



# Modular Fire Panel

FPA-5000



**BOSCH**

en

Networking Guide



## Table of contents

<b>1</b>	<b>Safety instructions</b>	<b>5</b>
<b>2</b>	<b>Introduction</b>	<b>6</b>
<b>3</b>	<b>Ethernet networking</b>	<b>7</b>
3.1	Procedure	7
3.1.1	Standard procedure for smaller projects	7
3.1.2	Medium-sized and large projects	7
3.2	Overview of the network	8
3.2.1	Protocols	8
3.2.2	Network diameter	8
3.2.3	Cables used	10
3.2.4	Extension of existing networks	10
3.2.5	Ethernet/IP communication	11
3.3	Topologies	12
3.3.1	Key	14
3.3.2	Ethernet loop	16
3.3.3	Ethernet loop with OPC server	17
3.3.4	Ethernet loop with OPC server to redundant panel controller	18
3.3.5	Ethernet/CAN double loop	19
3.3.6	Ethernet backbone with sub-loops (Ethernet/CAN)	20
3.3.7	Connecting Ethernet loops	22
3.4	UGM-2040 networks	23
3.5	Voice alarm system over IP	24
3.6	Condition Monitoring	24
3.7	Teleservice EffiLink	26
3.8	Remote connect	26
<b>4</b>	<b>CAN networking</b>	<b>29</b>
4.1	Connection to voice alarm system	31
4.2	Remote Connect	31
<b>5</b>	<b>Remote Services step-by-step</b>	<b>33</b>
5.1	Remote Connect	33
<b>6</b>	<b>RPS settings</b>	<b>36</b>
6.1	Network nodes	36
6.2	Line numbers	36
6.3	Switches	37
6.4	OPC servers	37
6.5	UGM-2040 servers	38
<b>7</b>	<b>Installation</b>	<b>39</b>
7.1	Installing media converters in the mounting frame	39
7.2	Installing media converters in PSS 0002 A/USF 0000 A	40
7.3	Settings on media converter	41
7.4	Installing switches in PSS 0002 A/USF 0000 A	42
7.5	Settings on switch	43
7.5.1	Assign IP address	44
7.5.2	Program redundancy settings	44
7.5.3	Programming the fault relay	45
7.5.4	Programming connection monitoring	46
7.5.5	QoS priority, only for UGM-2040	46
7.5.6	Activating IGMP snooping	46

---

7.6	CAN network	47
<b>8</b>	<b>Connections</b>	<b>57</b>
8.1	Cabling of panel controller	57
8.1.1	Media converters and power supply	57
8.2	Switch with power supply and fault relay	58
8.3	Cabling of FMR-5000 remote control unit	60
<b>9</b>	<b>Appendix</b>	<b>63</b>
9.1	Ethernet error messages	63
	<b>Index</b>	<b>65</b>

---



# 1 Safety instructions

**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.

**Notice!**

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.

**Caution!**

For access via the internet use only BOSCH Remote Services.

**Caution!**

EffiLink requires a secure IP connection. For this reason with EffiLink an IP network is provided, which is based on DSL with an optional wireless access on the panel side. EffiLink is only available for Bosch ST-IE in Germany.

**Notice!**

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

**Danger!**

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 light-emitting diode, wavelength 650 nm, output < 2 mW, in accordance with DIN EN 60825-1:2003-10.

## 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 networking guide provides an overview of the framework conditions, limit values, and general procedures for panel network planning and installation.

Detailed descriptions of the installation of the individual components can be found in the respective installation guides.

You find a description of the user interface of the MPC-xxxx-C in the user guide included with the device.

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



---

**Notice!**

Dear Customer,

We work tirelessly to keep our documentation up to scratch. Should you have any suggestions, however, or if you have discovered an error, please e-mail us at

[ST.TechComFire@de.bosch.com](mailto:ST.TechComFire@de.bosch.com).

---

## 3 Ethernet networking

### 3.1 Procedure

There are several procedures for creating a 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.

#### 3.1.1 Standard procedure for 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 the 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.
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.

#### 3.1.2 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 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 RPS. Import all of the necessary panel configurations. Configure the network settings and print them out.
  - Connect all panels to the 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.

## 3.2 Overview of the 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.

### MAC addresses

Each panel controller has 3 MAC addresses.

- MAC address for the host
- MAC address for network connection 1 (Eth 1)
- MAC address for network connection 2 (Eth 2)

The network diagnosis of the panel always shows you the MAC address of the hosts connected via the network.

### 3.2.1 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 following SNMP password: PUBLIC

#### 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 bus topology following the failure of a connection is automatically canceled once it has been repaired.

### 3.2.2 Network diameter

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



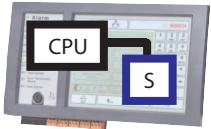

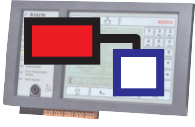

#### Definition

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.

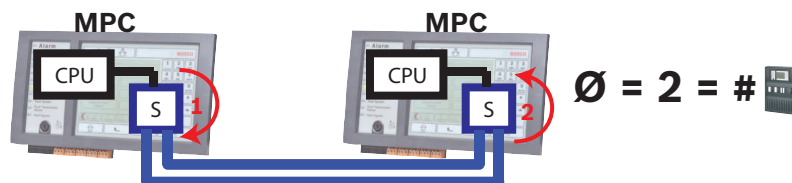
The following must be taken into account in relation to a FPA-RSTP Ethernet network:

- Each MPC contains an end point and an internal RSTP switch.
- A combination of MPC and redundant MPC 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**

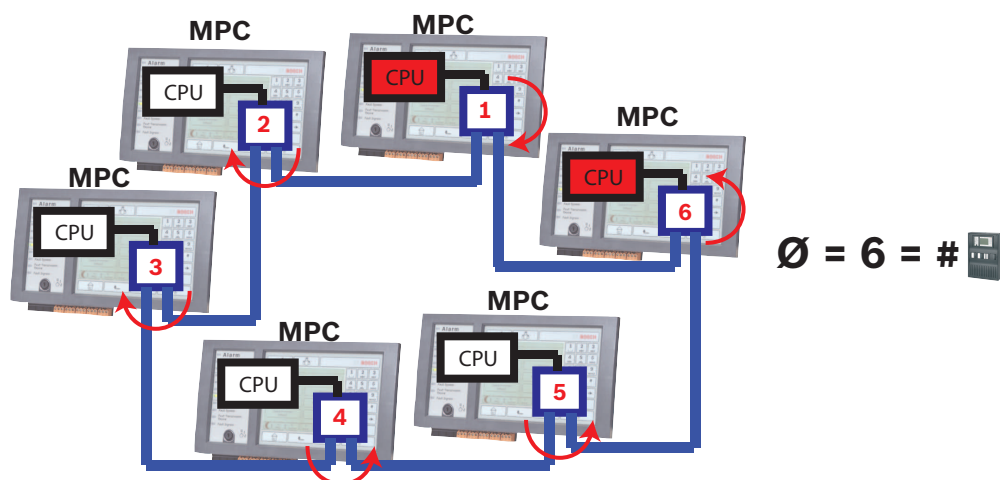
	Central processor in the MPC panel controller or the FMR remote control unit.
	Internal RSTP switch in the MPC panel controller or the FMR remote control unit.
	MPC panel controller/FMR remote control unit with central processor and internal RSTP switch.
	Redundant MPC panel controller with central processor and internal switch.
	MPC panel controller/FMR remote control unit Starting point/end point for determining the diameter in the examples.
	External RSTP switch

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



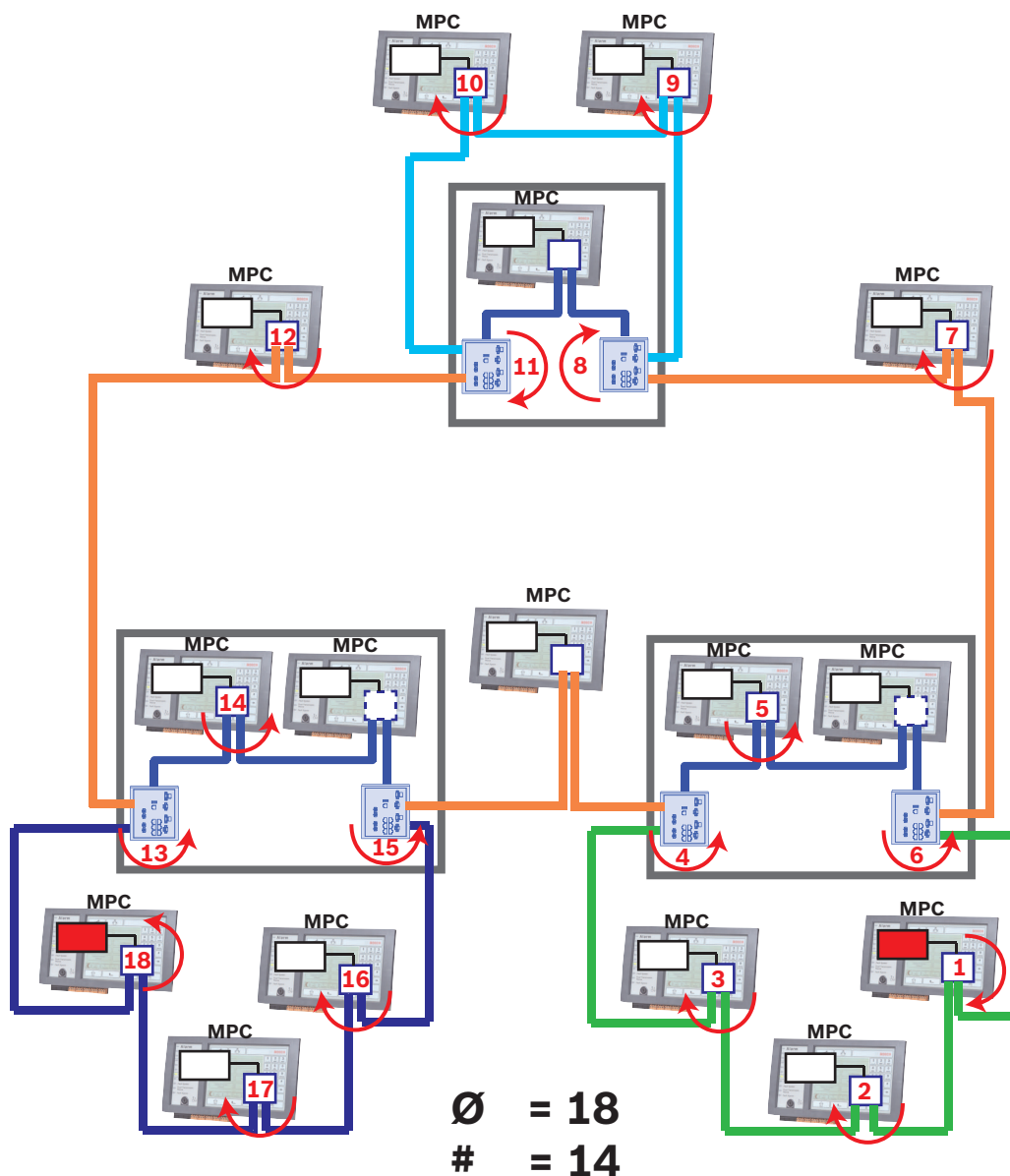
**Figure 3.1: Network diameter of a loop with 2 panels**

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



**Figure 3.2: Network diameter of a loop with 6 panels**

If a backbone and sub-loops are connected to each other via RSTP switches not integrated into the panel controller, then the RSTP switches must also be taken into account.



**Figure 3.3: Network diameter of a backbone with sub-loops**

The figure shows that the longest path must always be found for the diameter.

### 3.2.3

#### Cables used

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 50/125 $\mu$  or duplex I-VH2G 62.5/125 $\mu$ , SC plug.  
Single mode: fiber optic Ethernet patch cable, duplex I-VH2E 9/125 $\mu$ , SC plug.  
Note the minimum bending radii specified in the cable specification.

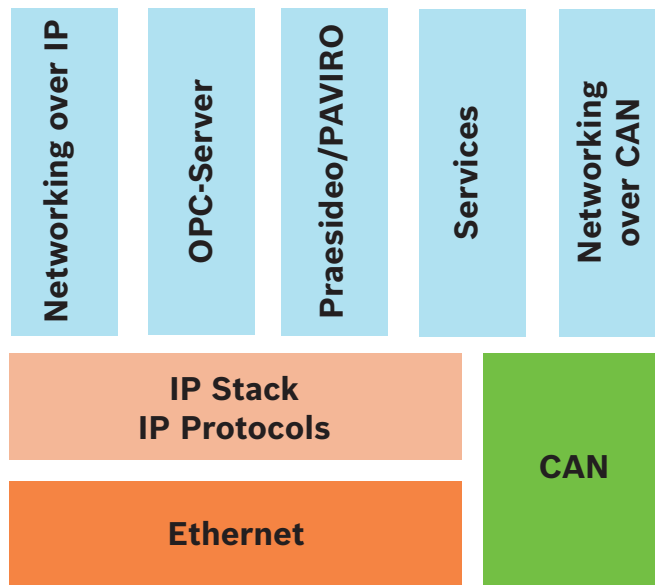
### 3.2.4

#### Extension of existing networks

In order to ensure fault-free communication between different panel versions (e.g. MPC, version B), all panels must have the same firmware version.

### 3.2.5

#### Ethernet/IP communication



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

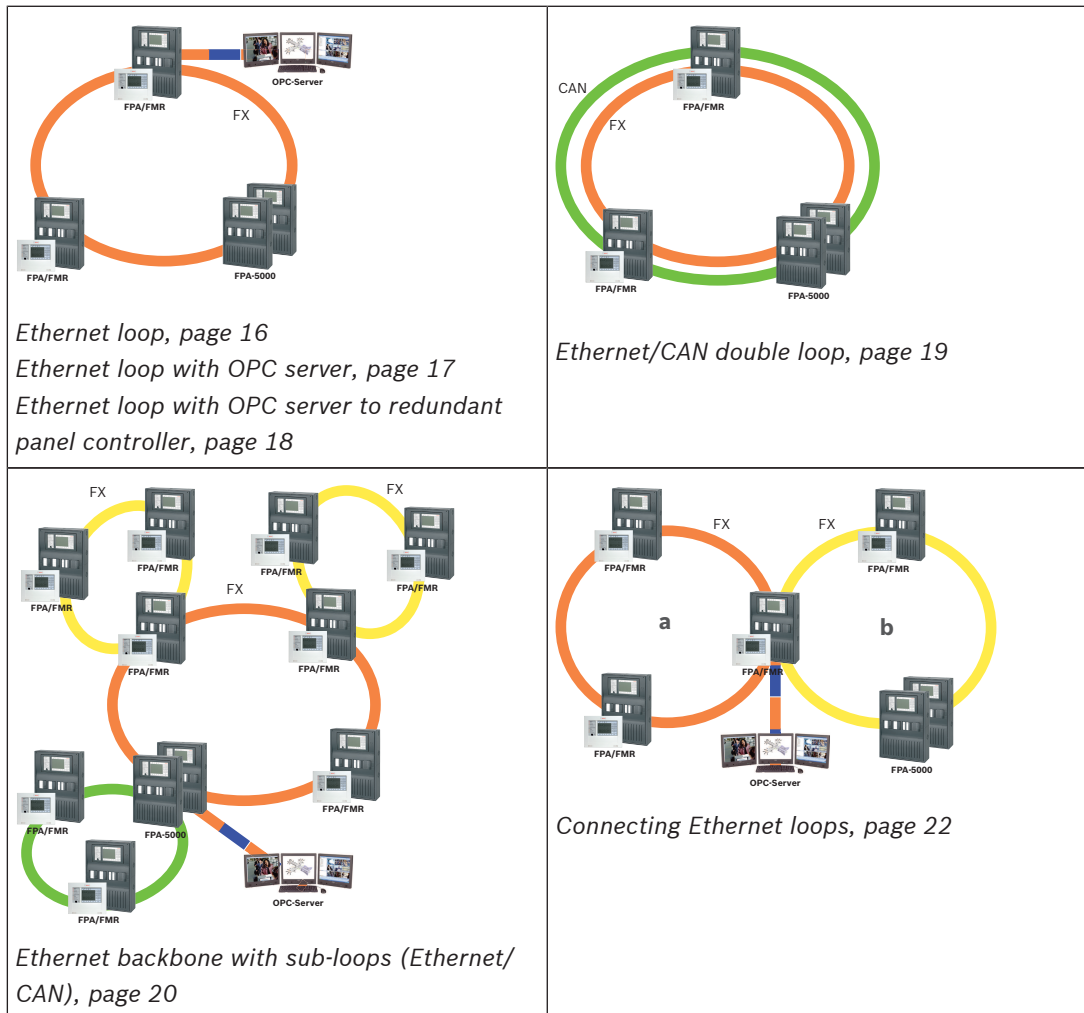
- networking over TCP/IP  
In FSP-5000-RPS, enable panel-to-panel communication in the Ethernet network
- OPC servers  
Add an OPC server to the FSP-5000-RPS configuration
- Praesideo/PAVIRO connection  
Add a Voice Alarm System to the FSP-5000-RPS configuration and configure virtual triggers.
- Condition Monitoring  
Activate the relevant check box in FSP-5000-RPS
- Remote Connect and EffiLink  
Add remote access to the FSP-5000-RPS configuration and set up the remote access in FSP-5000-RPS.

If the Ethernet interface of the panel controller is used only for communicating with an OPC server or for Condition Monitoring disable the panel communication over TCP/IP. Otherwise 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.

