

A man in a light blue shirt is seen from the side, holding a tablet. He is in a factory or industrial setting. Overlaid on the image are various digital graphics: a clock, a '24/7' icon with a circular arrow, a 'NEWS' section with a person icon, a 'Home' button, and a network diagram with three people icons connected by lines. The background shows industrial equipment and a clock on the wall.

SIEMENS

Ingenuity for life

Network and Communication Diagnostics

SCALANCE, SIMATIC

<https://support.industry.siemens.com/cs/ww/en/view/21566216>

Siemens
Industry
Online
Support



Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (<https://support.industry.siemens.com>) shall also apply.

Security information

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

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

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial security measures that may be implemented, please visit <https://support.industry.siemens.com>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: <https://support.industry.siemens.com>.

Table of Contents

Legal information	2
1 Introduction	4
1.1 Overview.....	4
1.2 Integrated Diagnostic Concept.....	5
2 Diagnostics in the TIA Portal.....	9
2.1 Module Symbolic Status Display	9
2.2 Diagnostics of Communication Connections.....	11
3 Diagnostics on the Device	12
3.1 Diagnostics with SIMATIC.....	12
3.1.1 CPU Display View	12
3.1.2 Status LED on the Module	13
3.1.3 System Diagnostics	14
3.1.4 System Diagnostics in the User Program	16
3.2 Diagnostics with SCALANCE	19
3.2.1 SCALANCE General Diagnostics	19
3.2.2 SCALANCE X Specific Diagnostics	25
3.2.3 SCALANCE W Specific Diagnostics	30
4 Diagnostics with External Tools	34
4.1 Wireshark	34
4.2 Remote Capture	36
4.3 SIMATIC Assessment Suite	37
4.4 PRONETA	38
4.5 SINEC NMS	39
5 Diagnostics with Network Protocols	40
5.1 SNMP	40
5.2 RMON.....	43
5.3 Ping	45
6 Appendix	46
6.1 Service and support	46
6.2 Links and literature	47
6.3 Change documentation	47

1 Introduction

1.1 Overview

Cause

The availability of plants is one of the most important goals of any plant operator. An integrated diagnostic concept is necessary to guarantee the availability of a plant.

With an integrated diagnostic concept, faults can be detected at an early stage and their cause can be localized. This can minimize failures in the plant.

There are numerous different diagnostic procedures in automation technology.

The following questions therefore arise for the user in the search for an optimal diagnostic option:

- What solutions are there?
- How do the solutions differ?

Motivation

This document provides an overview of the options available for diagnostics of a SIMATIC controller or SCALANCE network device, networks and communication.

Structure documentation

The documentation is divided in two parts: It begins with a general part. Here you will find general information on diagnostics and a rough overview of the common diagnostic options.

The general part is followed by a description of selected diagnostic tools. Each diagnostic tool has its own section. You will receive a short description of the diagnostic tool and answers to the following questions:

- WHEN or WHY can you use this diagnostic tool?
- WHAT is the result of the diagnostics?
- WHERE can you find this diagnostic tool?
- WHAT are the advantages and added value?

If you would like to know more about the diagnostic tool described, you will find a link to the corresponding article in Siemens Industry Online Support in each section.

1.2 Integrated Diagnostic Concept

SIMATIC S7-1500

In the SIMATIC S7-1500 automation system, integrated diagnostics are consistent across all automation levels. All SIMATIC products have integrated diagnostic functions with which errors can be efficiently analyzed and localized. This shortens commissioning times and minimizes downtimes in production.

Note

Additional information on diagnostics with SIMATIC S7-1500 can be found in the application example "Diagnostics overview for SIMATIC S7-1200 and S7-1500".

<https://support.industry.siemens.com/cs/ww/en/view/109752283>

An overview of available application examples for diagnostics with SIMATIC S71500 can be found by using the following filter:

<https://support.industry.siemens.com/cs/ww/en/ps/13716/ae>

SCALANCE

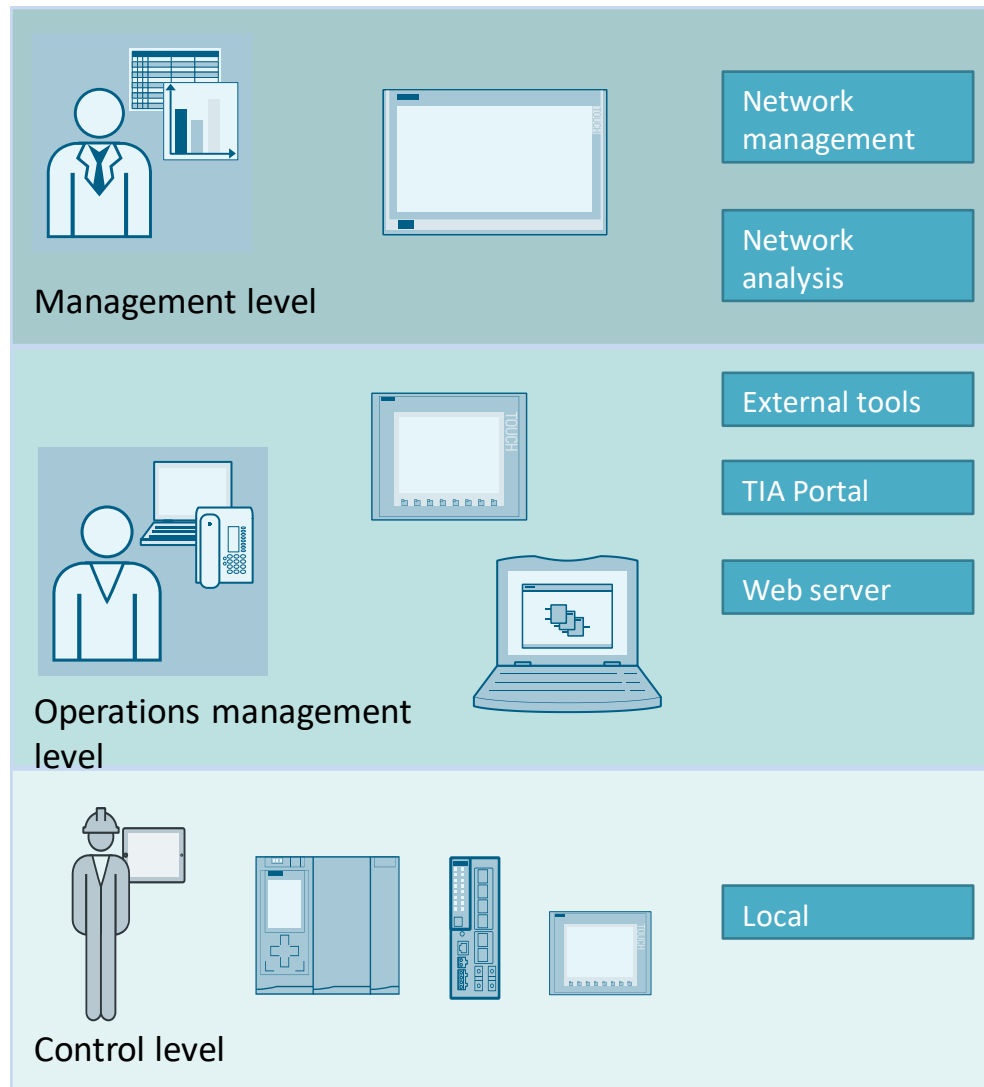
Thanks to their wide range of functions, the switches meet the requirements of a sustainable, industry-oriented Industrial Ethernet switch. The wide range of redundancy options, the multifaceted configuration and diagnostic options, and the wide selection of variants enable the automation engineer to implement their desired network concept with SCALANCE switches.

Various diagnostic tools - centralized as well as local - also help to keep downtimes as infrequent as possible. SCALANCE is characterized by a separate LED field for the hardware setup. There, the diagnostic LEDs can be identified at a glance, even when all the cables are plugged in. Port status, the status of the device via signaling contact, as well as the status of the redundancy manager, are clearly displayed here. On the software side, the configuration is supported not only by the text-based CLI interface, but also by a web server, in which the settings can be configured intuitively.

Diagnostics and diagnostic format

The following figure shows at which level, and in which form diagnostics can be ran on modules.

Figure 1-1



Overview of the diagnostic tools

The following table lists the diagnostic tools that are covered in this overview document. Use the link in the right-hand column of the table to jump straight to the corresponding section.

