



Visualisation; Diagnostics

Easy to Configure

Programming IEC 61131-3

Rapid Installation

PCOM sec br2


PILZ

THE SPIRIT OF SAFETY

This document is a translation of the original document.

All rights to this documentation are reserved by Pilz GmbH & Co. KG. Copies may be made for internal purposes. Suggestions and comments for improving this documentation will be gratefully received.

Pilz®, PIT®, PMI®, PNOZ®, Primo®, PSEN®, PSS®, PVIS®, SafetyBUS p®, SafetyEYE®, SafetyNET p®, the spirit of safety® are registered and protected trademarks of Pilz GmbH & Co. KG in some countries.

 SD means Secure Digital

1	Introduction	5
1.1	Validity of documentation	5
1.2	Using the documentation	5
1.3	Definition of symbols	5
1.4	Third-party manufacturer licence information	6
2	Safety	7
2.1	Intended use	7
2.2	Safety regulations	7
2.2.1	Use of qualified personnel	7
2.2.2	Warranty and liability	8
3	Security	9
3.1	General guidelines	9
3.2	Defense in depth	9
3.3	Operating environment	10
3.4	Commissioning	11
3.5	User accounts	11
3.6	Operation	11
3.7	Decommissioning	12
4	Overview	13
4.1	Unit features	13
4.2	Front view	14
5	Function description	15
5.1	Block diagram	16
5.2	VPN tunnel	16
5.3	Input and output	17
5.4	USB memory	18
6	Installation	19
6.1	General installation guidelines	19
6.2	Dimensions	19
7	Wiring	20
7.1	General wiring guidelines	20
7.2	Connection	21
7.3	Network interfaces	22
7.4	USB port X5	22
8	Configuration	23
8.1	User interface	23
8.2	Establish connection to SecurityBridge	23
8.3	Managing users	25
8.3.1	Permissions	25
8.3.2	User groups	26
8.3.3	Create user	26

8.3.4	Manage user via RADIUS server.....	26
8.4	Create device.....	28
8.4.1	Forwarding rules for PSS 4000.....	28
8.4.2	Access rules for Generic Devices.....	29
8.5	Manage certificates.....	30
8.6	Manage logging.....	32
8.7	Set operating modes.....	32
8.8	Save and secure the configuration.....	33
8.9	Check sum monitoring.....	33
9	Access to the system in the protected network	34
9.1	Install client.....	34
9.2	Create new client connection.....	34
9.3	Log in to client.....	35
9.4	Authentication procedure.....	35
10	Firmware update	38
11	Operation	39
11.1	LED indicators.....	39
11.2	Recovery.....	40
11.3	Error mode.....	41
11.4	Take SecurityBridge safely out of operation.....	42
12	Application examples	43
12.1	PNOZmulti with fieldbus module.....	43
12.2	Release of remote access with a key switch.....	44
12.3	PSS 4000 with an external control and OPC server.....	45
13	Technical details	46
14	Network data	49
15	Security-relevant log messages	50
16	Order reference	51
16.1	Product.....	51
16.2	Accessories.....	51

1 Introduction

1.1 Validity of documentation

This documentation is valid for the product PCOM sec br2. It is valid until new documentation is published.

This operating manual explains the function and operation, describes the installation and provides guidelines on how to connect the product.

1.2 Using the documentation

This document is intended for instruction. Only install and commission the product if you have read and understood this document. The document should be retained for future reference.

1.3 Definition of symbols

Information that is particularly important is identified as follows:



DANGER!

This warning must be heeded! It warns of a hazardous situation that poses an immediate threat of serious injury and death and indicates preventive measures that can be taken.



WARNING!

This warning must be heeded! It warns of a hazardous situation that could lead to serious injury and death and indicates preventive measures that can be taken.



CAUTION!

This refers to a hazard that can lead to a less serious or minor injury plus material damage, and also provides information on preventive measures that can be taken.



NOTICE

This describes a situation in which the product or devices could be damaged and also provides information on preventive measures that can be taken. It also highlights areas within the text that are of particular importance.



INFORMATION

This gives advice on applications and provides information on special features.

1.4 Third-party manufacturer licence information

This product includes Open Source software with various licenses.

You can receive further information by calling up the menu Technical Support → Licence information in the web application of the SecurityBridge.

The relevant source codes can be requested via opensource@pilz.de.

Your request should include the following: (a) the firmware name, (b) the firmware version, (c) your name, (d) your company name (if applicable), (e) your reply address and (f) your E-mail address (if possible).

Pilz can charge a fee for the data medium and for sending.

The request for the source code must be received 3 years at the latest after the receipt of the relevant GPL or LPGL. Irrespective of this period we will send you a complete, machine-readable copy of the source code as long as Pilz offers spares or technical support for this device.

Pilz permits the purchaser of this product to edit proprietary components from Pilz that are linked to Open Source components under the LGPL. Further, Pilz permits reverse engineering for debugging of the edited, proprietary components. The results of reverse engineering must not be disclosed to any third party and the edited software must not be distributed to any third party.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).


2 Safety

2.1 Intended use

The SecurityBridge PCOM sec br2 is used to protect the PSS 4000 and PNOZmulti system from network-based attacks and unauthorised access over the network.

The SecurityBridge PCOM sec br2 may only be connected to a head module from the PSS 4000 system or to a base unit of the configurable system PNOZmulti (please refer to the document "PNOZmulti System Expansion" for details of the base units that can be connected).

The following is deemed improper use in particular

- ▶ Any component, technical or electrical modification to the product,
- ▶ Use of the product outside the areas described in this operating manual,
- ▶ Use of the product outside the technical details (see [Technical details](#)  46]).



NOTICE

EMC-compliant electrical installation

The product is designed for use in an industrial environment. The product may cause interference if installed in other environments. If installed in other environments, measures should be taken to comply with the applicable standards and directives for the respective installation site with regard to interference.

2.2 Safety regulations

2.2.1 Use of qualified personnel

The products may only be assembled, installed, programmed, commissioned, operated, maintained and decommissioned by competent persons.

A competent person is a qualified and knowledgeable person who, because of their training, experience and current professional activity, has the specialist knowledge required. To be able to inspect, assess and operate devices, systems and machines, the person has to be informed of the state of the art and the applicable national, European and international laws, directives and standards.

It is the company's responsibility only to employ personnel who

- ▶ Are familiar with the basic regulations concerning health and safety / accident prevention,
- ▶ Have read and understood the information provided in the section entitled Safety
- ▶ Have a good knowledge of the generic and specialist standards applicable to the specific application.

2.2.2 **Warranty and liability**

All claims to warranty and liability will be rendered invalid if

- ▶ The product was used contrary to the purpose for which it is intended,
- ▶ Damage can be attributed to not having followed the guidelines in the manual,
- ▶ Operating personnel are not suitably qualified,
- ▶ Any type of modification has been made (e.g. exchanging components on the PCB boards, soldering work etc.).

3 Security

3.1 General guidelines

- ▶ Please refer to the chapter [Operating environment](#) [📖 10]. The product is not designed for connecting a network to the internet.
- ▶ Perform a risk analysis and plan the security measures carefully. If necessary, seek advice from Pilz Customer Support.
- ▶ Please note that the product forwards ICMP Echo Request and Response packages (ping) and ARP requests and responses between the unprotected and the protected network, independent of the configuration. However, the device limits the number of packages to make flooding attacks more difficult.
- ▶ Please report any security problems of the SecurityBridge to the following E-mail address: security@pilz.de

3.2 Defense in depth

Defense in depth is a security design concept. Several different security measures to protect from attacks are arranged in series and/or in layers. An attack is made difficult because the attacker has to circumvent different security measures one after the other. This concept can be illustrated as follows:

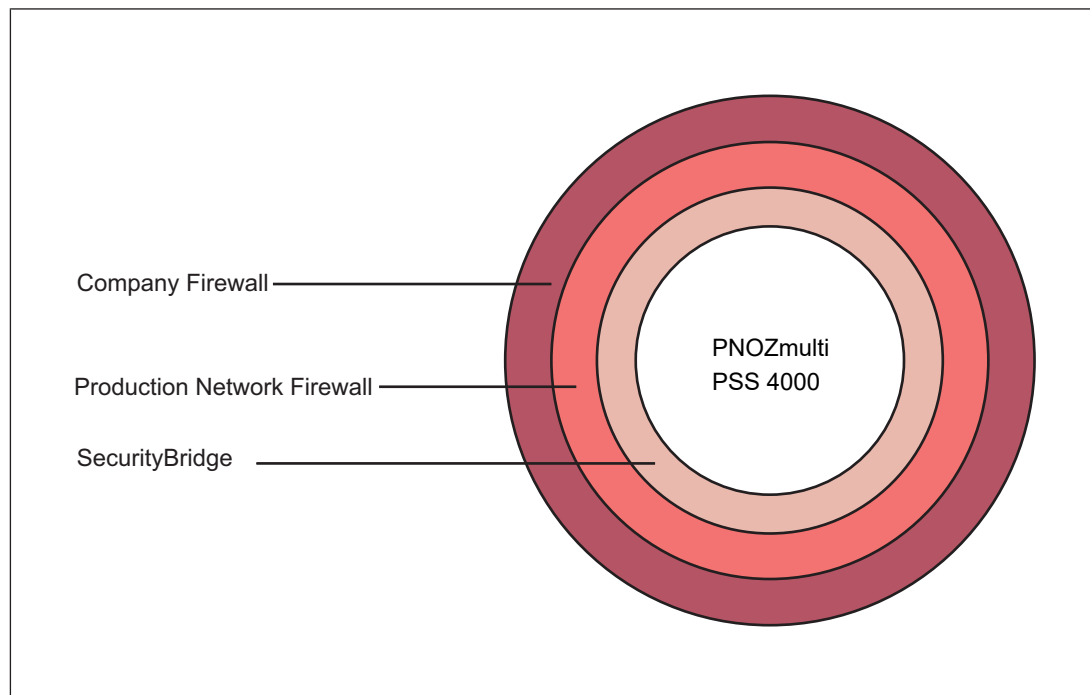


Fig.: DefenseInDepth

The product PCOM sec br2 secures the devices in the protected network from network-based attacks and/or unauthorised access via the network. The product is the last layer in the Defense in depth concept. To efficiently implement the concept, the measures described in the chapter [Operating environment](#) [📖 10] must be noted.

3.3 Operating environment

The product has no measures to protect against physical manipulation and/or against reading of memory content during physical access. Further, the product cannot secure the devices in the protected network when the attacker has physical access to the entire network. Therefore, the product in conjunction with the devices to be protected has to be installed in a lockable control cabinet. We recommend equipping the control cabinet with a suitable lock and organising the access to the control cabinet.

