SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE W760/W720

Operating Instructions

09/2017
C79000-G8976-C322-08

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C322-08
℗ 09/2017 Subject to change

Table of contents

Introduction 1

1.1 Information on the Operating Instructions

Validity of the Operating Instructions

These operating instructions cover the following products:

	Article number of the RoW version	Article number of the US version	Article number of the IL version
Access point			
SCALANCE W761-1 RJ-45	6GK5761-1FC00-0AA0	6GK5761-1FC00-0AB0	-
Ethernet client modules			
SCALANCE W722-1 RJ-45 (iFeatures)	6GK5722-1FC00-0AA0	6GK5722-1FC00-0AB0	6GK5722-1FC00-0AC0
SCALANCE W721-1 RJ-45	6GK5721-1FC00-0AA0	6GK5721-1FC00-0AB0	-

These operating instructions apply to the following software version:

- SCALANCE W760/W720 with firmware as of Version 6.2

Purpose of the Operating Instructions

Using the Operating Instructions, you will be able to install and connect the SCALANCE W760/ W720 correctly. The configuration and the integration of the device in a WLAN are not described in these instructions.

Documentation on the accompanying CD

You will find detailed information about configuration in the SCALANCE W700 configuration manuals on the accompanying SIMATIC NET IWLAN CD under the file name:

PH_SCALANCE-W760-W720-WBM_76.pdf and PH_SCALANCE-W760-W720-CLI_76.pdf

---

Note

Make sure that you read the explanations and instructions in the README.txt file

---

Security information

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

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

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

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information on industrial security measures that may be implemented, please visit
Link (https://www.siemens.com/industrialsecurity)

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
Link (https://www.siemens.com/industrialsecurity).

Trademarks

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

SIMATIC NET, SCALANCE, C-PLUG, RCoax

2 Security recommendations

To prevent unauthorized access, note the following security recommendations.

General

- You should make regular checks to make sure that the device meets these recommendations and/or other security guidelines.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- For communication via non-secure networks use additional devices with VPN functionality to encrypt and authenticate the communication.
- Terminate management connections correctly (WBM. Telnet, SSH etc.).

See also

Cell (https://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx)

Physical access

- Restrict physical access to the device to qualified personnel.
- The memory card or the PLUG (C-PLUG, KEY-PLUG, security PLUG) contains sensitive data such as certificates, keys etc. that can be read out and modified.

Software (security functions)

- Keep the software up to date. Check regularly for security updates of the product.
  You will find information on this on the Internet pages "Industrial Security"
- Inform yourself regularly about security advisories and bulletins published by Siemens ProductCERT.
- Only activate protocols that you really require to use the device.
- Use the security functions such as address translation with NAT (Network Address Translation) or NAPT (Network Address Port Translation) to protect receiving ports from access by third parties.
- Restrict access to the device with a firewall or rules in an access control list (ACL - Access Control List).

- If RADIUS authentication is via remote access, make sure that the communication is within the secured network area or is via a secure channel.
- The option of VLAN structuring provides good protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.
- Enable logging functions. Use the central logging function to log changes and access attempts centrally. Check the logging information regularly.
- Configure a Syslog server to forward all logs to a central location.
- Use WPA2/ WPA2-PSK with AES to protect the WLAN. If iPCF or iPCF-MC is used, use the AES encryption.

See also

Product cert (http://www.siemens.com/cert/en/cert-security-advisories.htm)

http://www.siemens.com/industrialsecurity (http://www.siemens.com/industrialsecurity)

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update passwords and keys to increase security.
- Change all default passwords for users before you operate the device.
- Only use passwords with a high password strength. Avoid weak passwords for example password1, 123456789, abcdefgh.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.
- Do not use the same password for different users and systems or after it has expired.

Keys and certificates

This section deals with the security keys and certificates you require to set up HTTPS (HyperText Transfer Protocol Secured Socket Layer).

- We strongly recommend that you create your own HTTPS certificates and make them available.
  There are preset certificates and keys on the device. The preset and automatically created HTTPS certificates are self-signed.
  We recommend that you use HTTPS certificates signed either by a reliable external or by an internal certification authority. The HTTPS certificate checks the identity of the device and controls the encrypted data exchange. You can install the HTTPS certificate via the WBM (System > Load and Save).
- Handle user-defined private keys with great caution if you use user-defined SSH or SSL keys.
- Use the certification authority including key revocation and management to sign the certificates.
- Verify certificates and fingerprints on the server and client to avoid "man in the middle" attacks.

- We recommend that you use certificates with a key length of 2048 bits.
- Change keys and certificates immediately, if there is a suspicion of compromise.

Secure/non-secure protocols

- For the DCP function, enable the "DCP read-only" mode after commissioning.
- Avoid and disable non-secure protocols, for example Telnet and TFTP. For historical reasons, these protocols are still available, however not intended for secure applications. Use non-secure protocols on the device with caution.
- The following protocols provide secure alternatives:
  - SNMPv1/v2 → SNMPv3
    Check whether use of SNMPv1 is necessary. SNMPv1 is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options.
    If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
    Use SNMPv3 in conjunction with passwords.
  - HTTP → HTTPS
  - Telnet → SSH
  - SNTP → NTP
- Use secure protocols when access to the device is not prevented by physical protection measures.
- To prevent unauthorized access to the device or network, take suitable protective measures against non-secure protocols.
- If you require non-secure protocols and services, operate the device only within a protected network area.
- Restrict the services and protocols available to the outside to a minimum.

Available protocols per port

The following list provides you with an overview of the open ports on this device.

The table includes the following columns:

- **Protocol**
  All protocols that the device supports
- **Port number**
  Port number assigned to the protocol
- **Port status**
  - Open
    The port is always open and cannot be closed.
  - Open (when configured)
    The port is open if it has been configured.

