

# SIEMENS

## SIMATIC NET

### Industrial Ethernet / Wireless HART IE/WSN-PA Link

#### Operating Instructions

---

#### Preface

---

Product description

1

---

Setting up network structures

2

---

Installation and  
commissioning

3

---

Configuration of the Link

4

---

Diagnostics

5

---

Service and maintenance

6

---

Technical specifications

7

---

Approvals and certificates

8

---

Biological compatibility

A

---




References

B

## Legal information

### Warning notice system

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

 <b>DANGER</b>
indicates that death or severe personal injury <b>will</b> result if proper precautions are not taken.
 <b>WARNING</b>
indicates that death or severe personal injury <b>may</b> result if proper precautions are not taken.
 <b>CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.
<b>NOTICE</b>
indicates that property damage can result if proper precautions are not taken.


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

### Qualified Personnel

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

### Proper use of Siemens products

Note the following:

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

### Trademarks

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

### Disclaimer of Liability

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

# Preface

## Validity of the Operating Instructions

These operating instructions are valid for the following versions of the IE/WSN-PA Link:

- Hardware product version 01
- Firmware version 4.4.45

## Device variants

The following variants of the IE/WSN-PA Link are available:

Device variant	Order number
IE/WSN-PA Link with integrated antenna	6GK1 411-6CA40-0AA0
IE/WSN-PA Link with redundancy function and connector for integrated antenna *	6GK1 411-6CA40-0BA0

\* An external antenna is available as an accessory, see section Accessories for the device variant with connector for external antenna (Page 16).

## Terms and abbreviations/acronyms used

- Link  
In this document, the name "Link" is used in place of the full product name "IE/WSN-PA Link".
- Field device  
The term "field device" is used for a WirelessHART sensor, a WirelessHART transducer or other WirelessHART field device.
- WSN (Wireless Sensor Network)  
WirelessHART network

## Documentation of the link

The documentation for the link device consists of the following parts:

- Operating instructions  
It ships with the product as a PDF on the data medium.  
The operating instructions contain the information you require for commissioning, configuring and operating the IE/WSN-PA Link.
- Compact operating instructions  
It ships with the product in printed form.  
The compact installation instructions describe how the Link is installed and connected up.

## New in this release

- New firmware version with the following functions:
  - Improved access protection with configurable passwords
  - Remote access to recording of the system activity (SysLog)
  - Errors corrected
- Editorial revision

## Replaced documentation

This manual replaces the manual edition 12/2012.

## Current manual release and further information on the Internet

You will also find the current version of this manual and other information on the product on the Internet pages of Siemens Automation Customer Support under the following entry ID:

39971776 (<http://support.automation.siemens.com/WW/view/en/39971776>)

There select the required information under "Entry type" (for example "Updates", "Manuals", "FAQs", "Download" etc.).

## License conditions

---

### Note

#### Open source software

The product contains open source software

Read the license conditions for open source software carefully before using the product. The acceptance of the disclaimers of liability and warranty it contains is a clear precondition of the use of open source software.

You will find license conditions in the document "Readme\_OSS\_74.pdf" on the supplied data medium with the product documentation.

---

## Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit <http://www.siemens.com/industrialsecurity>.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit <http://support.automation.siemens.com>.

## SIMATIC NET glossary

- You will also find the current version of the SIMATIC NET glossary on the Internet using the following entry ID:  
50305045 (<http://support.automation.siemens.com/WW/view/en/50305045>)
- You will find the product-specific glossary in the Appendix of this manual.

## Service & Support

In addition to the product documentation, the comprehensive online information platform of Siemens Automation Customer Support supports at any time and at any location in the world. You will find the Service & Support pages on the Internet at the following address:

(<http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo2&aktprim=99&lang=en>)

Apart from news, you will also find the following information there:

- Product information, Product Support, Applications & Tools
- Technical Forum
- Technical Support - Ask the Siemens experts
- Our service offer:
  - Technical Consulting, Engineering support
  - Field Service
  - Spare parts and repairs
  - Maintenance, optimization, modernization and more

You will find contact data on the Internet at the following address:

(<http://www.automation.siemens.com/partner/guiwelcome.asp?lang=en>)

## **SITRAIN - Siemens training for automation and industrial solutions**

With over 300 different courses, SITRAIN covers the entire Siemens product and system spectrum in the field of automation and drive technology. Apart from the classic range of courses, we also offer training tailored for individual needs and a combination of different teaching media and sequences, for example self-learning programs on CD-ROM or on the Internet.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address:

[www.siemens.com/sitrain](http://www.siemens.com/sitrain)

# Table of contents

	<b>Preface .....</b>	<b>3</b>
<b>1</b>	<b>Product description .....</b>	<b>11</b>
1.1	Functions and properties .....	11
1.1.1	Functions of the Link .....	11
1.1.2	Hardware interfaces .....	14
1.1.3	Housing .....	14
1.2	Components of the product and accessories .....	15
1.2.1	Components of the product .....	15
1.2.2	Accessories for attachment to Industrial Ethernet .....	15
1.2.3	Accessories for the device variant with connector for external antenna .....	16
1.3	Application .....	17
1.3.1	Connection to a wired Industrial Ethernet network .....	17
1.3.2	Connection to Industrial Ethernet via IWLAN .....	18
1.3.3	Connectable WHART field devices .....	18
1.3.4	Connecting the Link to SIMATIC S7 and SIMATIC PCS 7 .....	19
1.3.5	Redundant connection of the WSN network .....	20
1.4	System requirements .....	21
1.4.1	Configuration PC .....	21
<b>2</b>	<b>Setting up network structures .....</b>	<b>23</b>
<b>3</b>	<b>Installation and commissioning .....</b>	<b>27</b>
3.1	Installation .....	27
3.2	Battery: Replacement and disposal .....	27
3.3	User roles and passwords .....	28
3.4	Commissioning the Link .....	29
3.4.1	The configuration PC .....	29
3.4.2	Adapting the network address of the PC .....	30
3.4.3	Establishing a connection to the Link .....	31
3.4.4	Setting the IP address of the Link .....	32
3.4.5	Security settings .....	33
3.4.6	Network data .....	34
3.5	Commissioning and operating redundant Links .....	35
3.6	Adding field devices .....	38
<b>4</b>	<b>Configuration of the Link .....</b>	<b>39</b>
4.1	Web pages - layout and overview .....	39
4.2	Setup .....	41
4.2.1	Setup > Network > Settings .....	41
4.2.2	Setup > Network > Settings > Access Control List .....	42
4.2.3	Setup > Network > Speed .....	43

4.2.4	Setup > Network > Bandwidth .....	43
4.2.5	Setup > Network > Channels .....	44
4.2.6	Setup > Redundancy .....	44
4.2.7	Setup > Ethernet Protocol.....	46
4.2.8	Setup > Security > User Accounts .....	46
4.2.9	Setup > Security > User Options .....	48
4.2.10	Setup > Security > Certificates .....	49
4.2.11	Setup > Security > Protocols .....	49
4.2.12	Setup > Log Settings.....	50
4.2.13	Setup > Time.....	51
4.2.14	Setup > System Backup > Save .....	52
4.2.15	Setup > System Backup > Restore.....	52
4.2.16	Setup > Page Options > Point Pages .....	52
4.2.17	Setup > Page Options > Point Pages > Editing Custom Page .....	53
4.2.18	Setup > Page Options > Point Columns .....	53
4.2.19	Setup > Page Options > Home Pages.....	54
4.2.20	Setup > Restart Apps.....	54
4.2.21	Setup > Firmware Upgrade.....	55
4.2.22	Setup > Firmware Options .....	55
4.2.23	Setup > HART > Gateway .....	56
4.2.24	Setup > HART > Device.....	56
4.2.25	Setup > HART > Hierarchy .....	57
4.2.26	Setup > Changes .....	57
4.2.27	Setup > Modbus > Communications.....	58
4.2.28	Setup > Modbus > Mapping.....	60
4.2.29	Setup > Modbus > Import/Export.....	64
4.3	Explorer.....	65
4.4	Monitor .....	65
4.4.1	Monitoring data points.....	65
<b>5</b>	<b>Diagnostics.....</b>	<b>67</b>
5.1	Diagnostics > Network > Overview .....	67
5.2	Diagnostics > Network > Devices .....	69
5.3	Diagnostics > Network > Join Failure .....	70
5.4	Diagnostics > Network > Invalid MICs .....	70
5.5	Diagnostics > Advanced > Network Stats.....	71
5.6	Diagnostics > Advanced > Redundancy Status.....	72
5.7	Diagnostics > Advanced > HART Stats > UDP Stats .....	73
5.8	Diagnostics > Advanced > HART Stats > TCP Stats .....	73
5.9	Diagnostics > Advanced > Modbus Stats > Serial Stats .....	74
5.10	Diagnostics > Advanced > Modbus Stats > TCP Stats .....	74
5.11	Diagnostics > Advanced > System Log .....	74
5.12	Diagnostics > Advanced > System Stats.....	75
5.13	Diagnostics > Advanced > Client/Server .....	76



<b>6</b>	<b>Service and maintenance</b> .....	<b>77</b>
6.1	Replacing devices.....	77
6.2	Downloading a new firmware version.....	78
6.3	Reset to factory settings.....	79
<b>7</b>	<b>Technical specifications</b> .....	<b>81</b>
<b>8</b>	<b>Approvals and certificates</b> .....	<b>83</b>
<b>A</b>	<b>Biological compatibility</b> .....	<b>93</b>
<b>B</b>	<b>References</b> .....	<b>95</b>
B.1	/1/.....	95
B.2	/2/.....	95
B.3	/3/.....	95
B.4	/4/.....	95
	<b>Glossary</b> .....	<b>97</b>
	<b>Index</b> .....	<b>101</b>



## Product description

### 1.1 Functions and properties

#### 1.1.1 Functions of the Link



Figure 1-1 IE/WSN-PA Link (device variant with integrated antenna)

### Basic function

The IE/WSN-PA Link is a gateway between a WirelessHART™ network (wireless sensor network = WSN) and wired Ethernet network.

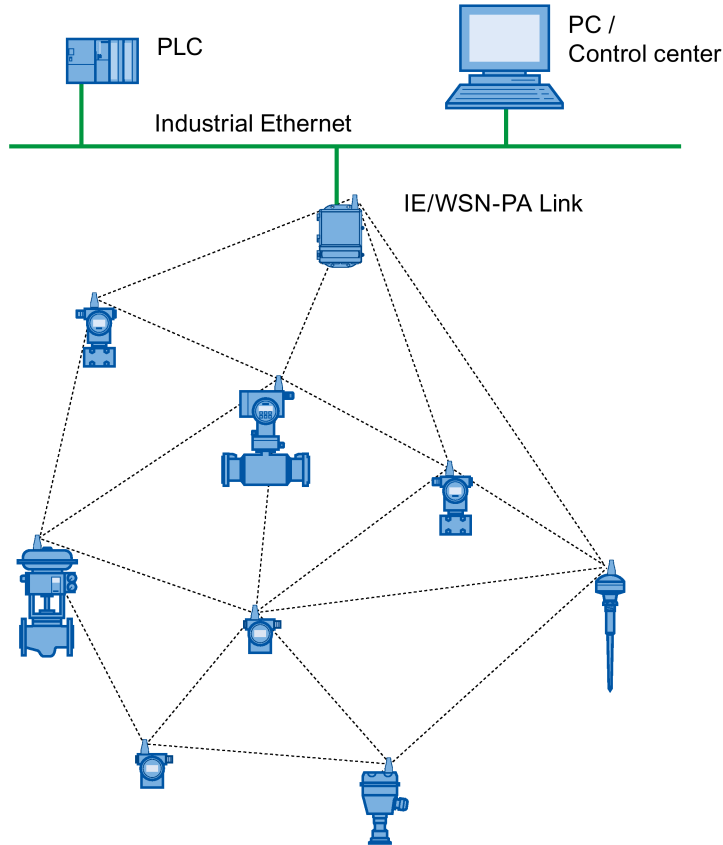


Figure 1-2 Use of the IE/WSN-PA Link as a gateway between a WirelessHART network (WSN) and a wired network

The IE/WSN-PA Link provides industry leading security, scalability, and functionality.

### Network structure and expansion

The IE/WSN-PA Link allows the setting up of a self-organizing WirelessHART network and manages security and connectivity functions.

The WSN network can be expanded easily with the IE/WSN-PA Link. Simply assign the network ID and a join key to the new field device and it becomes part of the existing network.

## Supported protocols

The Link is the input point for data from WirelessHART sensors. This data is converted to a format compatible with other systems. System integration can be achieved in conjunction with an HMI system:

- With TCP/IP via an HTTPS browser
- Via an OPC server
- With Modbus TCP/IP via Ethernet
- With Modbus RTU via a serial connection

## Web interface

The Link has a Web interface that is addressed via HTTP or HTTPS.

The Web interface allows the following functions:

- Basic configuration of the link
- Monitoring of data points
- Diagnostics of the network
- Security management

You can customize security levels to meet plant standards via the Web-based interface.

## Redundancy function

If requirements in terms of availability are higher, the Link can be used redundantly.

The redundancy function is available for the device variant with a connector for an external antenna as of firmware version 4.3.17.

To achieve redundancy, two Links are connected via a switch to the same Ethernet subnet. The two Links are then interconnected via an Ethernet cable (management connection). One of the two Links is configured as the active device and this handles communication between the control center and WSN in a normal situation. The second Link is used as the standby device.

## 1.1.2 Hardware interfaces

### Interfaces

- Wireless interface for connection to a WirelessHART network(WSN)
  - Wireless frequencies  
2.4 to 2.5 GHz DSSS "Direct Sequence Spread Spectrum method) distributed on 16 wireless channels on the basis of the IEEE 802.15.4 standard  
  
Continuous "hopping" between frequencies to reduce susceptibility to interference and to increase reliability.
  - Antenna  
Integrated omnidirectional antenna (device variant 6GK1 411-6CA40-0AA0)  
  
Option: Remote omnidirectional antenna (installed via N-Connect female connector of device variant 6GK1 411-6CA40-0BA0)
- Ethernet  
2 LAN interfaces as RJ-45 jacks for connection to an Industrial Ethernet network  
  
10baseT/100baseT Ethernet communication port, supports Modbus TCP/IP. Some configuration of the field devices (communication parameters) and monitoring is performed using Web pages generated by the IE/WSN-PA Link.
- RS-485  
  
2-wire communication link for Modbus multidrop connections transmission speed (bps): 57600, 38400, 19200 or 9600  
  
Protocol: Modbus RTU

## 1.1.3 Housing

### Housing design

- Rugged industrial housing  
  
The rugged housing of the Link allows field installation in any Zone 2 / Division 2 and is NEMA 4X / IP 65 rated.  
  
The cast aluminum housing encloses the electronics and circuitry of the Link. The front of the housing has two covers:
  - The upper cover  
  
Normally the upper cover does not need to be opened.
  - The lower cover  
  
The lower cover provides access to the junction box which contains the terminals for the power supply, and Ethernet and serial Modbus connections.

## 1.2 Components of the product and accessories

### 1.2.1 Components of the product

#### What the consignment contains

The following components are supplied with the IE/WSN-PA Link:

- IE/WSN-PA Link
- Mast fittings comprising 2 mast clamps (78 mm) and screws
- Threaded blind plugs 1/2 inch NPT for unused cable feedthroughs
- LAN cable (1 meter) for connecting a PC/laptop  
Crossover cable for direct connection without a hub or switch
- Compact operating instructions on paper
- CD with important documentation and software:
  - Operating Instructions for the IE/WSN-PA Link (PDF)
  - Compact operating instructions for the IE/WSN-PA Link (PDF)

### 1.2.2 Accessories for attachment to Industrial Ethernet

#### Accessories for the IE/WSN-PA Link

Suitable products are available for outdoor installation of the Ethernet cabling. The following products are not supplied with the IE/WSN-PA Link.