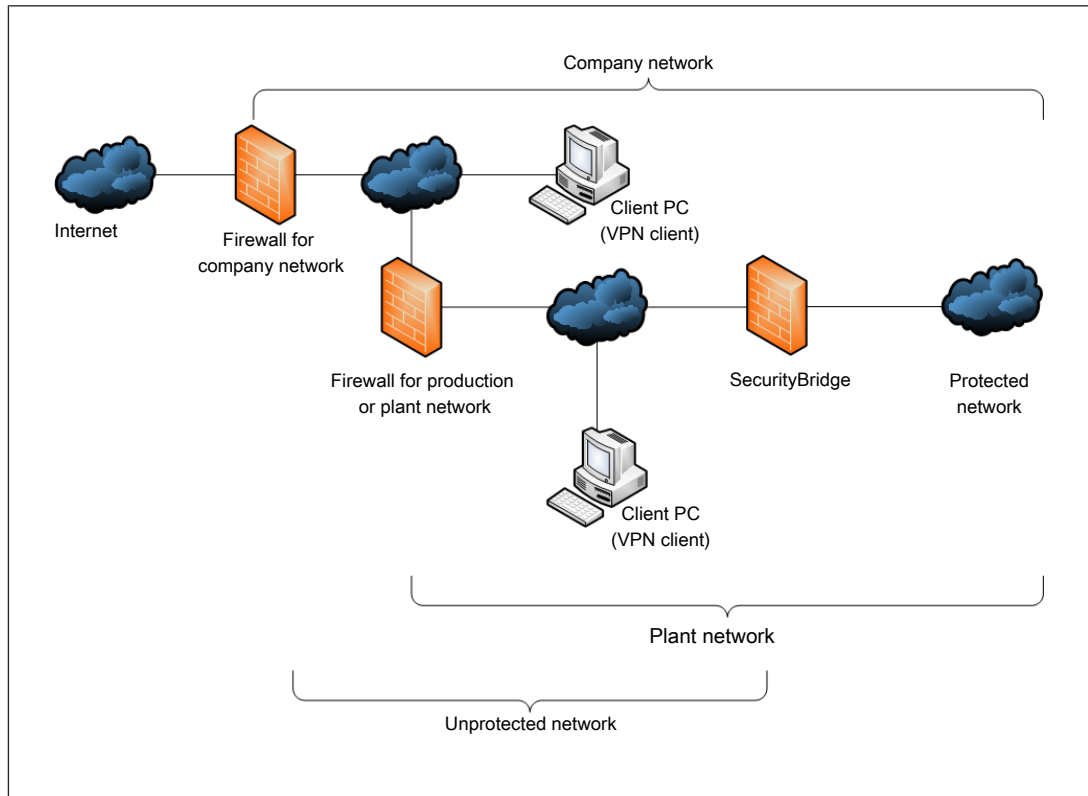


Fig.: Network overview

To implement the defense in depth concept provided, the product has to be arranged in the network as shown in the figure "Network overview". The chapter [Network data \[49\]](#) describes the network protocols that the product uses to communicate with other systems. Note these protocols when configuring your network environment.

The SecurityBridge cannot protect from network overload or flooding attacks in an unprotected network. When the unprotected network is overloaded, the protected system may not be accessible. Therefore, measures should be taken to protect the network infrastructure from flooding attacks or other overload situations.

The computer on which the VPN client and the configuration tool are run will have to be protected by a firewall or other appropriate measures against attacks from the internet. Further we recommend that you use a virus scanner on these computers. Protect the computer from unauthorised use by assigning passwords, and taking further measures, if required. We also recommend that the logged in user does not have administrator rights.

3.4 Commissioning

- ▶ Before commissioning, create the environment described in the chapter [Operating environment](#) [📖 10].
- ▶ For the VPN and HTTPS protocols, the device requires an encrypted key that is created during commissioning. To exclude an attack during commissioning, please follow the instructions in the chapter [Establish connection to SecurityBridge](#) [📖 23].
- ▶ Change the default password for the user account "admin".

3.5 User accounts

- ▶ Assign only safe passwords. Criteria for a safe password:
 - The password should have at least 8 characters.
 - The password should contain upper and lower case characters, as well as special characters and numbers.
 - If possible, the password should not be available in dictionaries.
 - The password should not be made up of standard variants and repetitions or keyboard patterns (so not: 1234abcd).
 - Use a password manager for optimum management of complex passwords.
 - When assigning the password, please note that language-dependent characters may not be available in all the keyboard languages.
- ▶ Make sure you regularly change the passwords of the user accounts on the system and/or ask the users to change their passwords themselves.
- ▶ Retain the passwords safely and train the personnel to deal with Phishing and Social Engineering attacks.
- ▶ Strictly separate the user accounts for the product administration and the access to the systems in the protected network.
- ▶ Make the users aware of the responsible use of their access data.


3.6 Operation

Please note the following measures when operation the device:

- ▶ The computers used to monitor the system must be secured to the general best practice rules for security.
- ▶ As soon as possible, install firmware updates that Pilz provides for the device.
- ▶ Make sure you regularly check the event log of the product for security-relevant entries. A list of security-relevant entries can be found in chapter [Security-relevant log messages](#) [📖 50].
- ▶ Wherever possible, forward the entries of the event log to a log server (see chapter [Manage logging](#) [📖 32]). This ensures that the entries will be available for a longer period of time, and that it is made more difficult for an attacker to delete entries.
- ▶ Regular safety updates for the operating system and the installed applications must be run on the computer that uses the VPN client.

- ▶ Ensure that the setup mode is used only by authorised users. Use a key switch at the input I0 to enable the setup mode, for example.
- ▶ Unless otherwise documented, you should ensure that all the files created by the SecurityBridge can only be used by authorised users.

3.7 Decommissioning

- ▶ Make sure that the SecurityBridge is safely decommissioned before disposing of the device (see chapter [Take SecurityBridge safely out of operation](#) [ 42]).
- ▶ Where possible, perform these steps also when servicing and sending the device to Pilz.

4 Overview

4.1 Unit features

Application of the product PCOM sec br2:

SecurityBridge for safe authentication and communication with a PSS 4000 or a PNOZmulti system.

The product has the following features:

- ▶ Configurable via a web-based user interface
- ▶ VPN server to build a VPN tunnel for safe transfer of data
- ▶ Forwarding rules for IP connections and fieldbuses
- ▶ Bypass mode (temporary deactivation of security functions for diagnostic purposes)
- ▶ Setup mode for maintenance work
- ▶ Output, e.g. to display the status of the connections or the operating mode
- ▶ Input to trigger certain functions or event messages (e.g. activating the setup mode)
- ▶ USB interface to secure and restore the configuration on a USB memory.
- ▶ LED display for:
 - Error messages
 - Diagnostics

4.2 Front view

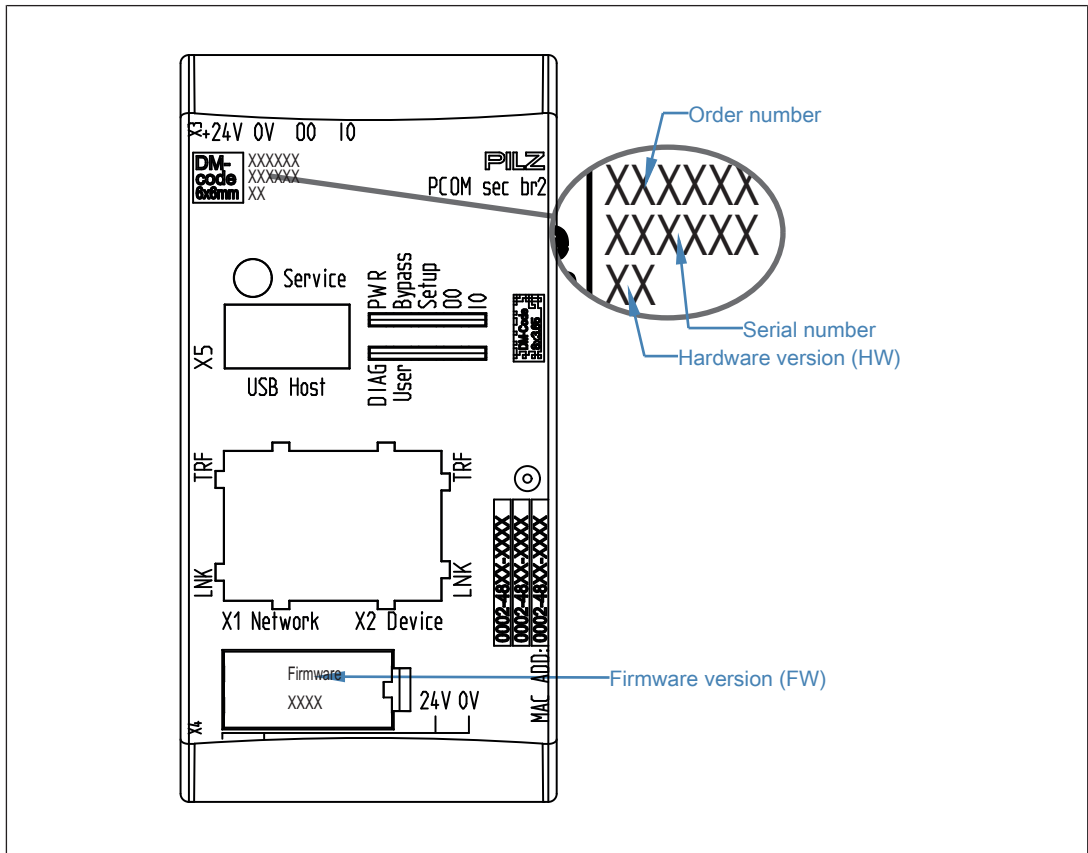


Fig.: PCOM sec br2

Legend

- X1 Network Ethernet port for connecting the configuration PC
- X2 Device Ethernet port for connecting to the protected system
- X3
 - ▶ 24 V, 0 V: Periphery supply
 - ▶ I0: Input
 - ▶ O0: Output
- X4 24 V (A1), 0 V (A2) Module Supply
- X5 USB interface for USB memory to save and restore the configuration
- LEDs PWR, DIAG, Bypass, User, Setup, I0, O0

