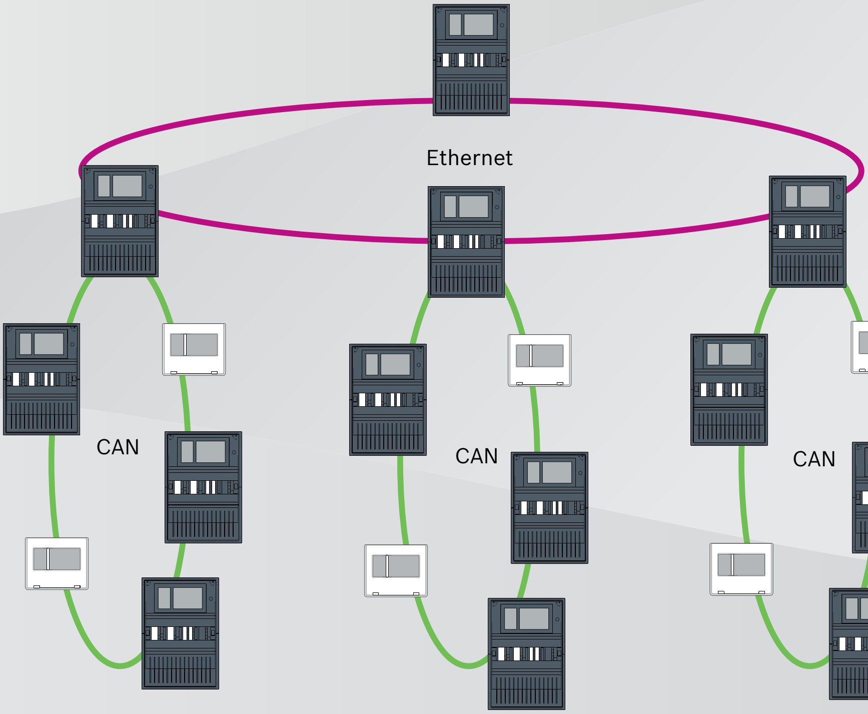
BOSCH

AVENAR panel series | FPA-5000 | FPA-1200



en Networking guide

Table of contents

1 Safety

In this chapter you find organizational measures for PC running service clients for the Bosch portfolio for fire products. You are obliged to comply with these contractual agreements.
You find also safety notices collected and sorted by topics. Later on, the safety notices are placed before the related instruction.

1.1 Organizational measures for PC running service clients

Introduction
The Bosch portfolio for fire products covers PC programs (Service-Clients) running on a computer, which requires physical connection to the fire alarm system. Due to security considerations and regulatory standard requirements, the fire alarm system must not be installed in a shared network. This in turn means the complete fire alarm system network and the PC running a service-client must build a physically dedicated network. Since Bosch only develops the service-clients but not the PCs they are running on, the computer cannot be controlled by Bosch. To reduce the risk of potential security issues this documents defines organizational measures.

Measures
If measures described below require an internet connection - or the service client requires a temporary internet connection for licensing, the PC must be physically isolated from the fire alarm system network before connecting the PC to the internet. The internet connection must be removed before reconnecting the PC to the fire alarm system network again.

1. Operating Systems
   Bosch documents prerequisites for the service clients including the operating system versions. The clients are guaranteed to be compatible with these versions. The operating system the client is running on must be updated on a regular base to fix potential security vulnerabilities.
   The system must be configured to allow write access only to those folders, which are required for the corresponding task. Per default, all users shall be granted read-only permissions.
2. Antivirus
   A state-of-the-art antivirus software must be installed and running on the computer. Its definition files must be updated on a regular base.
3. Firewall
   A software firewall must be installed and running on the PC. It has to be configured to allow traffic between the service client and the fire alarm system, updates for the operating system and the antivirus software. Additionally it must block all other traffic.
4. Secure user login
   The access to the PC must be restricted to operators using the installed service client. The login must be secured by state-of-the-art means. If a password is chosen to secure the access, policies shall enforce state-of-the-art password rules.
   The two-man rule (four-eyes principle) or multi-factor authentication are recommended approaches to strengthen the authentication if applicable.
5. Software and Services
   The amount of software installed on the PC shall be reduced to a minimum. Only software required by the service client and for corresponding tasks shall be installed.
6. Usage limitations
   The usage of the PC must be restricted to service related tasks by organizational means. This also covers using the internet for other purposes than described in this document.

7. Segregation of duties
   Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse, i.e. different tasks shall be assigned to different roles.
8. Monitoring
   All access attempts to the PC running the service client must be monitored to recognize unauthorized access to the PC and the internet.

1.2 Explanations of safety symbols

⚠ **Warning!**
Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠ **Caution!**
Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

ℹ **Notice!**
Indicates a situation which, if not avoided, could result in damage to the equipment, to the environment, or to data loss.

1.3 Safety notices

Media converter

⚠ **Warning!**
Laser light
Do not look directly into the beam with the naked eye or with visual instruments of any kind (e.g. magnifying glass, microscope). Failure to observe this notice poses a danger to the eyes at a distance of less than 100 mm. The light emerges at the visual terminals or at the end of the fiber optic cables connected to these. CLASS 2M laser diode, wavelength 650 nm, output < 2 mW, in accordance with IEC 60825-1.

Remote Services

⚠ **Caution!**
For access via the internet use only Bosch Remote Services.

⚠ **Caution!**
Remote Services require a secure IP connection. Bosch Remote Services or connection with Private Secure Network is required.
With Private Secure Network an IP network is provided, which is based on DSL with an optional wireless access on the panel side (EffiLink). Remote Services for Private Secure Network is only available in Germany with a service agreement with Bosch BT-IE.

Notice!
An exclusive Ethernet network is required in order to set up a central fire alarm network.
The use of a fire alarm system in any other Ethernet network is at the own risk of the user.
Bosch disclaims any and all warranties and liabilities for this misapplication.
In case of non-exclusive Ethernet network reliable alarm transmission and IT-security cannot be ensured.

Panel network

Notice!
EN 54
To ensure that the network is set up in compliance with EN 54, use only components that have been approved for use in central fire alarm networks.
External RSTP switches and media converters in Ethernet networks must be installed in panel housings. The installation outside of a panel housing is not compliant with EN 54.

Notice!
TX cable length
All IP connections must be direct or via media converters approved by Bosch. The node to node TX cable length must be less than 100 m.

Notice!
VdS 2540
To meet the requirements of VdS 2540 for data transmission paths use fiber optic cable for Ethernet connections. For connections within a housing you can use TX Ethernet cables.

Notice!
For standard applications, use standard network settings.
Changes to standard network settings are permitted only for experienced users with appropriate networking knowledge.

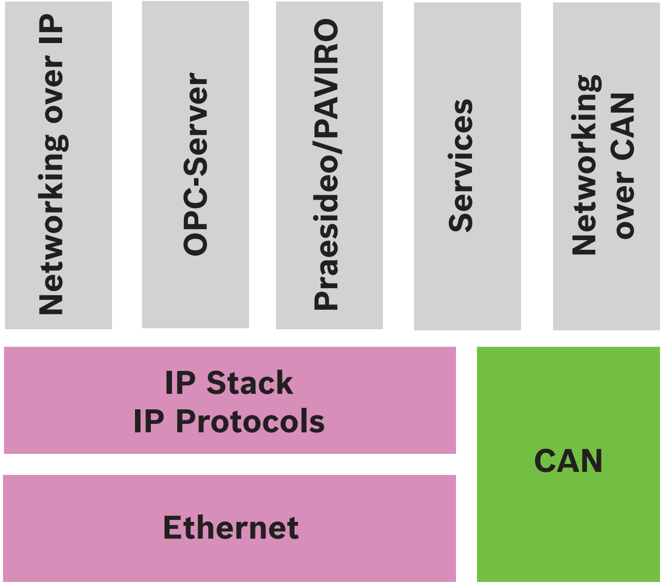
Notice!
Applicable topologies
The functionality and panel-to-panel communication is limited by the panel type. Refer to the panel specification for information on services, for number of connectable panels and for number of connectable remote keypads.

2 Introduction

This document is aimed at readers with experience in planning and installing EN 54 compliant fire alarm systems. In addition, you need networking knowledge.
This document describes a variety of fire alarm network topologies. The topologies are described independently of the fire panel type.
For building up panel networks corresponding to the introduced topologies and connecting services, you need the networking pattern described in this document.
The document provides an overview of the basic conditions, limit values, and general procedures for panel network planning and installation.
Detailed descriptions of the installation of the individual components can found in the respective installation guides.
You find a description of the user interface of the panel controller in the user guide included with the device.

The user interface of the FSP-5000-RPS programming software is described in the online help.

3 System overview



In the network, the Ethernet interface and IP protocols are used for different services. The Ethernet interface can be disabled completely or its use disabled only for networking over TCP/IP. Disabling may be necessary for networking over CAN.

Enabling services

- networking over TCP/IP
  In FSP-5000-RPS, enable panel-to-panel communication in the Ethernet network
- OPC servers
  Add an OPC server to the FSP-5000-RPS configuration
- Praesideo/PAVIRO connection
  Add a Voice Alarm System to the FSP-5000-RPS configuration and configure virtual triggers.
- Remote Services (Remote Connect as prerequisite, Remote Maintenance and Remote Alert)
  Activate the relevant check box in FSP-5000-RPS
- Remote Services (Remote Connect as prerequisite, Remote Maintenance and Remote Alert) for Private Secure Network
  Add remote access to the FSP-5000-RPS configuration and set up the remote access in FSP-5000-RPS.

Notice!
Unintentionally data transfer
If the Ethernet interface of the panel controller is used only for communicating with an OPC server or for Remote Services disable the panel communication over TCP/IP, in FSP-5000-RPS. Otherwise fire data could be transferred over the Ethernet unintentionally.

To operate Ethernet or TCP/IP-based services, the Ethernet interfaces must be enabled and the correct TCP/IP settings configured.

Network of panels and remote keypads

The table shows the options for networking panels/remote keypads depending on the network topology and the panel type. Consider the limits determined by the network topology.

Topology	AVENAR panel 8000, premium license	AVENAR panel 8000, standard license	AVENAR panel 2000, premium license	AVENAR panel 2000, standard license
Standalone	Possible	Possible	Possible	Possible
Loop	Max. 32 panels/ remote keypads, connectivity with AVENAR panel 2000, premium license, and FPA	Max. 32 panels/ remote keypads, connectivity with AVENAR panel 2000, premium license, and FPA	Max. 32 panels/ remote keypads, connectivity with AVENAR panel 8000 and FPA	1 panel and max. 3 remote keypads
Panel redundancy	Redundant panel controller must be premium as well. You can also use a remote keypad as redundant panel.	Redundant panel controller can be standard. You can also use a remote keypad as redundant panel.	Not possible	Not possible

Topology	FPA-5000	FPA-1200
Standalone	Possible	Possible
Loop	Max. 32 panels and remote keypads	1 panel and max. 3 remote keypads
Panel redundancy	Possible	Not possible (DIP 6 on panel controller is not functional.)

If you extend an FPA-5000 network, Bosch recommends to extend the network with a panel of the AVENAR panel series.
When exchanging a panel of the FPA series with a panel of the AVENAR panel series, then it is sufficient to exchange the panel controller solely. Remind, that the panels of the AVENAR panel series does not support address cards. In case of a plugged Ethernet switch, you can continue the usage of it.
When exchanging a remote keypad of the FPA series by a remote keypad of the AVENAR panel series, check if the line resistance is within the range specified for the remote keypad of the AVENAR panel series.

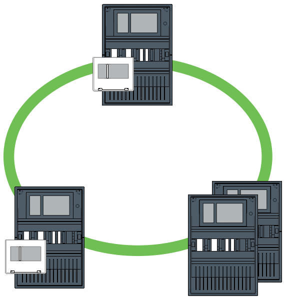
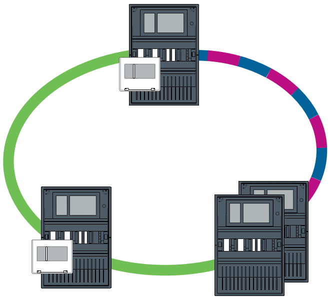
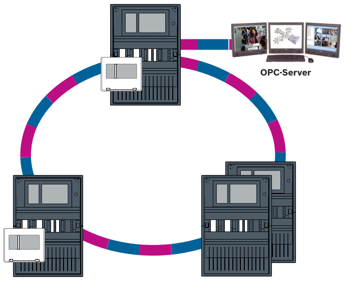
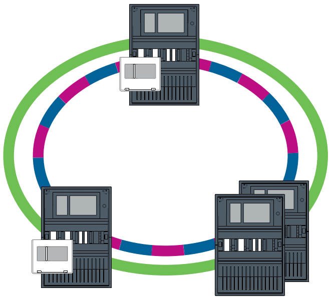
Notice!
Firmware installation
Connected panels must have the same firmware version.
A firmware installation is possible for the active panel solely. For redundant panels perform the firmware installation for both panels. To do so, you have to switch the panel roles and switch it back after successful firmware installation.

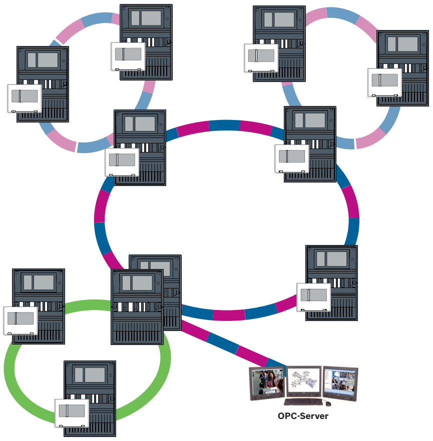
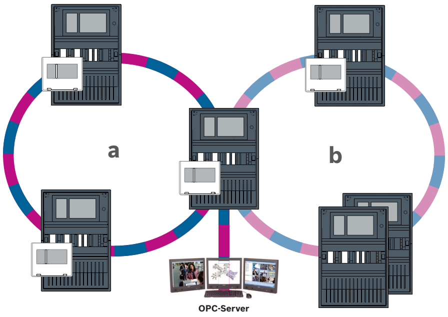
Notice!
Redundant panel controller
It is not possible to combine a panel controller of the AVENAR panel series and a panel controller of the FPA series for redundancy.

4 Topologies

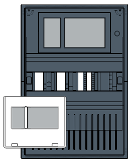
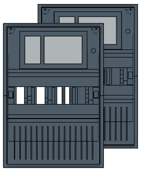
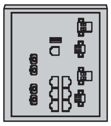
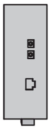
This document describes a variety of fire alarm network topologies. The topologies are described independently of the fire panel type.

Notice!
Applicable topologies
The functionality and panel-to-panel communication is limited by the panel type. Refer to the panel specification for information on services, for number of connectable panels and for number of connectable remote keypads.

 *CAN loop, page 15*	 *CAN loop with Ethernet segments, page 16*
 *Ethernet loop, page 15* *Ethernet loop with OPC server, page 15* *Ethernet loop with OPC server to redundant panel, page 16*	 *Ethernet/CAN double loop, page 16*

 *Ethernet backbone with sub-loops (Ethernet/ CAN), page 17*	 *Connecting Ethernet loops, page 18*

Cable	Description
🟦 🟦	TX Ethernet cable (copper), node to node TX cable length < 100 m
🟪 🟪	FX Ethernet cable (fiber optic cable)
🟦🟪🟦🟪🟦🟪🟦🟪	TX or FX Ethernet cable, node to node TX cable length < 100 m
🟩	CAN cable, node to node CAN cable length < 1000 m

Device	Description
	Panel or remote keypad (in Ethernet topology one internal RSTP switch each)
	Redundant panel (in Ethernet topology internal RSTP switch) A remote keypad can be used as a redundant panel controller. The network connections and the settings are identical for a redundant panel controller and a redundant keypad. Usage of a redundant keypad is applicable to AVENAR panel 8000 only.
	Ethernet switch as external RSTP switch (in general Ethernet switch MM)
	Media converter
	Secure network gateway for Remote Services

Limits in network

The number of panels and remote keypads that can be networked depends on the choice of network topology.

Networked panels and remote keypads are known as nodes.

- The number of detection points in a network is limited to 32768.

- The number of detection points per panel operated in a network is limited to 2048.
- The number of nodes per system depends on the type of topology.
  A node is either a panel controller or a remote keypad.
- The number of nodes in loop topology is limited to 32.
- With FSP-5000-RPS you can assign up to 3 configured remote keypads to one panel.

The cabling between nodes and the maximum permissible cable length is also determined by the choice of topology.
Up to 32 panel controllers, remote keypads and OPC servers can be combined to form a network.
Depending on the intended application, different panel controllers and remote keypads can be divided into groups and defined as network nodes or local nodes. As a rule, within any given group, only the status of control panels within the defined group can be displayed. The status of all control panels can be displayed and/or processed from network nodes, irrespective of the group to which the panels belong.

Physical node address
A panel or a remote keypad is identified in the network by a unique address, which is known as the physical node address.

Notice!
Physical node address for redundant panels
A redundant panel must have the same physical node address as the assigned primary panel.

Notice!
The network used must meet the following minimum requirements:
Minimum throughput: 1 Mbps
Maximum latency: 250 ms

Notice!
EN 54
To ensure that the network is set up in compliance with EN 54, use only components that have been approved for use in central fire alarm networks.
External RSTP switches and media converters in Ethernet networks must be installed in panel housings. The installation outside of a panel housing is not compliant with EN 54.

Notice!
Redundant panel - EN 54-2
For each panel, a maximum of 512 detection points can be connected according to EN 54-2. If this number is exceeded, you have to design the panel redundantly.
Also if a panel acts as an interface with a CAN sub-loop and more than 512 detection points are connected in the sub-loop, then you have to design the panel redundantly. The RSTP switch which connect 2 loops performs the redundancy.
For a standalone panel you can connect up to 4096 detection points, even though it is designed redundantly. If the panel is included in a network, then you can connect a maximum of 2048 detection points.

Notice!
Make sure that the physical node address assigned to the panel matches that in the programming software. The latter is responsible for setting the last number of the IP address in the standard settings.
Activate RSTP as the redundancy protocol and adopt the default standard values.

Standard Ethernet settings of fire panel
In the standard settings of the fire panel, both the FSP-5000-RPS programming software and the control unit adopt the set physical node address as the last number of the IP address.

Notice!
Correct setting of the physical node address on the panel controllers and in the FSP-5000-RPS programming software is a requirement for a run-capable network.

Notice!
Use of the Ethernet redundancy must be activated separately in the panel controller.