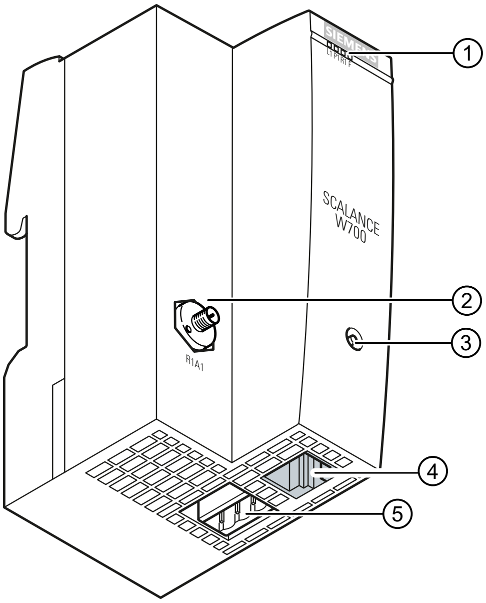
- **Factory setting**
  - Open
    The factory setting of the port is "Open".
  - Closed
    The factory setting of the port is "Closed".
- **Authentication**
  Specifies whether or not the protocol is authenticated.

Protocol	Port number	Port status	Factory setting of the port	Authentication
SSH	TCP/22	Open (when configured)	Open	Yes
TELNET	TCP/23	Open (when configured)	Open	Yes
HTTP	TCP/80	Open (when configured)	Open	Yes
HTTPS	TCP/443	Open (when configured)	Open	Yes
SNTP NTP	UDP/123	Open (when configured)	Closed	No
SNMP	UDP/161	Open (when configured)	Open	Yes
PROFINET	UDP/34964, UDP/49154, 49155	Open	Open	No
Syslog	UDP/514	Open (when configured)	Open	No
EtherNet/IP	TCP/44818, UDP/ 2222,44818	Open (when configured)	Open	No
DHCP	UDP/67,68	Open (when configured)	Closed	No
RADIUS	UDP/ 1812,1813	Open (when configured)	Closed	No
TFTP	UDP/69	Open (when configured)	Closed	No

Description of the device 3

3.1 Description of the device

W76x / W72x



① LEDs

② Antenna connector

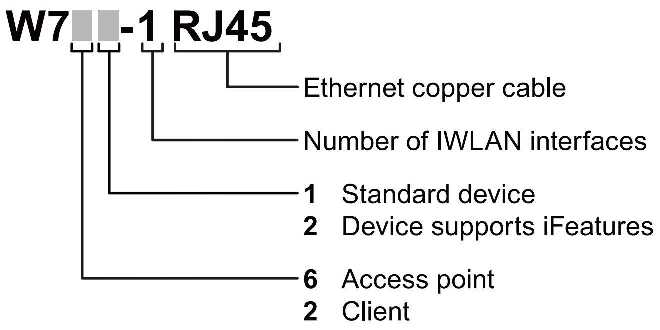
③ RESET button

④ Ethernet connector

⑤ Connector for power supply and grounding

3.2 Structure of the type designation

The type designation of the device is made up of several parts that have the following meaning:



3.3 Components of the product

The following components are supplied with the product:

- SCALANCE W761 or SCALANCE W722 or SCALANCE W721
- 1 protective cap for the antenna socket
- A 3-pin terminal block for the power supply
- SIMATIC NET Industrial Wireless LAN CD

Please check that the consignment you have received is complete. If the consignment is incomplete, contact your supplier or your local Siemens office.

3.4 Accessories

Technical data subject to change.

You will find further information on the accessories program in the Industry Mall. (https://mall.industry.siemens.com)

Cables Industrial Ethernet

Component	Description	Article number
IE FC TP STANDARD CABLE GP2X2 (PROFINET type A)	Standard bus cable, TP installation cable for connection to FC OUTLET RJ-45, for universal use, 4-wire, shielded, CAT 5E Sold by the meter	6XV1840-2AH10
IE FC TP ROBUST STANDARD CABLE GP 2X2 (PROFINET type A)	Standard bus cable, ATPE outer jacket for connection to FC RJ-45 PLUG and FC OUTLET RJ-45, fixed installation, for universal use, 4-wire, shielded, CAT 5 Sold by the meter	6XV1841-2A
IE FC TP ROBUST FLEXIBLE CABLE GP 2X2 (PROFINET type B)	Flexible bus cable, TPE outer jacket for connection to FC RJ-45 PLUG and FC OUTLET RJ-45, flexible wires, 4-wire, shielded, CAT 5 Sold by the meter	6XV1841-2B
IE FC TP FLEXIBLE CABLE GP 2X2 (PROFINET type B)	Flexible bus cable, TP installation cable, flexible wires, shielded, CAT 5 Sold by the meter	6XV1870-2B
IE FC TP TRAILING CABLE 2X2 (PROFINET type C)	Highly flexible bus cable, TP installation cable for connection to FC OUTLET RJ-45, for use in drag chains, 4-wire, shielded, CAT 5 Sold by the meter	6XV1840-3AH10
IE TP TORSION CABLE 2X2 (PROFINET type C)	Highly flexible bus cable, TP installation cable for use in highly flexible applications (torsion), 4-wire Sold by the meter	6XV1870-2F
IE CONNECTING CABLE M12-180/IE RJ45	Flexible IE connecting cable, 4-wire, preassembled with a 4-pin M12 plug (D-coded) and an IE FC RJ-45 plug 145	6XV1871-5T*
IE CONNECTING CABLE M12-180/M12-180	Flexible IE connecting cable, 4-wire, preassembled with two 4-pin M12 plugs (D-coded)	6XV1870-8A*

* Available in different lengths

Cabinet feedthrough

Component	Description	Article number
IE M12 PANEL FEEDTHROUGH	Cabinet feedthrough for conversion from M12 connector technology (D-coded, IP65) to RJ-45 connector technology (IP20) pack of 5	6GK1901-0DM20-2AA5
IE M12 PANEL FEEDTHROUGH PRO	Cabinet feedthrough for conversion from M12 connector technology (D-coded, IP65) to M12 connector technology (D-coded, IP65) pack of 5	6GK1901-0DM30-2AA5
IE M12 PANEL FEEDTHROUGH 4X2	Cabinet feedthrough for conversion from M12 connector technology (X-coded, IP65/67) to RJ-45 connector technology (X-coded, IP20) pack of 5	6GK1901-0DM40-2AA5
N-Connect/N-Connect female/female Panel Feedthrough	Panel feedthrough for wall thicknesses up to a maximum of 4.5 mm, two N-Connect female connectors.	6GK5798-2PP00-2AA6
N-Connect/SMA-Connect female/female Panel Feedthrough	Panel feedthrough for wall thicknesses up to a maximum of 5.5 mm, two N-Connect/SMA female connectors.	6GK5798-0PT00-2AA6