### 3.3 Topologies

The following topologies are possible:



The following settings, notes and restrictions apply to all topologies:



#### Notice!

For each panel, a maximum of 512 detection points may be connected according to EN 54-2. If this number is exceeded, the panel must be designed redundantly. For technical reasons, a maximum of 2048 detection points can then be connected.



#### 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.



#### Notice!

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



**Notice!**

The requirements of EN 54-13 for data transmission paths can only be met with fiber optic cable connections for Ethernet.

Connections within a housing may be established with Ethernet cables.

**Notice!**

Switches and media converters in Ethernet networks must be installed in panel housings.

Installation outside of a panel housing is not compliant with EN 54.

**Notice!**

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.

**Notice!**

Networks with more than 20 RSTP switches or a diameter greater than 20 require special settings.

The standard setting for the IP configuration is only designed for networks with a maximum of 20 RSTP switches or a maximum network diameter of 20.

Make sure that the RSN 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 FPA**

In the standard settings of the FPA, both the FSP-5000-RPS programming software and the control unit adopt the set RSN as the last number of the IP address.

**Notice!**

Correct setting of the RSN 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 RSN 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 (redundancy 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. In-depth knowledge of networks is required for this. The panel controllers and 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.

**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 8*.
- The Ethernet transmission sections outside of the panel housing must be designed as fiber optic cable connections.
- Switches must not be used outside of panel housings.
- Media converters must not be used outside of panel housings.
- A maximum of one panel only and 3 FMR-5000 can be used in a network, in the case of the FPA-1200.

**Features**

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

**Additional information when using the OPC server**

OPC servers in your network must be added to the RPS programming software.

You must perform the following settings in both the RPS software and on the OPC server:

- Network nodes
- Network group
- RSN
- IP Address
- Port

The OPC server uses port 25000 as standard.



**Notice!**




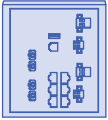


FSP-5000-RPS programming software:

Note that you must assign the OPC server to each network node from which statuses should be transmitted.

**3.3.1**

**Key**

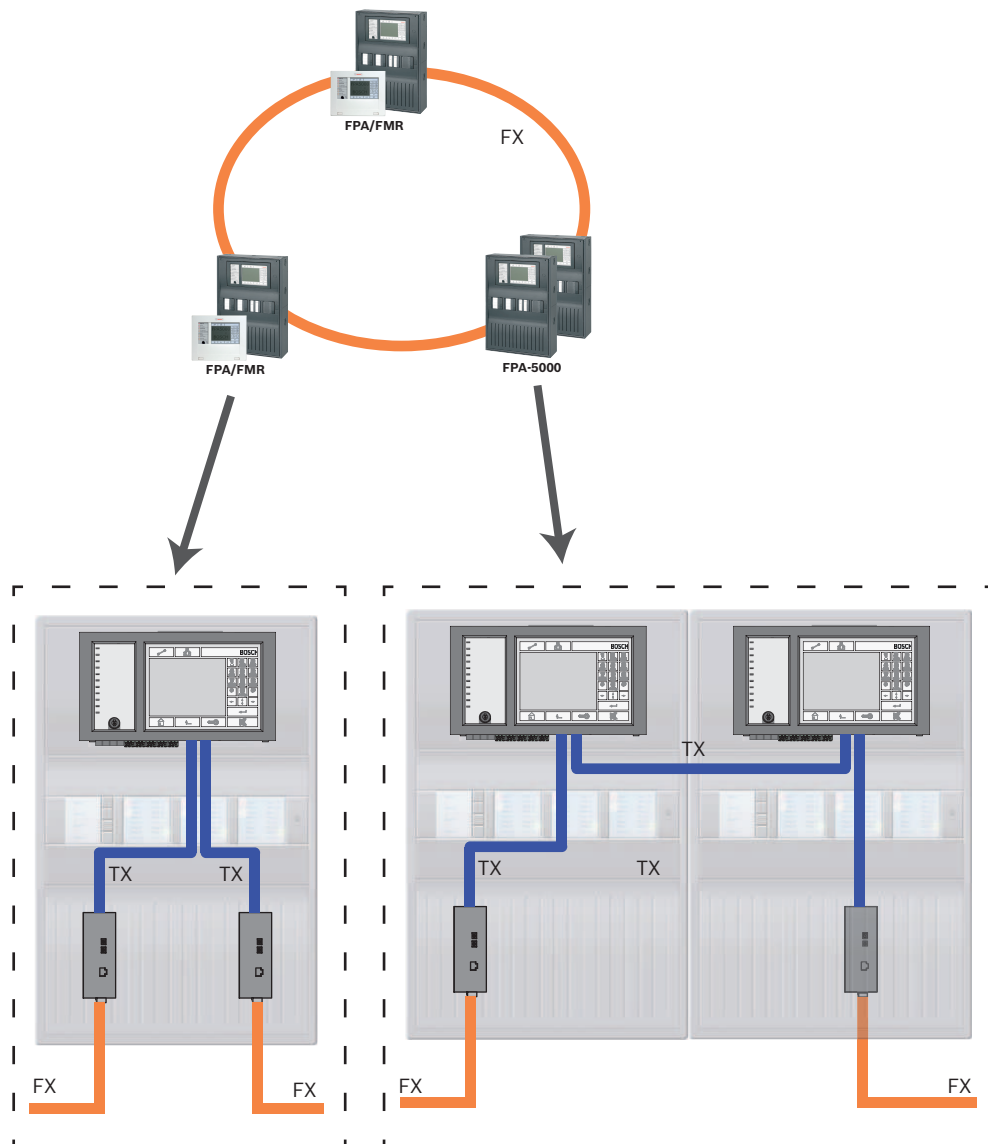
Icon	Description
	TX Ethernet cable (copper)
	FX Ethernet cable (fiber optic cable)
	TX or FX Ethernet cable
	CAN bus

Icon	Description
	Housing
 FPA/FMR	Panel/Remote Keypad
 FPA-5000	Redundant panel
	RSTP switch
	Media converter
	Secure Network Gateway

### 3.3.2

#### Ethernet loop

For this configuration, the notes, settings, parameters and features specified in *Topologies*, page 12 apply.



**Figure 3.4: Ethernet loop**

Key, see *Key*, page 14

### 3.3.3

#### Ethernet loop with OPC server

For this configuration, the notes, settings, parameters and features specified in *Topologies*, page 12 apply.

The information given here expands on *Topologies*, page 12.

##### Switch for connecting the OPC server 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, RPS programming software and switch are identical.

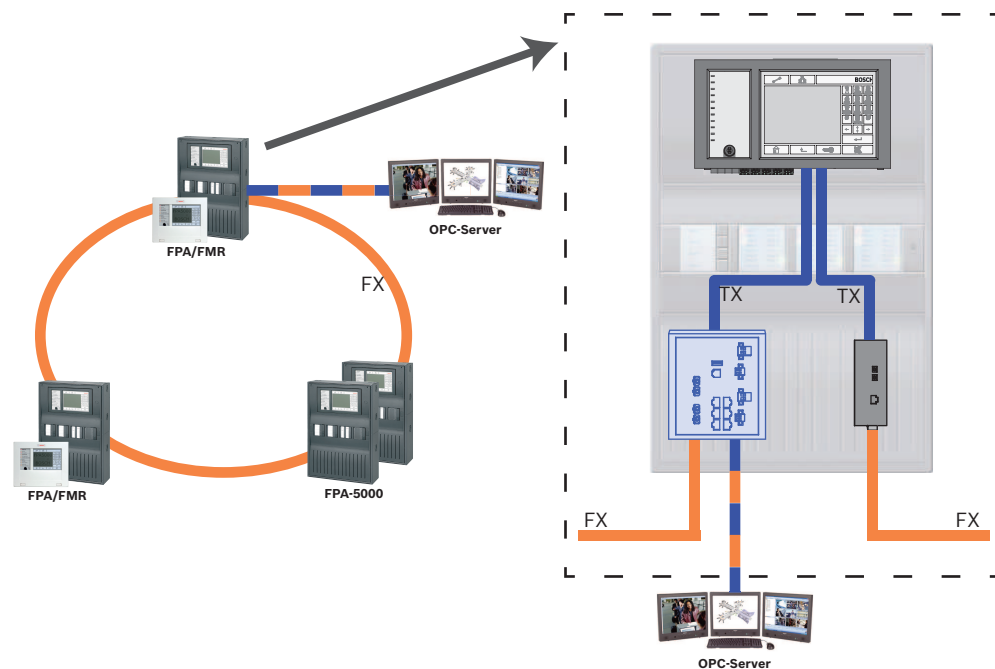
##### OPC server must be programmed separately

Program the IP address, network nodes, network group and RSN, see *OPC servers*, page 37. The OPC server uses port 25000 as standard.

Make sure that the settings in the RPS programming software and OPC server are identical.

##### Parameters

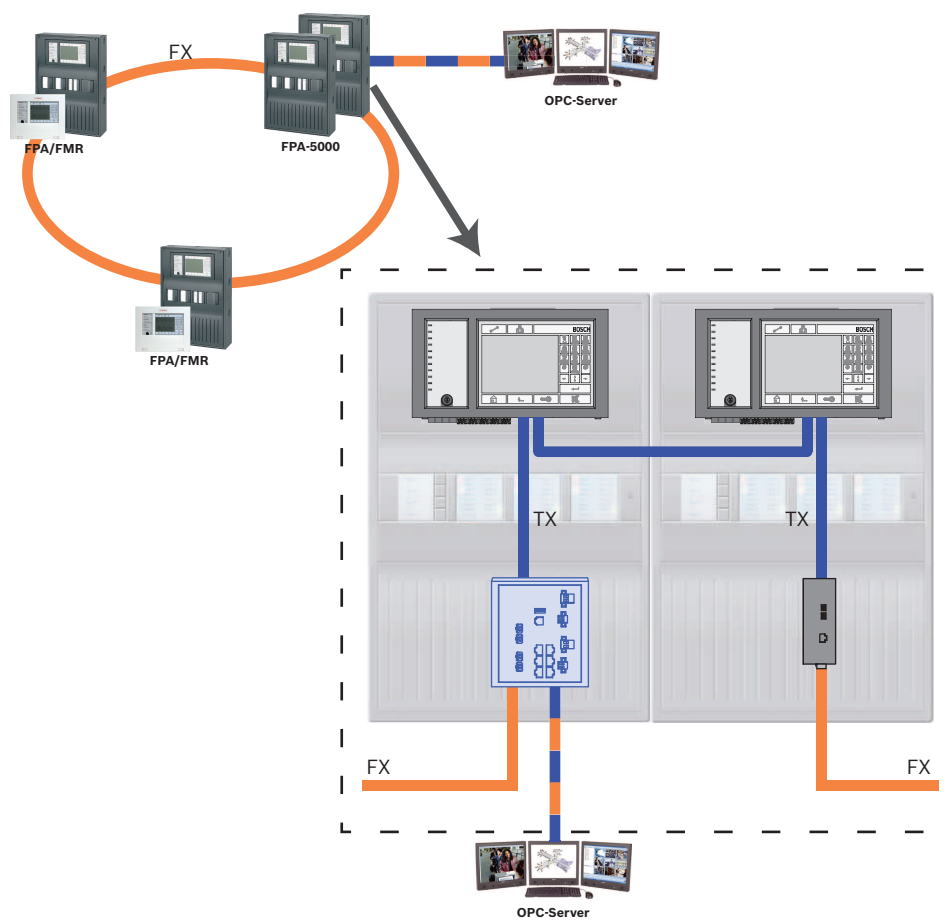
- The OPC server may be connected via an Ethernet cable (copper) or fiber optic cable.



**Figure 3.5: Ethernet loop with OPC server**

Key, see *Key*, page 14

### 3.3.4 Ethernet loop with OPC server to redundant panel controller



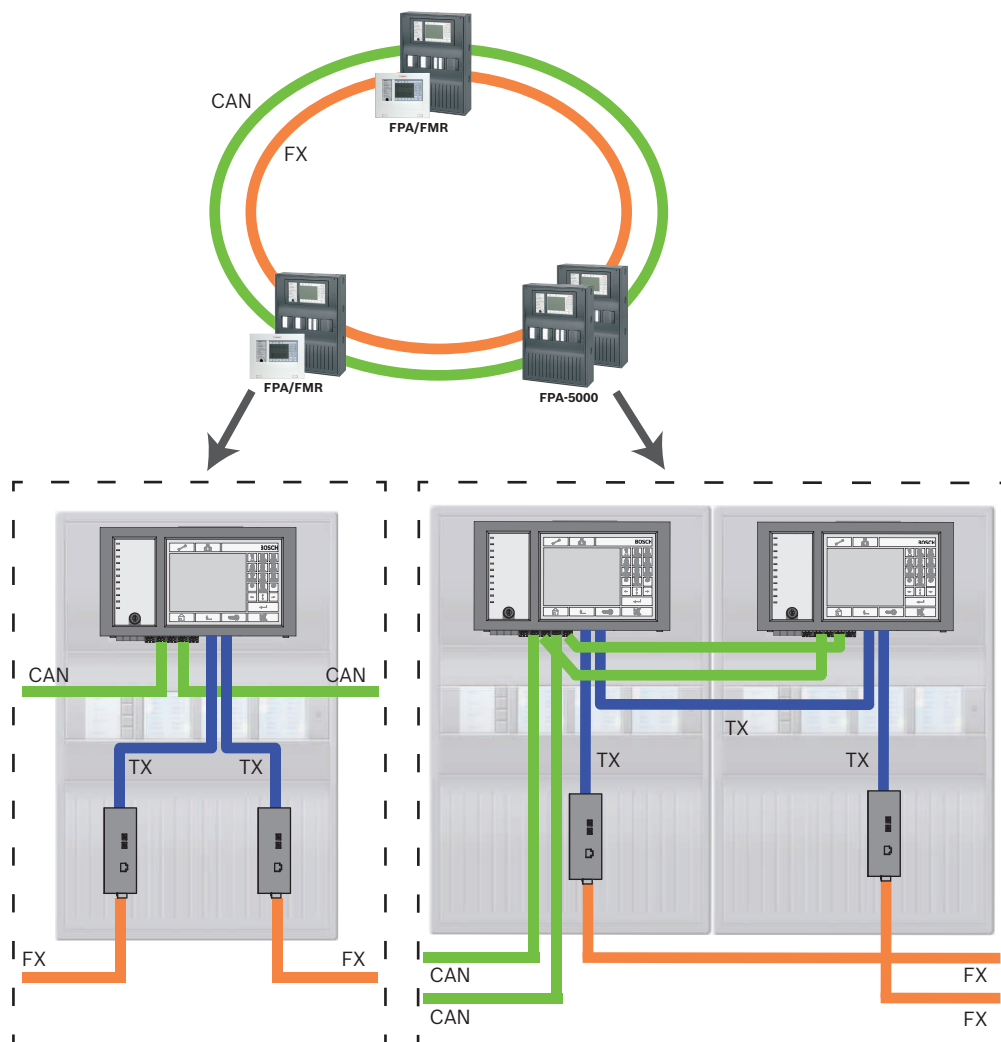
**Figure 3.6: Ethernet loop with OPC server to redundant panel controller**

Key, see *Key*, page 14

### 3.3.5

#### Ethernet/CAN double loop

For this configuration, the notes, settings, parameters and features specified in *Topologies*, page 12 apply.



**Figure 3.7: Double loop of Ethernet and CAN**

Key, see Key, page 14

### 3.3.6 Ethernet backbone with sub-loops (Ethernet/CAN)

For this configuration, the notes, settings, parameters and features specified in *Topologies, page 12* apply.

The information given here expands on *Topologies, page 12*.

**Notice!**

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

Please note that with this topology you are required to determine the network diameter, see *Network diameter, page 8*. Only RSTP devices are included in the network diameter, CAN-networked panels are disregarded.

**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 must be networked via the Ethernet.

**Notice!**

For all panels and 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 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.

**Settings for loops with more than 20 RSTP devices**

Panel controllers connected via CAN are not regarded as RSTP switches when determining the network diameter.

**Switches for connecting the OPC server and the sub-loops must be programmed separately**

Program the IP address and redundancy settings of the 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 *Switch with power supply and fault relay, page 58*.

Make sure that the RSTP settings in the panel controllers, RPS programming software and switch are identical.

**Notice!**

Change the RSTP priority for the switches for connecting the loops, as they belong to the backbone.



