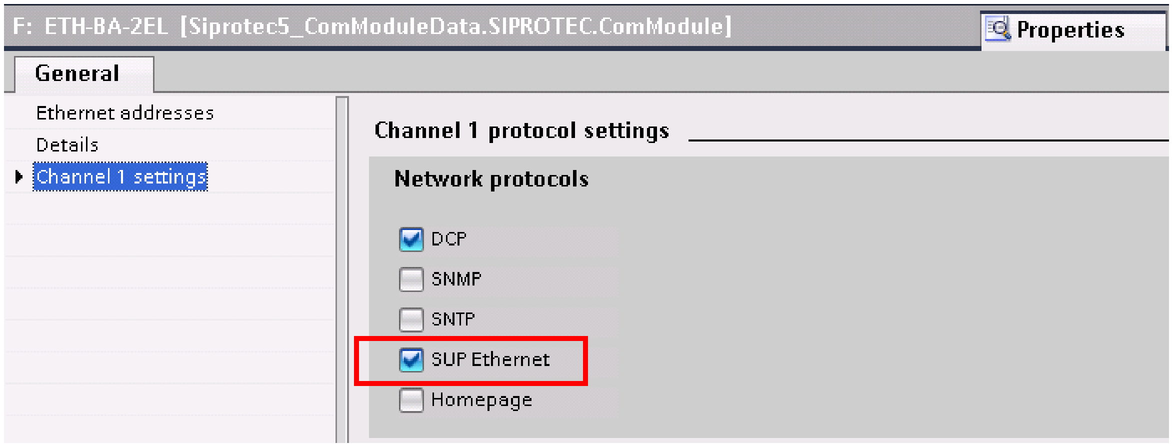
[sc_auser5, 2, en_US]

Figure 9-16 Making the Communication Settings

Activating SUP Ethernet

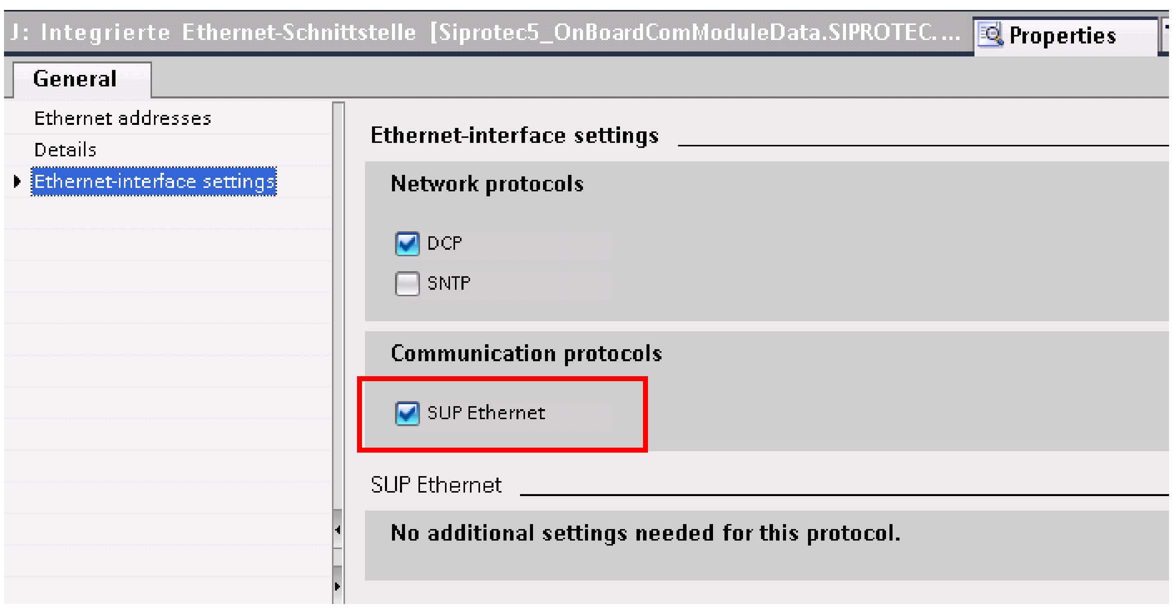
- ✧ Select the Ethernet communication module or the integrated Ethernet interface (Port J)
- ✧ Navigate to the **Channel 1 Settings** section.

✧ Select the **SUP Ethernet** network protocol.



[sc_autcp2, 2, en_US]

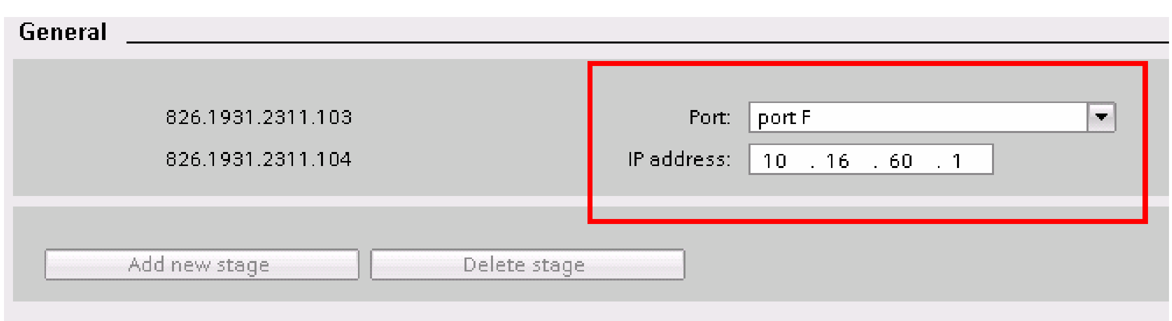
Figure 9-17 Activating the Protocol for the Ethernet Communication Module



[sc_autcp3, 2, en_US]

Figure 9-18 Activating the Protocol for the Integrated Ethernet Interface

✧ Now, set the port over which the SUP protocol runs.



[sc_autcp5, 2, en_US]

Figure 9-19 Setting the Port and IP Address

9.13 Homepage

9.13.1 Content and Structure

The homepage for communication modules is used for diagnostic purposes. On the homepage, you can find information on the communication module as well as the network and communication protocols that run on the communication modules.

The homepage is physically accessible using a Web browser via external Ethernet interfaces, for example, http://<Module-IP>:Port. The following table lists the details for port configuration.

Port	Number
J	8080
E	8081
F	8082
N	8083
P	8084

If you have configured Port J, you can reach all communication modules, that is, also the USART modules, via the homepage.

You cannot download software using the homepage. It does not offer direct access to device parameters.

The 3 standard Web browsers Internet Explorer, Chrome, and Firefox are supported.

NOTE

For security reasons, Siemens recommends using the homepage continuously only if there is a secure network connection.

NOTE

The homepage is available only in English.

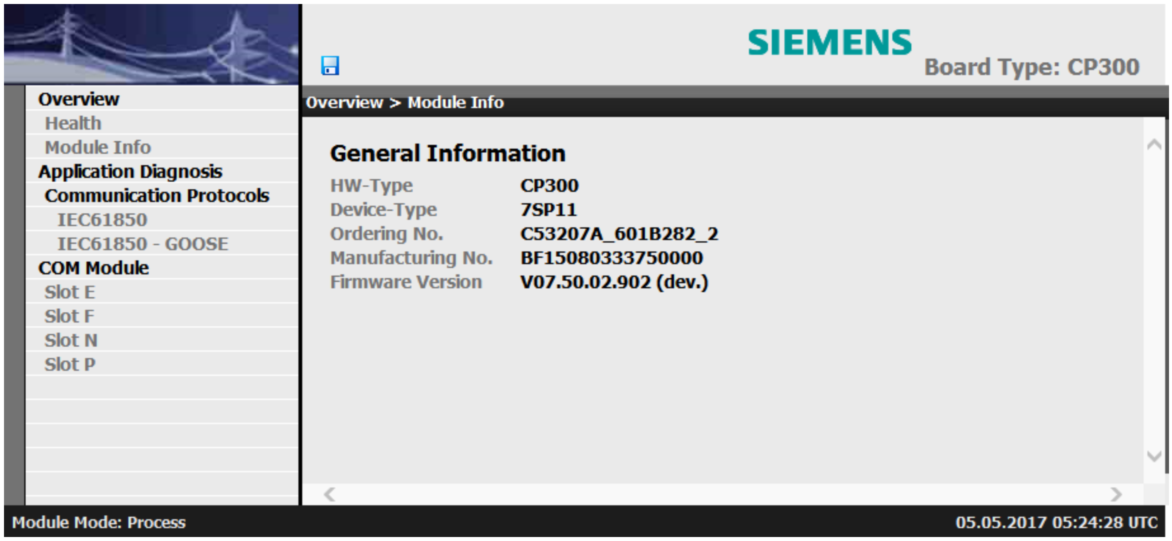
Homepage Content

The homepage shows system diagnostic values, various start/fault logs, and the accessible diagnostic values of the activated communication protocols.

It provides diagnostic values for the following protocols:

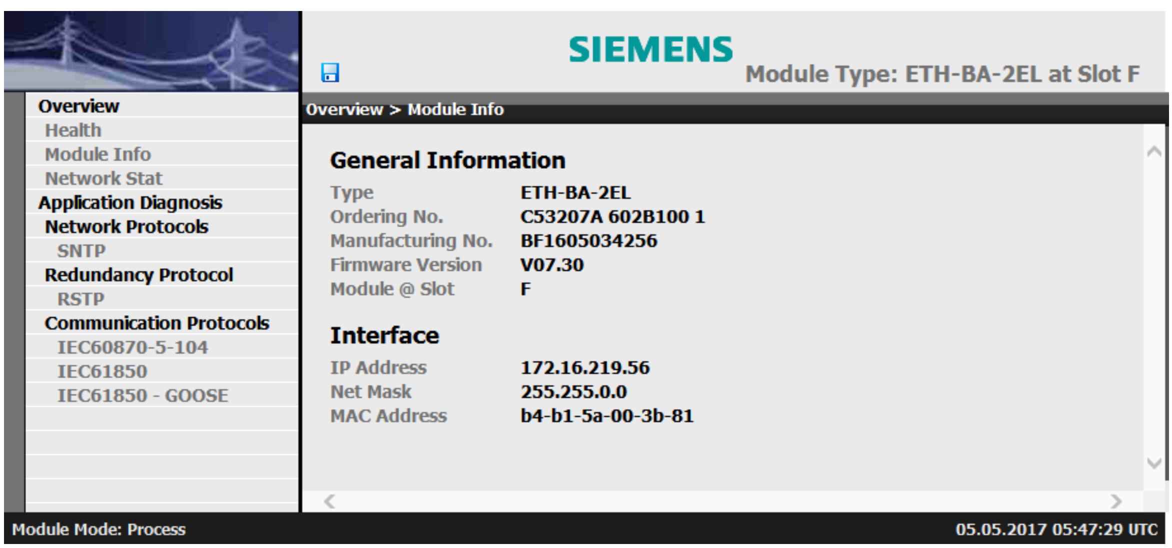
Protocols	Can Run on the Following Module Types or Slots		
	CPU (Port J)	Ethernet Modules	USART Modules
Network protocols	SNTP SUP Ethernet	SNTP SUP Ethernet IEEE 1588	–
Redundancy protocols	–	PRP HSR RSTP	–
Communication protocols	IEC 61850	DNP3 Ethernet IEC 61850 IEC 61850 – GOOSE IEC 60870-5-104 Modbus TCP	DNP3 IEC 60870-5-103 SUP Serial Protection interface

Homepage Structure



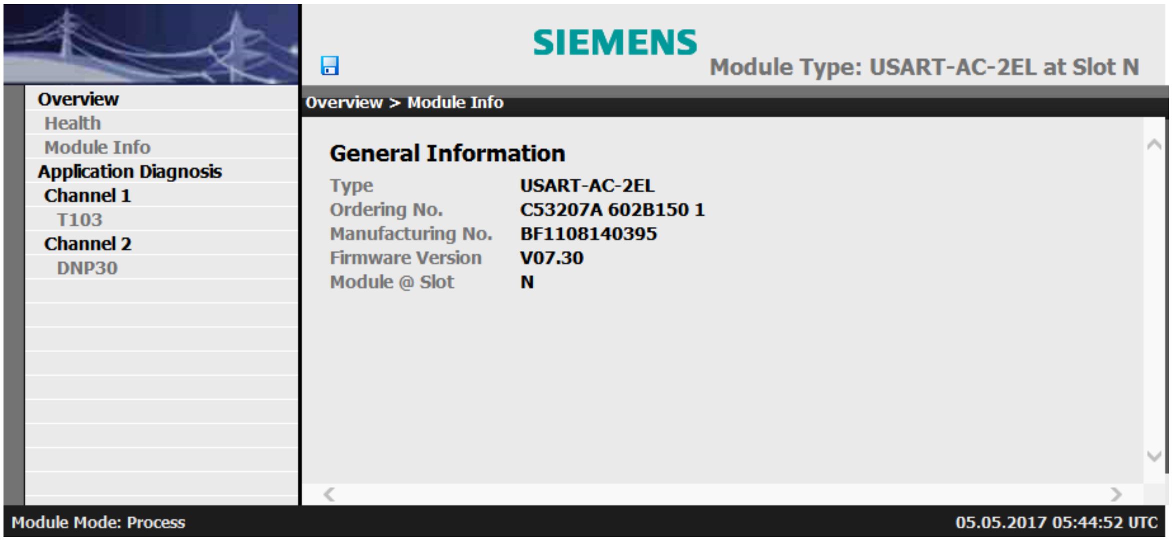
[sc_homepage_PortJ, 2, --_--]

Figure 9-20 Homepage Structure for Port J



[sc_homepage, 2, --_--]

Figure 9-21 Homepage Structure for Ethernet Modules



[sc_homepage_USART, 2, --_--]

Figure 9-22 Homepage Structure for Serial Modules

The homepage is divided into several sections:

- Header:
  In the header, you can find a floppy-disk download icon. In case of a failure, this icon provides a download with all relevant data for an error analysis. You can simply forward this download to our customer service.
- Menu area
  The menu area is divided into the following sections:
  - Overview
  - Application Diagnosis
  - COM Module (Port J)

  To display the values of the device in the right window section, select the **Application Diagnosis** field.
- Content section:
  The Content section contains the dynamic device information.
- Footer:
  The status is displayed at the lower left. The status indicates in which mode the module is running. There are 2 different modes:
  - **Process**
    This mode indicates that the module is in operation.
  - **Fallback**
    This mode indicates that an error has occurred, for example, when starting up the module.

9.13.2 Homepage Activation

NOTE

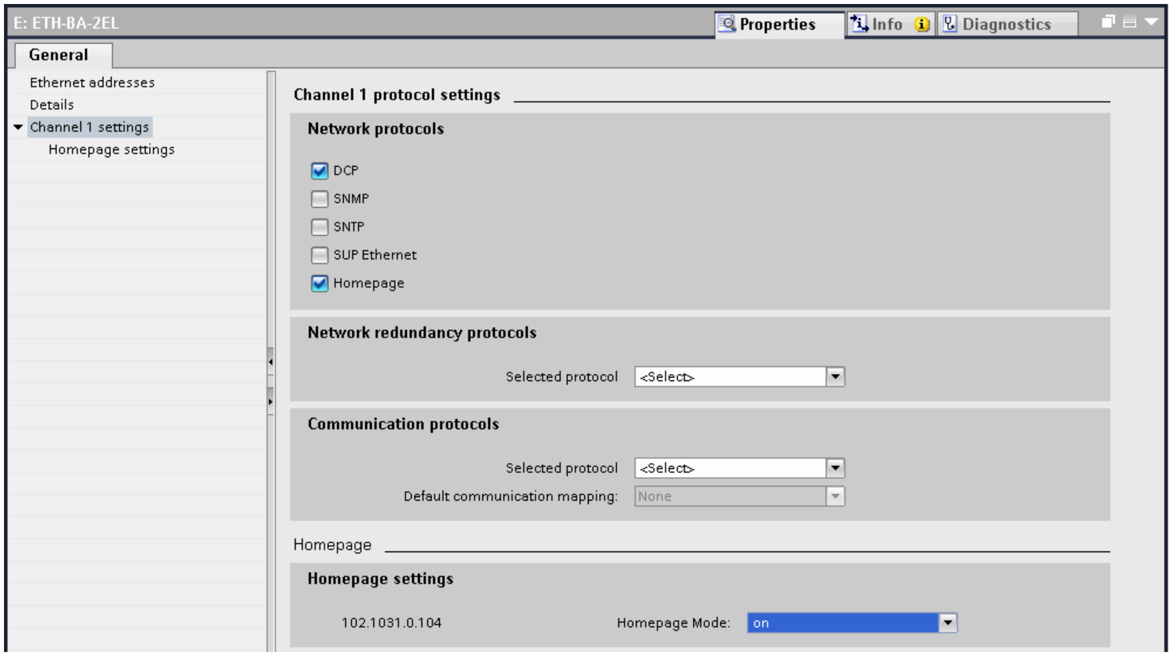
For security reasons, Siemens recommends using the homepage continuously only if there is a secure network connection.

Activation via DIGSI

✧ Check the **Homepage** check box in the channel settings for the Ethernet communication module or for Port J.

An additional **Homepage** section is displayed.

The default setting for the homepage is **off**.



[schomdig-290113-01.tif, 1, en_US]

Figure 9-23 Homepage Section in DIGSI

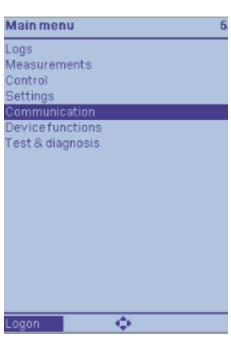
If the check mark is not set, the homepage is not loaded to the module. The homepage is deactivated. In this case, you cannot activate or deactivate the homepage in the on-site operation.

✧ To deactivate the homepage, select the **off** option in the list box.

Activation on the Device

To be able to activate or deactivate the homepage on the device, the homepage has to be activated via DIGSI.

✧ Use the arrow keys to navigate from **Settings** to **Communication**.



[sc_devmn1, 1, --_--]

Figure 9-24 Menu Settings -> Communication

✧ Select **Homepage**.

You can activate (on) or deactivate (off) the homepage there.

[sc_devmn2, 1, --_--]

Figure 9-25 Homepage Menu

Querying Diagnostic Data via the Homepage

NOTE

The homepage must be activated; otherwise, the diagnostic data are not visible.

✧ Enter the IP address of the communication module in the Internet Explorer. You can read the diagnostic data via the homepage.

9.13.3 Overview Section

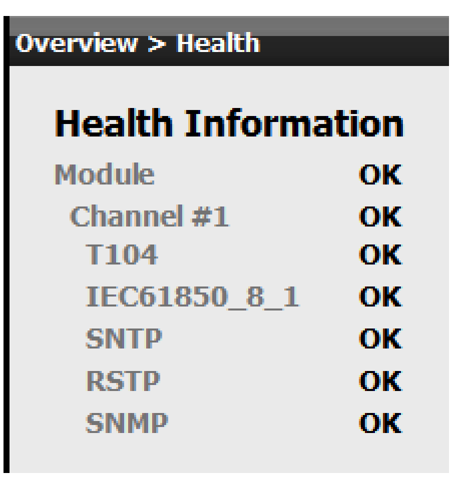
9.13.3.1 Structure

The **Overview** section contains the following sections:

- Health
- Module Info
- Network Stat
  (for Ethernet modules)

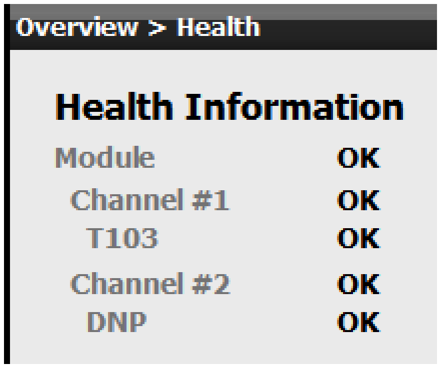
9.13.3.2 Health

The **Health** page is structured as follows:



[sc_overview_health, 2, --_--]

Figure 9-26 Overview – Health Information (Ethernet Modules)



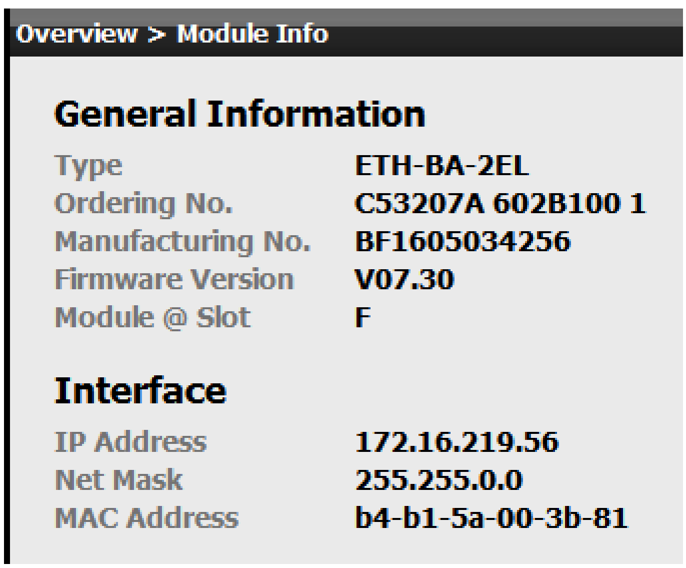
[sc_overview_health_USART, 2, --_--]

Figure 9-27 Overview – Health Information (Serial Modules)

The **Health** page provides information on the state of the modules and protocols.

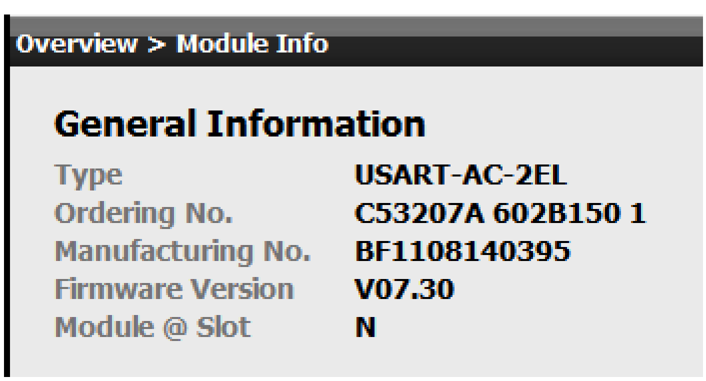
9.13.3.3 Module Info

The **Module Info** page is structured as follows:



[sc_overview_module_info, 2, --_--]

Figure 9-28 Overview – Module Info (Ethernet Modules)



[sc_overview_module_info_USART, 2, --_--]

Figure 9-29 Overview – Module Info (Serial Modules)

[sc_overview_module_mainboard, 1, --_--]

Figure 9-30 Overview – Module Info (Port J)

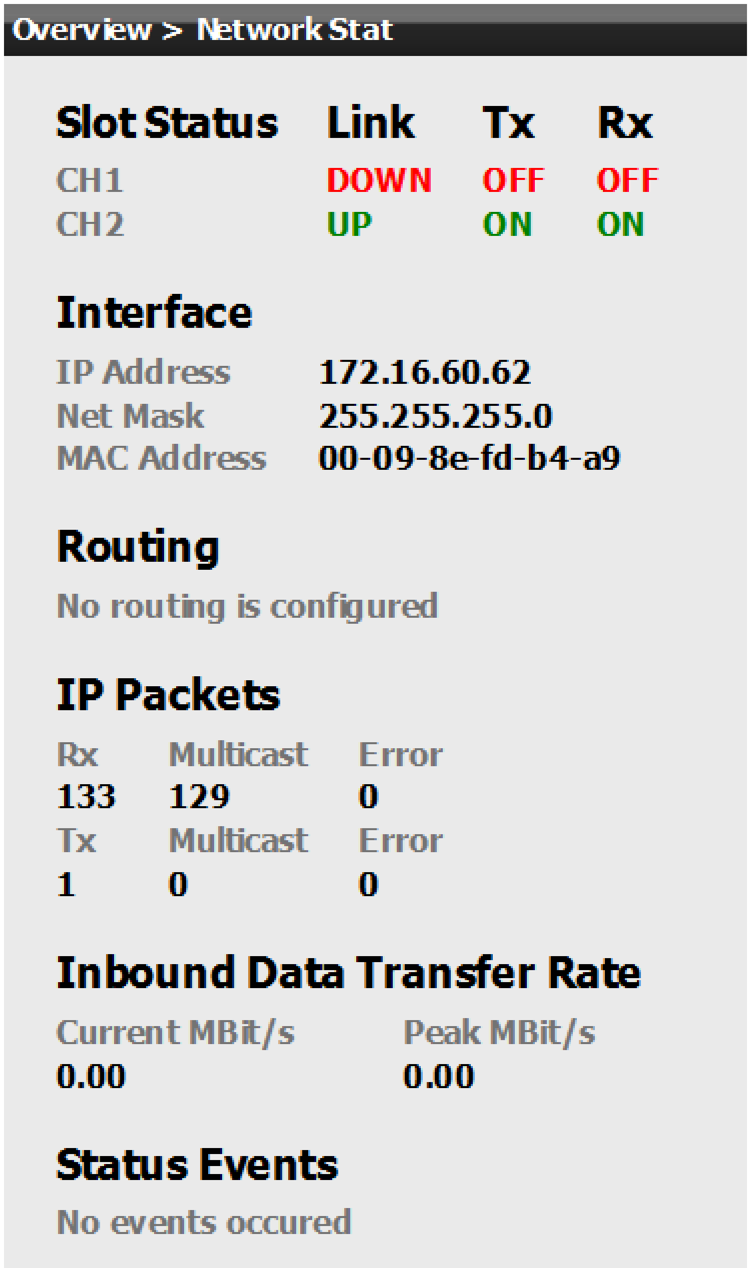
General Information

The **General Information** section contains the following information:

- Module type: electrical or optical
- Device type
- Ordering number of the communication module
- Manufacturing number (BF) of the communication module
- Firmware version of the communication module
- Communication-module slot in the device

9.13.3.4 Network Stat

The **Network Stat** page is structured as follows:



[sc_overview_network_stat, 3, --_--]

Figure 9-31 Overview – Network Stat

Slot Status

The **Slot Status** section contains information about the state of the channels.

Table 9-3 State Details

Entry	Meaning
Link	State of the connection
Tx	State of the counter of sent telegrams
Rx	State of the counter of received telegrams

Interface (for Ethernet Modules)

The **Interface** section contains the following information:

- IP Address
- Net mask
- MAC address

SFP Statistics

The **SFP Statistics** section contains the following values for each channel:

Entry	Meaning
Vendor	Name of the manufacturer
Identifier	Transceiver type
Part Number	Part number
Revision	Revision number of the product
Temperature	Internally measured temperature in the module Unit: °C
Power Supply	Internally measured supply voltage for the transceiver Unit: V
Tx Bias	Internally measured bias current Unit: A
Tx Power	Measured Tx output voltage Unit: mW
Rx Power	Measured Rx input voltage Unit: mW

NOTE

The **SFP Statistics** section is only available for Ethernet modules with an optical connection.

Routing

The **Routing** section contains details about the configured routings.

IP Packets

The **IP Packets** section contains various counters.

Table 9-4 Meaning of the Counters in the IP Packets Area

Entry	Meaning
Rx	Counter of received telegrams
Tx	Counter of sent telegrams
Multicast	Counter for multicast telegrams that occur
Errors	Counter for errors that occur

Inbound Data Transfer Rate

In the **Inbound Data Transfer Rate** section, you can find information on the current and maximum incoming transmission rate.

Entry	Meaning
Current Mbit/s	Instantaneous incoming transmission rate Unit: Mbit/s
Peak Mbit/s	Maximum incoming transmission rate Unit: Mbit/s

Status Events

The **Status Events** section contains information about special events on the Ethernet interface.
2 different events are displayed:

- Overload
- Receive error

Entry	Meaning
Count	Number of events that have occurred
Type	Event type
Last timestamp begin	Time stamp when event started
Last timestamp end	Time stamp when event ended If there is a receive error, this entry is empty.

9.13.4 Application Diagnosis Section for Ethernet Modules

9.13.4.1 Structure

The **Application Diagnostic** section contains diagnostic pages for the following protocols:

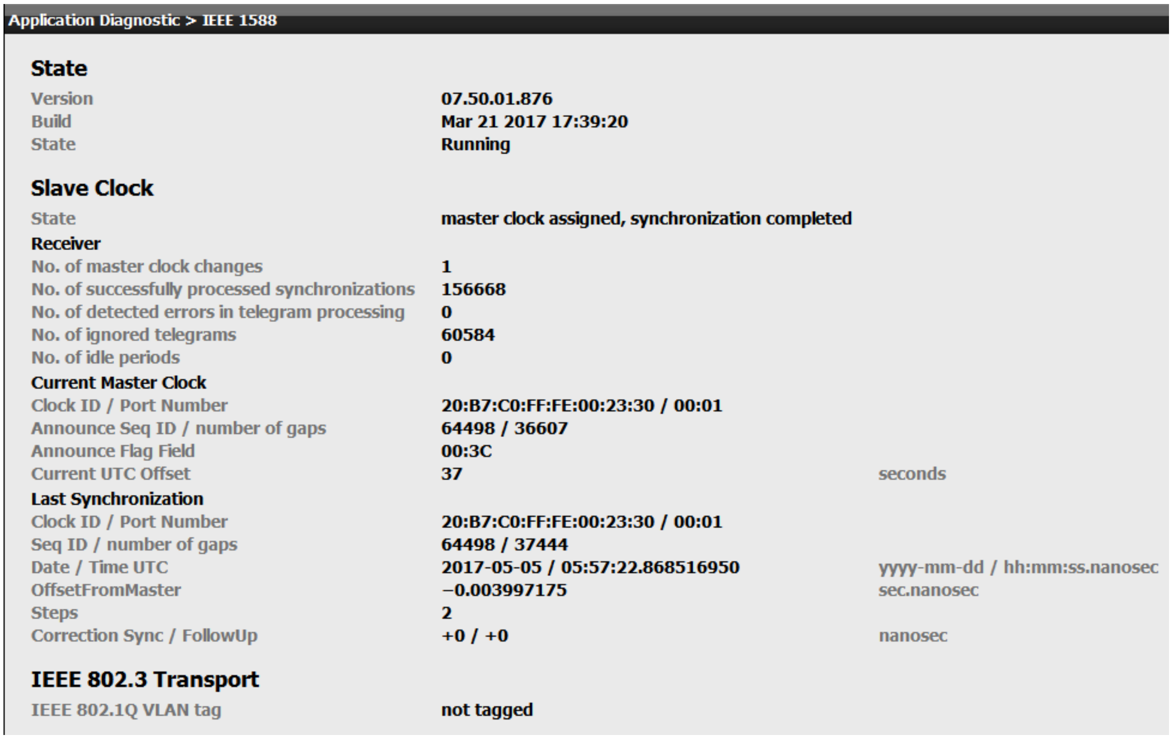
- **Network protocols**:
  - IEEE 1588
  - SNTP
- **Communication protocols**:
  - IEC 60870-5-104
  - IEC 61850
  - IEC 61850 - GOOSE

NOTE

The **Application Diagnostic** section is structured identically for electrical and optical modules.