Lightning protection

Component	Description	Article number
LP798-1N	Lighting protector with N/N female/female connector with gas discharge technology	6GK5798-2LP00-2AA6
LP798-2N	Lighting protector with N/N female/female connector with quarter wave technology	6GK5798-2LP10-2AA6

Terminating resistor

Component	Description	Article number
TI795-1R	Electrical connection RSMA-Connect, male	6GK5795-1TR10-0AA6

3.4.1 Flexible connecting cables and antennas

3.4.1.1 Flexible connecting cables

Flexible connecting cable N-Connect/R-SMA

Flexible connecting cable for connecting an antenna to a SCALANCE W700 with R-SMA connectors, preassembled with a connector N-male and R-SMA male

Length	Article number
0.3 m	6XV1875-5CE30
1 m	6XV1875-5CH10
2 m	6XV1875-5CH20
5 m	6XV1875-5CH50
10 m	6XV1875-5CN10

For railway applications, the following connecting cable are available:

Length	Article number
1 m	6XV1875-5TH10
2 m	6XV1875-5TH20
5 m	6XV1875-5TH50

Flexible connecting cable N-Connect/N-Connect

Flexible connecting cable for connecting an antenna to a SCALANCE W700 with N-Connect connectors.
Preassembled with two N male connectors:

Length	Article number
1 m	6XV1875-5AH10
2 m	6XV1875-5AH20
5 m	6XV1875-5AH50
10 m	6XV1875-5AN10

For railway applications, the following connecting cable are available:

Length	Article number
1 m	6XV1875-5SH10
2 m	6XV1875-5SH20
5 m	6XV1875-5SH50

Flexible connecting cable IWLAN QMA/N-Connect male/female

Adapter cable for connecting a MIMO antenna with QMA connectors with the flexible connecting cables. Preassembled with two connectors QMA male and N-Connect female. pack of 3

Length	Article number
1 m	6XV1875-5JH10

For railway applications, the following connecting cable is available Note: Scope of delivery: Pack of 1

Length	Article number
1 m	6XV1875-5VH10

3.4.1.2 Antennas

Note

When you select an antenna, keep in mind the national approvals for your device.

You will find more information in the following Link (http://www.siemens.com/wireless-approvals)

Type	Properties	Article number
ANT792-4DN	RCoax helical antenna, circular polarization, 4 dBi, 2.4 GHz, N-Connect female.	6GK5792-4DN00-0AA6
ANT792-6MN	Omni antenna, mast/wall mounting, 6 dBi 2.4 GHz, N-Connect female	6GK5792-6MN00-0AA6
ANT792-8DN	Directional antenna, mast/wall mounting, 14 dBi 2.4 GHz, N-Connect female	6GK5792-8DN00-0AA6
ANT793-4MN	RCoax λ5/8 antenna with vertical polarization, 6 dBi, 5 GHz, N-Connect female.	6GK5793-4MN00-0AA6
ANT793-6DG	Wide angle antenna, mast/wall mounting, 9 dBi 5 GHz, 2 x N-Connect female	6GK5793-6DG00-0AA0
ANT793-6DT	Wide angle antenna (MIMO), mast/wall mounting, 8 dBi 5 GHz, 3 x QMA connector female	6GK5793-6DT00-0AA0
ANT793-6MN	Omni antenna, mast/wall mounting, 5 dBi 5 GHz, N-Connect female	6GK5793-6MN00-0AA6
ANT793-8DJ	Directional antenna, mast/wall mounting, 18 dBi 5 GHz, 2 x N-Connect female	6GK5793-8DJ00-0AA0
ANT793-8DK	Directional antenna, mast/wall mounting, 23 dBi 5 GHz, 2 x N-Connect female	6GK5793-8DK00-0AA0

Type	Properties	Article number
ANT795-4MA	Omni antenna, directly on the device, 3/5 dBi 2.4 GHz and 5 GHz, IP30, R-SMA connector male for direct mounting on the device, connector angle adjustable 0° to 180°.	6GK5795-4MA00-0AA3
ANT795-4MC	Omnidirectional antenna, 3/5 dBi, 2.4 GHz and 5 GHz, IP65, N-Connect male for direct installation on the device, straight connector.	6GK5795-4MC00-0AA3
ANT795-4MD	Omnidirectional antenna, 3/5 dBi, 2.4 GHz and 5 GHz, IP65, N-Connect male for direct installation on the device, 90° connector.	6GK5795-4MD00-0AA3
ANT795-6DC	Wide angle antenna, mast/wall mounting, 9 dBi 2.4 GHz and 5 GHz, N-Connect female	6GK5795-6DC00-0AA0
ANT795-4MB	Omnidirectional antenna, 2/3 dBi 2.4 GHz and 5 GHz, IP30, R-SMA connector female for direct mounting on the device, connector angle adjustable 0° to 90°.	6GK5795-4MB00-0Ax0
ANT795-6MN	Omni antenna, mounted on roof/vehicle, 6/8 dBi 2.4 GHz and 5 GHz, N-Connect female	6GK5795-6MN10-0AA6
ANT795-6MT	Omni antenna (MIMO), mounted on roof/vehicle/ceiling, 5/7 dBi 2.4 GHz and 5 GHz, 3 x QMA connector female	6GK5795-6MT00-0AA0
ANT793-8DL	Directional antenna vertical-horizontal polarized, 5 GHz, 14dBi, IP66, 2xN-Connect female	6GK5793-8DL00-0AA0
ANT793-8DP	Directional antenna, mast/wall mounting, 13 / 13.5 dBi 4.9 GHz and 5 GHz, N-Connect female	6GK5793-8DP00-0AA0
ANT795-4MX	Omnidirectional antenna, 2/2,5 dBi, 2.4 GHz and 5 GHz, IP69K, N-Connect male	6GK5795-4MX00-0AA0
ANT795-6MP	Omnidirectional antenna, 5/7 dBi, 2.4 GHz and 5 GHz, IP65/67, N-Connect female	6GK5795-6MP00-0AA0
ANT896-6MM	Omnidirectional antenna for mobile wireless, WLAN and GPS, WLAN: 6/7 dBi, 2.4 GHz and 5 GHz, IP68, IP69 K, QMA-Connect female, port 2	6GK5896-6MM00-0AA0
IWLAN RCoax Cable 2,4 GHz PE 1/2"	Omni antenna, 0 dBi 2.400 - 2.485 GHz, N-Connect female.	6XV1875-2A
IWLAN RCoax Cable 5 GHz PE 1/2"	Omni antenna, 0 dBi 5.150 – 5.875 GHz, N-Connect female.	6XV1875-2D