### OPC server must be programmed separately

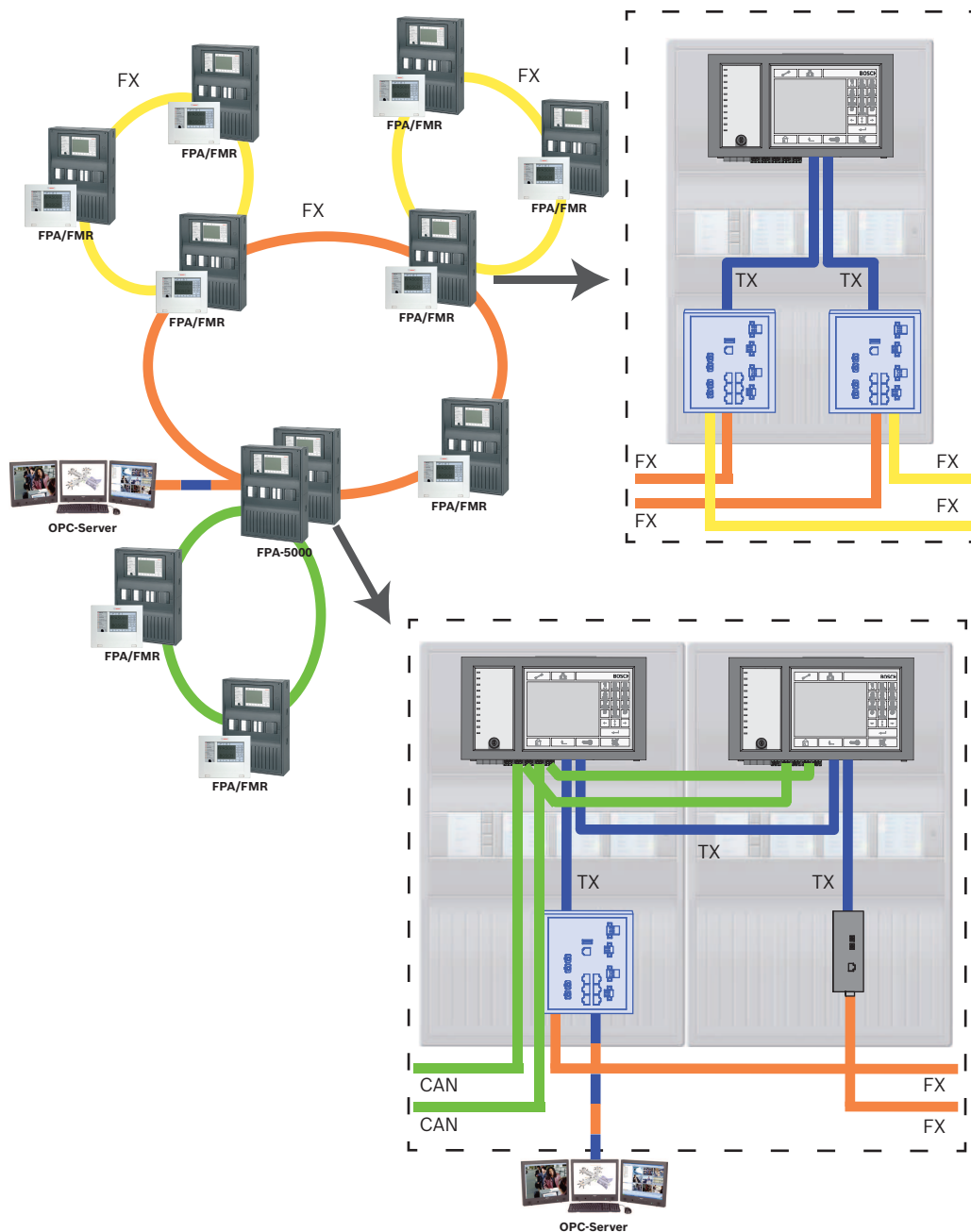
Program the IP address, network nodes, network group and RSN, see *OPC servers*, page 37.

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 or fiber optic cable



**Figure 3.8: Ethernet backbone with sub-loops**

Key, see Key, page 14

### 3.3.7

#### Connecting Ethernet loops

For this configuration, the notes, settings, parameters and features specified in *Topologies, page 12* apply.

The information given here expands on *Topologies, page 12*.



#### Notice!

This topology requires additional settings for all RSTP nodes 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), page 20*. 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 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, for connections see *Switch with power supply and fault relay, page 58*.

Make sure that the RSTP settings in the panel controllers, RPS programming software and 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 *OPC servers, page 37*.

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

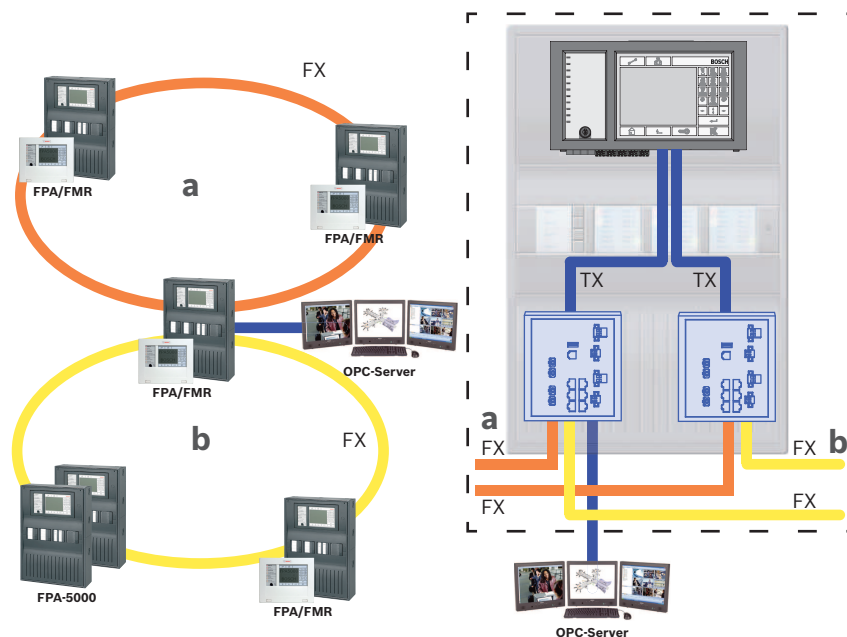


Figure 3.9: Connecting Ethernet loop via a non-redundant panel

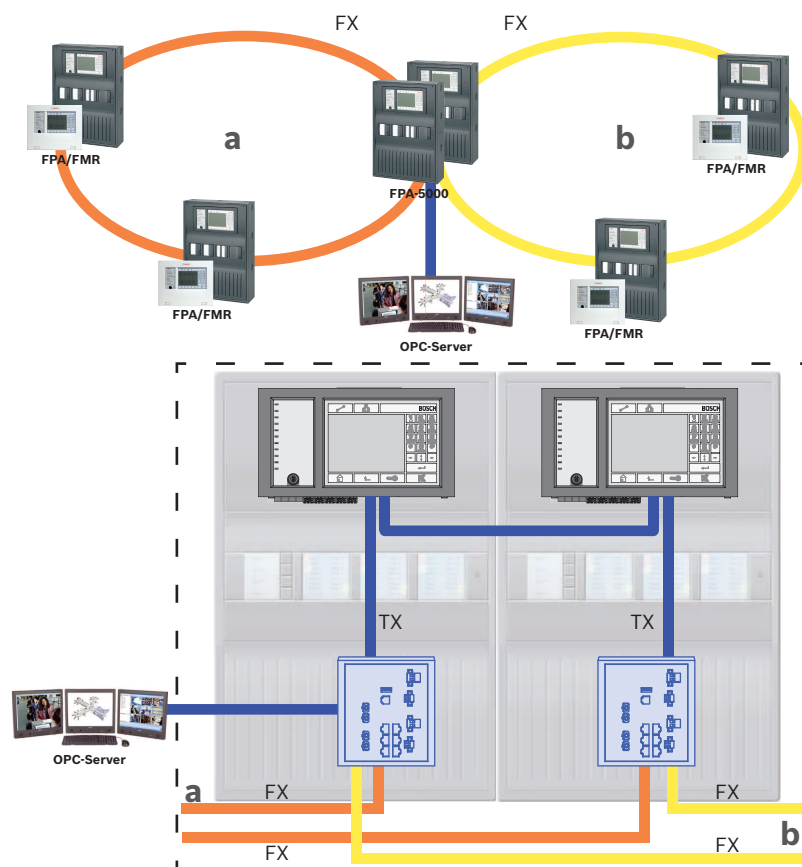


Figure 3.10: Connecting Ethernet loop via a redundant panel

Key, see Key, page 14

### 3.4

## UGM-2040 networks

The topologies to be installed and the network settings to be programmed can be obtained from your UGM 2040 BMA planner. See also the UGM 2040 BMA Anschaltehandbuch.

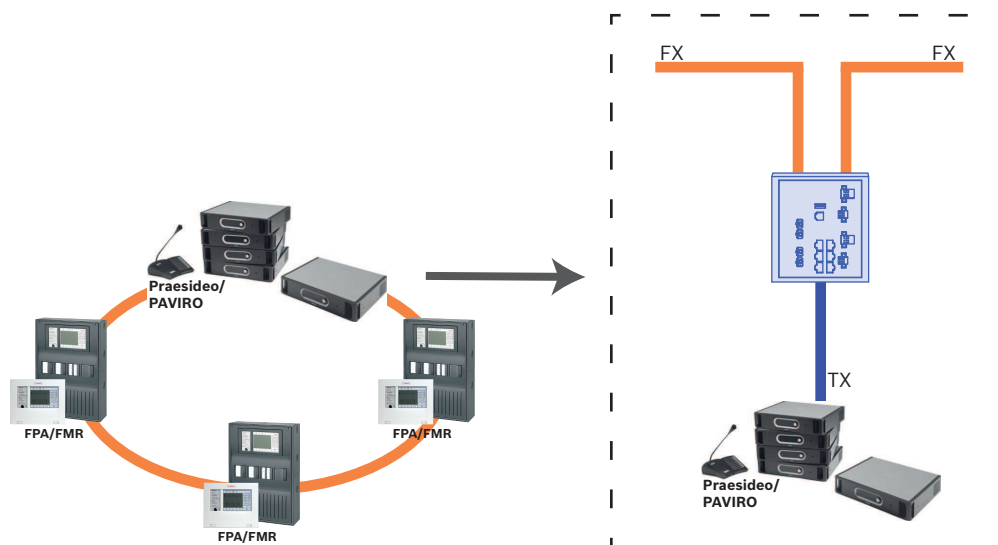
## 3.5 Voice alarm system over IP



### 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).

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



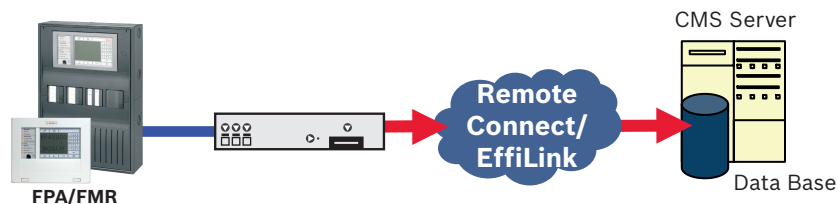
**Figure 3.11: Ethernet loop with Praesideo/PAVIRO**

Use the Hirschmann Rail Switch Rugged RSR20 (CTN Ethernet Switch MM: BPA-ESWEX-RSR20, CTN Ethernet Switch SM: RSR20-0800S2S2T), 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 Hirschmann Rail Switch Rugged RSR20, see *Activating IGMP snooping*, page 46.

## 3.6 Condition Monitoring

Condition Monitoring is a service provided by Bosch ST-IE to monitor the system regarding diagnostic data.



### Notice!

Ethernet connections used only to transfer Condition Monitoring data may be designed both as Ethernet cables and fiber optic connections. Note the permitted maximum cable lengths.

**Notice!**

The connection used for Condition Monitoring must be non-interacting.

**Notice!**

Note that Condition Monitoring data is transferred in unencrypted form.

**Notice!**

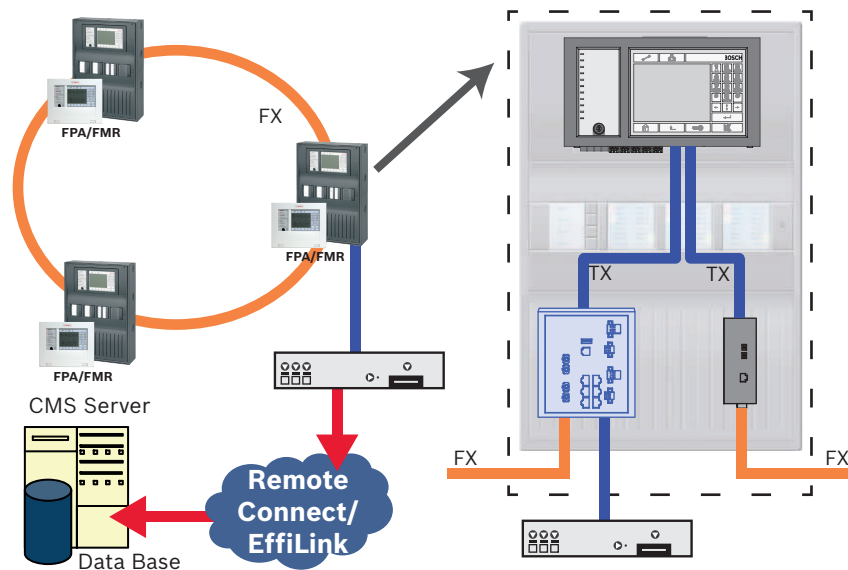
FSP-5000-RPS programming software:

Note that you must enable Condition Monitoring in each network node from which statuses should be transmitted.

In the FSP-5000-RPS programming software, you can temporarily start up Condition Monitoring for one month. This can be useful for troubleshooting, for example, and works without authentication of the Condition Monitoring system server. After a month, the function switches itself off again automatically.

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

### Condition Monitoring in the Ethernet network



When using Condition Monitoring with Ethernet networks, one panel in the network must be connected to the router for data transfer purposes. All Condition Monitoring data is transferred from the network via this connection.

### Switch for connecting the Condition Monitoring system server 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, RPS programming software and switch are identical.

### 3.7 Teleservice EffiLink

Teleservice EffiLink enables remote access to an FPA-5000 system via IP network. The Bosch service center has the possibility to perform setup and support tasks remotely.



#### Caution!

EffiLink requires a secure IP connection. For this reason with EffiLink an IP network is provided, which is based on DSL with an optional wireless access on the panel side. EffiLink is only available for Bosch ST-IE in Germany.

For realizing the Teleservice EffiLink with a panel network it is sufficient to connect only one panel to the router for data transfer purposes. On this panel, Teleservice EffiLink has to be enabled in the RPS configuration.

To connect the panel network to the router, use the Hirschmann Rail Switch Rugged RSR20, approved with FPA-5000 version 2.8.



#### Notice!

Use only media converters to connect the panel via FX.

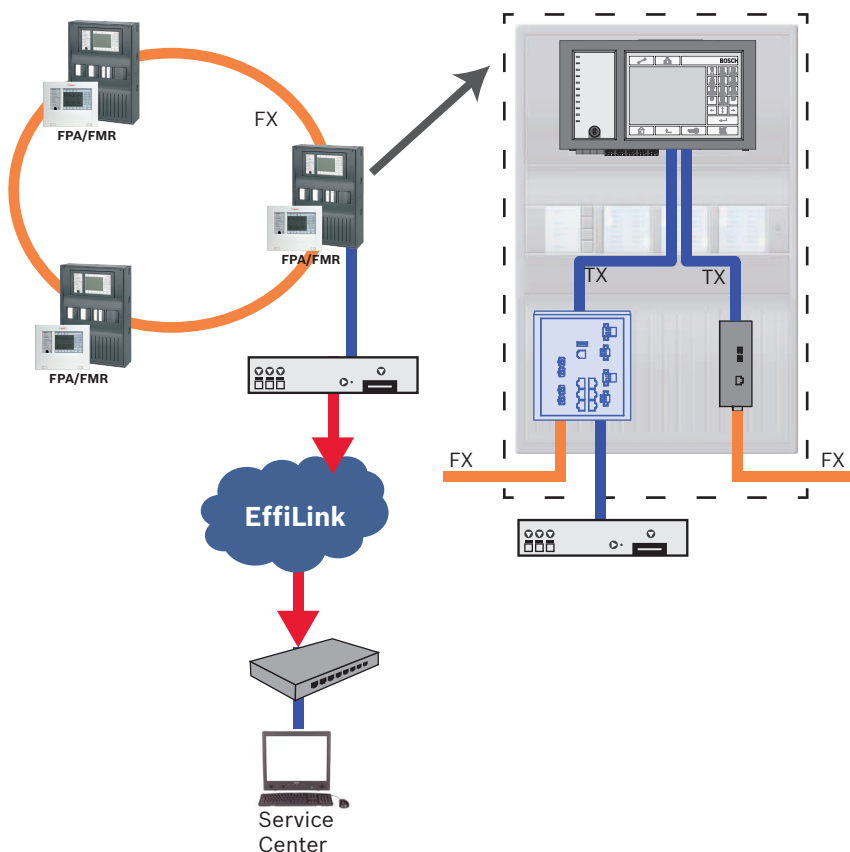


Figure 3.12: Teleservice EffiLink in the panel network

### 3.8 Remote connect

Remote Connect provides a trusted and secure internet connection, which enables remote access to a panel. For Remote Connect use the Secure Network Gateway (CTN: C1500) approved with panel version 2.14.7.

In case of a panel network, one panel of the panel network has to be connected to a Secure Network Gateway and 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 a Hirschmann Rail Switch Rugged RSR20.

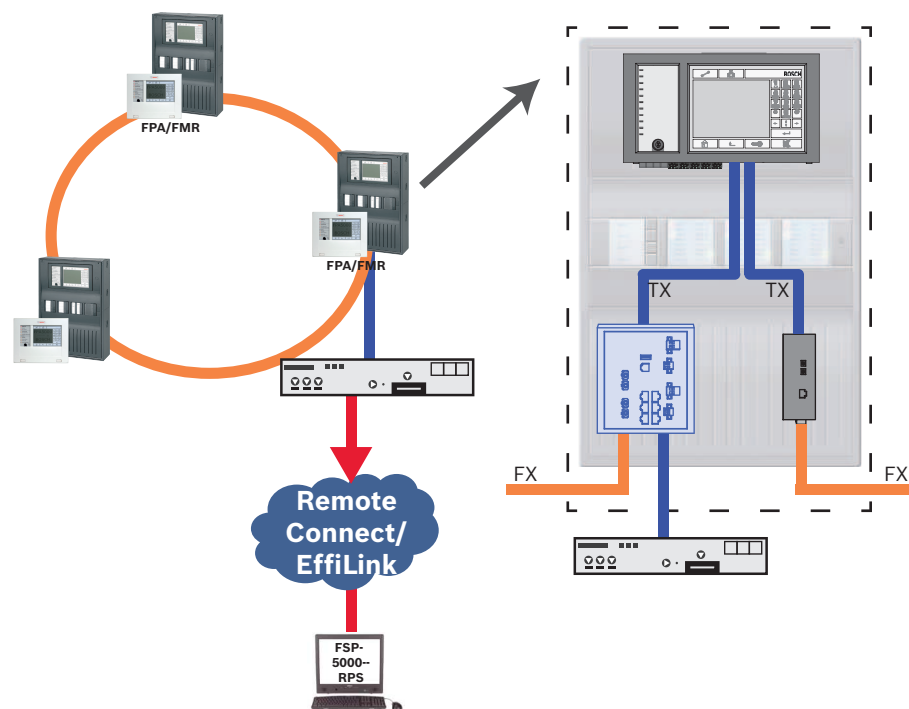


Figure 3.13: Remote Connect in an Ethernet loop



#### Notice!

Use only media converters to connect the panel via FX.