- IP settings
  - IP address 192.168.1.x
    The last digit of the IP address in the standard settings is always identical to the physical node address set on the panel controller.
  - Network screen 255.255.255.0
  - Gateway 192.168.1.254
  - Multicast address 239.192.0.1
  - Port number 25001 - 25008 (only the first port can be set, 8 consecutive ports are always used)
- RSTP parameters (default settings)
  - Bridge Priority 32768
  - Hello Time 2
  - Max. Age 20
  - Forward Delay 15

Notice!
You can use the standard settings of the IP configuration with networks of up to 20 RSTP switches.
In the case of networks with more than 20 RSTP switches, additional settings are required according to the topology. In-depth knowledge of networks is required for this.

Settings for loops with more than 20 RSTP switches
If there are more than 20 RSTP switches in the network, then you must adjust the RSTP settings on the panel controller and in the programming software. Panel controllers, remote keypads, and the connected external RSTP switches are regarded as RSTP switches. Redundant panel controllers are not regarded as RSTP switches, as the switch contained within these is not operated as an RSTP switch.

- RSTP parameters
  - Keep Bridge Priority 32768
  - Keep Hello Time 2
  - Change Max. Age from 20 to 40

- Change Forward Delay from 15 to 25

Parameters

- A maximum of 32 nodes can be used in a loop.
- The diameter of the network must not be greater than 32, see *Network diameter, page 21*.
- Ethernet switches must not be used outside of panel housings.
- Media converters must not be used outside of panel housings.

Features

- The network is EN 54-compliant.
- The network uses RSTP.

Connection to BIS with OPC server

When connecting to a building management system (BIS) via an OPC server and Ethernet 100BaseTX in multiple building networks, you must clarify with the network administrator:

1. Is the network designed for multiple building connections? (e. g. there must be no technical interference due to differences in grounding potential)
2. Is the bandwidth of the bus users sufficient for the network?

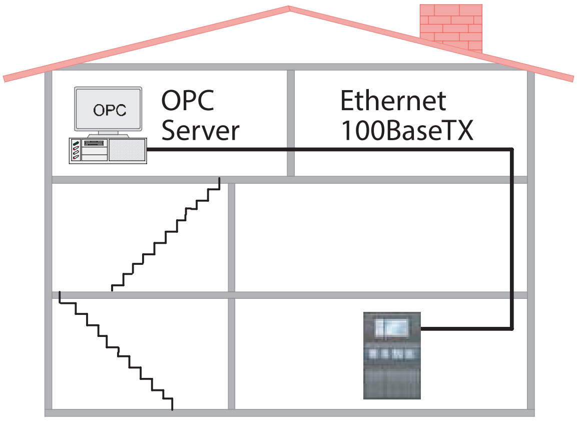


Figure 4.1: Connection to BIS via OPC server

Additional information when using an OPC server

OPC servers in your network must be added to the FSP-5000-RPS programming software. You must perform the following settings in both the FSP-5000-RPS software and on the OPC server:

- Network nodes
- Network group
- RSN
- IP address
- Port

The OPC server uses port 25000 as standard.

Notice!

EN 54

The connection of a building management system (e.g. BIS) via an Ethernet interface using an OPC server or an FSI server is EN54 compliant if the EN54 relevant functions are performed by the fire panel solely. Any EN54 relevant control or administration (e.g. control of notification appliances or administration of switch-off) by the building management system requires an individual EN54 certification of the overall system by a certification body.

Notice!
FSP-5000-RPS programming software
You must assign an OPC server to each network node from which statuses should be transmitted.

4.1 CAN loop

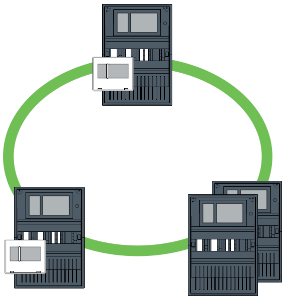


Figure 4.2: CAN loop

4.2 Ethernet loop

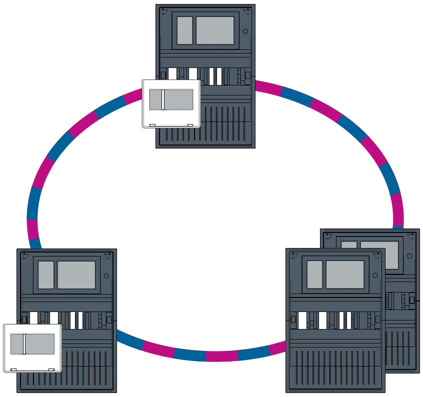


Figure 4.3: Ethernet loop

4.3 Ethernet loop with OPC server

Ethernet switch for connecting the OPC server must be programmed separately
Program the IP address and redundancy settings of the Ethernet switch, see *Settings on switch, page 43*. As the switch is installed in the immediate vicinity (without intermediate space), the power supply does not have to be designed redundantly and the fault outputs are therefore not used.
Make sure that the RSTP settings in the panel controllers, in FSP-5000-RPS and in the Ethernet switch are identical.

OPC server must be programmed separately
Program the IP address, network nodes, network group and RSN. See the corresponding section in the Installation chapter of the Networking Guide.
The OPC server uses port 25000 as standard.
Make sure that the settings in the FSP-5000-RPS programming software and in the OPC server are identical.

Parameters

- The OPC server may be connected via an Ethernet cable (copper) or fiber optic cable.

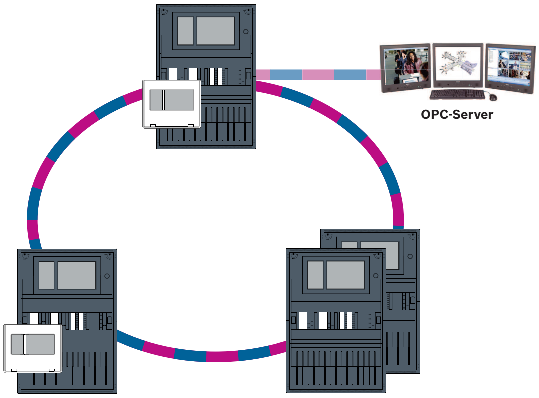


Figure 4.4: Ethernet loop with OPC server

4.4 Ethernet loop with OPC server to redundant panel

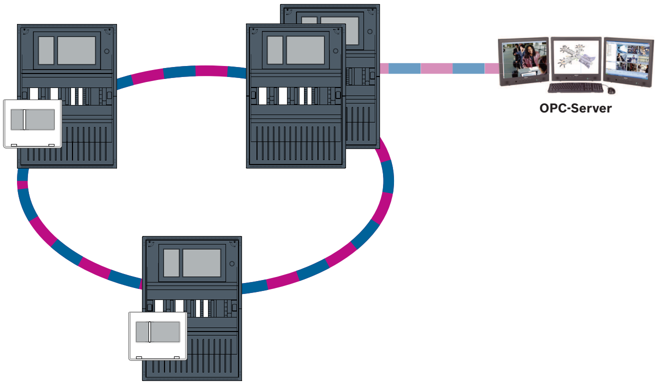


Figure 4.5: Ethernet loop with OPC server to redundant panel

4.5 Ethernet/CAN double loop

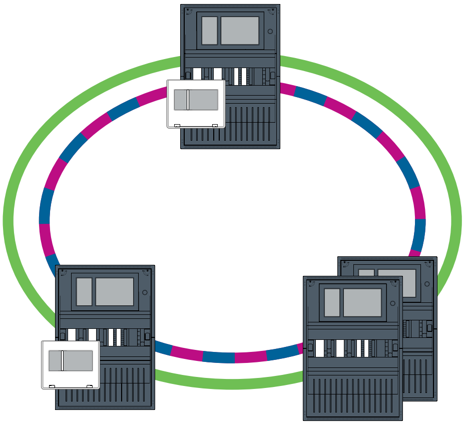


Figure 4.6: Double loop of Ethernet and CAN

4.6 CAN loop with Ethernet segments

The main topology is a CAN loop. When the distance between two nodes is longer than 1000 m, an FX Ethernet connection can be used to cover the distance.

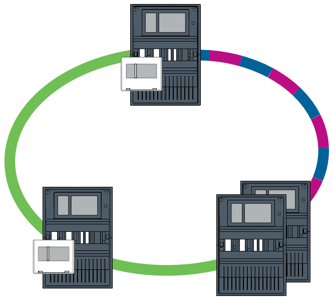


Figure 4.7: CAN loop with Ethernet segments

4.7 Ethernet backbone with sub-loops (Ethernet/CAN)

An Ethernet backbone is connected to all sub-loops, and therefore a connecting core area with high data transmission rates. The RSTP switches in the backbone are not superordinate, by default. Note that with this topology you are required to determine the network diameter. Panel controllers, remote keypads and the connected external RSTP switches are regarded as RSTP switches. CAN-networked panels are disregarded when determining the network diameter.

Consider the settings for loops with more than 20 RSTP switches, see *Settings for loops with more than 20 RSTP switches, page 13*.

Notice!

This topology requires additional settings for all RSTP switches in the backbone. More in-depth knowledge of networks is therefore required.

Notice!

If the panel acts as an interface with a CAN sub-loop, this panel must then also be designed redundantly according to EN 54-2 if more than 512 detection points are connected in the sub-loop.

This restriction does not apply in an Ethernet sub-loop, as the switches to connect the 2 loops perform the redundancy.

Additional settings

You must operate the central loop as the backbone. This central loop must be networked via Ethernet.

Notice!

For all RSTP switches in the backbone, set a higher RSTP priority than in the sub-loops. This ensures that the RSTP root bridge will always remain in the backbone, even in the event of a fault.

The RSTP switches to connect the loops are part of the backbone!

Use a RSTP priority of 16384 in the backbone.

Notice!

The lower the set value, the higher the RSTP priority.

Switches for connecting the OPC server and the sub-loops must be programmed separately
Program the IP address and redundancy settings of the Ethernet switches, see *Settings on switch, page 43*. For this topology, the fault outputs of the switch only have to be used if you have designed the power supply for the switch redundantly or there is a switch-to-switch connection, see *Ethernet switch, page 54*.
Make sure that the RSTP settings in the panel controllers, in FSP-5000-RPS and in the Ethernet switch are identical.

Notice!
Change the RSTP priority for the RSTP switches that connect the loops, as they belong to the backbone.

OPC server must be programmed separately
Program the IP address, network nodes, network group and RSN, see *OPC servers, page 60*.
The OPC server uses port 25000 as standard.
Make sure that the settings in the RPS programming software and OPC server are identical.

Parameters

- The OPC server may be connected via an Ethernet cable (copper) or fiber optic cable.

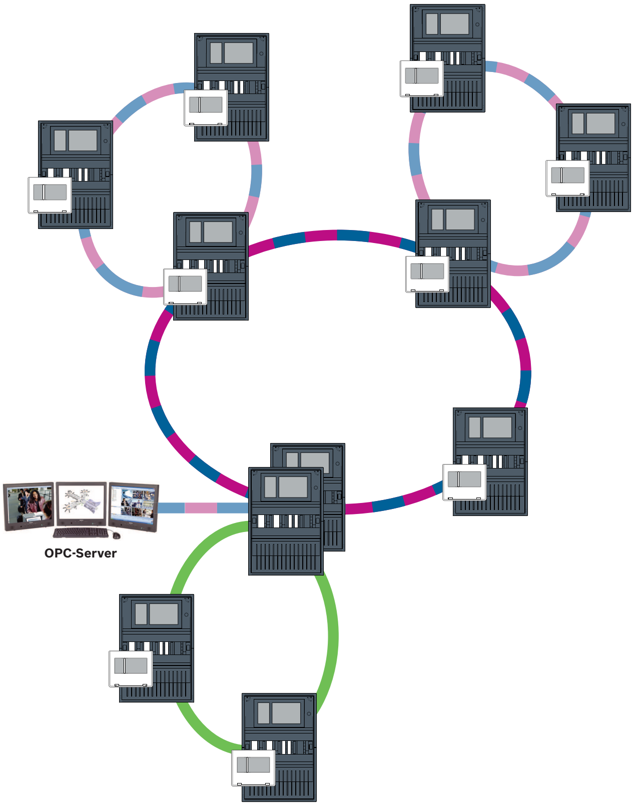


Figure 4.8: Ethernet backbone with sub-loops

4.8 Connecting Ethernet loops

Notice!
This topology requires additional settings for all RSTP switches in the backbone. More in-depth knowledge of networks is therefore required.

Additional settings

This topology is a special instance of the Ethernet backbone with sub-loops, see Ethernet backbone with sub-loops (Ethernet/CAN). You must operate one of the two loops as the backbone.

Notice!

For all panels and switches in the backbone, set a higher RSTP priority than in the sub-loops. This will ensure that the RSTP root bridge will always remain in the backbone, even in the event of a fault.
The switches to connect the two loops are part of the backbone!
Use a RSTP priority of 16384 in the backbone.

Notice!

The lower the set value, the higher the RSTP priority.

Switches for connecting the OPC server and the second loop must be programmed separately

Program the IP address and redundancy settings of the Ethernet switch, see *Settings on switch, page 43*. For this topology, the fault outputs of the switch only have to be used if you have designed the power supply for the switch redundantly, see *Ethernet switch, page 54*.
Make sure that the RSTP settings in the panel controllers, in FSP-5000-RPS and in the Ethernet switch are identical.
Change the RSTP priority for the switches for connecting the two loops, as they belong to the backbone.

OPC server must be programmed separately

Program the IP address, network nodes, network group and RSN. See the corresponding section in the Installation chapter of the Networking Guide.
The OPC server uses port 25000 as standard.
Make sure that the settings in the FSP-5000-RPS programming software and in the OPC server are identical.

Parameters

- The OPC server may be connected via an Ethernet cable (copper) or fiber optic cable.

In these examples, loop a is the backbone. Loop b is the sub-loop.

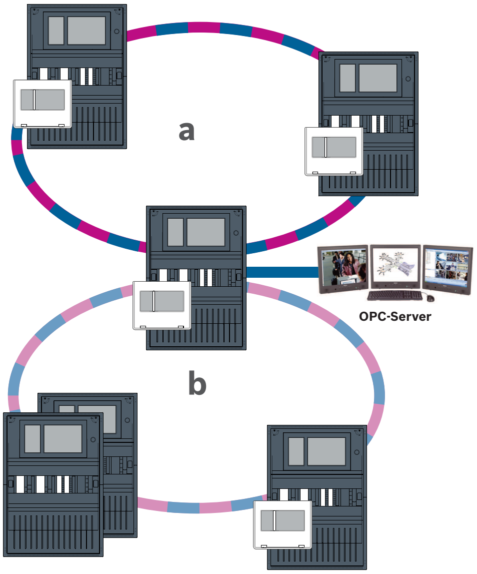


Figure 4.9: Connecting Ethernet loop via a non-redundant panel

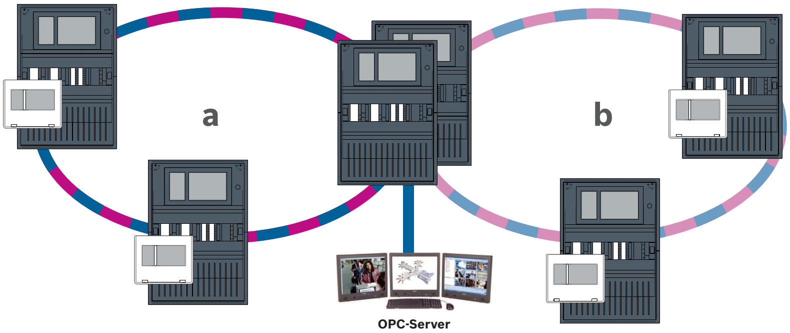


Figure 4.10: Connecting Ethernet loop via a redundant panel

5 Ethernet network

In the network, the Ethernet network connections are monitored continuously. If a connection has been severed, then the interruption is detected. Repaired connections are also detected. The network diagnosis of the panel always shows you the MAC address of the hosts connected via the network.

MAC addresses

For network connection each panel controller provides the following MAC addresses.

- MAC address for the host
- MAC address to identify the ETH1 port
- MAC address to identify the ETH2 port

Depending on panel controller type:

- MAC address to identify the ETH3 port
- MAC address to identify the ETH4 port

Rules for using 4 Ethernet ports

If your panel has 4 Ethernet ports, apply the following rules in the given order. Bosch supports networks, which are built according to the following rules, only.

1. For panel networking you have to use ETH1 and ETH2. An external RSTP switch on ETH1 or ETH2 must only be used for panel networking.
2. For connecting an OPC, an FSM-5000-FSI, a Praesideo/PAVIRO, an UGM-2040 you have to use ETH3. You may connect an external RSTP switch, which must not be used for panel networking.

3. For Remote Services you have to use ETH4. If no connection to Remote Services is required, then ETH4 can be used for connecting an OPC, an FSM-5000-FSI, a Praesideo/PAVIRO, or an UGM-2040.
4. If there is no panel networking via ETH1 and ETH2, then each can be used for connecting an OPC, an FSM-5000-FSI, a Praesideo/PAVIRO, or an UGM-2040.

5.1 Protocols

SNMP

SNMP is used to monitor and control network components. To this end, parameters of network nodes can be read out or modified. For this you require the appropriate network management software (e.g. Hirschmann HiVision).

Notice!

The network uses the fixed SNMP community string: PUBLIC

Consider, that the AVENAR panel series does not yet support the SNMP protocol.

LLDP

LLDP is a basic protocol standardized by the IEEE. It is used to share network information between neighboring devices. This information is

- provided as part of the SNMP data
- displayed via the panel controller as part of the network diagnostic data

RSTP

RSTP is a network protocol standardized by the IEEE. RSTP ensures that there are no loops in networks. Redundant paths are detected in the network, deactivated and activated when necessary (failure of a connection).

The protocol is used for exactly this purpose in the network.

A change to the topology following the failure of a connection is automatically canceled once it has been repaired.

5.2 Network diameter

The network diameter of RSTP Ethernet panel networks must not be greater than 32.

Definition

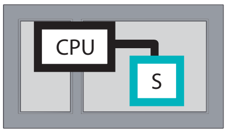
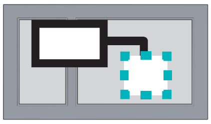
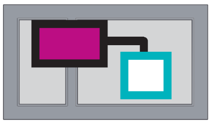
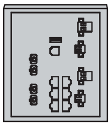
The diameter of a network corresponds to the number of RSTP switches on the longest possible section without loops between any 2 end points in the network.

The following must be taken into account in relation to a RSTP Ethernet panel network:

- Each panel controller contains an end point and an internal RSTP switch.
- A combination of panel controller and redundant panel controller counts as just one RSTP switch.
- Media converters are not regarded as RSTP switches.
- CAN connections may not be included in the longest possible section.
- OPC servers are not taken into account with respect to the diameter.

Key

CPU	Central processor in the panel controller or in the remote keypad.
S	Internal RSTP switch in the panel controller or in the remote keypad.