9.13.4.2 Network Protocols – IEEE 1588 for the Modules ETH-BA-2EL and ETH-BB-2FO

The **Application Diagnostic > IEEE 1588** section contains diagnostic data about IEEE 1588 for the modules ETH-BO-2EL and ETH-BB-2FO.



[sc_IEEE1588 application diagnostic, 3, --_--]

Figure 9-32 Application Diagnostic – IEEE 1588 for the Modules ETH-BA-2EL and ETH-BB-2FO

State

The **State** section contains information on the protocol.

Entry	Meaning
Version	Installed protocol version
Build	Protocol build date
State	Protocol bootup status

Slave Clock

The **Slave Clock** section contains information on synchronization.

Entry	Meaning
State	Receiving status of the Slave Clock
Receiver	Information on receiving the time
No. of master clock changes	No. of master logons (after failure or change)
No. of successfully processed synchronizations	No. of successful synchronizations
No. of detected errors in telegram processing	No. of detected errors in the telegram
No. of ignored telegrams	No. of ignored telegrams
No. of idle periods	No. of inactive periods (no receiving from the Master for a longer time)
Current Master Clock	Information on current Master Clock
Clock ID / Port Number	Clock ID and Port number acc. to IEEE 1588

Entry	Meaning
Announce Seq ID / number of gaps	Display of the currently received **Seq ID** of the Announce/number of recognized sequence gaps (brief telegram loss)
Announce Flag Field	Display of currently received flags
Current UTC Offset	UTC Offset (TAI to UTC) in seconds
Last Synchronization	Information on current synchronization
Clock ID / Port Number	Clock ID and Port number acc. to IEEE 1588
Seq ID / number of gaps	Display of the currently received **Seq ID** of the synchronization/number of recognized sequence gaps (brief telegram loss)
Date / Time UTC	Received synchronization time (corrected)
OffsetFromMaster	Calculated difference from synchronization time to local time
Steps	Mode of synchronization 1: one-step 2: two-step
Correction Sync / FollowUp	Contents of the correction information from the Sync and Follow Up Telegram

IEEE 802.3 Transport

The **IEEE 802.3 Transport** section contains information on the transmission of telegrams

Entry	Meaning
IEEE 802.1Q VLAN tag	Receive telegram with VLAN tag (tagged, info on priority and VLAN-ID) or without VLAN tag (not tagged)

9.13.4.3 Network Protocols – IEEE 1588 on the Module ETH-BD-2FO

For the module ETH-BD-2FO, the **Application Diagnostic > IEEE 1588** section contains diagnostic data about IEEE 1588.

Application Diagnostic > IEEE 1588

PTP General

PTP enable	Yes
PTP profile	IEC 61850-9-3:2016
Transport protocol	Layer 2 Multicast
VLAN tag	Not Support
Clock type	Ordinary clock
Slave only	Yes

Slave Clock

General

Clock ID	B4:B1:5A:FF:FE:06:33:76		
Domain number	0		
Path delay mechanism	Peer-to-Peer		
P2P request interval	1		seconds
Announce receipt timeout	3		seconds
Steps	2		
Servo status	Locked		
Channel live states	On		
	CH1	CH2	
Port state	SLAVE	---	
Offset	−16	+0	nanoseconds
Mean path delay	2223	0	nanoseconds

Current Master Clock Info

	CH1	CH2	
Clock ID	00:1D:7F:FF:FE:80:13:4B	---	
Port number	1	0	
Steps	1	0	
Domain number	0	0	
GM priority1	0	0	
GM priority2	0	0	
GM clock class	6	0	
GM clock accuracy	33	0	
GM clock ID	00:1D:7F:FF:FE:80:13:4B	---	
Current UTC offset	37	0	seconds
CurrentUtcOffsetValid	True	---	
Traceable	True	---	

Last Synchronization

	CH1	CH2	
Sync seq ID	22874	0	
Date	2019-11-05	---	yyyy-mm-dd
Time UTC	06:37:21.128066760	---	hh:mm:ss.nanosec

Last Synchronization

	CH1	CH2	
Sync seq ID	22874	0	
Date	2019-11-05	---	yyyy-mm-dd
Time UTC	06:37:21.128066760	---	hh:mm:ss.nanosec
Sync CF	10597	0	nanoseconds
Follow_up CF	0	0	nanoseconds

[sc_IEEE1588AppDiaBD, 2, --_--]

Figure 9-33 Application Diagnostic – IEEE 1588 on the Module ETH-BD-2FO

PTP General

The **PTP General** section contains information on the protocol.

Entry	Meaning
PTP enable	Enabling the IEEE 1588 protocol
PTP profile	Profile of the IEEE 1588 protocol
Transport protocol	Selecting layer 2 (Ethernet) multicast transport for PTP messages
VLAN tag	Not supported in V7.90
Clock type	PTP clock type
Slave only	Forcing an ordinary clock to be a slave-only clock that never enters the master state

Slave Clock

The **Slave Clock** section contains information on the synchronization.

Entry	Meaning
General	General diagnostic data on the slave clock
Clock ID	An 8-octet array clock ID
Domain number	The IEEE 1588 domain number for the slave clock. An IEEE 1588 domain is a logical grouping of PTP clocks that synchronize to each other using the IEEE 1588 protocol.
Path delay mechanism	The delay mechanism of the IEEE 1588 protocol
P2P request interval	The peer-to-peer time request interval
Announce receipt timeout	The time-out specifying the number of intervals that pass without receipt of an **Announce message**[22]
Steps	Mode of synchronization: 1: one-step 2: two-step
Servo status	The status of the clock servo: **Holdover**, **Acquiring**, **Locked**, and **Free running**
Channel live states	Indicating the state of the IEEE 1588 traffic during the IEEE 1588 running phase States of the channel live: **On**, **Off**
Port state	States of the port: **INITIALIZING**, **LISTENING**, **FAULTY**, **UNCALIBRATED**, and **SLAVE**
Offset	The offset between the master and slave clock
Mean path delay	The mean propagation time between a requester and a responder
Current Master Clock Info	Information on the current master clock
Clock ID	Clock ID according to IEEE 1588
Port number	Port number according to IEEE 1588
Steps	Mode of synchronization: 1: 1-step 2: 2-step
Domain number	The IEEE 1588 domain number for the master clock
GM priority 1	The grandmaster[23] priority 1. A lower value corresponds to a higher priority.
GM priority 2	The grandmaster priority 2. A lower value corresponds to a higher priority.
GM clock class	Grandmaster-clock class
GM clock accuracy	Grandmaster-clock accuracy

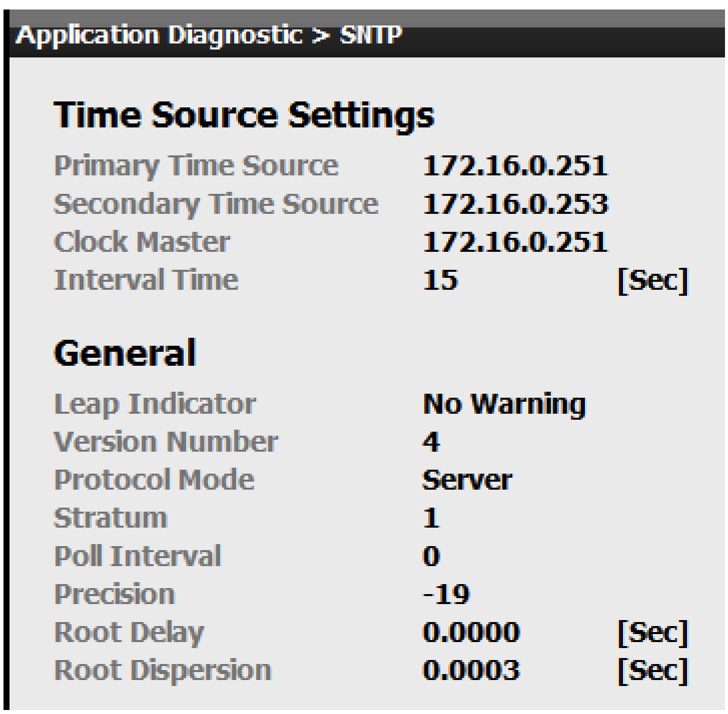
22 The **Announce message** is used to establish the synchronization hierarchy.

23 A grandmaster is the ultimate source of time for the time synchronization within a domain.

Entry	Meaning
GM clock ID	Grandmaster-clock ID. According to 13.5 of IEC 61588:2009, the value of the grandmaster-clock ID is the network order of the bytes representing grandmaster ID. The grandmaster-clock ID is also available in the information routing for further use by the customer.
Current UTC Offset	UTC Offset (TAI to UTC) in seconds
CurrentUTCOffsetValid	The UTC Offset (TAI to UTC) in seconds is valid.
Traceable	The grandmaster-clock time is traceable or not.
Last Synchronization	Information on current synchronization
Sync seq ID	Display of the currently received sequence ID of the synchronization
Date	Display the date variables
Time UTC	Universal Time Coordinated
Sync CF	Correction field in **Sync messages** calculated in nanoseconds
Follow_up CF	Correction field in **Follow-up messages** calculated in nanoseconds

9.13.4.4 Network Protocols – SNTP

The **Application Diagnostic > SNTP** section contains diagnostic data about SNTP.



[sc_SNTP_application_diagnostic, 2, --_--]

Figure 9-34 Application Diagnostic – SNTP

Time Source Settings

The **Time Source Settings** section contains information on the time sources.

Entry	Meaning
Primary Time Source	Primary time source
Secondary Time Source	Secondary time source
Clock Master	Time source used
Interval Time	Interval in seconds

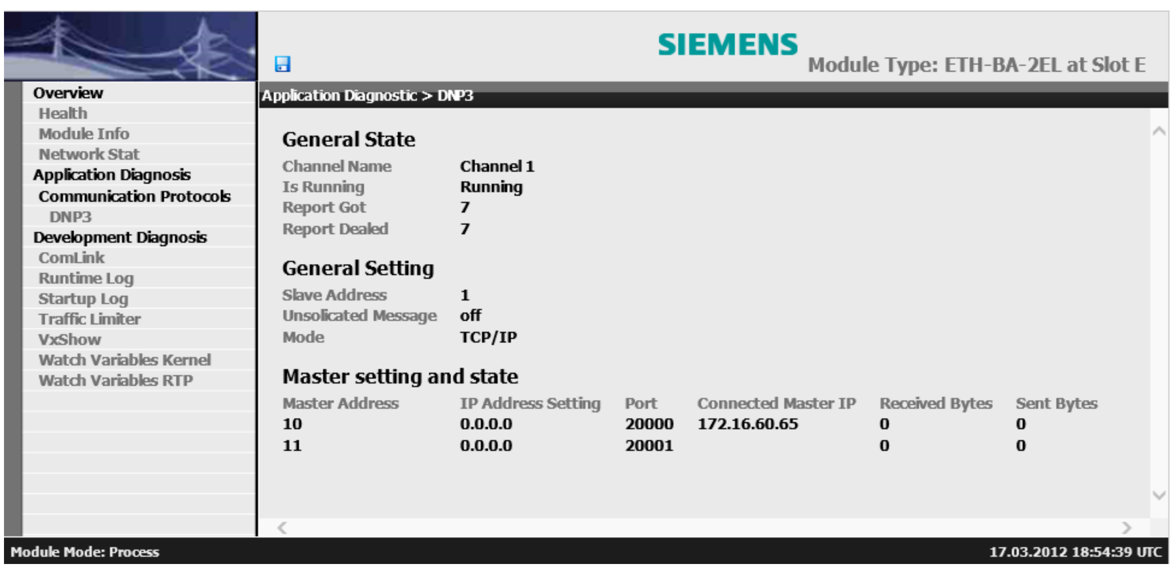
General

The **General** section contains the following information.

Entry	Meaning
Leap Indicator	Leap warning
Version Number	Protocol version
Protocol Mode	Protocol mode
Stratum	Server-relevant value as an indicator of the time source used
Poll Interval	Poll interval
Precision	Indicates the accuracy of the time-server clock Negative 8-bit value, expressed as a power of 2, for example: 2^{-16} = 15.3 µs 2^{-5} = 31.25 ms Additional details are available in RFC4330.
Root Delay	Server delay Total runtime of the NTP telegram from the root through the individual intermediate nodes
Root Dispersion	Previous total errors produced through calculations in the intermediate nodes

9.13.4.5 Application Diagnostic – DNP3 Ethernet

The **Application Diagnostic > DNP3 Ethernet** section contains diagnostic data about DNP3.



[sc_DNP3-Ethernet_Application_diagnostic, 3, --_--]

Figure 9-35 Application Diagnostic – DNP3 Ethernet

General State

The **General State** section contains the following entries.

Entry	Meaning
Channel Name	Internal channel description
Is Running	State display for the protocol (current state)
Report Got	Telegrams sent from device to module
Report Dealed	Telegrams arranged from device to module

General Setting

The **General Setting** section contains the following entries.

Entry	Meaning
Slave Address	Address of the slave
Unsolicited Message	Unsolicited transmission
Mode	Connection via Ethernet or serial connection

Master Setting and State

The **Master Setting and State** section contains the following entries.

Entry	Meaning
Master Address	Address of the master
IP Address Setting	Setting of the master IP address
Port	TCP/IP port number (only for Ethernet communication)
Connected Master IP	IP address of the connected master
Received Bytes	Received Bytes
Sent Bytes	Sent Bytes

9.13.4.6 Communication Protocols – IEC 60870-5-104

The **Application Diagnostic > IEC 60870-5-104** section contains diagnostic data about IEC 60870-5-104.

Application Diagnostic > IEC60870-5-104

General

Protocol Name	IEC 60870-5-104
Protocol Version	07.80.07.017
Report Got	4
MappingReport Dealed	1
GeneralSetting Report Dealed	1
SynSource	N/A
Timezone	UTC

Master

Status

MasterSettingReport Dealed	2
ChannelLive	False
Active Master	N/A
Connected Main Master	N/A
Main Received Bytes	0
Main Sent Bytes	0
Connected Backup Master	N/A
Backup Received Bytes	0
Backup Sent Bytes	0

Setting

Redundancy	On
Enable time sync.	Off
Common address	1
MV trans. type	Spontan. and GI
Cycle time	60
Grouped trans. time	0
DoubleTran	Off
Max. length of APDU	253
Main master IP	172.16.60.65
Main channel t0	5
Main channel t1	15
Main channel t2	10
Main channel t3	20
Backup master IP	172.16.60.66
Backup channel t0	5
Backup channel t1	15
Backup channel t2	10
Backup channel t3	20

[sc_IEC104_communication_protocols, 3, --_--]

Figure 9-36 Application Diagnostic – IEC 60870-5-104

General

The **General** section contains the following entries.

Entry	Meaning
Protocol Name	IEC 60870-5-104
Protocol Version	IEC 60870-5-104 version
Report Got	ACSI (Abstract Communication Service Interface) report received by mainboard
MappingReport Dealed	ACSI (Abstract Communication Service Interface) mapping report processed
GeneralSetting Report Dealed	ACSI (Abstract Communication Service Interface) general setting report processed
SynSource	IP address of the synchronization source
Timezone	Time zone

Status

The **Status** section contains the following entries.

Entry	Meaning
MasterSettingReport Dealed	ACSI (Abstract Communication Service Interface) master setting report processed
ChannelLive	Indicate if each master is transmitting and receiving data on the module
Active Master	The Master, which is the last to send STARTDT to the device
Connected Main Master	Display the IP of the connected Main Master
Main Received Bytes	Bytes received from Main Master. This number is updated continuously.
Main Sent Bytes	Bytes sent by Main Master. This number is updated continuously.
Connected Backup Master	Display the IP of the connected Backup Master
Backup Received Bytes	Bytes received from Backup Master. This number is updated continuously.
Backup Sent Bytes	Bytes sent by Backup Master. This number is updated continuously.

Setting

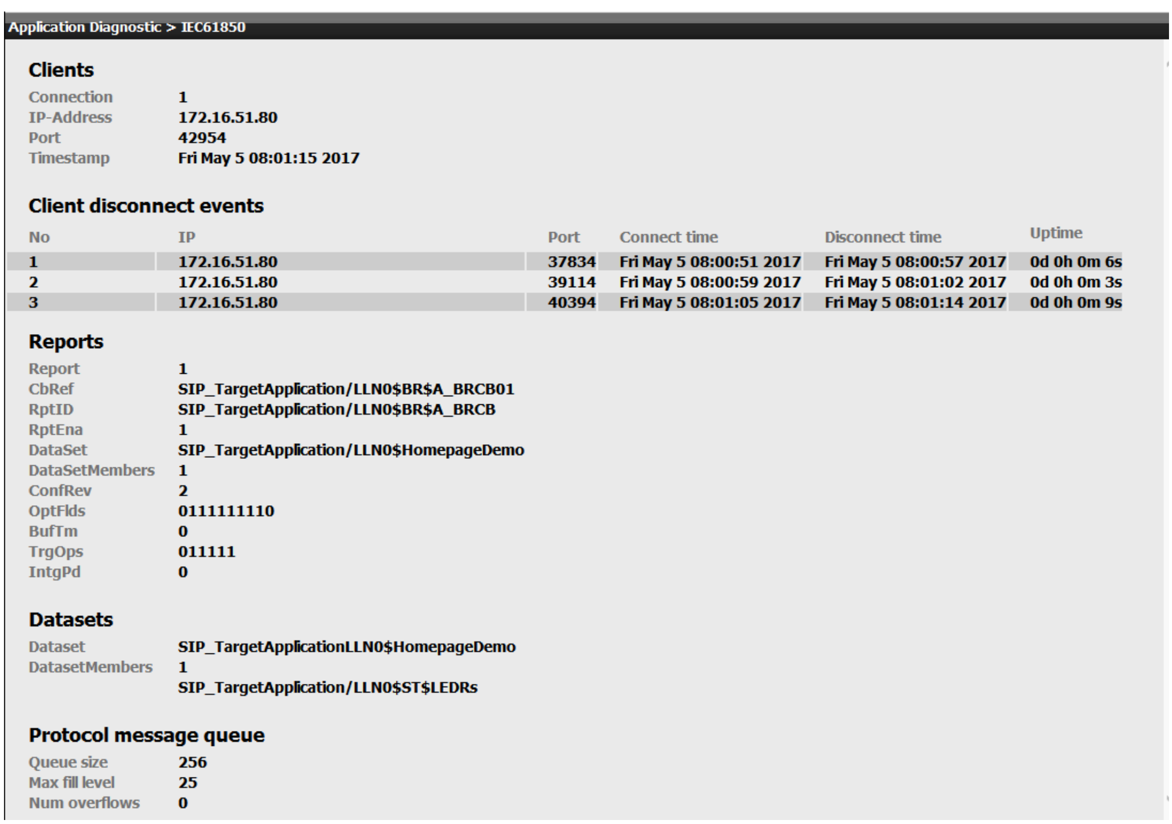
The **Setting** section contains the following entries.

Entry	Meaning
Redundancy	When redundancy is off, all settings for the backup master are ignored.
Enable time sync.	Determines whether the SIPROTEC 5 device expects and evaluates time synchronization from the IEC 60870-5-104 master.
Common address	IEC 60870-5-104 station address of the SIPROTEC 5 device
MV trans. type	Selection of the measured-values transmission type
Cycle time	Time for sending cyclic data. Relevant if **Cyclic only**.
Grouped trans. time	The time for measurement transmission as a group. Single changes of measurements are stored and commonly sent out after this time. Reduce of required bandwidth. 0 = deactivate group transmission
DoubleTran	Double Transmission Sends indications with or without time stamp. If double transmission is switched on, the indication is sent twice to the Master. Once with the time stamp and once without time stamp.
Max. length of APDU	Maximum length of APDU (application protocol data unit) per master in the monitoring direction

Entry	Meaning
Main master IP	• When redundancy is disabled and there is only 1 master: Ipv4 address 0.0.0.0 means that the slave can listen and contact every IP address. • When redundancy is disabled and there are 2 or 3 masters: Ipv4 address cannot be 0.0.0.0 or cannot be the same as the backup master IP. • When redundancy is enabled: Ipv4 address cannot be 0.0.0.0 or cannot be the same as the backup master IP.
Main channel t0	Connection establishment time-out
Main channel t1	ASDU reply time-out
Main channel t2	Wait next information transmission frame (I frame) time-out. t2 < t1
Main channel t3	Idle time-out
Backup master IP	Ipv4 address cannot be 0.0.0.0 or be the same as the main master IP.
Backup channel t0	Connection establishment time-out
Backup channel t1	ASDU reply time-out
Backup channel t2	Wait next information transmission frame (I frame) time-out. t2 < t1
Backup channel t3	Idle time-out

9.13.4.7 Communication Protocols – IEC61850

The **Application Diagnostic > IEC61850** section contains diagnostic data about IEC 61850.



[sc_IEC61850_communication_protocols, 2, --_--]

Figure 9-37 Application Diagnostic – IEC61850

Clients

The **Clients** section contains general information on the clients.

Entry	Meaning
Connection	Number of client connections
IP Address	Client IP address
Port	Port address
Timestamp	Time stamp of connection establishment

Client Disconnect Events

The **Client Disconnect Events** section lists in tabular form the most recent 10 IEC 61850 clients that have logged off the server after a successful connection establishment.

Entry	Meaning
No	Sequential number of the **Disconnect events**
IP	IP address of the client
Port	Port number of the client
Connect time	Time stamp of connection establishment
Disconnect time	Time stamp of the connection termination
Uptime	Duration of the connection

Reports

Every configured report is displayed with corresponding diagnostic values.

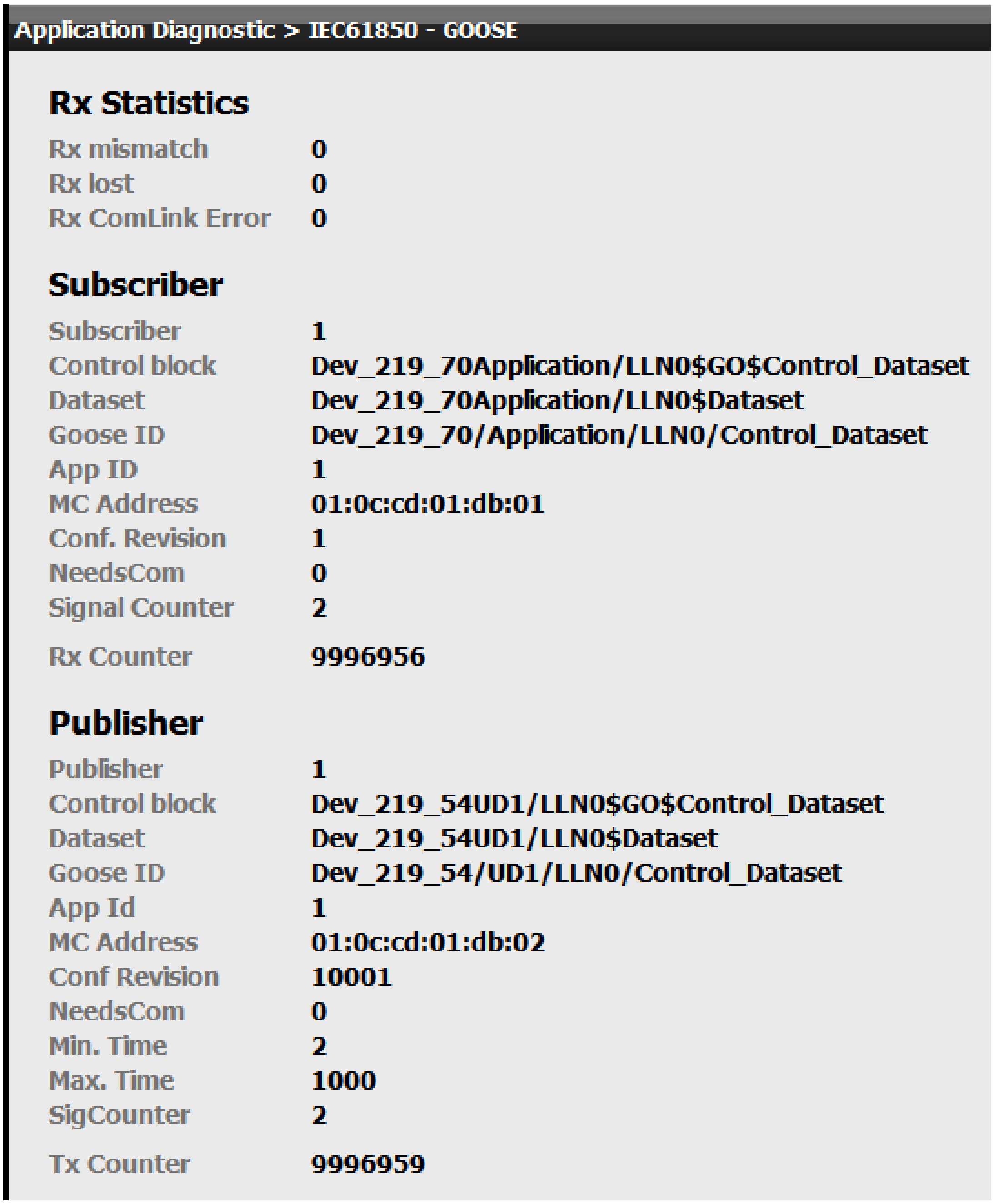
Table 9-5 Report Diagnostic Values

Entry	Meaning
Report	Sequential number of configured reports
CbRef	Control block reference
RptID	Report identifier
RptEna	Report state 0 = Not active 1 = Active
DataSet	Dataset reference
DataSetMembers	Number of signals of referenced reports
ConfRev	Configuration revision number
OptFlds	Optional field: • Bit0: Reserved • Bit1: sequence-number • Bit2: report-time-stamp • Bit3: reason-for-inclusion • Bit4: data-set-name • Bit5: Data reference • Bit6: buffer-overflow • Bit7: entryID • Bit8: conf-revision • Bit9: Reserved
BufTm	Buffer time in ms

Entry	Meaning
TrgOps	Trigger options: • Bit0: Reserved • Bit1: Data-Change • Bit2: Quality-Change • Bit3: Data-Update • Bit4: Integrity • Bit5: Reserved
IntgPd	Integrity period

9.13.4.8 Communication Protocols – IEC61850 - GOOSE

The **Application Diagnostic > IEC61850 - GOOSE** section contains diagnostic data about IEC 61850 GOOSE.



[sc_IEC61850_GOOSE_communication_protocols, 2, --_--]

Figure 9-38 Application Diagnostic – IEC61850 - GOOSE

Rx Statistics

The **Rx Statistics** section contains general diagnostic values.

Entry	Meaning
Rx mismatch	This field indicates that the parameterization is incorrect This is the case for example when the control block has the correct subscriber address, but the configuration does not fit with the expected signals.
Rx lost	This field indicates a possible connection break or failure.
Rx ComLink Error	Internal error counter

Subscriber

The **Subscriber** section displays all configured GOOSE receiver control blocks, each with the following diagnostic values.

Entry	Meaning
Subscriber	Sequential number of configured GOOSE control blocks
Control block	Control block reference
Dataset	Dataset reference
Goose ID	Control-block identifier
App ID	Application ID
MC Address	Multicast address
Conf. Revision	Configuration revision number
NeedsCom	Indicator for state of parameterization 0 = OK 1 = Not OK
Signal Counter	Number of signals in the referenced dataset
Rx Counter	Telegram receipt counter

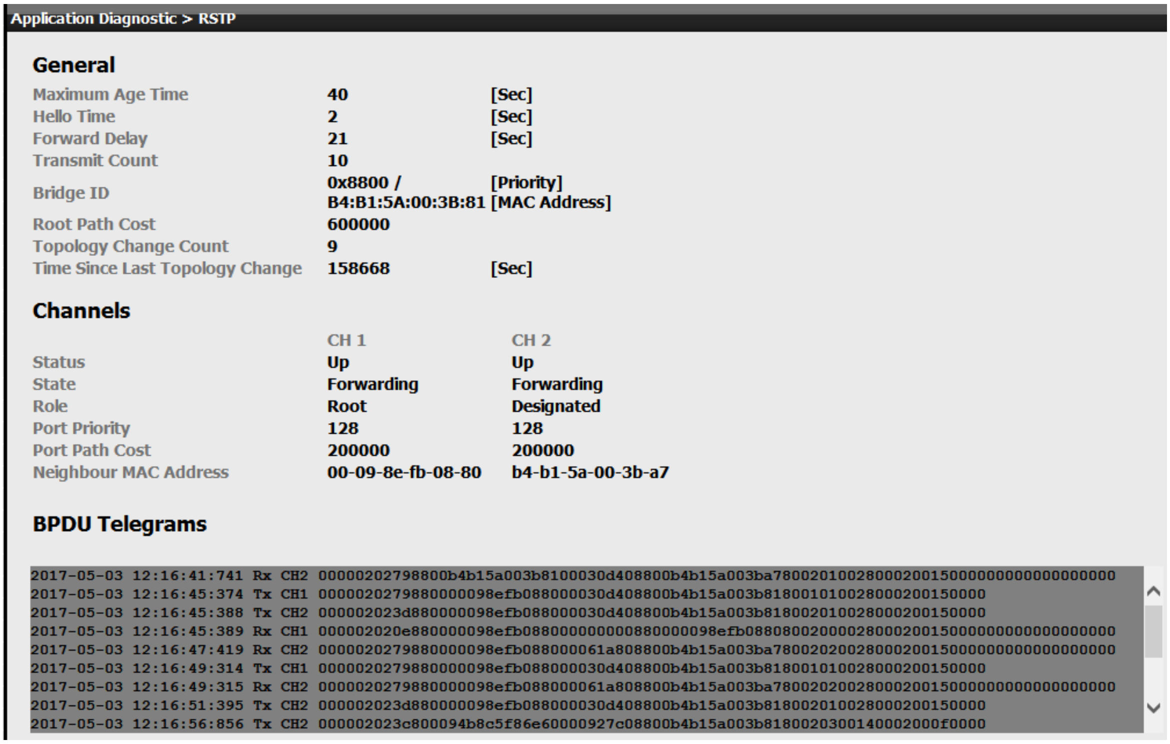
Publisher

The **Publisher** section displays all configured GOOSE transmitter control blocks, each with the following diagnostic values.