To prevent sending EN 54-2 relevant multicast traffic to the router, use the Hirschmann Rail Switch Rugged RSR20 (CTN Ethernet Switch MM: BPA-ESWEX-RSR20, CTN Ethernet Switch SM: RSR20-0800S2S2T) approved with panel version 2.8. Activate IGMP snooping of the Hirschmann Rail Switch Rugged RSR20, see *Activating IGMP snooping*, page 46.

**Notice!**

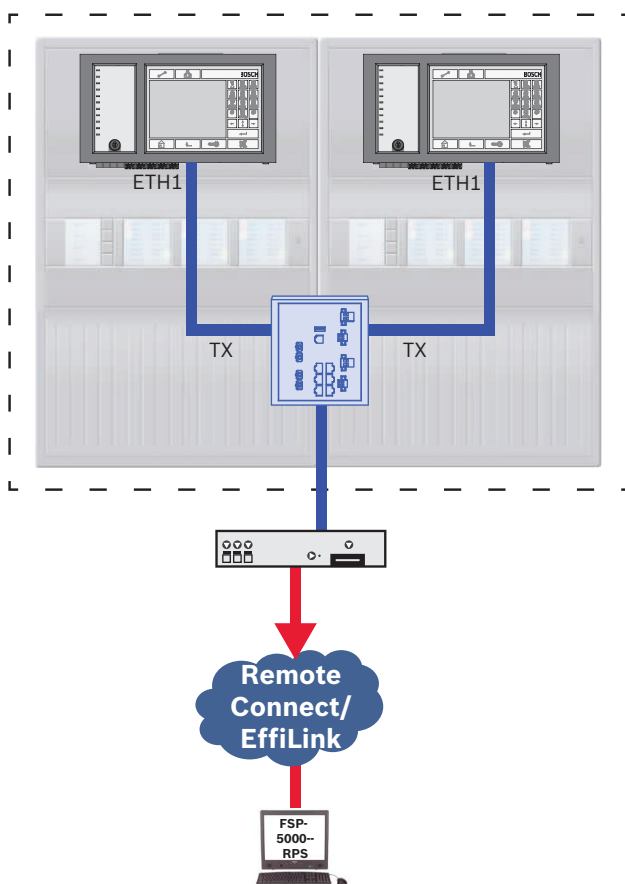
The internet router (or the company network which provides internet access) as well as the Secure Network Gateway must provide separated sub-networks. Panels of the panel network may not be placed in the sub-network of the internet router. Also overlapping of the sub-networks is not possible.

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.

For connecting the Secure Network Gateway to a redundant panel controller you can use the following topology.



For basic instructions in setting up Remote Services see *Remote Services step-by-step*, page 33



## 4 CAN networking

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.

The panels can be networked redundantly as a loop via CAN1 and CAN2.

### FOC networking

In a loop, panels can be connected using fiber optic cables via CAN/FOC adapters.

The CAN/FOC converters from EKS enable distances of up to 15 km between two nodes to be overcome in a network (depending on the converter type and the fiber optic cable used). The following converters are available (PzP CAN FOC system/MM):

- DL-CAN/1x13-MM-ST system
- DL-CAN/1x13-MM-SC system
- DL-CAN/1x13-SM-ST system
- DL-CAN/1x13-SM-SC system

### Loop topology



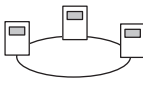
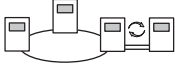
- In loop topology, the CAN cable is always routed from a CAN1 terminal to a CAN2 terminal [CAN1  $\Rightarrow$  CAN2].

A CAN segment thus consists of two bus users. The cable length depends on the cable cross-section.

- Due to the maximum of 32 nodes and the maximum cable length of 1000 m between nodes, a system can be installed with a total cable length of 32 km.

### Networking of panels and remote keypads

The table below shows the options for networking panels/remote keypads depending on the network topology.

Topology		FPA-1200	FPA-5000
	Standalone panel	Possible	Possible
	Standalone panel, redundant	Not possible	Possible
	Loop	1 FPA-1200 + max. 3 FMR-5000	Max. 32 FPA-5000/FMR-5000
	Loop with redundant panel	Not possible	Max. 32 FPA-5000/FMR-5000 + redundant FPA-5000

Refer to the limits determined by the network topology.

**As the FPA-1200 is not operated as the redundant panel, DIP 6 on FPA-1200-MPC is not functional!**

### 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 32,768.
- 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 an MPC Panel Controller or an FMR-5000 Remote Keypad.
- The number of nodes in loop topology is limited to 32.
  - The number of nodes per CAN segment is limited to eight.  
A CAN segment is the physical connection of a CAN line.
  - Up to 3 remote keypads to a specific panel can be directly assigned to the network using the FSP-5000-RPS Programming Software.

The cabling between nodes and the maximum permissible cable length is also determined by the choice of topology.

#### Cable type for networking

The CAN connection is a two-wire connection (CAN-H and CAN-L). 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. The shield wire of the CAN cable is only connected to the metal housing of the panel on one side.

#### Cable length for networking

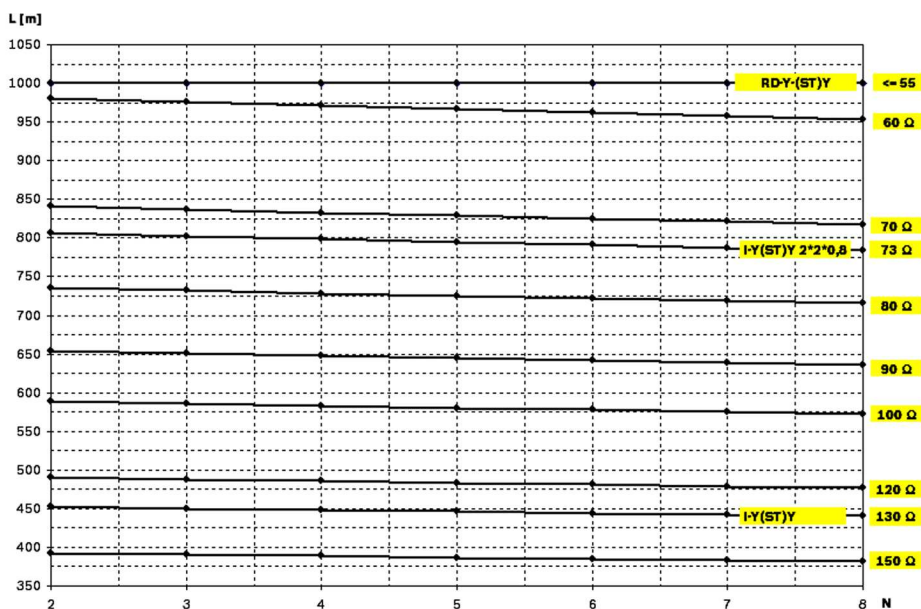
The maximum permitted cable length depends on the loop resistance of the cable used and on the number of communicating.

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 4.1: Network: Cable length** Achievable cable length, depending on the number of nodes and the cable resistance

L = cable length in meters

N = number of nodes

## 4.1 Connection to voice alarm system



### 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).

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.

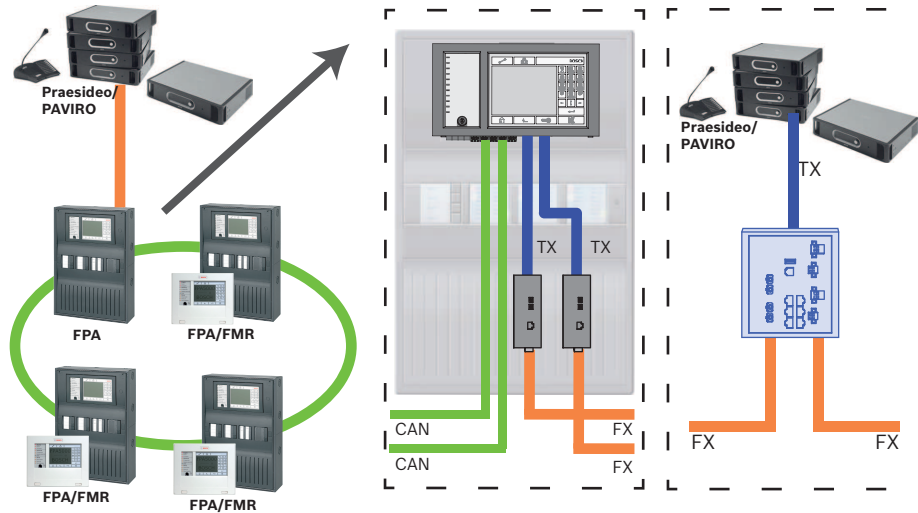


Figure 4.2: Praesideo/PAVIRO connection to a CAN network



### Notice!

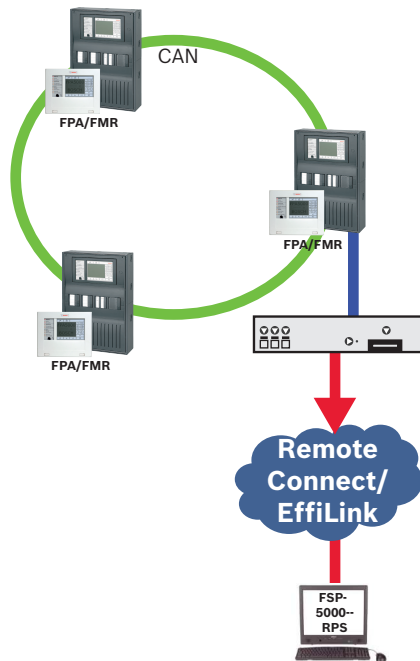
Because CAN network traffic shall not be transferred through the Ethernet connection, you must switch off networking over IP in the FSP-5000-RPS programming software. If this is not switched off, the network will not be compliant with EN 54.

## 4.2 Remote Connect

Remote Connect provides a trusted and secure internet connection, which enables remote access to a panel. For Remote Connect use the Secure Network Gateway (CTN: C1500) approved with panel version 2.14.7.

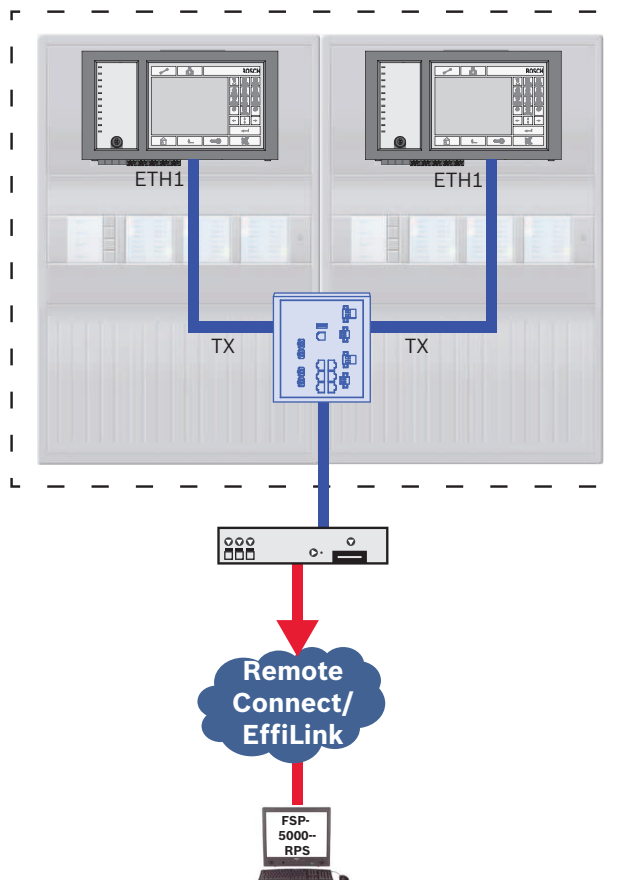
In case of a panel network, one panel of the panel network has to be connected to a Secure Network Gateway and Remote Connect has to be enabled in the FSP-5000-RPS configuration of this panel.

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



**Figure 4.3: Remote Connect in a CAN loop**

For connecting the Secure Network Gateway to a redundant panel controller you can use the following topology.



For basic instructions in setting up Remote Services see *Remote Services step-by-step*, page 33

## 5 Remote Services step-by-step

This chapter includes basic instructions for setting up Remote Services on <https://remote.boschsecurity.com>. For using Remote Services you must be user of a Remote Portal account. (You can have multiple users under one Remote Portal account.) Each Remote Portal account have one unique Remote ID.

### 5.1 Remote Connect



#### Notice!

Remote Connect is intended to work without reconfigurations or adjustments if the following requirements are fulfilled:

- panel with firmware - version 2.14.7, Ethernet interfaces enabled and standard Ethernet settings
- not configured panel controller or Remote Connect enabled in the FSP-5000-RPS panel configuration
- Secure Network Gateway for Remote Services available
- computer with FSP-5000-RPS 4.3.11 or higher installed and internet access

#### Step 1: Order Remote Connect license

Each network requires its own license.

- ▶ Order Remote Connect one-year licenses (F.01U.310.142) from BOSCH Fire Alarm Systems. Provide your email address at the time of order. If you are already user of a Remote Portal account, provide also your Remote ID.

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.

#### Step 2: Create a Remote Portal account

For using Remote Connect you must be user of a Remote Portal account. Each Remote Portal account have one unique Remote ID. If you don't have any Remote ID, perform the following:

1. On <https://remote.boschsecurity.com> -> **Sign Up** enter your name and your email address and create a password. Observe the terms and conditions and select **I agree to the terms and conditions**.
2. Click **Register**.  
The Remote Portal promptly sends an email containing an activation link.
3. For activating the account click the activation link. On the Remote Portal click your user name and select **Settings** -> **Account** and memorize the Remote ID.

The Remote ID is meant to represent one company. 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 **User Management** -> **Create user**. Then enter the required data and confirm with **Create**.

#### Step 3: Connect Secure Network Gateway

For establishing Remote Services use a Secure Network Gateway (C1500).

1. Connect the eth0 port of the Secure Network Gateway to the internet router or to the company network which provides the internet access.
2. Connect the eth1 port of the Secure Network Gateway to one of the Ethernet ports of the panel controller using the supplied CAT5 RJ45 network cable. Observe the possible topologies in *Ethernet networking, page 7* and in *CAN networking, page 29*.

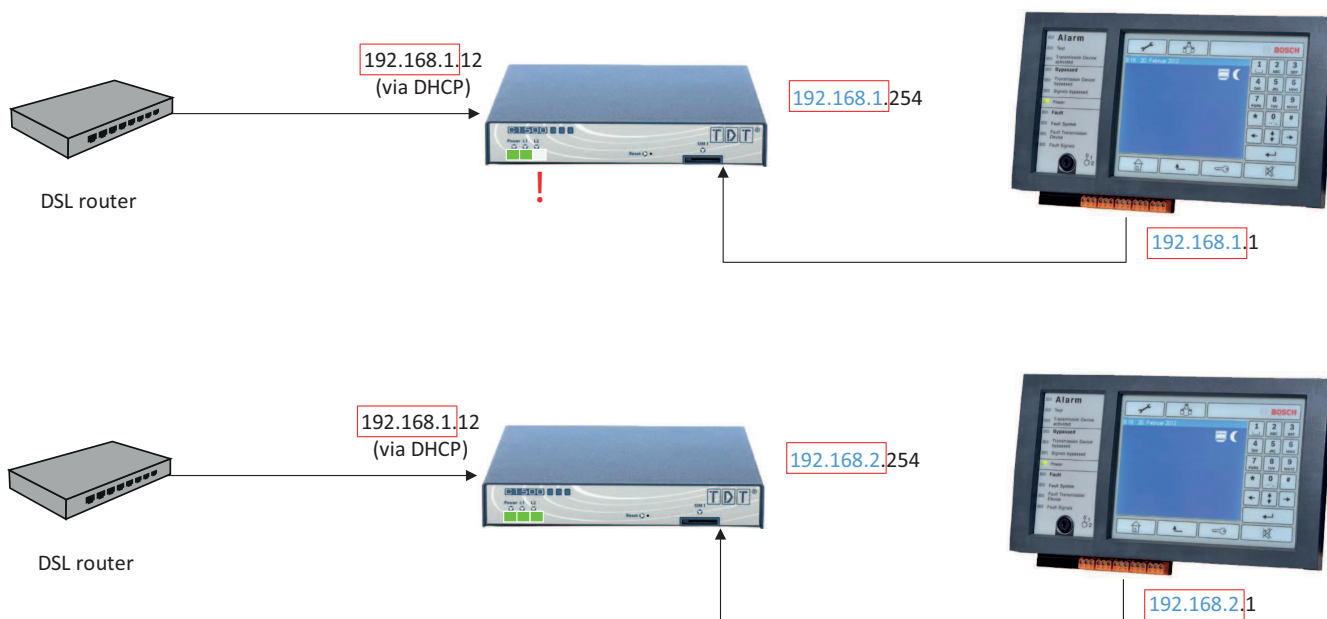
3. Connect the Secure Network Gateway to a 100 V - 230 V mains supply using the supplied power supply.