Table 1-1

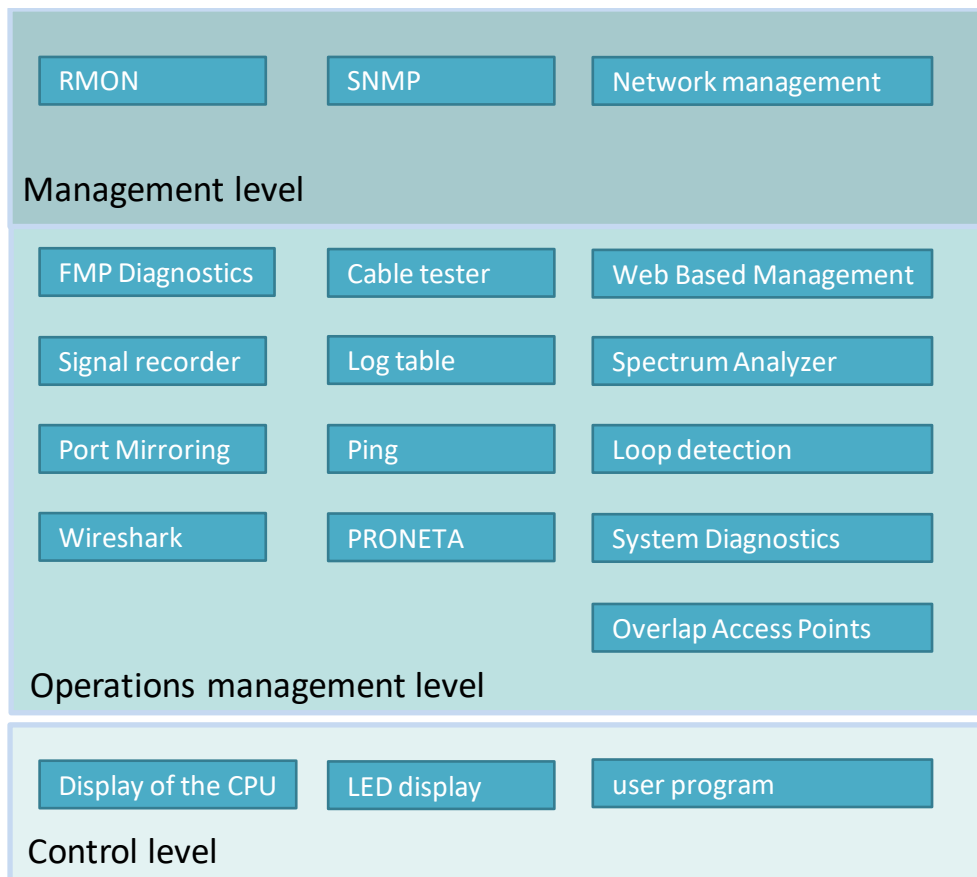
Diagnostic tools	Description	Link
Display of the CPU	View diagnostic buffer and module status. Detect errors.	Section 3.1.1
LED	First tool for containing errors using an on-site analysis of the state of the module.	Section 3.1.2 Section 3.2.1.1
System Diagnostics	Evaluate information. View text-based messages.	Section 3.1.3
System Diagnostics in the User Program	Configure reactions to diagnostic messages.	Section 3.1.4
LOG file/system messages	View diagnostic messages in plain text and recognize errors.	Section 3.2.1.2
Web Based Management	Read internal errors. Detect overload situations. Monitor the ring condition. View standby status. Check for module overheating.	Section 3.2.1.3
Cable tester	Check copper wires for faults.	Section 3.2.2.1
Cable tester	Detect interference in an optical transmission path.	Section 3.2.2.2
FMP Diagnostics	Detect power loss in an optical transmission path.	Section 3.2.2.3
Loop detection	Detect network loops.	Section 3.2.2.4
Signal Recorder	Check connection quality in a WLAN.	Section 3.2.3.1
Spectrum Analyzer	Check the radio channel for interference.	Section 3.2.3.2
Port Mirroring	Record data traffic.	Section 3.2.2.5
SMTP Client	Send events by email.	Section 3.2.1.4
Syslog Client	Log system events to a central syslog server.	Section 3.2.1.5
Monitoring Overlapping Access Points	Monitor the radio channels to ensure optimal data throughput.	Section 3.2.3.3
Wireshark	Record and evaluate network communication on a local interface.	Section 4.1
Remote Capture	Record and evaluate network communication across the entire network.	Section 4.2
SIMATIC Assessment Suite	Gather diagnostic and system information.	Section 4.3
PRONETA	Analyze and configure the PROFINET network.	Section 4.4
SINEC NMS	Central Network Management System for monitoring and managing industrial networks.	Section 4.5
Symbolic status display of the modules	Display operating state and output relevant information on pending errors in the system.	Section 2.1
Diagnostics for communication connections	View the status of the communication connections.	Section 2.2
SNMP	Monitor network components, as well as detect and report errors.	Section 5.1
RMON	Collect and save statistical data in a Network device for proactive monitoring and diagnostics.	Section 5.2

Ping	Check IP endpoint for accessibility.	Section 5.3
------	--------------------------------------	-----------------------------

Classification of diagnostic tools

The following figure shows how the diagnostic tools are to be classified in the automation pyramid:

Figure 1-2



2 Diagnostics in the TIA Portal

The TIA Portal offers extensive diagnostic possibilities. The application example only addresses the possibilities for network and communication diagnostics.

Note

For additional information on diagnostics with the TIA Portal, refer to the application example "Diagnostic Overview for SIMATIC S7-1200 and S7-1500".

<https://support.industry.siemens.com/cs/ww/en/view/109752283>

2.1 Module Symbolic Status Display

Description









When you establish an online connection to a module, the system also determines its diagnostic status and, if necessary, that of its subordinate components. If the module has an operating state, this is also determined. The diagnostic status and operating state are displayed with icons in the TIA Portal.

What do you see?

If you have established an online connection, you will see additional diagnostic icons for the diagnostic status and operating state.

The following table shows a selection of the diagnostic symbols:

Table 2-1

Symbol	Meaning
	No fault
	Maintenance required
	Maintenance request
	Error
	The module or the device is deactivated.
	The module or the device is not accessible from the CPU (valid for modules and devices below a CPU).
	The functionality of the module or submodule is not available.
	The connection is established, but the state of the module is currently being determined or is unknown.

Where can you find this?

If you have set up an online connection, you can find the symbols for the diagnostic status and operating state in all views in the TIA Portal. These include:

- Device overview
- Network view
- Topology
- Project navigation

The corresponding diagnostic symbol is displayed for each hardware component.

For hardware components with their own operating state, the operating status symbol is also displayed.

Additional information

Additional information on the symbolic status display can be found

In the manual "SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16" > Section 11 "Editing Devices and Networks" > Section 2.1 "Hardware Diagnostics":

<https://support.industry.siemens.com/cs/ww/en/view/109773506>

- In the FAQ "How do you use the 'Online & diagnostics' view in the TIA Portal to diagnose the distributed IO and lower-level modules?":
<https://support.industry.siemens.com/cs/ww/en/view/88628706>
- In the application example "System Diagnostics with S7-1500 and TIA Portal"
<https://support.industry.siemens.com/cs/ww/en/view/68011497>
- In the FAQ "Why are blocks marked differently in the STEP 7 (TIA Portal) Online View although they are identical?"
<https://support.industry.siemens.com/cs/ww/en/view/62964890>
- In the FAQ "How do you use the 'Online & diagnostics' view in the TIA Portal to diagnose the distributed IO and lower-level modules?"
<https://support.industry.siemens.com/cs/ww/en/view/88628706>
- In the application example "Diagnostics in User Program with S7-1500"
<https://support.industry.siemens.com/cs/ww/en/view/98210758>

2.2 Diagnostics of Communication Connections

Description

The TIA Portal provides you with a connection table. In the connection table, you can display the details of all communication connections created in the project or of selected communication connections.

If you have established an online connection to a module (CPU or CP) that is involved in one or more communication services, the connection diagnostics is started.

Diagnostic icons for the connection status are now added to the properties of the offline listed communication connections in the connection table.




In addition, the connection table now also contains entries for those communication connections that are only available online, e.g., connections for Open User Communication commands, PG and OP connections, and connections for web server access.

What do you see?

If you have established an online connection, you will see additional diagnostic symbols for the communication connections in the connection table.

The following table shows the diagnostic icons for communication connections:

Table 2-2

Symbol	Meaning
	Connection established.
	Connection is not established or is being established.
	Connection not available.

Where can you find this?

You can find the connection table in the tabular area of the network view.

Additional information

Additional information on connection diagnostics can be found in the "SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16" manual > Section 11 "Edit Devices and Networks" > Section 2.2 "Diagnosing Connections":

<https://support.industry.siemens.com/cs/ww/en/view/109773506>

3 Diagnostics on the Device

SIMATIC and SCALANCE have useful on-board equipment for the diagnostics and optimization of industrial networks. This chapter describes the diagnostic tools that the devices themselves come with.