- Adapter cable M12 female NPT 1/2" to RJ-45 jack, length 11 cm  
Harting Electronics GmbH & Co KG  
Order no. 21 03 683 6420  
You will find information on ordering options at the following address:  
([www.harting.com](http://www.harting.com)) → "contact" → "address"
- Ethernet SIMATIC NET IE FC standard cable GP 2x2  
Order no. 6XV1 840-2AH10  
The cable is not suitable for underground installation.
- M12 male connector IE FC M12 Plug PRO for assembly in the field  
Order no. 6GK1 901-0DB20-6AA0

### 1.2.3 Accessories for the device variant with connector for external antenna

#### Optional accessories

---

**Note****Minimum attenuation of 4 dB required**

When using the ANT792-6MN antenna (antenna gain 6 dBi), the antenna cable must have an attenuation of at least 4 dB. This is the case with the antenna cable 6XV1 875-5AN10 (length 10 m).

When using the antenna cable 6XV1 875-5AN10 (length 1 m), an additional attenuator with at least 4 dB must be inserted in the cable.

---

The following accessories for the device variant 6GK1 411-6CA40-0BA0 are not supplied with the IE/WSN-PA Link:

- External antenna ANT792-6MN  
Order no. 6GK5 792-6MN00-0AA6
- Lightning protector LP798-1N  
Order no. 6GK5 798-2LP00-2AA6
- Antenna cable (10 m) N-Connect Male/Male Flexible Connection Cable  
Order no. 6XV1 875-5AN10
- Antenna cable (1 m) N-Connect Male/Male Flexible Connection Cable  
Order no. 6XV1 875-5AH10
- 2.4 GHz coupling piece IWLAN RCoax N-Connect Male/Male Coupler  
Order no. 6GK5 798-0CP00-1AA0



## 1.3 Application

The Link is intended to link a WirelessHART network (WSN) to an Industrial Ethernet network.

Data transmission of the WirelessHART sensors can be configured via the Link and the data of the sensors can be transferred from the Link to the stations connected via Ethernet. The WirelessHART field devices can be displayed and diagnostics functions run.

The following two diagrams are typical sample configurations showing how the IE/WSN-PA Link can be connected to a control system, an operator control and monitoring station or, for example, to a maintenance station.

### 1.3.1 Connection to a wired Industrial Ethernet network

The following schematic shows a configuration in which the IE/WSN-PA Link is connected via a wired Industrial Ethernet network.

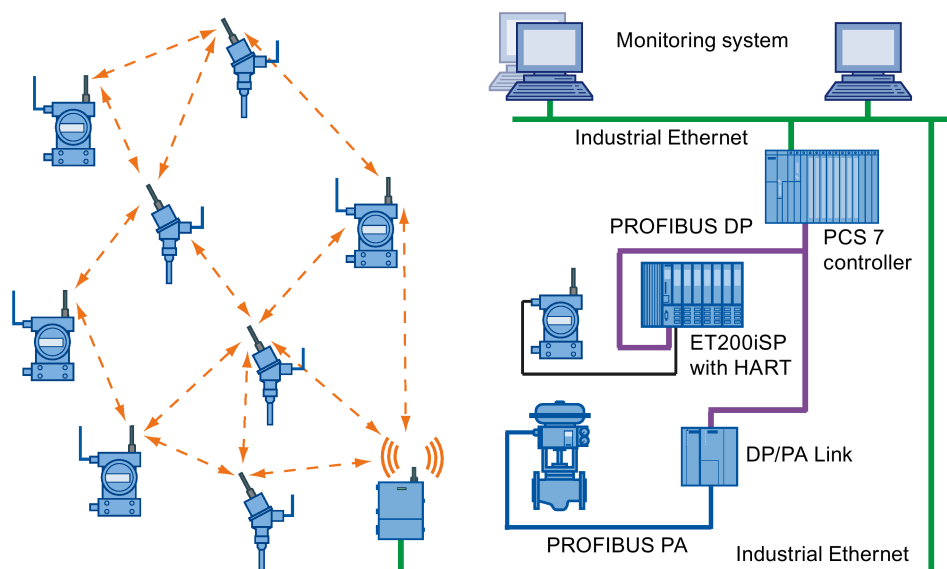


Figure 1-3 Example of a configuration of a Link with attachment to wired Industrial Ethernet

### 1.3.2 Connection to Industrial Ethernet via IWLAN

The following schematic shows a configuration in which the IE/WSN-PA Link is connected via IWLAN to an Industrial Ethernet network. This increases the flexibility in the location of the Link. By connecting the Link to an IWLAN node (client or access point), you can transfer data from the WSN via WLAN.

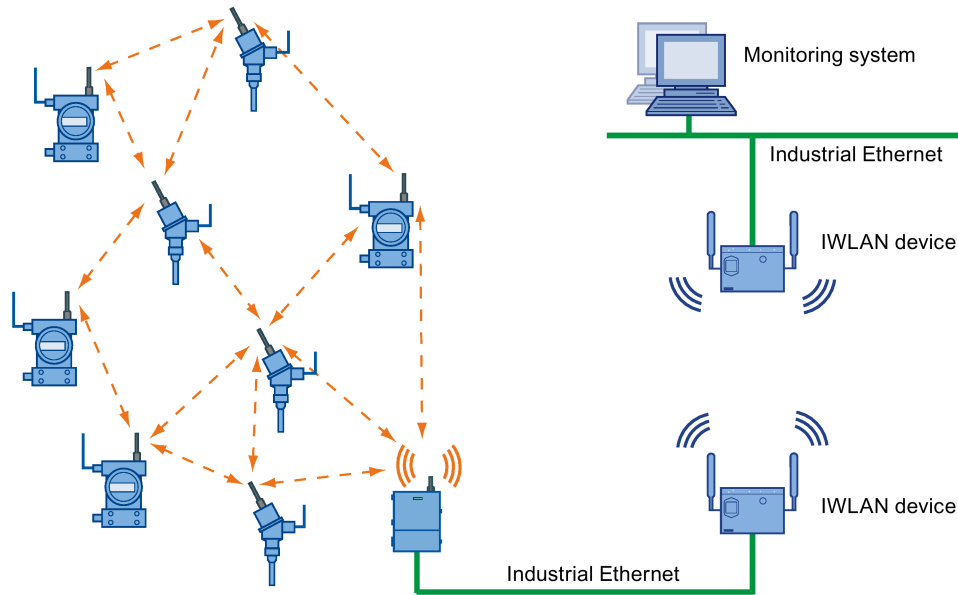


Figure 1-4 Example of a configuration of a Link with attachment to Industrial Ethernet via IWLAN

### 1.3.3 Connectable WHART field devices

#### Connection of WirelessHART devices in the WSN

As nodes in the WirelessHART network, WirelessHART sensors, measuring transducers or actuators with a wireless interface can be connected to the Link according to the IEEE 802.15.4 specification.

These can, for example, be the following WirelessHART devices from Siemens:

- Temperature transducer  
SITRANS TF280 WirelessHART  
Order number : 7MP1110-xxxxx-xxxx
- Pressure transducer  
SITRANS P280 WirelessHART  
Order number : 7MP1120-xxxxx-xxxx
- WirelessHART adapter  
SITRANS AW200  
Order number : 7MP3112-xxxxx-xxxx

You will find more detailed information on the Siemens WirelessHART products on the Internet on the pages of Siemens Industrial Automation Customer Support at the following address:

(<http://support.automation.siemens.com/WW/view/en/38158178>)

There select the required information under "Entry type" (for example "Updates", "Manuals", "FAQs", "Download" etc.).

### 1.3.4 Connecting the Link to SIMATIC S7 and SIMATIC PCS 7

To connect the IE/WSN PA Link to SIMATIC® S7-300/400 or to integrate it in SIMATIC® PCS 7, software blocks and technical support are available at the following addresses:

- For connecting to SIMATIC S7-300/400:

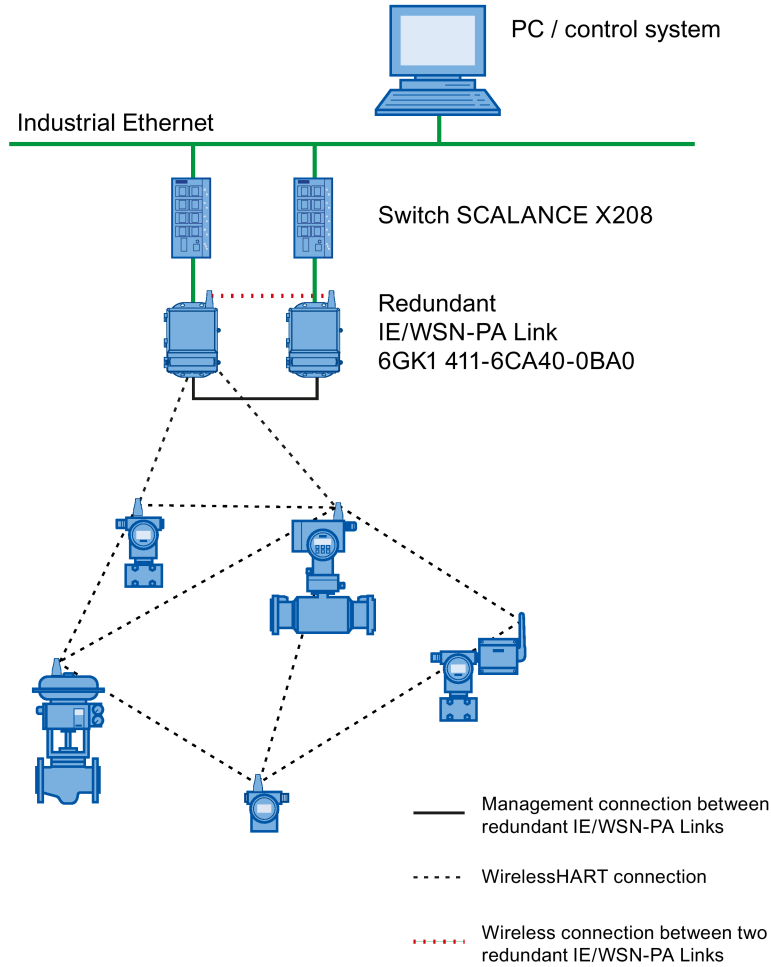
Siemens AG  
Industry Sector  
Industrial Solutions Division  
Industrial Technologies  
IT4Industry Team  
Werner-von-Siemens-Straße 60  
91052 Erlangen  
Germany  
Tel: +49 9131 7-46111  
Fax: +49 9131 7-44757  
E-mail (<mailto:it4.industry@siemens.com>)

- For integration in SIMATIC PCS 7:

Siemens AG  
Industry Sector  
Industrial Solutions Division  
Industrial Technologies  
Siemensallee 84  
76187 Karlsruhe  
Germany  
Tel: +49 721 595-6380  
E-mail (<mailto:function.blocks.industry@siemens.com>)

### 1.3.5 Redundant connection of the WSN network

The following schematic shows a configuration in which the IE/WSN-PA Link connects the WSN network redundantly to a wired Industrial Ethernet network.



Example of a configuration of a redundant Link with attachment to wired Industrial Ethernet

## **1.4 System requirements**

### **1.4.1 Configuration PC**

#### **System requirements for the configuration PC**

For the initial configuration, a PC/laptop must meet or exceed the following criteria:

- **Operating system:**
  - Windows 2000, service pack 4
  - Windows Server 2003
  - Windows XP (Home or Professional), Service Pack 1 or higher
- **Applications:**
  - An Internet browser, for example  
Microsoft Internet Explorer 6.0 or higher (recommended)  
Mozilla Firefox 1.5 or higher
  - Adobe® Acrobat® 5.0 (or higher) for the operating instructions



# Setting up network structures

## Taking into account the local conditions

---

**Note**

To make optimum use of the WirelessHART field devices, a site survey of the WSN network under local conditions is a must.

Where possible, mount the Link or the external antenna of the Link at a location where a connection to several WirelessHART field devices is possible.

To achieve ideal illumination, we recommend that each network node should have at least two neighbors.

---

## Overview

This chapter discusses ways to ensure good performance and security in the WirelessHART network. After commissioning the network, the connections should be checked and choke points in the network eliminated. If expansions to the network become necessary, they increase the span and reliability of the network.

This chapter lays out guidelines to increase and ensure the security of the network.

## Verify Connections

A good connection should have the following characteristics:

- The data reliability is greater than 99%.
- The data latency is less than three times the update time (burst rate).  
See also section Setup > HART > Device (Page 56).
- The battery life of the field devices is longer than the desired operating time at the fastest update rate.

Note the information from the field device vendor.

- A good RSSI value

The Radio Signal Strength Indication (RSSI) in the Link diagnostics is helpful. This check is listed last because it can be misleading on its own (weak signals can still get through if the path is stable), but it can help to identify a problems when they arise.

See also section Diagnostics > Network > Devices (Page 69).

### Choke points in the network

Next, identify choke points in the network. If messages from several field devices all have to pass through a single field device on their way to the Link, this may lead to a choke point in the available bandwidth.

This does not happen often because of the redundant communication paths in most self-organizing networks. The solution is simply to add additional field devices near the field device that represents the choke point to provide more communication paths.

---

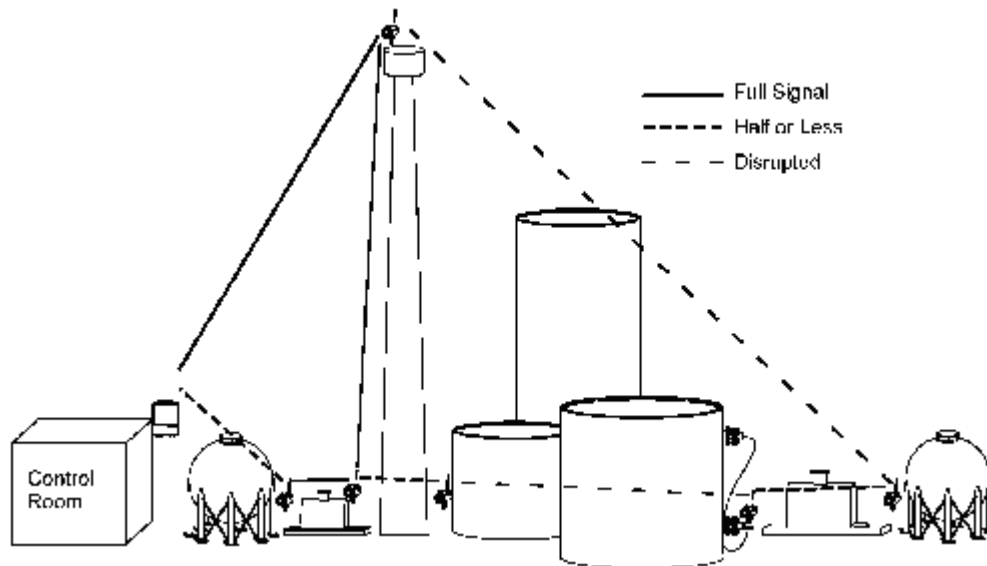
#### Note

Identification of choke points in the network should be performed 24 hours after all the field devices have joined the network. This will allow the network to stabilize and optimize itself.

---

### Obstacles to wireless

A typical plant contains numerous potential obstacles, such as buildings, dense piping, concrete walls and long distances. The diagram below shows how obstacles affect signal strength.