L1 LED on (green), when the connection to the internet has been established. L2 LED on (green) shortly after, which indicates that a VPN connection to the Remote Portal has been established.

### Seperating sub-networks (L2 LED off)

Connecting Secure Network Gateway for Remote Services fails in case of overlapping sub-networks (L2 LED off). In this case you have to separete the sub-networks by changing the IP addresses on panel network side.

The following example shows a Secure Network Gateway and a panel controller in the same address range as the DSL router. Separating the sub-networks is done by changing the third octet of the IP address.



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 4: Establish remote connection

1. At the panel use standard Ethernet settings, see *Standard Ethernet settings of FPA, page 13*.
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 5: Assign license in the Remote Portal

---

**Notice!**

An already assigned license cannot be reassigned.

- 
1. On <https://remote.boschsecurity.com> -> **Login** enter your email address and your password.
  2. Select the desired panel and click **Assign Licenses**.
  3. Select the license you want to assign and confirm with **Assign**.

You are now able to set up a remote connection with the FSP-5000-RPS programming software.

## 6 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.

### 6.1 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 nodes
  - 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.

### 6.2 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.



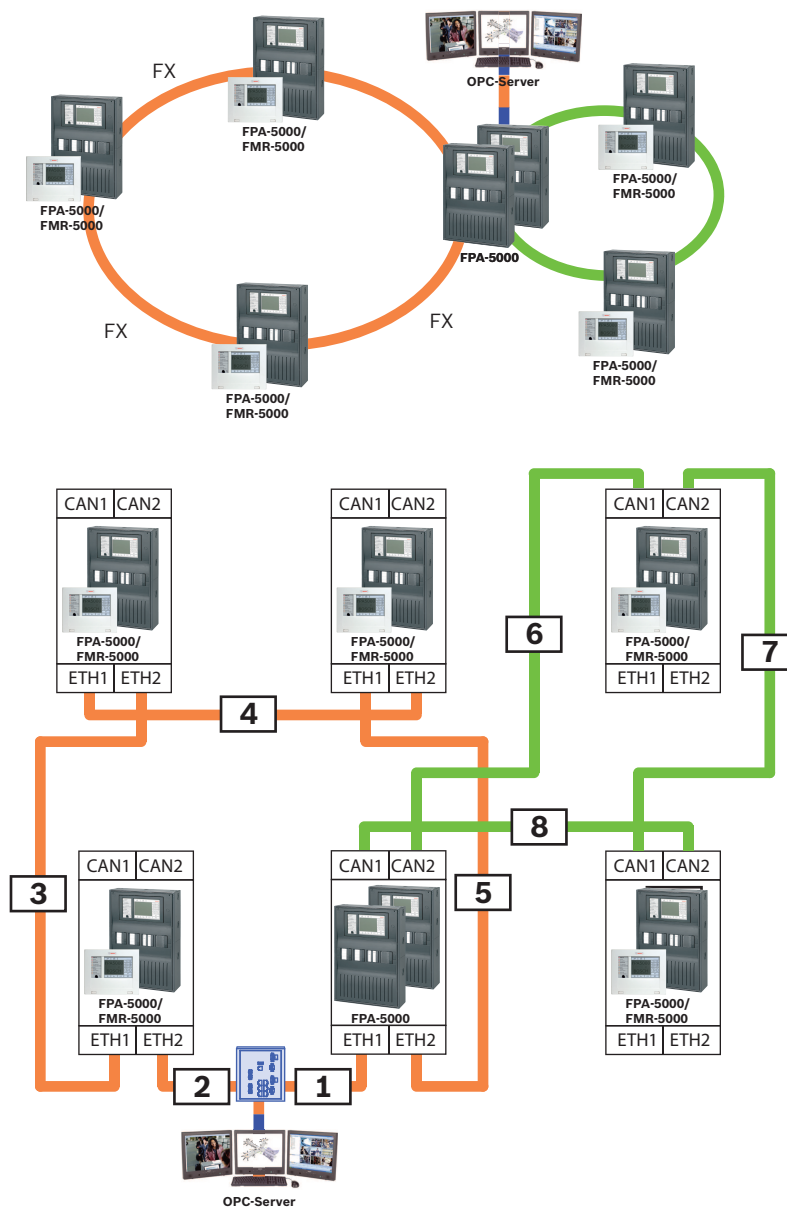


Figure 6.1: Example of a network and the possible line numbering

## 6.3 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.

## 6.4 OPC servers

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

- Network nodes
- Network group
- RSN
- IP Address
- Port

The OPC server uses port 25000 as standard.

**Notice!**

FSP-5000-RPS programming software:

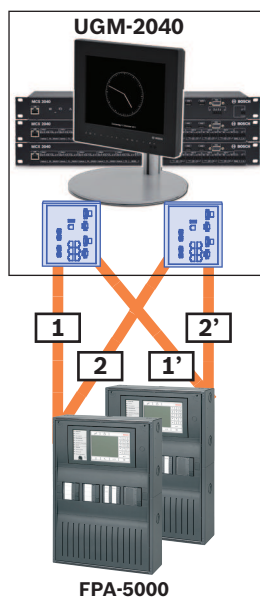
Note that you must assign the OPC server to each network node from which statuses should be transmitted.

**6.5****UGM-2040 servers****Notice!**

All FPA panel controllers and UGM servers must be located in the same subnetwork and have the same multicast address.

In the case of multiple FPA configurations or networks, these must be located in the same subnetwork. The multicast addresses must be different.

In order to connect the FPA 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 6.2: Example of line numbering for the UGM-2040**

**Notice!**

Please note that you must assign the UGM-2040 server to each network node from which statuses should be transmitted.

## 7 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 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.

### Danger!

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 light-emitting diode, wavelength 650 nm, output < 2 mW, in accordance with DIN EN 60825-1:2003-10.

### 7.1

## Installing media converters in the mounting frame

Install the media converters in the corresponding FPM-5000-KMC bracket

  6x KB40 x 12 mm

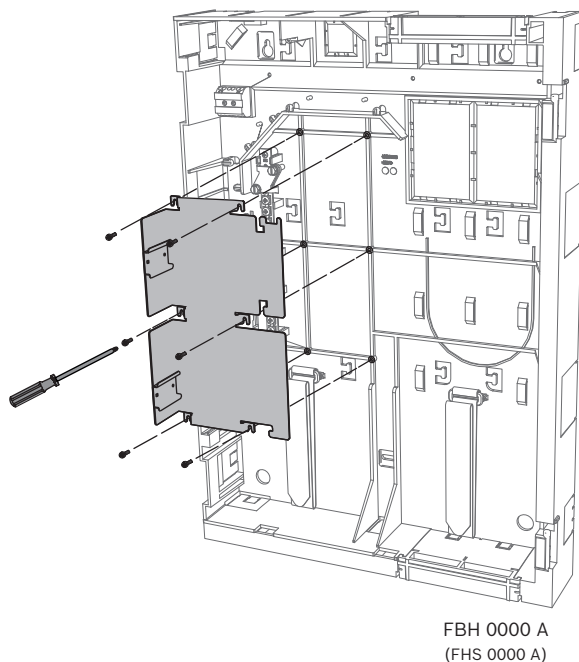


Figure 7.1: Installation of FPM-5000-KMC bracket in mounting frame

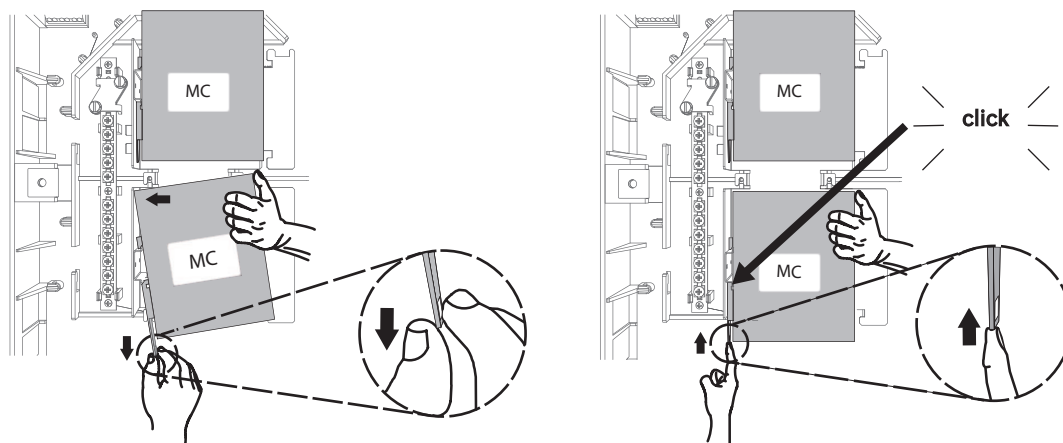


Figure 7.2: Installation of media converters in the FPM-5000-KMC bracket

## 7.2

### Installing media converters in PSS 0002 A/USF 0000 A

Install the media converters in the FPM-5000-KES. bracket

In the case of the USF 0000 A you need to remove the installed mounting plate.

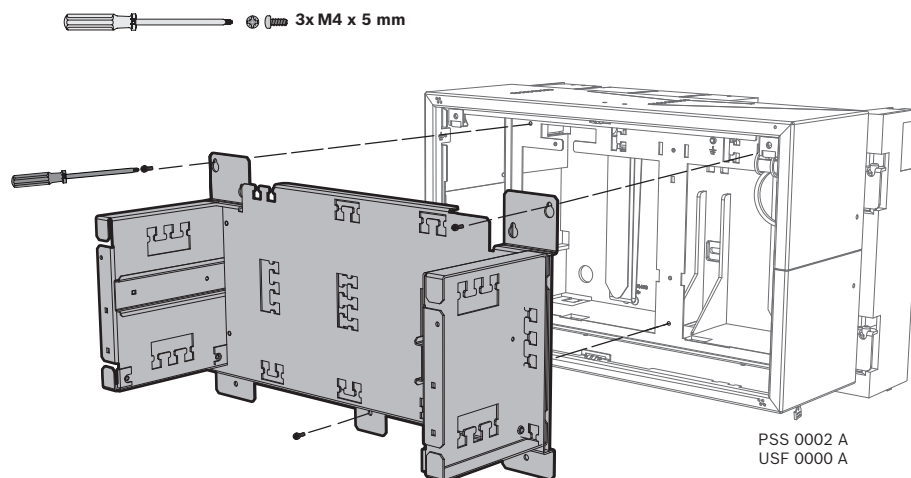


Figure 7.3: Installation of FPM-5000-KES bracket in housings

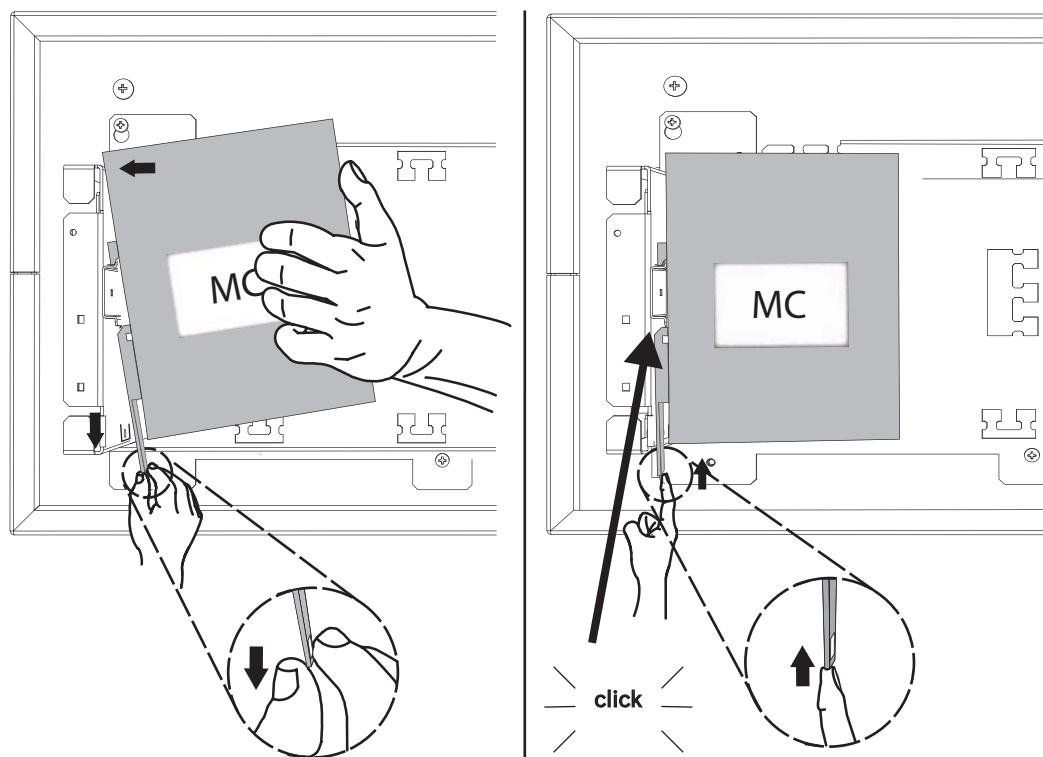


Figure 7.4: Installation of media converters in the FPM-5000-KES bracket

## 7.3

### 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)

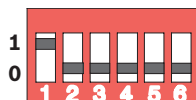
**Notice!**

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

## 7.4

### Installing switches in PSS 0002 A/USF 0000 A

**Notice!**

If you are using switches in the network, these must be included in the configuration in the FSP-5000-RPS programming software.

**Notice!**

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

Install the switches in the corresponding FPM-5000-KES. bracket

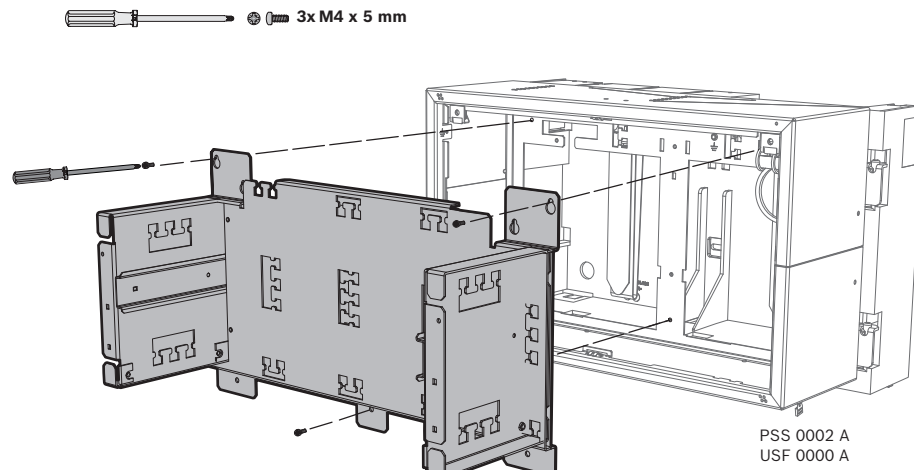


Figure 7.5: Installation of FPM-5000-KES bracket in housings

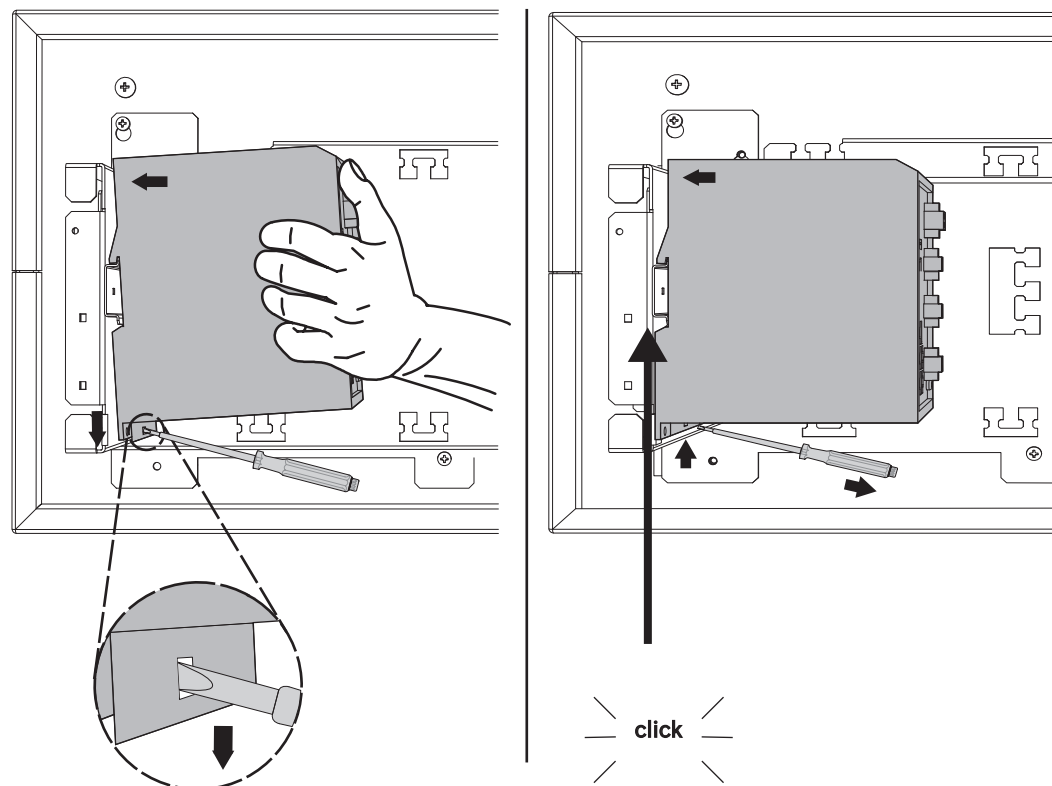


Figure 7.6: Installation of switches in the FPM-5000-KES bracket

## 7.5 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 46,
- Activating IGMP snooping, page 46.

**7.5.1****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 between the IP addresses of the panels and those of the switches.