3.1 Diagnostics with SIMATIC

The application example only addresses the possibilities for network and communication diagnostics.

Note

More information about the diagnostics of the device may be found in the application example "Diagnostics Overview for SIMATIC S7-1200 and S7-1500".

<https://support.industry.siemens.com/cs/ww/en/view/109752283>

3.1.1 CPU Display View

Description

The S7-1500 CPUs have a display with control buttons. You can use the display for the following purposes:

- Read out the status information for the configured modules.
- Diagnostics
- Adjust CPU settings.

What do you see?

There are two main menu items in the CPU display that are relevant for diagnostics:

- "Diagnostics" menu
- Menu "Module"

The "Diagnostics" menu contains:

- The display of diagnostic messages.
- The display of alarms.

The "Modules" menu contains information on the central and decentralized modules used in your configuration.

What are the advantages?

If you use the display of the CPU, you have the following advantages:

- Shorter downtimes of the system due to diagnostic messages in plain text.
- Reading of the diagnostic buffer and the module status directly on site. No PG / PC is required.

When do you use it?

You can use the display of the CPU at any time, even during operation of the system. In the event of service, system downtime is minimized by quick access to the diagnostic messages.

Additional information

Additional information about the display of the CPU can be found:

- In the "SIMATIC S7-1500, ET 200MP Automation System" manual:
<https://support.industry.siemens.com/cs/ww/en/view/59191792>
- In the "PROFINET with STEP 7 V16" function manual
<https://support.industry.siemens.com/cs/ww/en/view/49948856>
- In the "SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro Diagnostics" function manual:
<https://support.industry.siemens.com/cs/ww/en/view/59192926>

3.1.2 Status LED on the Module

Description

Most SIMATIC modules have an LED display on the housing for status and error indication. Depending on the status and error, one or more LEDs light up.

Diagnostics using LEDs is the first tool for localizing errors. Usually, the source of the error can be more precisely pinpointed by analyzing the module status information in STEP 7, or in the diagnostic buffer of the CPU.

What do you see?

The S7-1500, ET 200MP, ET 200SP, and ET 200AL systems have LEDs to indicate the status and errors.

The "RUN" LED indicates the operating status.

If there is an error in the system, the "ERROR" LED lights up red.

The S7-1500, ET 200MP, ET 200SP, and ET 200AL systems support the diagnostic concept and maintenance concept in PROFINET IO to recognize and eliminate potential faults at an early stage. As soon as network components need to be checked or replaced, the "MAINT" LED signals this to the user via a yellow flashing light.

With the ET 200SP decentralized peripheral system, you can also determine the information on the cause of the error via the LED error display. After an announcement by means of a flashing signal, the error type and then the error location and error code are displayed.

What are the advantages?

When you evaluate the LEDs of the module, you have the following advantages:

- You can see the condition of your system directly on site. No PG / PC is required.
- Shorter downtimes of the plant. In the event of a fault or maintenance, you can take immediate action to correct the fault or the cause of the maintenance request.
- You can identify and eliminate potential faults at an early stage.

When do you use it?

You can evaluate the LEDs of the CPU at any time, even during operation of the system.

If your CPU is not accessible, you can also view the status of the LEDs via the "Online & Diagnostics" function of TIA Portal.

Where can you find this?

The LEDs for the operating state of the CPU are located on the front above the operating panel.

The "RX/TX" LED is located at the interface connections. On the S7-1500 CPU, you will find this LED under the control panel with the display.

Additional information

A detailed description of all LEDs of the modules with error causes and remedial measures can be found in the respective module documentation.

3.1.3 System Diagnostics

Description

Hardware components and third-party devices can trigger a system reaction if a system error occurs and provide information on the system error that has occurred.

System diagnostics offers a convenient way of evaluating this information for S7-1500 CPUs and displaying it in the form of text-based messages.

System diagnostics is an integral part of STEP 7 and does not require an additional license. The system diagnostics of the S7-1500 CPUs is activated by default. You do not need to make any further settings here.

What do you see?

The system diagnostics displays all relevant information on pending errors in the system. This information is automatically packed into text messages.

The database of all messages is the diagnostic buffer in the CPU. The diagnostic buffer is designed as a ring buffer: The most recent event is in the diagnostic buffer on the first line. An entry consists of a timestamp and the event text.

A new entry is triggered by the following events, among others:

- Internal and external errors in one module
- System error in the CPU
- Operating state transitions
- User program error
- Removal and insertion of modules
- Security events

The following security events (event types) each lead to an entry in the diagnostic buffer:

- Go online
- Manipulation of communication data, the data on SIMATIC Memory Card, the firmware update file detected.
- A changed protection level (access protection) is loaded into the CPU.
- Password legitimization restricted or released.
- Online access denied because the number of simultaneous accesses was exceeded.
- Timeout due to inactivity of an existing online connection.

- Logging on to the Web server.
- A backup of the CPU is created.
- The CPU project planning is restored.

What are the advantages?

If you use the system diagnostics, you have the following added value:

- Programming the system diagnostics is not necessary.
- Errors can be localized quickly.
- The system diagnostics is automatically updated when the hardware configuration changes.
- Transparent status messages for controllers, peripherals, and drives (motion control messages).
- System diagnostics are activated by default for the SIMATIC S7-1500 CPU and are also available in the "STOP" operating state.
- Errors or events can be evaluated by the diagnostic buffer, even after an extended period of time, to determine the cause of a STOP or to trace and allocate the occurrence of individual diagnostic events.
- Settings can be configured for the system diagnostics, such as a confirmation requirement for the message, for example.

When do you use it?

As soon as the system diagnostics has received the information on the system error that has occurred from the module, the messages are made available to the user in text form.

You can view the system error messages at any time, even during system operation.

Where can you find this?

You can view the system diagnostics messages in the following places:

- In the "Diagnostics" tab of the TIA Portal Inspector window.
- On the web server of the CPU
- On the CPU's own display
- In the diagnostic buffer of the CPU
- Using the "System Diagnostics Display" tool on an HMI visualization.

Additional information

Additional information on integrated system diagnostics can be found at:

- In the "SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16" manual > Section 11 "Editing devices and networks" > Section 2.4 "System diagnostics for S7-1500 PLCs (S7-1500)":
<https://support.industry.siemens.com/cs/ww/en/view/109773506>
- In the "SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16" manual > Section 11 "Editing Devices and Networks" > Section 2.1 "Hardware Diagnostics":
<https://support.industry.siemens.com/cs/ww/en/view/109773506>

- In the "SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro Diagnostics" function manual:
<https://support.industry.siemens.com/cs/ww/en/view/59192926>
- In the application example "System Diagnostics with S7-1500 and TIA Portal"
<https://support.industry.siemens.com/cs/ww/en/view/68011497>

3.1.4 System Diagnostics in the User Program

Description

A manufacturer-independent structure for data records with diagnostic information applies. A manufacturer-independent structure for data records with diagnostic information applies.

The commands in the TIA module library and the library from Siemens Industry Online Support make it easier for you to read the information from the data sets.

What do you get?

The following **commands** are available to help determine the system diagnostics of a device:

Table 3-1

Command	Description
RDREC	The command reads data records of a component of a DP slave / IO device, which can contain error information.
RALAM	When the diagnostic alarm OB (OB 82) is called, the command reads the start information of the OB and provides information on the cause and location of the error.
DPNRM_DG	The command reads the current diagnostic data of a DP slave (DP standard diagnostics).
GEN_DIAG	The command generates diagnostic information.
Gen_UsrMsg	The command generates a message that is entered in the diagnostic buffer.
GET_DIAG	The command provides diagnostic information.
GTE_NAME	The command reads out the name of an IO device
T_DIAG	This command provides diagnostic and status information for a connection.
RD_SINFO	The command reads the start information of the OB that was last called up and not yet processed completely, and of the startup OB that was last called. The command provides general error information
LED	The command reads the status of the LED of the module.
Get_IM_Data	The command reads the Information & Maintenance data of the CPU.
Transfer_IM_Data	The command transmits Information & Maintenance data to the CPU.
DeviceStates	This command outputs the status of all devices of an IO system.
ModuleStates	This command outputs the status of all modules of a device.

In the Siemens Industry Online Support you will also find a module library for PROFINET data sets.

You can execute the following functions with these **library modules**:

- Reading the device information:
 - Information about the interface, e.g., IP and MAC address
 - Information about the device interface, e.g., status, medium, name
 - Information about the link status of the interfaces, e.g., link down, link up
 - Information about the role of the device in MRP, e.g., client, manager
 - Information on port statistics, e.g., number of Bytes received
- Reading the MRP status
- Modification of the parameters of an analog input module of the ET 200SP at runtime, e.g., for deactivating and activating the channel diagnostics.