5 Function description

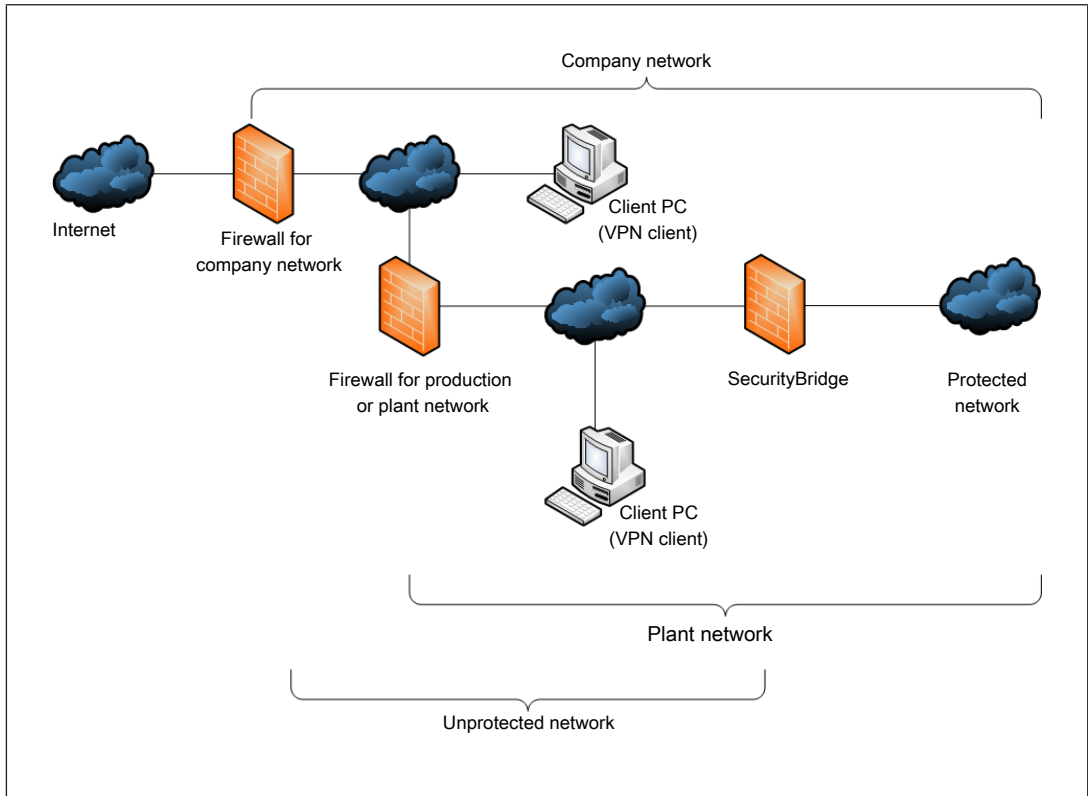
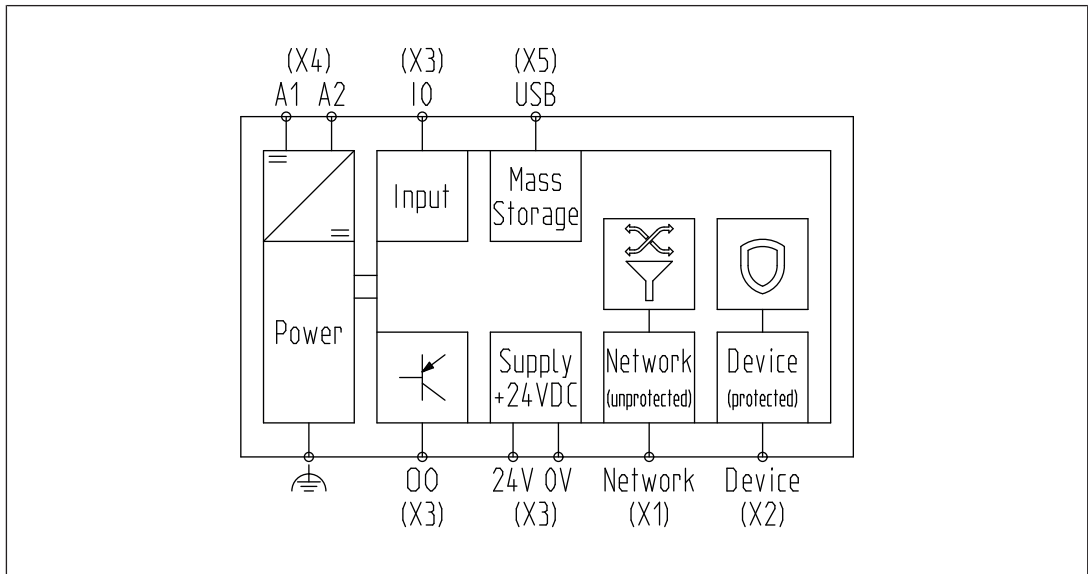


Fig.: Overview

The SecurityBridge is used with in the company network to prevent unauthorised access to downstream devices in a protected network. The access from the client PC to the devices in the protected network can only be achieved using a VPN tunnel. A VPN client is used to build up a VPN tunnel. In normal circumstances, the VPN client is within the company network.

Configuration changes to a project can only be performed by users who have a relevant permission.

5.1 Block diagram



5.2 VPN tunnel

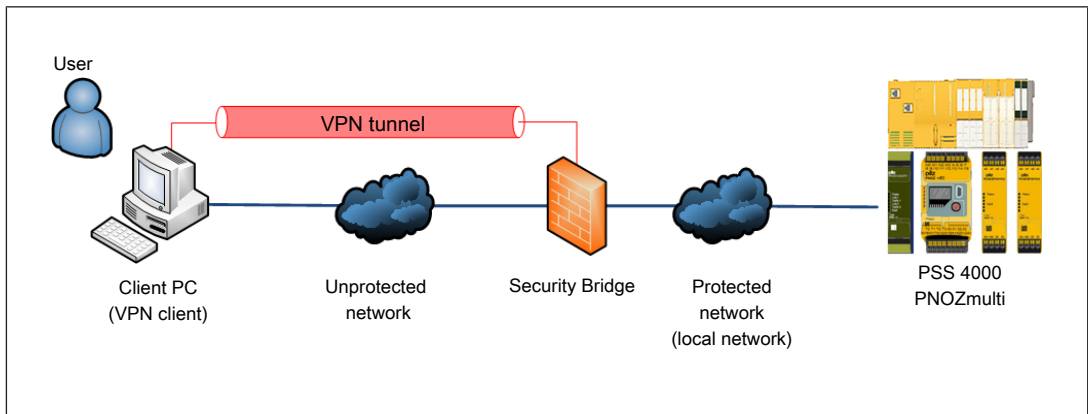


Fig.: VPN tunnel

The SecurityBridge acts as VPN server, through which a Virtual Private Network (VPN) can be established to one or more client PCs (configuration PC). This enables tap-proof, manipulation-proof data transfer between the client PC and SecurityBridge.

- ▶ Only the VPN client from Pilz is supported.
- ▶ Up to 5 client connections can exist simultaneously.
- ▶ A VPN tunnel can only be built by authenticated, authorised users.
- ▶ Data is transferred through the VPN tunnel in an encrypted form.
- ▶ Existing VPN connections can be displayed via a digital output on the module.
- ▶ As a minimum the user must have permission from the group "PNOZmulti permissions", "Network permission" or "PSS 4000 permissions" or "Generic Device permissions".

- ▶ After 5 failed login attempts from the same client IP address, further login attempts with the same IP address will be blocked for 10 minutes.
- ▶ The VPN connection can be controlled via a digital input.
- ▶ The VPN connection can be signalled via an LED.

5.3 Input and output

The SecurityBridge provides a digital input and a digital output. These can be used for various functions, as required.

The following functions can be configured on the user interface:

▶ Functions digital input:

– SSLVPN

Access to the SecurityBridge via a VPN connection is controlled via the digital input. New VPN connections can only be created when there is a 1-signal at the input or, in the case of an inverted input, a 0-signal. The connection is broken as soon as the configured signal is no longer present at the input.

– SETUP MODE

Setup mode can be activated via the digital input. Setup mode is active when there is a 1-signal at the input or, in the case of an inverted input, a 0-signal.

▶ Functions digital output

– SSLVPN

A VPN connection is signalled via the digital output. If there is a 1-signal at the output, then there is at least one VPN Client connected. If there is a 0-signal at the output, then no VPN Client is connected.

– BYPASS

Bypass mode is signalled via the digital output. If there is a 1-signal at the output, then bypass mode is activated. If there is a 0-signal at the output, then bypass mode is not activated.

– CRC

A change to the check sum is signalled via the digital output. If there is a 1-signal at the output, then at least one project check sum no longer matches the configured check sum. If there is a 0-signal at the output, then no check sum has changed. Please note that in the menu Security functions the option **Check sum monitoring** must be configured.

– DEVMON


Device monitoring is signalled via the digital output. If there is a 1-signal at the output, then at least one device that has been configured for monitoring is no longer accessible. If there is a 0-signal at the output, then all devices are accessible.

Please note that in the menu Security functions the option **Device monitoring** must be configured.

– SETUP MODE

Setup mode is signalled via the digital output. If there is a 1-signal at the output, then setup mode is activated. If there is a 0-signal at the output, then setup mode is not activated.

5.4 USB memory

The SecurityBridge has a USB connection, to which you can connect a USB memory to back up your configuration (see also [Save and secure the configuration](#) [ 33]).

Requirements of the USB memory

- ▶ Use only one USB memory from a secure source. A manipulated USB memory could damage the system.
- ▶ The USB memory must comply with the transfer protocol Mass Storage Device Class (USB MSC or UMS).
- ▶ The USB memory must contain a Master Boot Record (MBR).
- ▶ The first partition of the USB memory must be formatted as a VFAT file system.
- ▶ In the event of an ambient temperature of over 45 °C, note that the temperature of the connected USB memory could rise to over 70 °C.

Using the USB memory

An inserted USB stick can be formatted and incorporated via the user interface of the SecurityBridge.

When a USB stick is inserted and it has been formatted by the SecurityBridge, it is automatically incorporated.

You can save your configuration to the USB stick and restore it from there.

When the USB stick is incorporated, the configuration is saved automatically to the USB stick when the active configuration is transferred into the start configuration.



CAUTION!

When using the USB backup, make sure that the SecurityBridge and USB memory are protected against unauthorised access (by placing the SecurityBridge in a locked control cabinet, for example).

6 Installation

6.1 General installation guidelines

- ▶ The unit should be installed in a control cabinet with a protection type of at least IP54. Fit the unit to a horizontal mounting rail. The venting slots must face upward and downward. Other mounting positions could destroy the device.
- ▶ Use the locking elements on the rear of the unit to attach it to a mounting rail. Connect the device to the mounting rail in an upright position, so that the earthing springs on the device are pressed on to the mounting rail.
- ▶ The ambient temperature of the devices in the control cabinet must not exceed the figure stated in the technical details. Air conditioning may otherwise be required.
- ▶ To comply with EMC requirements, the mounting rail must have a low impedance connection to the control cabinet housing.

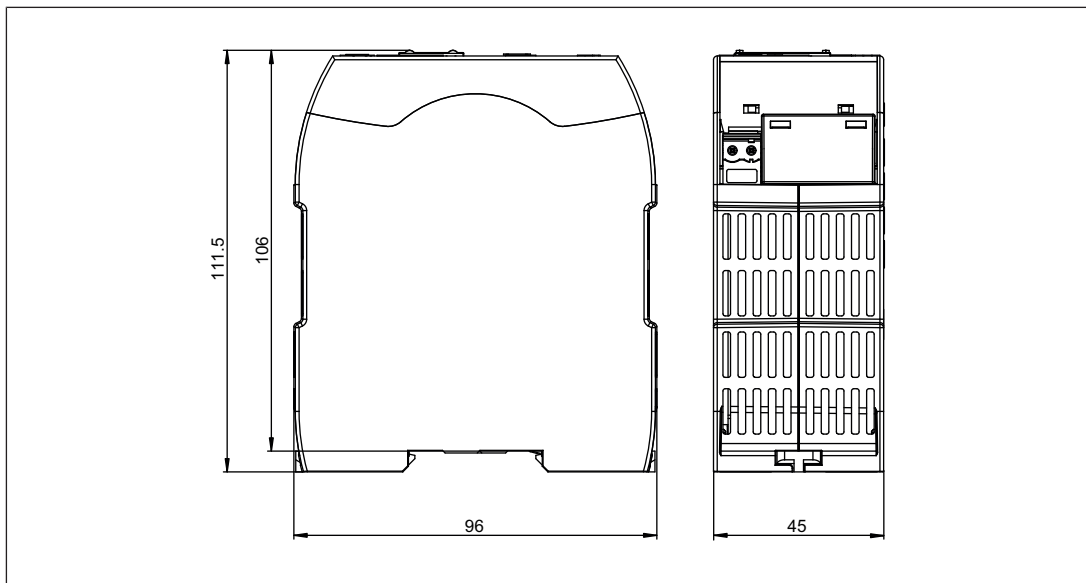


NOTICE

Damage due to electrostatic discharge!

Electrostatic discharge can damage components. Ensure against discharge before touching the product, e.g. by touching an earthed, conductive surface or by wearing an earthed armband.