NOTICE
ANT795-4MA The ANT795-4MA antenna has degree of protection IP30 and is therefore only suitable for dry environments.

Note

ANT793-8DJ

The antenna ANT793-8DJ may only be used with the flexible connecting cable 6XV1875-5CH50 (5 m length) or 6XV1875-5CN10 (10 m length). Other flexible connecting cables are not permitted.

Notice for USA/Canada

Only one antenna per device can be used (connected to R1A1, R1A2 or R2A1, R2A2).

Note

ANT793-8DK

The antenna ANT793-8DK may only be used with the flexible connecting cable 6XV1875-5CN10 (10 m length). Other flexible connecting cables are not permitted.

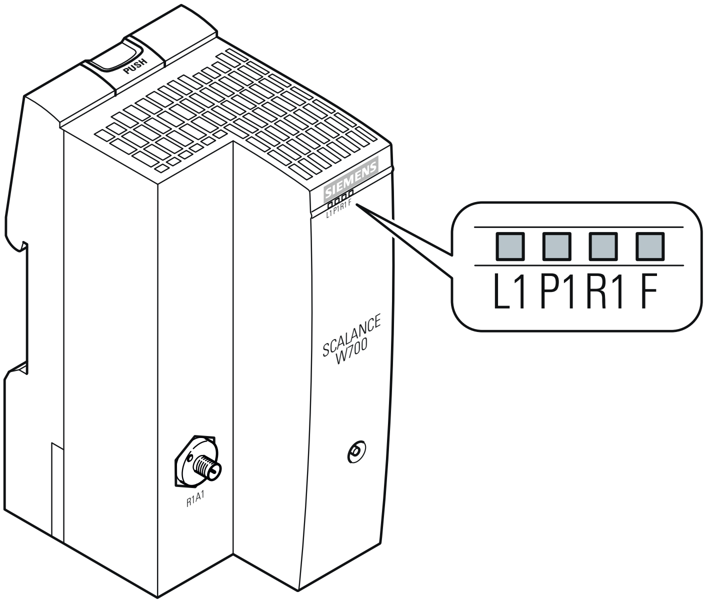
Notice for USA/Canada

Only one antenna per device can be used (connected to R1A1, R1A2 or R2A1, R2A2).

3.5 LED display

Information on operating status and data transfer

On the front of the housing, several LEDs provide information on the operating status of the device:



LED	Color	Meaning
L1	Green	Power supply L1.
P1	Green	There is a connection via the Ethernet interface (Link).
	Green and yellow flashing alternately	Data transfer via the Ethernet interface.
R1	Green	*SCALANCE W760 in access point mode:* The WLAN interface is initialized and ready for operation. *SCALANCE W760 in client mode or SCALANCE W720:* There is a connection via the WLAN interface.
	Green and yellow flashing alternately	Data transfer over the WLAN interface.
	Green flashing briefly	*SCALANCE W760 in access point mode:* With 802.11h, the channel is scanned for one minute for primary users before the channel can be used for data traffic. *SCALANCE W760 in client mode or SCALANCE W720:* The client waits for the MAC address due to the setting "Automatic" for the "MAC mode" parameter and is connected to no access point.
	Green flashing 3 x short, 1 x long	*SCALANCE W760 in client mode or SCALANCE W720:* The client waits for the MAC address due to the setting "Automatic" for the "MAC mode" parameter and is connected to an access point.

LED	Color	Meaning
F	Red	An error occurred during operation with the device.
	Red R1 flashing yellow at the same time	A primary user was detected on all enabled channels. (only when DFS is enabled or according to IEEE 802.11h)
P1 R1	Flashing yellow	"Flashing" enabled using SIMATIC NET Primary Setup Tool (PST).

Note

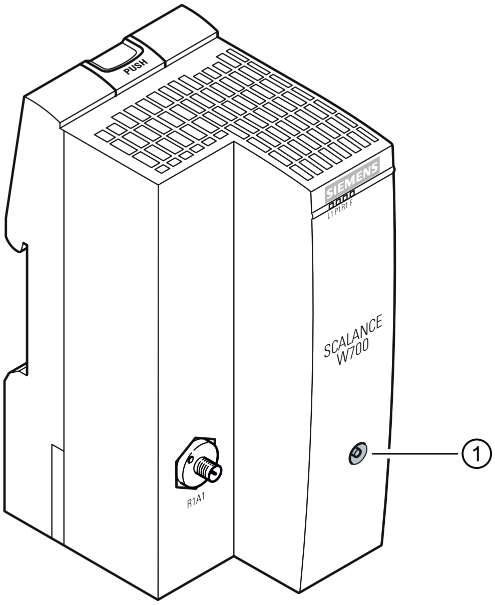
Primary user (radar) on all enabled channels (only when DFS is enabled)

If the device detects a primary user (for example radar signals) on all enabled channels of the WLAN interface, the LED **F** is lit and **R1** flashes. No data traffic is then possible for the next 30 minutes. After this time, the device runs the scan again and checks whether a primary user still exists. If no primary user is detected, data traffic is possible again.