An application example for "Diagnostics in User Program with S7-1500" may be found in the Siemens Industry Online Support portal under the Article ID: 98210758. <https://support.industry.siemens.com/cs/ww/en/view/98210758>

Where can you find this?

The commands for diagnostics can be found in the TIA block library. The block library for PROFINET datasets can be found in the Siemens Industry Online Support under the Article ID: 109753067.

<https://support.industry.siemens.com/cs/ww/en/view/109753067>

What are the advantages?

Using the system diagnostics in the user program provides the following advantages:

- The program technology can be configured to dictate how the system should react to certain diagnostic messages.
- The user can specify how diagnostic messages are processed and visualized.
- It is not necessary to know the structure of the diagnostic datasets.

When do you use it?

You can call the commands and the library modules at any time in the user program and evaluate the result.

Note

Some commands work asynchronously, that is, they are called up over several sessions.

Additional information

Additional information about the commands for the system diagnostics can be found:

- In the Online Help to STEP 7
- In the manual "SIMATIC STEP 7 Basic/Professional V16 and SIMATIC WinCC V16":
<https://support.industry.siemens.com/cs/ww/en/view/109773506>
- In the "SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro Diagnostics" function manual:
<https://support.industry.siemens.com/cs/ww/en/view/59192926>
- In the programming manual "From PROFIBUS DP to PROFINET IO":
<https://support.industry.siemens.com/cs/ww/en/view/19289930>
- In the "PROFINET with STEP 7 V16" function manual:
<https://support.industry.siemens.com/cs/ww/en/view/49948856>
- In the application example "Diagnostics in User Program with S7-1500":
<https://support.industry.siemens.com/cs/ww/en/view/98210758>
- In the FAQ "How do you implement module and channel diagnostics in the user program of the SIMATIC S7-1200/S7-1500?":
<https://support.industry.siemens.com/cs/ww/en/view/109480387>

3.2 Diagnostics with SCALANCE

3.2.1 SCALANCE General Diagnostics

3.2.1.1 LED display

Description

All managed SCALANCE devices have an LED display on the housing for status and error indication. Depending on the status and error, one or more LEDs light up. Diagnostics using LEDs is the first tool for localizing errors.

What do you see?

To indicate the status and error, most SCALANCE devices have the following LEDs:

- LED "F": Display of the error status
- LED "RM": Display of the "Redundancy Manager" function
- LED "SB": Displaying the "Standby" function
- LED "DM": Display of the display mode
- LED "L1/L2": Display of the power supply
- LED "P": Port status display. The number depends on the device.
- LED "PoE": Display of the power supply via PoE.
- LED "R1/R2": Displays the status of the IWLAN interface. The LED "R2" is only available on devices with two IWLAN interfaces.

Table 3-2

LED	Meaning
F	The LED "F" indicates the error status of the device.
RM	The "RM" LED indicates whether the device is a redundancy manager and whether the ring is operating without errors.
SB	The "SB" LED indicates the status of the standby function.
DM	The LEDs "DM1" and "DM2" indicate which display mode is set. The LEDs "L1", "L2" and the port LEDs display different information depending on the display mode set.
L1 / L2	The LEDs "L1" and "L2" indicate whether the power supply L1 / L2 is connected. The meaning of the "L1" and "L2" LEDs depends on the set display mode.
P	The port LEDs "P1", "P2", etc., display information on the corresponding ports. The meaning of LED "P" depends on the set display mode.
PoE	The "PoE" LED indicates whether the device is supplied via "Power over Ethernet".
R1/R2	The LEDs "R1" and "R2" indicate the status of the IWLAN interface. The meaning of the LED "R1" or "R2" depends on the mode set.

What are the advantages?

When you evaluate the LEDs of the module, you have the following advantages:

- You can see the condition of your system directly on site. No PG / PC is required.

- Shorter downtimes of the plant. In the event of a fault or maintenance, you can take immediate action to correct the fault or the cause of the maintenance request.
- You can identify and eliminate potential faults at an early stage.

When do you use it?

You can evaluate the LEDs of the SCALANCE at any time, even during operation of the system.

Depending on the installation location, however, direct access to the device is not always possible. For this reason, Web Based Management offers a simulation display for the light emitting diodes. Unused ports are shown as grey LEDs.

Where can you find this?

You will find the LEDs on the front of the SCALANCE housing. The arrangement of the LEDs depends on the device.

Additional information

A detailed description of all LEDs and corrective measures can be found in the respective SCALANCE documentation.

3.2.1.2 Log table

Description

SCALANCE allows you to log events that occur, some of which you can define yourself.

The contents of the event log table are retained even after the power is turned off.

What do you see in the log table?

You can define which system events are to appear in the log table in Web Based Management (WBM) or via the Command Line Interface (CLI).

You can generate an entry in the log table for the following system events:

- Cold start, warm start
- Link Change
- Authentication error
- RMON alarm
- Switching the power supply
- Changes in the spanning tree, MRP / HRP ring status or error status
- Loop detection
- Diagnostics alarms
- Status change Standby, 802.1X port authentication or PoE
- Secure NTP

What are the advantages?

The log table provides the following added value:

- The entries in the log table are generated automatically.
- The events are readable in plain text. The errors can be localized quickly.
- All system events can be read in at a central location.
- Errors or events can still be evaluated by the log table even after a long time in order to determine the cause of an error or to be able to trace and assign the occurrence of individual diagnostic events.

When do you use it?

Theoretically, the log table in SCALANCE can be viewed at any time.

If SCALANCE signals an error, e.g., via the error LED, it makes sense to look in the log table. All events are displayed in text form in the log table.

Where can you find this?

You can find the log table in Web Based Management.

Additional information

A detailed description of the log table can be found in the corresponding configuration manual for SCALANCE.

3.2.1.3 Web Based Management

Description

Each managed SCALANCE has an integrated web server for Web Based Management (WBM). You can configure the device using Web Based Management, but you can also read diagnostic and status information.

What do you see in Web Based Management?

Which diagnostic and status information can be read from the Web Based Management of SCALANCE depends on the SCALANCE version used.

The diagnostic and status information of the SCALANCE XC-200 are selected as examples in this section. In the "Information" menu, numerous menu items can be found that provide the user with the following diagnostic and status information:

- Internal error.
- State of the redundancy protocols, e.g., whether the ring is open.
- Statistics counter of Ethernet Telegrams to detect overload situations.
- Temperature values from the switch and connected devices in order to quickly recognize overheating.
- Security settings.

The following table explains the menu items and their contents in detail:

Table 3-3

Menu	Meaning
Error	If an error occurs, the error is displayed on this page. Errors are indicated on the device by the red error LED illuminating. Internal errors of the device and errors that you have configured are reported.
Redundancy	<p>The page is divided into several tabs and displays the current information and states of the redundancy protocols.</p> <ul style="list-style-type: none"> • Register Spanning Tree: Here you can see current information and the settings of the root bridge. • Redundancy tab: Among other things, here you will see: <ul style="list-style-type: none"> - The device redundancy function. - The state (open/closed) of the ring. - The configured ring ports. • Standby: Among other things, here you will see: <ul style="list-style-type: none"> - Standby ports. - Standby function. - The status (active/passive) of the standby port. • Link Check: Here, you can see: <ul style="list-style-type: none"> - The ports on which the Link Check can be enabled. - The current status. - The statistics of sent and received Link Check Telegrams of the monitored connections.
Ethernet statistics	The switch keeps an internal statistics counter which counts the number of received data packets for each port.
Diagnostics	<p>This page displays the temperature values of internal and external modules of the device. The modules are only displayed if they provide temperature information.</p> <p>If the temperature value falls below or exceeds the displayed threshold values, the status changes accordingly. You can configure that you are informed by a message.</p>
Security	This page displays the security settings and local user accounts.

What are the advantages?

If you use Web Based Management, you have the following advantages:

- You only need a web browser to monitor the status of your module and your network. No special software is required on the PC.
- You can log on to Web Based Management at any time of day and from anywhere in the world via the company network or a corresponding dial-in option.
- You will find all the necessary information in the event of a fault clearly arranged and easy to grasp.
- To use Web Based Management, you must log on to the device. It is not possible for unauthorized users to gain access to the device.

When do you use it?

If sporadic problems occur in the network, the cause may be an overload situation, for example. Fast and simple diagnostics are possible with Web Based Management and Ethernet statistics. The information from the Ethernet statistics gives you an overview of data traffic and any network problems that may occur.

If you have designed your network redundantly and a fault occurs, communication is still ensured by the redundant connection. However, communication is only possible as long as the redundant connection is intact. You can use Web Based Management to monitor redundancy in your network and react if redundancy is no longer guaranteed in the event of a fault.