	Panel controller or remote keypad with central processor and internal RSTP switch.
	Redundant panel controller with central processor and internal RSTP switch.
	Panel controller or remote keypad Starting or end point for determining the network diameter in the examples.
	Ethernet switch as external RSTP switch (in general Ethernet switch MM)

2 connected panels form the smallest possible loop. The diameter of this network is equal to 2, as the internal RSTP switches are located between the end points.

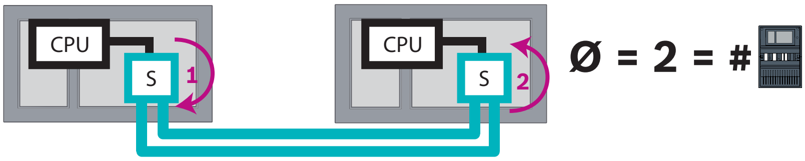


Figure 5.1: Network diameter of a loop with 2 panels

In a panel loop without external RSTP switches, the diameter of the network corresponds to the number of installed panels.

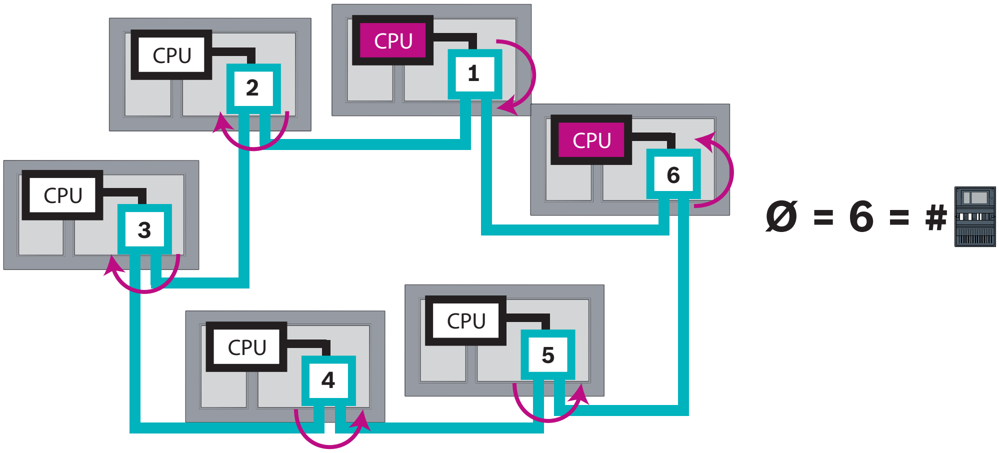


Figure 5.2: Network diameter of a loop with 6 panels

If a backbone and sub-loops are connected to each other via Ethernet switches, then these external RSTP switches must also be taken into account.

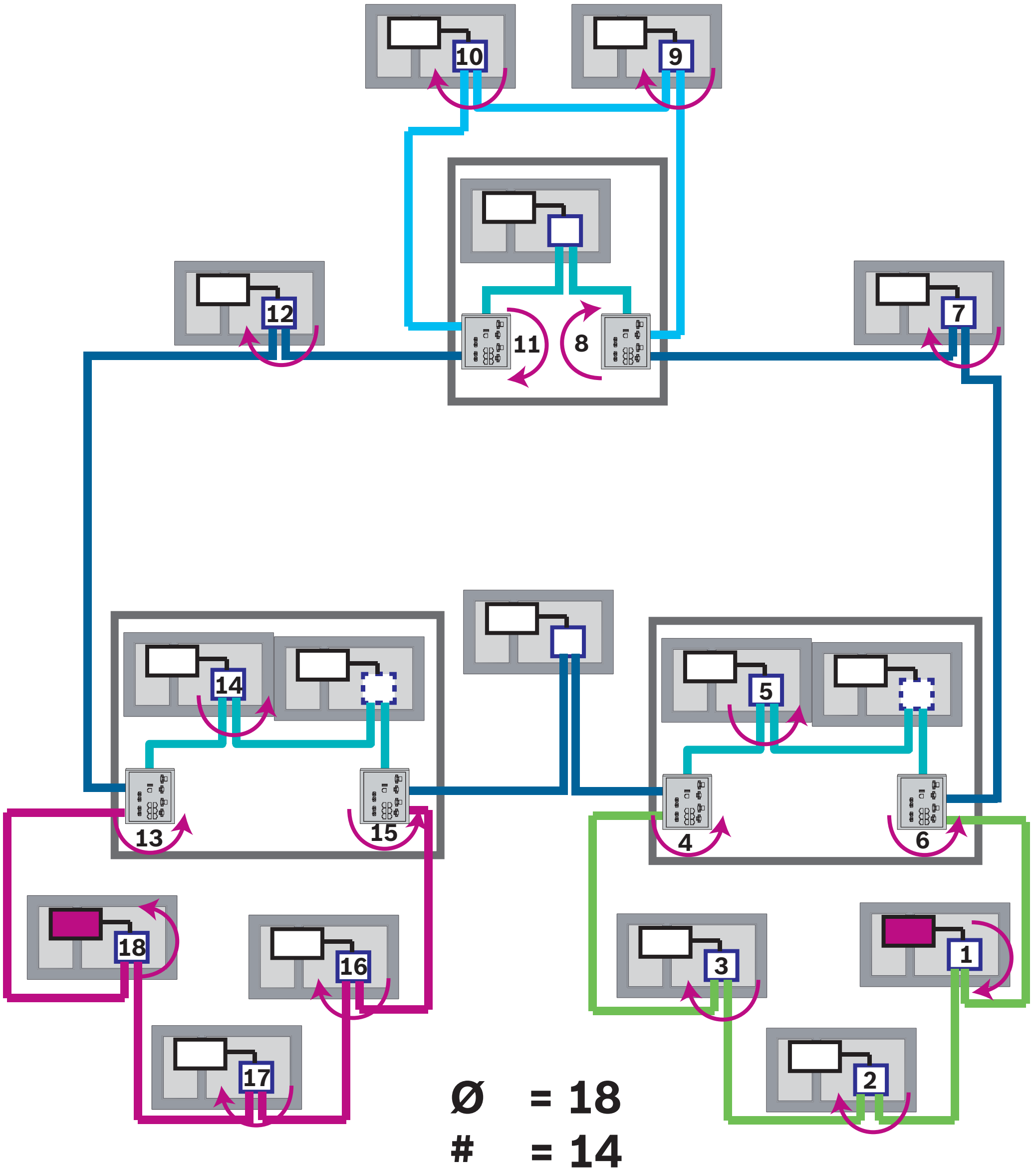


Figure 5.3: Network diameter of a backbone with sub-loops

The figure shows, for the diameter you have to find the longest path.

5.3 Cables used

Use only the following cables for networking. The usage of other cables is not conform to the safety standards in the EC directives.

- Ethernet cable
  Ethernet patch cable, shielded, CAT 5e or better.
  Note the minimum bending radii specified in the cable specification.
- Fiber optic cable
  Multi-mode: fiber optic Ethernet patch cable, duplex I-VH2G 50/125µ or duplex I-VH2G 62.5/125µ, SC plug.
  Single mode: fiber optic Ethernet patch cable, duplex I-VH2E 9/125µ, SC plug.
  Note the minimum bending radii specified in the cable specification.

Notice!
TX cable length
All IP connections must be direct or via media converters approved by Bosch. The node to node TX cable length must be less than 100 m.

Notice!
VdS 2540
To meet the requirements of VdS 2540 for data transmission paths use fiber optic cable for Ethernet connections. For connections within a housing you can use TX Ethernet cables.

5.4 Creating or modifying an Ethernet network

There are several procedures for creating an Ethernet network of fire alarm control panels. The 2 procedures described below differ in the size of the networks and the number of installation and configuration tasks carried out alongside each other.

Rules for using 4 Ethernet ports

If your panel has 4 Ethernet ports, apply the following rules in the given order. Bosch supports networks, which are built according to the following rules, only.

1. For panel networking you have to use ETH1 and ETH2. An external RSTP switch on ETH1 or ETH2 must only be used for panel networking.
2. For connecting an OPC, an FSM-5000-FSI, a Praesideo/PAVIRO, an UGM-2040 you have to use ETH3. You may connect an external RSTP switch, which must not be used for panel networking.
3. For Remote Services you have to use ETH4. If no connection to Remote Services is required, then ETH4 can be used for connecting an OPC, an FSM-5000-FSI, a Praesideo/PAVIRO, or an UGM-2040.
4. If there is no panel networking via ETH1 and ETH2, then each can be used for connecting an OPC, an FSM-5000-FSI, a Praesideo/PAVIRO, or an UGM-2040.

Creating an Ethernet network (smaller projects)

This procedure is suitable for projects involving only a small number of engineers working on the installation of the fire alarm system concurrently.

1. Plan out the network.
2. Create the network in FSP-5000-RPS and configure the network settings.
3. Print the network information out for safe keeping, or store the information on the laptop.
4. Install the control panels and network cables and connect them to a network.
5. Configure the network settings for the individual control panels directly at the control unit as per the printout.
6. Reset each of the control panels in the network in order to activate the network configuration.
7. Connect your computer with the FSP-5000-RPS programming software to a control panel in the network. Load this configuration to all other control panels across the network via this control panel. Redundant panels use the main panel configuration.
8. Carry out a reset in order to reset the pending error messages. Rectify any errors.

Configure the network settings on the control panels first. This gives you the advantage that you can program the other control panels in the network from one control panel.

Creating an Ethernet network (medium-sized and large projects)

This procedure is suitable for projects involving a number of tasks carried out concurrently by several teams. As many tasks performed during installation and configuration involve restarting the fire alarm control panel, the network is not started up in this procedure until a later stage.

1. Plan out the network.
2. Produce a configuration of the network without peripherals with FSP-5000-RPS.
3. Print the network information out for safe keeping, or store the information on the laptop.
4. Install the network cables and check individual sections or loops.
5. Install the panels and commission them as stand-alone panels.
6. Install the peripherals in the panels.
7. Configure each of the panels with FSP-5000-RPS.
8. Ensure that the individual panels are working correctly.
9. Commission the individual loops of the network one after the other, according to the topology.
   Start with the backbone.
   - Produce a configuration for the backbone in FSP-5000-RPS. Import all of the necessary panel configurations. Configure the network settings and print them out.
   - Connect all panels to a network.
   - Configure the network settings for the individual control panels directly at the panel controller as per the printout.
   - Reset each of the control panels in order to load the network configuration.
   - Ping the neighboring panels in order to check the network.
   - Commission the entire backbone and rectify any errors.

   Commission the sub-loops as per the example of the backbone.

Add a panel to a network

1. Change the network configuration in FSP-5000-RPS.
2. Print the network information out for safe keeping, or store the information on the laptop.
3. Install the control panel and network cables and connect them to the network.
4. Configure the network settings for the individual control panel directly at the control unit as per the printout.
5. Reset the panel and adjoining panels in order to activate the network configuration.

Remove a panel from the network

1. Change the network configuration in FSP-5000-RPS.
2. Print the network information out for safe keeping, or store the information on the laptop.
3. Configure the network settings for the adjoining control panels directly at the control unit as per the printout.
4. Shut off the panel, and the power supply (mains and battery) before removing it from the network.
5. Reset the adjoining panels in order to activate the network configuration.

6 CAN network

Loop topology

In loop topology, the CAN cable is always routed from a CAN1 terminal to a CAN2 terminal [CAN1 ⇒ CAN2]. The cable length depends on the cable cross-section.

CAN connection

The CAN connection is a two-wire connection (CAN-H and CAN-L). Connect CAN-H to CAN-H and connect CAN-L to CAN-L for a two-wire connection. A three-wire connection (CAN-H, CAN-L and CAN-GND) may be necessary in exceptional cases, e.g. with a high EMC load or a significant difference in grounding potential. Connect CAN-H to CAN-H, CAN-L to CAN-L and CAN-GND to CAN-GND for a three-wire connection. The shield wire of the CAN cable is only connected to the metal housing of the panel on one side.

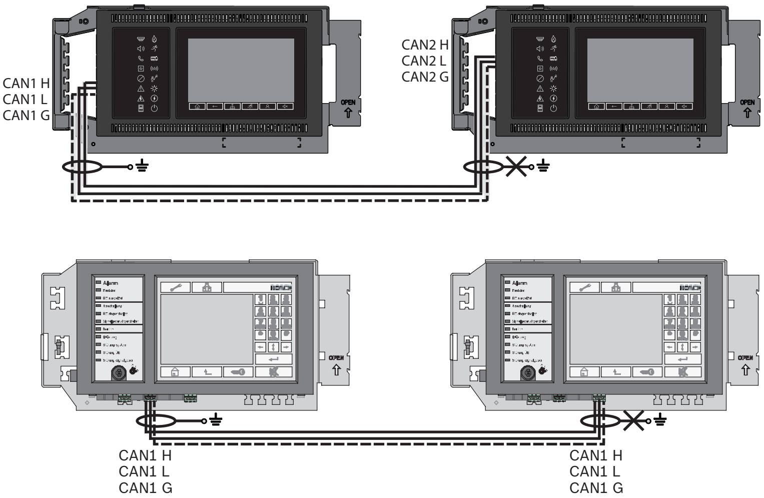


Figure 6.1: CAN connection (top: AVENAR, bottom: FPA)

Cable length for networking

The maximum permitted cable length depends on the loop resistance of the cable used and on the number of communicating.

Example: The J-Y (St) Y 2 x 2 x 0,8 mm red fire detector cable enables two nodes with a maximum distance of around 800 m to be connected.

Notice!

The distance between two nodes in loop topology can be determined by reading off the value at two nodes in the diagram.

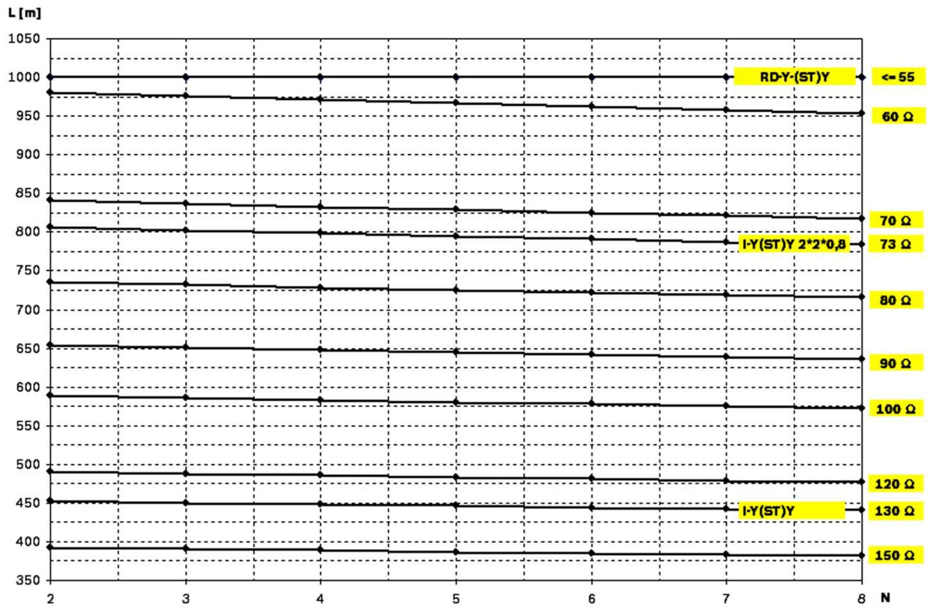


Figure 6.2: CAN network: Achievable cable length, depending on the number of nodes and the cable resistance

L = cable length in meters

N = number of nodes

6.1 Creating or modifying a CAN network

This procedure is suitable for projects involving only a small number of engineers working on the installation of the fire alarm system concurrently.

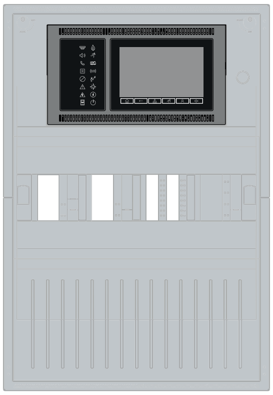
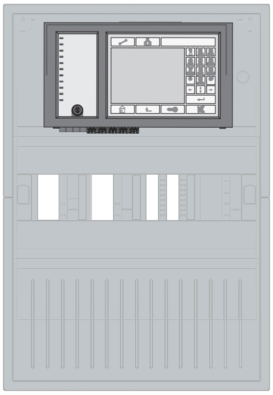
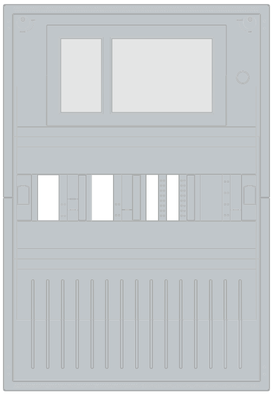
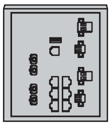
Procedure for creating a CAN network

1. Plan out the network.
2. Create the network in FSP-5000-RPS.
3. Print the network information out for safe keeping, or store the information on the laptop.
4. Install the control panels and connect them with CAN cables to a network.
5. Connect your computer with the FSP-5000-RPS programming software to a control panel in the network. Load this configuration to all other control panels across the network via this control panel. Redundant panels use the configuration of the main panel.
6. Carry out a reset in order to reset the pending error messages. Rectify any errors.

7 Ethernet and CAN networking pattern

For building up panel networks corresponding to the introduced topologies and connecting services, you need the networking pattern described in this document.

Icon	Description
▬ ▬	TX Ethernet cable (copper), node to node TX cable length < 100 m
▬ ▬	FX Ethernet cable (fiber optic cable)
▬▬▬▬▬▬▬▬	TX or FX Ethernet cable, node to node TX cable length < 100 m

Icon	Description
━━━━━━━━	CAN cable
– – – – – – –	Housing Note: In order to simplify the overview of various networking patterns, the figures in this chapter show always a small panel housing for symbolizing a panel. This small housing does **not** provide in all presented cases sufficient space to mount the displayed switches, media converters and gateways. Use the Safety Systems Designer to ensure, that you order the correct amount and the correct size of housings to install the equipment.
	AVENAR panel
	FPA
	AVENAR panel or FPA
	Ethernet switch as external RSTP switch (in general Ethernet switch MM)

Icon	Description
	Media converter
	Secure network gateway for Remote Services
IP	Connection to OPC server, FSM-5000-FSI, Praesideo/PAVIRO or UGM-2040

7.1 Panel network over Ethernet

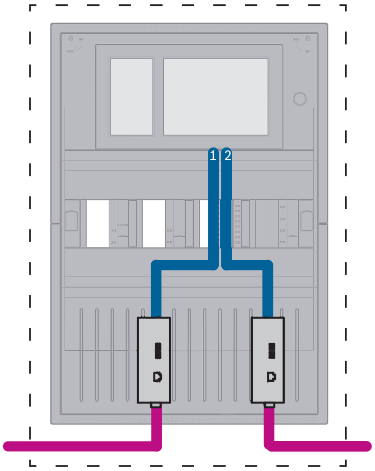


Figure 7.1: Panel network over Ethernet

For ranges greater than 100 m the range extension with media converters is mandatory. For ranges less than 100 m the media converters might not be required.