Entry	Meaning
Publisher	Sequential number of configured GOOSE control blocks
Control block	Control block reference
Dataset	Dataset reference
Goose ID	Control-block identifier
App ID	Application ID
MC Address	Multicast address
Conf. Revision	Configuration revision number
NeedsCom	Indicator for state of parameterization 0 = OK 1 = Not OK
Min. Time	Minimum time in ms
Max. Time	Maximum time in ms
SigCounter	Number of signals in the referenced dataset
Tx Counter	Telegram transmission counter

9.13.4.9 Application Diagnostic – RSTP

The **Application Diagnostic > RSTP** section contains diagnostic data about RSTP.



[scaprstp-270812-01.tif, 2, --_--]

Figure 9-39 Application Diagnostic – RSTP

General

The **General** section contains the following entries:

Entry	Meaning
Maximum Age Time	Counter that counts down with each pass through a bridge
Hello Time	The time between configuration messages that have been issued by the Root Bridge. With shorter Hello Times, there is a faster detection of topology changes, at the expense of a moderate increase of STP transmissions.
Forward Delay	The time that a bridge requires to register MAC addresses on a rising port before transmission can be started. With lower values, the port can reach the transmission status faster but then, unregistered addresses are transmitted to all ports.
Transmit Count	The maximum number of BDPUs on each port that can be sent within 1 second. With a larger value, the power system can be restored more quickly after failure of a connection/bridge.
Bridge ID	Bridge Identifier The bridge identifier provides a finer gradation of the switches. This enables you to set the location of the alternate switches in the network.
Root Path Cost	The total costs of the path to the root bridge, composed of the sum of costs for each connection in the path.

Entry	Meaning
Topology Change Count	Counter that registers changes of the network topology This value must remain constant during operation. When it remains constant, there has been no topology change in the network.
Time Since Last Topology Change	Time since the last change of the network topology This diagnostic value shows the time elapsed since the last topology change. It must be incremented continually.

Channels

The **Channels** section contains the following entries:

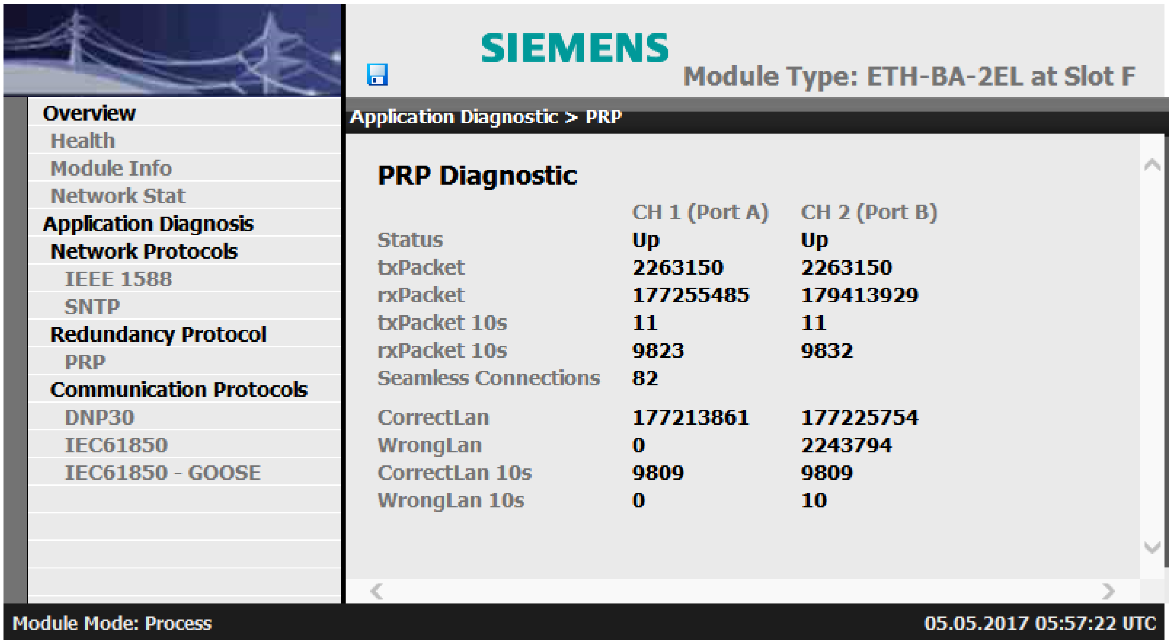
Entry	Meaning
Status	Status of the channel (**Up** or **Down**)
State	State of the port (**Forwarding** or **Discarding**)
Role	Role of the port: • Root • Designated • Alternate • Disabled
Port Priority	The Port Priority Port value is adjustable for each port. The port priority considers the valence of vectors on the receiver side and is taken into account by the port identifier.
Port Path Cost	The path costs indicate the quality of a line. The higher the value, the worse the line.
Neighbour MAC Address	MAC address of the neighboring RSTP bridge on this port

BPDU Telegrams

The **BPDU Telegrams** section contains information on the last RSTP topology changes.

9.13.4.10 Application Diagnostic – PRP

The **Application Diagnostic > PRP** section contains diagnostic data about PRP.



[sc_homepage_PRP, 2, --_--]

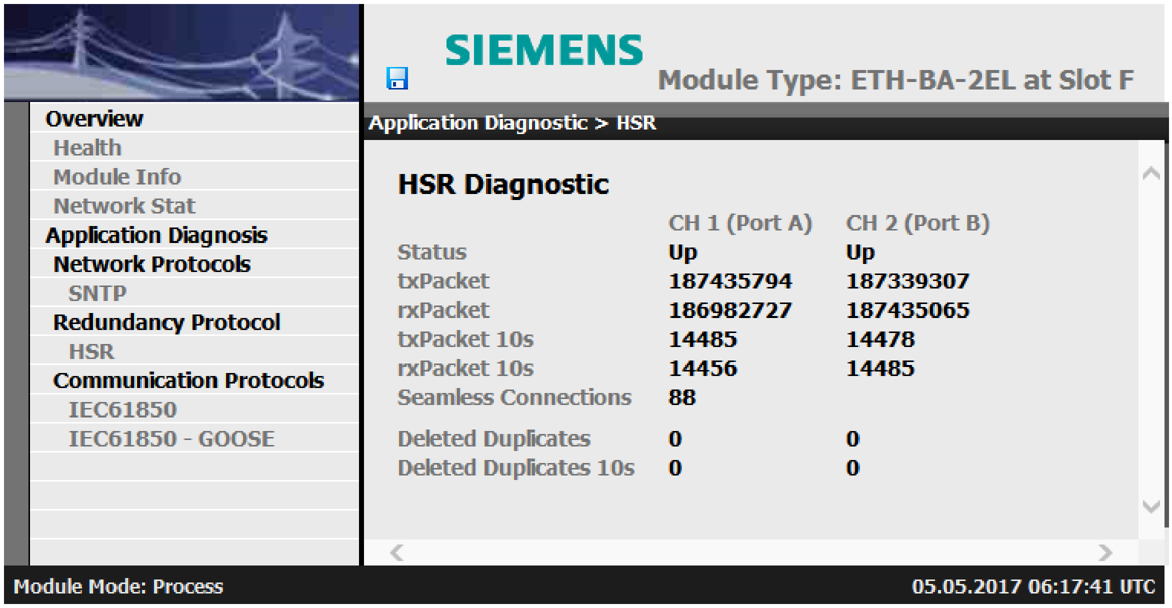
Figure 9-40 Application Diagnostic – PRP

In the **Application Diagnostic > PRP** section, you can find the following entries:

Entry	Meaning
Status	Link status indication
txPacket	Number of data packages sent from the port
rxPacket	Number of data packages received by the port
txPacket 10s	Number of data packages sent from the port within the last 10 s
rxPacket 10s	Number of data packages received by the port within the last 10 s
Seamless Connections	Number of modules to which a seamless connection exists. This value must be < 512.
CorrectLan	Number of PRP packages that were received with a correct PRP LAN ID.
WrongLan	Number of PRP packages that were received with an incorrect PRP LAN ID. If this counter does not equal 0, there may be a wiring error. A wiring error exists, for example, if all modules in the network do not have channel 1 connected to LAN A and channel 2 connected to LAN B.
CorrectLan 10s	Number of PRP packages that were received with a correct PRP LAN ID within the last 10 s.
WrongLan 10s	Number of PRP packages that were received with an incorrect PRP LAN ID within the last 10 s.

9.13.4.11 Application Diagnostic – HSR

The **Application Diagnostic > HSR** section contains diagnostic data about HSR.



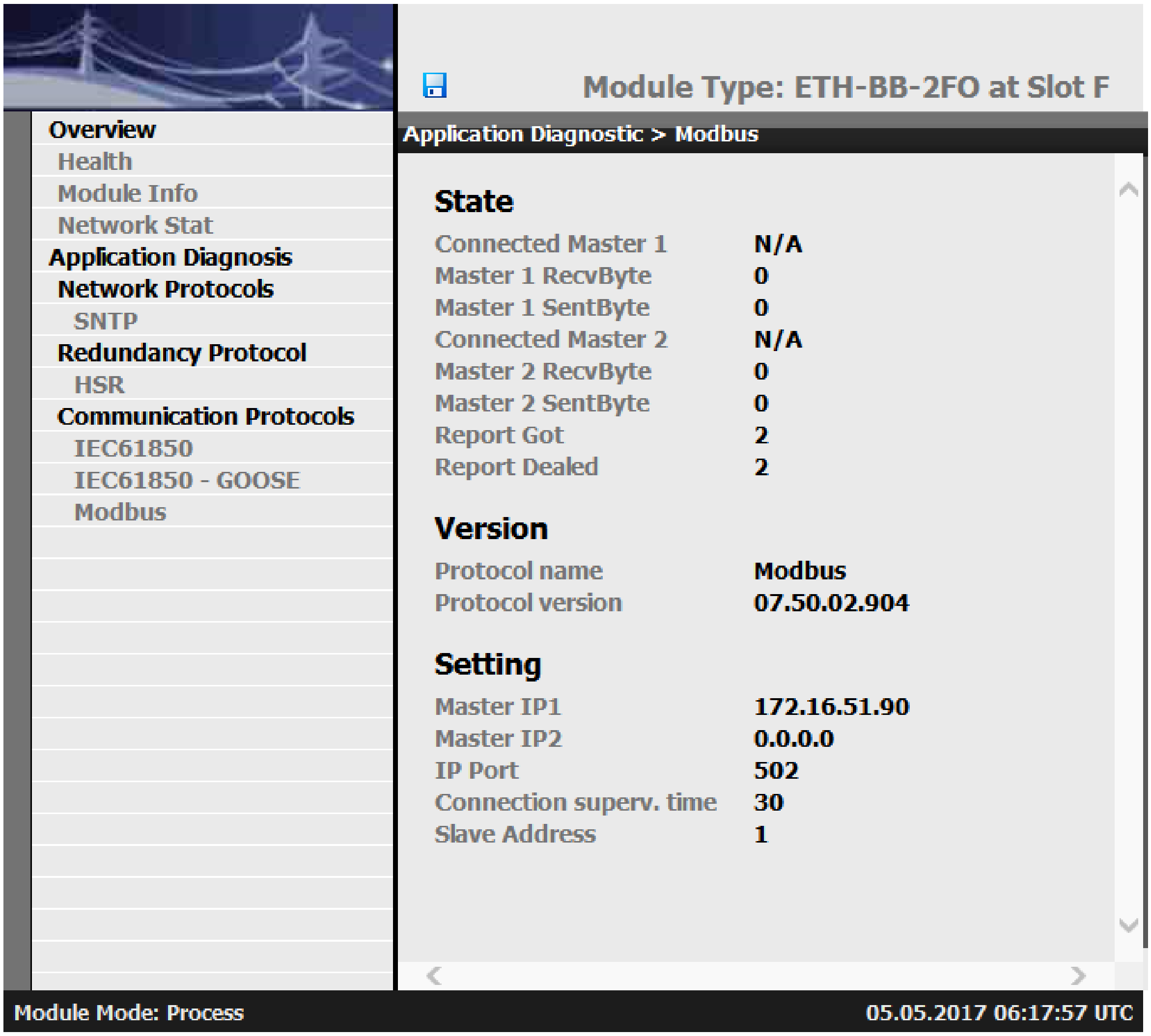
[schsrdia-220113-01.tif, 2, --_--]

Figure 9-41 Application Diagnostic – HSR

In the **Application Diagnostic > HSR** section, you can find the following entries:

Entry	Meaning
Status	Link status indication
txPacket	Number of data packages sent from the port
rxPacket	Number of data packages received by the port
txPacket 10s	Number of data packages sent from the port within the last 10 s
rxPacket 10s	Number of data packages received by the port within the last 10 s
Seamless Connections	Number of modules to which a seamless connection exists. This value must be < 512.
Deleted Duplicates	Number of packages removed from the ring via the HSR duplicate filter
Deleted Duplicates 10s	Number of packages removed from the ring via the HSR duplicate filter within the last 10 s

9.13.4.12 Application Diagnostic – Modbus



[Sc_DiaHomepg_Modbus, 2, --_--]

Figure 9-42 Application Diagnostic – Modbus

State

The **State** section contains the following entries.

Entry	Meaning
Connected Master 1	Display of the IP of Master 1.
Master 1 RecvByte	Bytes received from Master 1 This number is updated continuously.
Master 1 SentByte	Bytes sent from Master 1 This number is updated continuously.
Connected Master 2	Display of the IP of Master 2.
Master 2 RecvByte	Bytes received from Master 2 This number is updated continuously.
Master 2 SentByte	Bytes sent from Master 2 This number is updated continuously.

Entry	Meaning
Report Got	ACSI (Abstract Communication Service Interface) report received by mainboard
Report Dealed	ACSI (Abstract Communication Service Interface) report processed

Version

The **Version** section contains the following entries.

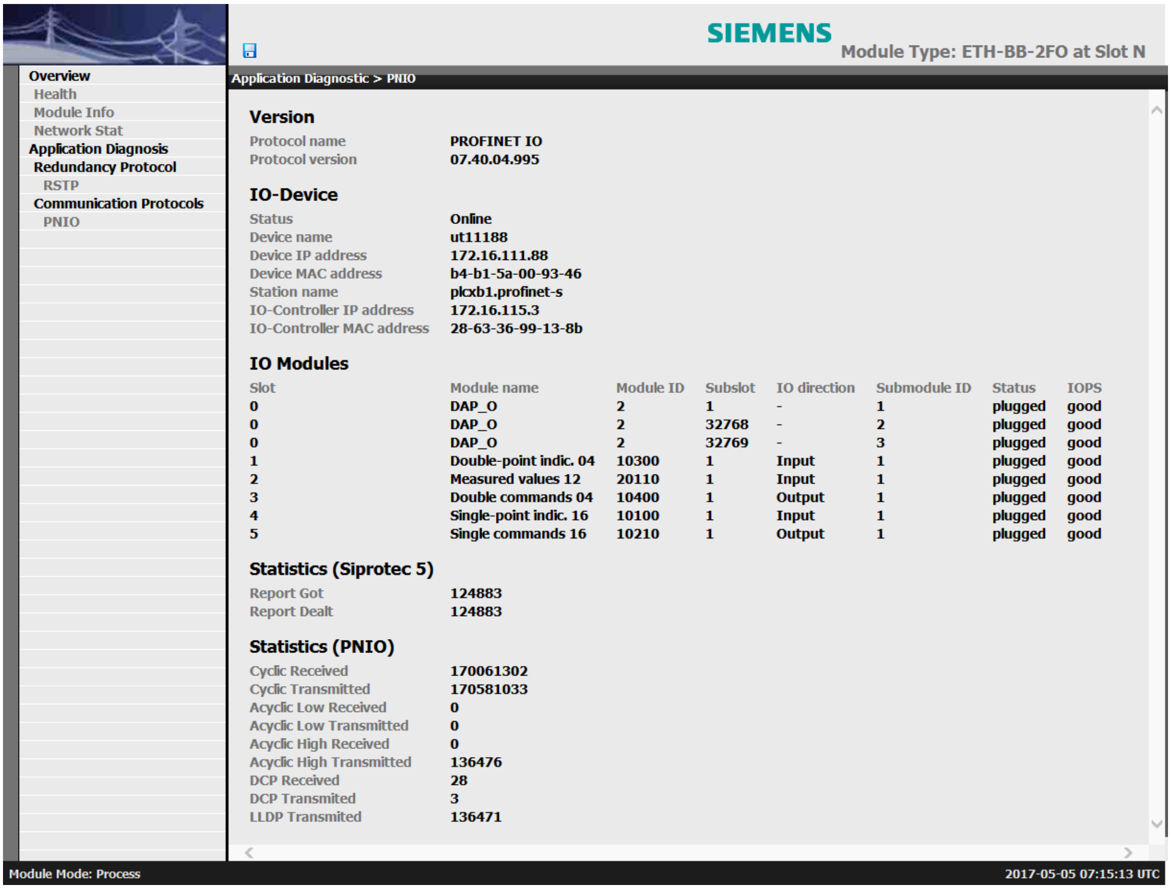
Entry	Meaning
Protocol name	Modbus
Protocol version	Modbus version

Setting

The **Setting** section contains the following entries.

Entry	Meaning
Master IP1	Ipv4 address 0.0.0.0 means that the slave hears and contacts each IP address
Master IP2	Ipv4 address 0.0.0.0 means that the slave hears and contacts each IP address
IP port	The TCP port that the COM module listens to for Modbus
Connection superv. time	TCP/IP Time-out
Slave Address	Modbus slave address of the device

9.13.4.13 Application Diagnostic – PROFINET IO



[sc_PNIO_Homepage, 2, --_--]

Figure 9-43 Application Diagnostic - PROFINET IO

Version

The **Version** section contains the following entries.

Entry	Meaning
Protocol name	PROFINET IO
Protocol version	PROFINET IO version

IO Device

The **IO Device** section contains the following entries.

Entry	Meaning
Status	Status of the IO device
Device name	Name of the IO device
Device IP address	IP address of the IO device
Device MAC address	MAC address of the Ethernet module
Station name	Name of the station
IO-Controller IP address	IP address of the IO controller
IO-Controller MAC address	MAC address of the IO controller

IO Modules

The **IO Modules** section contains the following entries.

Entry	Meaning
Slot	Slot number of the IO module (maximum 18 IO modules plus DAP can be plugged)
Module name	Name of the IO module
Module ID	Identification number of the IO module
Subslot	Subslot number
IO direction	Data direction (input data or output data)
Submodule ID	Identification number of the submodule type
Status	Status of the IO module • Plugged: the IO module is plugged and ready to exchange data • Empty: no IO module plugged/parameterized • Error: no mapping file assignment for the IO module possible; no data exchange with this module
IOPS	Value of the local IOPS for DAP and input data or value of the IO controller IOPA for output data

Statistics (SIP5)

The **Statistics (SIP5)** section contains the following entries.

Entry	Meaning
Report Got	ACSI (Abstract Communication Service Interface) report received
Report Dealt	ACSI report dealt

Statistics (PNIO)

The **Statistics (PNIO)** section contains the following entries.

Entry	Meaning
Cyclic Received	Amount of telegrams for cyclic data received from IO controller
Cyclic Transmitted	Amount of telegrams for cyclic data transmitted to IO controller
Acyclic Low Received	Amount of acyclic low priority telegrams received
Acyclic Low Transmitted	Amount of acyclic low priority telegrams transmitted
Acyclic High Received	Amount of acyclic high priority telegrams received
Acyclic High Transmitted	Amount of acyclic high priority telegrams transmitted
DCP Received	Amount of DCP telegrams received
DCP Transmitted	Amount of DCP telegrams transmitted
LLDP Transmitted	Amount of LLDP (Link Layer Discovery Protocol) telegrams transmitted

NOTE

Empty slots after the last plugged IO module are not displayed. A maximum of 18 slots is possible.

The diagnosis page is displayed in English language only.

9.13.5 Application Diagnosis Section for Serial Modules

9.13.5.1 Structure

The **Application Diagnostic** section contains diagnostic pages for the following protocols:

- DNP3
- IEC 60870-5-103

- SUP Serial
- Protection interface

NOTE

The **Application Diagnostic** section is structured identically for electrical and optical modules.

9.13.5.2 Application Diagnostic – IEC 60870-5-103

The **Application Diagnostic > IEC 60870-5-103** section contains diagnostic data about IEC 60870-5-103.

Application Diagnostic > T103

State

Channel Name	T103[COM2:1]
Channel State	Running
Frames Sent	0
Frames Received	0
Frames With Errors	0
Max. Receive Latency [ms]	0
Max. Processing Time [ms]	0
Max. Response Time [ms]	0
Max. Resp. TimeRecv. Latency [ms]	0
Responese Timeouts	0
Settings / Reports Processed	3
Settings / GI Starts	0
Settings / GI Started	0
Mappings / Reports Processed	3
Mappings / GI Starts	0
Mappings / GI Started	0

Setting

Slave Address	1
Baudrate	9600
Parity	Even
Data Bit	8
Stop Bit	1

[sc_T103_Application_diagnostic, 2, --_--]

Figure 9-44 Application Diagnostic – IEC 60870-5-103

State

The **State** section contains the following entries.

Entry	Meaning
Channel Name	Internal channel description
Channel State	Display of the state of the connection to the master
Frames Sent	Telegrams sent The number of telegrams is updated continuously.
Frames Received	Telegrams received The number of telegrams is updated continuously.
Frames With Errors	Faulty telegrams The number of telegrams is updated continuously.
Max. Receive Latency [ms]	Maximum latency for reception in ms
Max. Processing Time [ms]	Maximum processing time in ms
Max. Response Time [ms]	Maximum response time in ms
Max. Resp. TimeRecv. Latency [ms]	Maximum latency for the reaction in ms
Response timeouts	Reaction time-out
Settings / Reports Processed	Statistics of the Reports Processed parameter
Settings / GI Starts	Statistics of the GI Starts parameter
Settings / GI Started	Statistics of the GI Started parameter
Mappings / Reports Processed	Statistics of the Reports Processed mapping
Mappings / GI Starts	Statistics of the GI Starts mapping
Mappings / GI Started	Statistics of the GI Started mapping

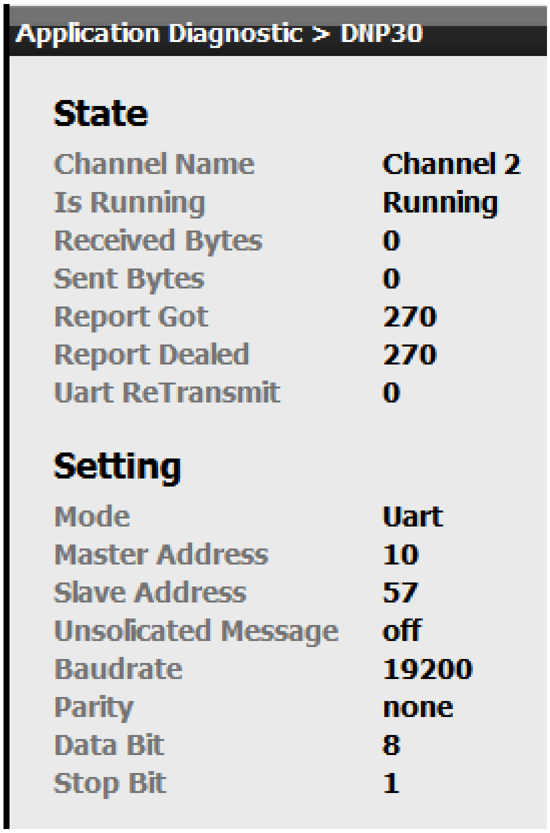
Setting

The **Setting** section contains the following entries.

Entry	Meaning
Slave Address	Device address
Baud rate	Set baud rate
Parity	Set parity
Data bit	Set data bits
Stop bit	Set stop bits

9.13.5.3 Application Diagnostic – DNP3

The **Application Diagnostic > DNP3** chapter contains diagnostic data about DNP3.



[sc_DNP3_Application_diagnostic, 2, --_--]

Figure 9-45 Application Diagnostic – DNP3

State

The **State** section contains the following entries.

Entry	Meaning
Channel Name	Internal channel description
Is Running	State display for the protocol (current state)
Received Bytes	Received Bytes
Sent Bytes	Sent Bytes
Report Got	Telegrams sent from device to module
Report Dealed	Telegrams arranged from device to module
Uart ReTansmit	Number of telegram repetitions on the interface

Setting

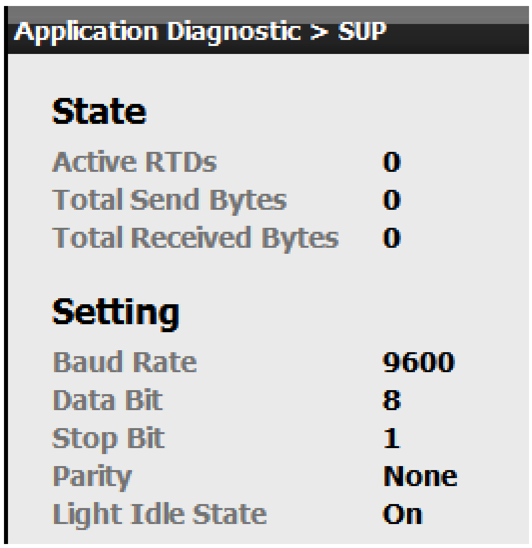
The **Setting** section contains the following entries.

Entry	Meaning
Mode	Connection via Ethernet or serial connection
Master Address	Address of the master
Slave Address	Address of the slave
Unsolicited Message	Unsolicited transmission

Entry	Meaning
Baud rate	Set baud rate
Parity	Set parity
Data bit	Set data bits
Stop bit	Set stop bits

9.13.5.4 Application Diagnostic – SUP Serial

The **Application Diagnostic > SUP Serial** section contains diagnostic data about SUP Serial.



[sc_SUP_diagnostic, 1, --_--]

Figure 9-46 Application Diagnostic – SUP Serial

State

The **State** section contains the following entries.

Entry	Meaning
Active RTDs	Number of active RTDs/20-mA units
Total Sent Bytes	Sent Bytes
Total Received Bytes	Received Bytes

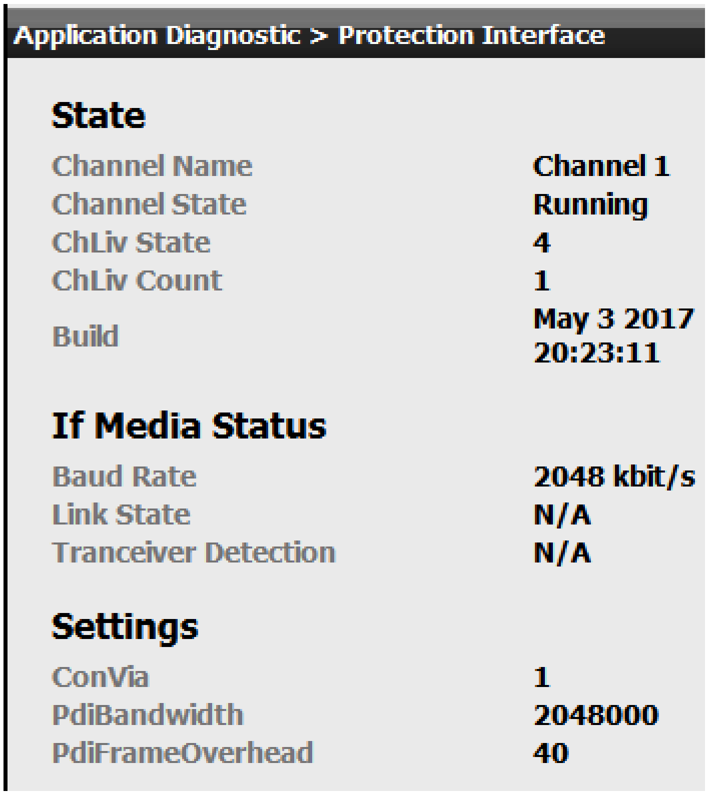
Setting

The **Setting** section contains the following entries.

Entry	Meaning
Baudrate	Set baud rate
Data Bit	Set data bits
Stop Bit	Set stop bits
Parity	Set parity
Light Idle State	Status of idle light

9.13.5.5 Application Diagnostic – Protection Interface

The **Application Diagnostic > Protection interface** section contains diagnostic data about the protection interface.



[sc_Protection interface diagnostic part 1, 1, --_--]

Figure 9-47 Application Diagnostic – Protection Interface, Part I

Application Diagnostic > Protection Interface

HDLC

Com Status / RXHPFramesOK	41134
Com Status / RXLPFramesOK	0
Com Status / RXHPFramesERR	0
Com Status / RXLPFramesERR	0
Com Status / RXHPSeqCountERR	0
Com Status / TXHPFramesOK	41127
Com Status / TXLPFramesOK	0
Com Status / TXHPFramesERR	0
Com Status / TXLPFramesERR	0
Com Status / TXHPSeqCountERR	0
Bridge Status / Status	1
Bridge Status / Bridge Status/ Action	1
Bridge Status / Priority	1
Bridge Status / Version	1
Bridge Status / StatusRegister	5
Bridge Status / RBdNum	16
Bridge Status / RBufLineNum	16
Bridge Status / RBufLineSize	1504
Bridge Status / TBdNum	16
Bridge Status / linkBurstCount	0
Bridge Status / linkBeatCount	0
Bridge Status / linkBurstMaxBeat	0
Bridge Status / linkRetriggerCount	0
Bridge Status / linkRetriggerFlag	0
Bridge Status / linkIRQTXReqCount	46178471
Bridge Status / linkIRQTXConCount	46178471
Bridge Status / linkIRQRXConCount	46178478

[sc_Protection interface diagnostic part 2, 1, --_--]

Figure 9-48 Application Diagnostic – Protection Interface, Part II

Application Diagnostic > Protection Interface

ComLink

Com Status / RXHPFramesOK	17139
Com Status / RXLPFramesOK	43983
Com Status / RXHPFramesERR	0
Com Status / RXLPFramesERR	237
Com Status / RXHPSeqCountERR	0
Com Status / TXHPFramesOK	16632
Com Status / TXLPFramesOK	46298
Com Status / TXHPFramesERR	0
Com Status / TXLPFramesERR	0
Com Status / TXHPSeqCountERR	0
Bridge Status / Status	1
Bridge Status / Bridge Status/ Action	1
Bridge Status / Priority	1
Bridge Status / Version	1
Bridge Status / StatusRegister	15
Bridge Status / RBdNum	64
Bridge Status / RBufLineNum	64
Bridge Status / RBufLineSize	1504
Bridge Status / TBdNum	64
Bridge Status / linkBurstCount	0
Bridge Status / linkBeatCount	0
Bridge Status / linkBurstMaxBeat	0
Bridge Status / linkRetriggerCount	668137
Bridge Status / linkRetriggerFlag	0
Bridge Status / linkIRQTXReqCount	92356856
Bridge Status / linkIRQTXConCount	92356856
Bridge Status / linkIRQRXConCount	92351341

[sc_Protection interface diagnostic part 3, 1, --_--]

Figure 9-49 Application Diagnostic – Protection Interface, Part III

State

The **State** section contains the following entries.