6.2 Dimensions



7 Wiring

7.1 General wiring guidelines

Note:

- ▶ Information given in the [Technical details \[46\]](#) must be followed.
- ▶ Use copper wire that can withstand 75° C.
- ▶ The cable length of the cables connected to the inputs and output must be a max. of 30 m.
- ▶ The supply of the module and the supply of the semiconductor outputs are galvanically isolated.

▶ Module supply:

- Polarity protection
- Overvoltage protection

Protect the supply voltage as follows:

- Circuit breaker, characteristic C - 6 A

or

- Blow-out fuse, slow, 6 A

▶ Supply to the semiconductor outputs:

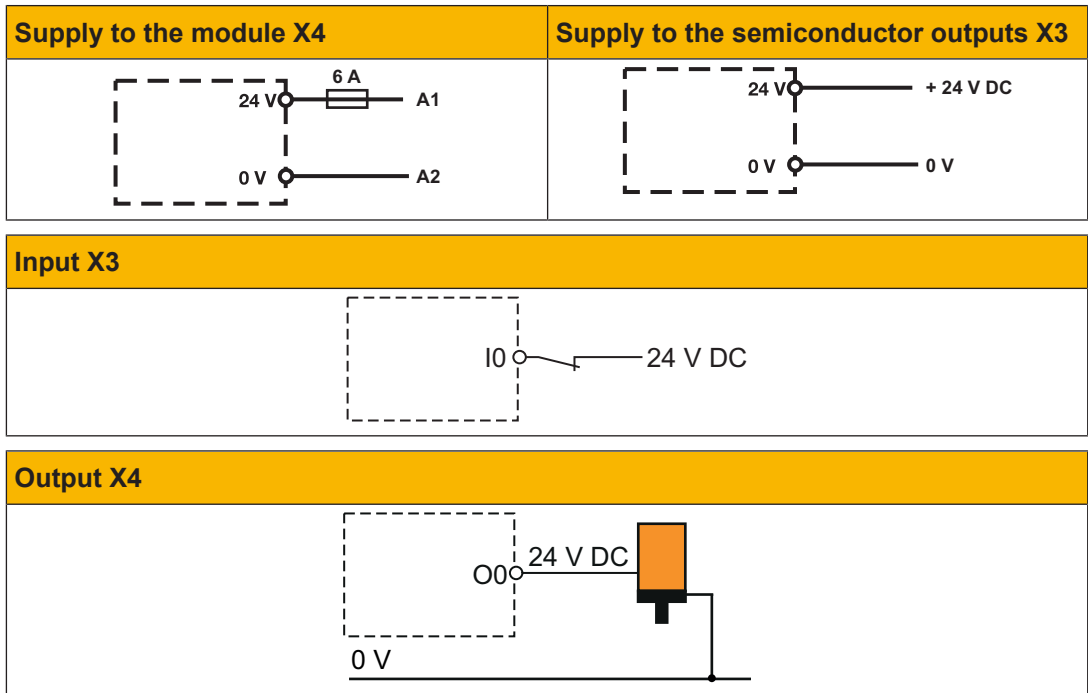
- Polarity protection
- No voltage stabilisation

Guidelines for UL approval

UL Markings

- ▶ The external circuits intended to be connected to this device shall be galv. separated from mains supply or hazardous live voltage by reinforced or double insulation and meet the requirements of PELV (Class III) circuit of UL/CSA/IEC 61010-1, 2-201.
- ▶ The modules have to be build-in the final safety enclosure, which has adequate rigidity according to UL 61010-1, 61010-2-201 and meets the requirements with respect to spread of fire.

7.2 Connection



7.3 Network interfaces

The device has 2 RJ45 sockets for connecting to Ethernet.

The Ethernet interfaces X1 and X2 must be used as follows:

- ▶ Ethernet interface X1 (network port)
 - Connection to the unprotected network (company network)
- ▶ Ethernet interface X2 (device port)
 - Connection to the protected network
- ▶ Supported Internet protocol: IPv4

Supported functions:

- ▶ Autonegotiation
 - When Autonegotiation is used, Autonegotiation must also be activated at the remote station.
- ▶ With deactivated autonegotiation:
 - Communication speed: 10 Mbits/s or 100 Mbits/s
 - Duplex: Half duplex or full duplex

7.4 USB port X5

The add-on module has a USB connection. You can use this to connect a USB memory to save and restore the configuration data.

Use of a USB extension cable is not permitted and is deemed improper use.



CAUTION!

Risk of burns!


With ambient temperatures $>45\text{ °C}$, a surface temperature of above 70 °C can arise when a USB memory is connected!

Take protective measures to prevent intended and unintended contact with an inserted USB memory (e.g. only leave the USB memory inserted briefly, never leave the USB memory inserted during productive mode).

8 Configuration

8.1 User interface

Configuration, diagnostics, monitoring and maintenance of the SecurityBridge are made with the help of a web-based user interface. The user interface contains all the important information about the SecurityBridge and the protected system.

Only users can access the user interface who have the relevant authorisations (see [Privileges](#)  25).

To handle and configure the SecurityBridge, please read the online help of the user interface.

Please note the following when calling up the online help:

The online help is displayed in a separate window. To display the online help, make sure to activate the setting in your browser that opens a new window when opening new web sites.

System requirements:

The user interface is called up via a standard browser.

The following web browsers will always be supported:

- ▶ Internet Explorer (IE), from Version 9
- ▶ Microsoft Edge
- ▶ Mozilla Firefox from Version 23.7.0
- ▶ Google Chrome from Version 27
- ▶ Safari from Version 5.1

8.2 Establish connection to SecurityBridge

The following section describes the typical procedure to create a connection to the SecurityBridge and to open the user interface.

1. Establish Ethernet connection

- ⇒ Connect the configuration PC directly to the Ethernet interface X1 of the SecurityBridge PCOM sec br2. Alternatively you can use a switch to which only the configuration PC and the SecurityBridge are connected.

This way, you avoid that an attack can occur during commissioning.

2. Adjust IP address of the configuration PC

To access the SecurityBridge the IP address of the PC has to be in the same subnet as the IP address of the SecurityBridge.

Module's default settings:

IP address: 192.168.222.1

Network mask: 255.255.0.0

- ⇒ Change the IP address in the network settings of your configuration PC.

3. Call up the user interface

⇒ Start the Internet browser and enter an IP address of the SecurityBridge.

If a certificate error is displayed in the internet browser, temporarily add an exception rule and/or circumvent this warning message to still access the user interface.

Default IP address: <https://192.168.222.1>

4. Register at the user interface

⇒ Enter the user name and the password

Default credentials:

User name: admin

Password: <Serial number of the SecurityBridge> (the serial number is on the front of the device (see [Front view \[14\]](#))).

A maximum of 5 failed attempts can be made. Further logon attempts will be blocked for 10 minutes.

5. Change initial password

A window for changing the password appears. Change the initial password. Enter a safe password with at least 8 characters (for features of a safe password see

[Security \[9\]](#)).

6. Change network settings

To access the SecurityBridge PCOM sec br2 from the company network, change the network settings of the SecurityBridge. The settings are adapted in the Web interface under **System** → **Settings** → **Network** (see also Online Help).

7. Start user interface with the new IP address

⇒ Start the Internet browser and enter a new IP address of the SecurityBridge.

8. Generate new certificate

⇒ On the user interface, select **System** > **Certificates** -> **Generate certificates**. Enter the new IP address as **General certificate name** of the new certificate.

9. Copy active configuration into the start configuration

⇒ On the user interface, select **Maintenance** > **Apply active configuration in start configuration**, to save the configuration permanently in SecurityBridge.

10. Download CA certificate

⇒ On the user interface, select **System** > **Certificates** -> **Certificate download**. Download the certificate in DER format (see [Manage certificates \[30\]](#)).

11. Install CA certificate

⇒ Install the CA certificate as a trustworthy root certificate (see [Install CA certificate \[30\]](#)).

8.3 Managing users

In order to access the device in the protected network via the SecurityBridge, a user must log in from a client PC via VPN client, using his login data. A user account must be created for each user in user management on the user interface.

Different access permissions can be defined for users. For this purpose user groups are created, which are assigned specific, pre-defined [permissions](#) [25].

The registration process is described in the chapter entitled [Log in to client](#) [35].

See the user interface's online help for details of how to configure the user management.

8.3.1 Permissions

The permissions are used to define which actions a user group is permitted to perform.

The following permissions can be assigned to a user group:

Permission	Description	ID for RADIUS
System permissions		
Administration	User can perform administrative functions on the SecurityBridge. However, he has no access to the protected system (PNOZmulti, PSS 4000)	1
User management	User may create, change or delete entries in the user management.	2
PSS 4000 permissions		
DeviceAdmin	User may perform all online functions on the PSS 4000 system.	50
PNOZmulti permissions		
DeviceAdmin	User may perform all online functions on the PNOZmulti system.	100
ReadOnly	On the PNOZmulti system, the user may only perform online functions that do not influence the status of the system	101
Operator	User may perform all online functions on the PNOZmulti system, except changes to the project.	102
Network permissions		
Modbus TCP	User may access the Modbus/TCP server in the protected PNOZmulti system.	150
Generic Device permissions		
AccessGroup-1	User is allowed to access the Generic Device belonging to one of these three groups if he is assigned to a user group with the same permission.	160
AccessGroup-2		161
AccessGroup-3		162

8.3.2 User groups

User groups are created on the user interface so that each user is assigned the permissions appropriate for their role.

You can create a maximum of 15 user groups with different permissions. Each user is assigned to a user group.

The following user group is pre-configured on delivery:

Name: Administrators

Permissions: Administration

Delegating allowed: No

Allow delegating

Management of user data can normally only be undertaken by system users with **Administration** permission.

For certain user groups, management of the user data can be delegated to system users with **UserManagement** permission.

With user groups whose user data management is to be delegated, the **Allow delegating** option must be activated.

The following actions can then be delegated:

- ▶ List users
- ▶ Create new user
- ▶ Change user data

8.3.3 Create user

A user account must be created for each user who wants to access the protected system via VPN client or the SecurityBridge user interface.

To do this, create a new user in the user interface:

- ▶ Specify user name and password
- ▶ Assign rights by selecting the user group and setup mode

8.3.4 Manage user via RADIUS server

User management can also be run via a central RADIUS server, as an alternative to local user management on the user interface of the SecurityBridge.

On the user interface, a primary and secondary RADIUS server can be configured. On the user interface you define which user groups or permissions are to be used for the RADIUS server.

- ▶ A secure Server Shared Secret must be entered to configure the RADIUS server. The same Server Shared Secret must be configured on the RADIUS server.
- ▶ Use a separate Server Shared Secret for each SecurityBridge that is configured via the RADIUS server.

- ▶ The RADIUS server can assign one or more permissions to a user. The permissions are transferred in the **Vendor Specific Attribute (VSA)** as numeric values in a comma-separated list (CSV) (for values see [Privileges \[25\]](#)). Only permissions that are enabled in the SecurityBridge for the RADIUS server are accepted.
- ▶ The RADIUS server can assign a user group to a user. The group name is transferred in the **Vendor Specific Attribute (VSA)**. Only user groups that are enabled in the Security-Bridge for the RADIUS server are accepted.



INFORMATION

Via the RADIUS server a user can either be assigned to a user group or be assigned one or more permissions. If you attempt to assign a user group and one or more permissions to a user, only the user group will be accepted.