**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. 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.

**7.5.2****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.

### 7.5.3

### 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.

## 7.5.4 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.

## 7.5.5 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.

## 7.5.6 Activating IGMP snooping

To prevent sending EN 54-2 relevant multicast traffic to other systems connected to the Hirschmann Rail Switch Rugged RSR20 (Praesideo/PAVIRO, Remote Connect) activate IGMP snooping.

On the IGMP configuration page of the Hirschmann Rail Switch Rugged RSR20 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.

## 7.6 CAN network

### Networking and Interfaces

The panel controller has

- two CAN interfaces (CAN1/CAN2) for networking (bus or loop topology)
- two signal inputs (IN1/IN2)
- two Ethernet interfaces
- USB and RS232 interfaces

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

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 whether

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

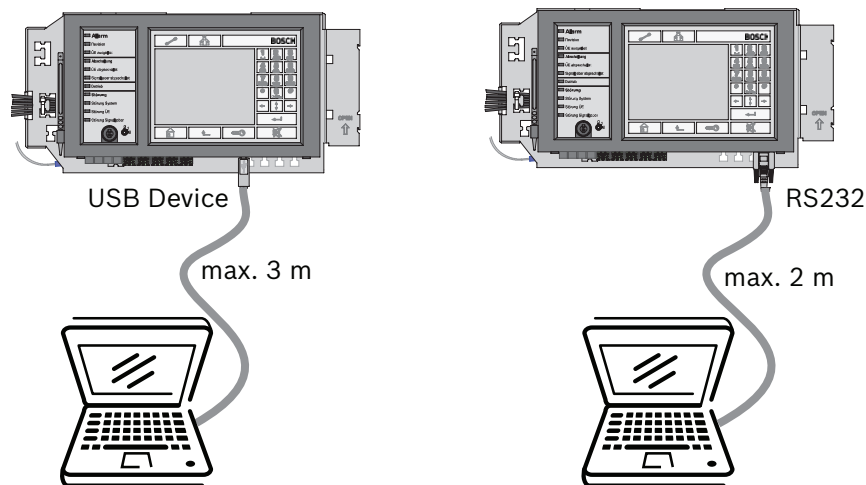


Figure 7.7: MPC, USB and RS232 interfaces

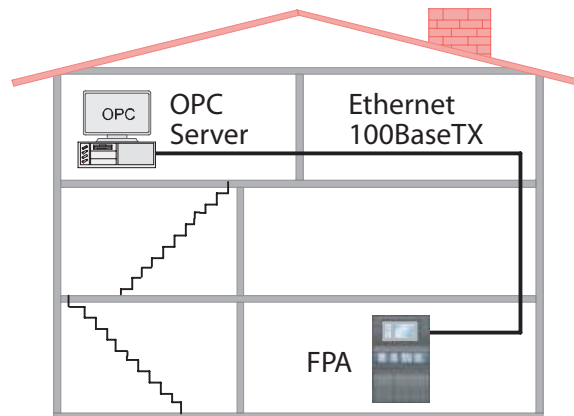
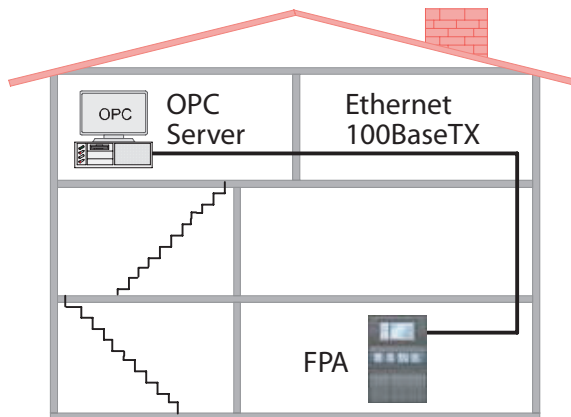


Figure 7.8: MPC connection to BIS via OPC server



**Figure 7.9: MPC connection to BIS via OPC server**

### Addressing and Settings in the Network

The following pages illustrate connections, addressing and the associated configuration via DIP switches for different loop and bus topologies:

- Standalone panel
- Standalone panel, redundant
- Loop topology
- Loop topology with redundant panel
- Bus Topology
- Bus topology with redundant panel
- Bus topology with redundant network
- Bus topology with redundant network and redundant panel

The panels and remote keypads are identified in the network by a unique address. This address is set on the rotary switches and is known as the rotary switch number (RSN) (see the figures in the circle on the circuit diagrams). The rotary switches are located on the rear of the panel controller (see *Addressing and Configuration of MPC Panel Controller, page 49*).

Note the address on the sign below the rotary switches (see *Addressing and Configuration of MPC Panel Controller, page 49, step 2*).

The DIP switches are located on the rear of the panel controller (see *Addressing and Configuration of MPC Panel Controller, page 49*).

Mark the selected setting on the sign above the DIP switches (see *Addressing and Configuration of MPC Panel Controller, page 49, step 4*).



### Notice!

Redundant panels must have the same RSN as the assigned primary panels.