The wait time of 30 minutes is necessary due to legal requirements and cannot be shortened even by restarting the device.

3.6 Reset button

The reset button (position ①) is on the front of the housing:



Functions of the reset button

The reset button has the following functions:

- **Restart of the device**
  To restart the device, press the reset button briefly.

  Note

  If you make changes to the configuration and restart immediately afterwards with the reset button, the changes may be lost. If you restart the device using the WBM (menu command "System > Restart") or using the CLI (command "restart" in the Privileged EXEC Modus), the configuration changes are always retained.

  Upkeep and maintenance

- **Loading new firmware**
  If the "Load & Save" menu command of Web Based Management is unsuccessful, the reset button can be used to load new firmware. This situation can occur if there is a power outage during the normal firmware update. You will find further information in the configuration manual in Downloading new firmware using TFTP without WBM and CLI (Page 41).

- **Resetting the device to the factory defaults**
  The device can be reset to the factory defaults during operation. You will find more detailed information in the configuration manual in Resetting the device to factory defaults (Page 40).

NOTICE
Previous settings If you reset, all the changes you have made will be overwritten by factory defaults.

NOTICE
Inadvertent reset An inadvertent reset can cause disturbances and failures in the configured network with further consequences.

Mounting 4

⚠ CAUTION
Minimum distance to antennas
Fit the device so that there is a minimum clearance of 20 cm between antennas and persons.

⚠ WARNING
If a device is operated in an ambient temperature of more than 50 °C, the temperature of the device housing may be higher than 70 °C. The device must therefore be installed so that it is only accessible to service personnel or users that are aware of the reason for restricted access and the required safety measures at an ambient temperature higher than 50 °C.

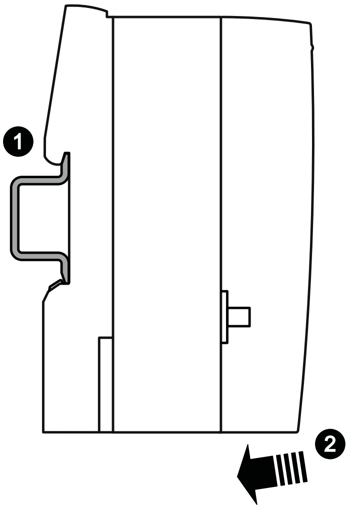
⚠ WARNING
When used in hazardous environments corresponding to Class I, Division 2 or Class I, Zone 2, the device must be installed in a cabinet or a suitable enclosure.

General notes on use according to ATEX and IECEx

⚠ WARNING
To comply with EC Directive 2014/34/EU (ATEX 114) or the conditions of IECEx, this enclosure or cabinet must meet the requirements of at least IP54 in compliance with EN 60529.

4.1 Installing on a DIN rail / removing

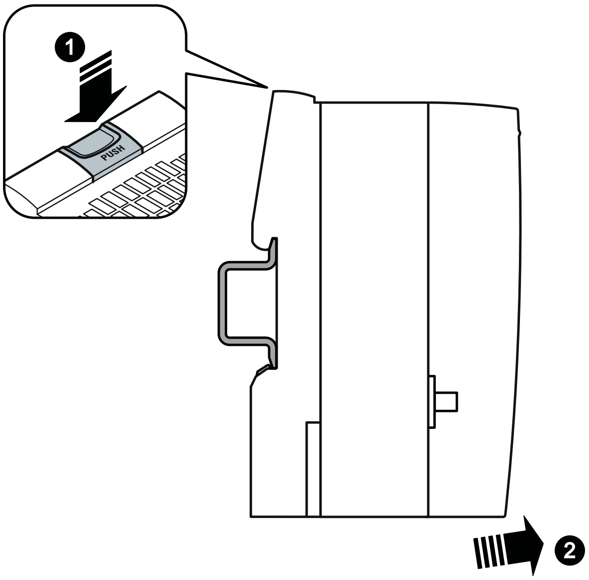
Procedure for installation



Follow the steps below to fit the SCALANCE W760/W720 to a DIN rail:

1. Place the device on the upper edge of the DIN rail as shown in the figure.
2. Press the device against the DIN rail until the DIN rail slider catch locks in place.
3. Mount the connecting cables and the antenna, see section "Connecting up (Page 29)".

Procedure when removing



Follow the steps below to remove the SCALANCE W760/W720 from a DIN rail:

1. Turn off the power to the device.
2. Disconnect all connected cables.
3. Press the release button on the top of the device to release the DIN rail catch.
4. Tilt the SCALANCE W760/W720 forward and remove the device from the DIN rail.

Connection 5

Safety notices

When connecting up the device, keep to the safety notices listed below.

⚠ **WARNING**

EXPLOSION HAZARD

SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2 OR ZONE 2.

⚠ **WARNING**

EXPLOSION HAZARD

DO NOT OPEN WHEN ENERGIZED.

Note

Strain relief of the interfaces

To prevent weights or mechanical movement that can affect an interface causing interrupted contact, fix the cables to a cable guide or rail at short intervals.

5.1 Lightning protection, power supply and grounding

Lightning protection

⚠ WARNING

Danger due to lightning strikes

Antennas installed outdoors must be within the area covered by a lightning protection system. Make sure that all conducting systems entering from outdoors can be protected by a lightning protection potential equalization system.

When implementing your lightning protection concept, make sure you adhere to the VDE 0182 or IEC 62305 standard.

Suitable lightning protectors are available in the accessories (Page 14) of SIMATIC NET Industrial WLAN.

Note

We recommend that you use the maintenance-free lightning protector LP798-2N.

Exception: When there is also DC power supplied via the antenna cable. In this case, only the lightning protector LP798-1N can be used.

⚠ WARNING

Danger due to lightning strikes

Installing this lightning protector between an antenna and a SCALANCE W700 is not adequate protection against a lightning strike. The LP798-1N lightening protector only works within the framework of a comprehensive lightning protection concept. If you have questions, ask a qualified specialist company.