Entry	Meaning
Channel Name	Internal channel description
Channel State	State display for the protocol (current state)

Entry	Meaning
ChLiv State	State of **Channel Live**
CLiv Count	Counter of **Channel Live**
Build	Build date of the protocol

If Media Status

The **If Media Status** section contains the following entries.

Entry	Meaning
Baud Rate	Set baud rate
Link State	Link status
Transceiver Detection	FO: N/A (always N/A) (NO transceiver detected, transceiver detected), fault event: N/A

Settings

The **Settings** section contains the following entries.

Entry	Meaning
ConVia	Protection interface is **`Connection via`**
PdiBandwidth	Bit rate (bit/s) for protection telegrams based on the parameter **`Connection via`**
PdiFrameOverhead	Overhead for every protection telegram in bit.

HDLC and COM link

The **HDLC** and **COM link** sections contain the following entries.

Entry	Meaning
Com Status / RXHPFramesOK	Number of the corresponding frames Incoming telegrams, high priority, OK
Com Status / RXLPFramesOK	Number of the corresponding frames Incoming telegrams, low priority, OK
Com Status / RXHPFramesERR	Number of the corresponding frames Incoming telegrams, high priority, faulty
Com Status / RXLPFramesERR	Number of the corresponding frames Incoming telegrams, low priority, faulty
Com Status / RXHPSeqCountERR	Number of the corresponding frames
Com Status / TXHPFramesOK	Number of the corresponding frames Sending telegrams, high priority, OK
Com Status / TXLPFramesOK	Number of the corresponding frames Sending telegrams, low priority, OK
Com Status / TXHPFramesERR	Number of the corresponding frames Sending telegrams, high priority, faulty
Com Status / TXLPFramesERR	Number of the corresponding frames Sending telegrams, low priority, faulty
Com Status / TXHPSeqCountERR	Number of the corresponding frames
Bridge Status / Status	Siemens-internal special diagnostic for fault search
Bridge Status / Bridge Status/ Action	Siemens-internal special diagnostic for fault search
Bridge Status / Priority	Siemens-internal special diagnostic for fault search
Bridge Status / Version	Siemens-internal special diagnostic for fault search
Bridge Status / StatusRegister	Siemens-internal special diagnostic for fault search
Bridge Status / RBdNum	Siemens-internal special diagnostic for fault search

Entry	Meaning
Bridge Status / RBufLineNum	Siemens-internal special diagnostic for fault search
Bridge Status / RBufLineSize	Siemens-internal special diagnostic for fault search
Bridge Status /TBdNum	Siemens-internal special diagnostic for fault search
Bridge Status / linkBurstCount	Siemens-internal special diagnostic for fault search
Bridge Status / linkBeatCount	Siemens-internal special diagnostic for fault search
Bridge Status / linkBurstMaxBeat	Siemens-internal special diagnostic for fault search
Bridge Status / linkRetriggerCount	Siemens-internal special diagnostic for fault search
Bridge Status / linkRetriggerFlag	Siemens-internal special diagnostic for fault search
Bridge Status / linkIRQTXReqCount	Siemens-internal special diagnostic for fault search
Bridge Status / linkIRQTXConCount	Siemens-internal special diagnostic for fault search
Bridge Status / linkIRQRXConCount	Siemens-internal special diagnostic for fault search

9.13.6 Application Diagnostic – SUP Ethernet

You can find more information on SUP Ethernet in the following manuals:

- SIPROTEC Transformer Differential Protection
- SIPROTEC Distance Protection, Line Differential Protection, and Overcurrent Protection for 3-Pole Tripping
- SIPROTEC Distance and Line Differential Protection, Breaker Management for 1-Pole and 3-Pole Tripping

10 Commissioning and Diagnostics

10.1 Diagnostic Information

10.1.1 Prerequisite

NOTE

In this chapter, the commissioning procedure is presented in compressed form.

All components must be installed and operating properly.

Creating a List of Addresses

NOTE

With the aid of an address list, you can obtain an overview of the network topology. This list contains all important information about the devices. In this way, you can find any errors quickly.

Siemens thus recommends that you first create a list of component addresses immediately.

The list must contain the following information at a minimum:

- Device type
- Product code
- Serial number
- Firmware version in the device
- Firmware version in the module
- IP address
  IP settings can be read only after the devices have been initialized, that is, the parameter sets have been loaded into the devices.
- Subnet mask
- Standard gateway
- MAC address
  The MAC addresses can be read directly on the display of the device (Menu 5-5 Enter).
- IED name under IEC 61850 for each device

It makes sense to also obtain the above-mentioned information for third-party devices, for example, switches.

Supplement this list with a description of the network topology. This topology description explains how the devices are connected to one another.

To obtain information about devices from the competition, follow the procedure in the Manuals.

Once the list is complete, check whether any IP addresses appear twice. MAC addresses do not appear twice when network components are identified unambiguously.

Additional commissioning information is available at www.siprotec.de.

Commissioning a Ring Structure

NOTE

Note that one part deals with the RSTP settings.

Prior to commissioning, check whether the system has been installed correctly.

Startup proceeds in the following sequence:

- Switch on the switches
  Siemens recommends waiting approximately 1 minute after switching on the power.
- Switch on the devices
  Siemens recommends switching the devices on one after another in accordance with their location in the ring and loading the new Config if necessary. After successfully loading the Config, wait until the device has started up before you switch on the next device.
  If Port J is used as the Config interface, all devices can remain switched on and be loaded all at once with DIGSI 5.

10.1.2 Additional Tests

Check Accessibility

After settings have been made and parameters loaded, all components must be accessible via their IP address. This must be possible regardless of whether the ring is open or closed.

NOTE

Note that modules can operate both in Line and in Switch mode. The homepages thus differ accordingly. You use DIGSI 5 to set the operating mode.

If a device cannot be reached, the following reasons can be the cause:

- A SIPROTEC 5 device connected to a switch via a Line connection is switched off.
- A SIPROTEC 5 device incorporated into an optical ring is switched off.
- A ring structure is cut at more than one point. As a result, some of the devices are no longer accessible.
  The following reasons can be the cause of the break:
  - Switched-off devices
  - Broken connections
  - Device in FW/Config loading/Fallback mode

Upon completion of these preliminaries, a ring structure is in operation. Additional settings are now possible.

10.1.3 General Information about the Diagnostic Information

The SIPROTEC 5 device offers various output options for diagnostic data.

- **Diagnostic data at the device**
  The device display shows various information.
  Main menu:
  - Communication
  - Test & diagnostics
    Device information
    Hardware/software information
    System protocol
- **Diagnostic data via DIGSI**
  Diagnostic data can be read out with DIGSI 5 and the DIGSI 5 protocol.
  The diagnostic pages and the communication log provide assistance during commissioning or when performing diagnoses during operation by providing important data online.

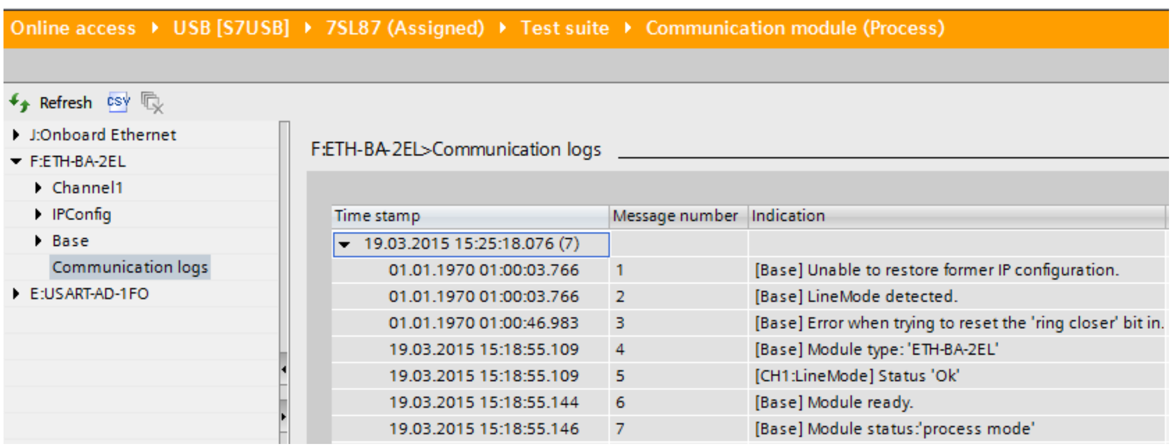
- **Diagnostic data via the homepage**
  You can find more information in chapter *9.13 Homepage*.
  If you want to download the data, click the floppy-disk icon.

10.1.4 Communication Log

Opening the Communication Log

You can open the communication log via the following steps:

- In DIGSI, select the area **Online Access** in the **Project Tree**.
- Then select the interface to which the device is connected.
- Next, select **Updating accessible participants**. The local network is searched for SIPROTEC 5 devices.
- Next, select the device and click **Get all data from device**. The configuration and process data are read out.
- Next, select **Test Suite** and then **Communication module**. You can now open the communication log for each communication module under the settings for the channels.



[sc_IEC_communication_log, 1, en_US]

Figure 10-1 Communication Log

Variables in the Communication Log

The communication log contains the following variables:

Variable	Description
Force the module into fallback mode!	The mainboard has sent a signal to start the fallback mode only for a certain reason, for example, inconsistent settings files DCF/CCF
The module has been rebooted for the 3rd time unsuccessfully!	A fault remains in the 1st or 2nd start level after the 3rd restart attempt and is in fallback (without the protocols having been started)
-- MODULE STOPS WORKING --	Module stopped.
Too many initialization errors during 1st level com startup!	Start of the 1st level has failed.
Wrong module at...	The module parameter settings do not match the module that is inserted.
Protocol[24] found in configuration file	Start of the 1st level OK. ComObj available (DCF parsing successful)

24 For example, protocol IEC 60870-5-103, IEC 60870-5-104, Modbus, or DNP3

Variable	Description
Launching protocol (handle 0x%x) failed!	Start of the protocol has failed. Possible reasons: Delayed connection failed? No .so file?
Protocol successfully launched.	Start of the 1st level OK ComObj available (DCF parsing successful) Protocols have started
Too many initialization errors during 2nd level com startup!	Start of the 2nd level has failed
Set of module Health failed!	No ComLink connection Problems with SessionMngr Wrong readiness path?
Startup finished	ComBase-Start finished Process mode: Protocols running Fallback mode: Protocols not running
Module PCB type	PCB type
Module[25] detected in slot 1 (port F).	Module is inserted in Port F Module core running NFS running!
Module detected in slot 2 (port E).	Module is inserted in Port E Module core running NFS running!
Module detected in slot 3 (port P).	Module is inserted in Port P Module core running NFS running!
Module detected in slot 4 (port N).	Module is inserted in Port N Module core running NFS running!
CCF GUID(%s) check failed at slot%i!	DCF and CCF are inconsistent, GUIDs are not identical.
CCF compKey(%s) check failed at slot%i!	DCF and CCF are inconsistent, compKeys are not identical.

10.1.5 Diagnostic Information for IEC 61850

Diagnostic Data at the Device

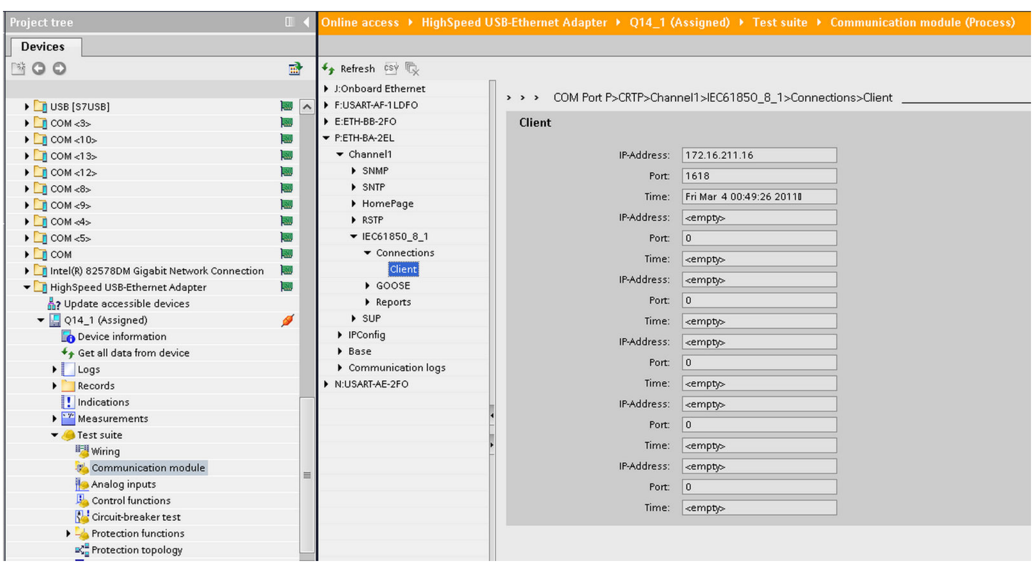
Table 10-1 Displayed Values and Their Description

Name	Values	Description
Channel name	Text	Internal channel description
Protocol State	Running/Stopped	State display for the protocol (current state)
Received Bytes	Number of bytes	Received Bytes
Sent Bytes	Number of bytes	Sent Bytes
Master Address	Number	Address of the master
Slave Address	Number	Address of the slave
Unsolicited Message	On/off	Unsolicited transmission
ReportDealed	Number	Telegrams arranged from device to module

25 This is where the type of module is indicated, for example, USART-AE-2FO V1.00.

Name	Values	Description
ReportGot	Number	Telegrams sent from device to module
TCP or Uart	TCP or Uart	Connection via Ethernet or serial
Baud rate	Number	Set baud rate (for serial communication only)
Parity	EVEN/ODD/NONE	Set parity (for serial communication only)
Data bits	7/8	Set data bits (for serial communication only)
StopBit	1 or 2	Set stop bits (for serial communication only)
IPPort	Number	Number of the IP port (for Ethernet communication only)
SubNetMask	Number	Subnet mask (for Ethernet communication only)
Gateway	Number	Gateway (for Ethernet communication only)

Diagnostic Data via DIGSI



[scdgclnt-280111-01.tif, 1, en_US]

Figure 10-2 Diagnostic Pages – Connections for the Client

Diagnostic indications regarding communication are displayed in a communication log. The communication log displays, for instance, whether a module has started up successfully and communication services have been initiated. The communication log can be retrieved from the device as an indication list by DIGSI 5.

Diagnostic Data via DIGSI – GOOSE Control Blocks and Reports Generated

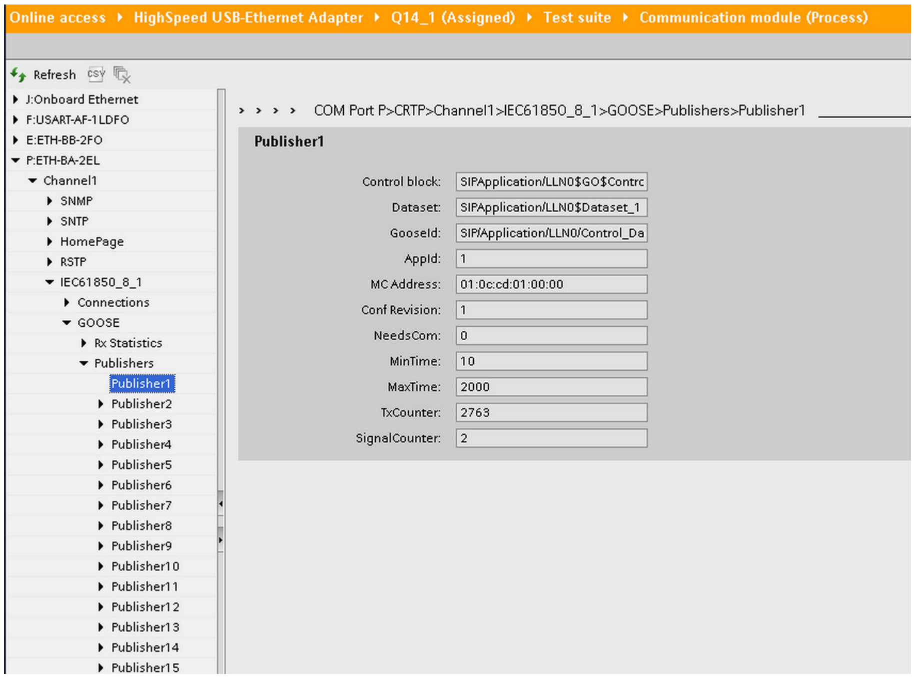
You can find the following information in the IEC 61850 protocol:

- Generated reports and GOOSE datasets that have been transmitted by the device are displayed.
- Once a connection has been established between the servers, objects that have been received via GOOSE messages from other devices are displayed.

  This allows you to recognize, for instance, whether configured GOOSE connections in DIGSI 5 are also communicating successfully.

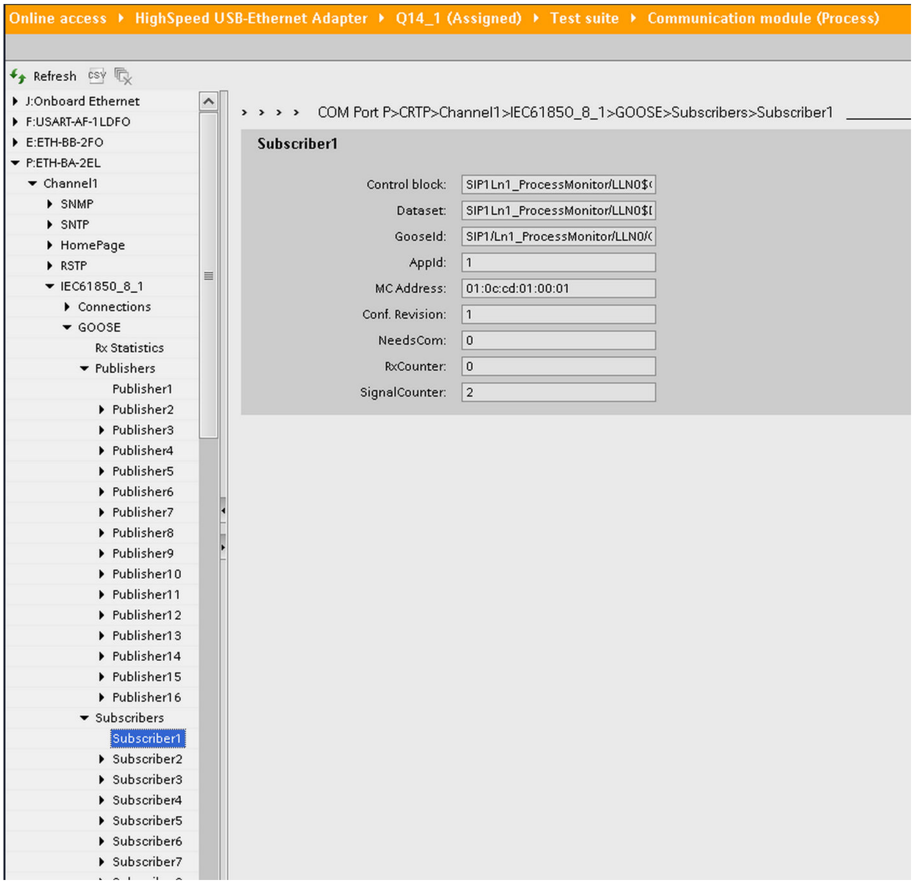
- Transmitted and received GOOSE messages are counted.
- Faulty telegrams are displayed.

The diagnostic pages are available for the GOOSE (Publisher, Subscriber) and Reports sections.



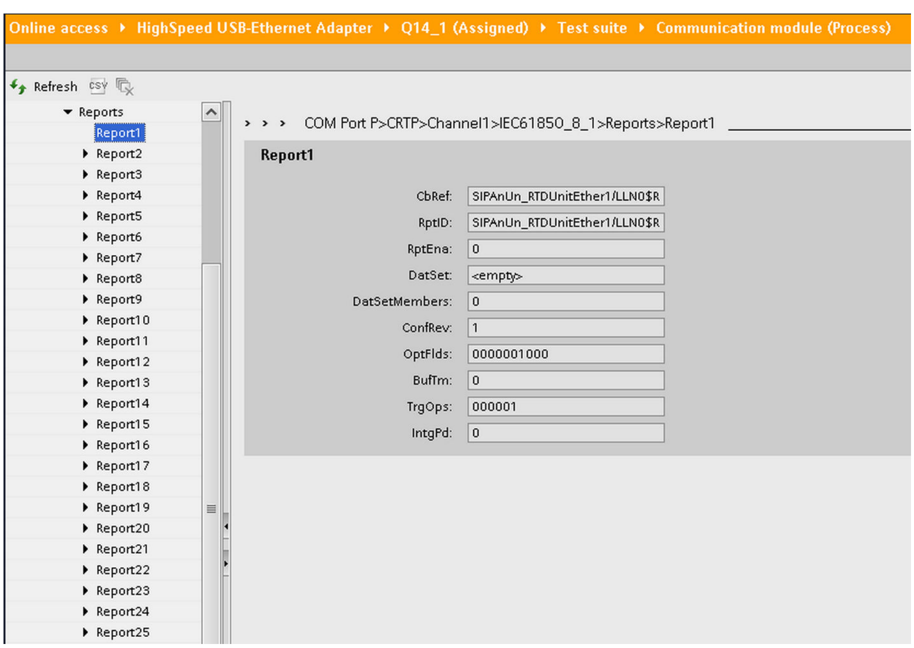
[scdgpubl-280111-01.tif, 1, en_US]

Figure 10-3 Diagnostic Pages for GOOSE – Publisher



[scdgsubs-280111-01.tif, 1, en_US]

Figure 10-4 Diagnostic Pages for GOOSE – Subscriber

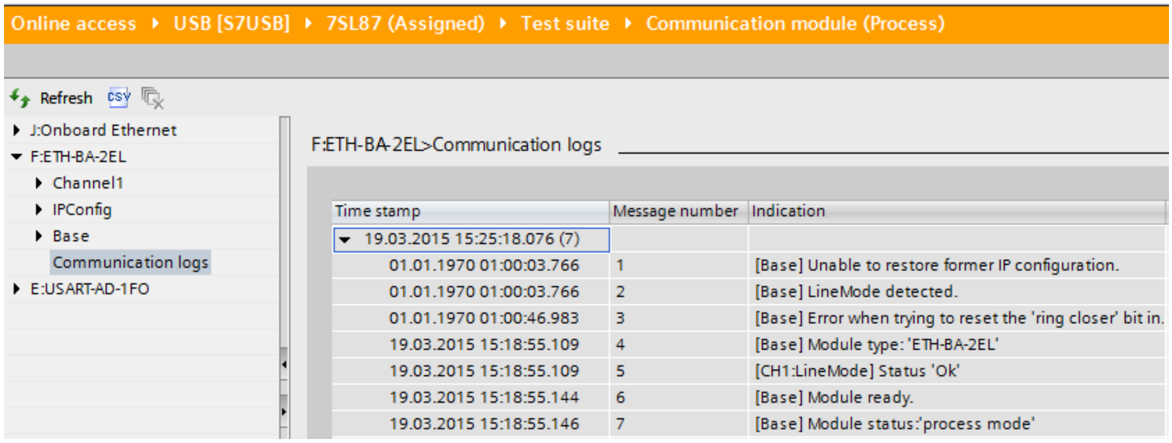


[scdgrept-280111-01.tif, 1, en_US]

Figure 10-5 Diagnostic Pages for Reports

Diagnostic Data for Time Synchronization

Diagnostic data can also be retrieved online for the configured SNTP time servers. This allows you to check successful time synchronization of the device.



[sc_IEC_communication_log, 1, en_US]

Figure 10-6 Communication Log

Diagnostic Data via the Homepage

You can find more information in chapter *9.13.4.7 Communication Protocols – IEC61850*.

10.1.6 Diagnostic Information for DNP3

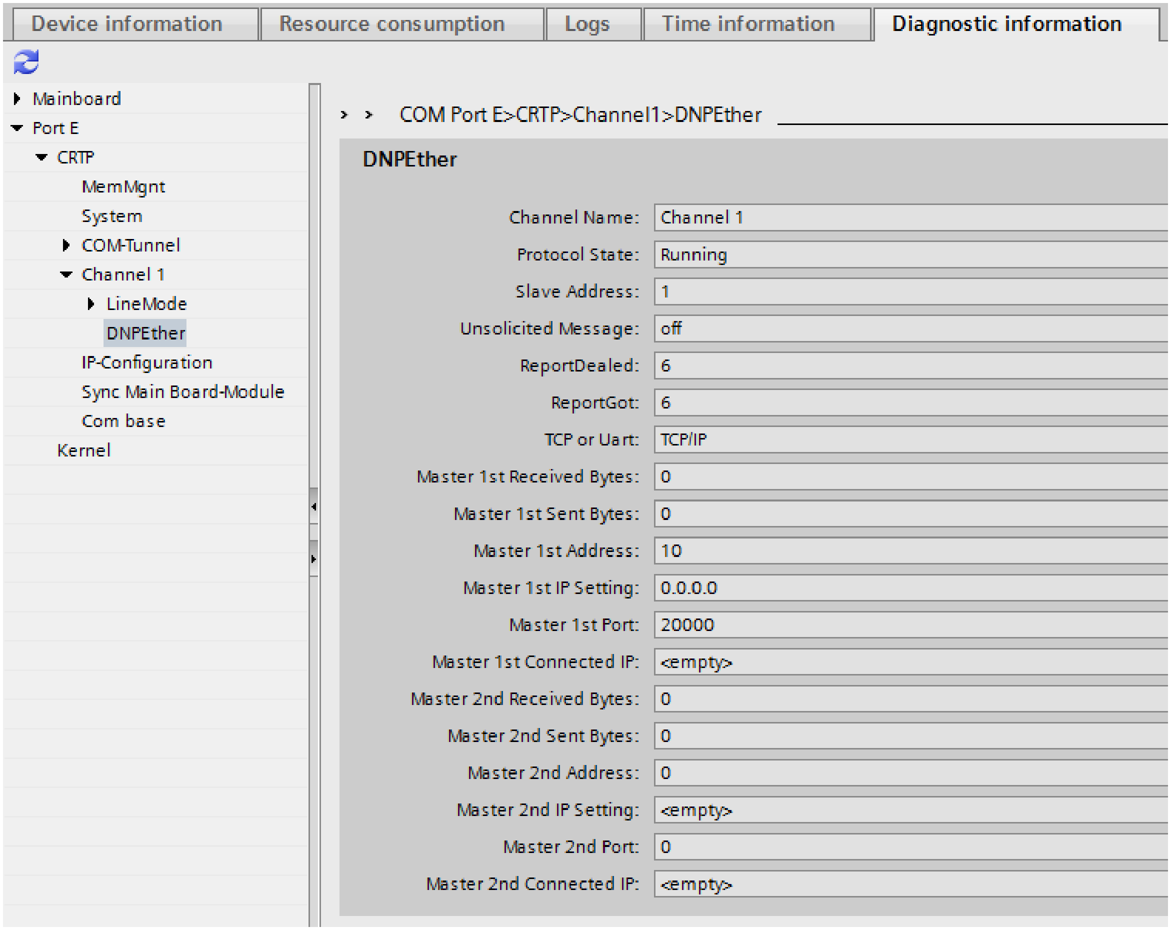
DNP3 Ethernet Diagnostic Data at the Device

Table 10-2 Displayed Values and Their Description

Name	Values	Description
Channel Name	Text	Internal channel description
Protocol State	Running/Stopped	State display for the protocol (current state)
Slave Address	Number	Address of the slave
Unsolicited Message	On/off	Unsolicited transmission
ReportDealed	Number	Telegrams arranged from device to module
ReportGot	Number	Telegrams sent from device to module
TCP or Uart	TCP or Uart	Connection via Ethernet or serial
Master 1st Received Bytes	Number of bytes	Received bytes from the first master
Master 1st Sent Bytes	Number of bytes	Sent bytes to the first master
Master 1st Address	Number	Master address of the first master
Master 1st IP Setting	Text	IP address of the first master
Master 1st Port	Number	TCP port setting of the first master
Master 1st Connected IP	Text	IP address of the first connected master
Master 2nd Received Bytes	Number of bytes	Received bytes from the second master
Master 2nd Sent Bytes	Number of bytes	Sent bytes to the second master
Master 2nd Address	Number	Master address of the second master
Master 2nd IP Setting	Text	IP address of the second master
Master 2nd Port	Number	TCP port setting of the second master
Master 2nd Connected IP	Text	IP address of the second connected master

DNP3 Ethernet Diagnostic Data via DIGSI

DNP3 Ethernet diagnostic data can be read out with DIGSI.