## Addressing and Configuration of MPC Panel Controller

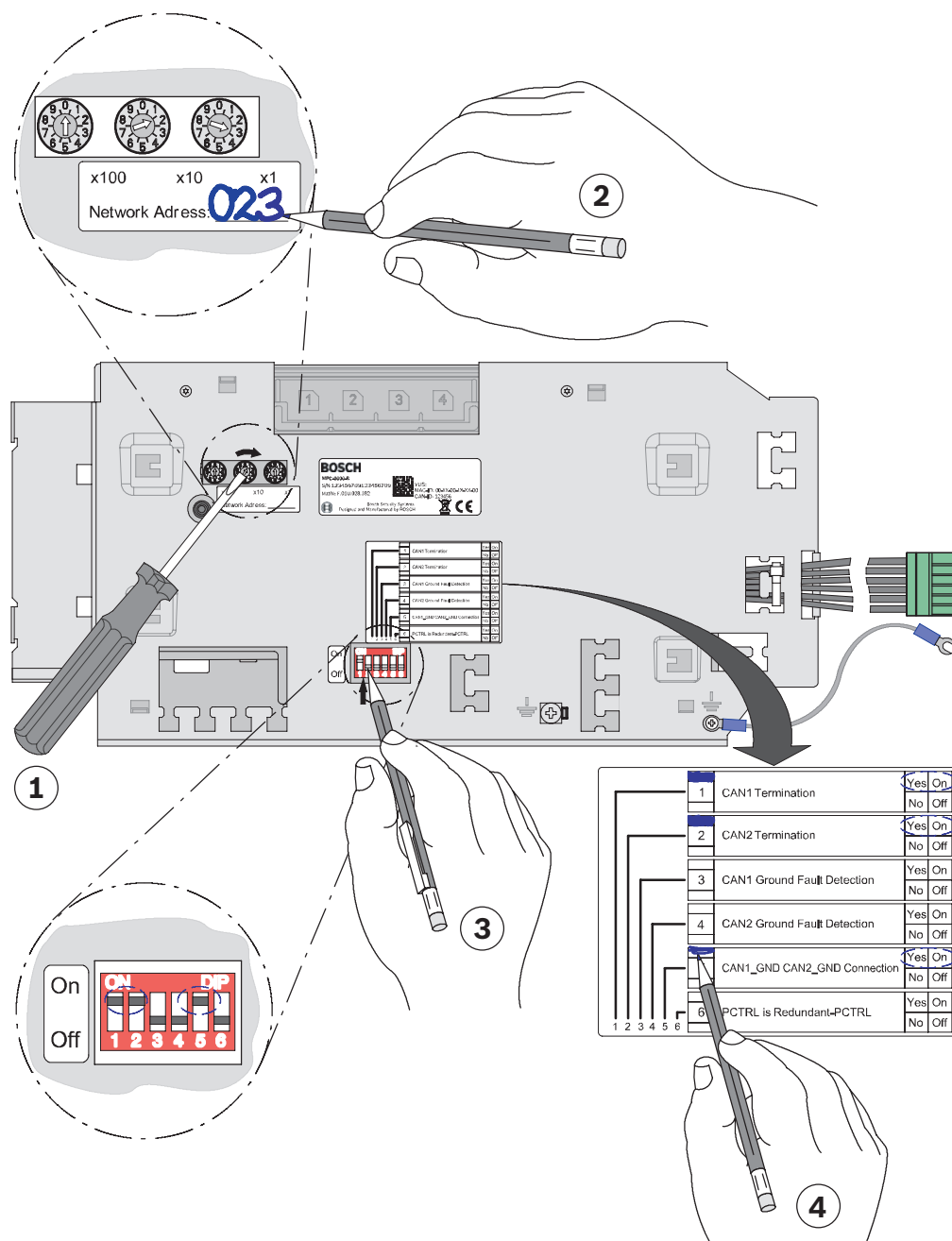


Figure 7.10: MPC Panel Controller, addressing

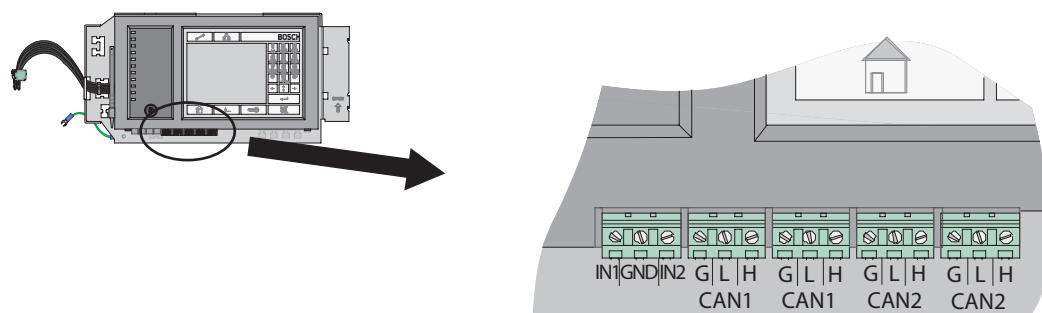


Figure 7.11: MPC Panel Controller, network connections

Standalone Panel and Redundant Standalone Panel

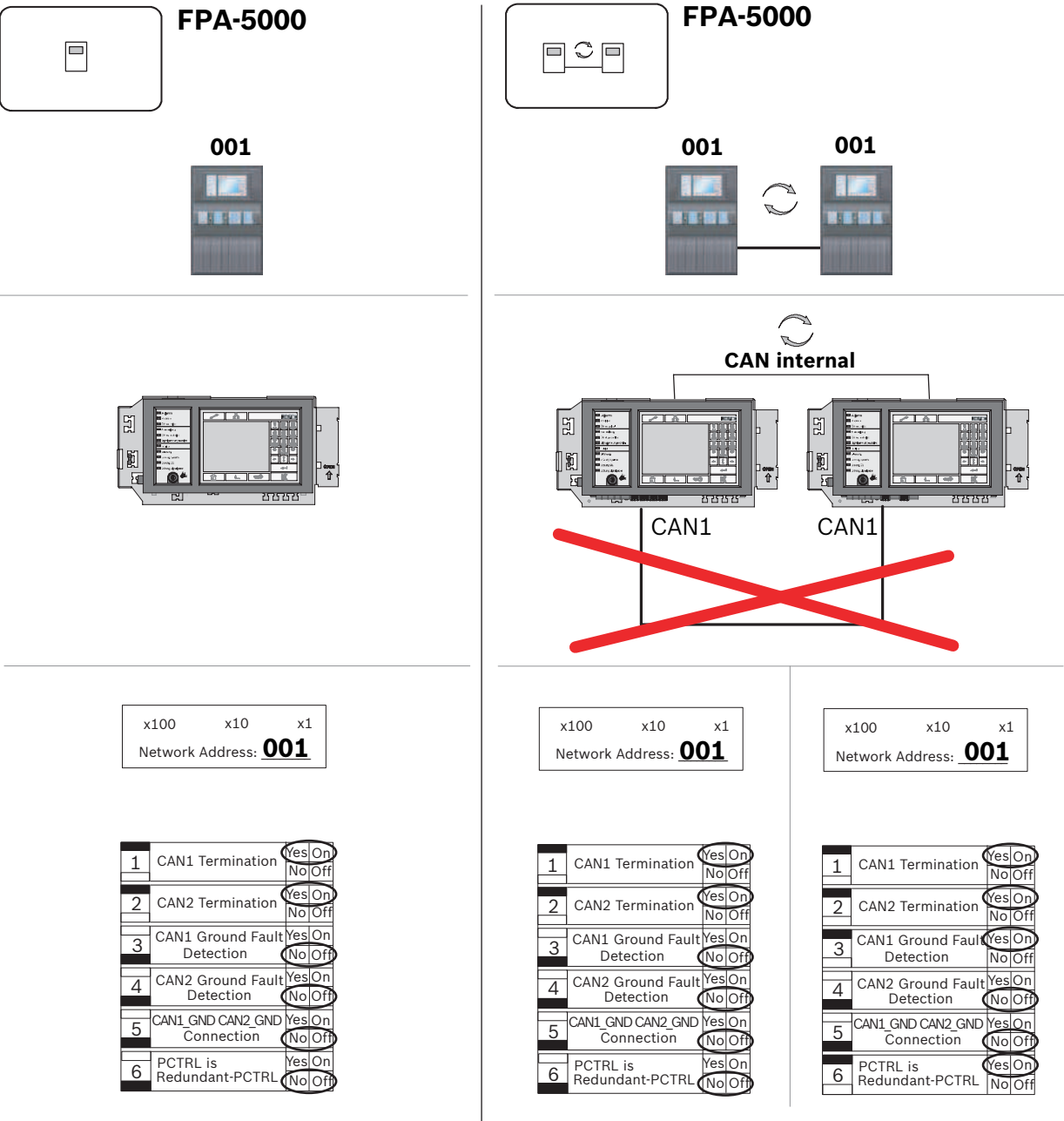


Figure 7.12: Standalone panel (regular and redundant): Configuration in network

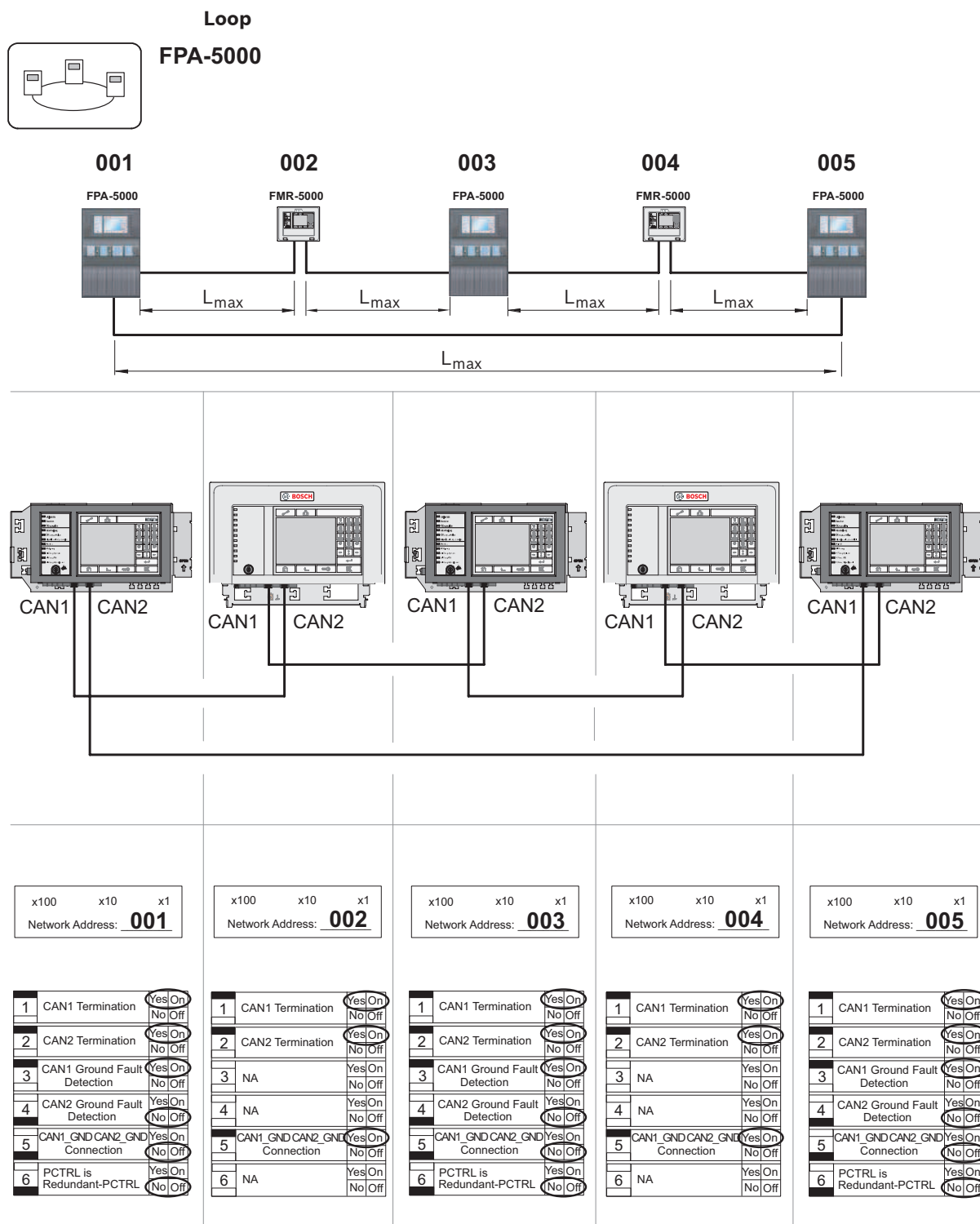


Figure 7.13: Loop topology

Loop with redundant panel

FPA-5000

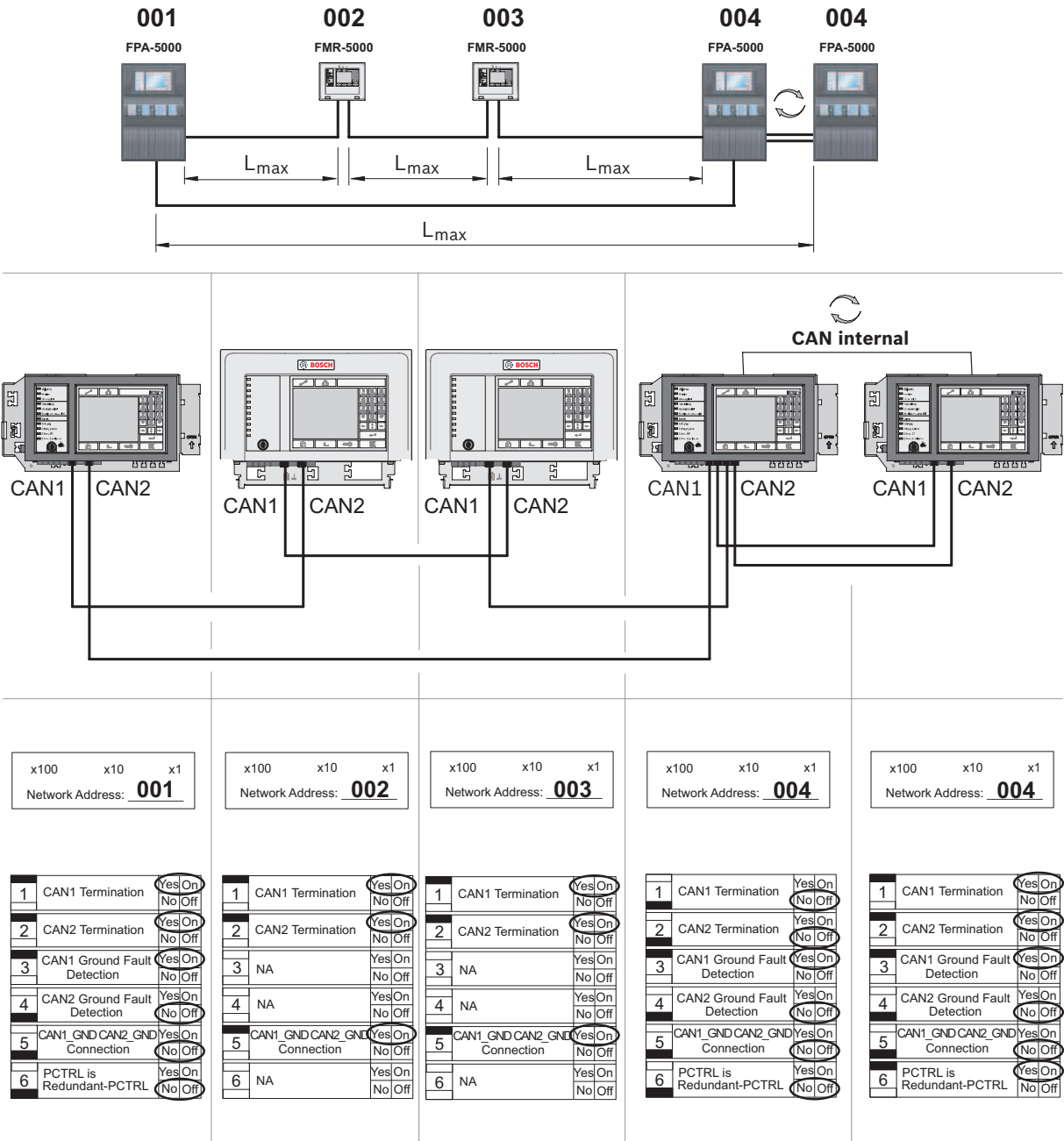
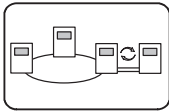


Figure 7.14: Loop topology with redundant panel



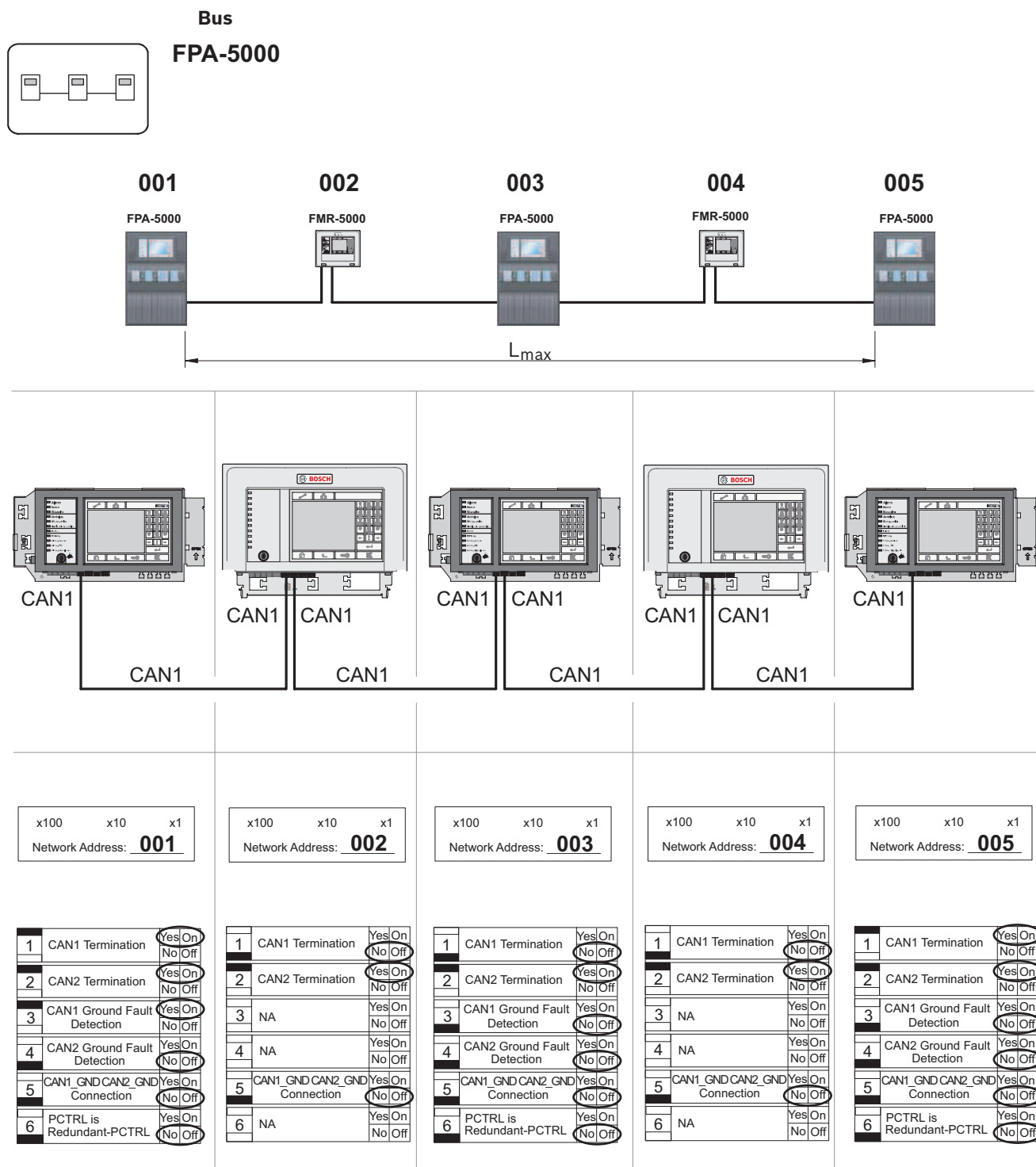


Figure 7.15: Bus Topology

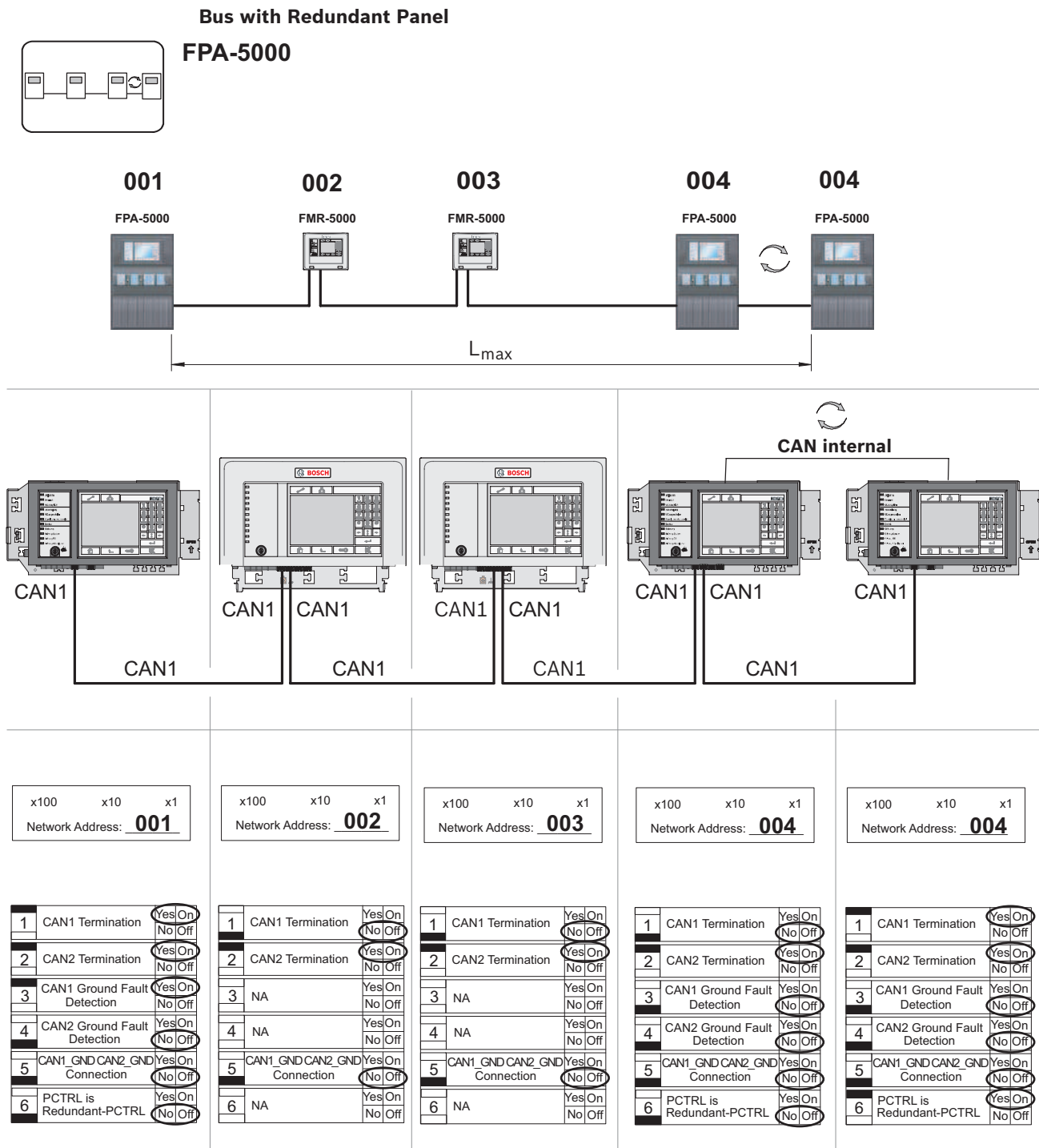
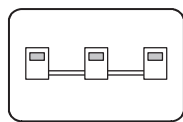


Figure 7.16: Bus topology with redundant panel

## Bus with Redundant Network



FPA-5000

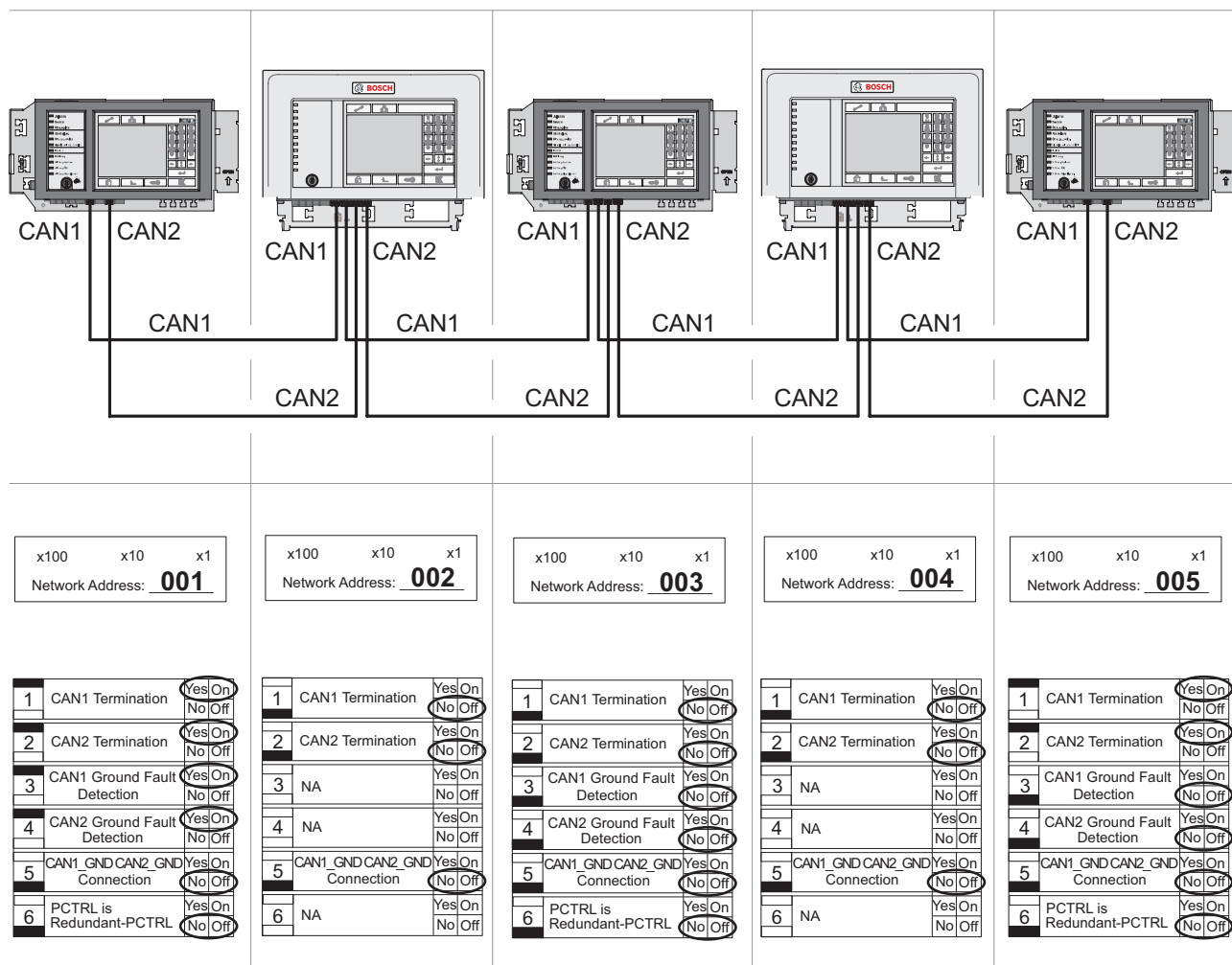
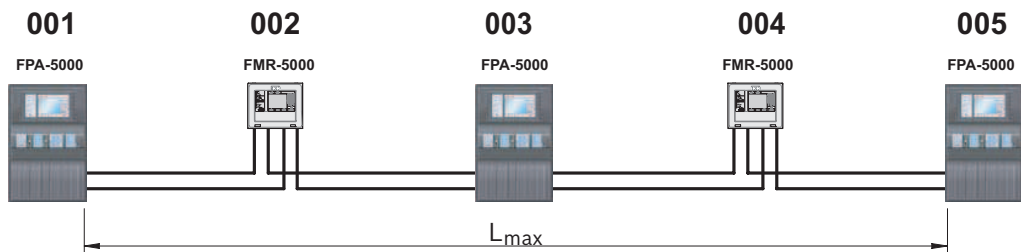


Figure 7.17: Bus topology with redundant network



## 8 Connections

In order to create an EN 54-2-compliant system, the switches and media converters must be connected via the monitored power supply of the fire alarm control panel.

- The 24 V output of either the BCM-0000-B or FPP-5000 must be used for the power supply to the media converters and switches.
- If you have connected a redundant power supply or are creating a switch-to-switch connection, then the fault outputs of the switch must be monitored via panel inputs. For example, use the inputs on the MPC 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.