7.2 Panel network over CAN

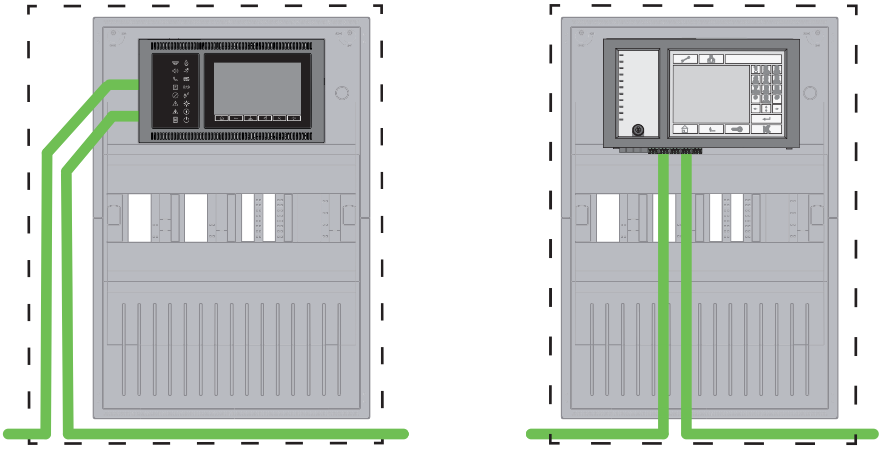


Figure 7.2: Panel network over CAN

7.3 Connect services to panel

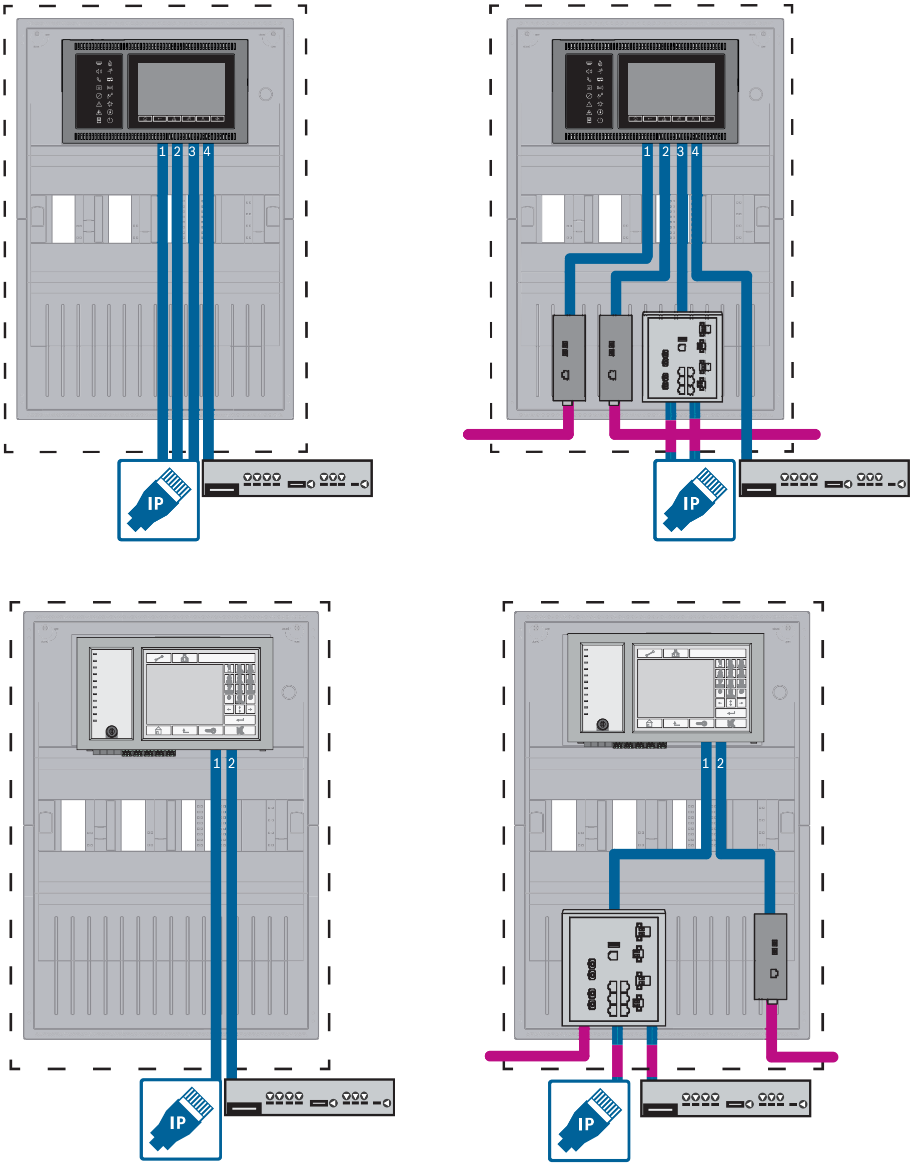


Figure 7.3: Left side: without panel network, Right side: with panel network

For ranges greater than 100 m the range extension with media converters is mandatory. For ranges less than 100 m the media converters might not be required.

7.4 Panel network over Ethernet with redundant panels

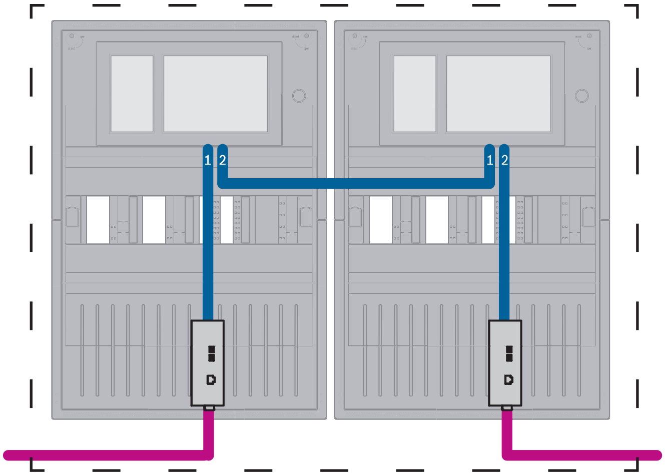


Figure 7.4: Panel network over Ethernet with redundant panels

For ranges greater than 100 m the range extension with media converters is mandatory. For ranges less than 100 m the media converters might not be required.

7.5 Panel network over CAN with redundant panels

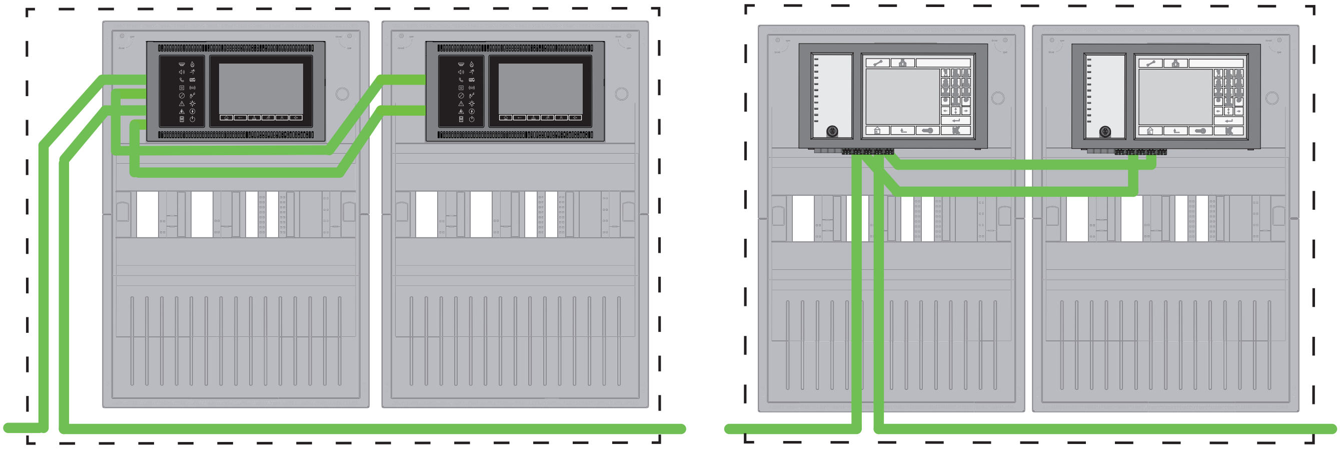


Figure 7.5: Panel network over CAN with redundant panels

7.6 Panel network over two Ethernet loops

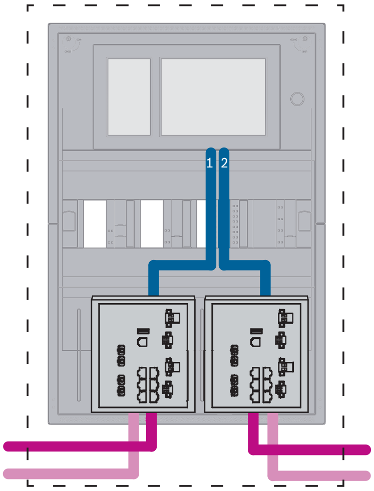


Figure 7.6: Connect Ethernet networks

7.7 Panel network over two Ethernet loops with redundant panels

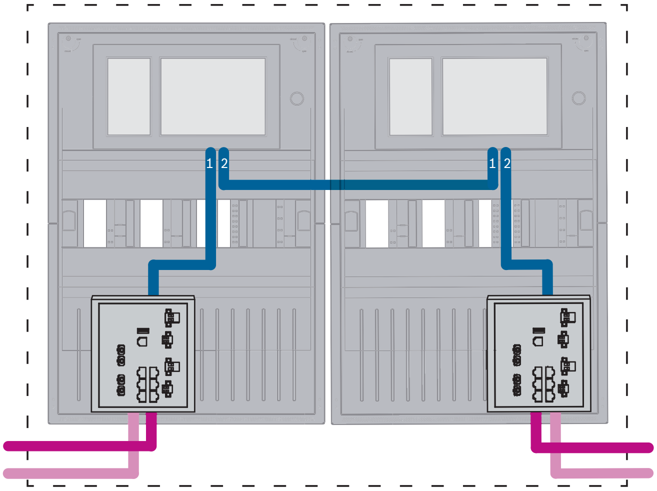


Figure 7.7: Connect Ethernet networks with redundant panels

7.8 Connect Ethernet and CAN network with redundant panels

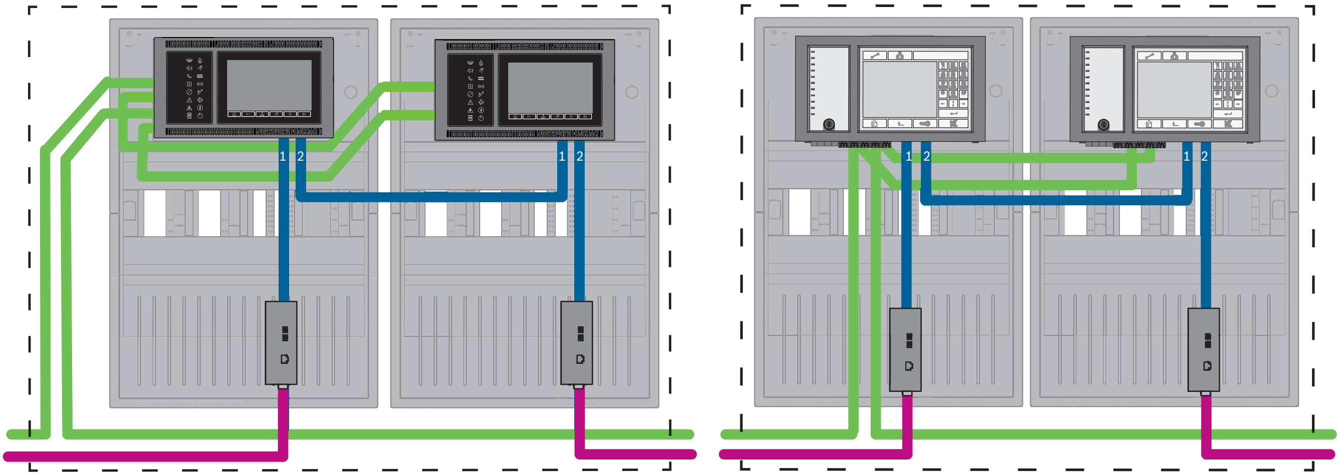


Figure 7.8: Connect Ethernet and CAN network with redundant panels

For ranges greater than 100 m the range extension with media converters is mandatory. For ranges less than 100 m the media converters might not be required.

7.9 Connect remote services to redundant panels

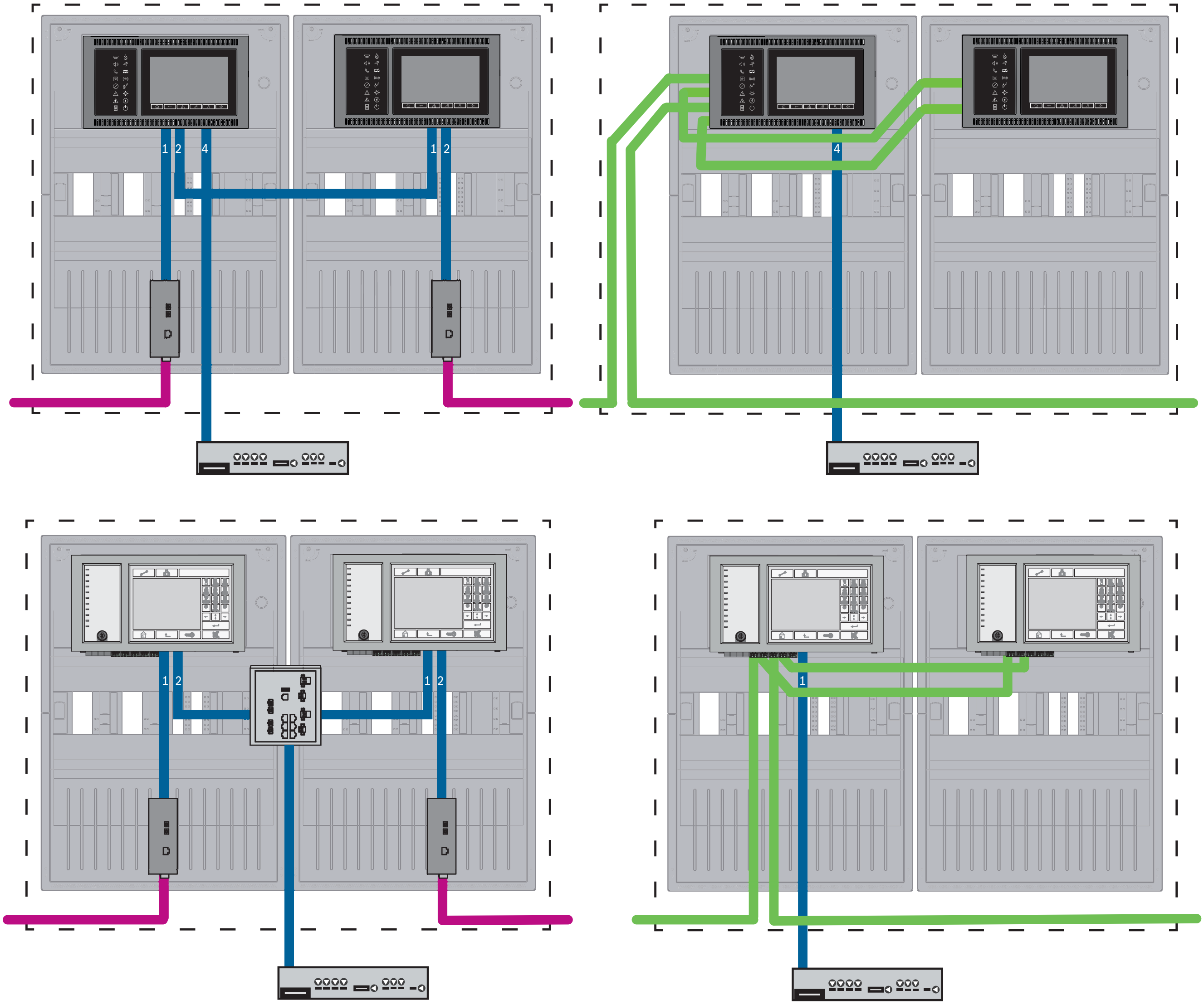


Figure 7.9: Left side: in Ethernet network Right side: in CAN network

For ranges greater than 100 m the range extension with media converters is mandatory. For ranges less than 100 m the media converters might not be required.

8 Remote Services

The following services belong to Remote Services:

- Remote Connect
- Remote Alert
- Remote Maintenance

Prerequisite for Remote Alert and Remote Maintenance is Remote Connect.

8.1 Remote Connect

Remote Connect provides a trusted and secure internet connection, which enables remote access to a panel via FSP-5000-RPS. Remote Connect is the basis for all Remote Services. For Remote Connect use the Secure network gateway.
In case of a panel network, one panel of the panel network has to be connected to a Secure network gateway. Exclusively this connection, needs to be a dedicated Ethernet connection.

Notice!
While Remote Connect supports connection to a panel network via Ethernet or CAN, Remote Alert and Remote Maintenance functionality is only supported when Ethernet networking between panels is provided and configured for service usage.

Remote Connect has to be enabled in the FSP-5000-RPS configuration of this panel.
The following topology shows panel controllers connected via Ethernet where a Secure network gateway is connected to the network via an Ethernet switch (in general MM).

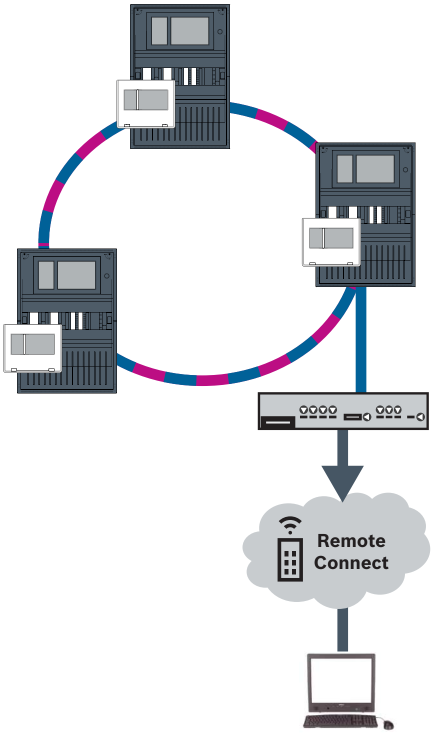


Figure 8.1: Remote Connect in an Ethernet loop

Notice!
To connect panels via FX, use media converters approved by Bosch.