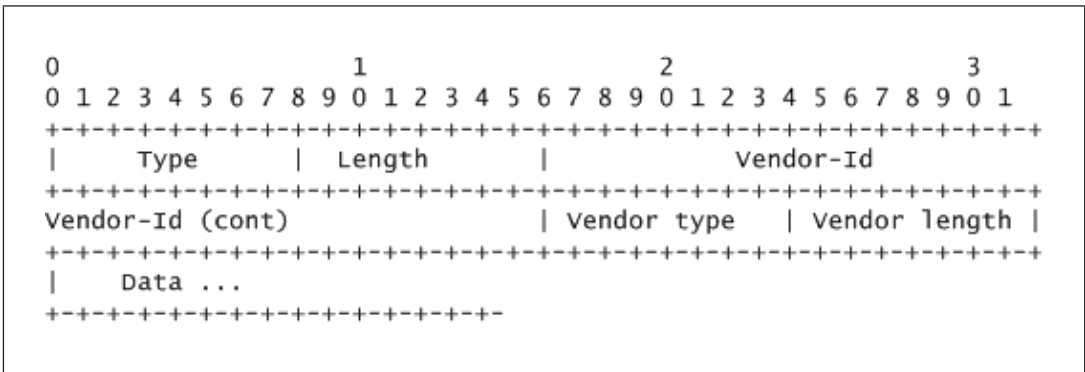


Fig.: Vendor Specific Attributes (VSA)

Legend

Type (1 Byte)	Vendor Specific Attribute Value: 26
Length (1 Byte)	Overall length of attribute
Vendor-ID (4 Bytes)	Format, see RFC 2865, SMI Network Management Private Enterprise Code Pilz-specific value: 43236
Vendor type (1 Byte)	0 = Group name contained in the transmitted data 1 = Permissions contained in the transmitted data as comma-separated values
Vendor length (1 Byte)	2 + data length

8.4 Create device

Create PNOZmulti and PSS 4000 devices

The devices that are to be protected must be created and configured on the user interface. Devices can be created manually or it is also possible to scan the network for connected devices.

Special feature for PNOZmulti:

- ▶ The **Network scan** function in the PNOZmulti Configurator can only be executed by users who have **PNOZmulti** permissions.

Special feature for PSS 4000 devices:

- ▶ The **Network scan** function in PAS4000 can only be executed by users who have **PSS4000** permissions.
- ▶ A maximum of 64 PNOZmulti and PSS 4000 devices can be created.

Create OPC server

The OPC server must be in the unprotected network. The communication between the device in the protected area and the OPC server is monitored by the SecurityBridge. Depending on the configured access permission, only read or read/write operations are permitted.

- ▶ A maximum of 5 OPC servers can be created. 4 OPC servers for the product range PSS 4000 and 1 OPC server for the product range PVIS.

Create Generic Devices

Generic Devices are all devices with a network interface that do not belong to the PSS 4000, PNOZmulti or OPC Server product family. These devices are located in the protected area. The devices can only be created manually. Scanning the network for generic devices is not possible.

- ▶ A maximum of 15 Generic Devices can be created.
- ▶ The IP address and/or the MAC address must be configured for each Generic Device.

8.4.1 Forwarding rules for PSS 4000

These rules monitor data traffic between a device in an unprotected network and the PSS 4000 in a protected network.

Please note the following when creating rules:

- ▶ You can define a maximum of 64 rules
- ▶ If you know the IP address and the port numbers, always enter a unique IP address and port number.

If you set unknown IP addresses or port numbers, multiple devices from an unprotected network will be able to access the PSS 4000 device in the protected network.

- ▶ Create precisely one rule for one connection, which has been configured for a PSS 4000 device.

- ▶ A rule is deemed to be unambiguous if the following properties have been configured:
 - IP address of the device in the unprotected network
 - Port number of the device in the unprotected network
 - IP address of the PSS 4000 device in the protected network
 - Port number of the PSS 4000 device in the protected network
- ▶ Ambiguous rules are permitted if the IP address and port number of a device in the unprotected network are unknown.
Potential problems with ambiguous rules:
 - One rule defines many connections
 - One rule opens undesired access to the PSS 4000 device in the protected network

For further information see Online help.

8.4.2 Access rules for Generic Devices

The rules allow administrative communication with the Generic Device via VPN tunnel and/or data communication between a device in the unprotected network and the Generic Device in the protected network. A maximum of 25 rules (administrative rules and forwarding rules) can be defined per device.

Administrative access rules

The system allows the definition of administrative access rules for Generic Devices. These rules are used to allow administrative access to a Generic Device via the VPN tunnel. An administrative access rule is always linked to a Generic Device. The source or destination IP address of the data traffic (depending on the direction) is always determined by the IP address of the Generic Device.

Forwarding rules

The rules monitor traffic between a device on an unprotected network and a Generic Device on a protected network. The following protocols are supported for the forwarding rules:

- ▶ UDP
- ▶ TCP
- ▶ Ethernet

For further information see Online help.

8.5 Manage certificates

The SecurityBridge uses X.509 certificates to secure communication between the VPN client and the SecurityBridge, plus the user interface.

By default the system uses a self signed CA certificate to sign the server certificate. The certificates are automatically generated by the SecurityBridge.

To enable communication, the certificate is downloaded to the PC by the user interface and is imported into the VPN client and web browser. If you use a self-signed CA certificate when you try to establish a connection to the SecurityBridge, a warning appears saying that the connection is not secure. In order to establish a connection, you must add a security exception rule to your web browser.



CAUTION!

Risk of data manipulation

Possible loss of data security.

You may add a security exception rule to your web browser only if you are sure that you are communicating with the SecurityBridge.

New certificates are generated when the SecurityBridge is reset to its factory settings. You can also upload your own CA certificate and server certificate with private key.

Certificates and private keys are part of the system configuration and are stored in the active configuration and start configuration (see [Save and secure the configuration](#) [📖 33]).

Certificate download

You can download the CA certificate and server certificate from the user interface to your PC. You can import the CA certificate into the browser PC (see [Install CA certificate](#)) or VPN Client.

Possible formats:

- ▶ PEM
- ▶ DER

Install CA certificate

To build up a secure connection between the user interface and the SecurityBridge, the CA certificate from the SecurityBridge must be saved in the web browser as a trustworthy root certificate. Otherwise, a certificate error will be displayed in the web browser.

Install a CA certificate using Microsoft 7 with Internet Explorer as an example.

1. Download the CA certificate from the user interface and save it to your PC.
2. Double-click the certificate.

The **Certificate** window is opened.

3. On the **General** tab, click **Install Certificate...**

The **Certificate Import Wizard** window is opened.

4. Click **Next**. Select the option **Place all certificates in the following store** and click **Browse**.
The **Select Certificate Store** window is opened.
5. Select **Trusted Root Certification Authorities** and click **OK...**
6. Click **Next**.
7. Click **Complete**. A safety warning may appear. Confirm that you wish to install the certificate.

Import certificate into the VPN client

To build up a secure connection between the VPN client and the SecurityBridge, the CA certificate from the SecurityBridge must be saved in the VPN client.

Procedure

1. To download the certificate directly from the SecurityBridge, enter a passphrase for the CA certificated in the SecurityBridge under "VPN->Settings"
2. Under "System->Certificates->Certificate download", download a CA certificate with format PEM on the PC.
3. Start the VPN client and click **Add...**

The **Add OpenVPN connection** window opens.

4. Under **Connection name**, enter a name for the connection and in the **SecurityBridge IP address** field enter the IP address of the SecurityBridge.
5. Select the certificate.

The following options are available:

- ▶ Select certificate from a local directory

You saved the certificate to your configuration PC. Click **Browse file...** and select the certificate (*.pem).

- ▶ Certificate download

The VPN client can automatically download the certificate. The download is secured by a passphrase. Further information on the password policy can be found in the Online Help on the SecurityBridge.

Generate certificates

You can generate new certificates with SecurityBridge. You can generate a server certificate if you want to renew the server certificate without having to redistribute the CA certificates to all the Clients. However, you cannot generate the server certificate if you have previously uploaded your own CA certificate to the SecurityBridge.

Certificate upload

If you want to use your own certificates, you can store the CA certificate and server certificate with its private key on the SecurityBridge. As they are uploaded the certificates are checked to ensure they the syntax is correct.

The CA certificate should be stored on the SecurityBridge in order to ensure that the SecurityBridge contains the appropriate CA certificate for the server certificate. The VPN client cannot download the correct CA certificate until the appropriate CA certificate has been uploaded.

Possible formats:

- ▶ PEM
- ▶ Effects:

When a CA certificate is uploaded, any existing private key will be deleted.

8.6 Manage logging

All the events are logged and displayed on the user interface. The event log is a ring memory, i.e. when the maximum number of entries has been reached, the most recent event overwrites the oldest event. The maximum number of events in the ring memory is 4096 entries.

The event log is saved in the Flash memory every 15 minutes. If the supply voltage is interrupted, any messages that have not been saved may be lost.

After the restart, the number of lost messages will be displayed in an event log entry.

External logging

The following options exist for forwarding the events to an external system:

- ▶ You can send the events in a configurable interval via SMTP as an E-Mail.
- ▶ You can send the events to an external Syslog server.

To configure the external logging, please read the online help of the user interface.

8.7 Set operating modes

Bypass mode

Bypass mode can be used for diagnostic purposes. In bypass mode, all the network data transferred between the unprotected and protected network is unfiltered.

The status is displayed on the user interface and on the device via a configurable LED.



CAUTION!

Loss of security when bypass mode is activated

The security functions are deactivated in bypass mode. Make sure that bypass mode is only active temporarily and that a network attack cannot occur while the system is in an unsafe state.

Setup mode

Setup mode can be used for maintenance and commissioning purposes. It is activated for certain users, who are to have temporary, limited access permissions for maintenance work only. This option is defined when a user is created. These users can only log in to the SecurityBridge when SecurityBridge is in setup mode.

Setup mode for the SecurityBridge is activated via the user interface or via the digital input. If setup mode is activated via the digital input, then it can no longer be modified via the user interface. The status is displayed via the user interface and an LED.

8.8 Save and secure the configuration

All the settings that you make on the user interface are initially saved only temporarily in the active configuration and are lost if the SecurityBridge is restarted.

If the active configuration is to be saved on the SecurityBridge and is to be available again on restart, it must be applied as the start configuration.

The start configuration can also be saved on the USB memory or on the computer as a ZIP file and it can be restored (see online help of the user interface).



CAUTION!

Save the backup file in a secure location, to which no unauthorised persons have access, to protect the file from espionage, sabotage and data loss.

Measures when no configuration has been found during startup of the SecurityBridge, or when the configuration is damaged:

- ▶ When a configuration is saved to the USB memory, the configuration is loaded automatically.
- ▶ When you saved a configuration on the computer, the configuration can be restored by uploading the backup file to the user interface.
- ▶ If you did not generate a backup file or if the backup file cannot be restored, you can reset the device to the factory settings (see [Recovery \[40\]](#)).

8.9 Check sum monitoring

The SecurityBridge can compare the configured project check sum for a protected device to the project check sum of the connected device. The check sum will be checked every 5 minutes. A message is generated when the check sum is changed in the connected device.

- ▶ The overall check sum for the project is used for PNOZmulti devices.
- ▶ The check sum for the FS project is used for PSS 4000 devices.

9 Access to the system in the protected network

To access the protected system via the SecurityBridge, a user has to register via the CPN client supplied. To do this, the user must have been created on the SecurityBridge user interface, and the protected system must have been created on the SecurityBridge interface as a device (see chapter [Configuration \[📖 23\]](#)).