Note

The requirements of EN61000-4-5, surge immunity tests on power supply lines, are met only when a Blitzductor is used with 24 VDC:

BVT AVD 24
article number: 918 422
Manufacturer: DEHN+SÖHNE GmbH+Co.KG, Hans Dehn Str. 1, Postfach 1640,
D - 92306 Neumarkt, Germany

Supply voltage

WARNING

Safety extra low voltage

The equipment is designed for operation with Safety Extra-Low Voltage (SELV) by a Limited Power Source (LPS).

This means that only SELV / LPS (Limited Power Source) complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 must be connected to the power supply terminals or the power supply unit for the equipment power supply must comply with NEC Class 2, as described by the National Electrical Code (r) (ANSI / NFPA 70).

If the equipment is connected to a redundant power supply (two separate power supplies), both must meet these requirements.

WARNING

Transient overvoltages

Take measures to prevent transient voltage surges of more than 40% of the rated voltage. This is the case if you only operate devices with SELV (safety extra-low voltage).

Grounding

WARNING

Danger to life from overvoltage, fire hazard

When using outdoor antennas, the shared or even grounded pin of the circuit must be connected to the shield of the coaxial cable and with all touchable conductive parts and circuits. Otherwise, in the event of a fault there may be illegally high voltages on touchable parts.

NOTICE

Damage to the device due to potential differences

To fully eliminate the influence of electromagnetic interference, the device must be grounded. There must be no potential difference between the following parts, otherwise the device or other connected device could be severely damaged:

- Grounding pin of the SCALANCE W700 and the ground potential of the antenna.
- Grounding pin of the SCALANCE W700 and the ground potential of a device connected over Ethernet.
- Grounding pin of the SCALANCE W700 and the shield contact of the connected Ethernet cable.

Connect both grounds to the same foundation earth or use an equipotential bonding cable.

General notes on use according to ATEX and IECEx

⚠ WARNING

EXPLOSION HAZARD

DO NOT CONNECT OR DISCONNECT EQUIPMENT WHEN A FLAMMABLE OR COMBUSTIBLE ATMOSPHERE IS PRESENT.

General notes on use in hazardous areas according to UL-HazLoc

⚠ WARNING

EXPLOSION HAZARD

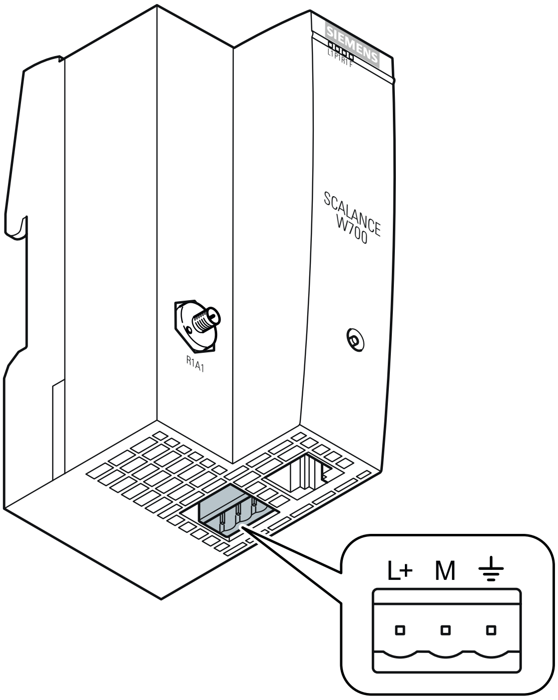
DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS AREA IS KNOWN TO BE NON-HAZARDOUS.

This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D or non-hazardous locations only.

This equipment is suitable for use in Class I, Zone 2, Group IIC or non-hazardous locations only.

5.2 Power supply

The power is supplied to the SCALANCE W760/W720 via the three-pin socket. Here the device is also grounded.



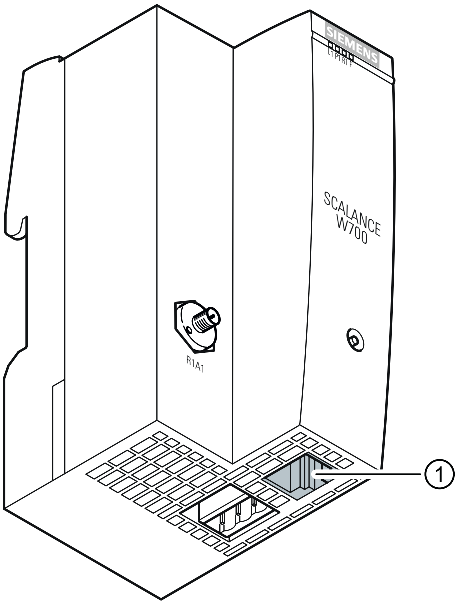
Socket

The three-pin socket has the following pin assignment:

Pin	Assignment
L+	+24 VDC
M	Ground
⏚	Grounding

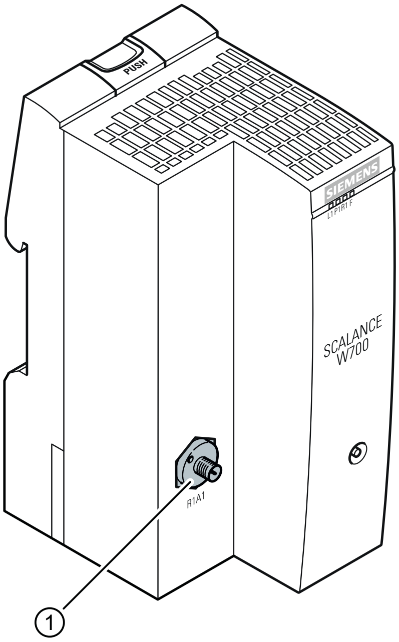
5.3 Ethernet

The SCALANCE W760/W720 has two Ethernet interfaces located on the underside of the device (position ①).



5.4 Antenna connector

The SCALANCE W760/W720 has an antenna connector R1 A1 of the type R-SMA located on the front of the device (position ①).