To prevent sending EN 54-2 relevant multicast traffic to the router, use the Ethernet switch (in general MM, BPA-ESWEX-RSR20) approved with panel version 2.8. Activate IGMP snooping of the Ethernet switch, see the corresponding section in the Installation chapter of the Networking guide.

Notice!
The internet router (or the company network which provides internet access) as well as the Secure network gateway must provide separated sub-networks. Panels of the panel network may not be placed in the sub-network of the internet router. Also overlapping of the sub-networks is not possible.
In case of overlapping sub-networks you have to separate the sub-networks by changing the IP addresses on panel network side.
Additionally you have to propagate the changes to the Secure network gateway. To do so, launch the web interface via a web browser:
- Address: https://192.168.1.254
- User name: bosch
- Password: ipti83
Under **Configuration** -> **Network (LAN)** you can change the IP address. Consider, that the **Default gateway:** address in the panel controller configuration must match the IP address of the Secure network gateway.

Notice!
In accordance with DIBt guidelines, remote resetting is not permitted via Remote Services to restore the operational readiness of door control systems with motorized opening assistance.

The following topology shows a CAN network where a Secure network gateway is connected to the network via Ethernet port.

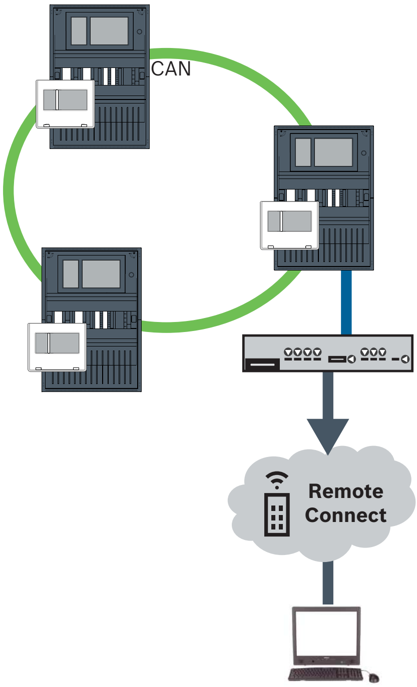


Figure 8.2: Remote Connect in a CAN loop

8.2 Remote Alert

Through Remote Alert, a panel pushes relevant status information to the Remote Portal. Transferred data are analyzed with Remote Alert. In case of an unexpected event, the user will be informed via SMS and/or E-Mail about the received alerts.
Remote Alert is also available for Private Secure Network.

8.3 Remote Maintenance

Remote Maintenance offers the possibility to remotely monitor certain parameters of various security items connected to a fire panel. Via the Remote Portal, you can conduct walk tests.

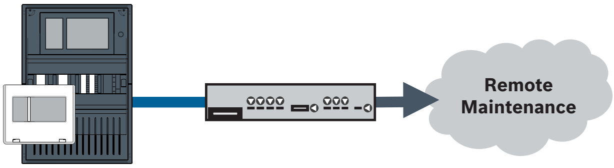


Figure 8.3: Remote Maintenance

Notice!
Ethernet connections used only to transfer Remote Maintenance data may be realized as Ethernet or fiber optic cables. Note the permitted maximum cable lengths.

Notice!
To connect panels via FX, use media converters approved by Bosch.

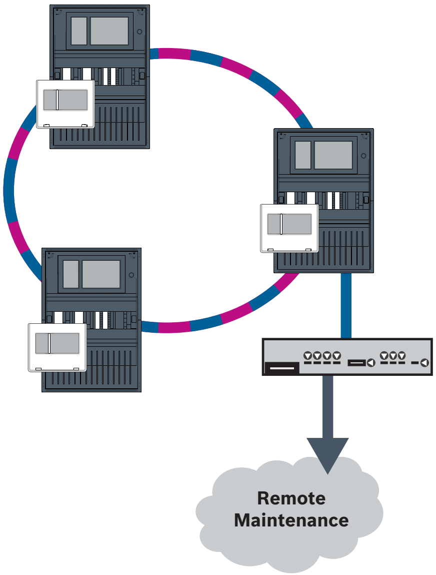


Figure 8.4: Remote Maintenance

When using Remote Maintenance with Ethernet networks, one panel in the network must be connected to the router for data transfer purposes. All collected data is transfered from the network via this connection.

Remote Maintenance for Remote Portal

Remote Maintenance collects data of relevant LSN devices and functional modules and sends them to the Remote Portal where they are analyzed and visualized for maintenance activities.

Remote Maintenance for Private Secure Network

Remote Maintenance can be configured for Private Secure Network: Collected data will be sent to a central management server system (CMS).

Caution!

Remote Services require a secure IP connection. Bosch Remote Services or connection with Private Secure Network is required.
With Private Secure Network an IP network is provided, which is based on DSL with an optional wireless access on the panel side (EffiLink). Remote Services for Private Secure Network is only available in Germany with a service agreement with Bosch BT-IE.

Notice!

To connect panels via FX, use media converters approved by Bosch.

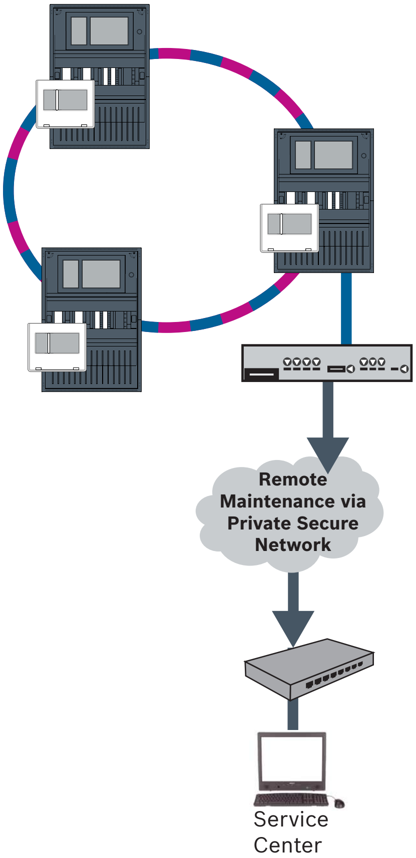


Figure 8.5: Remote Maintenance for Private Secure Network

For Remote Maintenance, you must enter the server IP address and port of the Remote Maintenance system server in the FSP-5000-RPS programming software.
Assign a unique Panel Network ID to the network.

Switch for connecting the CMS must be programmed separately

Program the IP address and redundancy settings of the switch, see *Settings on switch, page 43*. As the switch is installed in the immediate vicinity (without intermediate space), the power supply does not have to be designed redundantly and the fault outputs are therefore not used.
Make sure that the RSTP settings in the panel controllers, in FSP-5000-RPS and in Ethernet switch are identical.

8.4 Remote Portal

Requirements

Notice!
To avoid reconfigurations or adjustments when using Remote Services, ensure that the following requirements are met:
- panel with firmware 2.19.7 or higher, all panels connected via Ethernet, Ethernet interfaces enabled and standard Ethernet settings
- Remote Connect enabled in the FSP-5000-RPS panel configuration
- Secure network gateway for Remote Services available
- computer with FSP-5000-RPS 4.8 or higher installed and internet access

Notice!
Avoid update of Secure network gateway during connection.
Updates of the Secure network gateway run regularly in the early morning hours. Thus, specify the time zone under **System** -> **General Settings** -> **Timezone**.

Instructions
For using Remote Services you must be user of a Remote Portal account.

Step 1: Create a Remote Portal account
You can have multiple users under one Remote Portal account. Each Remote Portal account has one unique Remote ID, which is meant to represent one company. If you cannot use an existing Remote Portal account, you have to create one:

1. On https://remote.boschsecurity.com -> **Sign Up** enter your name, your company and your email address and create a password. Observe the terms and conditions and select **I agree to the terms and conditions**. Also observe the privacy statement and select **I agree to the privacy statement**.
2. Click **Register**.
   The Remote Portal promptly sends an email to the provided address containing an activation link.
3. For activating the account click the activation link. On the Remote Portal click your user name and select **Account Settings**. Here you find your Remote ID. You will need this Remote ID at the panel controller later.

To give each of your technicians an own account you can create several users for the same Remote ID:
You are logged in to the Remote Portal.

- Select **Users** -> **New Technician**. Then enter the required data and confirm with **Save**.

Step 2: Connect Secure network gateway
For establishing Remote Services use a Secure network gateway.

1. Connect the WAN port of the Secure network gateway to the internet router or to the company network which provides the internet access.
2. On the internet router or company network check the availability of the following protocols and ports, to the Secure network gateway (required for connection to Remote Services).

Protocol	Default port	Description
HTTP	80 and 8080	for Remote Connect registration and Remote Maintenance

Protocol	Default port	Description
IPsec VPN	UDP 500 and UDP 4500	for Remote Connect

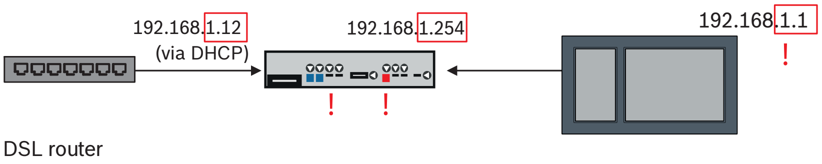
3. Connect the LAN1 port of the Secure network gateway to the designated Ethernet port of the panel controller using the supplied CAT5 RJ45 network cable. Observe the possible topologies.
4. Connect the Secure network gateway to a 100 V - 230 V mains supply using the supplied power supply.

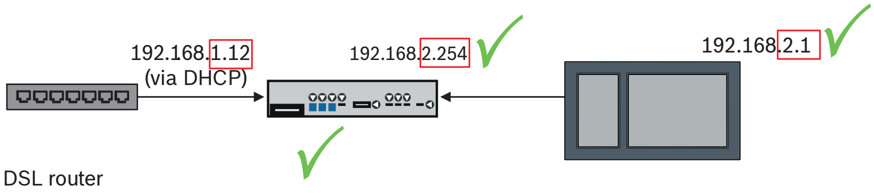
WAN LED on (blue), when the connection to the internet has been established. VPN LED on (blue) shortly after, which indicates that a VPN connection to the Remote Portal has been established.

Each connected panel or panel network has one unique System ID.

Separating sub-networks (VPN LED off)

Connecting the Secure network gateway for Remote Services fails in case of overlapping sub-networks (VPN LED off). The following example shows a Secure network gateway and a panel controller in the same address range as the DSL router.





A Secure network gateway detects overlapping sub-networks unambiguously: The Alarm LED is blinking continuously.

Separating the sub-networks is done by changing the third octet of the IP address. You change the IP addresses on panel network side. After changing the IP address you have to propagate the changes to the Secure network gateway. To do so, launch the web interface via a web browser:

- Address: https://192.168.1.254
- User name: bosch
- Password: ipti83

Under **Configuration** -> **Network (LAN)** you can change the IP address. Consider, that the **Default gateway:** address in the panel controller configuration must match the IP address of the Secure network gateway.

Step 3: Establish remote connection

1. At the panel use standard Ethernet settings.
2. Restart the panel.

3. For authentication select **Configuration** -> **Network Services** -> **Change date / time**, enter the current date, and confirm your settings.
4. Select **Configuration** -> **Network Services** -> **Remote Services**, and enter the Remote ID.

You can check the status of the remote connection: Select **Diagnostics** -> **Network Services** -> **Remote Services** at the panel controller.

Step 4: Assign license in the Remote Portal

To activate the usage of the Remote Services you have to assign a license in the Remote Portal. One license is automatically supplied to your account with the first successful connection.

Notice!
An already assigned license cannot be reassigned or suspended.

1. On https://remote.boschsecurity.com -> **Login** enter your email address and your password.
2. Select **Systems**.
3. Select the system.
4. Under **Services** click the **Add Service** button underneath the service.
5. As a default the license will automatically renewed (**Service Settings**, option **With Auto-Renew**).
6. Click **Save** to confirm your settings.

After assigning the license you can use the corresponding service. An assigned license is shown by a green hook.

Step 5: Reorder license

1. Order one-year licenses from Bosch Fire Alarm Systems. Each network requires its own licenses.
   Bosch sends an email to the address provided. The email includes unique license registration numbers for the quantity of licenses ordered, as well as instructions and a link to the Remote Portal.
2. On https://remote.boschsecurity.com -> **Login** enter your email address and your password.
3. Select **Licenses**.
4. Click the **+** button.
5. Follow the instructions given in the **Add Licenses** window and confirm with **Save**.
6. The list of licenses is updated.

9 Voice alarm systems

The following topology shows panel controllers connected via Ethernet where the Praesideo/ PAVIRO system is integrated in the panel loop using an Ethernet interface.

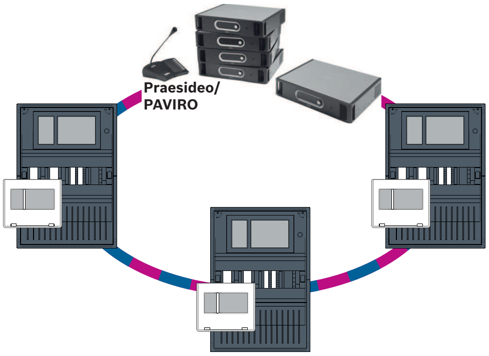


Figure 9.1: Ethernet loop with Praesideo/PAVIRO

Use the Ethernet Switch (in general MM BPA-ESWEX-RSR20) approved with panel firmware version 2.8.

To prevent sending EN 54-2 relevant multicast traffic to the Praesideo/PAVIRO system, activate IGMP snooping of the MM, see the corresponding section in the Installation chapter of the Networking Guide.

In every panel controller of a CAN network you can connect one Praesideo/PAVIRO system using an Ethernet interface. The following topology shows panel controllers connected via CAN where the Praesideo/PAVIRO system is connected to one panel controller using an Ethernet interface.

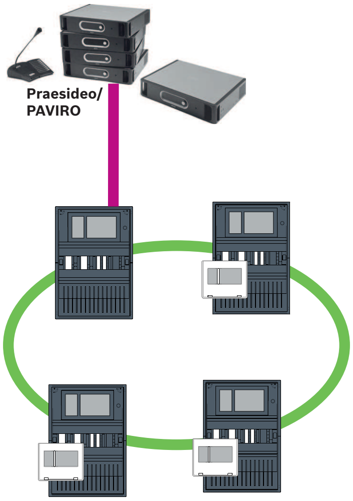


Figure 9.2: Praesideo/PAVIRO connection to a CAN network

Notice!

Because CAN network traffic shall not be transferred through the Ethernet connection, you must switch off networking over IP in the FSP-5000-RPS programming software.

If this is not switched off, the network will not be compliant with EN 54.

Notice!

If an MPC-xxxx-B panel controller shall be used for the direct connection to a Praesideo/PAVIRO system a cross-over patch cable is required as neither Praesideo/PAVIRO nor the MPC-xxxx-B supports Auto-MDI(X).

10 Installation

Checklist

Before starting with the installation of the network, please review all of the points set out below.

- Ethernet and CAN
  - The requisite line lengths of the Ethernet TX, Ethernet FX and CAN TX and CAN FX cables are less than their maximum length.
  - The entire peripherals and their cabling in the individual panels are planned.
- Network planning
  - All IP addresses and network settings for the individual panels and additional network components are planned and at your disposal.
  - An overview of the additional components to be installed, such as Ethernet switches and media converters, and their cabling with neighboring panels is at your disposal.
  - An overview of the network topology to be installed is at your disposal.
  - All network redundancy settings have been planned and are at your disposal.

10.1 Settings on media converter

Only a few steps are required to use the media converter:

- Set the DIP switches.
- Connect the media converter to the FX network cables and CAT5e network cables.
- Supply the media converter with power via the internal BCM battery controller module.

Notice!
The media converters are only supplied with power via power supply terminal 1.
The error LED on the media converter is therefore continuously lit. However, this does not affect the functionality of the device.

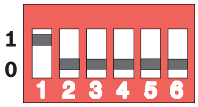
Notice!
Use only the following cables for networking:
Ethernet cable
Ethernet patch cable, shielded, CAT5e or better.
Note the minimum bending radii specified in the cable specification.
Fiber optic cable
Multi-mode: fiber optic Ethernet patch cable, duplex I-VH2G 50/125μ or duplex I-VH2G 62.5/125μ, SC plug.
Single mode: fiber optic Ethernet patch cable, duplex I-VH2E 9/125μ
Note the minimum bending radii specified in the cable specification.

Notice!
Refer to the installation guides for the mounting kits for information on how to install a media converter in the housing of a panel: FPM 5000 KMC (F.01U.266.845) FPM-5000-KES (F.01U.266.844)

Notice!
The maximum transmission section for multimode media converters via FX is 2000 m.
The maximum transmission section for single mode media converters via FX is 40 km.

Using the DIP switches, configure the media converter as shown in the following figure.

Notice!
Only change the DIP switch settings on media converters when they are de-energized.



DIP switch number	Setting
1	Link Fault Pass-Through activated
2	Ethernet: automatic mode
3	Ethernet: 100 MBit
4	Ethernet: fully duplex
5	Fiber optic cable: fully duplex
6	Link down: off

10.2 Installing Ethernet switch

Warning!
Laser light
Do not look directly into the beam with the naked eye or with visual instruments of any kind (e.g. magnifying glass, microscope). Failure to observe this notice poses a danger to the eyes at a distance of less than 100 mm. The light emerges at the visual terminals or at the end of the fiber optic cables connected to these. CLASS 2M laser diode, wavelength 650 nm, output < 2 mW, in accordance with IEC 60825-1.

Notice!
Refer to: Installation guide for the Mounting kit for Ethernet switch FPM-5000-KES (F.01U.260.523).

10.3 Settings on switch

In order to be able to use the switches in the network, you need to program them.
Connect your laptop to the network and use the HiDiscovery software supplied by the manufacturer to carry out the initial programming of the switches. Using this software, search for the switches in the network. Double-click on a switch to select it and assign an IP address to it.
Following the initial programming of the IP address, you can use a web browser to call up the configuration user interface for the switch.

Notice!
Refer to the manufacturer's user guide for an exact description of the installation and configuration of the switches. Access data:
User: admin
Password: private

Use a browser to call up the configuration user interface for the switches.
You must perform the following settings in the switch:
- *Assign IP address, page 44*,
- *Program redundancy settings, page 44*.

Furthermore, optional settings e. g.:
- *Programming the fault relay, page 45*,
- *Programming connection monitoring, page 45*,

- *Activating IGMP snooping, page 46*.

10.3.1 Assign IP address

Notice!
Practical tip:
In the device part of IP addresses, use numbers greater than 200 (xxx.xxx.xxx.200) for switches, if your network configuration allows this. This will give you a clearer separation from the host identifier of an IP address.
Example:
Switch 192.168.1.201 is assigned to the panel with the IP address 192.168.1.1.

