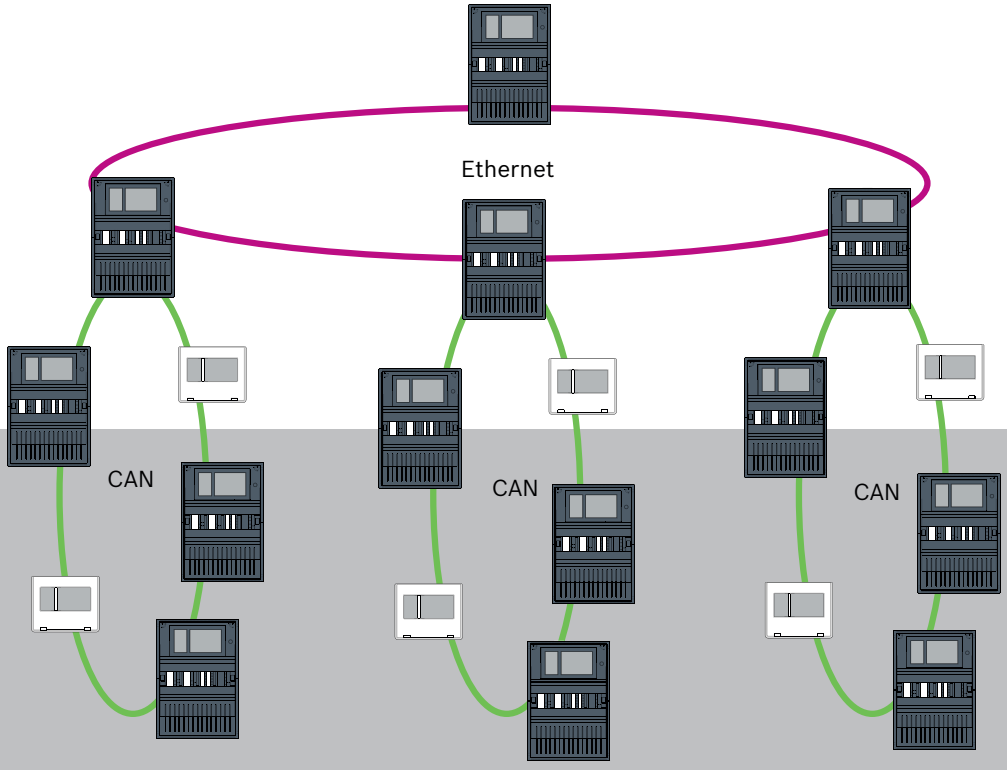
AVENAR panel



en Networking manual

Table of contents

1	**Safety**	**5**
1.1	Organizational measures for PC running service clients	5
1.2	Explanations of safety symbols	6
1.3	Safety notices	6
2	**Introduction**	**7**
3	**System overview**	**8**
4	**Topologies**	**9**
4.1	CAN loop	13
4.2	Ethernet loop	14
4.3	Ethernet/CAN double loop	14
4.4	CAN loop with Ethernet segments	14
4.5	Ethernet backbone with sub-loops (Ethernet/CAN)	14
4.6	Connecting Ethernet loops	16
5	**Ethernet network**	**17**
5.1	Network diameter	17
5.2	Cables used	19
5.3	Creating or modifying an Ethernet network	20
6	**CAN network**	**21**
6.1	Creating or modifying a CAN network	22
7	**Ethernet and CAN networking pattern**	**22**
7.1	Panel network over Ethernet	24
7.2	Panel network over CAN	24
7.3	Connect services to panel	24
7.4	Panel network over Ethernet with redundant panels	25
7.5	Panel network over CAN with redundant panels	25
7.6	Panel network over two Ethernet loops	26
7.7	Panel network over two Ethernet loops with redundant panels	26
7.8	Connect Ethernet and CAN network with redundant panels	26
7.9	Connect remote services to redundant panels	27
7.10	Connect life safety services to redundant panels	27
8	**Remote Services**	**28**
8.1	Preconditions for Remote Services	28
8.1.1	Remote Connect	28
8.1.2	Fire System Explorer	31
8.2	Remote Alert	32
8.3	Remote Maintenance	32
8.4	Remote Maintenance for Private Secure Network	33
9	**Building management system**	**34**
10	**Smart Safety Link**	**36**
10.1	One direct VAS interface	37
10.1.1	Praesideo and PAVIRO	37
10.1.2	PRAESENSA	38
10.2	Multiple direct VAS interfaces	39
10.3	VAS integrated in Ethernet panel network	40
11	**Hierarchy panel**	**41**
12	**Installation**	**42**
12.1	Settings on media converter	42
12.2	Installing external Ethernet switch BRS20	44
12.2.1	Configure external Ethernet switch	44
12.2.2	Configure RSTP	45
12.2.3	Enable QoS priority	45