### 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.



### 8.1 Cabling of panel controller

#### 8.1.1 Media converters and power supply

##### Connection of media converters

### Notice!

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



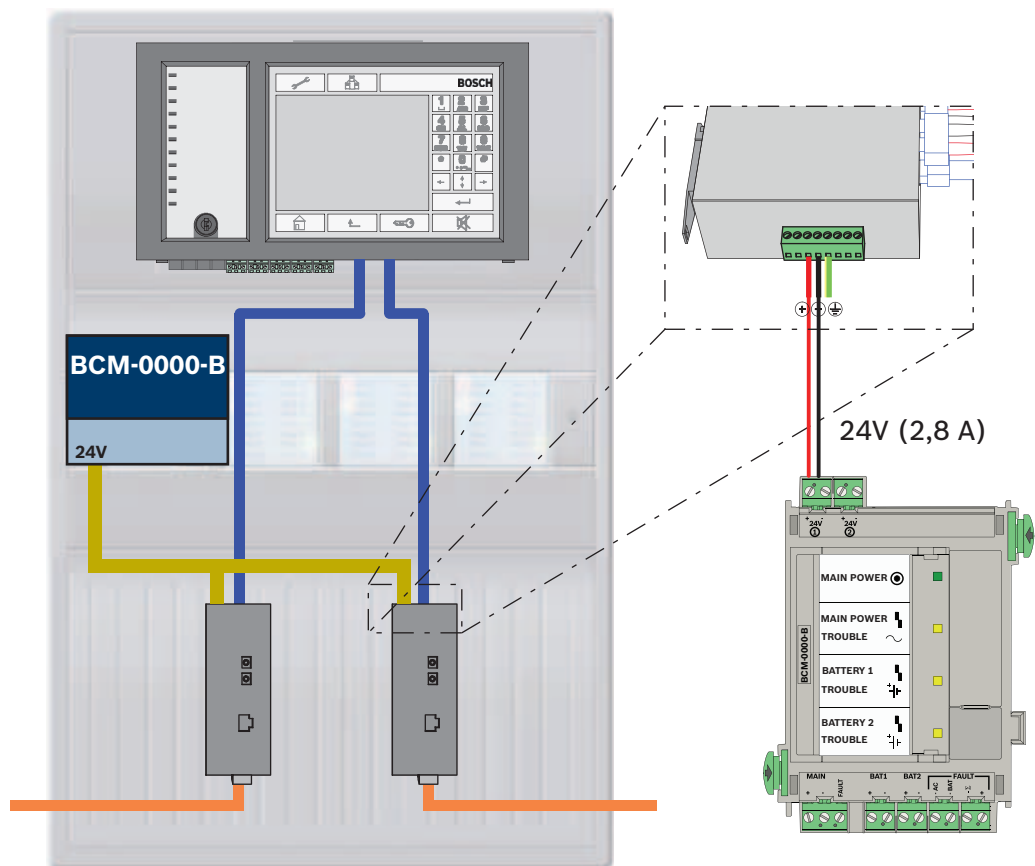


Figure 8.1: Connection of media converter to the power supply and panel controller

Icon	Description
	TX Ethernet cable (copper)
	FX Ethernet cable (fiber optic cable)
	24 V power supply
	Transmission of fault
	Media converter

## 8.2 Switch with power supply and fault relay



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

### Connection of switch

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



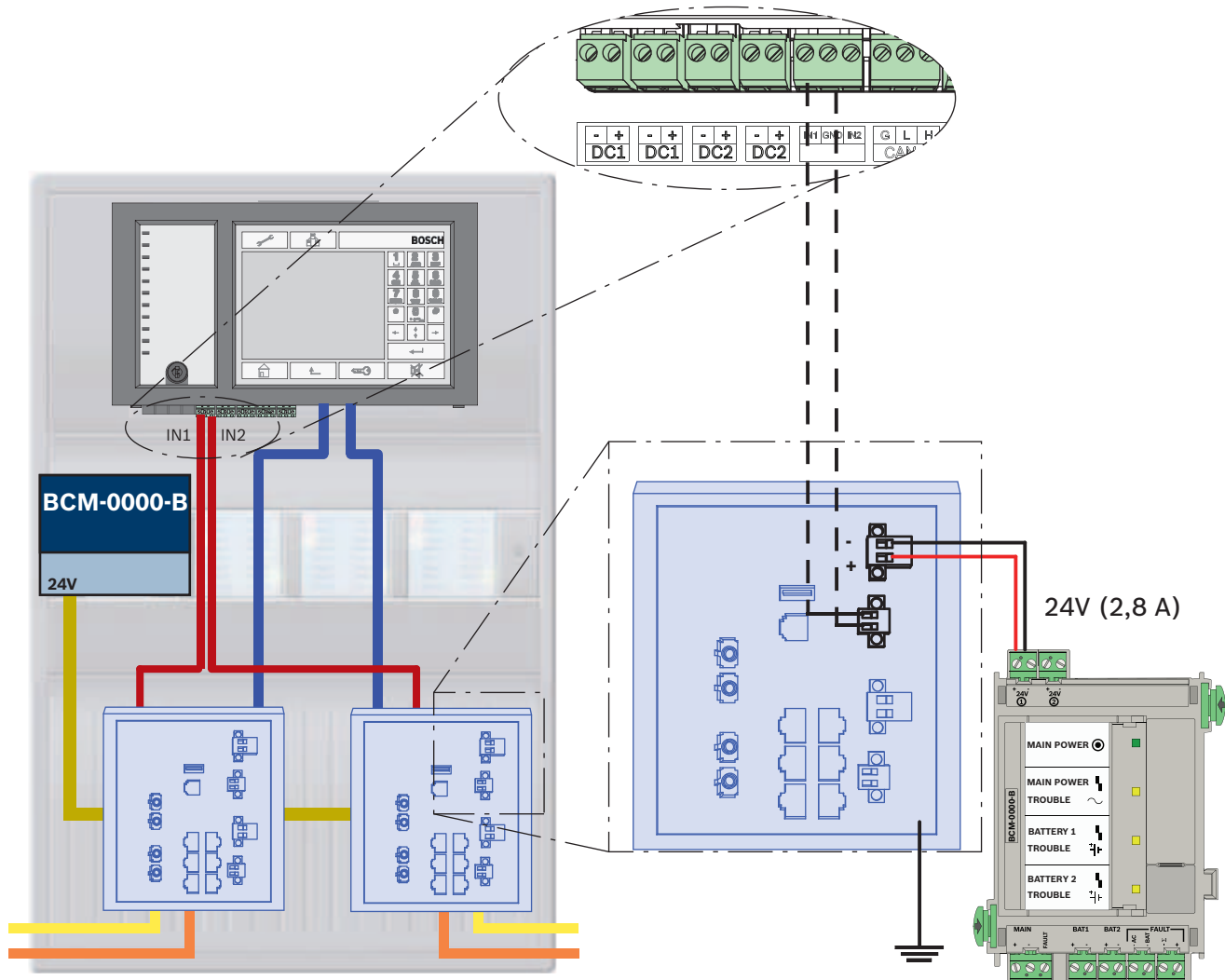
### Notice!

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 MPC inputs



**Figure 8.2: Connection of switch to the power supply and panel controller**

Icon	Description
	TX Ethernet cable (copper)
	FX Ethernet cable (fiber optic cable)
	24 V power supply
	Transmission of fault
	Switch

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

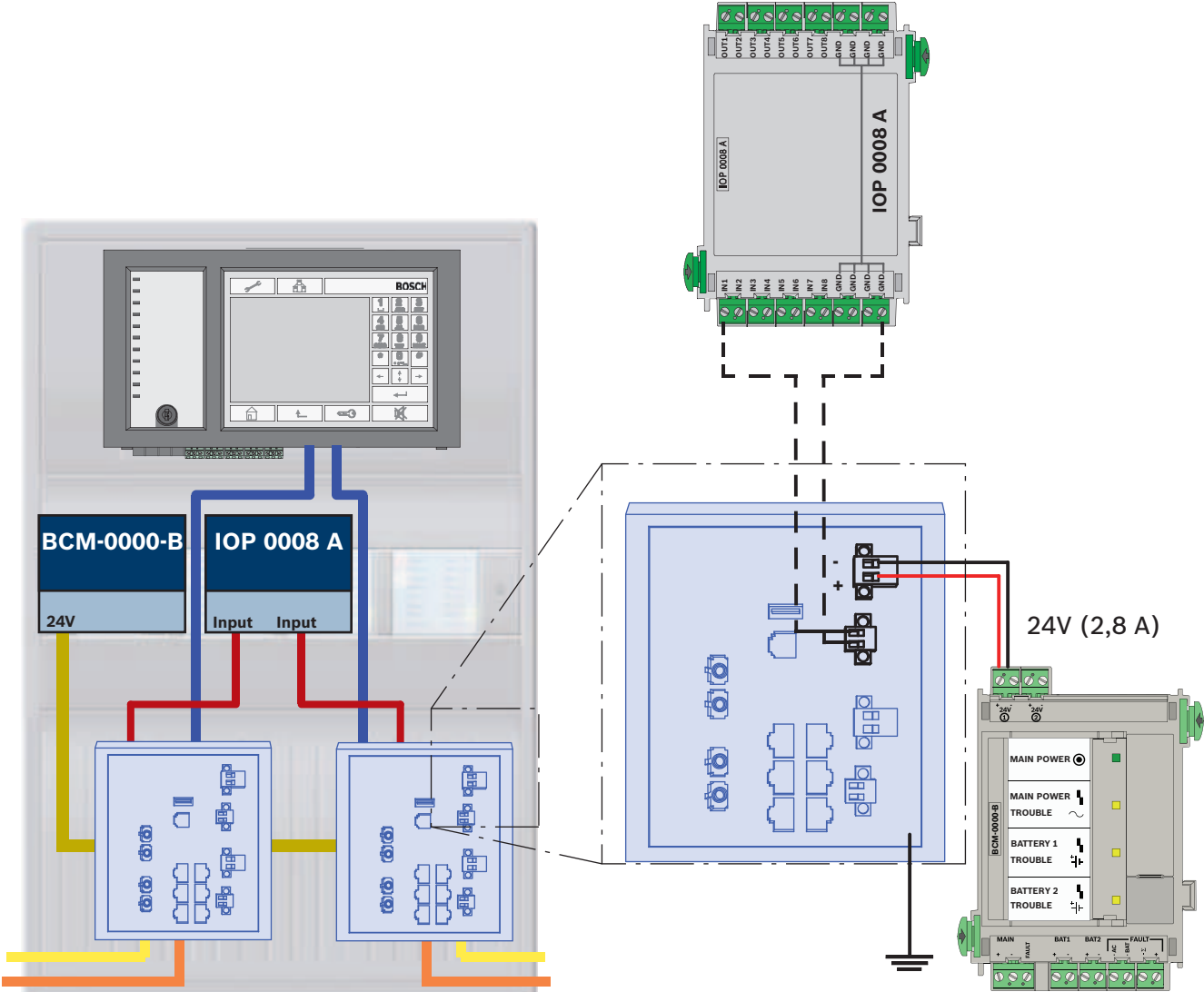


Figure 8.3: Connection of switch to the power supply and IOP

Icon	Description
	TX Ethernet cable (copper)
	FX Ethernet cable (fiber optic cable)
	24 V power supply
	Transmission of fault
	Switch

8.3 Cabling of FMR-5000 remote control unit

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



**Notice!**

Please note that in accordance with EN 54-13 the FPP-5000 external power supply unit and the PSF 0002 A (PSS 0002 A) must be installed in the immediate vicinity (without intermediate space) of the FMR-xxxx remote control unit. It must not be possible to touch the connecting cables between the components, as they are not monitored as per EN 54-13.

**Notice!**

Use only media converters to connect a FMR-5000 remote control unit to an Ethernet panel network.

The use of switches is not permitted for the remote control unit.

**Notice!**

The functional earth of the FMR-5000 remote control unit must always be placed in position when connecting the unit to an Ethernet panel network.

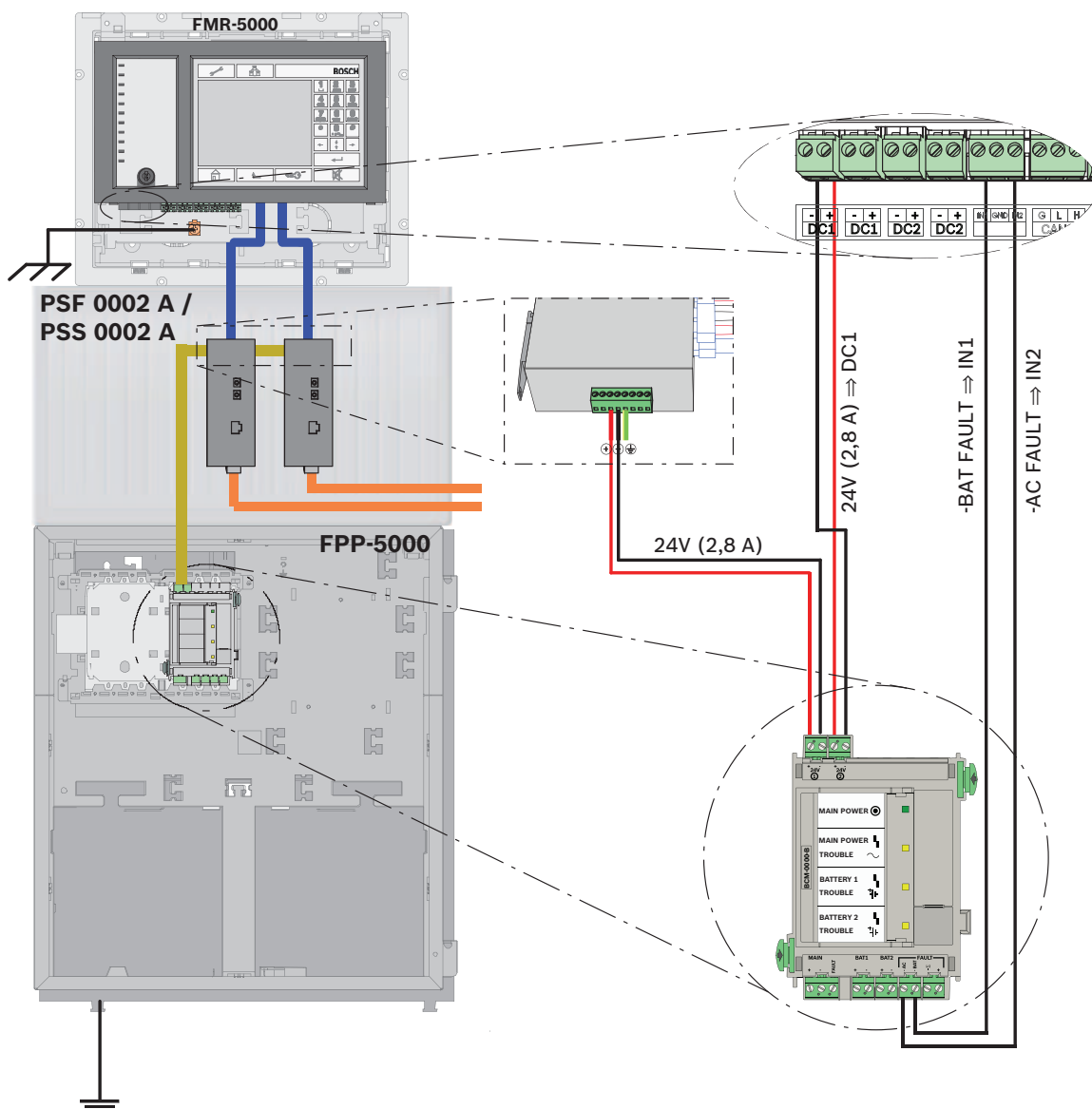






Figure 8.4: Cabling of remote control unit

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

## 9 Appendix

### 9.1 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	<b>General Network Trouble</b>	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	<b>Duplicate IP Address</b>	An IP address has been assigned twice.
135.0.6.2	Network 2.2	<b>IP Settings</b>	The IP configuration of the reporting panel is different to the RPS configuration
135.0.6.3	Network 2.3	<b>Redundancy Settings</b>	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	<b>RSTP Fallback</b>	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	<b>RSTP Topology Change</b>	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	<b>RSTP Link Type Point2Point</b>	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	<b>CAN 1 Trouble</b>	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	<b>CAN 2 Trouble</b>	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	<b>Ethernet 1 Trouble</b>	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	<b>Ethernet 2 Trouble</b>	Data transmission to Ethernet line 2 is restricted. Possible causes include: cable breaks, cable not connected, cable interference.

# Index

## A

Addressing	48
Rotary switch	48

## B

Bus topology	48
--------------	----

## C

CAN interface	29, 47
CAN network	11
Condition Monitoring	25

## D

DIP switches	48
--------------	----

## E

EffiLink	26
Ethernet interface	47
Ethernet network	11
Ethernet topologies	12
Ethernet, standard settings	13

## F

Fiber optic cables	
EKS	29

## L

Limits: Network	29
LLDP	8
Loop topology	48

## M

MAC address	8
Maximum limits	29

## N

Network	
Addressing	51
Cable	30
Fiber optic cable	29
Limits	29
Network diameter	8
Network: Cabling	30
Network: Panel controller	47
Networking	29, 48
Bus topology	48
Cable length	29
Loop topology	29, 48
Networking over CAN	11
Networking over TCP/IP	11

## O

OPC Server	11, 47
------------	--------

## P

Panel controller	
Networking	47
Parameters	
RSTP	13
PAVIRO	11, 24, 31
Praesideo	11, 24, 31

## R

Redundancy	
Addressing	48
Redundant	48
Remote Connect	33
Remote Portal	33
Remote Services	33
Connect Secure Network Gateway	33
Seperating sub-networks	34
Rotary switch	48
Rotary switch number (RSN)	48
RS232 interface	47
RSTP	8
RSTP parameters	13

## S

Secure Network Gateway	33
Services	11
Standard settings, Ethernet	13

## T

Teleservice EffiLink	26
Topologies, Ethernet	12
Topology: Bus	48
Topology: Loop	48

## U

USB interface	47
---------------	----

## V

Voice alarm system	24, 31
--------------------	--------





**Bosch Sicherheitssysteme GmbH**

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Sicherheitssysteme GmbH, 2016