Notice!
Please refer to the following manufacturer documents for an exact description of the installation and configuration of the switches:
Installation user guide
Web-based interface reference guide

Use a browser to go to the configuration user interface for the switch.
In the **Basic Settings -> Network** menu, set the following values depending on the topology chosen:
- Mode: local
- IP address: the required IP address, e.g. 192.168.1.201
- Network screen: the required network screen, e.g. 255.255.255.0
- Gateway: the required gateway, e.g. 192.168.1.254, or 0.0.0.0 if no gateway is required

Click on **Write**.

Notice!
The settings in the individual menu items in the switch configuration take effect after clicking on **Write**.
The settings are only saved permanently, i.e. so that they are retained even after the device is restarted, if under **Basic Settings -> Load/Save** in the **Save** field you select the item **On the device** and click on the **Save** button.

10.3.2 Program redundancy settings

As the FPA panel networks use RSTP as the redundancy protocol, you must activate and program the protocol in the configuration user interface:
In the **Redundancy -> Spanning Tree -> Global** menu, set the following values:
- Function: On
- Protocol version: RSTP
- Protocol configuration: Same settings as for the panel controllers

Click on **Write**.

Notice!
The settings in the individual menu items in the switch configuration take effect after clicking on **Write**.
The settings are only saved permanently, i.e. so that they are retained even after the device is restarted, if under **Basic Settings -> Load/Save** in the **Save** field you select the item **On the device** and click on the **Save** button.

10.3.3 Programming the fault relay

Notice!
The fault relay only has to be programmed for applications where at least one of the following requirements is met:
There is a connection between 2 switches. This is possible in the case of a backbone with sub-loops, for example.
The power supply to the switch is designed redundantly.

Notice!
Please refer to the following manufacturer documents for an exact description of the installation and configuration of the switches:
Installation user guide
Web-based interface reference guide

Use a browser to go to the configuration user interface for the switch.
Under **Diagnosis -> Signal Contact** in the **Signal Contact 1** tab, set the **Signal Contact Mode** to **Device Status**.
Under **Diagnosis -> Device Status** in the **Monitoring** field, set the following values:

- **Power Supply 1**: **Monitor**
- **Connection Error**: **Monitor**

All other settings must be set to **Ignore**.

Notice!
The settings in **Device Status** also apply to the fault LED of the switch.

Click on **Write**.

Notice!
The settings in the individual menu items in the switch configuration take effect after clicking on **Write**.
The settings are only saved permanently, i.e. so that they are retained even after the device is restarted, if under **Basic Settings -> Load/Save** in the **Save** field you select the item **On the device** and click on the **Save** button.

10.3.4 Programming connection monitoring

Notice!
You only need the setting for the connection monitoring if you are using the fault relay of the switch.

If you want to use the fault relay to monitor the connections of the switch, then you must specify in the switch configuration which ports of the switch should be monitored.
Activate the **Forward Connection Error** check box for the individual ports in the **Basic Settings -> Port Configuration** menu.
Only connections for which **Forward Connection Errors** has been activated are monitored.
Click on **Write**.

Notice!
The settings in the individual menu items in the switch configuration take effect after clicking on **Write**.
The settings are only saved permanently, i.e. so that they are retained even after the device is restarted, if under **Basic Settings -> Load/Save** in the **Save** field you select the item **On the device** and click on the **Save** button.

10.3.5 QoS priority, only for UGM-2040

If you use the switches for communication between FPA networks and the UGM-2040, then the QoS priority must be set in the switches of the UGM.
In the QoS/Priorität -> Global menu, change the settings of the drop-down list field under Trusted Mode to trustIpDscp.
Click on **Write**.

Notice!
The settings in the individual menu items in the switch configuration take effect after clicking on **Write**.
The settings are only saved permanently, i.e. so that they are retained even after the device is restarted, if under **Basic Settings -> Load/Save** in the **Save** field you select the item **On the device** and click on the **Save** button.

10.3.6 Activating IGMP snooping

To prevent sending EN 54-2 relevant multicast traffic to other systems connected to the Ethernet Switch (Praesideo/PAVIRO, Remote Connect) activate IGMP snooping.
On the IGMP configuration page of the Ethernet Switch select the following options:

1. Switch on the **IGMP** snooping operation.
2. Activate the **IGMP Querier**.
3. Configure the transmission interval, in which the RSR20 sends IGMP query packets (e.g. 4 seconds).
4. Configure the time within multicast group members are supposed to respond to IGMP queries (e.g. 3 seconds).
5. Select **Discard** for packets with unknown multicast addresses.
6. Select **Send to Query and registered Ports** for packets with known multicast addresses.
7. Enable IGMP only for ports where other systems connected to the switch are connected. Disable the **Static Query Port** option for all ports.

10.4 CAN network

Networking and interfaces

The panel controller has

- two CAN interfaces (CAN1/CAN2) for networking (loop or stub topology)
- two signal inputs (IN1/IN2)
- two Ethernet interfaces
- USB interface

Depending on panel controller type:

- two more Ethernet interfaces
- RS232 interface

Note the maximum cable length of 3 m for connection to the USB interface or 2 m for connection to the RS232 interface.

Addressing and settings in the network

Depending on panel controller type:

- Physical node address set in the panel firmware, when switching on the panel for the first time
- RSN on mechanical rotary switches on the rear of the panel

To show the physical node address, if it is saved in the panel controller:

- ▸ Select **Configuration** -> **Network services** -> **Ethernet** -> **Use Ethernet settings** -> **IP settings** -> **Default settings**

To change the physical node address, saved in the panel controller:

- ▸ Show the default settings and change the last number of **IP address**.

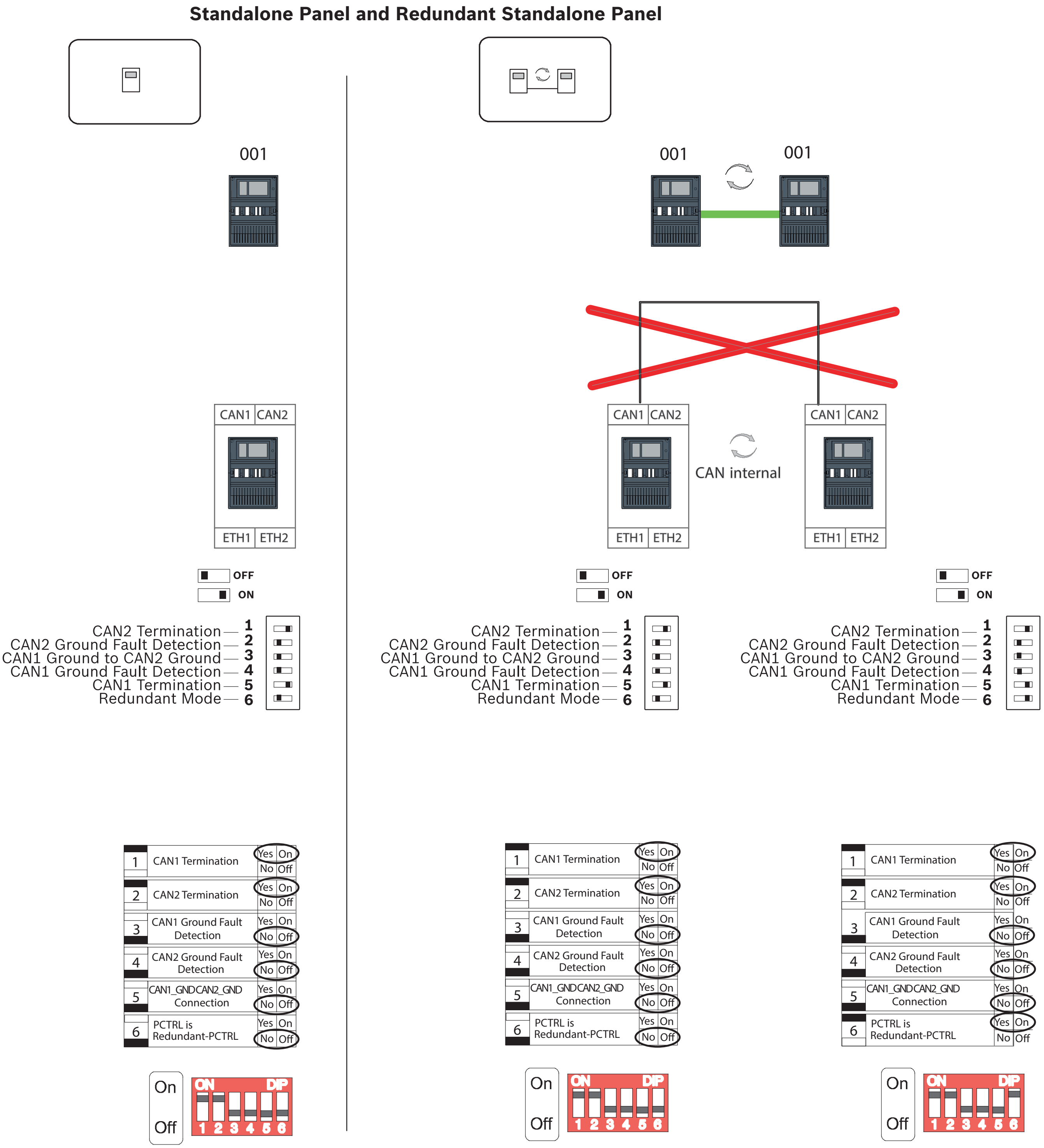
To change a mechanical RSN:

- ▸ On mechanical rotary switches on the rear of the panel set the RSN with, and note it on the sign below the rotary switches.

Configuration of the topology

The DIP switches for the configuration of different topologies are located on the rear.

- ▸ Mark the selected setting on the sign near to the DIP switches.


Standalone Panel and Redundant Standalone Panel
001
001
001
CAN internal
CAN1
CAN2
ETH1
ETH2
OFF
ON
CAN2 Termination — 1
CAN2 Ground Fault Detection — 2
CAN1 Ground to CAN2 Ground — 3
CAN1 Ground Fault Detection — 4
CAN1 Termination — 5
Redundant Mode — 6
On
Off
ON
DIP
1 2 3 4 5 6

Left (regular):

1	CAN1 Termination	[✓ Yes On] No Off
2	CAN2 Termination	[✓ Yes On] No Off
3	CAN1 Ground Fault Detection	Yes On [✓ No Off]
4	CAN2 Ground Fault Detection	Yes On [✓ No Off]
5	CAN1_GNDCAN2_GND Connection	Yes On [✓ No Off]
6	PCTRL is Redundant-PCTRL	Yes On [✓ No Off]

Middle (redundant):

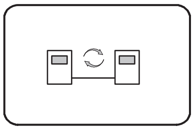
1	CAN1 Termination	[✓ Yes On] No Off
2	CAN2 Termination	[✓ Yes On] No Off
3	CAN1 Ground Fault Detection	Yes On [✓ No Off]
4	CAN2 Ground Fault Detection	Yes On [✓ No Off]
5	CAN1_GNDCAN2_GND Connection	Yes On [✓ No Off]
6	PCTRL is Redundant-PCTRL	Yes On [✓ No Off]

Right (redundant):

1	CAN1 Termination	[✓ Yes On] No Off
2	CAN2 Termination	[✓ Yes On] No Off
3	CAN1 Ground Fault Detection	Yes On [✓ No Off]
4	CAN2 Ground Fault Detection	Yes On [✓ No Off]
5	CAN1_GNDCAN2_GND Connection	Yes On [✓ No Off]
6	PCTRL is Redundant-PCTRL	[✓ Yes On] No Off

Figure 10.1: DIP switch settings for standalone panel (top: AVENAR, bottom: FPA, left: regular, right: redundant)

Remote keypad as redundant panel



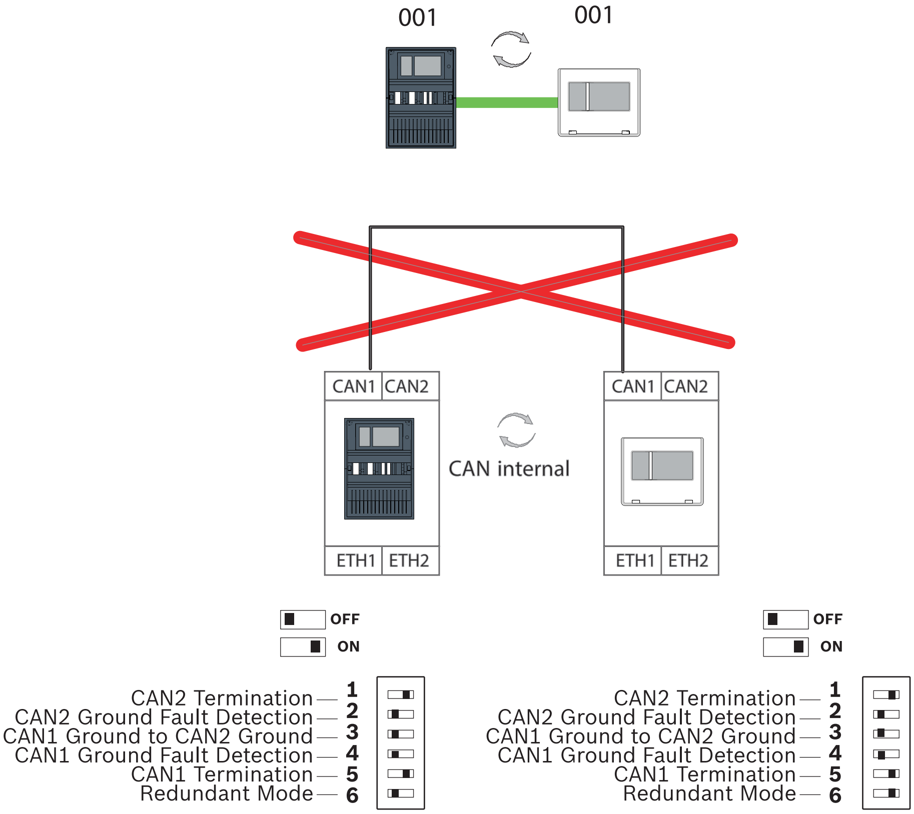
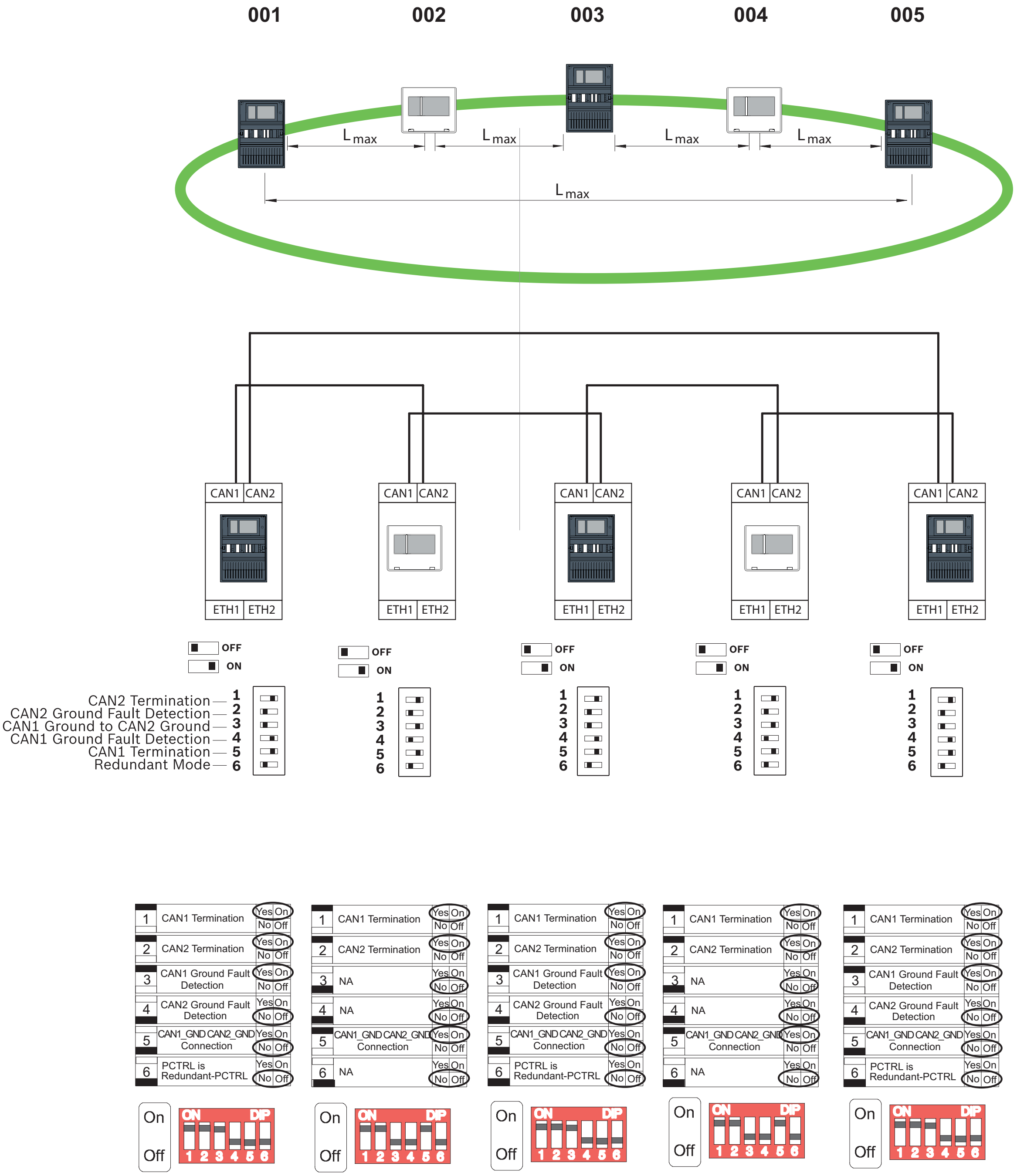

001
001
CAN1
CAN2
CAN internal
CAN1
CAN2
ETH1
ETH2
ETH1
ETH2
OFF
ON
CAN2 Termination 1
CAN2 Ground Fault Detection 2
CAN1 Ground to CAN2 Ground 3
CAN1 Ground Fault Detection 4
CAN1 Termination 5
Redundant Mode 6
OFF
ON
CAN2 Termination 1
CAN2 Ground Fault Detection 2
CAN1 Ground to CAN2 Ground 3
CAN1 Ground Fault Detection 4
CAN1 Termination 5
Redundant Mode 6

Figure 10.2: DIP switch settings for remote keypad as redundant panel (AVENAR only)