You can use Web Based Management to view the current operating temperature of your module. If the module is in a critical temperature range, you can be informed and react accordingly.

Where can you find this?

To open the Web Based Management of SCALANCE, enter the IP address or the URL of the device in the address field of the Internet browser. If a connection to the device exists, the login page of Web Based Management (WBM) appears.

Additional information

A detailed description of Web Based Management can be found in the corresponding configuration manual for SCALANCE.

3.2.1.4 SMTP Client

Description

The device offers the option of automatically sending an email if an alarm event occurs (to the network administrator, for example). The email contains the identification of the sending device, a description of the cause of the alarm in plain language, and a timestamp. This allows a simple central network monitoring for networks with few stations to be established using an email system. When an email event message is received, the WBM can be started by the internet browser, which uses the identification of the sender to read further diagnostic information. Configuration of up to three SMTP servers and the corresponding email addresses can be accomplished on this page.

What do you see with the SMTP client?

The following options are available in the overview:

- **SMTP Client**
Enable or disable the SMTP client.
- **Email address of the sender**
Enter the sender name to be specified in the email, for example, the device name. This setting applies to all configured SMTP servers.
- **Send test email**
Send a test email to test the configuration.

- **SMTP port**
Enter the port through which the SMTP server can be reached. Default setting: 25. This setting applies to all configured SMTP servers.
- **SMTP Server Address** – Enter the IP address, FQDN (Fully Qualified Domain Name), or host name of the SMTP server.

What are the advantages?

Use of the "SMTP-Client" function allows the user to react quickly to network faults. The service personnel receive a precise description of the origin, type, and time of the fault/alarm.

When do you use it?

To inform service personnel as quickly as possible about faults in the network, these events can be communicated by email.

Where can you find this?

The "SMTP-Client" function can be added in the Web Based Management of SCALANCE X.

3.2.1.5 Syslog Client

Description

In accordance with RFC 3164, Syslog is used for communicating short, unencrypted text messages over UDP in the IP network. This requires an accessible syslog server in the network.

The most important caveat when considering the use of any syslog system is that it must be routinely monitored by someone or something. Siemens provides a syslog server as part of the NMS solution SINEC NMS.

What do you see in the syslog client?

The following options are available in the overview:

- **Syslog Client**
Activate or deactivate the syslog function.
- **Address of the syslog server**
Enter the IP address, FQDN (Fully Qualified Domain Name) or host name of the syslog server.

What are the advantages?

If the "Syslog-Client" function is used, system events can be logged and saved centrally.

When do you use it?

All system events can be logged in a central server and thereby monitor the entire system.

Where can you find this?

The "Syslog-Client" function can be found in the Web Based Management of SCALANCE.

3.2.2 SCALANCE X Specific Diagnostics

3.2.2.1 Cable Tester for Copper Cables

Description

You can use cable testers to find errors at the cabling level. Nearly all the managed SCALANCE X devices offer an integrated cable tester for copper cables. With the cable tester, each individual Ethernet port can perform independent fault diagnostics on the cable. This test is performed without the cable being disconnected, a cable tester connected and a loopback module installed at the other end.

What will you learn from this test?

If you use the integrated cable tester, you can locate short circuits and line interruptions to within a few meters. You can view the test result in Web Based Management.

The tester can return the following result statements:

- The status of the line, e.g., "Short circuit", "OK".
- The distance to the open cable end, cable break, or short circuit in meters.

Note

The test is only allowed if no data connection is established on the port to be tested. If there is a data connection on the port to be tested, the connection is briefly interrupted.

What are the advantages?

If you use the integrated cable tester, you do not need any additional software or hardware. The cable tester is integrated in the SCALANCE.

When do you use it?

If you detect faults in the network, the cause of the fault may also be on the physical layer.

A fault in the network can manifest itself as follows:

- Defective performance
- Incorrect data packages
- Sporadic interruptions
- Complete breakdown

You can use the integrated cable tester to diagnose and eliminate errors at the cabling level.

Where can you find this?

You will find the integrated cable tester in the Web Based Management of SCALANCE.

Additional information

Additional information on the cable tester can be found in the corresponding SCALANCE X configuration manual.

3.2.2.2 Cable Tester for Optical Fibers

Description

If transmission errors occur with optical lines, the cause of the problem will generally not be obvious. The problem can be the transmitter, the receiver, or the transmission path.

In many cases SCALANCE can help you with the diagnostics. The plug-in transceivers provide valuable information for troubleshooting.

With the SFP diagnostics integrated in the SCALANCE, you carry out an independent fault diagnostics for each individual SFP port. This test is performed without a cable being disconnected, a cable tester connected and a loopback installed at the other end.

What will you learn from this test?

If you use the SFP, SFP+, SCP or STP plug-in transceivers, the plug-in transceivers provide you with important information. You can read this information with the integrated SFP diagnostics.

The SFP diagnostics provides you with the current operating data, the lower limit and the upper limit for each plug-in transceiver.

The current operating data consists of the following values:

- The nominal bit rate of the SFP port.
- The port temperature.
- The voltage applied to the port.
- The power supplied to a device on this port.
- The reception and transmission power of the port.

You can read the result of the SFP diagnostics in Web Based Management. If you compare the current operating data with the permissible limits, you can determine whether you should rather check the lines and connectors or the transceivers in the event of a fault in an optical transmission path. The operating temperature of the plug-in transceiver can be an important indication of thermal problems of the network component.

What are the advantages?

If you use SFP diagnostics in the event of interference in an optical transmission path, you have the following advantages:

- You do not need any additional software or hardware. SFP diagnostics is integrated in SCALANCE.
- You can limit the error. If the current operating data of the plug-in transceiver are within the normal range, then the cause of the error could be in the line.

When do you use it?

If you detect faults in the network, the cause of the fault may also be on the physical layer.

A fault can manifest itself as follows:

- Defective performance
- Incorrect data packages
- Sporadic interruptions
- Complete breakdown

You can use the integrated SFP diagnostics to diagnose and limit faults at the cabling level for optical fibers.

Where can you find this?

You can find the integrated SFP diagnostics in the Web Based Management of SCALANCE.

Additional information

Additional information on SFP diagnostics can be found in the corresponding SCALANCE X configuration manual.

3.2.2.3 FMP Diagnostics

Description

To monitor an optical path, you can use the Fiber Monitoring Protocol (FMP). This function continually monitors the transmission and reception power of an optical port. An alarm is triggered as soon as the temperature falls below the limit values.

What you will receive with the FMP diagnostics?

Fiber monitoring allows you to monitor reception power and power loss on optical links between two switches.

If the value of the received power or the amount of the power drop exceeds or falls below the set limit values, an event is triggered. You can set limits in two steps for messages with the severity levels "Warning" and "Critical".

What are the advantages?

If you use FMP diagnostics, you have the following advantages:

- You do not need any additional software or hardware. FMP diagnostics is integrated in SCALANCE X.
- You can continually monitor your optical path and detect fiber breaks or fiber degradation at an early stage.

When do you use it?

If you detect faults in the network, the cause of the fault may also be on the physical layer.

A fault can manifest itself as follows:

- Defective performance
- Incorrect data packages
- Sporadic interruptions
- Complete breakdown

You can use the integrated FMP diagnostics to detect errors on an optical path at an early stage and to be warned of deviations.

Where can you find this?

If your SCALANCE X device supports FMP diagnostics, you can find the integrated FMP diagnostics in the Web Based Management of SCALANCE X.

Additional information

Additional information on FMP diagnostics can be found in the corresponding SCALANCE X configuration manual.

3.2.2.4 Loop Detection

Description

A loop is an error in the network structure. In most situations, a network loop causes the network to come to a complete standstill because the network is overloaded by the high flood of multicast and broadcast packets. Due to the high network load, the diagnostics is also severely impeded.

"Loop Detection" is a proprietary protocol from SIEMENS that resolves local loops in a network. To resolve network loops, the function specifically switches off ports of a switch on which a loop has been detected.

What will you learn from the "Loop Detection"?

You can use the "Loop Detection" function in Web Based Management to specify the ports for which loop detection is to be activated. The user should specify how the port should react in the event a remote loop occurs.

The following options are available for selection:

- No action: A loop has no effect on the port.
- Deactivate: The port is blocked.

When a port is blocked in the SCALANCE X, the corresponding "P" LED flashes on the device housing.

You will also see a corresponding entry in the log table.

Note

The "Loop Detection" function is not a redundancy protocol. Ports that have been blocked by this function must be reactivated manually using the switch's Web Based Management.

What are the advantages?

If you use the "Loop Detection" function, you can find and correct the error more quickly.

When do you use it?