[sc_diaDNPEthernet, 1, en_US]

Figure 10-7 DNP3 Ethernet Diagnostic Data in DIGSI

DNP3 Serial Diagnostic Data at the Device

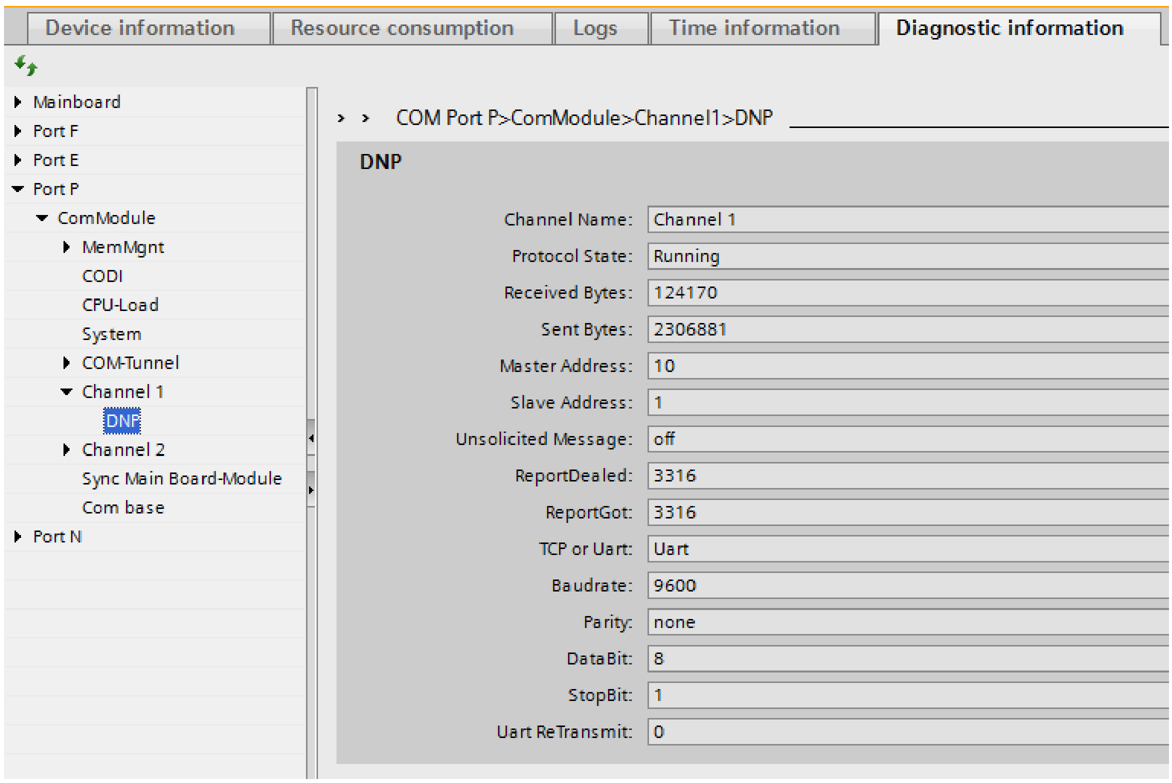
Table 10-3 Displayed Values and Their Description

Name	Values	Description
Channel name	Text	Internal channel description
Protocol State	Running/Stopped	State display for the protocol (current state)
Received Bytes	Number of bytes	Received Bytes
Sent Bytes	Number of bytes	Sent Bytes
Master Address	Number	Address of the master
Slave Address	Number	Address of the slave
Unsolicited Message	On/off	Unsolicited transmission
ReportDealed	Number	Telegrams arranged from device to module
ReportGot	Number	Telegrams sent from device to module
TCP or Uart	TCP or Uart	Connection via Ethernet or serial
Baudrate	Number	Set baud rate
Parity	EVEN/ODD/NONE	Set parity
DataBit	7/8	Set data bits

Name	Values	Description
StopBit	1 or 2	Set stop bits
Uart ReTransmit	0	Retransmission times in case of the communication failure via serial port

DNP3 Serial Diagnostic Data via DIGSI

DNP3 serial diagnostic data can be read out with DIGSI.



[scdiadnp-060511-01.tif, 3, en_US]

Figure 10-8 DNP3 Serial Diagnostic Data in DIGSI

10.1.7 Diagnostic Information for IEC 60870-5-104

Diagnostic Data at the Device

You can find the diagnostic data in the HMI under **Test & Diagnosis** -> **Siemens internal** -> **Runtime data** -> **Analysis** -> **COM Port E/F/N/P** -> **CRTP** -> **Channel 1** -> **T104**.

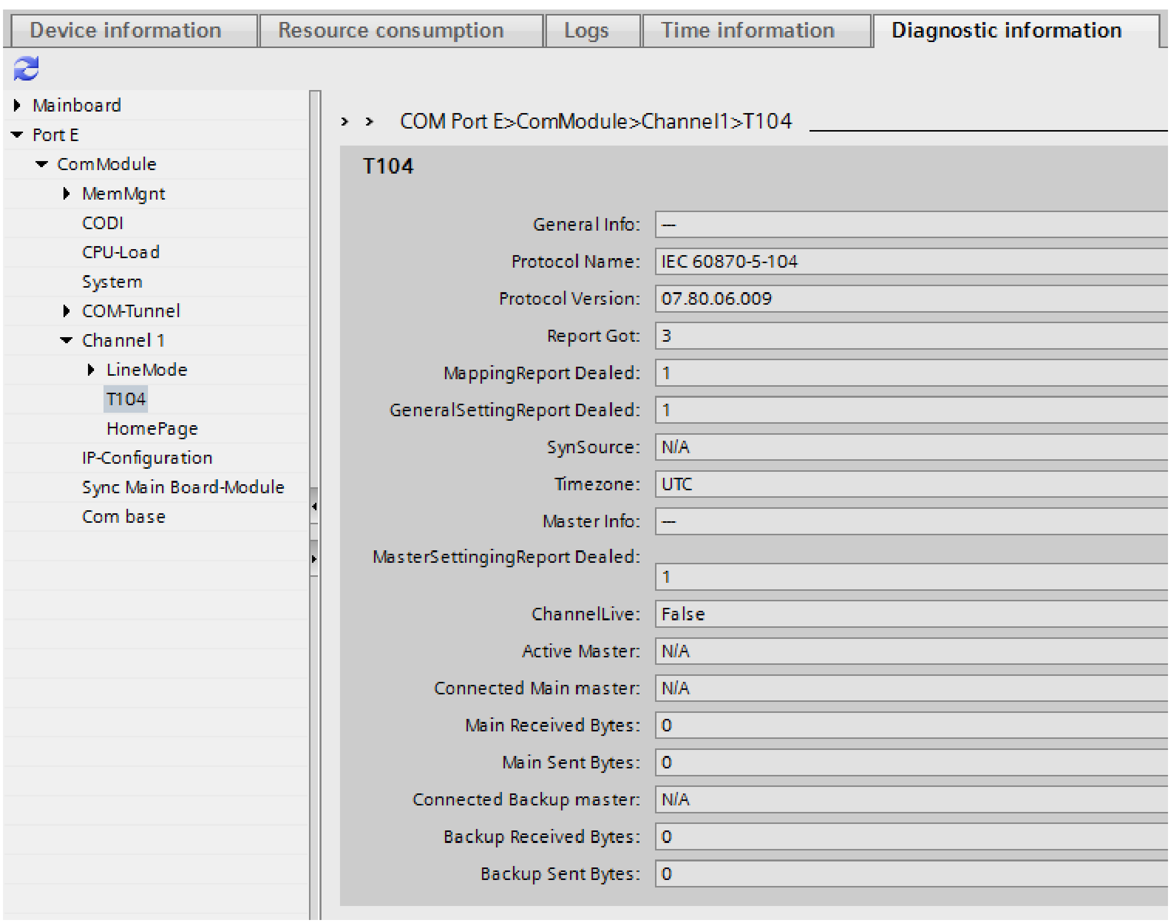
Table 10-4 Displayed Values and Their Description

Name	Values	Description
Protocol Name	String	IEC 60870-5-104
Protocol Version	String	IEC 60870-5-104 version
Report Got	Uint32	ACSI (Abstract Communication Service Interface) report received by mainboard
Mapping Report Dealed	Uint32	ACSI (Abstract Communication Service Interface) mapping report processed
General Setting Report Dealed	Uint32	ACSI (Abstract Communication Service Interface) general setting report processed
SynSource	String	IP address of the synchronization source

Name	Values	Description
Timezone	String	Time zone
MasterSettingReport Dealed	Uint32	ACSI (Abstract Communication Service Interface) master setting report processed
ChannelLive	String	Indicate if each master is transmitting and receiving data on the module
Active Master	String	The Master, which is the last to send STARTDT to the device
Connected Main Master	String	Display the IP of the connected Main Master
Main Received Bytes	Uint32	Bytes received from Main Master This number is updated continuously.
Main Sent Bytes	Uint32	Bytes sent by Main Master This number is updated continuously.
Connected Backup Master	Uint32	Display the IP of the connected Backup Master
Backup Received Bytes	Uint32	Bytes received from Backup Master This number is updated continuously.
Backup Sent Bytes	Uint32	Bytes sent by Backup Master This number is updated continuously.

Diagnostic Data via DIGSI 5

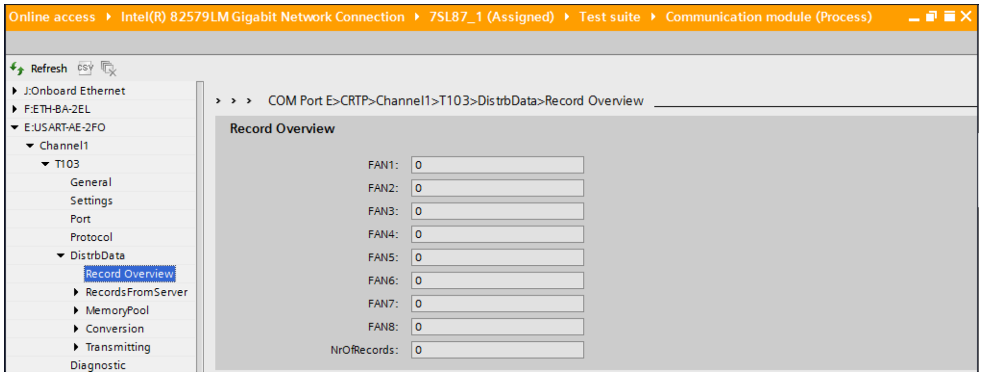
Diagnostic data that can be read out with DIGSI 5.



[Sc_Diagnostic Data DIGSI T104 280814, 2, --_--]

Figure 10-9 Diagnostic Data via DIGSI 5 for the Protocol

You can display the routed fault record channels in a subdirectory.



[sc_103rov, 2, en_US]

Figure 10-10 Diagnostic Data under Record Overview

This and all other displays under **Disturbance Data** contain internal Siemens information.

Diagnostic Data via the Homepage

You can find more information in chapter *9.13.4.6 Communication Protocols – IEC 60870-5-104*.

10.1.8 Diagnostic Information for Modbus

Diagnostic Data at the Device

You can find the diagnostic data in the HMI under **Test & Diagnosis** -> **Siemens internal** -> **Runtime data** -> **Analysis** -> **COM Port E/F/N/P** -> **CRTP** -> **Channel 1/2/3** -> **Modbus**.

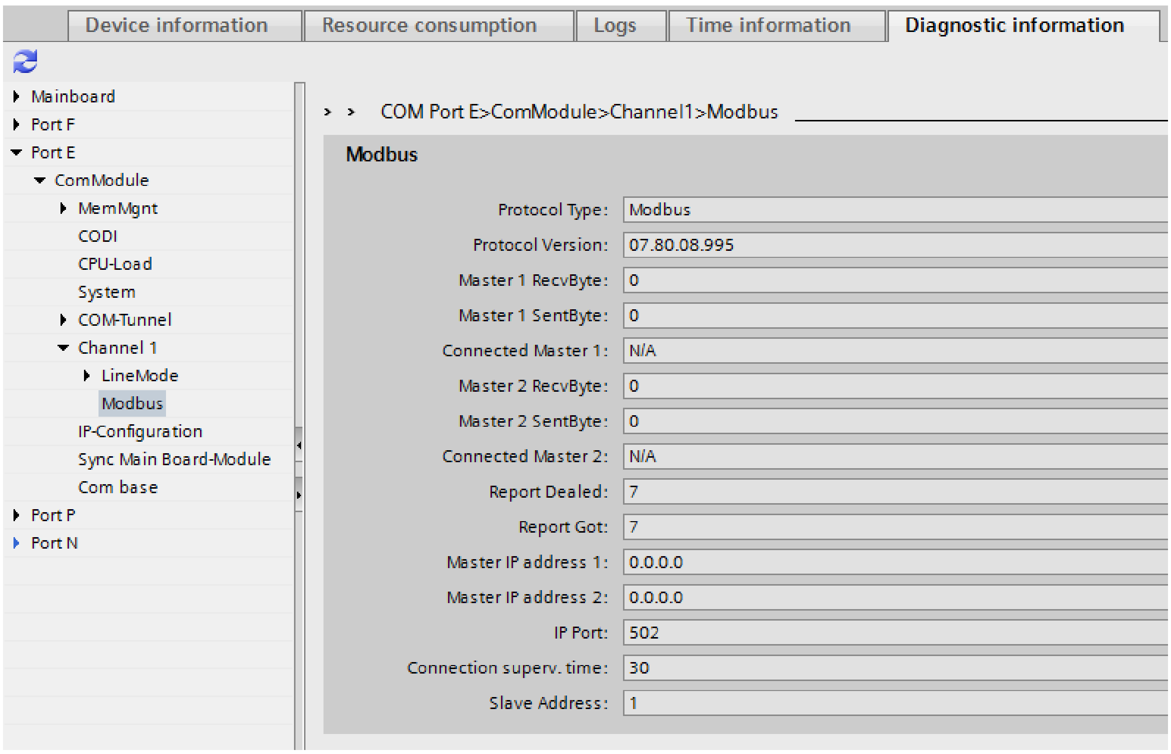
Table 10-5 Displayed Values and Their Description

Name	Values	Description
Connected master 1	String	Display of the IP of Master 1.
Master 1 RecvByte	Int16	Bytes received from Master 1 This number is updated continuously.
Master 1 Sentbyte	Int16	Bytes sent from Master 1 This number is updated continuously.
Connected master 2	String	Display of the IP of Master 2.
Master 2 RecvByte	Int16	Bytes received from Master 2 This number is updated continuously.
Master 2 Sentbyte	Int16	Bytes sent from Master 2 This number is updated continuously.
ReportDealed	Int16	ACSI (Abstract Communication Service Interface) report processed
ReportGot	Int16	ACSI (Abstract Communication Service Interface) report received by mainboard
Protocol Type	String	Modbus
Protocol Version	String	Modbus version
Connection super. time	Int16	TCP/IP Time-out
Slave Address	Int16	Modbus slave address of the device
IP port	Int16	The TCP port that the COM module listens to for Modbus

Name	Values	Description
Master IP address 1	String	Ipv4 address 0.0.0.0 means that the slave hears and contacts each IP address
Master IP address 2	String	Ipv4 address 0.0.0.0 means that the slave hears and contacts each IP address

Diagnostic Data via DIGSI 5

Diagnostic data that can be read out with DIGSI 5.



[sc_DiaDtDIGSI_Modbus, 1, en_US]

Figure 10-11 Diagnostic Data via DIGSI 5 for the Protocol

Diagnostic Data via the Homepage

Enter the IP address of the communication module in Internet Explorer. You can read the diagnostic data via the homepage.

NOTE

The homepage must be activated; otherwise, the diagnostic data are not visible.

You can find more information in chapter *9.13.4.12 Application Diagnostic – Modbus*.

10.1.9 Diagnostic Information for IEC 60870-5-103

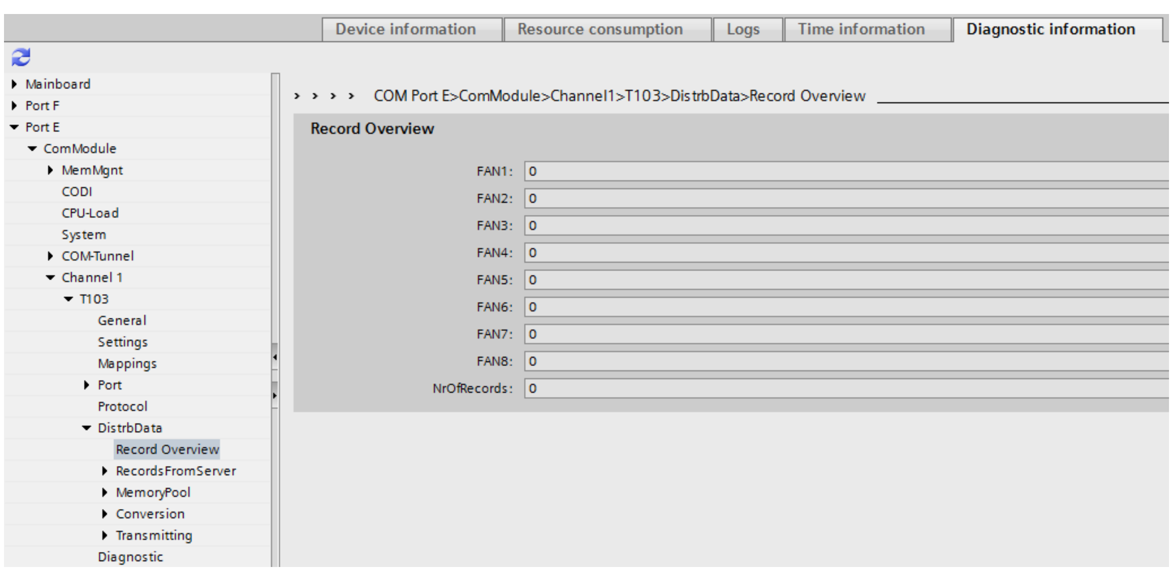
Diagnostic Data at the Device

Table 10-6 Displayed Values and Their Description

Name	Values	Description
Channel name	Text	Internal channel description
Channel type	Text	Protocol configured for the channel
Channel version	Number	Protocol version
Channel location	Number	Channel number
Channel Mode	ON/OFF/TEST	Set mode for the protocol
Channel behavior	ON/OFF/TEST	State display for the protocol (current state)
Connection Status	ON/OFF	Display of the state of the connection to the master
CCF version	Number	Version of the communication mapping used
Parameter status	OK/INVALID	State display for parameterization
Device address	Number	Device address
Baud rate	Number	Set baud rate
Parity	EVEN / ODD / NONE	Set parity
Data bit	7/8	Set data bits
Stop bit	1 or 2	Set stop bits
Send frame	Frame number	Telegrams sent The number of telegrams is updated continuously.
Received frame	Frame number	Telegrams received The number of telegrams is updated continuously.
Error frame	Frame number	Faulty telegrams The number of telegrams is updated continuously.

Diagnostic Data via DIGSI 5

Diagnostic data that can be read out with DIGSI 5.
You can display the routed fault record channels in a subdirectory.



[sc_T103 Record Overview, 1, en_US]

Figure 10-12 Diagnostic Data under Record Overview

This and all other displays under **Disturbance Data** contain internal Siemens information.

10.1.10 Diagnostic Information for PROFINET IO

Diagnostic Data at the Device

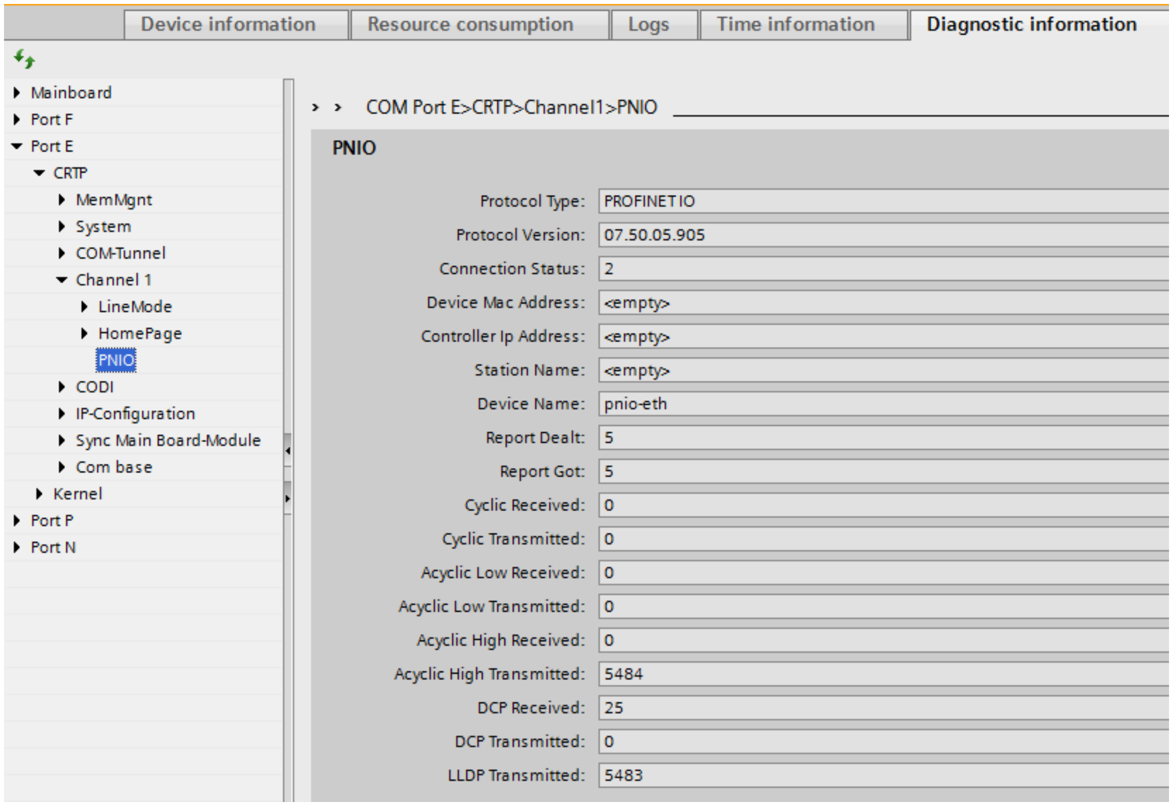
You can find the diagnostic data in the HMI under **Test & Diagnosis** → **Siemens internal** → **Runtime data** → **Analysis** → **COM Port E/F/N/P** → **CRTP** → **Channel 1** → **PNIO**.

Table 10-7 Displayed Values and Their Description

Name	Values	Description
Protocol Type	String	PROFINET IO
Protocol Version	String	PROFINET IO version
Connection Status	Int16	The connection status of IO device to IO controller
Device Mac Address	String	MAC address of the Ethernet module
Controller IP Address	String	IP address of the IO controller
Station Name	String	Name of station
Device Name	String	Name of IO device
Report Dealt	Int32	ACSI (Abstract Communication Service Interface) report processed
Report Got	Int32	ACSI report received
Cyclic Received	Int32	Cyclic data received from IO controller
Cyclic Transmitted	Int32	Cyclic data transmitted to IO controller
Acyclic Low Received	Int32	Acyclic low priority telegrams received
Acyclic Low Transmitted	Int32	Acyclic low priority telegrams transmitted
Acyclic High Received	Int32	Acyclic high priority telegrams received
Acyclic High Transmitted	Int32	Acyclic high priority telegrams transmitted
DCP Received	Int32	DCP frames received
DCP Transmitted	Int32	DCP frames transmitted
LLDP Transmitted	Int32	LLDP frames transmitted

Diagnostic Data via DIGSI 5

Diagnostic data that can be read out with DIGSI 5.



[sc_diag_data_digsi, 2, en_US]

Figure 10-13 Diagnostic Data via DIGSI 5 for the Protocol

NOTE

In case of high load on the communication module caused by changes of many processes, the performance can slow down.

I&M – Identification and Maintenance

The PROFINET IO implementation in the SIPROTEC 5 device supports reading of I&M0 data plus reading and writing of I&M1, I&M2, I&M3, and I&M4 data. The SIPROTEC 5 device only supports the I&M writing via Slot0\Subslot1.

Table 10-8 Content of I&M0 Data

Name	Content
Vendor ID	0x002A (PROFINET vendor ID of Siemens AG)
Order ID	Identification of the device or module
Serial Number	Serial number of the Ethernet module
Hardware Revision	Hardware revision of the Ethernet module
Software Revision	Software revision of the Ethernet module
Revision Counter	Indication of the changes of hardware or of its parameters
Profile ID	Profile of the item if applicable
Profile Specific Type	Information about profile-specific details according to the respective definitions of the application profile.

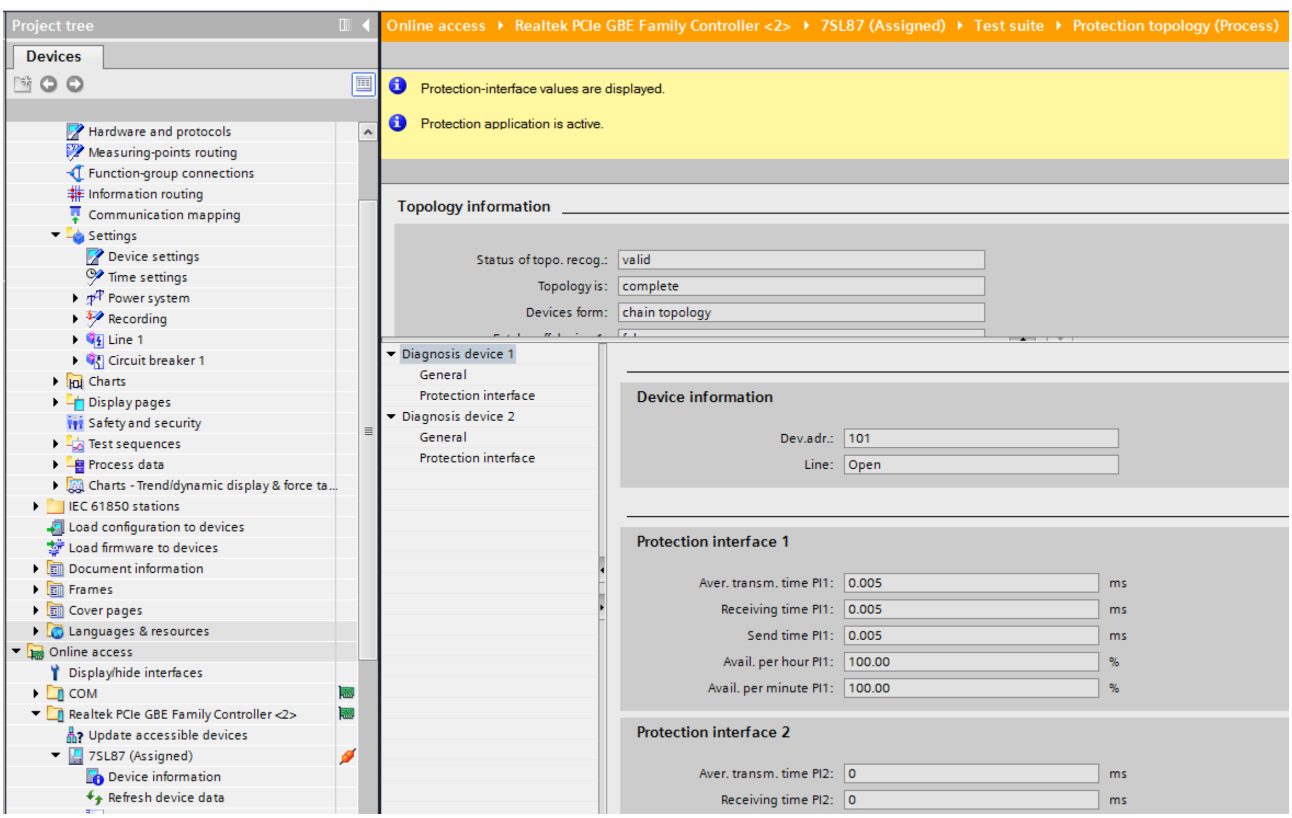
Name	Content
I&M Version Major	Major version of the profile Guidelines Part 1 **I&M Functions**, you can find more information on the following Internet page: *https://www.profibus.com/nc/download/profiles/*
I&M Version Minor	Minor version of the profile Guidelines Part 1 **I&M Functions**, you can find more information on the following Internet page: *https://www.profibus.com/nc/download/profiles/*
I&M Supported	Bitmask defining which I&M objects (I&M 1-15) are supported

10.1.11 Diagnostic Measured Values of the Protection Interface

The following diagnostic data is provided via the protection interfaces by the devices in the constellation:

- Address of the device in the constellation
- Circuit-breaker switch position (open/closed/undefined) (only for protection interfaces of type 1)
- Availability of protection-interface communication within the last minute, as percentage
  Availability of protection-interface communication within the last hour, as percentage
- Time delay in the send and receive direction of the telegrams between local and neighboring device

You can find this diagnostic data in DIGSI under the following menu structure (see *Figure 10-14*):



[sc_diagnose_wskanäle_geräteadresse, 2, en_US]

Figure 10-14 Protection-Interface Channel Diagnostic Data – Device Address

NOTE

You can use the following procedure to reset the measured values for the protection interface directly in the device:

Device functions > x Device protection comm. > Protection interface y > Reset measured values.

Output Signals of the Protection Interface

Each individual protection interface provides the following indications for commissioning and diagnosing communication:

Indication	Description
(_:5161:301) Status of lay. 1 and 2	The output signal gives you information about the state of communication layers 1 and 2 (1: Physical Layer, 2: Data Link Layer). The following indications values are possible: • *initialized*: The protection interface is not connected and is in the Initial state. • *PI connected*: The protection interface is connected to the protection interface of a device. • *PI data fault*: The protection interface has not received any valid telegrams for the time set in parameter **(_:5161:107) Disturbance alarm after**. • *PI data failure*: The protection interface has not received any valid telegrams for the time set in parameter **(_:5161:108) Transm. fail. alarm after**. • *not existing*: The protection interface has not been assigned to a communication channel.
(_:5161:302) Status of lay. 3 and 4	The output signal gives you information about the state of communication layers 3 and 4 (3: Network Layer, 4: Transport Layer). The following indications values are possible: • *no error*: The protection interface is operating correctly. • *SW ver.incomp.*: The firmware versions of the connected devices are incompatible. Update the firmware. • *wrong dev. ID*: The device address of the partner device is incorrect. Check the settings for parameters **Address of device 1** to **address of device n** (_:5131:102 and following). • *const.sett.error*: Check that the same setting has been made for parameter **(_:5131:122) Lowest appearing bit rate** in all devices. • *diff.sett error*: The line differential protection settings for the connected devices are incompatible. Check whether both devices are set to operate with or without line differential protection. The rated current of the line (parameter **(_:9001:101) Rated current**) must be set equal at all ends of the line. If a transformer is installed in the line, the rated apparent power **(_:9001:103) Rated apparent power** must be set equal at all ends of the line. • *net mirroring* The protection interface is receiving its own data. Check the wiring. • *wrong dev. idx.* The device index in the partner device is wrong. Check the setting of parameter **(_:5131:101) Local device is device** in the partner device.

In order to clarify faults, each individual protection interface provides the following binary signals:

Binary Output Signal	Description
(_:5161:303) Connection broken	Signal *Connection broken* indicates that during a parameterized time (parameter **(_:5161:107) Disturbance alarm after**) faulty or missing telegrams were continuously received. If the 'Connection interrupted' indication occurs, the affected protection interface link will be terminated. This can cause the blocking of an active differential protection or a ring topology can change to a chain topology.
(_:5161:316) Error rate / min exc.	Signal *Error rate / min exc.* indicates that the set maximum error rate per minute (parameter **(_:5161:106) Max. error rate per min**) has been exceeded.
(_:5161:317) Error rate / hour exc.	Signal *Error rate / hour exc.* indicates that the set maximum error rate per hour (parameter **(_:5161:105) Max. error rate per hour**) has been exceeded.
(_:5161:318) Time delay exceeded	Signal *Time delay exceeded* indicates that the threshold value for the set signal-transit time (parameter **(_:5161:109) Delay time threshold**) has been exceeded.
(_:5161:319) Time delay different	Signal *Time delay different* indicates that the threshold value for asymmetrical transit times has been exceeded. The setting value results from the setting value of the parameter **(_:5161:110) Difference Tx and Rx time**.
(_:5161:320) Time delay jump	Signal *Time delay jump* indicates that the data transit times changed abruptly. This is caused by switching the communication path in the communication network.
(_:5161:321) PI synchronized	Signal *PI synchronized* indicates that the protection-interface connection is synchronized with the opposite end.
(_:5161:340) Telegram lost	Signal *Telegram lost* indicates that an expected telegram has failed to arrive or a faulty telegram has been received. If you would like to allocate the communications failures or faults to other events, move the signal *Telegram lost* temporarily into the operational log. Such events can be switching operations in the primary system or operations on the components of the communication network. **Note:** If the signal is constantly routed, the operational log can overflow. Siemens recommends routing the signal only for clarification of faults.