At any layer, increasing distance can also weaken signals. In general, if obstacles disrupt direct transmission between WirelessHART sensors, simply add additional field devices to provide alternative communication paths around the obstacle.



## **Expanding the network**

The network itself detects that a field device has joined the network and routing algorithms in the field devices and Link automatically find the best path to the destination. The only limitation is the amount of traffic that can be handled by each Link and by the field devices.

---

### **Note**

Depending on the size of the network and the number of nodes, adding a node may take several minutes.

---




# Installation and commissioning

## 3.1 Installation

### Description of installation in the compact operating instructions

You will find a description of installing the Link in the compact operating instructions that are available as a PDF on the supplied data medium and that also ship with the Link on paper.

## 3.2 Battery: Replacement and disposal

 <b>WARNING</b>
<b>Risk of explosion and danger of release of harmful substances!</b>
Do not throw batteries into a fire, do not solder the body of the cell, do not open batteries, do not short-circuit batteries, do not reverse the polarity of batteries, do not heat batteries above 100 °C.
Protect batteries from direct sunlight, dampness and condensation.
Dispose of batteries according to the regulations.

### Replacing the backup battery

The device contains a lithium battery. The battery must not be replaced during operation of the device according to the permitted environmental conditions (see technical specifications).

If the battery, nevertheless, does need to be replaced, have the battery replaced only by the Repair Center. If you have any questions, please contact your service center or your marketing partner.

### Disposal

Batteries and rechargeable batteries can be recycled. Their components can be used as raw materials for new batteries or other products. Effective recycling procedures are only possible if batteries of the used batteries of the same type are collected together.

---

#### Note

#### Regulations for disposal of batteries and rechargeable batteries

Keep to the local regulations for disposal of batteries and rechargeable batteries.

---

### 3.3 User roles and passwords

Before configuring and commissioning the Link, decide who should be assigned which user role.

Only an administrator can create or modify user roles and their passwords.

#### User roles

Role	User name (login)	Rights for HTML access
Executive	exec	Read access to configuration pages
Operator	oper	Read access to configuration pages
Maintenance	maint	<ul style="list-style-type: none"><li>• Read access to configuration pages</li><li>• Modbus configuration<ul style="list-style-type: none"><li>– Setting device tags</li><li>– Configuring Modbus communications connections</li><li>– Configuring Modbus register assignments</li></ul></li></ul>
Administrator	admin	<ul style="list-style-type: none"><li>• Configuring the Link, including:<ul style="list-style-type: none"><li>– Network settings (address, security settings etc.)</li><li>– Redundancy link</li><li>– Specifying options for default home page</li><li>– Specifying passwords for user roles</li><li>– Specifying time-of-day settings</li></ul></li><li>• Restarting applications</li><li>• Updating the firmware of the Link</li></ul>

You will find a description of creating users and their roles and rights in the section Setup > Security > User Accounts (Page 46).

#### Passwords

---

**Note****Default password set in the factory**

The factory-set password for all user roles is: default

---

Passwords should be changed periodically once the network is installed. Consult your local IT personnel or your network administrator for guidance on changing passwords.

## 3.4 Commissioning the Link

---

**Note****Order of powering up**

The power supply of the WirelessHART field devices should not be turned on before the IE/WSN-PA Link is installed and working correctly. WirelessHART field devices should be powered up in the order of their distance to the IE/WSN-PA Link starting with the nearest field device to the Link. This procedure allows the wireless sensor network to be established more quickly.

---

### 3.4.1 The configuration PC

#### Requirements for the configuration PC

- To be able to access the integrated HTML pages of the IE/WSN-PA Link, you require a PC/laptop with an Internet browser.
  - Microsoft Internet Explorer version 6.0 or higher (recommended)
  - Mozilla Firefox 1.5 or higher
- JavaScript must be activated in your browser.

You will find information on JavaScript at the following address: (<http://java.com/en>)
- The PC/laptop must be connected to the LAN connector P1 of the IE/WSN-PA Link using a crossover cable.

<b>NOTICE</b>
Under no circumstances, use the covered "POE" connector on the Link, this can cause damage to the PC/laptop.

You will find the other requirements in the operating instructions in System requirements > Configuration PC.

#### See also

Configuration PC (Page 21)

### 3.4.2 Adapting the network address of the PC

Follow the steps below to commission the IE/WSN-PA Link:

---

#### Note

If you use a PC/laptop from a different network, you should note the current IP address and other settings carefully so that the PC/laptop can be assigned to its original network again after configuring the IE/WSN-PA Link.

---

#### Note

When commissioning the Link, remember that other wireless systems in the 2.4 gigahertz band be affected by interference or may cause interference.

You will find a list of WHART and WLAN channels in Setup > Network > Channels (Page 44).

---

To be able to reach the IE/WSN-PA Link using the standard IP address, you will first need to adapt the network address of the PC/laptop.

1. Select the menu command Start > Settings (> Control Panel) > Network and Dial-up Connections.

The "Network connections" dialog opens.

2. Select the "Local Area Connection" entry.
3. Select "Properties" in the shortcut menu.

The "Properties of Local Area Network" dialog opens at the "General" tab.

4. In the box "This connection uses the following items", select the entry "Ethernet Protocol (TCP/IP)".
5. Click the "Properties" button.

The "Properties of Ethernet protocol (TCP/IP)" dialog opens.

6. Select the "Use following IP address" option.
7. In the "IP address" input box, enter an IP address for your configuration PC that differs from the factory-set IP address of the Link, for example 192.168.1.12.
8. Enter the value 255.255.255.0 in the "Subnet mask" input box.
9. Click the "OK" button.

10. Close the "Network and Dial-up Connections" dialog.

Your PC/laptop can now be reached using the IP address set above.

### 3.4.3 Establishing a connection to the Link

1. Start your Internet browser.
2. Select the "Tools" > "Internet Options..." menu command.  
The "Internet Options" dialog opens.
3. Select the "Connections" tab.
4. In the "Local Area Network (LAN) Settings" area, click the "LAN Settings..." button.  
The "Local Area Network (LAN) Settings" dialog opens.
5. If selected, deselect the following options:
  - "Automatically detect settings"
  - "Use automatic configuration script"
  - "Use a proxy server for your LAN"These settings will not apply to dial-up or VPN connections.
6. Click the "OK" button.
7. To start the Web pages of your IE/WSN-PA Link, enter the following in the address line:
  - https://192.168.1.10 (IP address set in the factory for the P1 LAN interface of the Link)
  - or
  - https://192.168.2.10 (IP address set in the factory for the P2 LAN interface of the Link)
8. Enter the following in the "Connect to IE/WSN-PA Link" dialog:
  - User name (login): admin
  - Password: defaultSee also section Security settings (Page 33).
9. Click the "Yes" button in the "Security Alert" dialog.  
The home page of the Link is opened.

---

#### Note

##### Warning message of the browser / certificates

The Link uses self-signed certificates and not a public key certificate.

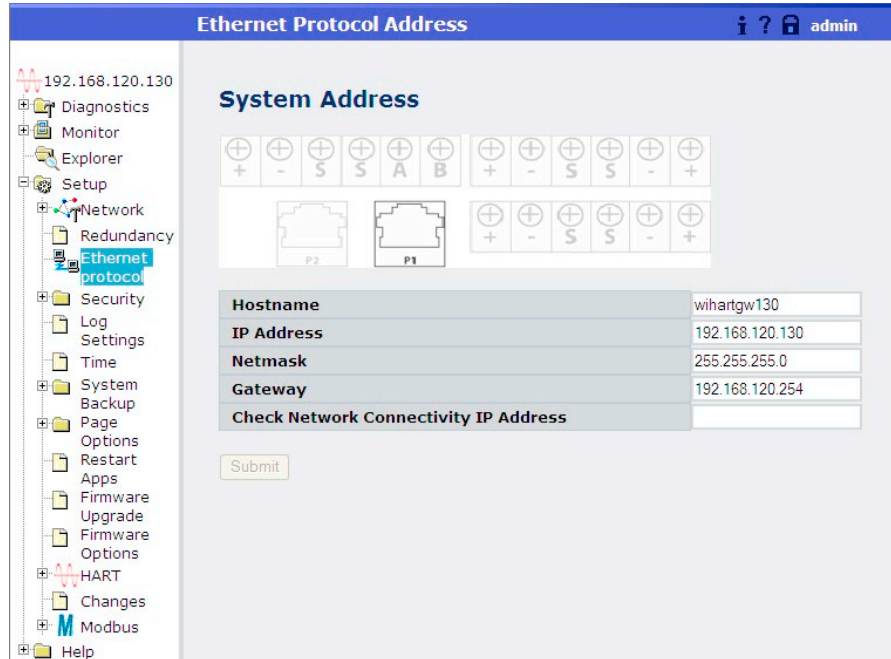
Since the certificate of the Link was not issued by an authorized certification center, when logging in to the link with the browser, you may receive a warning or error message from the browser relating to the certificate. Ignore this message.

---

### 3.4.4 Setting the IP address of the Link

1. Select the "Setup" > "Ethernet Protocol" menu command.

The "Ethernet Protocol Address" dialog opens.



2. Enter the required IP address of the Link in the "IP Address" box under "Primary Interface".

If you use a DHCP server on the other hand, select the "Obtain an IP address from a DHCP server" option and enter the host name in the "Hostname" input box.

3. Click the "Submit" button, button to save the changes.
4. If the "Restart apps" message appears, click "Restart apps" and confirm this by clicking "Yes".

In this case, close the Web browser of your PC and reconnect to the Link using the modified address parameters.



### 3.4.5 Security settings

#### Assigning the administrator name and password

Select the "Setup" > "Security" > "User Accounts" menu command. The "User Accounts" dialog opens.

Name ▲	Password	Confirm password	Admin	Maint	Oper	Exec	Enable	Delete
admin	Using default password		<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
exec	Using default password		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
maint	Using default password		<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
oper	Using default password		<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

|<< First   << Previous   Search   Page 1 of 1   Next >>   Last >>

New entry   Submit

#### NOTICE

##### Loss of the administrator password

Use caution when changing the administrator password. If the administrator password is lost, you will not be able to operate the IE/WSN-PA Link with the administrator role. In this case, contact Siemens Automation Customer Support.

1. Assign or change the name and password of the administrator who will configure the device.
2. Repeat the assigned password in the "Confirm password" input box.
3. Select the "Admin" and "Enable" options for the administrator.
4. Click the "Submit" button.

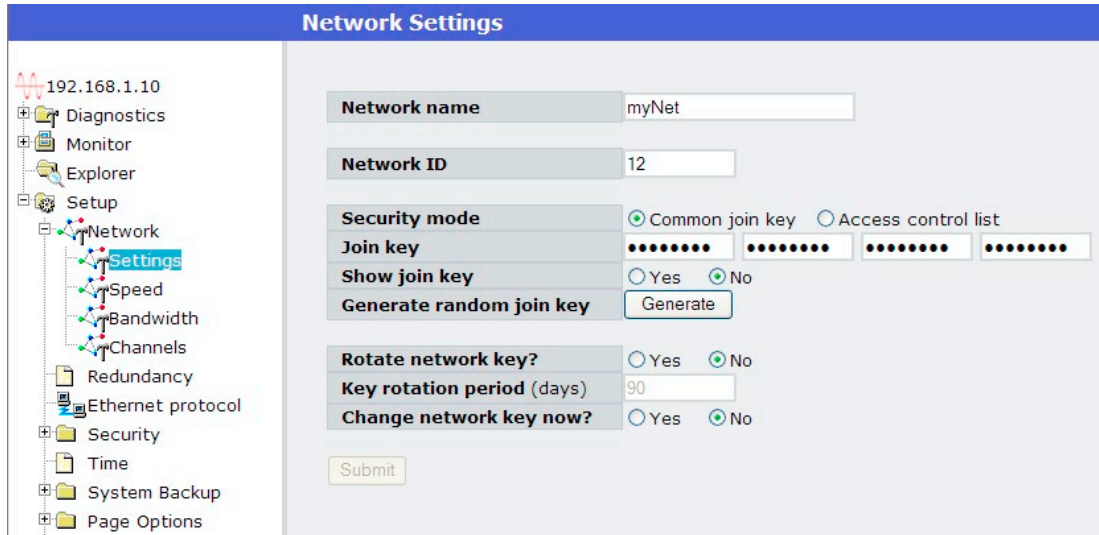
The possible user roles, their rights and the factory-set passwords can be found in the section Adding field devices (Page 38).

You will find further information on the settings for the users and the password qualities in the sections Setup > Security > User Accounts (Page 46) and Setup > Security > User Options (Page 48).

### 3.4.6 Network data

1. Select the "Setup" > "Network" > "Settings" menu command.

The "Network Settings" dialog opens.



2. Enter the network ID of your WirelessHART network in the "Network ID" input box. Numbers in the range 0 to 65535 are permitted.
3. Enter the join key of your WirelessHART network in the "Join key" input box as a hexadecimal number.
4. Click the "Submit" button.
5. Select the "Setup" > "Restart Apps" menu command.

This completes the initial commissioning of the IE/WSN-PA Link. You can remove the PC/laptop and restore the original settings on the PC/laptop.

## 3.5 Commissioning and operating redundant Links

### Requirements for the redundancy function

- 2 Links with order number 6GK1 411-6CA40-0BA0  
(Device variant with connector for an external antenna)

The two Links must meet the following requirements:

- Identical hardware product version
- Identical firmware version (at least version 4.3.17)
- Identical firmware options
- Both devices have a static IP address

You also require the following:

- 1 switch (to improve reliability, 2 switches are recommended.)
- 2 Ethernet cables for connection of the 2 Links to the switch
- 1 Ethernet cable for connecting the two Links (management connection)
- 1 Ethernet cable for connecting the configuration PC to the network

### Redundant operation

During operation, the active Link handles the data traffic. The two Links monitor each other. The standby device monitors the communication of the active device on the wireless interface. If there is a disruption or following a failover, the active link sends an alarm to the connected control system.

### Failover between the active and standby device

The two redundant devices can be switched over manually via the Web interface. They then swap over their roles as active or standby device.

An automatic failover is triggered by a problem on the active device. The following events on the active device lead to a failover to the standby device:

- Interruption of the power supply
- Interruption of the wireless link with the WSN
- Failure of the Link
- Interruption of the connection to the Ethernet subnet
  - Physical interruption
  - Interruption on the connection to the control system (via Modbus or clients connected to HART-IP)

The failover is displayed on the "Diagnostics" > "Advanced" > "Redundancy Status" page of the Web interface of the Link: When there is a failover, the display of the active device first changes to "Standby" status on the diagnostics page, then briefly to "offline" and then finally to "Standby" status.

### 3.5 Commissioning and operating redundant Links

The failover takes place within a maximum of 30 seconds. During this time, the WSN remains established.

During a failover, a Modbus TCP connection can be interrupted which means that the connection must be re-established by the Modbus TCP client.

---

**Note**

**Data loss**

During a failover, a maximum of 1 frame from each field device can be lost.

---

### Management link for connecting the two redundant Links

The Ethernet cable with which the two redundant Links are interconnected at port 2 can be a crossover or a straight-through cable. The Link detects this on port 2 with the autocrossover function.

The connection between the two Links can run via a switch.

---

**Note**

**No disconnection of the management link**

After connecting the two redundant devices, the management link at port 2 of the two Links must not be disconnected again.

---

### Addressing of the redundant Links by the central control system

The two redundant Links are considered to be one device by the control system; in other words, they are addressed with a single IP address.

### Further protocols

STP or RSTP can be used in networks with redundant Links.

### Commissioning and configuring redundant Links

With redundant Links, it is adequate if only one of the two links is configured. This is the active device. The standby Link connected via port 2 adopts all the parameters from the active Link.