You can use the "Loop Detection" function to protect your network from local and remote loops.

Note

"Loop Detection" is a proprietary protocol from SIEMENS and is only supported by SCALANCE devices.

To detect loops, test frames are sent from the switches. The test frames create an additional network load.

Where can you find this?

You can find the "Loop Detection" function in the Web Based Management of SCALANCE X.

Additional information

Additional information on the "Loop Detection" function can be found in the corresponding configuration manual for SCALANCE X

3.2.2.5 Port Mirroring

Description

If you want to record network traffic on an Ethernet hub, you can use your analyzer to hang on any port on the hub. The hub forwards all incoming data frames to all ports.

A switch, on the other hand, forwards a data packet only to the port where the target device is located. To record traffic from a switch port, the analyzer should be plugged into the port to which the target device is already connected. The problem is that only one device can hang on a switch port. To solve this problem, all managed SCALANCE X devices have the "Port Mirroring" function.

With port mirroring, all traffic that passes through one switch port is mirrored to another switch port. This allows the target device to remain plugged into the original port and the analysis device—e.g., a PC with Wireshark—to be connected to the monitor port.

What do you see during the port mirroring?

The "Port Mirroring" function maps the data traffic of one port (mirror port) to another port (monitor port). You can then analyze the data traffic at the monitor port without feedback.

You can make the following settings for each mirror port:

- The incoming and outgoing data traffic is copied.
- Only incoming traffic is copied.
- Only outgoing traffic is copied.

Note

If your switch is VLAN-enabled, the monitor port should not be used in any VLAN. Mark the monitor port in all VLANs with "-".

What are the advantages?

If you use the "Port Mirroring" function, you can record and analyze the data traffic that passes through a switch port using an analysis tool.

When do you use it?

If you want to record and analyze the data traffic or the network load at a specific switch port with an analysis tool, then use the "Port Mirroring" function.

Where can you find this?

You can find the "Port Mirroring" function in the Web Based Management of SCALANCE X.

In Web Based Management, you can select the original port and the mirror port. The mirror port is only used for analysis purposes at times.

Additional information

Additional information on the "Port Mirroring" function can be found in the corresponding SCALANCE X configuration manual.

3.2.3 SCALANCE W Specific Diagnostics

3.2.3.1 Signal Recorder

Description

The SCALANCE W components have an integrated signal recorder. The signal recorder records the signal strength of the access point and other connection data on the IWLAN client side. The signal recorder is a helpful tool for obtaining initial information about the connection quality and the illumination of a system, as well as for finding possible optimization possibilities.

The "Signal recorder" function is only available in client mode.

What do you see with the signal recorder?

You can use the signal recorder to record the effective useful signal between the access point and the client. This data helps you to find the areas with insufficient useful signal.

The measurement result can be viewed in Web Based Management.

In Web Based Management, the measurement result is divided into two areas:

- The "Client" section shows the measurement of the client.
- The "Access Point" area represents the measurement of the access point to which the client is currently connected.

Both areas contain two figures with additional information, e.g., signal strength, noise floor, and roaming.

What are the advantages?

If you use the signal recorder, you have the following advantages:

- With the signal recorder you can obtain initial information about the connection quality and the illumination of a system.
- You can save the measurement results as a PDF file. The PDF file contains a graphical representation of the course of the effective useful signal in dBm and the course of the data rate in Mbps.

When do you use it?

You use the signal recorder when planning your WLAN channel.

In order to obtain a meaningful recording of the signal, it is necessary to plan the signal recorder recording in advance. Among other things, the following questions need to be clarified:

- Is it a static or a mobile application?
- Where can the IWLAN clients be located in the system?
- Which critical points (shielding, sources of interference,...) are in the system?
- Is the system already in full operation during the test run (from a technical radio point of view)?

The signal recorder can be used particularly advantageously if the client is moving along a fixed path.

Where can you find this?

You can find the integrated signal recorder in Web Based Management for SCALANCE W.

Additional information

For additional information on the signal recorder, see:

- In the configuration manual for SCALANCE W.
- In the FAQ "What information can you obtain from the signal recorder of the SCALANCE W components?"
<https://support.industry.siemens.com/cs/ww/en/view/109470655>

3.2.3.2 Spectrum Analyzer

Description

When designing a WLAN system in Industry, an interference-free channel is a basic requirement for robust communication.

If there is interference present in the WLAN, the cause may be that other systems besides the WLAN devices also transmit on the same frequency as the WLAN. The "Spectrum Analyzer" analysis tool can be used to detect errors or analyze problems. The spectrum analyzer is used to acquire and display a signal in the frequency domain.

The SCALANCE W access points, as of firmware V5.2, have an integrated spectrum analyzer.

What do you see with the spectrum analyzer?

If you use the integrated spectrum analyzer, you can recognize and display electromagnetic signals of a frequency range. You can measure the strength of all signals in the vicinity of the access point. The measurement result can be viewed in Web Based Management.

The measured values of the spectrum analysis are recorded in three output windows:

- The maximum values, the current values and the average values of the received signal strength in dBm are displayed in the "Realtime" output window. This helps you to diagnose faults at different positions.
- In the "Spectrogram" output window, the time course is displayed in the form of a waterfall diagram of the first display. The spectrogram displays the received signals in a complete system.
- The output window "Density Chart" shows the percentage signal strength depending on the dBm value.

What are the advantages?

Use of the spectrum analyzer provides the following advantages:

- Spectrum analysis can be used to identify the causes and effects of WLAN interference.
- To evaluate the result of the spectrum analysis, save the absolute dBm values of the last recording as a CSV file.

When do you use it?

You use the spectrum analyzer when planning your WLAN channel. With the spectrum analyzer you can determine whether the channel is free or disturbed by other systems.

Note

If you activate the spectrum analyzer, all connected clients lose connection to the access point as long as the signal analyzer is running.

Where can you find this?

You can find the integrated spectrum analyzer in the Web Based Management of the SCALANCE W Access Point.

Additional information

You can find additional information about the spectrum analyzer:

- In the configuration manual for SCALANCE W.
- In the FAQ "What information does the spectrum analyzer of a SCALANCE W Access Point provide?"
<https://support.industry.siemens.com/cs/ww/en/view/109483544>

3.2.3.3 Monitoring Overlapping Access Points

Description

For optimum data throughput, it is important that the set wireless channel is not used by other access points. An access point not only occupies the set channel, but also the adjacent 2–3 channels. Adequate channel spacing to neighboring access points should therefore be ensured. The associated WBM page shows all access points that are visible on the set or adjacent channels. If there are entries here, the maximum data throughput of the access point and the availability of the communication link to the access point is potentially affected.

What do you see on the WBM page "Overlap AP"?

The following options are available in the overview:

- Radio interface
Displays the available WLAN interfaces in this column.
- Type
Displays the operating mode of the WLAN interface.
- SSID
Displays the SSID of the Access Point.
- BSSID
Displays the MAC address of the access point.
- System name
Displays the system name of the SCALANCE W unit. The entry depends on the access point. Not all access points support this parameter.
- Channel
Displays the channel through which the client communicates with the access point.
- Signal strength [dBm]
Displays the signal strength of the client in dBm.
- Signal strength [%]
Displays the signal strength of the client in a percentage.
- Age [s]
Displays the time that has passed since the last activity of the access point.
- Security
Displays which authentication method is used.
- Wireless mode
Displays the transmission standard.

What are the advantages?

Use of the "Overlap AP" function can allow recognition and elimination of potential traffic interference

When do you use it?

For example, if there are problems with data throughput in the network, check whether access points are interfering with each other.

Where can you find this?

The "Overlap AP" function can be found in the Web Based Management of SCALANCE W.

4 Diagnostics with External Tools

If the cause of an error cannot be clearly determined with the on-board means of the module, external tools can help you in your search.

4.1 Wireshark

Description

Wireshark is a network analyzer and is installed on a PC. With this tool, network packets that are sent to and received by any local interface can be recorded over a period of time. The recording can be analyzed and evaluated via a graphical interface.

Wireshark has powerful filter functions. The filters are mainly used to limit the expected data volume and analysis to the ports or protocols to be examined.

What do you see with the "Wireshark"?

Wireshark records all data traffic on a local interface of your choice. The recording appears in a graphical interface. You can follow the recording live there. To ensure an optimal overview, the scanned packets are displayed in different colors depending on the protocol.

If you select a specific package in the recording, the selected package is displayed in more detail in Wireshark.

Wireshark's graphical interface consists of several areas. The most important areas are:

- In the "Filter Bar" you can define filter rules which type of traffic should be shown or hidden in the packet list.
- The "Package List" shows the live recording of the imported data packages. In addition to consecutive numbering, a timestamp relative to the beginning of the recording, the source and the destination address, the protocol to which the respective packet belongs is displayed here.
- In the "Package Details" section, the selected package is broken down into its components and analyzed.
- In the "Bytes" area, you see the package in its raw form as a hex and ASCII dump.