Measured Values of the Protection Interface

The protection interface provides the following measured value to diagnose the protection interface communication:

Measured Value	Description
(_:5161:308) Tx tel/h	Telegrams sent during the last hour
(_:5161:309) Rx tel/h	Telegrams received during the last hour
(_:5161:310) Tx tel/min	Telegrams sent during the last minute
(_:5161:311) Rx tel/min	Telegrams received during the last minute
(_:5161:312) Tx err/h	Transmission failure rate during the last hour
(_:5161:313) Rx err/h	Receive error rate during the last hour
(_:5161:314) Tx err/min	Transmission failure rate during the last minute

Measured Value	Description
(_:5161:315) Rx err/min	Receive error rate during the last minute
(_:5161:325) Aver.Δt	Mean signal-transit time (average value of the transit time in transmission and reception direction divided by 2, without GPS synchronization)
(_:5161:326) Rec. Δt	Signal-transit time in reception direction (with GPS synchronization)
(_:5161:327) Sen. Δt	Signal-transit time in transmission direction (with GPS synchronization)
(_:5161:334) Miss.tel/min	Number of telegram failures within the last minute
(_:5161:335) Miss.tel/h	Number of telegram failures within the last hour
(_:5161:336) Miss.tel/d	Number of telegram failures within the last day
(_:5161:337) Miss.tel/w	Number of telegram failures within the last week
(_:5161:338) M. loss/d	Longest lasting telegram failure within the last day
(_:5161:339) M. loss/w	Longest lasting telegram failures within the last week

NOTE

You can reset the measured values of the protection interface directly in the device. Proceed as follows: **Device functions > x Device protection comm. > Protection interface y > Reset measured values**.

10.1.12 Diagnostic Data for the Protection Interface

Diagnostic Data of the Channel in DIGSI 5

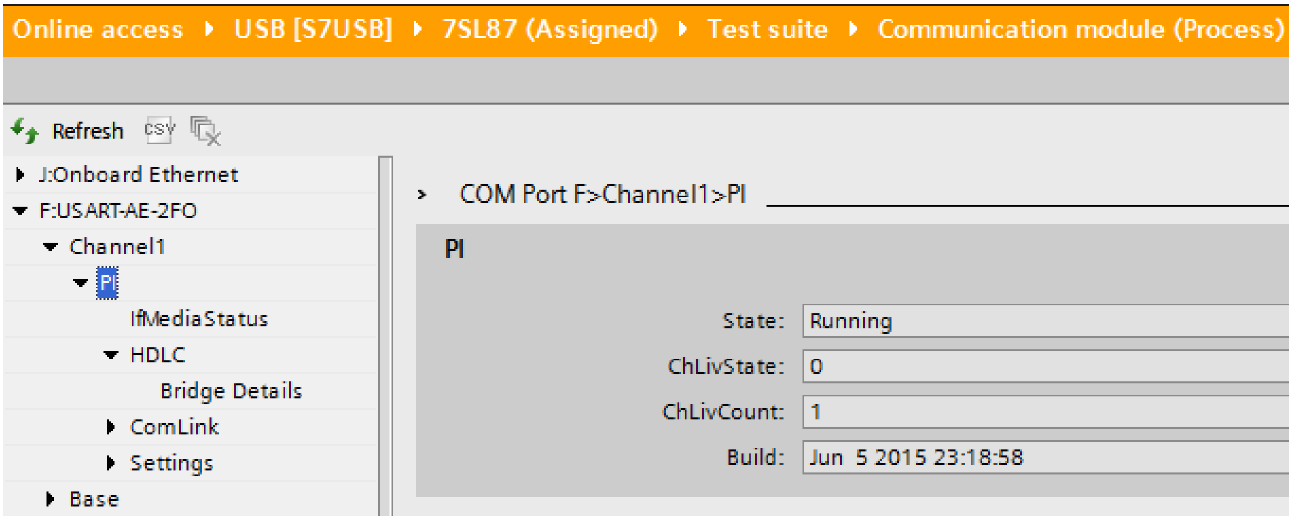
Different diagnostic data can be read with DIGSI 5.

For this, connect with the device via DIGSI 5 and query the device information. Diagnostic data for a module whose channel is configured with the protection interface can be received by selecting the module slots (for example, F) and the corresponding channel (1 or 2). The following figures show the extensive diagnostic data for the protection interface. It is particularly helpful if data failures occur or other irregularities in a communication connection (for example, transmission time fluctuations).

NOTE

The diagnostic data can also be read via the device control on the display of the device. The overview of DIGSI 5 does not offer this option, however.

The following table describes the displays.



[scdiapin-140912-01, 1, en_US]

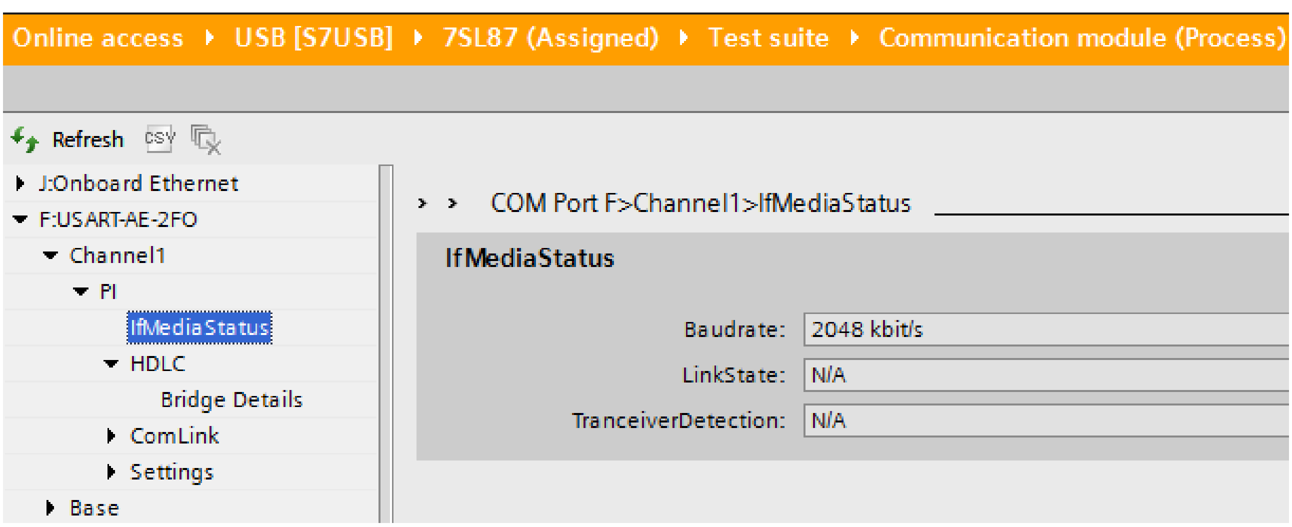
Figure 10-15 Diagnostic Data of a Channel Configured with the Protection Interface

Table 10-9 Description of the Diagnostic Data under Protection Interface

Channel Type	Name	Values	Description - Diagnostic Information for Log PI
Protection interfaces - log	Status	Initial, Running, Error	Runtime status of the log
Protection interfaces - log	Build	Date/time	Date and time of the log version

Diagnostic Data of the Protection-Interface Log in DIGSI 5

The following figures and tables describe the displays of the protection-interface log.

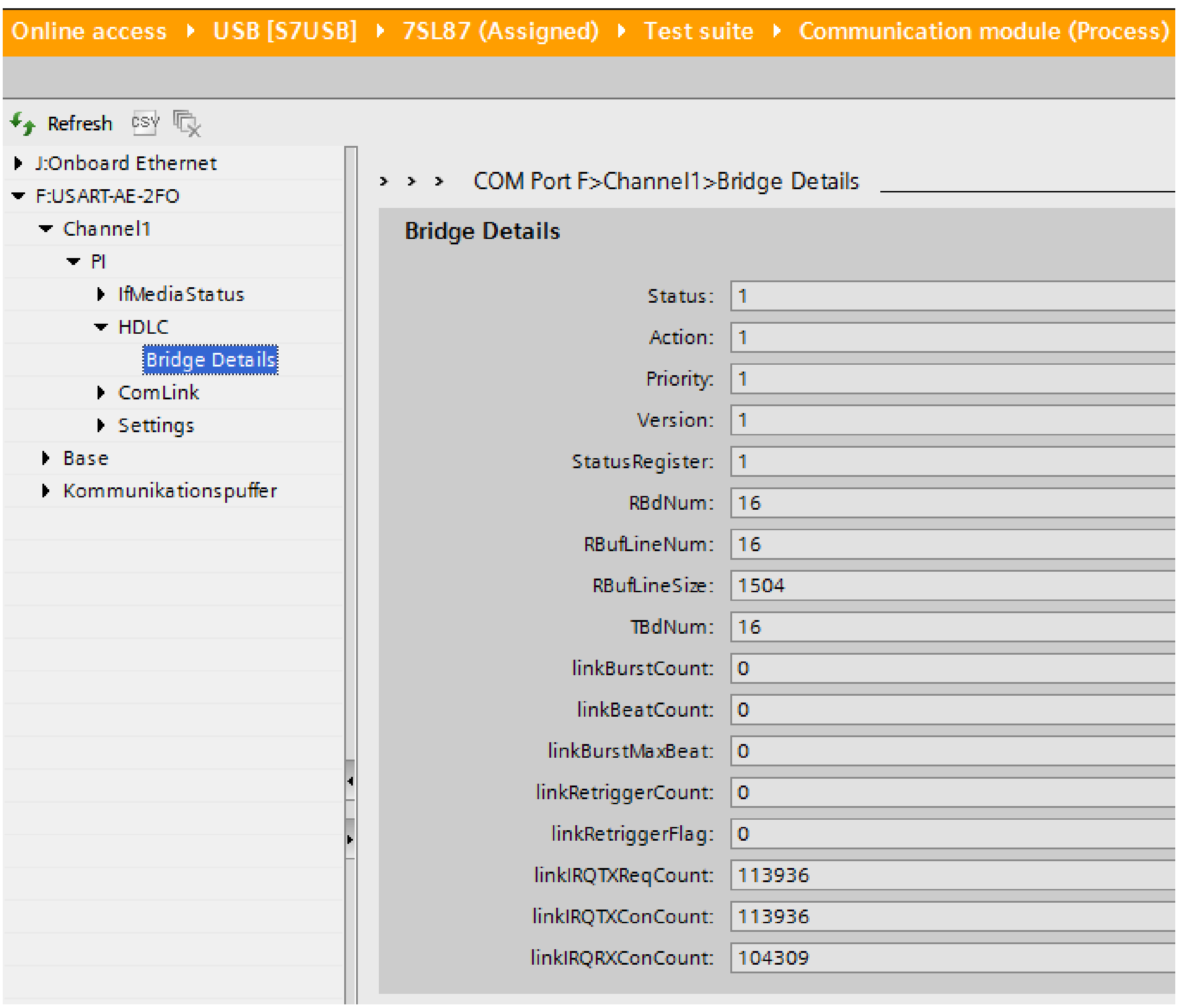


[scdiamed-140912-01, 1, en_US]

Figure 10-16 Diagnostic Data of the Protection-Interface Log - Media Status

Table 10-10 Description of Diagnostic Data under Media Status

Protection Interfaces - Log Type	Name	Values	Description - Media Status Interface (in Direction of Outside Interface)
Media Status	Baudrate	64 kbit/s; 128 kbit/s; 512 kbit/s; 2048 kbit/s; 30 Mbit/s; <unknown>	HDLC baud rate: FO: 64 kbit/s to 2048 kbit/s for 820-Nm USART modules LDFO: 30 Mbit/s for 1300-Nm/1500-Nm long-distance modules Error case: <unknown>
Media Status	LinkState	N/A, UP, DOWN	FO: N/A (always display N/A)
Media Status	TransceiverDetection	N/A, NO Transceiver detected, Transceiver detected	FO: N/A (always N/A) (NO Transceiver detected, Transceiver detected), Error case: N/A

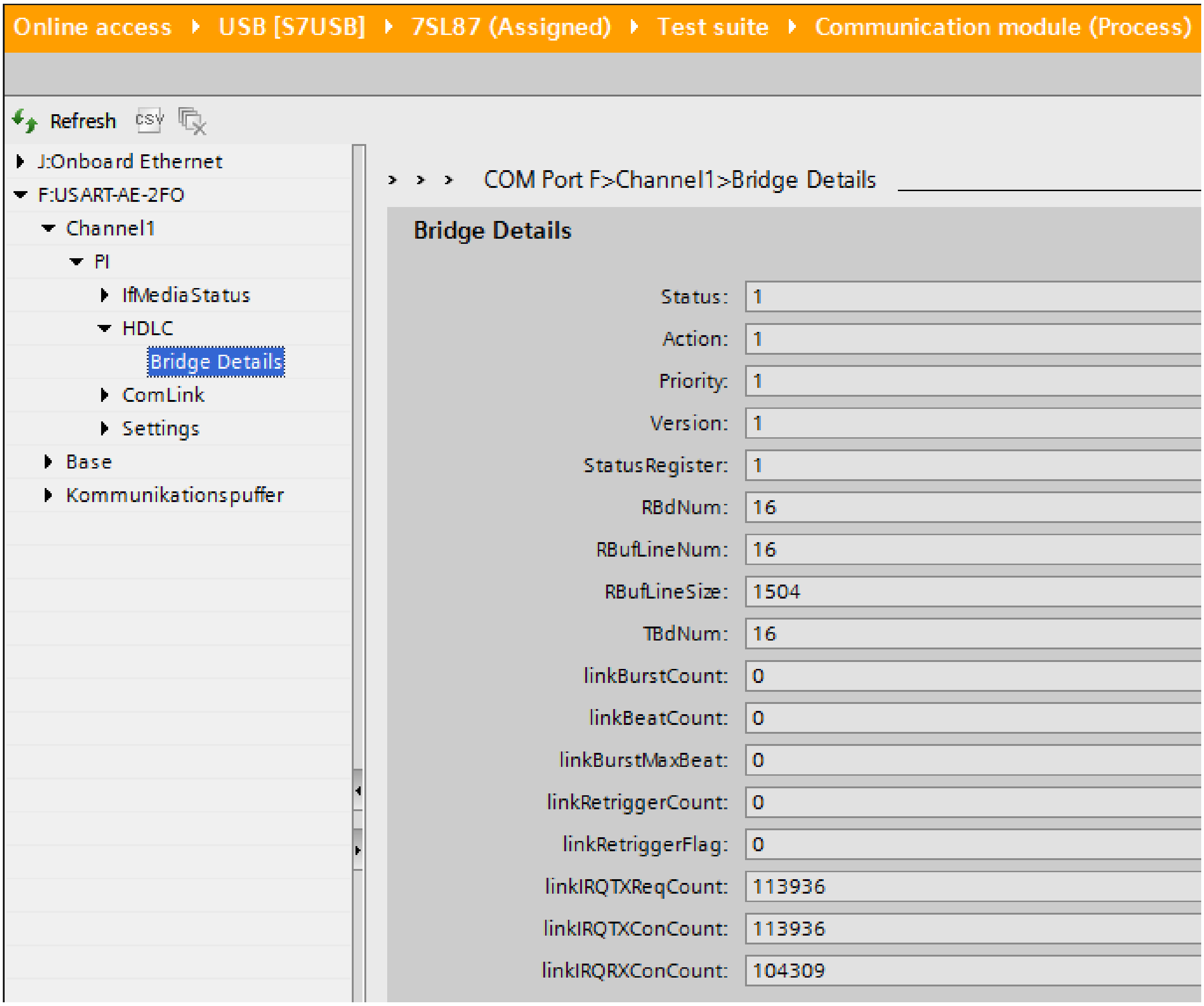


[scdiacom-140912-01, 1, en_US]

Figure 10-17 Diagnostic Data of the Protection-Interface Log - HDLC (Log - Layer)

Table 10-11 Description of Diagnostic Data of the Protection-Interface Log - HDLC (Log - Layer)

Protection Interfaces - Log Type	Name	Values	Description - HDLC Link Layer Diagnostic Information (in Direction of Outside Interface)
HDLC	RXHPFramesOK	Number of corresponding frames (16 bit counter)	Incoming telegrams, high priority, OK
HDLC	RXLPFramesOK	Number of corresponding frames (16 bit counter)	Incoming telegrams, low priority, OK
HDLC	RXHPFramesERR	Number of corresponding frames (16 bit counter)	Incoming telegrams, high priority, faulty
HDLC	RXLPFramesERR	Number of corresponding frames (16 bit counter)	Incoming telegrams, low priority, faulty
HDLC	TXHPFramesOK	Number of corresponding frames (16 bit counter)	Sending telegrams, high priority, OK
HDLC	TXLPFramesOK	Number of corresponding frames (16 bit counter)	Sending telegrams, low priority, OK
HDLC	TXHPFramesERR	Number of corresponding frames (16 bit counter)	Sending telegrams, high priority, faulty
HDLC	TXLPFramesERR	Number of corresponding frames (16 bit counter)	Sending telegrams, low priority, faulty
HDLC	Bridge Details Sub-nodes	Sub-nodes	Siemens-internal special diagnostic for fault search



[scdiahdl-140912-01, 1, en_US]

Figure 10-18 Diagnostic Data of the Protection-Interface Log - COM Interface (Internal COM Link Interface Between Module and Mainboard)

Table 10-12 Description of Diagnostic Data of the COM Interface (Internal COM Link Interface Between Module and Mainboard)

Protection Interfaces - Log Type	**Name**	**Values**	**Description - COM Interface Layer Diagnostic Information (Internal COM Link Interface in Mainboard Direction)**
COM interface	RXHPFramesOK	Number of corresponding frames (16 bit counter)	Incoming telegrams, high priority, OK
COM interface	RXLPFramesOK	Number of corresponding frames (16 bit counter)	Incoming telegrams, low priority, OK
COM interface	RXHPFramesERR	Number of corresponding frames (16 bit counter)	Incoming telegrams, high priority, faulty
COM interface	RXLPFramesERR	Number of corresponding frames (16 bit counter)	Incoming telegrams, low priority, faulty

Protection Interfaces - Log Type	Name	Values	Description - COM Interface Layer Diagnostic Information (Internal COM Link Interface in Mainboard Direction)
COM interface	TXHPFramesOK	Number of corresponding frames (16 bit counter)	Sending telegrams, high priority, OK
COM interface	TXLPFramesOK	Number of corresponding frames (16 bit counter)	Sending telegrams, low priority, OK
COM interface	TXHPFramesERR	Number of corresponding frames (16 bit counter)	Sending telegrams, high priority, faulty
COM interface	TXLPFramesERR	Number of corresponding frames (16 bit counter)	Sending telegrams, low priority, faulty
COM interface	Bridge Details Sub-nodes	Sub-nodes	Siemens-internal special diagnostic for fault search

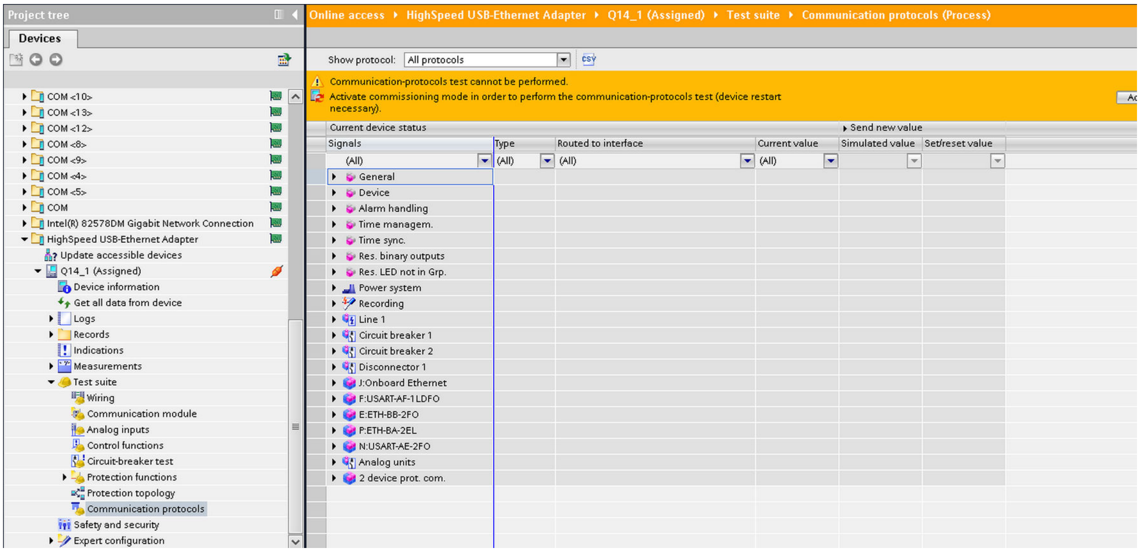
Table 10-13 Description of Diagnostic Data of some Setting Values of the Protection Interface

Protection Interfaces - Log Type	Name	Values	Description - Protection Interface Setting Values
Settings	`Connection via`	Integer number - display of the internal coding of the settings variant	Protection interface is `Connection via`
Settings	`PDI bandwidth`	Bit-rate display	Bit rate (bit/s) for protection telegrams depending on the parameter `Connection via`
Settings	`PDI Telegram.Overhead`	Display of bits	Overhead for every protection telegram in bit.

10.1.13 Test Editor

For the protocol test, DIGSI 5 is used to set and reset specific values for objects that are routed through communication interfaces. The object will always be transmitted using a test bit. If the objects are to be designed with receivers, then the receivers must also be placed into the test state. A Test Editor is provided in DIGSI 5 for this purpose.

You can set objects for IEC 61850. If this object is configured in a dataset that is to be transmitted as a GOOSE message or report, then the object can be received spontaneously by a client or other server. In this way, you can change states and test their response via the IEC 61850 communication.



[sctested-280113-01.tif, 1, en_US]

Figure 10-19 DIGSI 5 Communication Protocol Test Editor

The time stamp of the change is transmitted.

10.1.14 IEC 61850

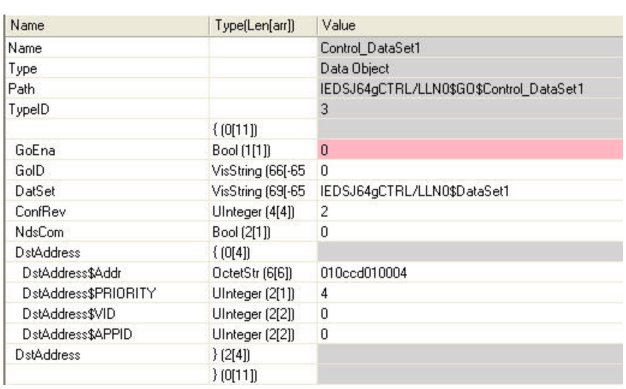
10.1.14.1 Switching off GOOSE Messages

Using an IEC 61850 client, you can switch off GOOSE messages in a device.

Controlling GOOSE Messages

A GOOSE message is controlled by a GOOSE control block. It is located in the LLN0 of the logical device in which the GOOSE message was created. All relevant data for the GOOSE message can be found there.

The variable **GoEna** is needed to switch off GOOSE messages. The variable **GoEna** controls the transmission of the GOOSE message. If a client sets this variable from 1 to 0, the device stops the transmission of this GOOSE message and the objects it contains. You can now check the receivers of GOOSE messages to see whether an interruption of data reception is detected reliably. An object that is not received is set to the value **Invalid** or its state can be updated manually at the receiver.



Name	Type(Len[arr])	Value
Name		Control_DataSet1
Type		Data Object
Path		IEDSJ64gCTRL/LLN0GOControl_DataSet1
TypeID		3
	{ (0[11])	
GoEna	Bool (1[1])	0
GoID	VisString (66[-65	0
DatSet	VisString (69[-65	IEDSJ64gCTRL/LLN0$DataSet1
ConfRev	UInteger (4[4])	2
NdsCom	Bool (2[1])	0
DstAddress	{ (0[4])	
DstAddress$Addr	OctetStr (6[6])	010ccd010004
DstAddress$PRIORITY	UInteger (2[1])	4
DstAddress$VID	UInteger (2[2])	0
DstAddress$APPID	UInteger (2[2])	0
DstAddress	} (2[4])	
	} (0[11])	

[scgoenab-081210-01.tif, 1, en_US]

Figure 10-20 Variable GoEna with Value 0

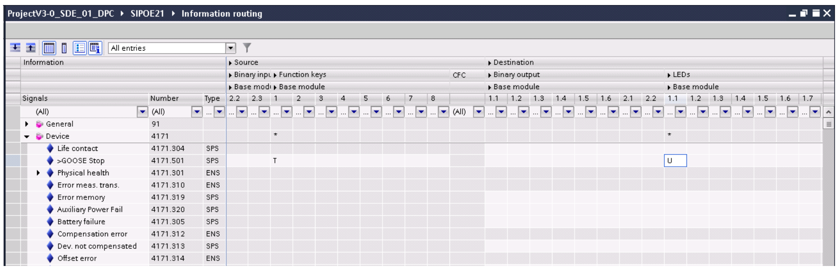
If a device transmits several GOOSE messages, then you must set all **GoEna** variables to 0 to switch off the GOOSE messages completely.

The GOOSE messages are switched on by setting the value of the variable **GoEna** to 1.

For testing purposes, you can use the IEC 61850 Browser, as it displays and can set GOOSE control blocks and variables.

Switching off GOOSE Messages in Information Routing

You can switch off GOOSE messages in the information routing by routing the **>GOOSE Stop** signal to a binary input or function key. You cannot route this signal to a binary input and a function key simultaneously.



[scgostop-110113-01.tif, 1, en_US]

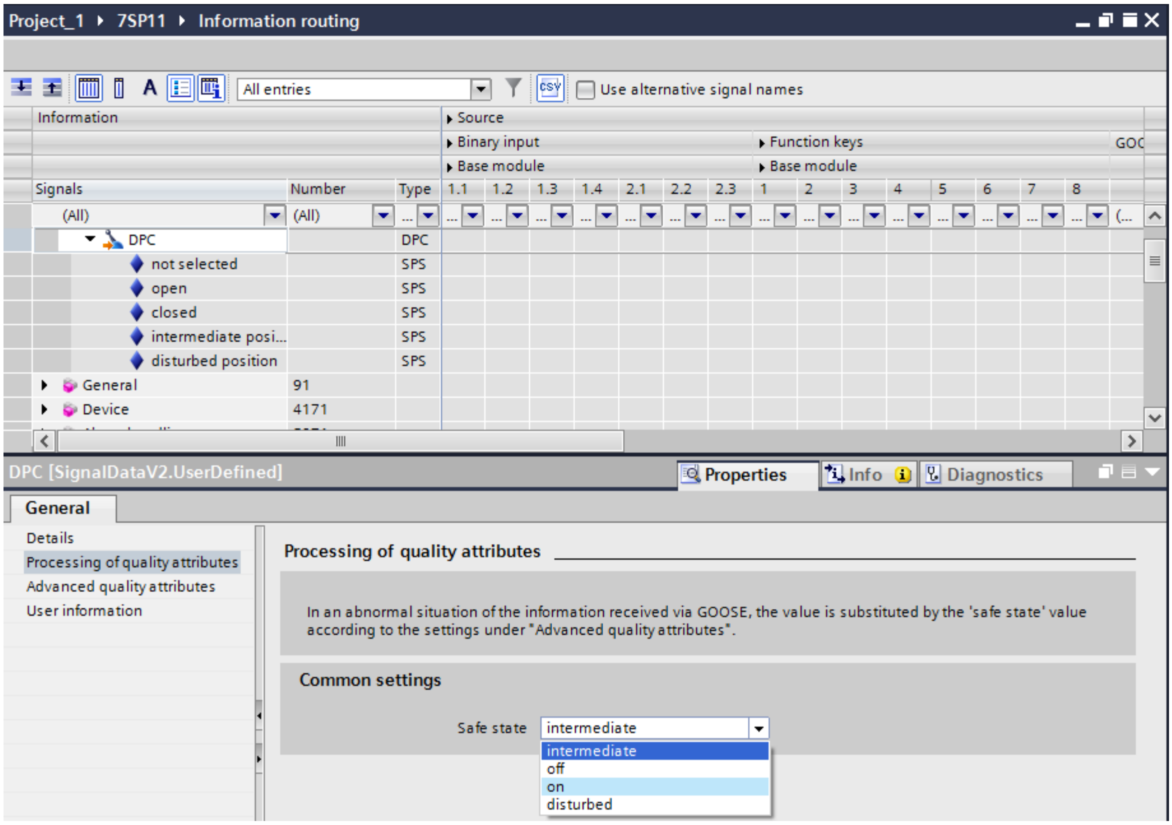
Figure 10-21 Routing the >GOOSE Stop Signal

10.1.14.2 Quality Processing/Affected by the User for Received GOOSE Values

The properties of quality processing have changed with the introduction of GOOSE Later Binding. You can find information about the former quality processing in chapter *Previous Quality Processing/Affected by the User for Received GOOSE Values, Page 343*.

In the **Information Routing** Editor, you can influence the data value and quality of all data types. The following figure shows the possible influence using the example of a DPC data type. All setting options are effective for the device receiving the data.

- In the DIGSI 5 project tree, double-click **Information Routing**.
- Select either the desired signal in the **External Signals** group or the signal of a function activated via the GOOSE column.
- Open the **Properties** window and select the **Processing Quality Attributes** sheet.