Procedure

Follow the steps below to connect a cable for an external antenna to a SCALANCE W760/720:

1. Insert the connector on the antenna cable into the R-SMA socket R1 A1 (position ①) and tighten the retainer nut on the socket (key size SW8, tightening torque 1 Nm).

Note

Cabinet installation

When installing the SCALANCE W760/720 in a cabinet, you need to use a detached antenna. Suitable flexible connecting cables for a connection between SCALANCE W760/720 and a detached antenna are available from SIMATIC NET. You will find detailed information in the following section.

5.5 Grounding

A functional grounding must be established for example by connecting a cable from the three-pin socket to the DIN rail, refer to the section "Description of the device (Page 11)“ or section “Power supply (Page 33)“. Such a cable should be kept as short as possible.

If cables are installed permanently, it is advisable to remove the insulation of the shielded cable and to establish contact on the shield/PE conductor bar.

Upkeep and maintenance

6

6.1 Device configuration with PRESET-PLUG

Please not the additional information and security notes in the operating instructions of your device.

NOTICE
Do not remove or insert a PLUG during operation
A PLUG may only be removed or inserted when the device is turned off.

Note

Support as of V6.0

The PRESET-PLUG functionality is supported as of firmware version V6.0.

With the PRESET-PLUG, you can install the same device configuration (start configuration, user accounts, certificates) including the corresponding firmware on multiple devices.

The PRESET PLUG is write-protected.

You configure the PRESET PLUG using the Command Line Interface (CLI).

Creating a PRESET-PLUG

You create the PRESET PLUG using the Command Line Interface (CLI). You can create a PRESET-PLUG from any PLUG. To do this, follow the steps outlined below:

Note

Using configurations with DHCP

Create a PRESET-PLUG only from device configurations that use DHCP. Otherwise disruptions will occur in network operation due to multiple identical IP addresses.

You assign fixed IP addresses extra following the basic installation.

Requirement

- A PLUG is inserted in the device on which you want to configure the PRESET-PLUG functionality.

Procedure

1. Start the remote configuration using Telnet (CLI) and log on with a user with the "admin" role.
2. Change to the Global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.

4. Create the PRESET-PLUG with the "presetplug" command.
   The firmware version of the device and the current device configuration incl. user accounts and certificates are stored on the PLUG and the PLUG is then write protected.
5. Turn off the power to the device.
6. Remove the PRESET-PLUG.
7. Start the device either with a new PLUG inserted or with the internal configuration.

Procedure for installation with the aid of the PRESET-PLUG

1. Turn off the power to the device.
2. If it exists, remove the PLUG from the slot. You will find further information on this in the operating instructions of your device.
3. Insert the PRESET-PLUG correctly oriented into the slot. The PRESET-PLUG is correctly inserted when it is completely inside the device and does not jut out of the slot.
4. Turn on the power to the device again.
   If there is a different firmware version on the device to be installed compared with that on the PRESET-PLUG, an upgrade/downgrade of the firmware is performed. You can recognize this by the red F-LED flashing (flashing interval 2 sec. on/2 sec. off). Afterwards the device is restarted and the device configuration incl. users and certificates on the PRESET-PLUG is transferred to the device.
5. Wait until the device has fully started up.
   (the red F-LED is off)
6. Turn off the power to the device after the installation.
7. Remove the PRESET-PLUG.
8. Start the device either with a new PLUG inserted or with the internal configuration.

Note

KEY-PLUG

If you have created the PRESET-PLUG from a KEY-PLUG, for operation with this configuration, you require an inserted KEY-PLUG.

IN this case before recommissioning the device you need to insert the relevant KEY-PLUG.

Note

Restore factory defaults and restart with a PRESET PLUG inserted

If you reset a device to the factory defaults, when the device restarts an inserted PRESET PLUG is formatted and the PRESET PLUG functionality is lost. You then need to create a new PRESET PLUG. The keys stored on the KEY-PLUG for releasing functions are retained.

We recommend that you remove the PRESET PLUG before you reset the device to the factory settings.

Formatting a PRESET-PLUG (resetting the preset function)

You format the PRESET PLUG using the Command Line Interface (CLI) to reset the preset function. To do this, follow the steps outlined below:

1. Start the remote configuration using Telnet (CLI) and log on with a user with the "admin" role.
2. Change to the Global configuration mode with the command "configure terminal".
3. You change to the PLUG configuration mode with the "plug" command.
4. Enter the command "factoryclean".
   The PRESET-PLUG is formatted and the preset function is reset.
5. Write the current configuration of the device with the "write" command.

6.2 Restoring the factory settings

NOTICE

Previous settings

If you reset, all the settings you have made will be overwritten by factory defaults.

NOTICE

Inadvertent reset

An inadvertent reset can cause disturbances and failures in a configured network with further consequences.

With the reset button

When pressing the button, remember the information in the section "Reset button" in the operating instructions.

Follow the steps below to reset the device parameters to the factory settings:

1. Turn off the power to the device.
2. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit.
4. Now release the button and wait until the fault LED (F) goes off again.
5. The device then starts automatically with the factory settings.

Via the configuration

You will find detailed information on resetting the device parameters using the WBM and CLI in the configuration manuals:

- Web Based Management, section "Restart"
- Command Line Interface, section "Reset and Defaults"

6.3 Firmware update via WBM or CLI not possible

Cause

If there is a power failure during the firmware update, it is possible that the device is no longer accessible using Web Based Management or the CLI.

When pressing the button, make sure you adhere to the instructions in the section "Reset button".

Solution

You can then also assign firmware to a SCALANCE W700 using TFTP.
Follow the steps below to load new firmware using TFTP:

1. Turn off the power to the device.
2. Now press the Reset button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED (F) starts to flash after approximately 2 seconds.
4. Now release the button. The bootloader waits in this state for a new firmware file that you can download by TFTP.
5. Connect a PC to the SCALANCE W700 over the Ethernet interface.
6. Assign an IP address to the SCALANCE W700 with the Primary Setup Tool.
7. Open a DOS box and change to the directory where the file with the new firmware is located and then execute the command "tftp -i <ip address> PUT <firmware>". As an alternative, you can use a different TFTP client.
8. Close the cover to ensure that the device is closed and water and dust proof.