What are the advantages?

If you use the Wireshark tool, you have the following advantages:

- You can conveniently record and analyze the entire data traffic.
- The user can specify when the recording will automatically be ended and how the data is to be recorded.
- Wireshark offers the possibility to set filters, e.g., network protocol, source and destination address or TCP port. If a filter is set, it ensures that the data that must be evaluated later remains a manageable size.
- Wireshark offers a wide range of analysis and statistics functions.
- The recording can be saved in a file and given to a specialist for evaluation, for example.

When do you use it?

Use the Wireshark tool to detect any network and security problems. Recording the data packets can be useful when troubleshooting or evaluating the communication content.

Wireshark can also be used to test the function of a software, e.g., whether the activated encryption works.

Wireshark is a vital tool for monitoring which devices in the network are sending and receiving data. The network analyzer logs and analyzes all data traffic. This enables you to determine whether an IP address unknown to you is causing interference or is communicating without permission.

Note

Before using Wireshark for network analysis, check whether the use of the tool is allowed in the network environment or whether data protection regulations have to be considered.

Intercepting connections and storing, using, or passing on the data read along may be punishable under certain circumstances.

Where can you find this?

The Wireshark analysis tool is "open source" software and can be downloaded free of charge from the Internet.

Additional information

Additional information about the Wireshark tool can be found on their homepage <https://www.wireshark.org/>

4.2 Remote Capture

Description

Wireshark allows you to record network traffic on the local interface. With the function "Remote Capture" Wireshark can also read data traffic from remote interfaces.

The SCALANCE W devices support the "Remote Capture" function from firmware V6.1 (CLI) and from V6.2 (WBM and CLI). You can use the "Remote Capture" function to record network traffic from remote interfaces at the access point using Wireshark.

What do you see with the "Remote Capture"?

If you have activated the "Remote Capture" function in SCALANCE, the remote interface can be integrated into Wireshark. Wireshark records the data traffic flowing through the interface over a period of time. You can then view the contents of the frames from the recording or filter them according to specific contents.

What are the advantages?

If you use the "Remote Capture" function, you have the following advantages:

- You can use the Remote Capture function to record network traffic from remote interfaces at the access point using Wireshark.
- The function can be activated at several interfaces simultaneously.
- No special hardware, e.g., a TAP, or certain tools, e.g., AirPCap, is required.
- The SCALANCE W Client can be located at a remote location.

When do you use it?

To analyze transmission errors or the network load at remote interfaces at the access point, use the "Remote Capture" function.

Note

If the "All Traffic" option is activated at the access point, all connected clients lose the connection to the access point as long as the recording is running.

Note

Before using Wireshark for network analysis, check whether the use of the tool is allowed in the network environment or whether data protection regulations must be considered.

Intercepting connections and storing, using, or passing on the data read along may be punishable under certain circumstances.

Where can you find this?

To enable Wireshark to record network data from the remote SCALANCE W, you must activate the "Remote Capture" function in SCALANCE W via the Command Line Interface or Web Based Management and configure a "Remote Capture" interface in Wireshark.

Additional information

For additional information on the "Remote Capture" function, see:

- In the configuration manual for SCALANCE W.
- In the FAQ "How do you record the network traffic on the SCALANCE W with Wireshark?"
<https://support.industry.siemens.com/cs/ww/en/view/109750887>

4.3 SIMATIC Assessment Suite

Description

The "SIMATIC Assessment Suite" tool enables you to collect diagnostic and system information for service, support and maintenance from a local system or from systems in the network. This diagnostic and system information is stored in system-specific archives.

What do you learn with the SIMATIC Assessment Suite?

If you want to read the log files of the installed SIMATIC software from a computer, you can use the "SIMATIC Assessment Suite" tool. The tool collects the LOG files of the installed software and archives the collected information in a ZIP format.

What are the advantages?

If you use the "SIMATIC Assessment Suite" tool for diagnostics, you have the following advantages:

- Collect a wide range of diagnostic and system information.
- Collect with one "click". The time-consuming, manual collection of diagnostic and system information per system is no longer necessary.
- No installation required.
- Once created, configurations can be saved and reused.
- Configurations can be passed on.
- Diagnostic and system information of all configured systems is available centrally on one computer after one run.

Where can you find this?

The tool can be found via the following article:

<https://support.industry.siemens.com/cs/ww/en/view/65976201>

4.4 PRONETA

Description

The PROFINET network analyzer PRONETA is a simple tool for fast analysis and configuration of PROFINET networks and for simple testing of decentral ET 200 peripheral systems and other components. It is particularly suitable for basic tasks for commissioning PROFINET systems.

What do you learn with PRONETA?

PRONETA is divided into two parts and consists of the following components:

- Network analysis
- I/O test

The "network analysis" gives you an overview of the devices connected to PROFINET.

The "network analysis" has simple configuration options. For example, the user can set the network parameters of a device or assign the network names to the devices. However, "network analysis" also has powerful mechanisms for comparing several network topologies.

You can use the "I/O test" to test the I/O wiring of a system with numerous decentralized peripheral devices. The "I/O test" checks the wiring and automatically generates a protocol of the test procedure. You can export this log for documentation purposes.

What are the advantages?

If you use the "PRONETA" tool, you have the following advantages:

- Free download from the SIEMENS support websites.
- Allows configuration of networks in early project phases before a CPU is installed in the network.
- No additional hardware or software required.
- No installation required.
- Support of PROFINET devices from all manufacturers.
- I/O test that supports numerous SIMATIC ET 200 peripheral modules.
- Support of project files from STEP 7 V5.4, 5.5 and 5.6.

Where can you find this?

The tool can be found via the following article:

<https://support.industry.siemens.com/cs/ww/en/view/67460624>

4.5 SINEC NMS

Description

The SINEC NMS software is a Network Management System for monitoring and managing industrial networks. It enables the user to fully visualize and monitor networks. Additionally, SINEC NMS also offers the possibility to configure the network infrastructure. Using the rule-based approach, cross-device configurations can be made independent of device types on the network, and regular backups of device configurations can be made to keep track of configuration changes. Another important point is the central function for a firmware update in the network infrastructure.

Occurring errors are reported to SINEC NMS and can be directly forwarded to the service personnel.

How can you use SINEC NMS for diagnostic purposes?

Industrial networks are complex and errors on PROFINET devices can be difficult to locate and correct in large networks. SINEC NMS collects the PROFINET diagnostics and archives the diagnostic data of all monitored PROFINET devices centrally. Diagnostic states are reported as events, assigned to the corresponding devices, and highlighted in color in the device list and topology.

What are the advantages?

Using SINEC NMS offers the following advantages:

- Quick and easy fault localization
- Exact status overview for fast response in the event of an error
- Maximum transparency by structuring the network
- Reliable diagnostics thanks to central evaluation of the network load

When do you use it?

With SINEC NMS industrial networks, tens of thousands of stations can be monitored, managed, and configured centrally and around the clock. This simplifies device diagnostics many times over.

Where can you find this?

The software can be downloaded from Siemens Industry Online Support. The license for the software can be obtained from the Siemens Industry Mall.

5 Diagnostics with Network Protocols

The advent of "intelligent devices" has changed the diagnostic strategy, as Managed Devices provide a wealth of information about standard protocols, e.g., SNMP, communication quality, or Topology. These can be actively read from the devices network-wide at runtime. Powerful tools are available for this.

5.1 SNMP

Description

The Simple Network Management Protocol (SNMP) is a UDP/IP-based, open protocol based on the client/server model.

SNMP allows the user to monitor and control network components such as routers or switches from a central station. SNMP distinguishes between an SNMP agent (client function) and an SNMP manager (server function).

The role of an SNMP agent can usually be assumed by any network device to be managed, e.g., routers, switches. The role of the SNMP manager is usually assumed by a universal, centrally accessible computer in the network.

An important component of SNMP is the Management Information Base (MIB). All SNMP agents have a large number of variables, the SNMP objects. All SNMP objects of an agent are collected in its MIB and logically structured. The SNMP objects provide information about the status of the user's resource, e.g., IP address and firmware version, or it can be described with new parameters, e.g., configuration parameters.

Each SNMP-enabled network component is delivered with a collection of standard MIBs. If component-specific, non-standardized data is required for network monitoring, then these special SNMP objects can be described in the "Private MIB" of the manufacturer.

You achieve this with SNMP?

SNMP offers read and write access. With the read access you have the possibility to query the value of an SNMP object from the SNMP agent. With the write access you describe an SNMP object in the SNMP agent with a new value.