9.1 Install client

To install the VPN client, run the **SecurityBridgeVpnClient-setup.exe** file. The installation file is available in the download area of the Pilz website (www.pilz.de -> Downloads).

System requirements:

The VPN client can be installed on a PC with one of the following operating systems:

- ▶ Windows 7 (32 or 64 Bit version)
- ▶ Windows 8.1 (32 or 64 Bit version)
- ▶ Windows 10 (32 or 64 Bit version)

9.2 Create new client connection

To create a connection to SecurityBridge for the first time, a new client connection has to be created. Proceed as follows:

1. Start the VPN client by clicking **All programs > Pilz > SecurityBridge VPN Client**.
2. Double-click on the symbol of the VPN client in the task bar to open the VPN client. Click **Add connection**. The **Add VPN connection** window opens.
3. Under **Connection name**, enter a name for the connection and in the **SecurityBridge IP address** field enter the IP address of the SecurityBridge.

The text may only contain alphanumerical characters.

4. Import the CA certificate of the SecurityBridge.

The following options are available:

- Select certificate from a local directory (browse file)
Select this option when you stored the certificate on your configuration PC.
- Download certificate

The VPN client can automatically download the certificate from the SecurityBridge. The download is secured by a passphrase. Further information on the password policy can be found in the Online Help on the SecurityBridge.

9.3 Log in to client

When a Client connection has been created for a user, he can log in with his credentials to the SecurityBridge to access the protected system. The credentials must be created on the user interface of the SecurityBridge.

⇒ Open the VPN client, click **Connect**, select a connection and enter your user name and your password.

9.4 Authentication procedure

During authentication, the user name is always searched first in the local user management on the SecurityBridge's user interface. If the user name cannot be found in the internal user management and a RADIUS server is configured, a request is sent to the RADIUS server.

Authentication procedure via the local user management of the SecurityBridge

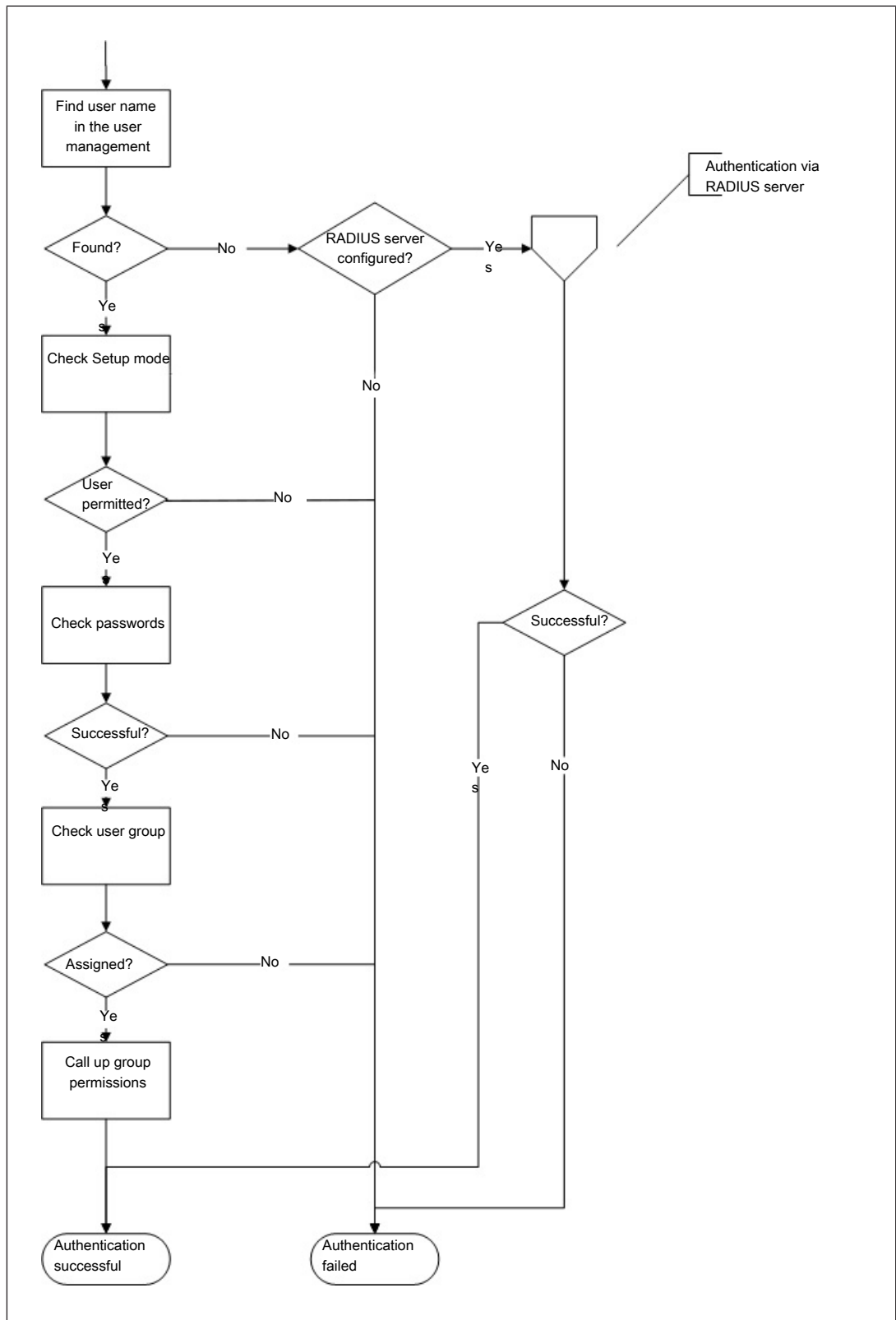


Fig.: Authentication via the internal user management

Authentication procedure via the RADIUS server

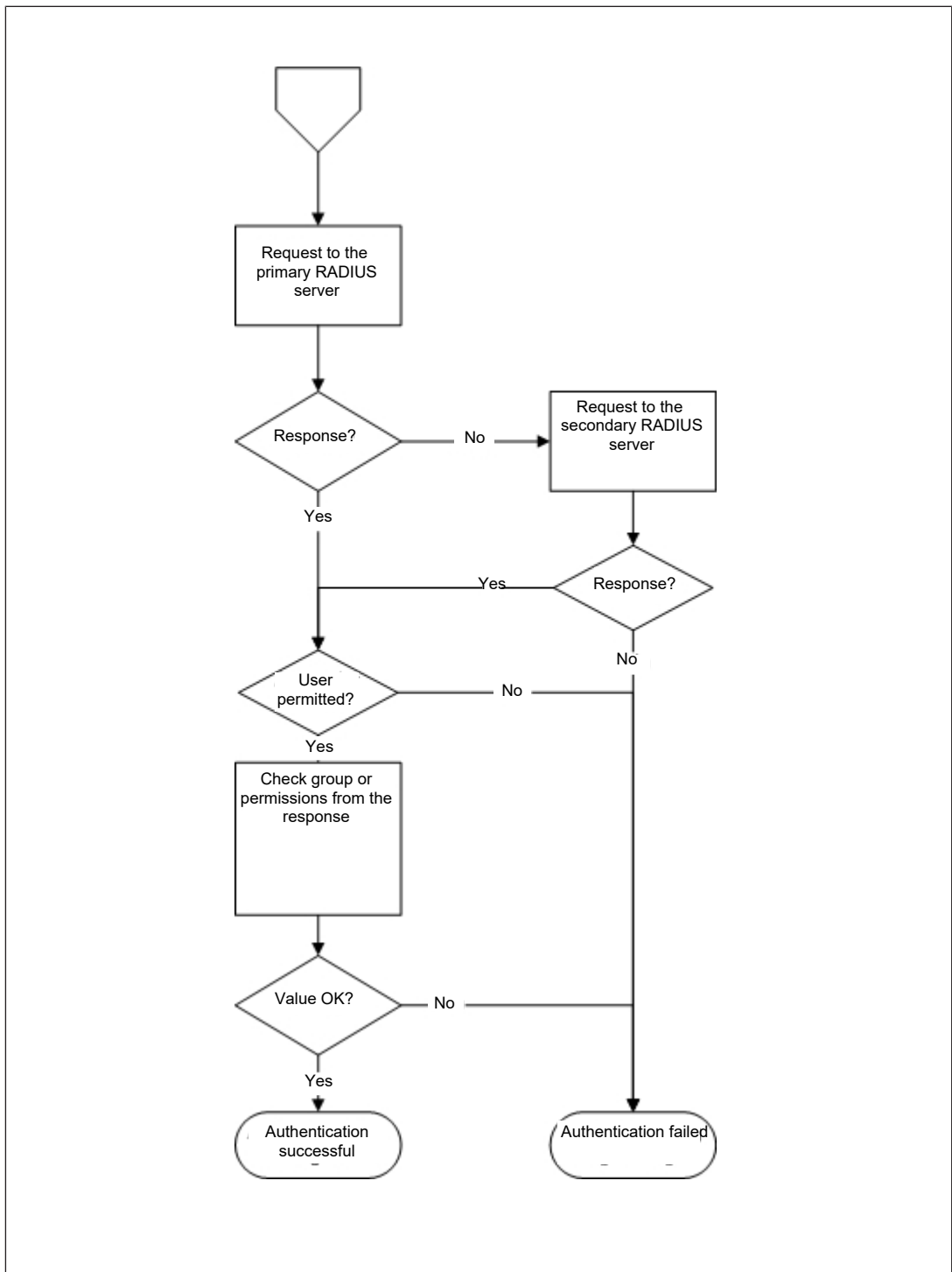


Fig.: Authentication via the RADIUS server

10 Firmware update

If a new firmware version is available, the firmware on the SecurityBridge can be updated.

The update is performed on the user interface.

The firmware can only be updated by users with **Administration** permission.

The update packet is digitally signed to prevent manipulation.

An update packet can be downloaded to the device from the download area on the Pilz website (file extension .fw) or via the software tool **PASupdate**. **PASupdate** will let you know when a new update is available.







CAUTION!

Update the firmware regularly to obtain security-related updates.



11 Operation

11.1 LED indicators





Legend

-  LED on
-  LED flashes
-  LED flashes briefly
-  LED off

PWR


Colour	State	Meaning
---	●	No supply voltage
Green		Supply voltage present. SecurityBridge is operational.
Red		SecurityBridge is in recovery mode

DIAG

Colour	State	Meaning
---	●	Unit is not ready for operation
Green		No error present
Red		One or more recoverable errors on the SecurityBridge (for more information see event log).
Red		One or more internal errors on the SecurityBridge (for more information see event log).
Red		Unreleased firmware is being used.


Bypass

You can configure the colour of the bypass LED.

Colour	State	Meaning
---	●	Bypass mode is deactivated
Green or red		Bypass mode is activated

User

You can configure the function and colour of the user LED.

Colour	State	Meaning
---	●	No function configured
Green or red		Function depends on the configuration

Setup

Colour	State	Meaning
- - -	●	Setup mode is deactivated
Green	☀	Device is in setup mode

I0

Colour	State	Meaning
- - -	●	No signal at the input
Green	☀	There is a 1 signal at the input

O0

Colour	State	Meaning
- - -	●	No signal at the output
Green	☀	There is a 1 signal at the output

TRF

Colour	State	Meaning
- - -	●	No data traffic
Yellow	☀	Data traffic present

LNK


Colour	State	Meaning
- - -	●	No network connection
Green	☀	Network connection exists

11.2

Recovery

If you experience problems with the configuration, a failed firmware update or any other situation in which the system is no longer functional, it may be necessary to reset the system.