[sc_LB_GOOSE_2, 2, en_US]

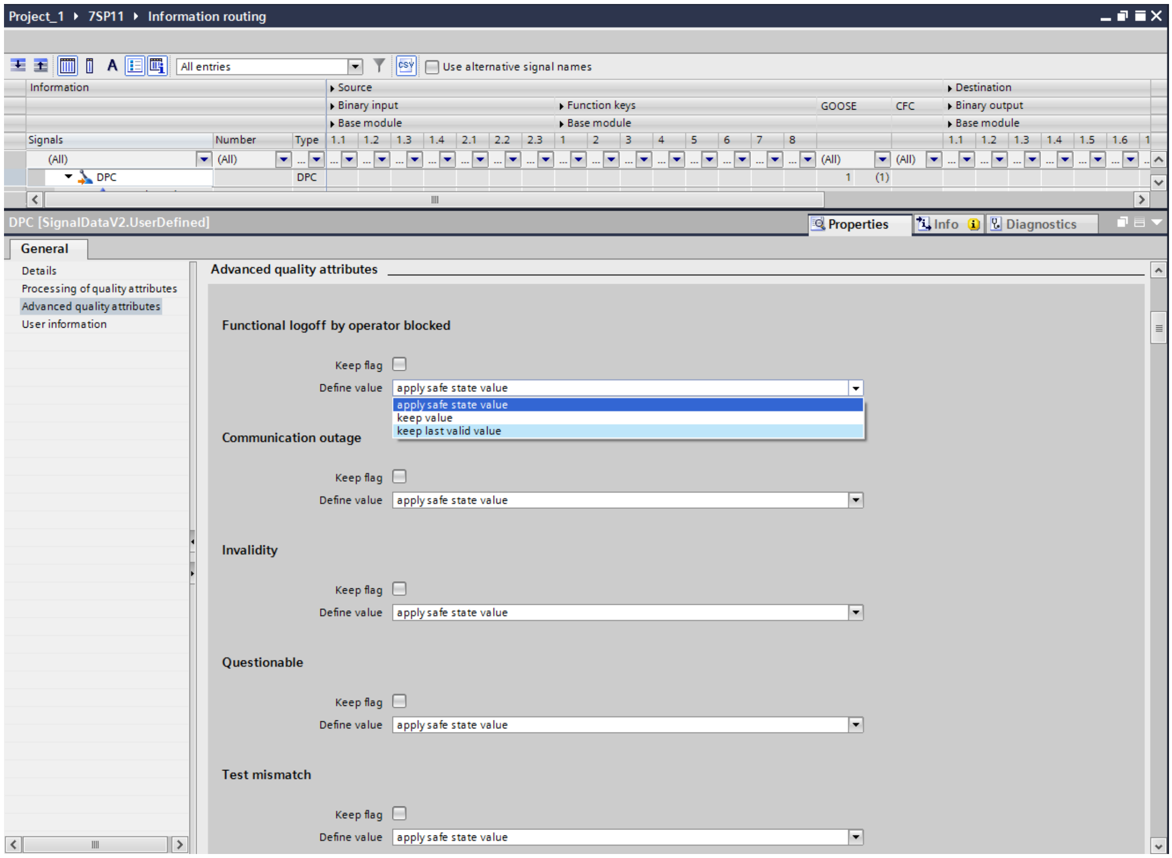
Figure 10-22 Influence Option When Linking a DPC Type Data Object

Depending on the selected data type of the object, various selection options are offered to you for the `Safe state` item in the **Common settings** section. At this point, you select the manually updated values that allow a safe operating state as soon as the data access via the communication path is disturbed.

- Select the property for the selected data object.

You can also set the **Advanced quality attributes** of the data object for GOOSE Later Binding.
The following figure shows the advanced quality attributes using the example of a DPC data type.

- Open the **Properties** window and select the **Advanced quality attributes** sheet.



[sc_LB_GOOSE_1, 2, en_US]

Figure 10-23 Advanced Quality Attributes for GOOSE Later Binding

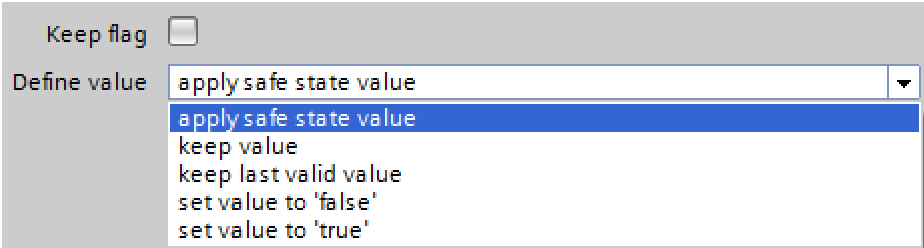
With the following advanced quality attributes, you can filter the transmitted GOOSE indications and check and set their quality. The values that have been adapted, if necessary, are forwarded to the receiver.

For the tests, you can select from the following setting options depending on the data type.

Table 10-14 Value Definitions

Setting Value	Description
Apply safe state value	The value configured in the **Safe state** is forwarded as valid to the application as soon as communication disturbance occurs.
Keep value	The disturbed quality attribute is overwritten with *good* and the received value is forwarded as valid to the application. If no value was received, the output value is assumed being in safe state.
Keep last valid value	If an invalid quality attribute is received, the last valid value is forwarded to the application. If no value has yet been received, the output value is assumed being in safe state.
Set value to "false"	Applies only to Boolean communication objects. Every invalid quality attribute causes the valid value *false* to be forwarded to the application.
Set value to "true"	Applies only to Boolean communication objects. Every invalid quality attribute causes the valid value *true* to be forwarded to the application.

These settings of the **Advanced quality attributes** apply to the advanced quality attributes listed below. The selection can vary depending on the data type.



[sc_LB_GOOSE_3, 2, en_US]

Figure 10-24 Value Definition of a Data Object of the SPS Type

You can also forward the quality attributes unchanged. To do this, you must mark the **Keep flag** check box.

Functional Logoff by Operator Blocked

You have set the *Operation mode* to *Device logoff* = *true* in the transmitting device. As a result, every indication issued from the functions and subject to *Device logoff* is transmitted with the quality information *operator blocked* and **Validity** = *good*. The receiver recognizes this for this indication and reacts according to the settings (*Table 10-14*). A different quality processing can take place only once you have set the *Operation mode* to *Device logoff* = *false* in the transmitting device.

Communication Outage

There is communication disturbance (time allowed to live) between the transmitter and the receiver indicated by the transmitter. The indication is set in accordance with the settings (*Table 10-14*).

Invalidity

The transmitting device sends this indication with the quality information **Validity** = *invalid*. The receiver recognizes this for this indication and reacts according to the settings (*Table 10-14*).

Questionable

The transmitting device sends this indication with the quality information **Validity** = *questionable*. The receiver recognizes this for this indication and reacts according to the settings (*Table 10-14*).

Test Mismatch

The transmitting device or the function in the transmitting device that issues this indication is in test mode. As a result, the indication is transmitted with the quality information *test*. The receiving function block recognizes this for this indication and reacts, depending on its own test-mode state (specified in IEC 61850-7-4 Annex A), according to the settings (*Table 10-14*).

NOTE

Follow the sequence of tests. First, the **Functional logoff by operator blocked** is tested. Then comes **Communication outage** and so on. If a case is recognized as *active*, the test chain is canceled with the configured setting for the active case.

In the case of **Invalidity**, the tests are first performed for **Functional logoff by operator blocked** (not applicable) and then for **Communication outage** (not applicable) and canceled with the configured action for **Invalidity**.

If an indication is routed into the log, manual updating of a value is also logged based on the conditions listed above and on the reason for the manual update. Manually updating a value based on the conditions listed above causes a change in the *Health Warning* function block, inherited up to *Device health* (specified in IEC 61850-7-4).

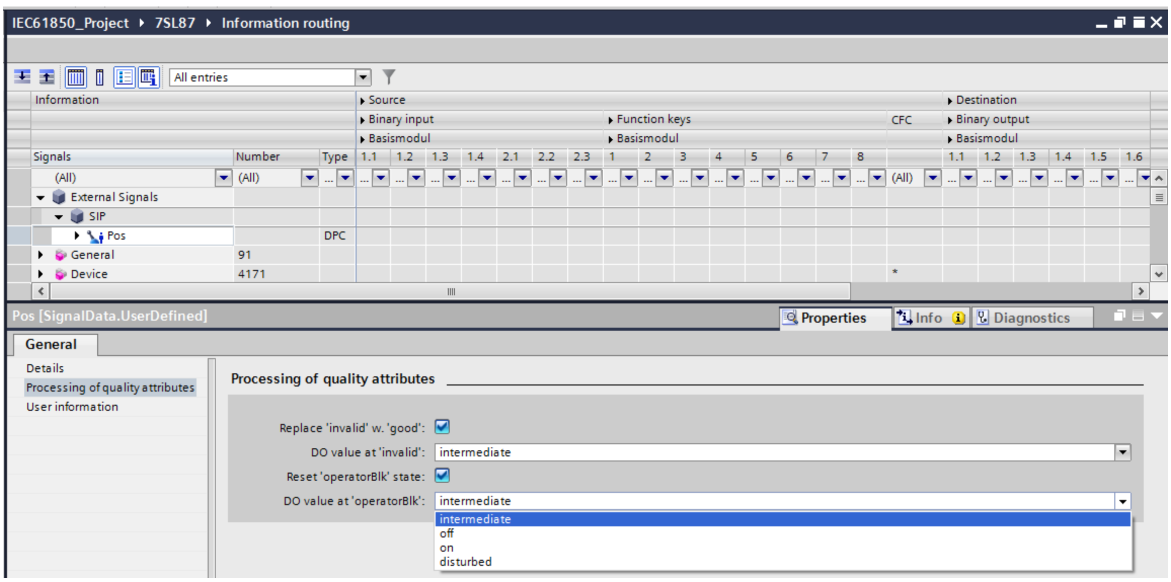
Keep Flag

The quality attributes and values indicated by the transmitter are accepted without change. Quality processing must be performed by the user via a logic diagram. The outputs of the logic diagram following the user-specific quality processing can be connected to the function-block inputs as before.

Previous Quality Processing/Affected by the User for Received GOOSE Values

In the **Information Routing** editor, you can influence the data value and quality of all data types. The following figure shows the possible influence using the example of a DPC data type.

- In the DIGSI 5 project tree, double-click **Information Routing**.
- Select the desired signal in the **External Signals** group.
- Open the **Properties** window and select the **Processing Quality Attributes** sheet.



[sc_GOOSE values, 1, en_US]

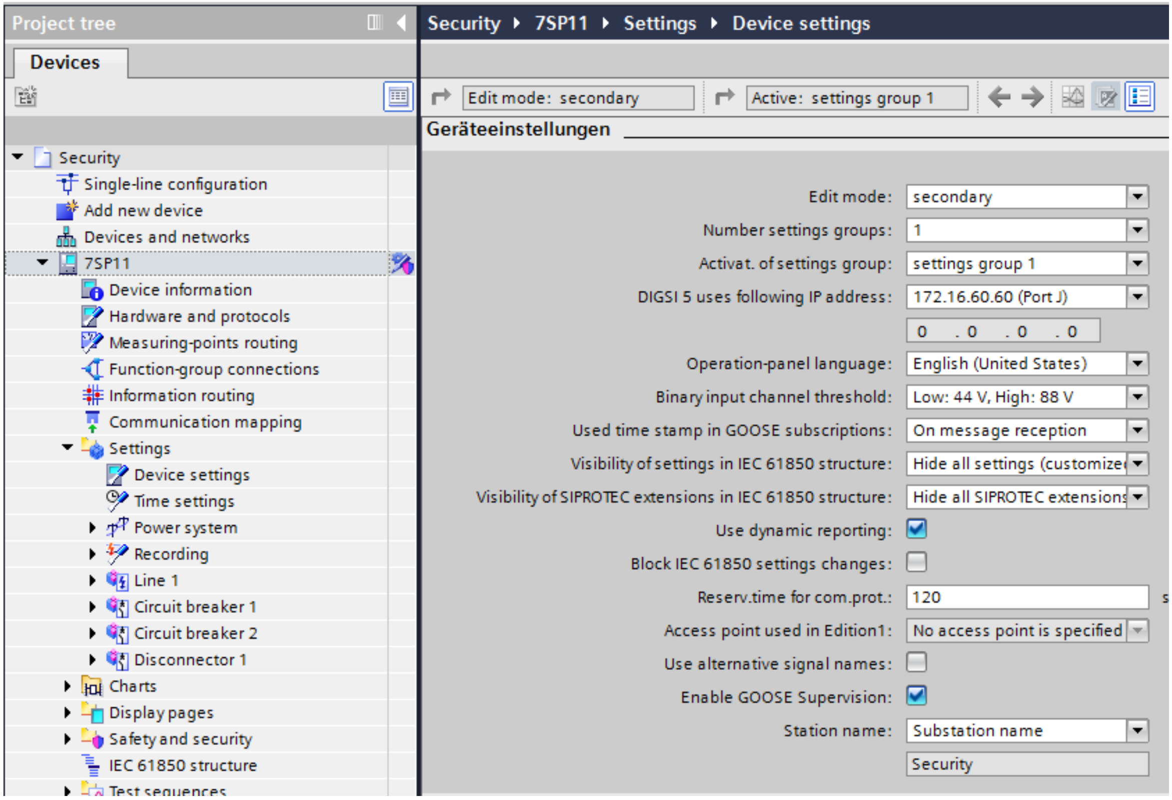
Figure 10-25 Influence Option When Linking a DPC Type Data Object

The setting options work for the device receiving the data.

10.1.14.3 Supervision of GOOSE Connections

With the standard IEC 61850-7-4 Edition 2, a new logical node for monitoring GOOSE connections has been introduced. This logical node can be used to easily monitor GOOSE communication at station level.

In order to be able to use GOOSE supervision, you must activate the setting **Enable GOOSE Supervision** in DIGSI 5 under **Settings > Device settings**.



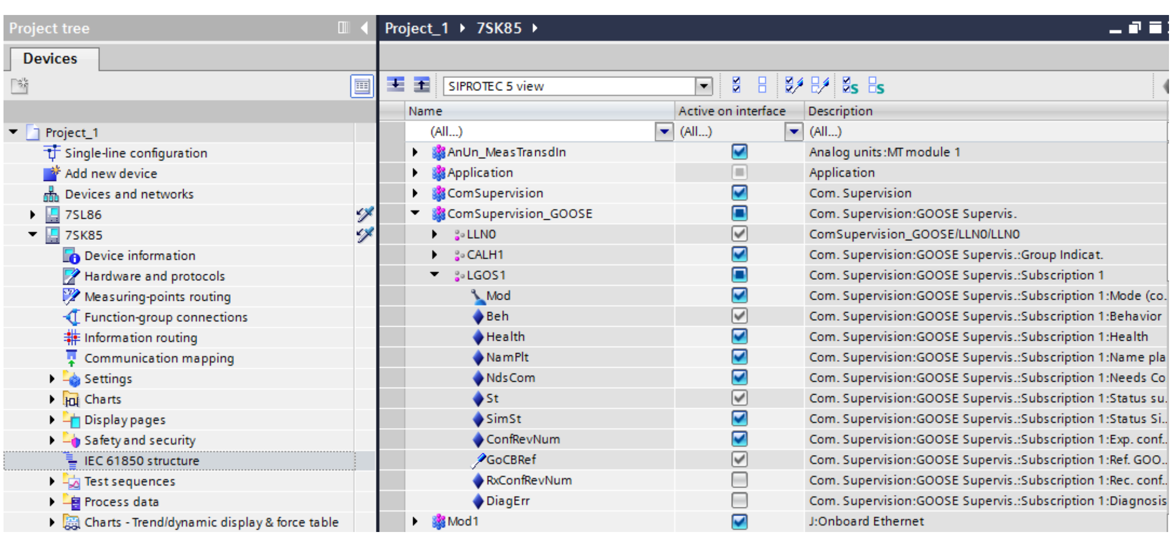
[sc_IEC61850_device_settings, 4, en_US]

Figure 10-26 Device Settings for IEC 61850 – Enable GOOSE Supervision

NOTE

This setting can only be done in Edition 2.

You can instantiate 1 LGOS logical node per GOOSE connection in an SCT conforming to IEC 61850. The logical nodes **LGOS** contain the following objects:



[sc_GOOSE-connection-LN-LGOS, 1, en_US]

Figure 10-27 Objects in LN LGOS

In the logical node **LGOS**, you can request the status of the GOOSE connection with the following objects:

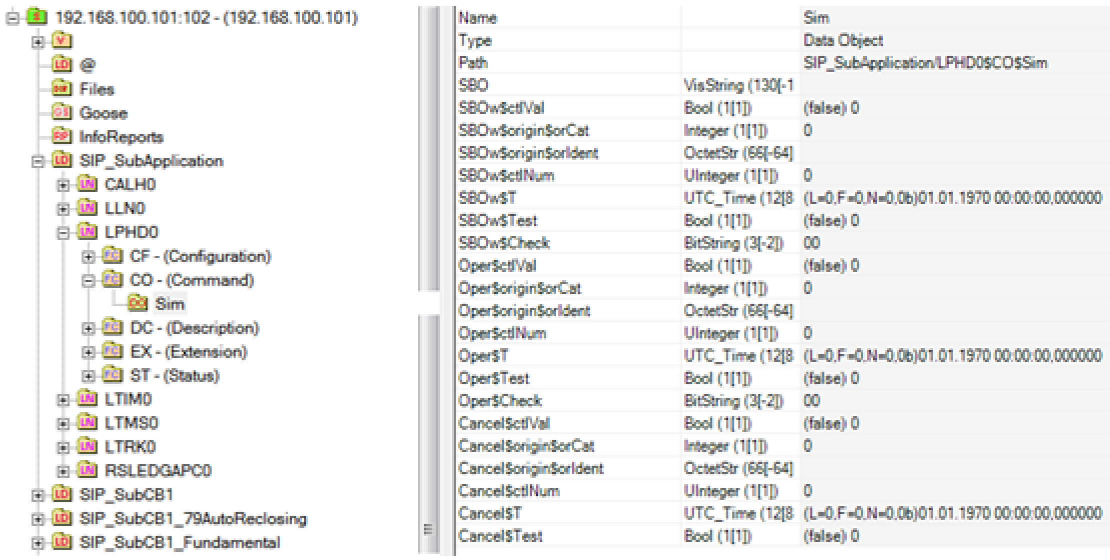
- **NdsCom**:
  If the value is **TRUE**, this indicates that the parameterization of the subscription is faulty.
  You can find detailed information in the object **DiagErr**.
- **St**:
  If the value is **TRUE**, the GOOSE connection is active. If the value is **FALSE**, the GOOSE connection is inactive.
- **SimSt**:
  If the value is **TRUE**, GOOSE messages with set simulation bit are accepted and received. For this, you must switch the device to the GOOSE simulation mode. You can find more information in chapter *10.1.14.4 GOOSE Simulation Mode*. If GOOSE messages with set simulation bit are no longer received, the value remains **TRUE** until the simulation is turned off.
- **ConfRevNum**:
  This object contains the expected ConfigRev number according to GOOSE parameterization.
- **RxConfRevNum**:
  This object contains the received ConfigRev number of the GOOSE connection. This number must match the **ConfRevNum**, otherwise, **NdsCom** is set to **TRUE** and you must adapt the parameterization.
- **DiagErr**:
  This object contains the following information in case of GOOSE-connection errors:
  - 0: NoError
  - 1: WaitingForTelegram
  - 2: ConfRevMismatch
  - 3: GoIDMismatch
  - 4: DataSetReferenceMismatch
  - 5: NeedsCommisioning
  - 6: DataSetMemberMismatch
- **GoCBRef**:
  This object contains the object reference of the monitored received GOOSE control block.

10.1.14.4 GOOSE Simulation Mode

You can switch the device to the GOOSE simulation mode using an IEC 61850 Client.

Controlling GOOSE Messages

In order to switch the device to the GOOSE simulation mode, the variable **Sim** is required in the logical node **LPHD**. The variable **Sim** controls switching on and off the GOOSE simulation mode. If a client sets this variable from **FALSE** to **TRUE**, the device can process simulated GOOSE messages. If a client sets the variable back to **FALSE**, the device is no longer in the GOOSE simulation mode and only processes normal and non-simulated GOOSE messages.



[sc_GOOSE simulation mode, 1, --_--]

Figure 10-28 Variable Sim of the LPHD in the IEC 61850 Browser

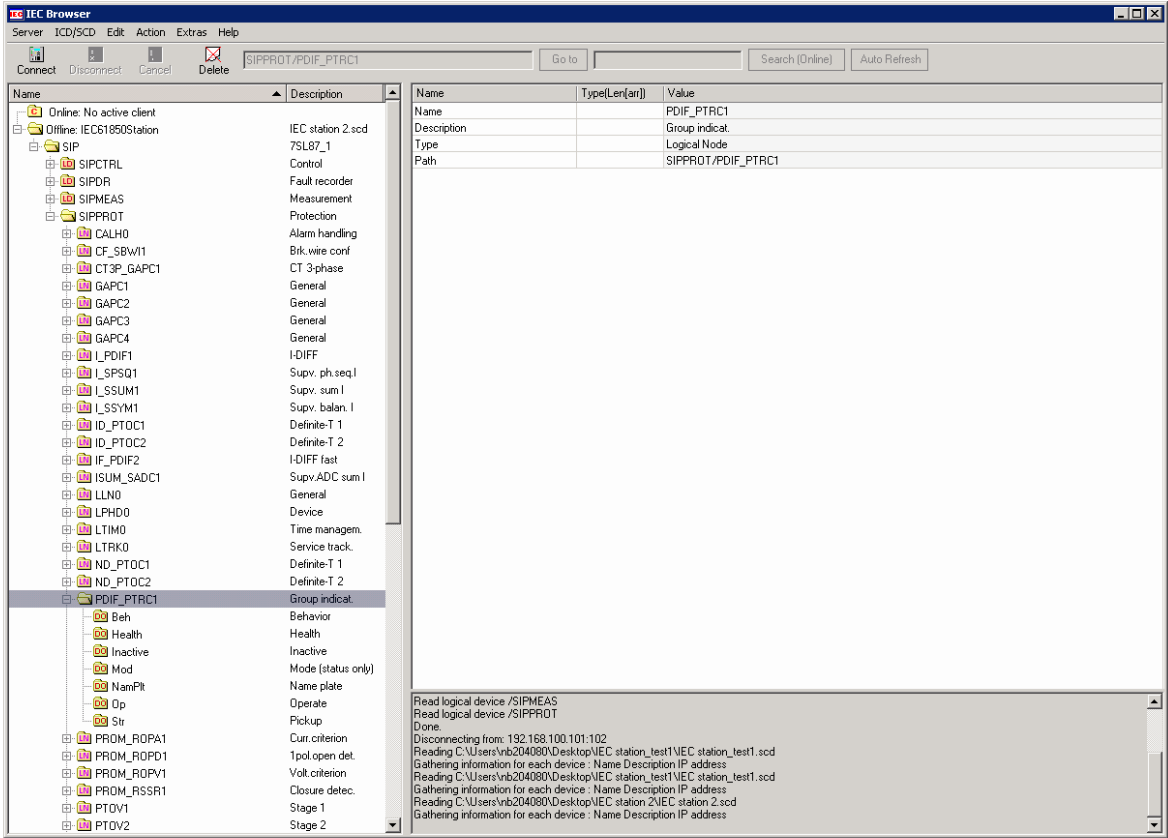
For testing purposes, you can use the IEC 61850 browser to control the variable **Sim** of the logical node **LPHD**.

10.1.15 Working in the IEC 61850 Browser

10.1.15.1 IEC 61850 Browser

The IEC 61850 Browser is a PC program that allows the IEC 61850 structure of a device to be displayed online. It is supplied as a debugger together with DIGSI 5 and provides valuable information about the IEC 61850 structure of a device during commissioning. The IEC 61850 Browser displays datasets configured in the device, for example, for static reports or GOOSE messages, as well as the data objects they contain.

The Browser behaves like an IEC 61850 client and can, for instance, receive reports from a device.



[sciecbrw-081210-01.tif, 2, en_US]

Figure 10-29 IEC 61850 Browser

To display the IEC 61850 structure of a device, connect to the IP address of the device over the network. The IEC 61850 Browser reads the entire IEC 61850 structure of a device online and displays it in a tree structure with logical devices, logical nodes, and data objects. For test purposes, you now have read and write access to the device.

If you have exported SCL data as ICD or SCD files, then you can import these files into the IEC 61850 Browser and in this way trasfer the data in the IEC 61850 Browser. In this case, the browser displays the IEC 61850 structure of the device offline. In this offline display, you can also recognize the descriptions of the IEC 61850 objects. They are incorporated from the ICD or SCD files and improve reading of the IEC 61850 structure noticeably. In the SCD file, you can see all devices and the IP addresses configured. You can now connect to a device and browse through the IEC 61850 structure of this device.

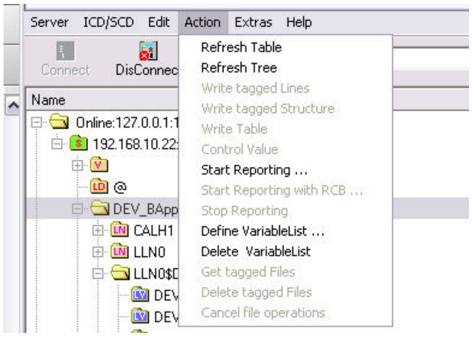
You can finde more information on the IEC 61850 Browser in the Help system of the program.

10.1.15.2 Dynamic Datasets

Creating Dynamic Datasets

The IEC Browser supports creation of dynamic reports as well. At the moment, this function is supported by only a few servers and clients. SIPROTEC devices support this function, which may allow the temporary creation of datasets. To do this, it is not necessary to create a dataset in the system configurator. In the following example, a new dataset is created for protection indications.

✧ Select the **Action** menu, then click the **Define VariableList ...** context menu.

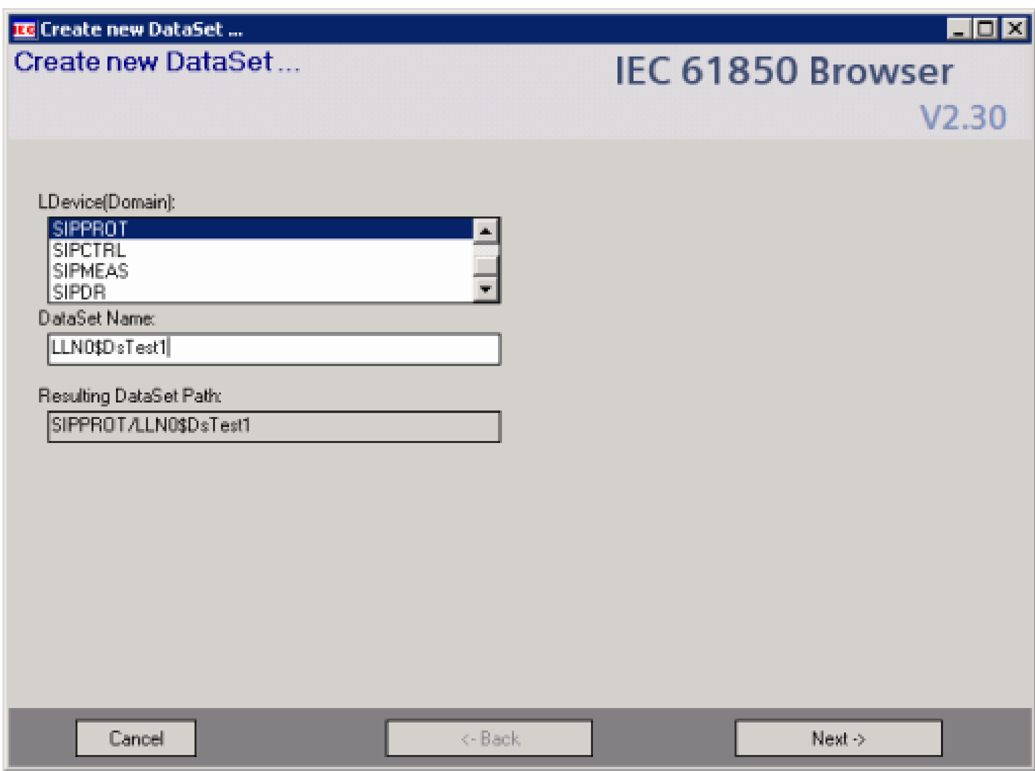


[scdfdats-240311-01.tif, 1, --_--]

Figure 10-30 Creating a Dataset

A dialog with all logical devices contained in the server appears.

- Select the logical device in which the new dataset is to be created.
- Enter the name of the dataset.



[scnwdats-240311-01.tif, 2, --_--]

Figure 10-31 Entering the Name of the Dataset

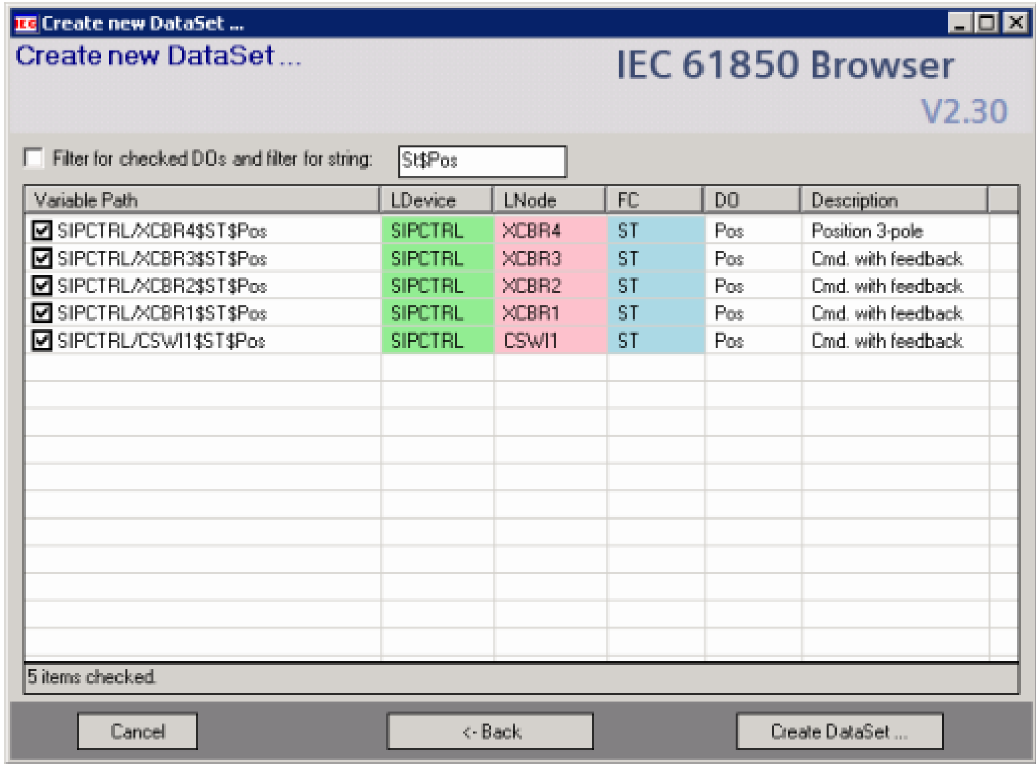
In the example, the dataset has been given the name **DsTest1**.