These two types of access enable you to perform the following management functions with SNMP:

- Monitor network components.
- Diagnose network components.
- Detect and inform of errors.
- Remote configuration of network components.

There are the following ways to read or write to an SNMP agent using SNMP:

- You can connect to the SNMP agent using SNMP manager software (also called MIB browser). You can then browse through the MIB and read and write values. To browse through the MIB objects, the private MIB of the SNMP agent must be imported into the MIB browser.
- There are numerous SNMP management systems that provide support with the mentioned management functions, e.g., SINEC NMS. After installation and configuration, the system works autonomously.
- To make a CPU SNMP-enabled, use the SNMP blocks from Siemens Industry Online Support. These modules simulate the SNMP protocol and take on the role of the SNMP manager.

What are the advantages?

If you use SNMP, you have the following advantages:

- SNMP is an open protocol supported by many manufacturers.
- The SNMP protocol is widely used in Ethernet networks.
- Many different network components are supported, e.g., switches, routers, and controllers.
- The standardized MIBs and SNMP access mechanisms allow heterogeneous networks to be optimally monitored and controlled.
- With SNMP, event-triggered communication via traps is also possible. This means there is little network load due to SNMP communication.
- Common SNMP management systems help you to diagnose and optimize networks.

When do you use it?

SNMP is used to control networks and their components.

These include, for example, the following areas of application:

- Detect individual network components.
- Reconfigure devices by changing SNMP objects.
- Determine the entire network topology.
- Identify significant problem situations.
- Alert and alarm management.
- Network analysis and monitoring.
- Edit errors.
- Distribute software (installation and configuration).
- Modify network topology.

Common SNMP management systems, e.g., SINEC NMS, help provide diagnostics and optimize networks. The software SINEC NMS was developed specifically for industrial applications. To analyze and observe networks in an automation environment, SINEC NMS is the ideal tool. The collected data is stored in a long-term archive and can, therefore, be evaluated and displayed as required.

Note

Only use the secure variant SNMP v3 and change the insecure variant SNMP v1/2 at least to "ReadOnly" in the configuration of the switch.

Where can you find this?

SNMP is implemented in all SIMATIC modules and managed SIMATIC NET devices.

For some SIMATIC NET devices, you must explicitly enable SNMP communication during project planning.

Managed SCALANCE devices have a private MIB. To use the Private MIB file independently of the device (e.g., to open the MIB file with an MIB browser), the file must first be saved outside the SCALANCE. The Private MIB can be downloaded and saved via the Web Based Management of SCALANCE.

Additional information

Additional information about SNMP can be found:

- In the configuration manual for SCALANCE X
- In the diagnostic manual "SIMATIC NET: Network Management Diagnostics and configuration with SNMP"
<https://support.industry.siemens.com/cs/ww/en/view/103949062>
- In the FAQ "How do you find examples, explanations and additional information about SNMP and the SIMATIC NET SNMP OPC server?"
<https://support.industry.siemens.com/cs/ww/en/view/18621775>
- In the FAQ "MIB (Management Information Base) at SNMP"
<https://support.industry.siemens.com/cs/ww/en/view/15177711>
- In the FAQ "Downloading the Private MIB (Management Information Base) V4.2 and SNMP OPC Profile V1.3 and the PROFINET GSDML File V2.2 for SCALANCE W-700"
<https://support.industry.siemens.com/cs/ww/en/view/35842319>
- In the FAQ "AutomationMIB now available for Download in Version V02.00.00.02"
<https://support.industry.siemens.com/cs/ww/en/view/67637278>
- In the application example "Diagnostics and Control of Network components with SIMATIC S7 PN-CPU's using SNMP"
<https://support.industry.siemens.com/cs/ww/en/view/57249109>
- In the application example "Getting Started: Understanding and Using SINEC NMS"
<https://support.industry.siemens.com/cs/ww/en/view/109762792>

The "SINEC NMS" Network Management System is available from Siemens Industry Online Support at

<https://support.industry.siemens.com/cs/ww/en/view/109776939>

5.2 RMON

Description

SNMP lacks the ability to analyze communication relationships, e.g., communication partners, protocols used, and data streams. Remote Monitoring (RMON) is an adequate solution for better evaluating the status of a network, e.g., load, logical errors, protocol errors, and archiving the corresponding information.

RMON is one of the most important extensions of SNMP management. The RMON MIB is an extension of the SNMP MIB and defines the most important indicators for Ethernet networks. This supports comprehensive error diagnostics and statistics functions that enable the network operator to monitor network performance and make network expansions as easy as possible.

You can read the RMON data from an SNMP agent from an SNMP manager via SNMP.

What do you learn with RMON?

RMON is a tool for data collection. RMON collects all Ethernet diagnostic data in the device, prepares it and makes it available in the form of tables. To organize the abundance of data, the RMON-MIB is divided into nine groups:

- The statistics group contains information about usage and error statistics. The number of packets sent, packet size, broadcasts, multicasts, network errors and collisions are recorded.
- In the history group, trend analyses of usage are created based on information from the statistics group.
- In the alarm group, the user can configure alarms for each managed device. Separate alarm levels can be set for the values recorded by the RMON agent.
- In the event group, rising and falling threshold values can be recorded and triggered for each event accordingly.
- The host group consists of a statistics table based on the MAC addresses. There are counters for broadcast, multicast and error packets as well as for the number of Bytes.
- The HostTopN group contains ordered host statistics.
- In the traffic matrix group, the user and error information is displayed in matrix form in relation to a send and receive address.
- The Filter group gives the network administrator tools to set filters to select certain packages on the network.
- The Packet Capture Group is an extension of the filter group and allows a flexible definition of trace buffers that are filled according to the currently set filters.

The SCALANCE devices support the RMON groups "Statistics" and "History". For each port, you can specify whether statistical data is to be collected and, if so, how many samples in which interval.

You can view the RMON history in the Web Based Management of SCALANCE.

What are the advantages?

If you use RMON, you have the following advantages:

- RMON is based on SNMP and is supported by many manufacturers.
- You can collect statistical data in network-compatible devices and store it in databases.
- RMON includes network performance data in all 7 layers of the OSI model.
- RMON configurations can be used just as advantageously in routed site LANs as in LAN-WAN networks.

When do you use it?

The diagnostic data, e.g., the port-related load curves, enable the user to detect and eliminate problems in the network at an early stage.

The RMON History group offers the option to read historical data from the switch after a fault. In this group, counting processes are registered, which can give conclusions about the use in a certain time interval and for certain data types.

In Web Based Management of SCALANCE, you can activate RMON for individual ports.

Where can you find this?

RMON is implemented in all managed SCALANCE X devices.

Additional information

Additional information on RMON can be found in the configuration manual for SCALANCE X.

5.3 Ping

Description

You can use the ping command to test the function of a network connection.

By default, Ping sends four packets to the specified device and lists the answers with a small statistic.

The program is usually executed as a console command.

What do you learn from the ping?

You can use the ping to check whether a device is accessible in a network. Ping sends an ICMP packet to the destination address of the device to be checked (echo request). The receiver must, if it supports the protocol, send back a reply (echo reply).

The tool measures the time between echo request and echo reply and displays the time span as output.

If the destination device is not reachable, the message "Network unreachable" or "Host unreachable" is displayed as the response.

Note

It cannot be concluded from a missing response whether the remote station is unreachable because some devices, such as the firewall, are configured to ignore and discard ICMP packets.

What are the advantages?

When you use the Ping tool, you have the following advantages:

- The network connection can be easily checked.
- The ping command is simple and requires no special administrative knowledge.
- The ping command can be operated via a console.

When do you use it?

With the ping test you can check the connection to a web page, your local network or another network device.

After you have connected a network device to your network, it is helpful if you check with a PC and the Ping tool whether the network device is accessible in the network.

If you do not receive a response from the target device, there may be an error in the network connection.

Where can you find this?

The program is included in the scope of delivery of every common operating system.

6 Appendix

6.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

<https://support.industry.siemens.com/>

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:

www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

www.siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

<https://support.industry.siemens.com/cs/sc>

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for Apple iOS, Android and Windows Phone:

<https://support.industry.siemens.com/cs/sc>

6.2 Links and literature

Table 6-1

No.	Subject
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/21566216
\3\	Application example "Diagnostics Overview for SIMATIC S7-1200 and S7-1500". https://support.industry.siemens.com/cs/ww/en/view/109752283

6.3 Change documentation

Table 6-2

Version	Date	Change
V1.0	10/2007	First version
V2.0	08/2018	Complete revision
V2.1	11/2018	Title and content modified
V2.2	06/2020	Addition of new diagnostics options