Typical problems that require a system reset:

- ▶ Interrupting the supply voltage during the firmware update
- ▶ Forgotten password
- ▶ Incorrect configuration of the IP address
- ▶ All the data must be deleted, when the SecurityBridge is to be decommissioned for example (see operating instructions, Section [Take SecurityBridge safely out of operation](#) [ 42]).

To reset or restore the system, proceed as follows:

1. Switch off the supply voltage to the device.
2. Connect the Ethernet interface X1 to the configuration PC.
Make sure that the connection is secure (e.g. direct network cable between Security-Bridge and configuration PC), because the system is not HTTPS and password-protected in recovery mode.
3. Using a pointed object, press the red service button on the front of the device and keep it held down.
4. Switch on the supply voltage while the service button is held down.
5. Let go of the service button when the Power LED lights up red.
6. Enter the default IP address ***http://192.168.222.1*** in the browser.
The user interface opens in ***Recovery mode***. This interface is only available in English.
7. To restore the system you can choose between the following options:
 - ***Firmware Recovery***
The firmware is reset and restored. The configuration and event messages are retained.
Upload the recovery firmware and then click on ***Firmware Update***.
The system is restarted in operational mode.
 - ***Configuration Recovery***
The system is reset to the factory settings. All the configuration data is deleted. All the event messages are deleted.
Click on ***Configuration Recovery***.
The system is then restarted in operational mode.
 - ***Reboot***
Recovery mode is exited and the system is restarted in operational mode.

11.3 Error mode

If the system detects an internal error, it will switch to error mode.


Settings for how the system should behave in error mode can be made on the user interface:

- ▶ ***Availability***
All data is forwarded
- ▶ ***Security***
No more data is forwarded

11.4 Take SecurityBridge safely out of operation

Before disposal, SecurityBridge has to be safety decommissioned. To do this, all the data have to be deleted from the device.

Proceed as follows:

- ▶ Reset the configuration to the factory settings as described in the chapter [Recovery](#)  40].
- ▶ Switch off the SecurityBridge.
- ▶ If you used an USB memory, remove the USB memory from the SecurityBridge and format it on the configuration PC. Do not carry out a quick formatting. Alternatively, you can use a program to safely delete data or destroy the memory mechanically.

12 Application examples

12.1 PNOZmulti with fieldbus module

The PNOZmulti system in the example consists of the following modules:

- ▶ PNOZmulti base unit PNOZ m B1
- ▶ PNOZmulti input/output module PNOZ m EF
- ▶ PNOZmulti fieldbus module with Ethernet interface

Description:

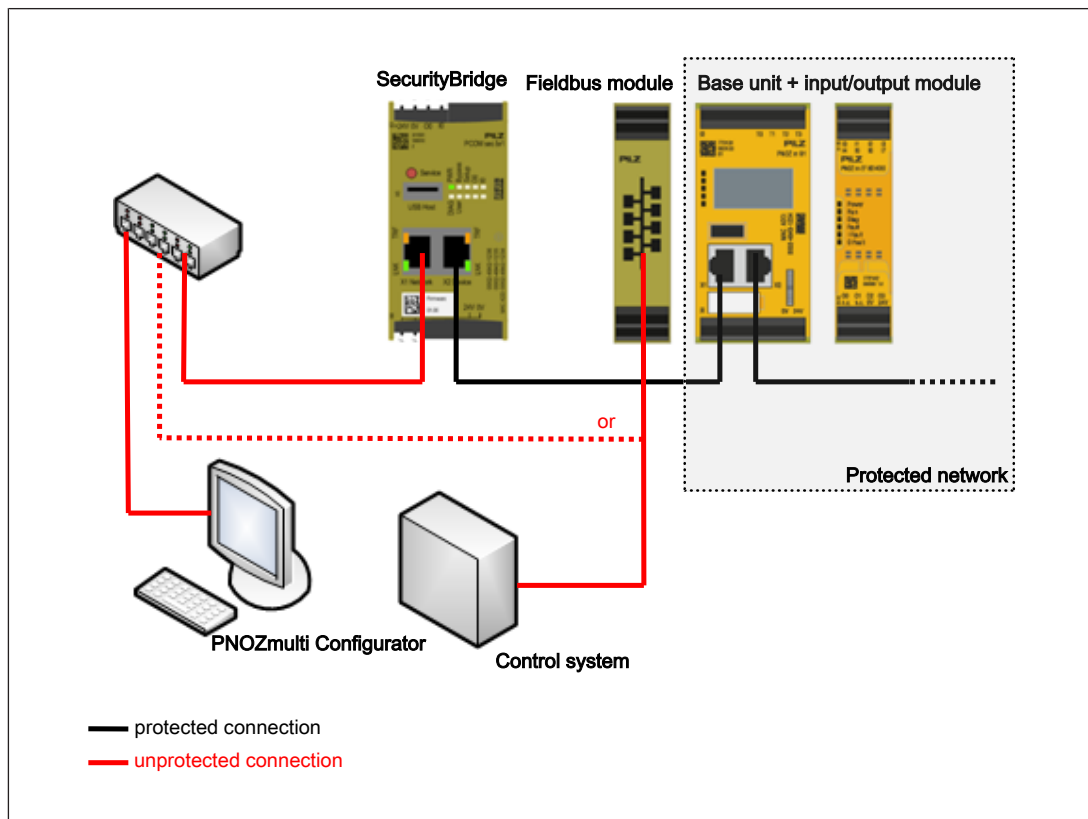
The PNOZmulti system has 2 Ethernet modules in networks that are independent of each other.

- ▶ Base unit in protected network:

The connection to the configuration tool PNOZmulti Configurator is created via the Ethernet interfaces at the base unit. The project is changed via this connection and transferred to the PNOZmulti. This connection is protected. The PNOZmulti base unit is in the protected network. Access to the base unit is only performed with the VPN client via the SecurityBridge.

- ▶ Fieldbus module in unprotected network:

Via the Ethernet interfaces of the left-hand side fieldbus module, process data are exchanged in a control system. This module is in an independent network. The connection to the control system is not protected. The fieldbus module is in the protected network.



12.2 Release of remote access with a key switch

The digital input I0 has several configurable functions. The digital input I0 can be used, for example, for the release of the remote access to a protected network. The release of the connection between the client PC (VPN client) and the protected network can be made via a key switch, for example.

Prerequisites:

- ▶ A key switch is connected to the digital input I0.
 - ⇒ Connect the opening contact of the key switch to the input I0.

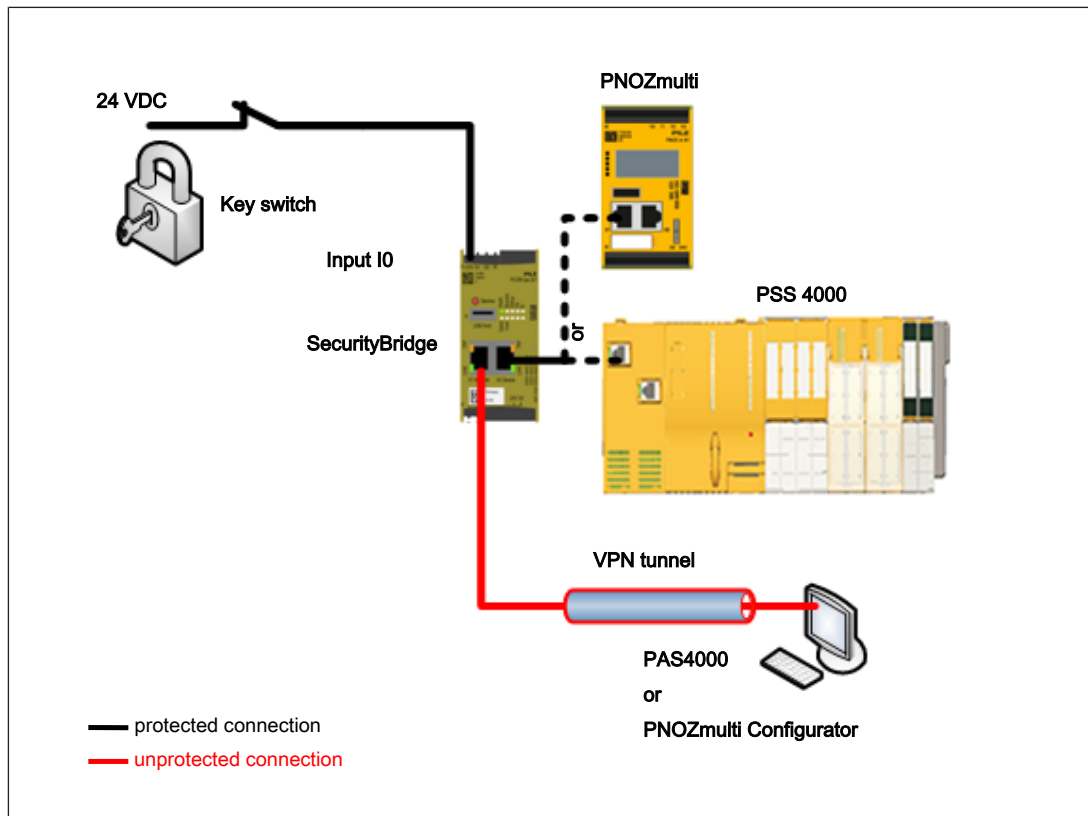


Fig.: Key switch to release the remote access

Procedure:

- ▶ Configure the function of the digital input via the user interface.
 - ⇒ Select **System** -> **Settings** -> **Digital inputs and outputs** -> **Digital input-> Function** and select the option **SSLVPN** from the drop-down list.
- ▶ Establish a connection as described under [Establish connection to SecurityBridge](#) [23].

The release of the connection is made by a "1" signal at the input I0. If there is no release, all the connection attempts via the VPN client are prevented.

12.3 PSS 4000 with an external control and OPC server

The PSS 4000 system is in an unprotected network and it communicates with an external control system and an OPC server in the unprotected network.

Procedure:

1. [Establish connection to SecurityBridge](#) [📖 23]
2. [Create user](#) [📖 26]
3. [Create device](#) [📖 28]
4. [Forwarding rules for PSS 4000](#) [📖 28]

Here you have to configure the forwarding rule for the communication of both PSS 4000 in the protected network with the external control system.