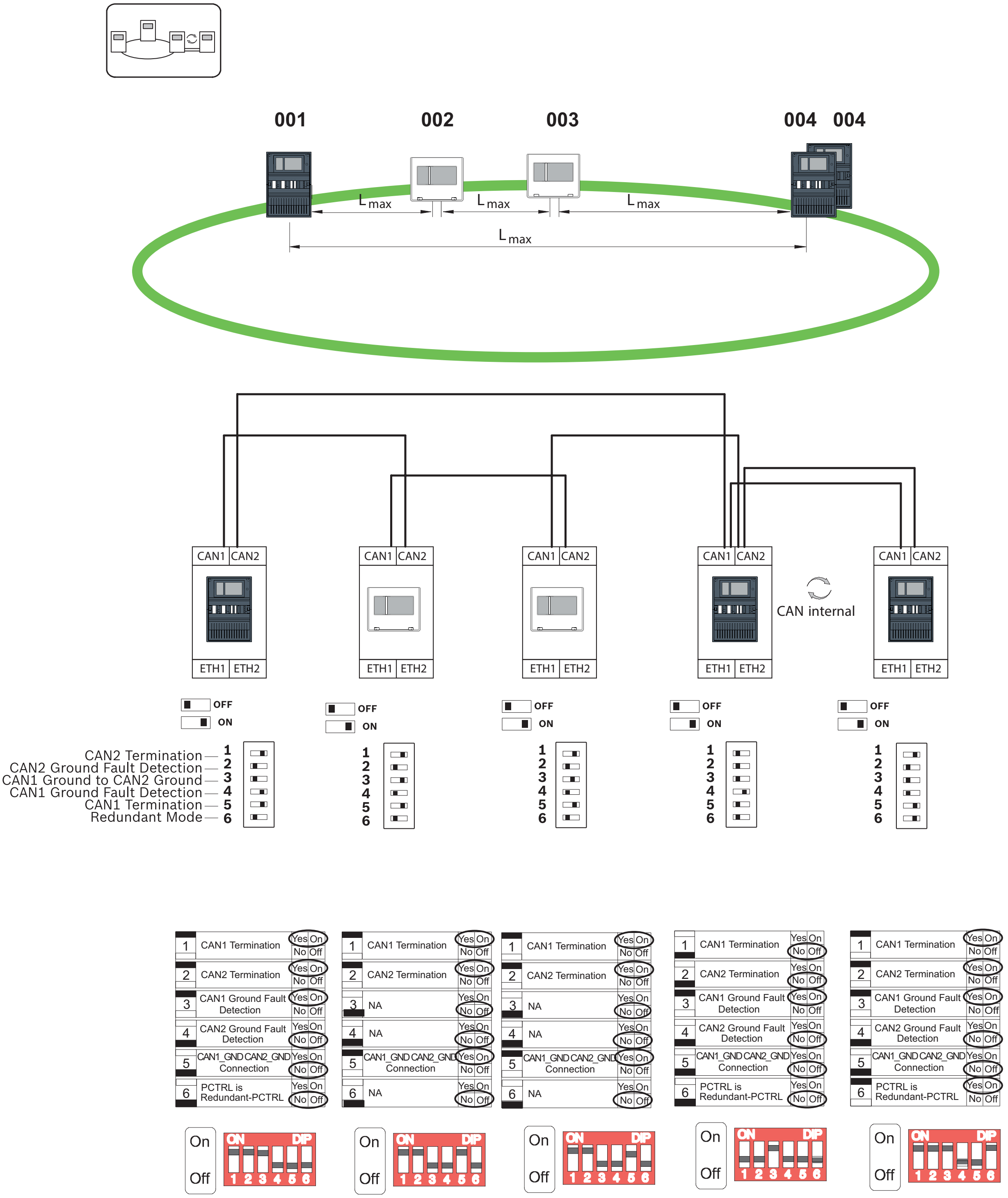
Loop



		001	002	003	004	005
1	CAN1 Termination	[✓ Yes On] No Off	[✓ Yes On] No Off	[✓ Yes On] No Off	[✓ Yes On] No Off	[✓ Yes On] No Off
2	CAN2 Termination	[✓ Yes On] No Off	[✓ Yes On] No Off	[✓ Yes On] No Off	[✓ Yes On] No Off	[✓ Yes On] No Off
3	CAN1 Ground Fault Detection / NA	CAN1 Ground Fault Detection: [✓ Yes On] No Off	NA: Yes On [✓ No Off]	CAN1 Ground Fault Detection: [✓ Yes On] No Off	NA: Yes On [✓ No Off]	CAN1 Ground Fault Detection: [✓ Yes On] No Off
4	CAN2 Ground Fault Detection / NA	CAN2 Ground Fault Detection: Yes On [✓ No Off]	NA: Yes On [✓ No Off]	CAN2 Ground Fault Detection: Yes On [✓ No Off]	NA: Yes On [✓ No Off]	CAN2 Ground Fault Detection: Yes On [✓ No Off]
5	CAN1_GND CAN2_GND Connection	Yes On [✓ No Off]	[✓ Yes On] No Off	Yes On [✓ No Off]	[✓ Yes On] No Off	Yes On [✓ No Off]
6	PCTRL is Redundant-PCTRL / NA	PCTRL is Redundant-PCTRL: Yes On [✓ No Off]	NA: Yes On [✓ No Off]	PCTRL is Redundant-PCTRL: Yes On [✓ No Off]	NA: Yes On [✓ No Off]	PCTRL is Redundant-PCTRL: Yes On [✓ No Off]

Figure 10.3: DIP switch settings for loop (top: AVENAR, bottom: FPA)

Loop with redundant panels



1	CAN1 Termination	[✓ Yes On] No Off
2	CAN2 Termination	[✓ Yes On] No Off
3	CAN1 Ground Fault Detection	[✓ Yes On] No Off
4	CAN2 Ground Fault Detection	Yes On [✓ No Off]
5	CAN1_GND CAN2_GND Connection	Yes On [✓ No Off]
6	PCTRL is Redundant-PCTRL	Yes On [✓ No Off]

1	CAN1 Termination	[✓ Yes On] No Off
2	CAN2 Termination	[✓ Yes On] No Off
3	NA	Yes On [✓ No Off]
4	NA	Yes On [✓ No Off]
5	CAN1_GND CAN2_GND Connection	[✓ Yes On] No Off
6	NA	Yes On [✓ No Off]

1	CAN1 Termination	[✓ Yes On] No Off
2	CAN2 Termination	[✓ Yes On] No Off
3	NA	Yes On [✓ No Off]
4	NA	Yes On [✓ No Off]
5	CAN1_GND CAN2_GND Connection	[✓ Yes On] No Off
6	NA	Yes On [✓ No Off]

1	CAN1 Termination	Yes On [✓ No Off]
2	CAN2 Termination	Yes On [✓ No Off]
3	CAN1 Ground Fault Detection	[✓ Yes On] No Off
4	CAN2 Ground Fault Detection	Yes On [✓ No Off]
5	CAN1_GND CAN2_GND Connection	Yes On [✓ No Off]
6	PCTRL is Redundant-PCTRL	Yes On [✓ No Off]

1	CAN1 Termination	[✓ Yes On] No Off
2	CAN2 Termination	[✓ Yes On] No Off
3	CAN1 Ground Fault Detection	[✓ Yes On] No Off
4	CAN2 Ground Fault Detection	Yes On [✓ No Off]
5	CAN1_GND CAN2_GND Connection	Yes On [✓ No Off]
6	PCTRL is Redundant-PCTRL	[✓ Yes On] No Off

Figure 10.4: DIP switch settings for loop with redundant panels (top: AVENAR, bottom: FPA)

Loop with remote keypad as redundant panel

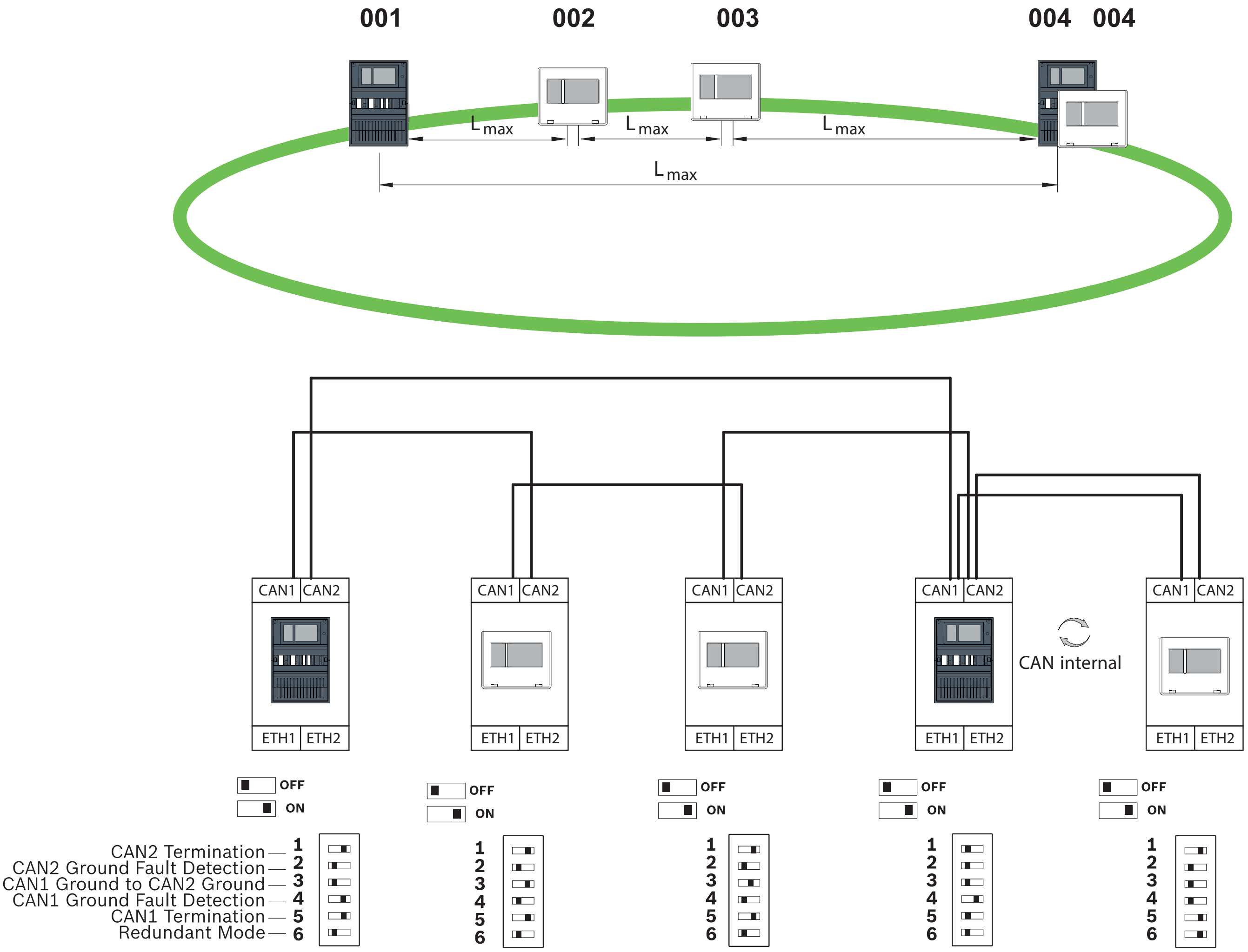


Figure 10.5: DIP switch settings for loop with remote keypad (AVENAR only)

11 Cabling

To create an EN 54-2-compliant system, connect the RSTP switches and the media converters via the monitored power supply of the fire alarm control panel.

- For the power supply to the media converters and to the RSTP switches use the 24 V output of either the BCM 0000 B or FPP-5000.
- If you have connected a redundant power supply or are creating a switch-to-switch connection, then the fault outputs of the RSTP switch must be monitored via panel inputs. For example, use the inputs on the panel controller or IOP 0008 A.
- In the case of the media converter, the Link Fault Pass-Through function must be activated. Configuration is performed via the DIP switch of the media converter.

Notice!
Use only the following cables for networking:
Ethernet cable
Ethernet patch cable, shielded, CAT5e or better.
Please note the minimum bending radii specified in the cable specification.
Fiber optic cable
Multi-mode: fiber optic Ethernet patch cable, duplex I-VH2G 50/125µ or duplex I-VH2G 62.5/125µ, SC plug.
Single mode: fiber optic Ethernet patch cable, duplex I-VH2E 9/125µ, SC plug.
Please note the minimum bending radii specified in the cable specification.

11.1 Media converter

Connection of media converters

Notice!
Note the direction of transmission of the FOC fibers when connecting the FX cabling of the media converters.

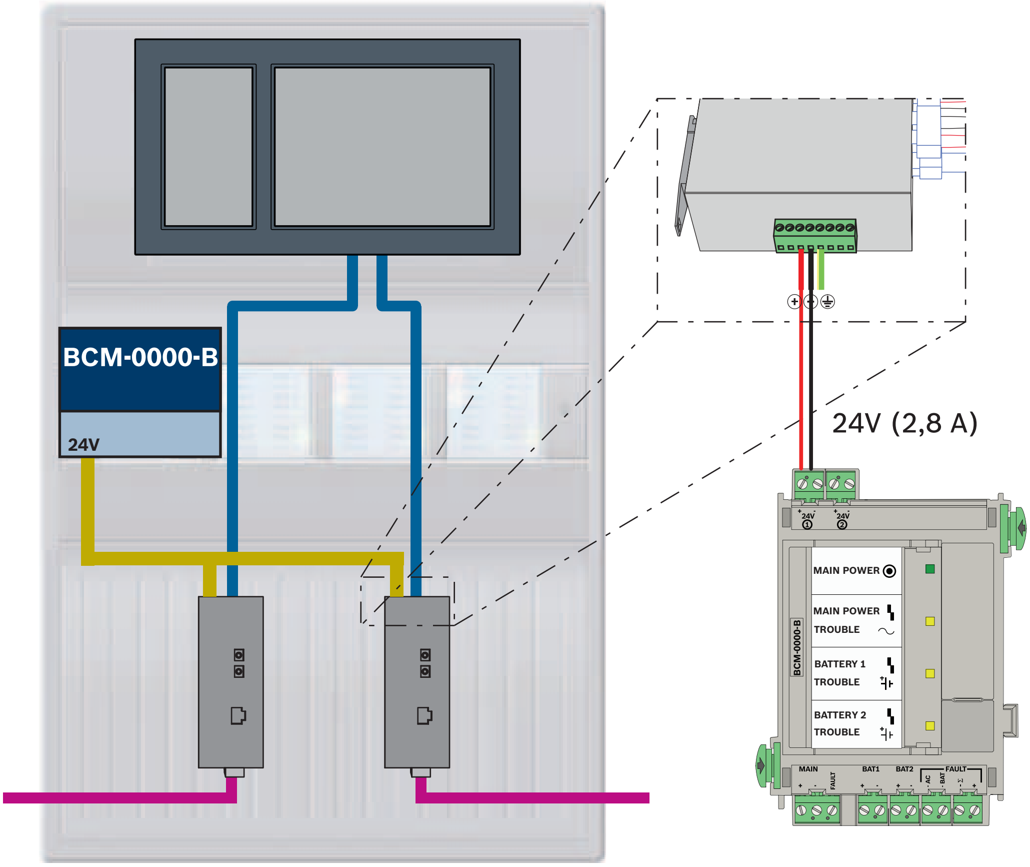
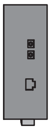


Figure 11.1: Connection of media converter to power supply and to panel controller IN1/IN2

Icon	Description
▬ ▬	TX Ethernet cable (copper)
▬ ▬	FX Ethernet cable (fiber optic cable)
▬	24 V power supply

Icon	Description
▬	Transmission of fault
	Media converter

11.2 Ethernet switch

Connection of switch

You can connect the fault outputs of the switches to the inputs of the panel controller or an IOP input and output module.

Notice!

The fault relay only has to be connected for applications where at least one of the following requirements is met:

There is a connection between 2 switches. This is possible in the case of a backbone with sub-loops, for example.

The power supply to the switch is designed redundantly.

Connection of switches with reporting of faults to the inputs of the IOP module:

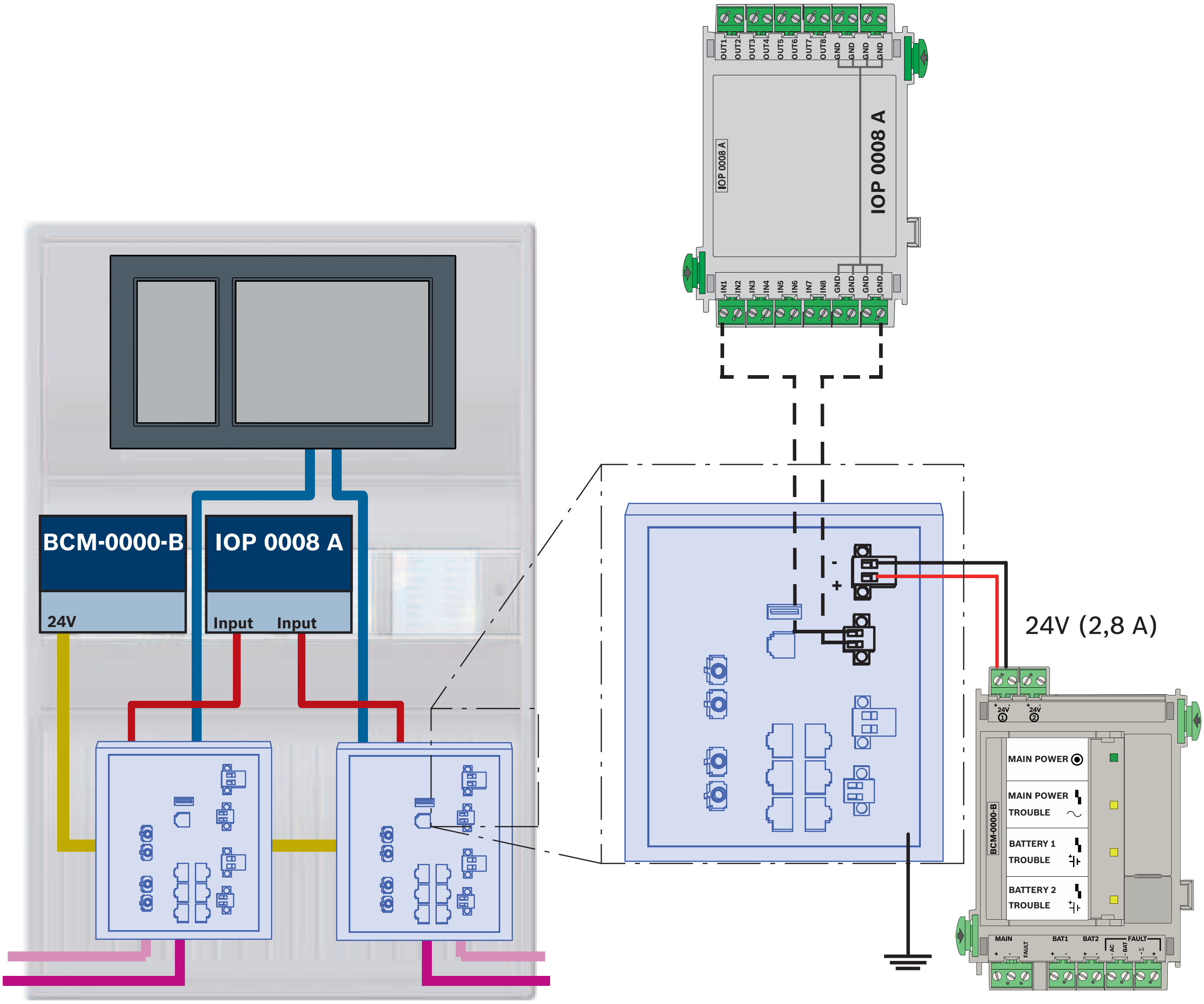
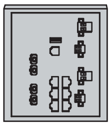