---

**Note**

**Initial commissioning of a WSN with redundant Links**

During initial commissioning, allow the redundant Link adequate time to detect the field devices and to set up the WSN. This can take up to half an hour and with very large networks even up to one hour.

---

This means that the two Links also have the same IP address.

To configure and commission redundant Links, follow the steps below:

1. Connect the two Links to the power supply.
2. Connect to your PC to port 1 of the Link that is intended to be the active device.
3. Enter the address "https://192.168.1.10" to connect to the Link.
4. Log on with the "administrator" role.
5. Go to the Web page "Setup > Redundancy" and specify the name and position for Link A and Link B.
6. Go to the "Diagnostics > Advanced > Redundancy Status" page.
7. Connect the two Links (management connection, in each case via port 2)  
A dialog appears on the "Setup > Redundancy" Web page.
8. Click the "Form redundant pair" button to connect the two Links to form a redundant pair.  
After forming the redundant pair, the status "Pairing to redundant peer" changes to green.
9. Click "Return to page".
10. Create the remaining configuration of the Links.

## See also

Setup > Redundancy (Page 44)

Redundant connection of the WSN network (Page 20)

## 3.6 Adding field devices

### Expanding the WSN network - adding field devices

To be able to set up or expand a Wireless Sensor Network (WSN), you simply need to assign the network ID for a WirelessHART field device on the configuration pages of the IE/WSN-PA Link and assign a join key and it becomes part of the network.

### Network ID and join key

The network ID and join key are codes for connecting field devices to the Link. These codes must be identical on the field device and on the Link to be able to establish a connection between the Link and field device.

- Network ID

The network ID is a numeric code for the WSN network.

- Join key

The join key is a hexadecimal code for a field device. This can be generated as a random join key by IE/WSN-PA Link or you can create your own.

You will find a description of configuring the network ID and the join key in the section Setup > Network > Settings (Page 41).

# Configuration of the Link

## 4.1 Web pages - layout and overview



Figure 4-1 Start page of the Web-based configuration tool of the Link

The "Monitor" pages are displayed if you have set up self-configured Web pages, see "Setup > Page Options...".

### Information in the title bar

The title bar contains the following information:

- **IP address**  
IP address of the connected Link
- **? (online help)**  
If you click on the question mark, you open the online help of the configuration tool.  
Here, you will find the following information on the device:
  - **About Gateway**  
Here you will find the serial number and firmware version of the Link.
  - **Manual**  
Here, you will find the manual of the Link and the address of the Internet page of Siemens Automation Customer Support with the current release of the manual
  - **Notices**  
Here, you will find the license conditions and copyright information
- **Padlock symbol for users**  
To the right of the icon, you will see the role of the currently logged in user.  
For a description of the user roles, refer to the section Adding field devices (Page 38).

### Structure of the HTML pages

The HTML pages of the Link have the following basic structure:

Entry	Description
Diagnostics	Check the communication status, the client/server parameters etc. See section Diagnostics (Page 67).
Monitor	Customized Web pages for monitoring the data of the field devices
Explorer	View of the values of the field devices
Setup	Configuration pages of the Link for operation, security settings and host system integration

From the navigation area on the left, you can expand the structure of the HTML pages and jump to specific pages by clicking with the mouse.



## 4.2 Setup

### 4.2.1 Setup > Network > Settings

**Note**

It is not advisable to change the network ID while the network is operating. This resets the network and it needs to be re-established.

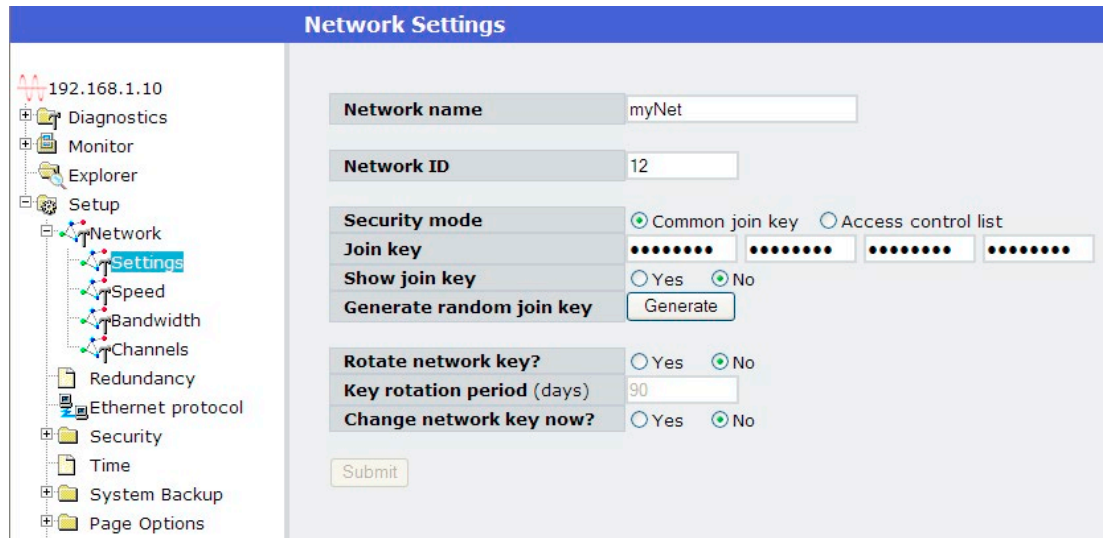


Figure 4-2 Network Settings

Entry	Description
Network name	Network name (plain text)
Network ID	Network ID
Security mode	<p>WirelessHART communication is encrypted according to the AES 128 specification.</p> <p>Select either a common key (join key) for all network nodes or individual join keys that are assigned to the individual WirelessHART field devices in an access control list.</p> <ul style="list-style-type: none"> <li>• Common join key                     <p>With this security mode, all the field devices in the WirelessHART network use the same join key.</p> </li> <li>• Access control list                     <p>With this security mode, the Link manages an access control list with a unique join key for each individual field device.</p> <p>If you select the "Access control list" option, the next page "Access control list" opens in which each field device is assigned an individual join key.</p> </li> </ul>

4.2 Setup

Entry	Description
Join key	Input boxes for the join key If you do not require all 4 boxes for the join key, leave the remaining positions filled with zeros.
Show join key	Shows the current common join key for the WirelessHART network on this HTML page.
Generate random join key	This means that the Link generates a common join key with randomly selected combinations of numbers for all WirelessHART field devices. Any change is passed on to all WirelessHART field devices currently connected to the WirelessHART network.
Rotate network key	This option instructs the Link to generate and use a new network key periodically for encryption. This increases the protection against unauthorized access.
Key rotation period (days)	Time after which the Link generates a new common network key.
Change network key now?	Starts the immediate generation of a new common network key. <b>Caution</b> Configuration changes must be saved first ("Submit" button).
Submit	Accepts all changes (highlighted in yellow).

See also

Network data (Page 34)

4.2.2 Setup > Network > Settings > Access Control List

Parameter settings for the access control list

On this page, you make the parameter settings for the access control list with which you allow individual WSN field devices access to your WirelessHART network.

Entry	Description
Device ID	The unique device ID of the field device
Device Name	The long HART tag of the field device
Generate New Join Key	Generates a new unique join key for the field device
Online	Indicates that the field device is communicating on the WirelessHART network.
Common Join Key	Indicates that the field device is using a common join key.
Default Join Key	Indicates that the field device is using the default join key.
<< First	Takes you to the first page of this table.
<< Previous	Takes you to the previous page of this table.
Next >>	Takes you to the next page of this table.
Last >>	Takes you to the last page of this table.
Search	Finds the next occurrence of the characters entered in this field.

Entry	Description
New entry	Creates a new entry in this table.
Show Join failure	Takes you to the "Diagnostics" > "Network" > "Join failures" page.
Add entries for join failure	Creates new entries in this table and enters data relating to the current join failures.
Delete selected	Removes the selected entry from this table.
Check generate key for selected	Checks the "Generate New Join Key" box for all selected entries.
Select All	Selects all table entries.
Select None	Deselects all table entries.
Select Online	Selects all online field devices in this table.
Select New Join key recommended	Selects all field devices with a common join key or a default join key.
Submit	Accepts all changes (highlighted in yellow).

### 4.2.3 Setup > Network > Speed

Entry	Description
Active advertising	Shows whether "active advertising" is enabled or disabled. If the "Active Advertising" option is enabled, the Link sends advertising frames at short intervals after it starts up to accelerate the integration of field devices in the WirelessHART network.
Duration (minutes)	Decides the time for which advertising frames are sent when the network ready signal is present. Default: 30 minutes
Activate	Enables the sending of advertising frames after the device is turned on.

### 4.2.4 Setup > Network > Bandwidth

Entry	Description
Analyze again	Analyzes the WirelessHART network to determine if any field devices require more bandwidth.

### 4.2.5 Setup > Network > Channels

#### Channel activation

On this page, you can enable or disable the individual wireless channels.

Entry	Description
Enable	Select the option (check mark) to enable the channel.
Channel	Number of the channel
Frequency (GHz)	Frequency of the channel in GHz
Clear channel access assessment (CCA)	WirelessHART function that automatically enables/disables individual channels depending on the wireless load on channels. It is recommended that this option is set to "no".

It may be useful to disable channels if there are other wireless nodes in your plant that do not belong to your WirelessHART network (for example IWLAN nodes) and with which overlaps or interference may occur on certain channels.

#### Frequency ranges of WLAN and WHART systems

Overlapping frequency ranges in WLAN and WHART systems in the 2.4 GHz band:

WLAN channel 802.11b/g	WHART channel 802.15.4
1	11-16
6	15-20
7	16-21
11	20-25
13	21-25

### 4.2.6 Setup > Redundancy

#### Redundancy System Settings

On this page, you enable the redundancy function and specify the active device and the standby device for the redundant pair.

Connected Links are recognized based on their serial number.

### Assignment of the Links to the diagnostics page

Based on the following names, the two Links are identified and positioned on the diagnostics Web page for the redundancy function:

- Name of the active link
- Name of the standby link
- "Left"
- "Right"

The names of the two devices can be freely assigned. The devices can, for example, be identified for diagnostics purposes based on the names. To be able to identify the Links clearly during operation, it is helpful if you write the names assigned here on the devices themselves.

For information on the diagnostics page, to section Diagnostics > Advanced > Redundancy Status (Page 72).

### Requirement for configuring the redundancy function

You will find the basics of redundancy mode and its requirements in the section Commissioning and operating redundant Links (Page 35).

### Setting up the redundancy function

Entry	Description
Redundant Mode	Select one of the following two options: <ul style="list-style-type: none"> <li>• Standalone Disables the redundancy mode. Only the active Link is used.</li> <li>• Redundant Enables the redundancy mode.</li> </ul>
First Node (Serial No. ....)	Here, you specify the name of the active device.
Second Node (Serial No. ....)	Here, you specify the name of the standby device.
Place Node Gate- way - A on	With this option, you specify whether or not the active Link is shown on the left or right on the "Diagnostics" > "Advanced" > "Redundancy Status" diagnostics page. <ul style="list-style-type: none"> <li>• Left Shows the active Link on the left on the diagnostics page.</li> <li>• Right Shows the active Link on the right on the diagnostics page.</li> </ul>
Submit	Accepts all changes (highlighted in yellow).

### 4.2.7 Setup > Ethernet Protocol

#### Ethernet protocol address

**Note**

The best protection against accidental errors during assignment of the IP address of the Link is not to change the IP addresses of Ethernet port P1 and P2 at the same time. If P1 has the wrong setting, you can still access the device via P2.

You will find a screenshot of the page in section Setting the IP address of the Link (Page 32).

Entry	Description
Primary interface	Refers to Ethernet port P1
Secondary interface	Refers to Ethernet port P2
Specify an IP address	The interface is assigned a fixed IP address.
Obtain an IP address from a DHCP server	The interface obtains an IP address assigned by a DHCP server.
Obtain domain name from DHCP server	The interface obtains a domain name assigned by a DHCP server.
Hostname	Host name of the Link
Domain name	Domain name
IP Address	IP address set by the user for the associated interface.
Netmask	Netmask set by the user for the associated interface.
Gateway	Gateway set by the user for the associated interface (not to be confused with the IE/WSN-PA Link)
Submit	Accepts all changes (highlighted in yellow).

### 4.2.8 Setup > Security > User Accounts

#### Specifying user names, passwords and roles

The possible user roles, their rights and the factory-set passwords can be found in the section Adding field devices (Page 38).

<b>NOTICE</b>
<b>Loss of the administrator password</b>
Use caution when changing the administrator password. If the administrator password is lost, you will not be able to operate the IE/WSN-PA Link with the administrator role. In this case, contact Siemens Automation Customer Support.

**Note****Changing passwords**

We recommend that you change the default passwords for security reasons.

The password of the device can be configured. Consult your network administrator for guidelines on setting passwords.

<b>Entry</b>	<b>Description</b>
Name	Box for entering a new user name
Password	Box for entering a new password
Confirm password	Box to confirm the new password for this user
Admin	Specifies the Administrator user role
Maint	Specifies the "Maintenance" user role
Oper	Specifies the "Operator" user role
Exec	Specifies the "Executive" user role
Enable	Activates the user
Delete	Deletes the user
Search	Enter a user name in the input box. If you click "Search", the user name is searched for and displayed.
I<< First	The display jumps to the first entry.
<< Previous	The display jumps to the previous entry.
Next >>	The display jumps to the next entry.
Last >>I	The display jumps to the last entry.
New entry	Adds a new user
Enable factory support accounts	Enabling this option allows trained service personnel to run extra diagnostics functions. Note the following information.
Submit	Accepts all changes (highlighted in yellow).

## 4.2.9 Setup > Security > User Options

### Configuration of the password qualities

Below, the protection level is configured by specifying the quality of the passwords to be assigned (password strength).

The password strength can be assigned in 4 default classes (default parameters set) or according to individual settings (parameters individually configurable). The parameters of the password strength can be shown or hidden.

Table 4- 1 Configuration of the password strength (details hidden)

Entry	Description
Password strength	<ul style="list-style-type: none"> <li>• None: no protection</li> <li>• Minimal: minimum protection</li> <li>• Normal: normal protection</li> <li>• Strong: strong protection</li> <li>• Custom: Configurable protection; the configurable parameters are described in the following table.</li> </ul>
Show Details	Displays the parameters of the password strength. (see following table).
Hide Details	Hides the parameters of the password strength.
Login page message	Here, you edit the text displayed in the dialog when logging on with the device.
Enable factory support accounts	Enabling this option allows trained service personnel to run extra diagnostics functions. Note the following information.
Submit	Accepts all changes (highlighted in yellow).

#### Note

Changes to the setting for "Enable factory support accounts" are effective only after restarting the application. After a cold start on the Link (power OFF → ON), the option is automatically disabled again.

Table 4- 2 Parameters for configuration of the password strength (details shown)

Entry	Description
For the classes of the password strength, refer to the previous table	
Show Details	Hides the parameters of the password strength (see following table).
Minimum length	Minimum length of the passwords
Lowercase count	Number of lowercase letters
Uppercase count	Number of uppercase letters
Digit count	Number of digits
Symbol count	Number of special characters



Entry	Description
Session idle timeout	Time after which a session in which no entries are made will be aborted [minutes].
Maximum session lifetime	Maximum duration of a session [hours]
Minimum password lifetime	Minimum period of validity of the passwords [hours]
Maximum password lifetime	Maximum period of validity of the passwords [days] After this time, a new password must be assigned for the user involved that is different from the previous password is (see also "Password history depth" parameter).
Password failure limit	Maximum number of unsuccessful attempts to enter the password
Password failure lock	System lock after incorrect password input: <ul style="list-style-type: none"> <li>• Yes: system is locked</li> <li>• No: system is not locked</li> </ul>
Password failure wait	Waiting time after incorrect password input until it is possible to enter a password again [minutes]
Password history depth	Number of different passwords before a password can be reused (see also "Maximum password lifetime" parameter).
Submit	Accepts all changes (highlighted in yellow).