NOTE

Only change the part of the name following the **$** symbol.

- Click **Next**.

A list with all available signals will be displayed.



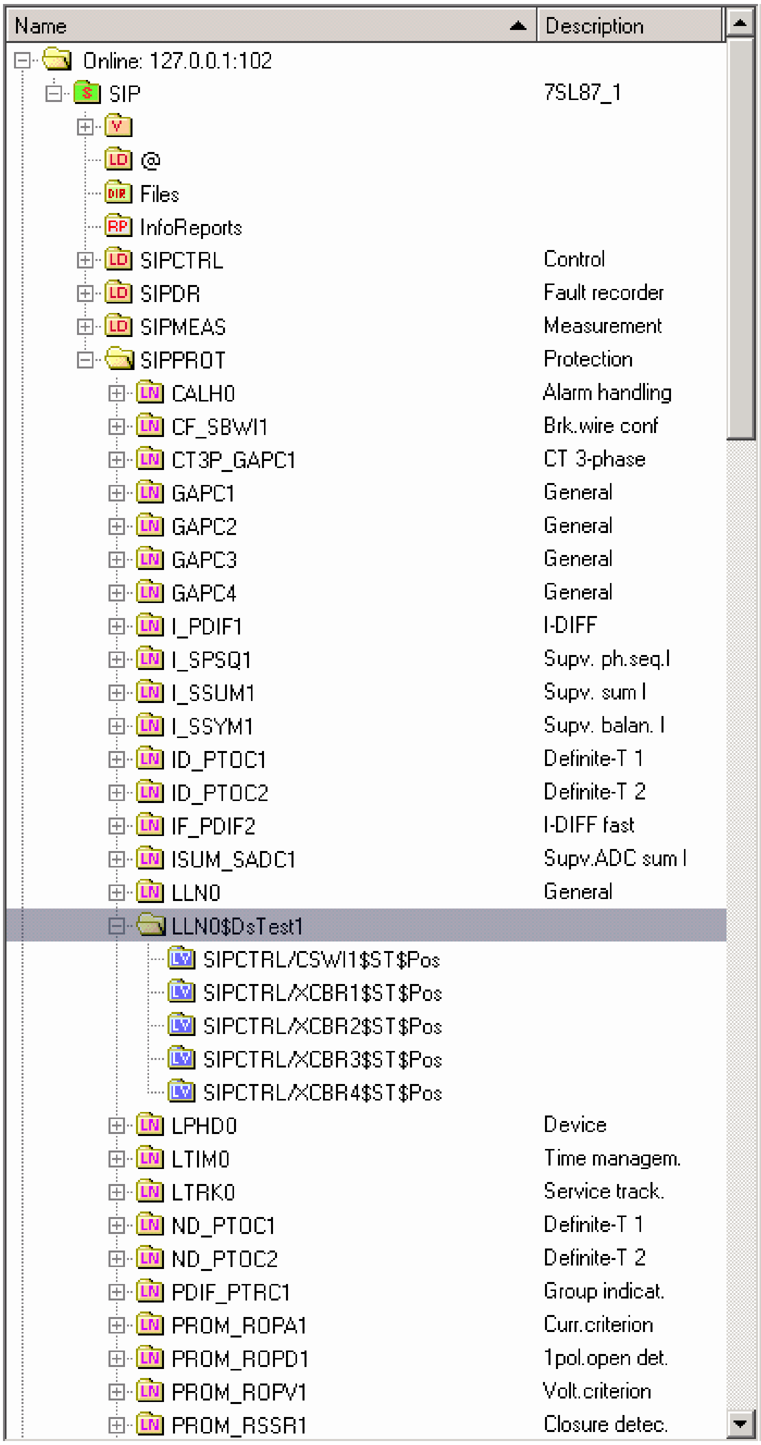
[scsglist-240311-01.tif, 2, --_--]

Figure 10-32 Signal List

✧ From this signal list, select the signals applicable for the dataset.

✧ Click **Create DataSet**.

The dataset is created in the server and the data objects set to the current status.

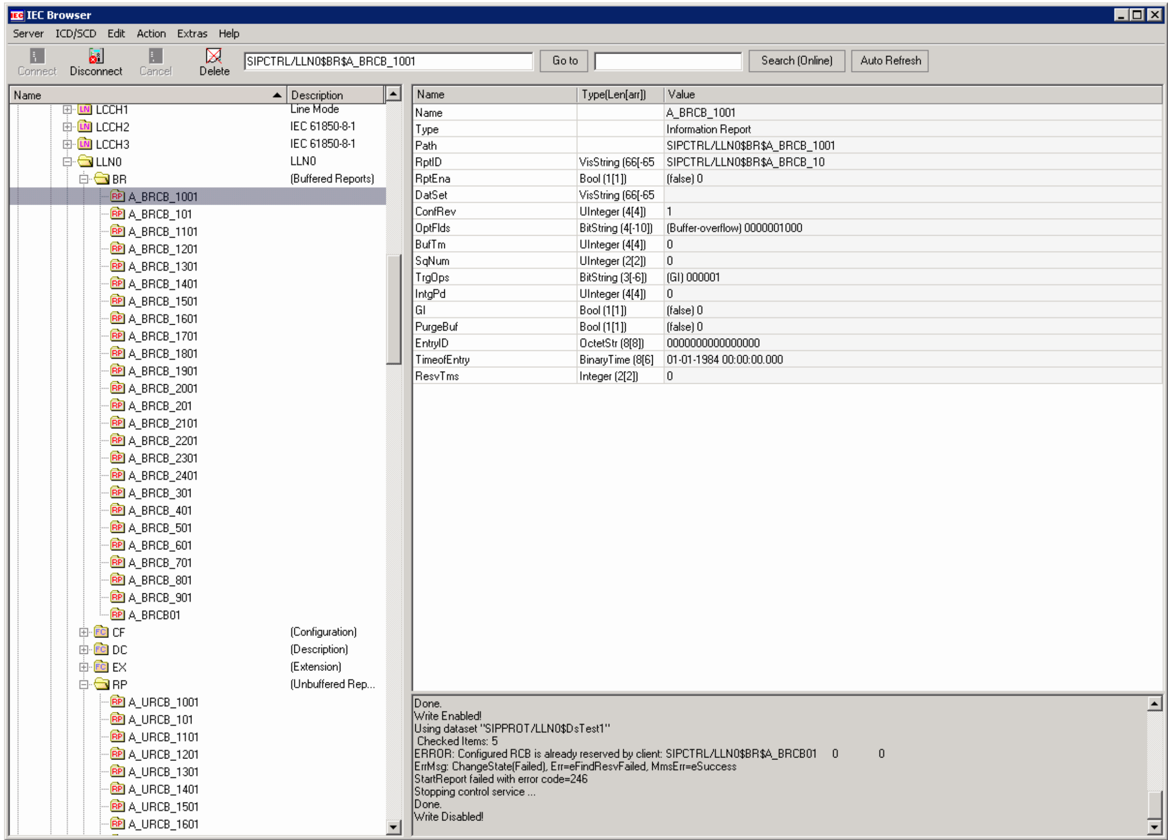


[sccrdats-240311-01.tif, 2, --_--]

Figure 10-33   Dataset LLN0$DsTest1

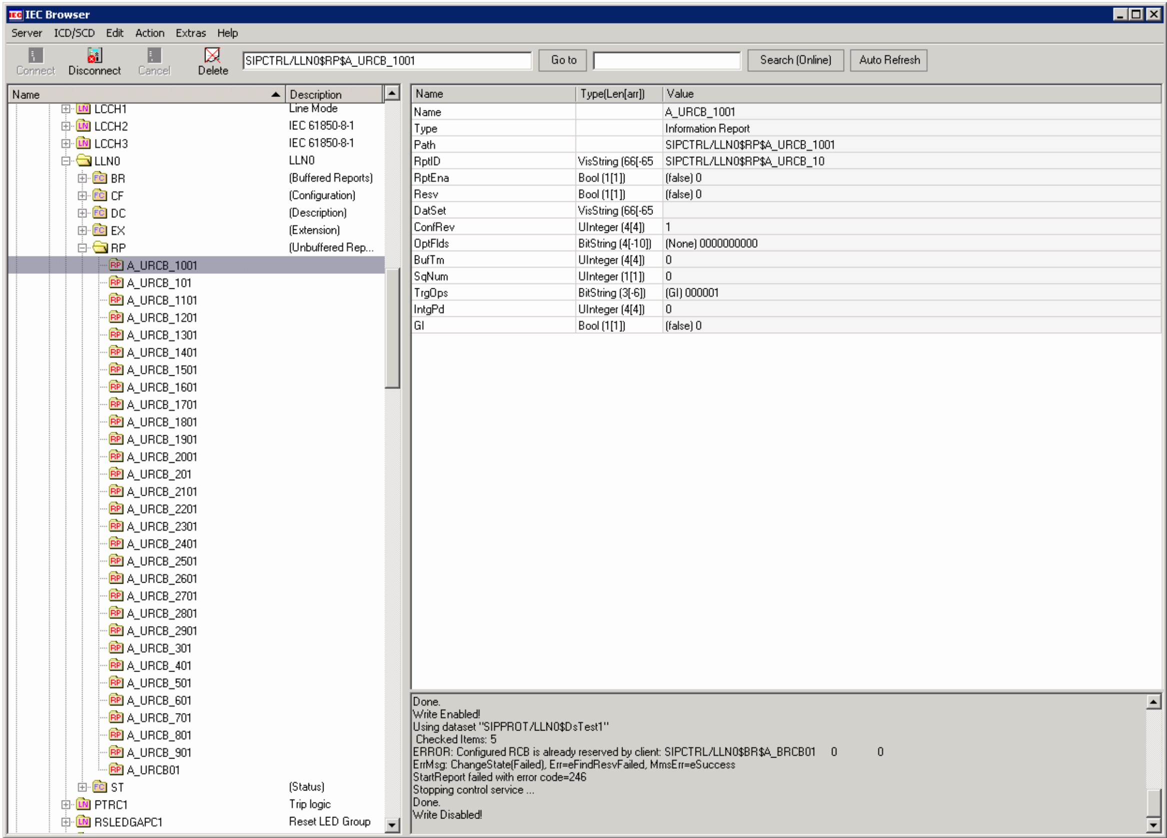
Reviewing Dynamic Datasets

In order to test a dataset, you must create a report control block. The buffered reports can be found in the **BR** folder, the unbuffered reports are located in the **RP** folder.



[scbufrcb-240311-01.tif, 2, --_--]

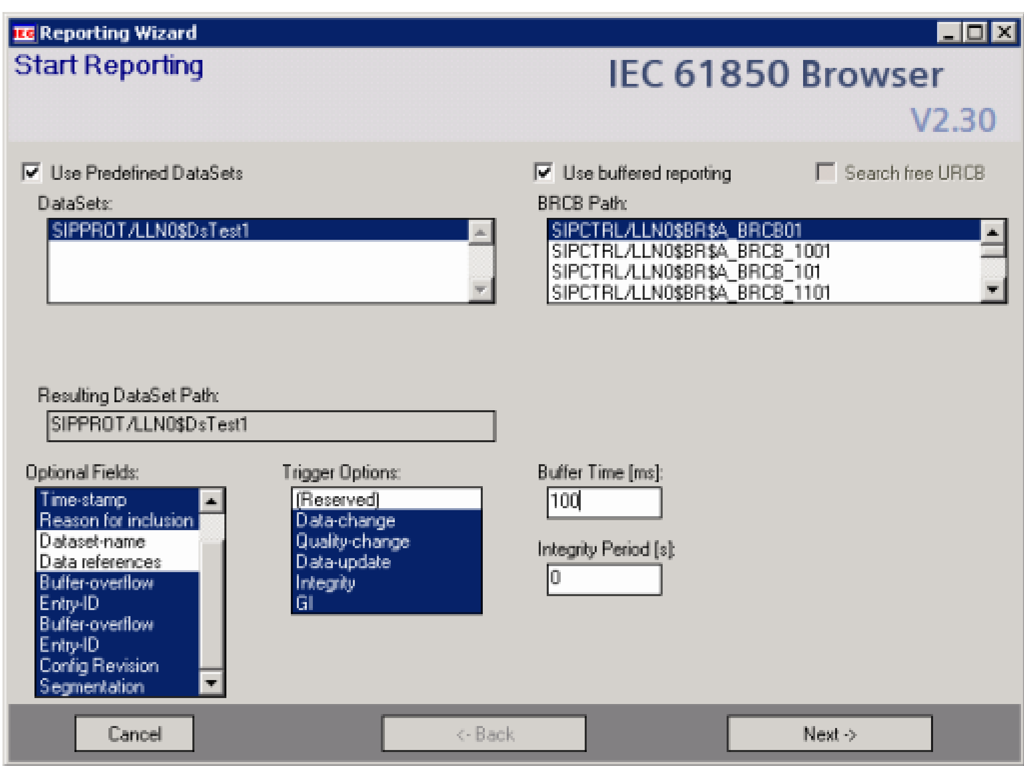
Figure 10-34 Buffered Reports



[scunbrcb-240311-01.tif, 2, --_--]

Figure 10-35 Unbuffered Reports

✧ Activate a free ReportControlBlock.



[sc_activate RCB, 1, --_--]

✧ In order to connect the control block with the dataset, copy the path of the dataset into the **DatSet** field.

✧ From the **Options** menu select the option **Enable write**.

✧ Enter the password **000000**.

✧ In order to activate the report, set the variable **RptEna** (Enable Report) to **1**.

If a signal changes, a report is being generated.

✧ In the right column **Write**, insert a check mark for all fields you have changed.

✧ From the **Action** menu, select the option **Write tagged Lines**.

✧ Click the **Auto Refresh** button.
The signals will be reread. If any signals have been changed on the device, these changes will be visible.

10.1.15.3 Activating the Reports

In order to subscribe to the report, the datasets must be defined. To do this, the datasets must be connected to the report control block. Subscribing is described here using the example of the IEC61850 Browser.

✧ Click the respective datasets.

✧ Copy the path.

✧ Select the report control block.

✧ Click the **Auto Refresh** button.

- or -

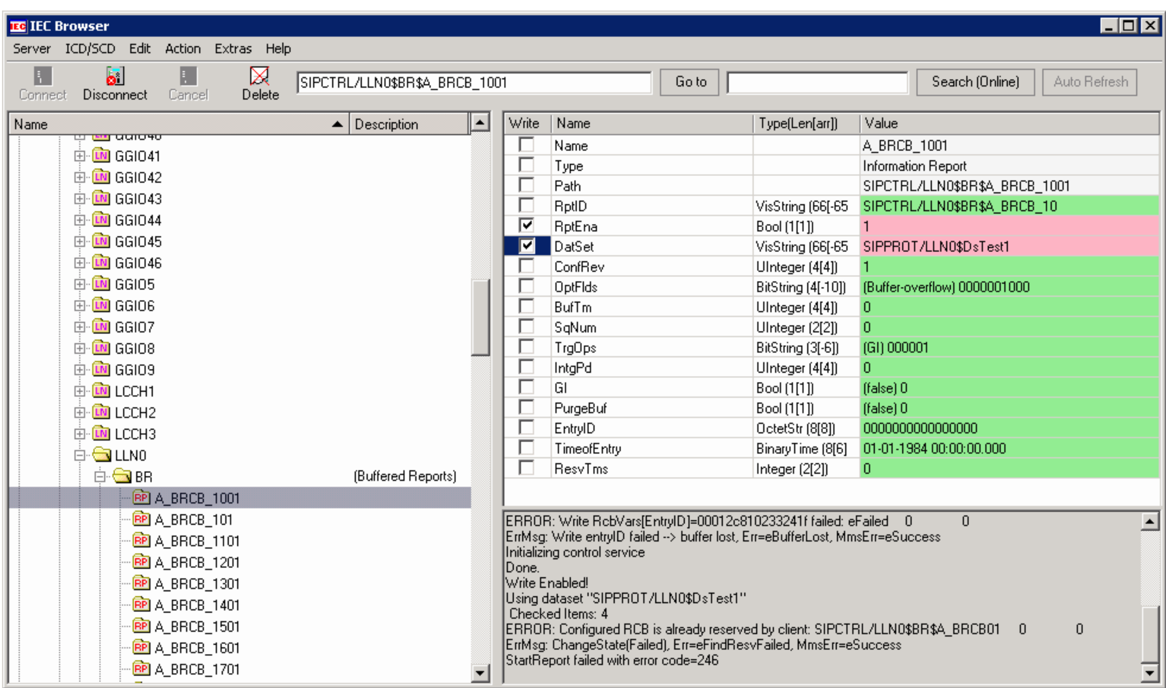
✧ Select the **Start Reporting** menu and click the report control block with the right mouse button.

✧ Add the path.

✧ In order to activate the report, set the variable **RptEna** to **1**.

✧ Activate the option **Write tagged Lines** for **RptEna** and the dataset

✧ Insert a check mark in the right column **Write**.



[sc_RptEna-130315, 1, --_--]

Figure 10-36 Variable RptEna

You have now subscribed to the report.

NOTE

You may subscribe to static as well as dynamic reports.
For static reports, all datasets are predefined, in dynamic reports, signal lists are always newly generated.

10.2 Signals to the Communication Modules

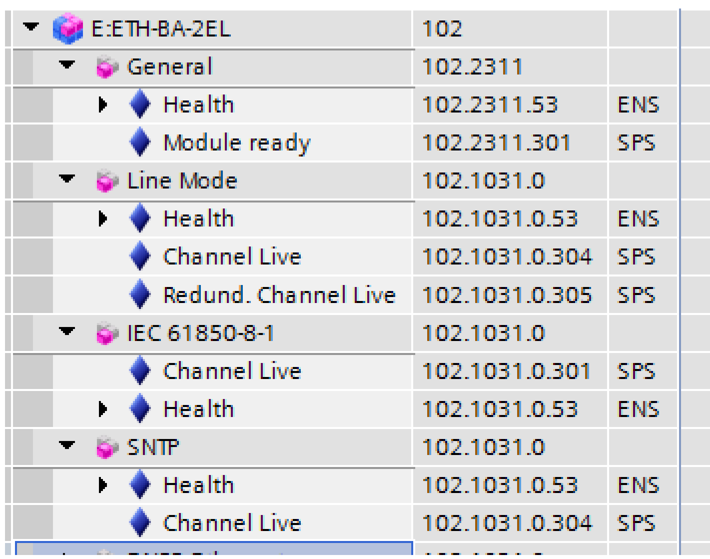
Indications and Representation of the Interface in Information Routing

A function group is provided for the protocol in Information routing. The indication **Channel Live** is issued there if the module is no longer communicating with the master (parameterized monitoring time has expired).

Description of the Signals to the Communication Modules

There are different signals for each communication module:

- **Channel Live**
  The signal **Channel Live** indicates the data flow. Therefore, the signal indicates that the communication service is transmitting and receiving data on the module.
  Consider that multiple services can run in parallel on one Ethernet module.
- **Redund. Channel Live** (redundant channel live)
  The signal **Redund. Channel Live** indicates whether the 2nd communication port can also transmit and receive.



[sc_redundant_channel_live, 1, en_US]

Figure 10-37 Signal Redund. Channel Live in the Information Routing

- **Module ready**
  The signal **Module ready** indicates that the module has started and the protocol applications have started. You can reallocate this signal to LED or log. Then, you can recognize whether the IEC 61850 services, for example, GOOSE, are started on an Ethernet module and are working correctly.

NOTE

The communication modules are started after the protection device is started. For this reason, it takes a bit longer for the communication protocols to be ready for operation.

- **Health**
  The signal **Health** indicates the state of the module. The following 3 states can occur in this case:
  - **OK**
    Module OK indicates, that the module is working.
  - **Warning**
    This state is not used.
  - **Alarm**
    The state **Alarm** is set when there is a failure of the module.

Each protocol application has a **Health** node. If a protocol has problems at startup – for example, missing parameters, no mapping, no hardware support – the status is set to **Alarm**. An alarm in a protocol causes an alarm of the module; that is, the higher-level element provides an overview.

Signal >Block monitoring direction

The signal **>Block monitoring direction** is provided for protocols with a master-slave architecture, for example, IEC 60870-5-103.

For an IEC 61850 client-server connection, a general blocking of the reporting is not desired. For this reason, the **>Block monitoring direction** signal is not available for IEC 61850. Other methods are available there.

To prevent too much incoming information during commissioning, there are the following options:

- Finish communication to the clients, for example, stop the device in the SICAM PAS UI – Operation.
  To start and stop transmitting IEC 61850 reports from the server, the clients activate or deactivate the report control blocks. In the SICAM PAS UI – Operation, you can use the **Bay blocking** function.
- Set the device into test mode (**Mod/Beh=3=test**), for example, by routing the signal **>Test mode on** in DIGSI.
  In this mode, all data objects are set with a test bit (in the quality attribute). This sends these quality changes by report to the client or via GOOSE.
- Disconnect the server physically from the network.
  This step is usually of little help with **Buffered Reporting** since all messages are sent later, as soon as the server is reconnected.

11 Troubleshooting

11.1 Troubleshooting

Information on the Communication Module

NOTE

If you wish to rectify faults, Siemens recommends using the information on the communication module.

- Refer to the documentation for information about the communication module or the display on the device (see **Commissioning and Diagnostics** chapter).

Connection Not Possible

Proceed as follows during the troubleshooting:

- Check whether all connection lines are correctly installed:
  - In the case of serial connections: between the device and the communication master
  - In the case of Ethernet connections: between the device and the switch
- Check whether the device address and settings of the data-link layer (data bits, stop bits, and parity) are set in the device (only applies for communication protocols DNP3 and IEC 60870-5-103).
- Check whether the correct protocol firmware is loaded.

Time Synchronization Not Possible

Proceed as follows during the troubleshooting:

- Check whether the master sends a valid time telegram.
- Check whether the time synchronization is parameterized via the corresponding communication protocol in the device.

DNP3: Error Message Msg[transmit failed, will retry] Number: 5292

NOTE

The error message **Msg[transmit failed, will retry] number: 5292** can occur. This error message is not relevant. You can ignore the error message.

Glossary

ACD

IEC 61850 data type: Directional protection activation information

ACK

Data transfer acknowledgment

ACT

IEC 61850 data type: Protection-activation information

APC

Controllable analog set point information

Big-endian

Big-endian and little-endian describe the order in which a sequence of bytes is stored. In big-endian systems, the most significant byte is stored at the lowest storage address. In little-endian systems, the most significant byte is stored at the highest storage address.

BSC

Binary Controlled Step Position

CRC

Cyclic **r**edundancy **c**heck

Data unit

Information item with a joint transmission source. Abbreviation: DU – **D**ata **U**nit

DCP

Discovery and Basic **C**onfiguration **P**rotocol

DIGSI

Configuration software for SIPROTEC

Discovery and Basic Configuration Protocol

The DCP protocol is used to detect devices without IP addresses and to assign addresses to these devices.

DPS

IEC 61850 data type: **D**ouble **P**oint **S**tatus

Drag and drop

Copying, moving, and linking function, used in graphic user interfaces. The mouse is used to highlight and hold objects and then move them from one data area to another.

DU

Data **U**nit

ENC

Enumerated Status **C**ontrollable

ENS

Enumerated **S**tatus

General Interrogation

The state of all process inputs, of the status, and of the error image are scanned on system startup. This information is used to update the system-side process image. Likewise, the current process state can be interrogated after data loss with a general interrogation (GI).

Generic Object-Oriented Substation Event

GOOSE. Protocol of IEC 61850 for communication between bay units.

GOOSE

Generic **O**bject-**O**riented **S**ubstation **E**vent

High Availability Seamless Redundancy Protocol

Like PRP (Parallel Redundancy Protocol), HSR (High Availability Seamless Redundancy Protocol) is specified in IEC 62439-3. Both protocols offer redundancy without switching time.

The principal function can be found in the definition of PRP. With PRP, the same indication is sent via 2 separated networks. In contrast to this, in the case of HSR the indication is sent twice in the 2 directions of the ring. The recipient receives it correspondingly via 2 paths in the ring, takes the 1st message and discards the 2nd (see PRP).

Whereas NO indications are forwarded in the end device in the case of PRP, a switch function is installed in the HSR node. Thus, the HSR node forwards indication in the ring that are not directed at it.

In order to avoid circular messages in the ring, corresponding mechanisms are defined in the case of HSR.

SAN (Single Attached Node) end devices can only be connected with the aid of a RedBox in the case of HSR. PRP systems and HSR systems can be coupled redundantly with 2 REDBOXES.

HSR

High Availability **S**eamless **R**edundancy Protocol

IEC

International **E**lectrotechnical **C**ommission - International electrotechnical standardization body

INC

Controllable Integer Status

INS

Integer **S**tatus

Internet Protocol

An Internet protocol (IP) enables the connection of participants which are positioned in different networks.

IP

Internet **P**rotocol

Link address

The link address indicates the address of a SIPROTEC device.

Management Information Base

A Management Information Base (MIB) is a database which saves information and statistics concerning each device in a network continuously. The performance of each device can be monitored with this information and statistics. In this way, it can also be ensured that all devices in the network function properly. MIBs are used with SNMP.

Manufacturing Message Specification

The standard Manufacturing Message Specification (MMS) serves for data exchange. The standard is used for the transmission protocols IEC 61850 and IEC 60870-6 TASE.2.

Metered value

Metered values are a processing function, used to determine the total number of discrete similar events (counting pulses), for example, as integral over a time span. In the power supply utility field, electrical energy is often recorded as a metered value (energy import/delivery, energy transport).

MIB

Management **I**nformation **B**ase

MMS

Manufacturing **M**essage **S**pecification

NACK

Negative **ack**nowledgment

Offline

If there is no communication connection between a PC program (for example, configuration program) and a runtime application (for example, a PC application), the PC program is **offline**. The PC program executes in Offline mode.

Online

If there is a communication connection between a PC program (for example, configuration program) and a runtime application (for example, a PC application), the PC program is **online**. The PC program executes in Online mode.

Parallel Redundancy Protocol

Parallel Redundancy Protocol (PRP) is a redundancy protocol for Ethernet networks that is specified in IEC 62439-3. Unlike conventional redundancy procedures, such as RSTP (Rapid Spanning Tree Protocol, IEEE 802.1D-2004), PRP offers uninterruptible switching, which avoids any down time in the event of a fault, and thus the highest availability.

PRP is based on the following approach: The redundancy procedure is generated in the end device itself. The principle is simple: The redundant end device has 2 Ethernet interfaces with the same address (DAN, Double Attached Node). Now, the same indication is sent twice, in the case of PRP (**parallel**) to 2 separate networks, and uniquely marks both with a sequence number. The recipient takes the information that it receives first, stores its ID based on the source address and the sequence number in a duplicate filter and thus recognizes the 2nd, redundant information. This redundant information is then discarded. If the 1st indication is missing, the 2nd indication with the same content comes via the other network. This redundancy avoids a switching procedure in the network and is thus interruption-free. The end device forwards no messages to the other network. Since the process is realized in the Ethernet layer (same MAC address), it is transparent and usable for all Ethernet payload protocols (IEC 61850, DNP, other TCP/IP based protocols). In addition, it is possible to use one of the 2 networks for the transmission of non-redundant messages.

There are 2 versions of PRP: PRP-0 and its successor PRP-1. Siemens implements PRP-1.

Parameterization

Comprehensive term for all setting work on the device. You can set parameters for the protection functions with DIGSI 5 or sometimes also directly on the device.

PB Client

Process-**b**us Client. The subscriber of Sampled Measured Values can also be called process-bus client.

PICS

Protocol **I**mplementation **C**onformance **S**tatement

PLC

Programmable **L**ogic **C**ontroller

Protection device

A protection device detects erroneous states in distribution networks, taking into account various criteria, such as error distance, error direction or fault direction, triggering a disconnection of the defective network section.

PRP

Parallel **R**edundancy **P**rotocol

Rapid Spanning Tree Protocol

The Rapid Spanning Tree Protocol (RSTP) is a standardized redundancy process with a short response time. In the Spanning Tree Protocol (STP protocol), structuring times in the multidigit second range apply in the case of a reorganization of the network structure. These times are reduced to several 100 milliseconds for RSTP.

RedBox

Reduncancy box

The RedBox is used for the redundant connection of devices with only one interface to both the LAN A and the LAN B PRP network. The RedBox is a DAN (Double Attached Node) and operates as a proxy for the devices connected to it (VDANs). The RedBox has its own IP address in order to be able to configure, manage, and monitor it.

RSTP

Rapid **S**panning **T**ree **P**rotocol

SAN

Single **A**ttached **N**ode

A SAN is a non-redundant node in the PRP network. It is only connected with one port to one network (LAN A or LAN B). It can only communicate with nodes in the connected network. Via a RedBox, devices with only one connection can be redundantly connected to the 2 LAN A and LAN B networks. In order to obtain symmetrical LAN A and LAN B networks, Siemens recommends avoiding SANs and to connect the devices either via a RedBox or in a separate network without PRP support.

SBO

Select **b**efore **o**perate

SCD

Substation **C**onfiguration **D**escription

SFP

Small **F**orm-Factor **P**luggable

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is an Internet standard protocol and serves for the administration of nodes in an IP network.

Simple Network Time Protocol

The Simple Network Time Protocol (SNTP) is a protocol for the synchronization of clocks via the Internet. With SNTP, client computers can synchronize their clocks via the Internet with a time server.

SIPROTEC

The registered trademark SIPROTEC designates the product family of protection devices and fault recorders.

SIPROTEC 5 device

This object type represents a real SIPROTEC device with all the contained setting values and process data.

SNMP

Simple **N**etwork **M**anagement **P**rotocol

SNTP

Simple **N**etwork **T**ime **P**rotocol

SPS

IEC 61850 data type: **S**ingle **P**oint **S**tatus

Station description

A station description is an IEC 61850-compliant file for data exchange between the system configurator and the IED configurator. The station description contains information on the network structure of a substation. The station description contains for example, information on the assignment of the devices to the primary equipment, as well as on the station-internal communication.

TAI

Temps **A**tomique **I**nternational - International Atomic Time

TCP

Transmission **C**ontrol **P**rotocol

Time stamp

A time stamp is a value in a defined format. The time stamp assigns a time point to an event, for example, in a log file. Time stamps ensure that events can be found again.

Transmission Control Protocol

The Transmission Control Protocol (TCP) is a transmission protocol for transport services in the Internet. TCP is based on IP and ensures connection of the participants during the data transmission. TCP ensures the correctness of the data and the correct sequence of the data packages.

UTC

Universal **T**ime **C**oordinated

Index

I

M

N

O

P

Q

R

S

T

U