Note

Use of CLI and TFTP in Windows 7

If you want to access the CLI or TFTP in Windows 7, make sure that the relevant functions are enabled in Windows 7.

Result

The firmware is transferred to the device.

Note

Please note that the transfer of the firmware can take several minutes. During the transmission, the red error LED (F) flashes.

Once the firmware has been transferred completely to the device, the device is restarted automatically.

Technical data 7

The following technical specifications apply to the following devices:

- SCALANCE W761-1 RJ-45
- SCALANCE W722-1 RJ-45
- SCALANCE W721-1 RJ-45

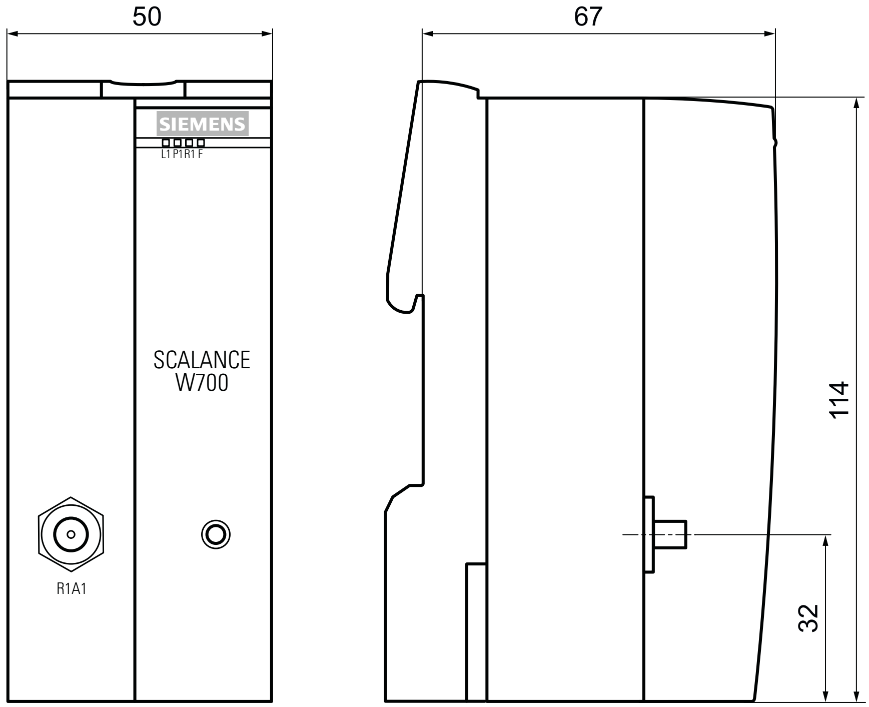
Note

You will find detailed information on the transmit power and receiver sensitivity in the document "Performance data 802.11 abgn SCALANCE W760/W720" on the supplied data medium (REF_W760-RadioInterface.pdf).

SCALANCE W761/W722/W721		
Data transfer		
Ethernet transfer rate		10 / 100 Mbps
Wireless transmission rate		1 ... 150 Mbps
Wireless standards supported		IEEE 802.11a IEEE 802.11b IEEE 802.11g IEEE 802.11n
Attachment to Industrial Ethernet		
	Quantity	1
	Design	RJ-45 jack
	Properties	Half duplex/full duplex, autocrossover, autonegotiation, autosensing, floating
Permitted cable lengths (Ethernet)	**(Alternative combinations per length range)**	
	IE TP torsion cable	0 ... 55 m 0 ... 45 m + 10 m TP cord
	IE FC TP marine cable IE FC TP trailing cable IE FC TP flexible cable IE FC TP FRNC cable IE FC TP festoon cable IE FC TP food cable	0 ... 85 m 0 ... 75 m + 10 m TP cord
	IE FC TP standard cable	0 ... 100 m 0 ... 90 m + 10 m TP cord
Wireless interface		

SCALANCE W761/W722/W721		
Antenna connector	Quantity	1
	Design	R-SMA female
	Impedance	50 Ω nominal
Frequency range		2412 ... 2480 MHz 4920 ... 5875 MHz
Electrical data		
Power supply	Supply voltage	24 VDC Safe Extra Low Voltage (SELV)
	Permitted range	19.2 to 28.8 VDC
	Design	Terminal block, 3 terminals
Fusing		2.5 A / 24 VDC
Current consumption	At 24 VDC / typical	150 mA
Power loss at 24 VDC	At 24 VDC / typical	3.6 W
Permitted ambient conditions		
Ambient temperature	During operation with the rack installed horizontally / vertically	0 ℃ to +55 ℃
	During storage	-40 ℃ to +85 ℃
	During transportation	-40 ℃ to +85 ℃
Relative humidity	During operation	≤ 95% at 25 °C, no condensation
Operating altitude	During operation	≤ 2,000 m above sea level at max. 55 °C ambient temperature
Contaminant concentration		According to IEC 60721
Degree of protection		
	IP code	IP20
Dimensions and weight		
Dimensions	W x H x D	50 x 114 x 74 mm
Weight		130 g
Installation options		
	Installation on a DIN rail	
Mean time between failure (MTBF)		
	at 40 °C ambient temperature	106.51 years

8 Dimension drawings



Approvals 9

You will find the approvals of the products in the reference work "Approvals SCALANCE W700 802.11n" on the Internet pages of Siemens Industry Online Support:

- Using the search function:
  support.automation.siemens.com (http://support.automation.siemens.com/WW/view/en)
  Enter the entry ID of the relevant manual as the search item.
- In the navigation panel on the left-hand side in the area "Industrial Communication":
  Industrial communication (http://support.automation.siemens.com/WW/view/en/10805878/133300)
  Go to the required product group and make the following settings:
  "Entry list" tab, Entry type "Manuals / Operating Instructions"

You will find the documentation for the SIMATIC NET products relevant here on the data storage medium that ships with some products:

- Product CD / product DVD
- SIMATIC NET Manual Collection
- SIMATIC NET IWLAN CD

Index