#### 4.2.10 Setup > Security > Certificates

Entry	Description
Import GW certificate into webbrowser	Sends security certificates of the Link to the Internet browser.
Rebuild GW certificates	Rebuilds the security certificates for the Link.

#### 4.2.11 Setup > Security > Protocols

Entry	Description
<b>Columns</b>	
Enable	Enables associated communication protocol and opens the specified TCP / UDP port.
Protocol	Type of Ethernet communication protocol
TCP port	The TCP port used by the associated communication protocol
UDP port	The UDP port used by the associated communication protocol
<b>Protocols</b>	
By selecting the check boxes, you enable the protocols you want to use for the link. In the input boxes, you set the required TCP or UDP port.	

Entry	Description
DHCP	Dynamic Host Configuration Protocol for assigning network parameters from a DHCP server <ul style="list-style-type: none"> <li>• Default UDP port: 68</li> </ul>
HART-IP	Protocol for communication with nodes with HART IP capability via Ethernet <ul style="list-style-type: none"> <li>• Default TCP port: 5094</li> <li>• Default UDP port: 5094</li> </ul>
HTTP	Ethernet communication protocol used for the Link's Web-based user interface <ul style="list-style-type: none"> <li>• Default TCP port: 80</li> </ul>
HTTPS	SSL-compliant Ethernet communication protocol used for the Link's Web-based user interface <ul style="list-style-type: none"> <li>• Default TCP port: 443</li> </ul>
Modbus TCP	Ethernet communication protocol used for communication with Modbus TCP-compliant hosts <ul style="list-style-type: none"> <li>• Default TCP port: 502</li> </ul>
NTP	Network Time Protocol for communication with an NTP server for transfer of the time of day <ul style="list-style-type: none"> <li>• Default UDP port: 123</li> </ul>
Ping	If the option is enabled, the Link can respond to ping queries.
SSH	"Secure Shell" (SSH) protocol for encrypted network connections <ul style="list-style-type: none"> <li>• Default TCP port: 22</li> </ul>
Submit	Accepts all changes (highlighted in yellow).

### 4.2.12 Setup > Log Settings

#### Configuring remote access to recording of the system activity (SysLog)

On this page, you configure access by a remote SysLog server to the system activity recording files of the Link.

Entry	Meaning
Enable Remote Logging	Allow access by a remote SysLog server
Remote Server IP Address	The IP address of the remote Syslog server
Remote Server Port	Protocol port of the remote Syslog server
SysLog Protocol	SysLog protocol: <ul style="list-style-type: none"> <li>• IETF (acc. to RFC 5424) - more recent protocol</li> <li>• BSD (acc. to RFC 3164)</li> </ul>

Entry	Meaning
SysLog Transport	SysLog transport protocol: <ul style="list-style-type: none"> <li>• UDP</li> <li>• TCP</li> <li>• TLS (Transport Layer Security, successor to SSL) with encrypted transfer</li> </ul>
Require Trusted Server Certificate?	Specifies whether the SysLog server needs to authorize itself on the Link with a certificate when transferring using TLS.
Log keep-alive message?	Specifies whether keepalive frames are used to monitor the connection to the SysLog server.
Keep-alive message frequency (minutes)	Specifies the time after which a keepalive frame is sent if there has been no data transfer.
Download log definitions	Loads the SysLog configuration data into a file in the file system. Note that the SysLog configuration data must be saved prior to loading by clicking "Submit".
Submit	Accepts all changes (highlighted in yellow).

### 4.2.13 Setup > Time

#### Note

Note that setting the date or time causes a restart on the Link and therefore a temporary loss of communication.

Entry	Description
Your PC's time	The time used by the PC client
GW time	The time currently used by the Link.
Difference	The difference between the PC client time and the Link time
Method used to set time	Selected what method to use when setting the Link time.
Network Time Protocol (NTP)	Uses NTP time.
Set with PC time	Uses the current PC client time.
Manual entry	Uses the Date and Time fields.
Date (mm/dd/yy)	Manually enter the date (mm/dd/yy)
Time (hh:mm:ss)	Manually enter the time (hh:mm:ss)
Submit	Accepts all changes (highlighted in yellow).

**4.2.14 Setup > System Backup > Save**

Entry	Description
Include diagnostic information in system backup	Saves Link diagnostic log information with the system backup file.
Save Configuration	Collects the Link configuration data and creates a system backup file. This system backup file is saved on the PC client as a zip file (*.zip).

**4.2.15 Setup > System Backup > Restore**

**Note**

Note that resetting to factory defaults deletes the entire configuration of the Link.

Entry	Description
Browse...	Opens a navigation window to locate a system backup file (zip file) on the PC client.
Upload configuration	Uploads the configuration of the selected system backup file to the Link.
Reset defaults	Returns the Link to default factory configuration. See also section Reset to factory settings (Page 79).

**4.2.16 Setup > Page Options > Point Pages**

Entry	Description
Name	Name of the custom point page (user specified)
Order	Order in which custom point pages appear in the "Monitor" section of the navigation menu
UP	Moves the associated point page up in the navigation order.
Down	Moves the associated point page down in the navigation order.
Actions	The actions you can perform on the associated point page.
Edit	Navigates to the configuration of the associated page and allows the user to make changes.
Delete	Deletes the associated page.
Go to	Navigates to the associated point page in the web interface.
New	Starts a new custom point page.
Submit	Accepts all changes (highlighted in yellow).

## 4.2.17 Setup &gt; Page Options &gt; Point Pages &gt; Editing Custom Page

Entry	Description
Page Name	Name of this custom point page as it will appear in the "Monitor" navigation menu.
Point Name	Identifies the data point to display. Data point names have the following syntax: (longHARTTag.parameter).
Name	Name set by the user for the data point.
Description	Description of the data point entered by the user.
Order	The order in which the associated data point appears on the custom point page.
Up	Moves the associated data point up in the order.
Down	Moves the associated data point down in the order.
I<< First	Takes you to the first page of this table.
<< Previous	Takes you to the previous page of this table.
Next >>	Takes you to the next page of this table.
Last >>I	Takes you to the last page of this table.
Search	Finds the next occurrence of the characters entered in this field.
Delete selected	Removes the selected entry from this table.
Select All	Selects all table entries.
Select None	Deselects all table entries.
Select Errors	Selects all table entries with error messages.
Submit	Accepts all changes (highlighted in yellow).

## 4.2.18 Setup &gt; Page Options &gt; Point Columns

Entry	Description
Device	Indicates whether or not the "Device" column appears as default in the point pages.
Device Desc	Indicates whether or not the "Device desc" column appears as default in the point pages.
Parameter	Indicates whether or not the "Parameter" column appears as default in the point pages.
Point	Indicates whether or not the "Point" column appears as default in the point pages.
Name	Indicates whether or not the "Name" column appears as default in the point pages.
Description	Indicates whether or not the "Description" column appears as default in the point pages.
Value	Indicates whether or not the "Value" column appears as default in the point pages.
Units	Indicates whether or not the "Units" column appears as default in the point pages.

4.2 Setup

Entry	Description
Status description	Indicates whether or not the "Status description" column appears as default in the point pages.
Status icon	Indicates whether or not the "Status icon" column appears as default in the point pages.
Submit	Accepts all changes (highlighted in yellow).

4.2.19 Setup > Page Options > Home Pages

In this table, you specify the start page that is displayed after logging on to the Web-based user interface of the Link.

Entry	Homepage (start page)
Gateway menu overview	Overview page of the Web interface
Userpage1 *	Start page 1 configured by the user (see section Setup > Page Options > Point Pages (Page 52))
Userpage2 *	Start page 2 configured by the user (see section Setup > Page Options > Point Pages (Page 52))
Explorer	Explorer page
Network Device Status	"Diagnostics > Network > Devices"
Submit	Accepts all changes (highlighted in yellow).

4.2.20 Setup > Restart Apps

Entry	Description
Restart the application software now?	Software reset. This is required for some configuration changes to take affect. A physical power cycle may erase configuration changes before they take affect.
Yes	The application is restarted immediately.
No	Delays the restart. Configuration changes are first saved.

- Application software:  
Software for the web user interface, program manager, operating system, etc.
- Suspend Gateway operations:  
The Link will temporarily be inaccessible via the Web-based user interface. The device stops signaling Modbus or OPC values.

### 4.2.21 Setup > Firmware Upgrade

Entry	Description
Select a firmware release to upload (zip file)	Displays the selected firmware file to be installed. The firmware file must be available as a packed "zip" file in the file system of the connected PC (refer to the "Browse" button).
Browse	Starts the search for the firmware file in the file system of the connected PC.
Upgrade	Starts installation of the new firmware.

#### Note

Installation of a new firmware version may take several minutes. Do not interrupt the procedure before you have received the message that the firmware has been completely installed.

### 4.2.22 Setup > Firmware Options

#### Setup > Firmware Options

Entry	Description
Firmware Options	Firmware options are properties installed in the factory that do not normally need to be changed. These firmware properties can be changed later for when using certain functions. Caution: Updating the firmware leads to a restart on the device during which communication is interrupted in the WSN. You should therefore check the procedure for loading a new firmware option file carefully before downloading this to the device.
Gateway Option	A firmware options file provided by the vendor with the file extension .txt that changes the interface properties of the device. Firmware options files can only be used for a specific device with a unique serial number. Remember that the device has new properties after loading a firmware options file.
Installed	Shows the currently installed firmware options. Marked options are currently installed, unmarked options are not installed. Certain options are not compatible with others.
Option	Interface options that can be used for communication with the device.
Description	Brief description of the options
Browse	Button for searching for the saved firmware options file to be loaded on the device. The zip file provided by the vendor must not be extracted before loading it.
Submit	Starts the installation of a previously selected firmware options file.

4.2.23 Setup > HART > Gateway

Entry	Description
Use Internet protocol host name for gateway name	Uses the "Hostname" box on the the "Internet Protocol" page to replace the Link name. This is a one time action that happens when the box is checked. Further hostname changes will not be taken into account on this page.
Gateway name	Long HART tag for the Link
HART master type	Indicates whether the Link is communicating as the HART primary or secondary master. Most host systems operate as a secondary master and leave primary master status to a handheld device.
Primary	The Link will have priority over a secondary master when outputting commands to WirelessHART field devices.
Secondary	Commands from the Link to a WirelessHART device have lower priority than those of a primary master.
Network retry count	Number of times the Link will attempt to resend a message when it does not get a confirmation.
Submit	Accepts all changes (highlighted in yellow).

4.2.24 Setup > HART > Device

**Note**

If there is a change, in particular a reduction, in the burst rate, you will need to analyze the bandwidth, refer to the section Setup > Network > Bandwidth (Page 43).

Note the information from the field device vendor when you set the burst rate.

Entry	Description
Device ID	Device ID of the field device
HART Tag	Configures the long HART tag (32 characters).
Short Tag	Configures the HART tag (8 characters).
Descriptor	Configures the description.
Units	Configures the units.
Burst Rate	Configures the interval in which the WirelessHART field device transmits its measurement data to the Link (update time). Some field devices bundle multiple messages and send at different rates. Setting options: <ul style="list-style-type: none"> <li>In the seconds range: 4, 8, 16, 32</li> <li>In the minutes range: In the format "hh:mm:ss" up to a maximum of 60 minutes</li> <li>Note the information from the field device vendor when you set the burst rate.</li> </ul>
Delete	Removes the WirelessHART field device from the WirelessHART network.
% Range	Percentage of user-defined range assigned to the HART primary variable.



Entry	Description
Edit	Configure the lower range limit and upper range limit.
<< First	Takes you to the first page of this table.
<< Previous	Takes you to the previous page of this table.
Next >>	Takes you to the next page of this table.
Last >>	Takes you to the last page of this table.
Search	Finds the next occurrence of the characters entered in this field.
Submit	Accepts all changes (highlighted in yellow).

#### 4.2.25 Setup > HART > Hierarchy

Entry	Description
Include gateways	Allows the display of the Link as a field device on the "Monitor" and "Explorer" pages.
Include adapters	Allows the display of WSN adapters as a field device on the "Monitor" and "Explorer" pages.
Submit	Accepts all changes (highlighted in yellow).

#### 4.2.26 Setup > Changes

Entry	Description
Description	Description of the changes adopted.
From	Initial value
To	Final value
Requested	Time stamp of the implementation of the change
Status	Indicates whether the change was adopted, is still being processed, or has failed.

### 4.2.27 Setup > Modbus > Communications

Make the settings for IE/WSN-PA Link Modbus communication suitable for the Modbus settings of the host.

---

**Note**

Modbus connections will fail if they are not configured identically on the Host and the IE/WSN-PA Link.

---

#### Default register addressing

The Link saves data in four separate tables. Two tables are for discrete parameters and two are for numeric parameters. Each table contains up to 9999 values. The discrete parameters are saved in one-bit registers and numeric parameters are saved in 16-bit registers.

Register description	Register type	Register number	Address area of the internal data table
Discrete output values - coils	Read - write	1 – 9999	0x0000 to 0x270E
Discrete input values - contact	Read only	10001 – 19999	0x0000 to 0x270E
Analog input	Read only	30001 – 39999	0x0000 to 0x270E
Analog output - hold	Read - write	40001 – 49999	0x0000 to 0x270E

#### Access to data types

Discrete data is stored in one-bit registers. If the read or write request does not contain 16 registers, the response is returned as a 16-bit value left justified.

Analog data is returned either as an integer in 16-bit registers or as a floating-point value depending on the configuration of the Link. If floating-point representation is selected, each floating-point value is returned as 2 linked registers that together produce a floating-point value with single accuracy.

The following example shows the values in the client display when the holding register 40001 has the following value:

Analog value = -100.234

IEEE equivalent = 0xC2 0xC8 0x77 0xCF

Register values:

- (40001) C2C8
- (40002) 77CF

## Setting options

Entry	Description
One Modbus address	Selects a single Modbus RTU slave address to be used.
Multiple Modbus address	Allows multiple Modbus RTU slave addresses to be used. These addresses are configured per point in the Modbus mapping page.
Modbus TCP port	The TCP Port used to access Modbus TCP data directly from the Link.
Baud rate	Data transmission speed for Modbus RTU.
Parity	Selects the parity bits for Modbus RTU messages.
Stop bits	Sets the number of stop bits for Modbus RTU messages.
Response delay time (ms)	After receiving a request, the Link will wait this long before it sends a response.
Unmapped register read response?	The response the Link returns if no data points are mapped to the register addressed by the read request. The following options are available for the response: <ul style="list-style-type: none"> <li>"Zero fill": The Link responds with "0" (zero)</li> <li>"Illegal data addr": The Link does not send a response</li> </ul>
Unmapped register write response?	The response the Link returns if no data points are mapped to the register addressed by the write job. For the response, only the "Illegal data addr" option is available; in other words, the Link does not send a response.
Floating point representation	Modbus data format
Float	Floating point number that is given over two 16 bit Modbus registers.
Round	Rounded integer that is specified via one 16-bit Modbus register. If measured value = 2711.97, the rounded value = 2712.
Scale	Scaled integer specified via a 16-bit Modbus register. The Link uses the equation $y = Ax - (B - 32768)$ . y = scaled integer returned by the Link, A = gain, x = measured value, B = offset.
Use swapped floating point format?	Reverses which significant register used in a floating point representation.
Incorporate value's associated status as error?	If the HART variable status indicates a critical failure, it will be reported through the Modbus register.
Value reported for error (floating point)	Chooses what value is reported if the value's associated status indicates a critical failure. Only used if the Link is using floating-point representation.
NaN	Not a number is reported if the value's associated status indicates a critical failure.
+Inf	Positive infinity is reported if the value's associated status indicates a critical failure.
-Inf	Negative infinity is reported if the value's associated status indicates a critical failure.
Other	User-defined value is reported if the value's associated status indicates a critical failure.
Value reported for error (rounded or native integer)	User-defined value is reported if the value's associated status indicates a critical failure. Only used if the Link is using rounded or scaled representation.