Figure 11.2: Connection of switch to the power supply and IOP

Icon	Description
🟦 🟦	TX Ethernet cable (copper)
🟪 🟪	FX Ethernet cable (fiber optic cable)
🟨	24 V power supply
🟥	Transmission of fault
	RSTP switch

Connection of switches with reporting of faults to the panel controller inputs

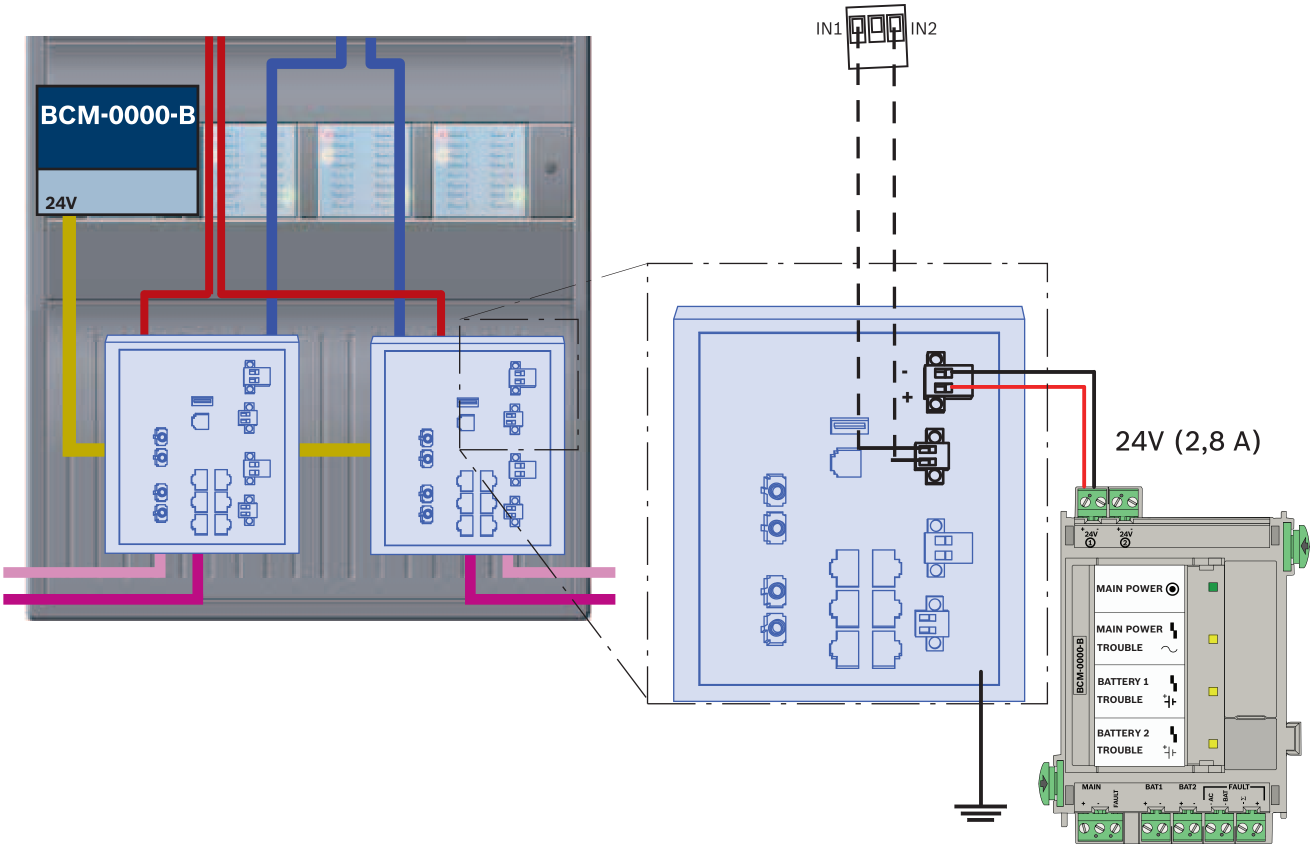
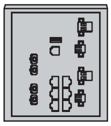


Figure 11.3: Connection of switch to the power supply and to the panel controller

Icon	Description
🟦 🟦	TX Ethernet cable (copper)
🟪 🟪	FX Ethernet cable (fiber optic cable)
🟨	24 V power supply
🟥	Transmission of fault
	RSTP switch

Notice!

Do not use the supplied network cable to connect the switches.
Use an Ethernet patch cable, shielded, CAT5e or better.

11.3 Remote keypad

A remote keypad must be supplied with power via an FPP-5000 External power supply. Connection to the network is established via 2 media converters in a PSS 0002 A or USF 0000 A.

Notice!
Note that the FPP-5000 External power supply and the PSF 0002 A (PSS 0002 A) must be installed in the immediate vicinity (without intermediate space) of the remote keypad. It must not be possible to touch the connecting cables between the components, as they are not monitored for creeping short circuit and creeping open monitoring.

Notice!
Use only media converters to connect a Remote keypad to an Ethernet panel network. The use of switches is not permitted for the Remote keypad.

Notice!
The functional earth of the Remote keypad must always be placed in position when connecting the unit to an Ethernet panel network.

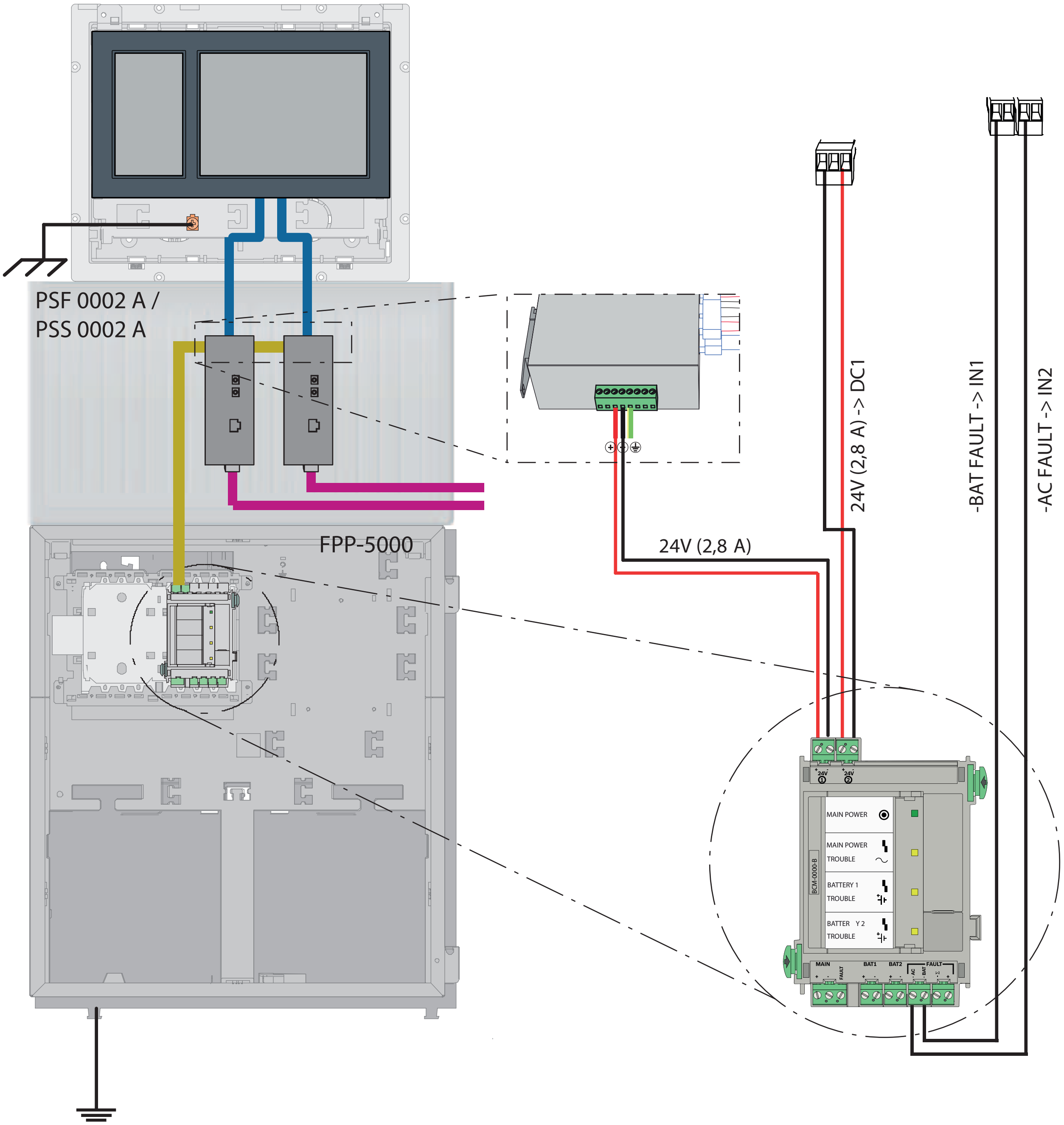
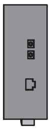


Figure 11.4: Cabling of Remote keypad

Icon	Description
🟦 🟦	TX Ethernet cable (copper)
🟪 🟪	FX Ethernet cable (fiber optic cable)
🟨	24 V power supply
	Media converter

12 FSP-5000-RPS settings

You can program the entire network with the RPS programming software via the USB port, network interface or the serial interface of a panel. To do this, you must have configured the network settings on the panel and restarted these in order to commission the network. Alternatively, you can also use the network interface of a switch that is connected to the network.

12.1 Network nodes

You must program the entire network with all network nodes in the FSP-5000-RPS programming software and upload this to the network. To do so, proceed as follows:

- Connect the FPA nodes
  - Set the RSN at the individual nodes
- Adjust the line numbers of the network cabling so that you create the planned topology
- Check the topology display to make sure that the topology is correct
- Where necessary, connect the OPC server, the Praesideo/PAVIRO system, UGM-2040 server and switches
- Edit the Ethernet and IP configuration
  - Assign the IP addresses or use the standard settings if using a topology with fewer than 20 RSTP switches
  - Choose the appropriate redundancy protocol for the set topology
- Perform a consistency check
- Connect to the network via Ethernet, USB or the serial interface
- Complete a multiple login
- Carry out a complete auto-detection for each panel
- Request the configuration information and complete all tasks

Check the error messages after the restart of the network and rectify any errors where necessary.

12.2 Line numbers

You must assign a line number to each connection to the network used. It is irrelevant whether this is a CAN connection or an Ethernet connection.

It is possible to use one line number for both a CAN connection and an Ethernet connection. However, to get a better overview of the connections, you should use different number ranges. Consider, that if you use **Network** as **Line Type** in the **Net interface** window, then the line number must be 0 for all connections.

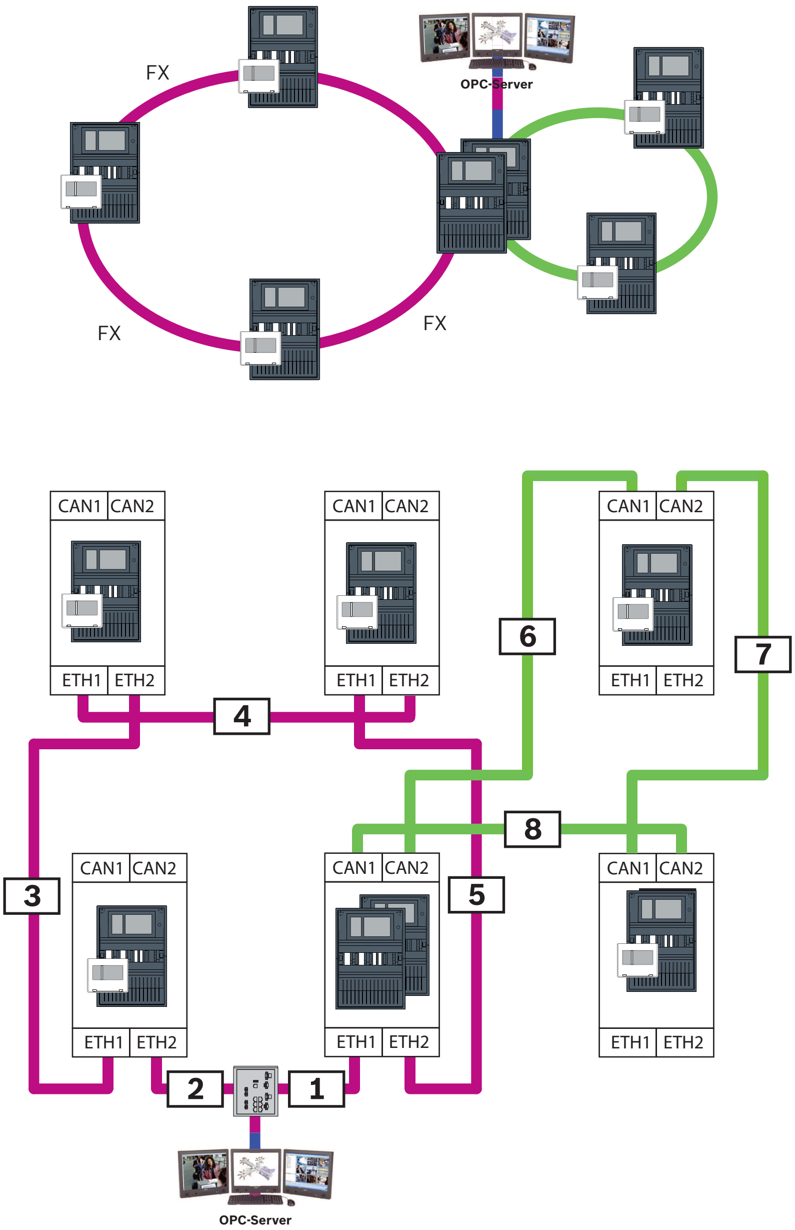


Figure 12.1: Example of a network and the possible line numbering

12.3 Switches

If you are using switches in your network, you must create these switches in the FSP-5000-RPS programming software. You can assign up to 128 ports to each created switch. In order to create your network, you can assign the connected line numbers to the individual ports.

12.4 OPC servers

OPC servers in your network must be added to the FSP-5000-RPS programming software. You must perform the following settings in both the FSP-5000-RPS software and on the OPC server:

- Network nodes
- Network group
- RSN
- IP address
- Port

The OPC server uses port 25000 as standard.

Notice!
EN 54
The connection of a building management system (e.g. BIS) via an Ethernet interface using an OPC server or an FSI server is EN54 compliant if the EN54 relevant functions are performed by the fire panel solely. Any EN54 relevant control or administration (e.g. control of notification appliances or administration of switch-off) by the building management system requires an individual EN54 certification of the overall system by a certification body.

Notice!
FSP-5000-RPS programming software
You must assign an OPC server to each network node from which statuses should be transmitted.

12.5 UGM-2040 servers

Notice!
All panel controllers and UGM servers must be located in the same subnetwork and have the same multicast address.
In the case of multiple panel configurations or networks, these must be located in the same subnetwork. The multicast addresses must be different.

Notice!
You must assign the UGM-2040 server to each network node from which statuses should be transmitted.

In order to connect a panel to the UGM-2040, you must simulate the physical structure of the network in RPS. This also includes the line numbers between the connecting panel controller and the switches of the UGM-2040.

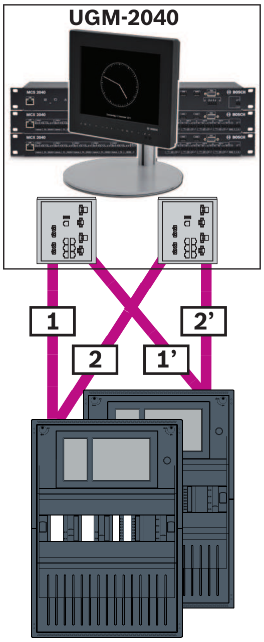


Figure 12.2: Example of line numbering for the UGM-2040

13 Appendix

13.1 Ethernet error messages

Please note that in the event of an error, the error message plus the group error is displayed in each instance.

Physical address	Logical address	Error message	Description and possible cause
Group faults relating to general network malfunction			
135.0.1.0	Network 1.0	**General Network Trouble**	There is an incompatible version of the panel network software. There are 2 different software versions
Group faults relating to network			
135.0.6.1	Network 2.1	**Duplicate IP Address**	An IP address has been assigned twice.
135.0.6.2	Network 2.2	**IP Settings**	The IP configuration of the reporting panel is different to the RPS configuration
135.0.6.3	Network 2.3	**Redundancy Settings**	The redundancy configuration (RSTP, RSTP parameter, dual homing or nothing) of the reporting panel is different to the RPS configuration.
Group faults relating to Rapid Spanning Tree Protocol (RSTP)			
135.0.7.1	Network 3.1	**RSTP Fallback**	The reporting panel has switched from RSTP mode to STP mode (compatibility mode). A STP device has been connected to the network.
135.0.7.2	Network 3.2	**RSTP Topology Change**	The RSTP network topology has changed. For example, another RSTP device has been added to the network. This message may also arise in the event of an interruption to the line.
135.0.7.3	Network 3.3	**RSTP Link Type Point2Point**	An RSTP port of the reporting panel is not in the point-2-point status. Several RSTP devices have been connected to an RSTP port, for example. Or another RSTP device has been connected to the RSTP port via a half-duplex line.
Group faults relating to network connection			
135.0.5.1	Network connection 1.0	**CAN 1 Trouble**	Data transmission to CAN bus 1 is restricted. Possible causes include: cable breaks, cable not connected, cable interference.
135.0.5.2	Network connection 2.0	**CAN 2 Trouble**	Data transmission to CAN bus 2 is restricted. Possible causes include: cable breaks, cable not connected, cable interference.
135.0.5.3	Network connection 3.0	**Ethernet 1 Trouble**	Data transmission to Ethernet line 1 is restricted. Possible causes include: cable breaks, cable not connected, cable interference.

Physical address	Logical address	Error message	Description and possible cause
135.0.5.4	Network connection 4.0	**Ethernet 2 Trouble**	Data transmission to Ethernet line 2 is restricted. Possible causes include: cable breaks, cable not connected, cable interference.

Index

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com