5. [Access to the system in the protected network](#) [📖 34]

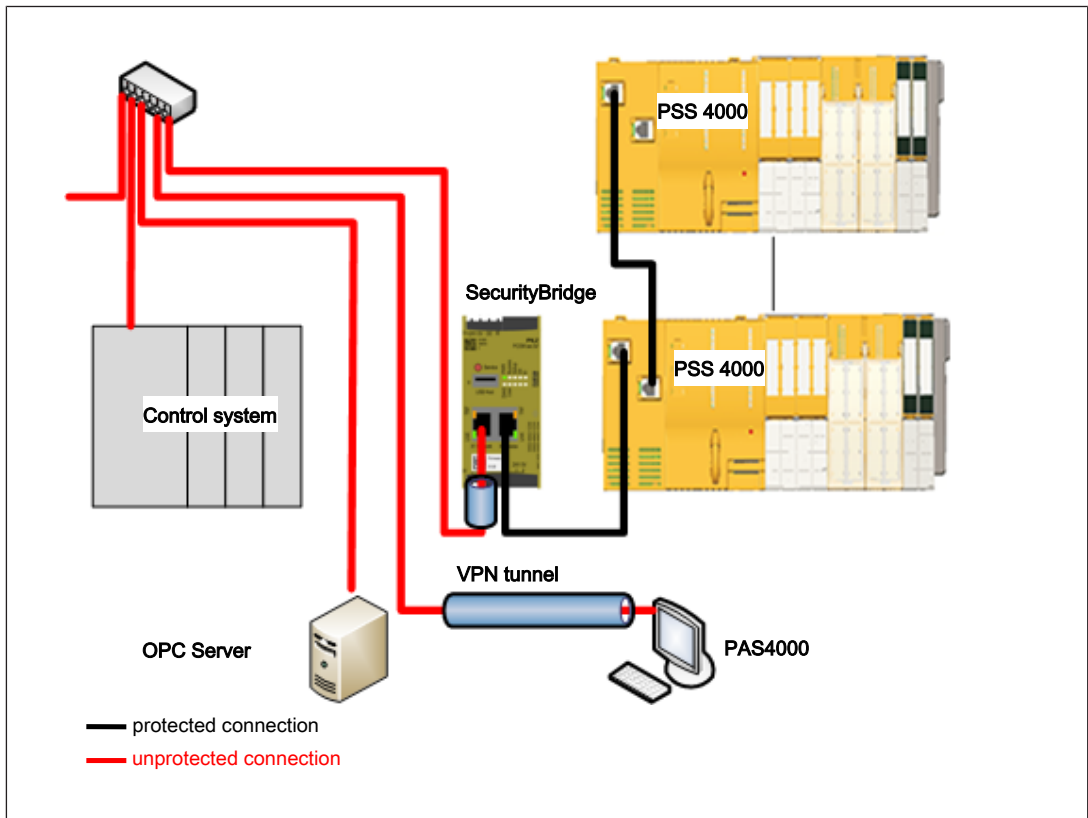


Fig.: Application example PSS 4000 with external control

13 Technical details

General	
Certifications	CE, UKCA, cULus Listed
Application range	Standard
Electrical data	
Supply voltage	
for	Module supply
Voltage	24 V
Kind	DC
Voltage tolerance	-30 %/+25 %
Output of external power supply (DC)	5,5 W
Supply voltage	
for	Periphery supply
Voltage	24 V
Kind	DC
Voltage tolerance	-30 %/+25 %
Output of external power supply (DC)	60 W
Max. power dissipation of module	5,5 W
Status indicator	LED
Inputs	
Number	1
Voltage at inputs	24 V DC
Input type in accordance with EN 61131-2	3
Input current at rated voltage	10 mA
Semiconductor outputs	
Number	1
Current	2 A
External supply voltage	24 V
Voltage tolerance	-30 %/+25 %
Utilisation category in accordance with EN 60947-1	DC-12
Utilisation category in accordance with UL 61010-2-201	DC General use, DC Resistance
USB interface	
Number of USB Hosts	1
Max. voltage	5 V
Max. current	500 mA
Ethernet interface	
Number	2
IP address, factory setting	192.168.222.1
Connection type	RJ45
Transmission rate	10 MBit/s, 100 MBit/s
Environmental data	
Climatic suitability	EN 60068-2-1, EN 60068-2-14, EN 60068-2-2, EN 60068-2-30, EN 60068-2-78

Environmental data	
Ambient temperature	
In accordance with the standard	EN 60068-2-14
Temperature range	0 - 60 °C
Storage temperature	
In accordance with the standard	EN 60068-2-1/-2
Temperature range	-25 - 70 °C
Climatic suitability	
In accordance with the standard	EN 60068-2-30, EN 60068-2-78
Humidity	93 % r. h. at 40 °C
Condensation during operation	Not permitted
Max. operating height above sea level	2000 m
EMC	EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-6-4, EN 61131-2
Vibration	
In accordance with the standard	EN 60068-2-6
Frequency	5 - 8,4 Hz, 8,4 - 150 Hz
Amplitude	3,5 mm
Acceleration	1g
Shock stress	
In accordance with the standard	EN 60068-2-27
Acceleration	15g
Duration	11 ms
Airgap creepage	
In accordance with the standard	EN 61131-2
Overvoltage category	II
Pollution degree	2
Rated insulation voltage	30 V
Protection type	
In accordance with the standard	EN 60529
Housing	IP20 (not evaluated by UL)
Terminals	IP20 (not evaluated by UL)
Mounting area (e.g. control cabinet)	IP54
Potential isolation	
Potential isolation between	Periphery supply and module supply
Type of potential isolation	Basic insulation
Rated surge voltage	500 V
Mechanical data	
Mounting position	vertical
DIN rail	
Top hat rail	35 x 7,5 EN 50022
Recess width	27 mm
Material	
Bottom	PC
Front	PC

Mechanical data	
Connection type	Spring-loaded terminal, screw terminal
Mounting type	plug-in
Conductor cross section with screw terminals	
1 core flexible	0,25 - 2,5 mm², 24 - 12 AWG
2 core with the same cross section, flexible without crimp connectors or with TWIN crimp connectors	0,2 - 1,5 mm², 24 - 16 AWG
Torque setting with screw terminals	0,5 Nm
Conductor cross section with spring-loaded terminals:	
Flexible with/without crimp connector	0,2 - 2,5 mm², 24 - 12 AWG
Spring-loaded terminals: Terminal points per connection	2
Stripping length with spring-loaded terminals	9 mm
Dimensions	
Height	96 mm
Width	45 mm
Depth	111,5 mm
Weight	170 g

Where standards are undated, the 2017-06 latest editions shall apply.

14 Network data

Interface	Log	Direction	Transport log	Port no.	Can be deactivated	Description
User interface	HTTP	In	TCP	0 ... 65535 Def.: 80	No	Browser is always forwarded to HTTPS
User interface	HTTPS	In	TCP	0 ... 65535 Def.: 443	No	Transport protection by TLSv1.2 or TLSv1.3. Access to the user interface via user name and password. The server is authenticated via an X.509 certificate.
VPN access	proprietary	In	TCP	1194	Yes Def.: Active	Authenticated and encrypted log. The connection setup is protected by user name and password. The server is authenticated via X.509 certificate.
VPN Web Service	HTTP	In	TCP	4080	Yes Def.: Active	Critical services are only accessible via the VPN tunnel.
NTP Server	NTP	In	UDP	123	No	accessible only via device port X2
NTP client	NTP	Out	UDP	123	Yes Def: Inactive	Protection configurable by shared encrypted key.
DNS client	DNS	Out	UDP	53	Yes Def: Inactive	
E-Mail log forwarding	SMTP	Out	TCP	0 ... 65535 Def.: 25	Yes Def: Inactive	Optional use of TLS and SMTP authentication
Syslog-log forwarding	SYSLOG	Out	UDP	0 ... 65535 Def.: 514	Yes Def: Inactive	
RADIUS client	RADIUS	Out	UDP	0 ... 65535 Def.: 1812	Yes Def: Inactive	Protected by Server Shared Secret
Switching Loop detection	proprietary	In/out	Layer2	0x88b5	No	Frames are received only via device port X2

15 Security-relevant log messages

Entry ID	Error message
107	The file "{{filename}}" on the USB memory was changed.
108	The active configuration was changed by the user "{{username}}".
109	The start configuration was changed by the user "{{username}}".
200	IO device {{ip_address}}: MAC address monitoring in the protected network led to contradictory answers: {{mac1}} vs {{mac2}}
201	IO controller {{ip_address}}: MAC address monitoring in the unprotected network led to contradictory answers: {{mac1}} vs {{mac2}}
401	User "{{username}}", IP address: {{ip}}: Login attempt failed.
402	The IP address {{ip}} is locked because too many login attempts have failed.
600	Device "{{name}}", IP address {{ip}}: The project CRC has been changed to "{{crc}}".
701	Device "{{name}}", IP address {{ip}}: The device's MAC address was changed to {{mac}}.
702	Device "{{name}}", IP address {{ip}}: Device is not active.
1000	The start configuration was reset and the logging events were deleted in recovery mode.
1001	The firmware with version {{version}} has been installed in recovery mode.
1002	The firmware with version {{version}} has been installed in recovery mode.
1100	User: "{{user}}"; IP address: {{clientIP}}: IP spoofing has been detected. Fake IP address: {{spoofedIP}}
1101	User: "{{user}}"; IP address: {{clientIP}}: MAC spoofing has been detected. Fake MAC address: {{spoofedIP}}.
1105	User "{{username}}", IP address: {{ip}}: Login attempt failed.
1106	Some Client connections have been rejected because the maximum number of Clients has been reached.
1107	The IP address {{ip}} is locked because too many login attempts have failed.
1108	Access to web service denied for IP address {{ip}}.
1109	User "{{username}}", IP address {{ip}}: The IP address is blocked. Too many attempts to change the password.

16 Order reference

16.1 Product

Product type	Features	Order no.
PCOM sec br2	Module for secure authentication and communication with PNOZmulti 2 and PSS 4000	311502

16.2 Accessories

Connection terminals

Product type	Features	Order no.
Set4 Spring Terminals	1 set of spring-loaded terminals	751016
Set4 Screw Terminals	1 set of screw terminals	750016

▶ Support

Technical support is available from Pilz round the clock.

Americas

Brazil

+55 11 97569-2804

Canada

+1 888 315 7459

Mexico

+52 55 5572 1300

USA (toll-free)

+1 877-PILZUSA (745-9872)

Asia

China

+86 21 60880878-216

Japan

+81 45 471-2281

South Korea

+82 31 778 3300

Australia and Oceania

Australia

+61 3 95600621

New Zealand

+64 9 6345350

Europe

Austria

+43 1 7986263-0

Belgium, Luxembourg

+32 9 3217570

France

+33 3 88104003

Germany

+49 711 3409-444

Ireland

+353 21 4804983

Italy, Malta

+39 0362 1826711

Scandinavia

+45 74436332

Spain

+34 938497433

Switzerland

+41 62 88979-32

The Netherlands

+31 347 320477

Turkey

+90 216 5775552

United Kingdom

+44 1536 462203

You can reach our international hotline on:

+49 711 3409-222

support@pilz.com

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.



We are represented internationally. Please refer to our homepage www.pilz.com for further details or contact our headquarters.

Headquarters: Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone: +49 711 3409-0, Telefax: +49 711 3409-133, E-Mail: info@pilz.com, Internet: www.pilz.com

PILZ

THE SPIRIT OF SAFETY

CECE®, CHRE®, CMSE®, InduraNET p®, Leansafe®, Master of Safety®, Master of Security®, PAS4000®, PAScal®, PAScontig®, Pilz®, PIT®, PLID®, PMCPirimo®, PMCPiritego®, PMCTendo®, PMD®, PMJ®, PNOZ®, PRCM®, PRM®, PRMNET p®, PSS®, PVIS®, SafetyBUS p®, SafetyBUS p®, SafetyEYE®, THE SPIRIT OF SAFETY® are registered and protected trademark of Pilz GmbH & Co. KG in some countries. We would point out that product features may vary from the details stated in this document, depending on the status at the time of publication and the scope of the equipment. We accept no responsibility for the validity, accuracy and entirety of the text and graphics presented in this information. Please contact our Technical Support if you have any questions.

1004534-EN-06, 2022-02 Printed in Germany
© Pilz GmbH & Co. KG, 2019