4.2 Setup

Entry	Description
Scaled floating point maximum integer value	Highest integer proportional to the measured value. Default = 65534. This is generally the highest integer value accepted by the host system.
Use global scale gain and offset	Determines if scaled integers use the Global scale gain and offset or unique gain and offsets for each measured value.
Global scale gain	Gain used by all measured values for scaled integers. The Link uses the equation $y = Ax - (B - 32768)$ . y = scaled integer returned by the Link, A = global scale gain, x = measured value, B = global scale offset.
Global scale offset	Offset used by all measured values for scaled integers. The Link uses the equation $y = Ax - (B - 32768)$ . y = scaled integer returned by the Link, A = global scale gain, x = measured value, B = global scale offset.
Submit	Accepts all changes (highlighted in yellow).

4.2.28 Setup > Modbus > Mapping

**Configuring the Modbus mapping of status and process values**

The following paragraphs explain the mapping of parameters to Modbus registers. Examples illustrate the mapping of device status values as integer registers or as discrete registers and the mapping of process and status values is described.

**Device tags for Modbus mapping**

The Link provides numerous parameters for mapping to Modbus RTU/TCP and OPC. Both the OPC interface used for mapping and the Modbus interface contain only some of the data points used most frequently to accelerate the user interface.

**Mapping the additional device status and standardized status to Modbus registers**

The additional status and the standardized status of a device can be mapped to Modbus registers in two ways:

- You can map to standard integer analog input registers.
- The individual bits in the relevant bytes can be mapped to registers for discrete inputs.

The parameter tags for these bits are ADDITIONAL\_STATUS\_0 – ADDITIONAL\_STATUS\_N, where N depends on the number of status bytes supported by the field device and on STANDARDIZED\_STATUS\_0 – STANDARDIZED\_STATUS\_3.

Other status tags such as EXTENDED\_STATUS (Maintenance required, Device variable alert) and STATUS\_CODE (Device malfunction, Cold start) are also available.

The bit masks required to map individual status bits to discrete Modbus registers can be found in the "HART Common Tables" specification or in the documentation of the particular field device.

The standard parameter mapping "DEVICE\_TAG.PARAMETER" is used for the Link. For this reason, the device tag must first be specified before correct register mapping is possible. When mapping discrete registers, the "State" box (see figure) is also used to enter the bit mask that is applied to the parameter and that generates the discrete value. The "Invert" box (see figure) is used to invert the bit (conversion 0 → 1 and 1 → 0), as may be required by the logic of the user program.

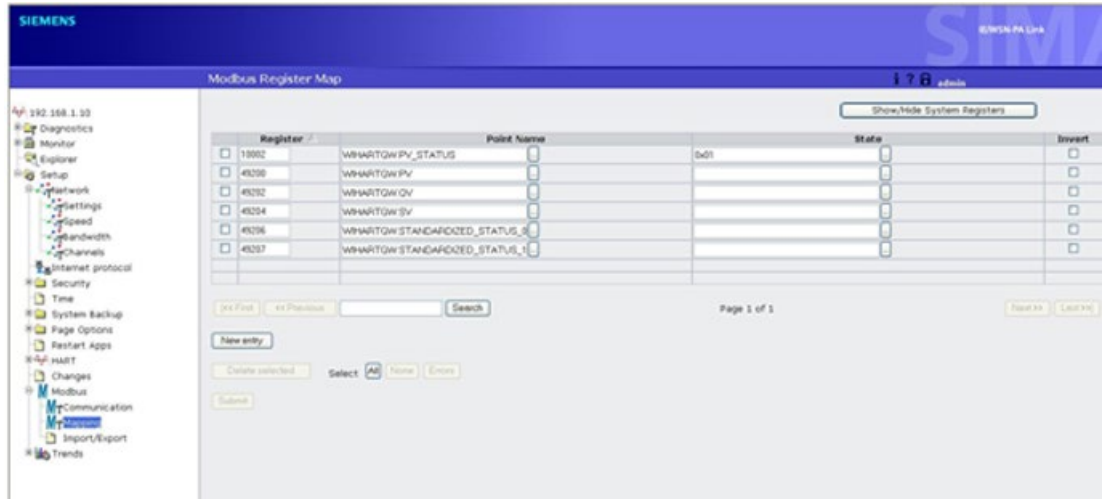


Figure 4-3 Status mapped to an analog input

In the example (see figure above), bit 0 of STANDARDIZED\_STATUS\_0 is mapped to a discrete register. This corresponds to the bit for "simulation active" of STANDARDIZED\_STATUS\_0. Other single status bits can be mapped to registers for discrete inputs in the same way. The figure (see below) shows an example of a Modbus client that reads the discrete inputs of the "STANDARDIZED\_STATUS\_0" status (simulation active).



Figure 4-4 Example of a Modbus client that reads a discrete input

### Dynamic device variables and device status

The dynamic variables and the status of a field device can also be mapped to Modbus registers. The status of the dynamic variables can be mapped to an analog input register or to an analog holding register. The floating-point value of the dynamic variables can either be mapped as a floating-point value to two analog holding registers at the same time or using scaling of the register to a single analog holding register. You also have the option of mapping the variable status mixed with the floating-point values or separate from them to another register section such as the registers for analog inputs.

The figure "Status mapped to an analog input" shows an example of this (see figure below). This option allows maximum flexibility for the different register mappings of host systems. The figure (see below) shows an example of a Modbus RTU client, that first reads out a mixed register map of floating-point values of a dynamic variable followed by the status value etc.

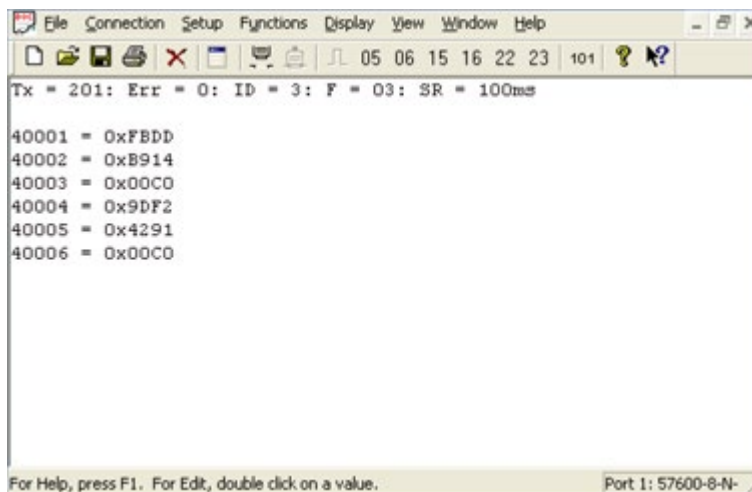


Figure 4-5 Example of a Modbus client that reads the variables "PV" and "PV\_STATUS"

Here, the standard parameter mapping "DEVICE\_TAG.PARAMETER" of the Link is used. For this reason, the device tag must first be specified before correct register mapping is possible.

The default dynamic variables for floating-point values are PV, SV, TV and QV. The device variables can, however, also be mapped according to the variable number. These are followed by the status values as PV\_STATUS, SV\_STATUS, TV\_STATUS and QV\_STATUS. These values are unsigned single byte values and they must be mapped to a single analog input register or a single analog holding register.

## Setting options

On this page, Modbus Registers can be mapped to the measurement points.

To create a new entry, click the "New Entry" button. This will activate a row of text fields in the Modbus Register table. Begin by filling in the register number, then choose or type in the point name. Remember to click "Submit" to apply the changes.

Entry	Description
Show / Hide System Registers	Shows/hides predefined system registers. The predefined system registers follow in the form of a table.
Address Modbus RTU slave address	Only used if multiple Modbus addresses is selected on the "Modbus" > "Communications" page.
Register	Memory location used to reference point data using the Modbus protocol. Modbus holding register.
Point Name	Assigned data point in the format "LongHARTtag.parameter".
State	For Bool values, indicates which value is represented as 1. For integers, identifies a special bit that is represented as 1. Reserved for registers lower than 20 000.
Invert	Switches the 0 or 1 response for discrete measurement values.
Gain	Special register gain for the format of the scaled integers. Not used if use global scale gain and global offset was selected on the "Modbus" > "Communications" page.
Offset	Special register offset for the format of the scaled integers. Not used if use global scale gain and global offset was selected on the "Modbus" → "Communications" page.
<< First	Takes you to the first page of this table.
<< Previous	Takes you to the previous page of this table.
Next >>	Takes you to the next page of this table.
Last >>	Takes you to the last page of this table.
Search	Finds the next occurrence of the characters entered in this field.
Submit	Accepts all changes (highlighted in yellow).

### 4.2.29 Setup > Modbus > Import/Export

#### Saving/loading a configuration file

On this page, you can save the current Modbus configuration of the Link in a file or load an existing Modbus configuration file.

Entry	Description
CSV file	File format with comma as separator
Browse...	Opens a navigation window to locate a Modbus mapping backup file (CSV file) on the PC client.
Upload configuration	Restores the selected Modbus mapping backup file to the Link.
Download configuration	Collects the Link Modbus mapping data and creates a backup file. This Modbus mapping backup file is saved on the PC client as a CSV file (*.csv).



## 4.3 Explorer

### Network overview

The "Explorer" page shows you an overview of your WirelessHART network.

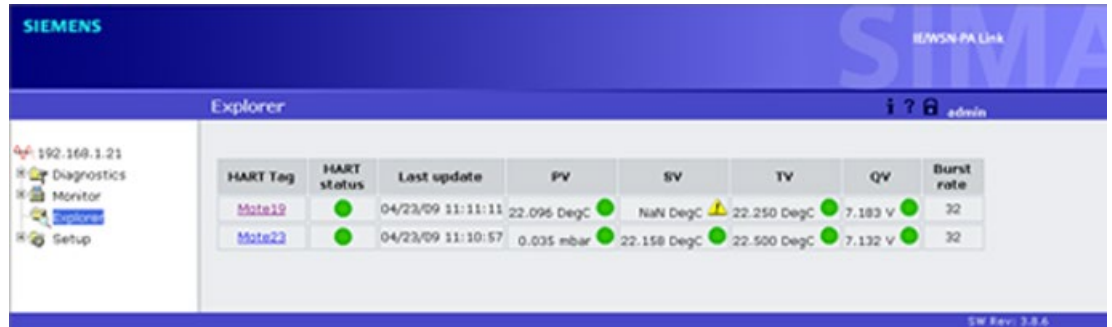


Table 4- 3

Entry	Description
HART tag	Long HART tag or HART tag.
HART status	HART status parameter, this is the overall field device status. Hover over the status icon with the mouse button for a more descriptive message.
Last update	Time stamp of the last measurement received by the WirelessHART field device
PV	Value of the primary HART variables
SV	Value of the secondary HART variables
TV	Value of the tertiary HART variables
QV	Value of the quaternary HART variables
Burst rate	Interval in which the WirelessHART field device transmits its measurement data to the Link (see also section Setup > HART > Device (Page 56)). Some field devices bundle multiple messages and send at different rates.

## 4.4 Monitor

### 4.4.1 Monitoring data points

The "Monitor" pages are displayed if you have set up self-configured Web pages, see "Setup > Page Options...".

On the "Monitor" pages, you can monitor measuring points.



# Diagnostics

## 5.1 Diagnostics > Network > Overview

Entry	Description
Active advertising	Shows whether active advertising is enabled or disabled. When active advertising is enabled, the WirelessHART network sends messages looking for new or unreachable field devices to join the network. Active advertising is automatically enabled for 60 minutes when the Link is first powered up, a field device becomes unreachable, or no field devices are found. Click "Setup" to enable/disable the function. The "Setup" → "Network" → "Speed" menu opens.
Fast pipe	Shows whether the "Fast Pipe" function is enabled or disabled. This function creates a dedicated channel for communication with the selected field device. Used for large data transfers. As default, this function is disabled.
Wireless device count	Total number of expected field devices
Live	Number of field devices that are currently communicating on the WirelessHART network.
Stale	Number of field devices that have missed several updates, but are not yet classified as unreachable.
Unreachable	Number of field devices that have not communicated for 10 minutes or more (also considered as offline).
Unknown	Number of field devices with an unknown state (i.e. not "live", "late", "stale", etc...).
Wired HART device count	Number of wired HART field devices that are connected via a WirelessHART adapter.
Devices with service denied	Number of devices that were denied bandwidth. Reason: <ul style="list-style-type: none"> <li>• There are too many field devices in the WirelessHART network</li> <li>or</li> <li>• The field device has requested an update rate not currently supported by the Link.</li> </ul>
Devices with critical power failure	Number of field devices that have indicated a critical power failure and have stopped sending updates.
Devices with unknown names	Number of field devices whose long HART tag or HART tag is not currently known (typical during the join process).
Devices with undefined names	Number of field devices whose long HART tag or HART tag has been left blank.
Devices with duplicated names	Number of field devices with duplicate long HART tags or HART tags.
Devices with invalid names	Number of field devices whose long HART tag or HART tag begins with a slash or contains either a dot or comma.

Entry	Description
Factory support accounts enabled	Indicates whether or not factory support accounts are enabled. These accounts are used to program factory settings, type and serial number and optional device functions. The box appears only if the option is enabled.
Using common join key	Indicates whether or not field devices entered in the access control list use the common join key. The box appears only if the option is enabled.
Weak server certificate	Shows whether the certificate key has the correct length. Click the "Setup" button to adapt the key.
System up time	The total time the system has been operational without an interruption (power cycle, restart, failure, etc. - only when the Link is in standalone mode).

## 5.2 Diagnostics > Network > Devices

Entry	Description
HART tag	32 character long HART tag. If you click on a field device in the "HART Tag" column, the "Network details", "Burst statistics" and "Service status" submenus for this device are called and display additional network information about the device.
Node state	Status of the field device: live, late, stale, joining, unreachable, or unknown. <ul style="list-style-type: none"> <li>• Green = live</li> <li>• Yellow = late</li> <li>• Red = stale, joining, unreachable, or unknown</li> <li>• Position the mouse pointer over the node status icons to display more detailed information.</li> </ul>
Active neighbors	Names of other field devices with a connection to this field device.
Service denied	Indicates whether or not the field device has been denied bandwidth. Reason: <ul style="list-style-type: none"> <li>• There are too many field devices in the WirelessHART network</li> <li>or</li> <li>• The field device has requested an update rate not currently supported by the Link.</li> </ul>
Reliability	Percentage of expected data packets that have been received by the Link. 100% reliability means that every expected data packet was received. This is calculated in 15 minute cycles.
Missed updates	Total number of updates that have not been received by the Link. A...x...C...D... (x indicates a missed update where B should have been)
Path stability	Percentage of transmitted packets that have successfully reached their destination over a given path, averaged for all neighbor paths of this field device and calculated in 15 minute cycles. Example: <ul style="list-style-type: none"> <li>• Path stability neighbor path A = 100</li> <li>• Path stability neighbor path B = 90</li> </ul> Result for path stability = 95
RSSI	Average received signal strength indication (dBm) for the field device, as seen by all its neighbors. This is calculated in 15 minute cycles.
Joins	Number of times the field device has joined the network within the last 15 minute cycle.
Join time	Time that the field device made its last successful join.

### 5.3 Diagnostics > Network > Join Failure

Entry	Description
Join failure	When a WirelessHART field device fails to join the WirelessHART network. Most join failures are due to security reasons (missing or incorrect join key, not on access control list, etc...).
Last Failure Time	Time the field device last attempted to join the WirelessHART network
Failure Count	Total number of join failures for this field device
Device ID	Unique identification number of the field device
Name	Long HART tag or HART tag of the field device
In Access Control List	Indicates whether the device ID appears in the access control list (only when in access control mode).
Online	Indicates whether the field device is communicating with the WirelessHART network.
Reset List	Clears all entries for the join failure table.
Edit access control list	Navigates to the access control list page in the Web-based user interface.

### 5.4 Diagnostics > Network > Invalid MICs

Entry	Description
Message Integrity Check	Diagnostics information in each data packet that allows the Link to verify the packet source and contents.
Invalid MIC	Packet received from field device is not valid. May indicate a security problem.

## 5.5 Diagnostics > Advanced > Network Stats

The values are the numbers since the commissioning the Link, the last restart or the last counter reset.

Entry	Description
Tx requests	Number of HART messages sent by the Link to the field devices
Tx request timeouts	Number of send requests from the Link without a response from the field devices
Rx response messages	Number of HART messages received by the Link from the field devices as responses. Equal to the difference "Tx requests - Tx request timeouts".
Rx burst messages	Number of messages received by the Link that were sent unsolicited by the field devices. These messages are sent by the field devices without being requested by the Link.
Requests received	Number of HART messages requested by an application. These messages are forwarded to the wireless network (field devices). An example of an application is the Web interface of the Link.
Responses sent	Number of HART responses received from field devices and then forwarded to the requesting application.
Upstream packets lost	Number of data packets sent by the Link whose receipt was not acknowledged by the field devices.
Average latency	<p>Average difference between the time a message is time stamped on a field device and the time it is received by the WirelessHART wireless device of the Link. This value represents the average latency for the entire WirelessHART network.</p> <ul style="list-style-type: none"> <li>• 15 minute Average latency of the last 15 minutes (s)</li> <li>• Lifetime Average latency since the last Link startup (s)</li> </ul>
Reset counts	Resets all values of this table.

## 5.6 Diagnostics > Advanced > Redundancy Status

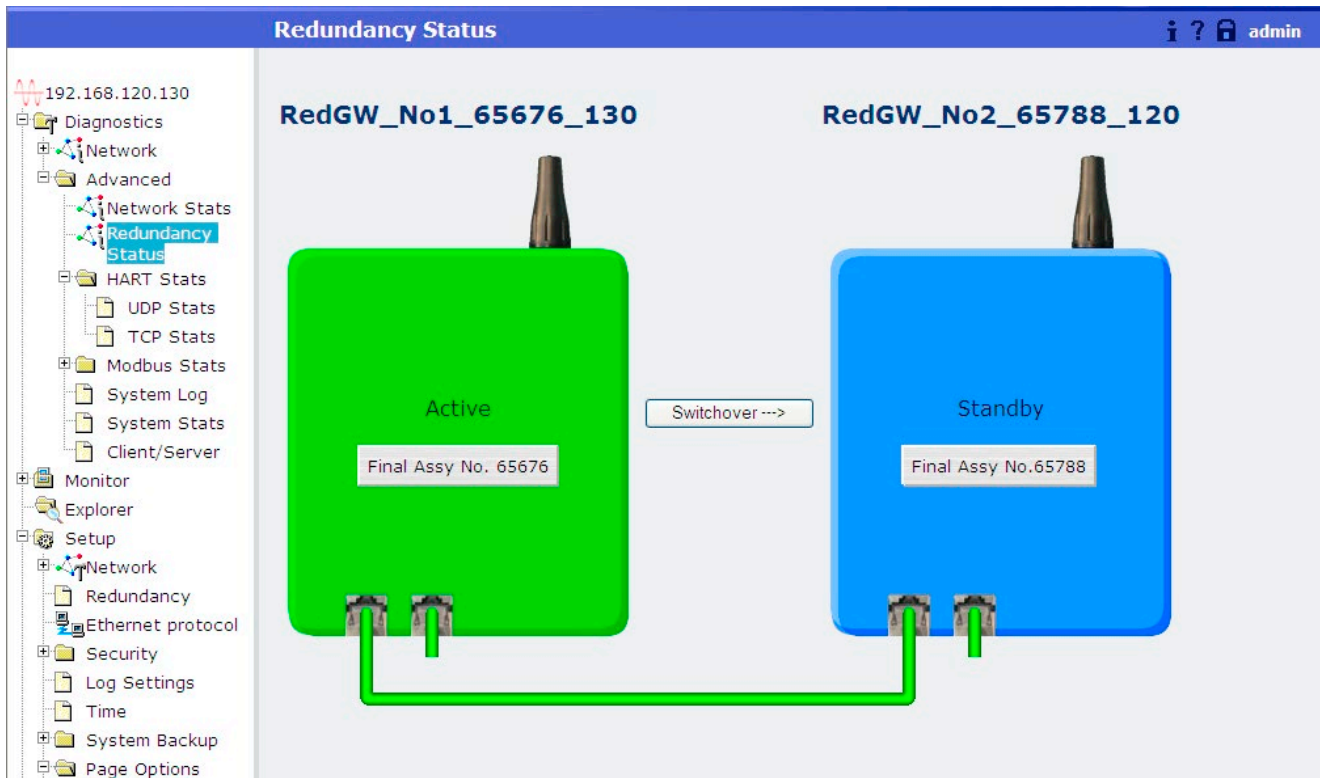
This page shows the two Links of the redundancy pair as they were specified on the "Setup > Redundancy" Web page.

The roles of the two Links as active and standby device are indicated by the color of the device:

- Green: Active device
- Blue: Standby device
- Gray: Status unknown, no connection to device

(for example possibly caused by an interrupted management connection between the two Links)

Above the two Links, the name assigned to the device on the "Setup > Redundancy" Web page is displayed. The Final Assembly Number is displayed in the device symbol.



Entry	Description
Switchover →	Switches over the "active device" and "standby device" function of the two Links.
<b>Symbols used</b>	
	Indicates an error or a disruption, for example a wireless link is too weak or there are interruptions on the connection.
	Indicates an interrupted connection.
If you place the mouse pointer over a symbol, the displayed tooltips provide you with further information.	



## 5.7 Diagnostics > Advanced > HART Stats > UDP Stats

### Diagnostics > Advanced > HART Stats > UDP Stats

Statistics of HART communication using the UDP protocol

Entry	Description
Messages Received	Number of frames that the device has received from a client application.
Messages Returned	Number of frames that the device has returned to a client application.
Messages Broadcast	Number of periodic broadcast frames that the device has received from a client application.
Requests Forwarded	Number of frames forwarded to wireless field devices
Responses Returned	Number of frames that the device has received as the reply to forwarded calls from wireless field devices.
Accepted Connections	Total number of connections with client applications since the last device startup
Reset Counts	Resets all values in the table to zero.

## 5.8 Diagnostics > Advanced > HART Stats > TCP Stats

### Diagnostics > Advanced > HART Stats > UDP Stats

Statistics of HART communication using the TCP protocol

Entry	Description
Messages Received	Number of frames that the device has received from a client application.
Messages Returned	Number of frames that the device has returned to a client application.
Messages Broadcast	Number of periodic broadcast frames that the device has received from a client application.
Requests Forwarded	Number of frames forwarded to wireless field devices
Responses Returned	Number of frames that the device has received as the reply to forwarded calls from wireless field devices.
Accepted Connections	Total number of connections with client applications since the last device startup
Reset Counts	Resets all values in the table to zero.

## 5.9 Diagnostics > Advanced > Modbus Stats > Serial Stats

Entry	Description
Messages Receive	Number of messages received from the Modbus master device.
Crc errors	Number of cyclic redundancy check errors. Crc errors generally indicate noise in transmission or problems with data integrity.
Messages Transmit	Number of response messages transmitted by the Link.
Error responses	Number of error response messages transmitted by the Link.
Reset counts	Resets all values for this table.

## 5.10 Diagnostics > Advanced > Modbus Stats > TCP Stats

Entry	Description
Messages received	Number of messages received from the Modbus TCP field device.
Messages transmitted	Number of response messages transmitted by the Link
Error responses	Number of error response messages transmitted by the Link
Open connections	Number of connections in which the other Modbus TCP field device is not communicating.
Accepted connections	Number of connections to other Modbus TCP field devices
Reset counts	Resets all values for this table.

## 5.11 Diagnostics > Advanced > System Log

This page shows the SysLog messages relating to system activity. You can download the messages from the device to your admin PC and output a test message.

Entry	Description
Description	Output box for SysLog messages
<< First	Takes you to the first message.
<< Previous	Takes you to the previous message.
Next >>	Takes you to the next message.
Last >>	Takes you to the last message.
Download log	Loads the messages as a text file on the connected admin PC.
Add test message	Outputs a test message.

## 5.12 Diagnostics > Advanced > System Stats

Entry	Description
CPU Usage	Central Processing Unit (CPU) utilization (time used by a process) by application or kernel
User	Percentage of CPU utilization that occurred while executing at the user level (application).
System	Percentage of CPU utilization that occurred while executing at the system level (kernel).
Total	Total CPU utilization, user and system (as a percentage)
Ram	Random Access Memory
Size	Total memory or disk space
Used	Portion of memory or disk space that is being used
Main Filesystem	Disk space reserved for Link operating system, user interface pages and configuration data
Temporary Filesystem	Disk space reserved for log files and user-defined pages
Logs	Disk space taken by diagnostics log files

## 5.13 Diagnostics > Advanced > Client/Server

Entry	Description
<b>Server Information</b>	<b>Web server application of the IE/WSN-PA Link</b>
HG version	Firmware version of the IE/WSN-PA Link
Name	Host name of the Link
HG Final Assembly Number	Final assembly number of the Link
HG serial number	Serial number of the Link
HG device ID	Unique identification number of the Link (= serial number)
HG hardware revision	Hardware product version of the IE/WSN-PA Link
Network Frequency	Wireless frequency band for operating the WirelessHART field network. WirelessHART networks operate at 2.4 GHz
HART Universal Revision	The major revision of the HART specification that applies to this Link.
<b>Client Information</b>	<b>PC client that is currently logged onto the Link</b>
Browser Name	The Web browser application that is currently accessing the Link.
Browser Version	The Web browser version
Operating System	Operating system of the PC client currently accessing the Link.
Screen Width	Screen width resolution for the PC client
Screen Height	Screen height resolution for the PC client
Color Depth	Number of colors used by the PC client to display images.
User Agent Info	Information provided by Web browser for further identification
IP Address	IP address of the PC client
Remote User	User role used to log onto the Link

## Service and maintenance

### 6.1 Replacing devices

#### Replacing a device

Follow the steps below to replace your Link with a new IE/WSN-PA Link:

1. Save the configuration of the Link you are replacing on a PC ("Setup" > "System Backup" > "Save").
2. Check to make sure the saved configuration file is valid and undamaged  
The configuration file is saved in CSV format as a ZIP file.
3. Disconnect the Link from the power supply.
4. Connect the new IE/WSN-PA Link to the power supply and turn on the power.
5. Wait until the device startup is complete.
6. Go to the Web pages of the Link (see section Configuration of the Link (Page 39)) and load the previously saved configuration file on the new Link ("Setup" > "System Backup" > "Restore" > "Upload Configuration").
7. Re-analyze the bandwidth ("Setup" > "Network" > "Bandwidth") as soon as all field devices are connected to the Link and are returning measured data. Update the bandwidth if necessary.

## 6.2 Downloading a new firmware version

### Requirements

The following requirements must be met to load a new firmware version:

- The firmware file is stored on the PC/laptop.
- The PC/laptop is connected to the Link.  
See section Commissioning the Link (Page 29).
- You are logged onto the Link with the required administrator privileges.  
See section Adding field devices (Page 38).
- The Link is in standalone mode.

If the Link is used in redundant mode, before upgrading the firmware you need to change both devices to standalone mode, see section Setup > Redundancy (Page 44).

### Loading firmware

To load a new firmware version, go to the "Setup" > "Firmware Upgrade" menu and follow the steps listed in the description, refer to the section Setup > Firmware Upgrade (Page 55).

Once loading the firmware is completed, the Link automatically returns to productive operation.

## 6.3 Reset to factory settings

### Restoring the default parameter settings

---

**Note**

Note that resetting to factory defaults deletes the entire configuration of the Link.

---

To reset to factory settings, follow the steps outlined below:

1. Open the page "Setup" > "System Backup" > "Restore" in the Web pages for configuring the Link (see section Setup > System Backup > Restore (Page 52)).
2. Click "Reset Defaults".
3. Click "OK".
4. To complete resetting the Link to default settings, select the "Restart Apps" button.

The restart takes several minutes to complete. The Link then works with the default factory settings. It may be necessary to configure the network settings of the PC to restore communication with the Link.

For network configuration, refer to section Commissioning the Link (Page 29).





## Technical specifications

### IE/WSN-PA Link

The following technical specifications apply to the IE/WSN-PA Link:

<b>Technical specifications</b>		
Order numbers	6GK1 411-6CA40-0AA0 6GK1 411-6CA40-0BA0	
<b>Attachment to Industrial Ethernet</b>		
Number	2	
Design	RJ-45 jack	
Properties	10100BASE-T / 100BASE-Tx, IEEE 802, half duplex/full duplex, autocrossover, autonegotiation, autosensing	
Transmission speed	10/100 Mbps	
<b>Attachment to Modbus</b>		
Number	2	
Transmission speed	Modbus RTU: 57600, 38400, 19200 or 9600 bps	
Design	Terminals A + B	
<b>Wireless interface</b>		
Antenna for device with order number 6GK1 411-6CA40-0AA0	Number	1
	Design	Integrated
Antenna connector for device with order number 6GK1 411-6CA40-0BA0	Number	1
	Design	N-Connect Female
Wireless technology and frequency range	WirelessHART™ 2.4 - 2.5 GHz DSSS	
Update time (burst rate)	Can be set (up to 60 minutes)	
Maximum network size per IE/WSN- PA Link	100 field devices	
Delay with a network size of	<ul style="list-style-type: none"> <li>• 100 field devices:</li> <li>• 50 field devices:</li> </ul>	<ul style="list-style-type: none"> <li>• max. 8 s</li> <li>• max. 4 s</li> </ul>
Maximum distance from the IE/WSN- PA Link to the next WirelessHART field device	100 m	
Reliability	> 99 %	

**Technical specifications**

**Electrical data**

External power supply	Power supply	24 VDC
	Permitted range	12 ... 30 V
	Design	Terminal block, 2 terminals
	Grounding	Grounding terminal on underside of the device
Current consumption	Maximum	500 mA
Electromagnetic compatibility	EMC approval:	EN 61326-1:2006

**Permitted ambient conditions**

Ambient temperature	During operation, without accessories	-40 °C to +70 °C
	During operation when using the Harting adapter cable	-25 °C to +60 °C
Relative humidity	During operation	≤ 90 %

**Design, dimensions and weight**

Housing	Low copper aluminum	
Degree of protection	IP65 / NEMA 4X	
Dimensions without antennas (W x H x D)	229 x 306 x 89 mm	
Weight	4.54 kg	
Cable guides	4 cable feedthroughs 1/2" NPT	
Seal	Silicon	
Installation options	Wall mounting	

**Product functions \***

Self-organizing WirelessHART network	Advanced Encryption Standard	Encryption of the WirelessHART communication according to the AES-128 specification
--------------------------------------	------------------------------	---

\* You will find further properties of the device in the following section:

Functions and properties (Page 11)

# Approvals and certificates

## Approvals issued

---

**Note****Issued approvals on the type plate of the device**

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

Approvals for shipbuilding are not printed on the device type plate.

---

## Compliance with telecommunications standards

All WirelessHART devices require certification to ensure that they adhere to regulations regarding the use of the RF spectrum. Nearly every country requires this type of product certification. Siemens cooperates with government bodies worldwide. The aim is to supply fully compliant products and remove the risk of violating country directives or laws governing use of WirelessHart devices.

## Current approvals on the Internet

You will also find the current approvals for the product on the Internet pages of Siemens Industry Online Support under the following entry ID:

39971776 (<http://support.automation.siemens.com/WW/view/en/39971776>)  
→ "Entry list" tab, entry type "Certificates"

## Approvals for SIMATIC NET products

You will find an overview of the approvals for SIMATIC NET products including approvals for shipbuilding on the Internet pages of Siemens Industry Online Support under the following entry ID:

57337426 (<http://support.automation.siemens.com/WW/view/en/57337426>)

## FCC and IC approval

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation. This device must be installed to ensure a minimum antenna separation distance of 20 cm from all persons.

---

### Note

#### Device variant with connector for external antenna (6GK1 411-6CA40-0BA0)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instruction manual, this equipment may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference. In which case users will be required to correct the interference at their own expense.

---

### Note

#### Installation and operation of devices with an external antenna

To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.

---

## FCC USA

- For article number 6GK1 411-6CA40-0AA0: FCC ID: SJC-M2140
- For article number 6GK1 411-6CA40-0BA0: FCC ID: LYH-IEWSNPA1

## Canada

IC Canada

- For article number 6GK1 411-6CA40-0AA0: IC ID: 5853A-M2140
- For article number 6GK1 411-6CA40-0BA0: IC ID: 267AA-IEWSNPA1

## Ordinary Location Certification for FM

As standard, the Link has been examined and tested to determine that the design meets basic electrical, mechanical, and fire protection requirements by FM, a nationally recognized testing laboratory (NRTL) as accredited by the Federal Occupational Safety and Health Administration (OSHA).

## FM certification (explosion protection)



NEMA TYPE 4X  
TEMP CODE T4  
(T<sub>amb</sub> = -40 °C TO 60 °C)

FM Division 2, Non-Incendive

Non-incendive for Class I, Division 2, Groups A, B, C, and D.

Dust Ignition-proof for Class II, III, Division 1,  
Groups E, F, and G; Indoors/outdoor locations;

NEMA Type 4X

Temperature code: T4 (T<sub>a</sub>: - 40 °C to + 60 °C)

## CSA HAZ LOC. (Canadian Standards Association, Hazardous Locations)



TYPE 4X  
TEMP CODE T4

CSA Division 2, Non-Incendive

Suitable for Class I, Division 2, Groups A, B, C, and D.

Dust Ignition-proof for Class II, Groups E, F, and G;

Suitable for Class III Hazardous Locations.;

Install per Siemens drawing A5E02467236A.

Temperature code: T4 (T<sub>a</sub>: - 40 °C to + 60 °C)

CSA Enclosure Type 4X

**CSA certificate of compliance**

2165440 (April 27, 2009)

### Applied standards

CAN/CSA C22.2 No. 0-M91 (R2001) - General Requirements - Canadian Electrical Code, Part II

CSA Std C22.2 No. 30-M1986 - Explosion Proof Enclosures for Use in Class I Hazardous Locations

CAN/CSA C22.2 No. 94-M91 (R2001) - Special Purpose Enclosures

CSA Std C22.2 No. 142-M1987 - Process Control Equipment

CSA Std C22.2 No. 213-M1987 - Non-Incendive Electrical Equipment for Use in Class I, Division 2 Hazardous Locations

### EC declaration of conformity



The EC Declaration of Conformity is available for all responsible authorities at:

Siemens Aktiengesellschaft  
Process Industries and Drives

Process Automation (PD PA)  
76181 Karlsruhe  
Germany

You will find the EC Declaration of Conformity for this product on the Internet at the following address:

10805878 (<http://support.automation.siemens.com/WW/view/en/10805878>)

→ "Entry list" tab

Filter settings:

- Entry type: "Certificates"
- Certificate type: "EC Declaration of Conformity"
- Search item(s): IE/WSN-PA Link

The product described in these operating instructions meets the requirements of the following EC directives:

- 1999/5/EC (R&TTE)

R&TTE directive of the European Parliament and of the Council of 9 March 1999 on Radio Equipment and Telecommunications Terminal Equipment and the mutual recognition of their conformity.

- 94/9/EC (ATEX)

ATEX - Directive of the European Parliament and the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres.

Which of the described standards apply to the products can be found in the section "Products".

The current versions of the standards can be seen in the EC Declaration of Conformity.

**R&TTE****Protection of health and safety****Article 3 (1) a) of the R&TTE directive**

## Harmonized standards

1	EN 61010-1 Safety requirements for electrical equipment for measurement, control and laboratory use. General requirements
2	EN 62479 Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz)

**EMC****Article 3 (1) b) of the R&TTE directive**

## Harmonized standards

3	ETSI EN 301 489-17 Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility for radio equipment and services - Part 17 : Specific conditions for 2.4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5.8 GHz broadband data transmitting systems
4	EN 61326-1 Electrical equipment for measurement, control and laboratory use. EMC requirements. General requirements

**Efficient use of the radio spectrum****Article 3 (2) of the R&TTE directive**

## Harmonized standards

5	ETSI EN 300 328 Electromagnetic compatibility and radio spectrum matters (ERM) - wideband transmission systems - data transmission equipment operating in the 2.4 GHz ISM band and using wideband modulation techniques
---	--

## ATEX

### Harmonized standards

6	EN 60079-0 Explosive atmospheres. Equipment. General requirements
7	EN 60079-15 Explosive atmospheres. Equipment protection by type of protection "n"
8	EN 60079-31 Explosive atmospheres. Equipment dust ignition protection by enclosure "t"

## Products

### Product designation and standards

The standards that apply to the product are described in the sections "R&TTE" and "ATEX".

Article number	Product name	Standards
6GK1411-6CA40-0AA0	IE/WSN-PA Link	1, 2, 3, 4, 5, 6, 7, 8
6GK1411-6CA40-0BA0	IE/WSN-PA Link	1, 2, 3, 4, 5, 6, 7, 8



## ATEX certification (explosion protection)

 **WARNING****No use in hazardous zones with the adapter cable**

Note that using the adapter cable reduces the protection for hazardous areas and that use in the hazardous zones listed in this section is no longer permitted. If you use the Harting adapter cable for the Ethernet connection, the requirements for the hazardous areas approval are no longer met. In this case, if you want to use the device for an application to which hazardous areas directive applies, you will need to obtain approval from the test center responsible.

- N1


ATEX type n

See notes below

Certificate number: Baseefa10ATEX0044X

Certified according to:

- EN 60079-0
- EN 60079-15

ATEX identification mark:  II 3 G

Ex nA IIC T4 Gc (T<sub>a</sub>: - 40 °C to + 65 °C)

Rated voltage: 28 V

- ND


ATEX Dust Ignition-proof

See note below

Certificate number: Baseefa10ATEX0045X

Certified according to:

- EN 60079-0
- EN 60079-31

ATEX identification mark:  II 3 D

Ex tc IIIC T135°C Dc (T<sub>a</sub>: - 40 °C to + 65 °C)

Rated voltage: 28 V

The current versions of the standards can be seen in the currently valid ATEX certificates.

### IECEX certification (explosion protection)

- N7  
IECEX type n  
See notes below  
Certificate number: IECEX BAS 10.0014X  
Certified according to:
  - EN 60079-0
  - EN 60079-15Ex nA IIC T4 Gc (T<sub>a</sub>: - 40 °C to + 65 °C)  
Rated voltage: 28 V
- NF  
IECEX Dust Ignition-proof  
See note below  
Certificate number: IECEX BAS 10.0015X  
Certified according to:
  - IEC 60079-0
  - IEC 60079-31Ex tc IIIC T135°C Dc (T<sub>a</sub>: - 40 °C to + 65 °C)  
Rated voltage: 28 V

The current versions of the standards can be seen in the currently valid IECEX certificates.

### Conditions for safe procedures when installing N1 and N7

The device is not capable of withstanding the 500 V insulation test required by Clause 6.8.1 of EN 60079-15:2005. This must be taken into account when installing the device.

### Conditions for safe procedures when installing N1, N7, ND and NF

---

#### Note

The sheet resistance of the antenna is greater than one gigaohm. It must not be rubbed or cleaned with a dry cloth or solvent to avoid electrostatic charges.

---

## RCM



The device meets the requirements of the AS/NZS 2064 standards (Class A)

## Approval for the People's Republic of China

---

### Note

The IE/WSN-PA Link may only be installed by trained personnel.

After purchase or installation, the antenna may not be removed from the device.

---

## Approval for China

SRRC approval with certification number: CMIIT ID: 2011DJ0423

## Approval for Mexico

Certification number: RCPSIIE10-1312

## Approval for Argentina

Certification number(CNC): C-9870



## Biological compatibility

### Electromagnetic fields and health

The independent German Commission on Radiological Protection was commissioned by the German Federal Ministry for the Environment to determine the possible thermal and non-thermal dangers posed by electromagnetic fields in the range from 0 Hz to 300 GHz according to current scientific knowledge and came to the following conclusion in issue 29 (see References):

"The German Commission on Radiological Protection concludes that according to the latest scientific literature no new scientific research is available with respect to proven health hazards which would throw doubt upon the scientific evaluation which serves as the basis for the ICNIRP safety concepts and the recommendations of the EU commission."

The SSK also concludes that below the current limit values, there is also no scientific suspicion of health risks.

This assessment agrees with those of other national and international scientific commissions and of the WHO ([www.who.int/emf](http://www.who.int/emf)).

Accordingly and in view of the fact that WirelessHART devices are significantly below the scientifically established limit values, it can be assumed that there are no health risks from the electromagnetic fields of WirelessHART products.

For detailed information on this topic, refer to the references.



## References

### B.1 /1/

SIMATIC NET  
WirelessHART  
Getting Started (Application)  
Siemens AG  
53813938 (<http://support.automation.siemens.com/WW/view/en/53813938>)

### B.2 /2/

Limit Values and Precautionary Measures to Protect the General Public from  
Electromagnetic Fields  
Radiation Protection Commission (SSK), Bonn, Germany  
Issue 29, 2001, ISBN 3-437-21527-2  
Internet address SSK: ([www.ssk.de/en](http://www.ssk.de/en))  
Recommendation of the Radiation Protection Commission (SSK) with scientific justification

### B.3 /3/

#### Various information on the topic of electromagnetic fields and science

- World Health Organization WHO: ([www.who.int/emf](http://www.who.int/emf))
- International Commission of Non-ionizing Radiation Protection ICNIRP: ([www.icnirp.de](http://www.icnirp.de))
- German Association for Information Technology, Telecommunications and New Media  
BITKOM: ([www.bitkom.org/de/themen\\_gremien/38383.aspx](http://www.bitkom.org/de/themen_gremien/38383.aspx))

### B.4 /4/

SIMATIC NET  
Industrial Ethernet - Network Manual  
system manual  
Siemens AG  
Entry ID:  
(<http://support.automation.siemens.com/WW/view/en/27069465>)

*References*

---

*B.4 /4/*



# Glossary

## ACL

Access Control List

List with addresses of nodes that have the right to access a network. The access control list serves as access protection for a network.

The IE/WSN-PA Link manages an access control list in which the addresses (device ID) of the WirelessHART sensors allowed to access the connected network (WSN) are administered.

## Bandwidth

Width of a frequency band. The bandwidth that is assigned to a WSN node has a direct influence on the maximum data throughput of its wireless connections with other nodes.

## DHCP

Dynamic Host Configuration Protocol

A protocol for automatic assignment of IP addresses

## Domain name

Name of the domain. A unique identifier used on the Internet. It consists of characters with dots as delimiters, for example: this.domain.com

## HART

Highway Addressable Remote Transducer

HART is a standardized, widespread communications system used to set up industrial fieldbuses. It allows digital communication of multiple nodes (field devices) over a common data bus. HART is based on the widespread 4-20 mA standard (for transmission of analog signals). Existing cables of older systems can be used directly and both systems operated parallel to each other. HART was developed in the 1980's by the Rosemount company for their field devices. In 1989, the HART specification was initiated by the HART Communication Foundation (HCF). HART Communication Foundation in Europe is based in Basle (Switzerland).

## HART Version 7

HCF specification

The main focus is on "WirelessHART" communication of HART devices.

**HCF**

HART Communication Foundation

**Host name**

A unique designator in a domain associated with the IP address of a device. In the address example "device.this.domain.com", "device" is the host name.

**HTML**

Hypertext Markup Language  
Markup language for Websites

**HTTPS**

Hypertext Transfer Protocol Secure  
Protocol for transmission of encrypted data. Expansion of HTTP for secure transmission of confidential data with the aid of SSL.

**ICNIRP**

International Council on Non-Ionizing Radiation Protection

**IEEE**

Institute of Electrical and Electronics Engineers

**IEEE 802.15.4**

Specification for a protocol for wireless data transmission of devices with a low power consumption and short range. It is used mainly for WirelessHART networks (WSN).

**RSSI**

Received Signal Strength Indication  
Value for specifying the received signal strength [dBm].

**Subnet**

A subnet is part of a network whose parameters must be matched. The subnet includes bus components and all the attached stations. Subnets can, for example, be connected together by gateways to form a network.

**WHART**

→ *HART Version 7*

**WirelessHART**

→ *HART Version 7*

**WSN**

Wireless Sensor Network



# Index

## A

Abbreviations/acronyms, 3  
Adding a field device, 38  
AES (encryption method), 41

## B

Burst rate, 23, 56

## C

Certificate (public key), 31  
Certificate, warning / error message, 31  
Components of the IE/WSN-PA Link product, 15  
Configuring the Link  
    Monitor, 65  
    Network, 41  
    Setup, 41  
Connecting the configuration PC, 29  
Contact, 5  
Copyright information, 40  
Current information, 4

## D

Disable channel, 44  
Documentation, 15

## E

Encryption, 42  
Explorer, 65

## F

Factory set password, 28  
FAQs, 4  
Field device, 3  
Firmware  
    Update, 4, 55  
    Version, 3  
Firmware version, 40  
Frequency ranges, 44

## H

Hardware product version, 3  
HART variables, 65

## I

IWLAN node, 44

## J

Join key, 38, 42

## L

License conditions, 40

## M

Management link, 36  
Manual, 40  
Manual on the Internet, 4

## N

Network expansion, 25, 38  
Network ID, 38, 41  
Network key, 42

## O

Obstacles (wireless), 24  
Online help, 40

## P

Password lost, 33, 46

## R

Redundancy  
    Commissioning, 36  
    Diagnostics, 72

- Firmware version, 13
- Function, 13
- Order number, 3
- Project engineering, 44
- Requirements, 35
- Replacing a device, 77
- Roles, 28
- RSSI, 23

## **S**

- Serial number, 40
- Support, 5, 19

## **T**

- Training, 6

## **U**

- Update time, 23, 56
- User roles, 28

## **W**

- Warning message, certificate, 31
- WHART channels, 44
- Wireless channels, 44
- WSN, 3