12.2.4	Activate IGMP snooping	45
12.2.5	Configure fault relays	45
12.2.6	Configure connection monitoring	46
12.2.7	Configure security settings	46
12.2.8	Configure system information	46
12.2.9	Change IP address	46
12.3	CAN network	47
13	**Ethernet cabling**	**50**
13.1	Media converter	51
13.2	External Ethernet switch	52
13.3	Remote keypad	55
14	**FSP-5000-RPS settings**	**57**
14.1	Network nodes	57
14.2	Line numbers	57
14.3	Switches	58
15	**Appendix**	**58**
15.1	Ethernet error messages	58
	Index	**60**

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!
A caution tells you that there is a risk of damage to objects.



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 (Remote Assistant). Remote Services for Private Secure Network is only available in Germany with a service agreement with Bosch BT-IE.

Caution!
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.

Smart Safety Link

Notice!
VdS 2540
When connecting a voice alarm system to a panel using Smart Safety Link the system must be installed in the same room as the fire panel and positioned directly adjacent to it. Otherwise, the requirements of VdS 2540 regarding data transmission paths are not fulfilled.

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 Ethernet 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 - Ethernet network
Consider for Ethernet panel networks, that for installations in Germany, where compliance to VdS 2540 is required, fiber optic cable has to be used for all data transmission paths. The only exception is inside a housing.

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

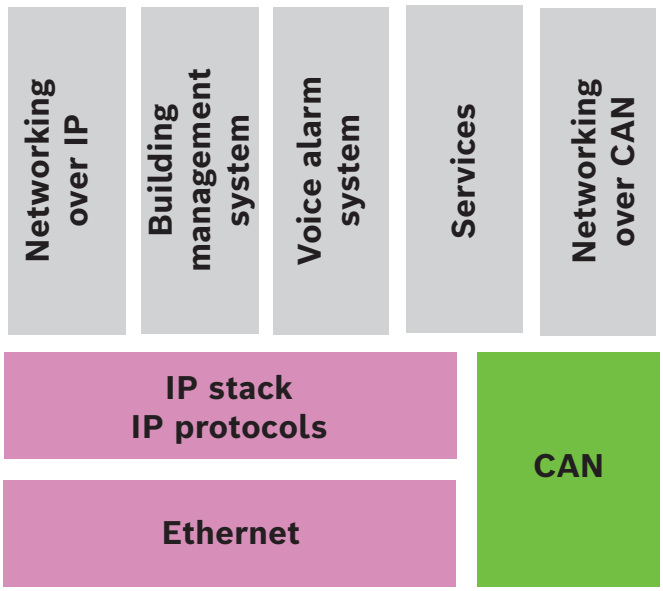
This document is aimed at readers with experience in planning and installing EN 54 compliant fire alarm systems. In addition, you need networking knowledge.
This document describes a variety of fire alarm network topologies. The topologies are described independently of the fire panel type.
For building 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 be 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

Caution!
Risk of cybersecurity
Install and run the latest firmware version, especially when the panel is connected to an Ethernet network. This action reduces cybersecurity risk.

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.



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 via TCP/IP
  In FSP-5000-RPS, enable panel-to-panel communication in the Ethernet network
- Building management system
  Create a server in the FSP-5000-RPS configuration
- Voice Alarm System 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)

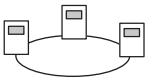
Activate the relevant check box in FSP-5000-RPS

– 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 the building management system, or for OPC server, or for Remote Services, then 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.

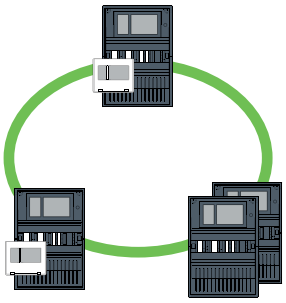
Network of panels and remote keypads
The table shows the options for networking panels/remote keypads depending on the network topology and the panel type. Consider the limits determined by the network topology.

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	Max. 32 panels/ remote keypads, connectivity with AVENAR panel 2000, premium license	Max. 32 panels/ remote keypads, connectivity with AVENAR panel 8000	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

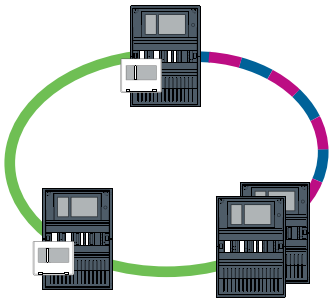
4 Topologies

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

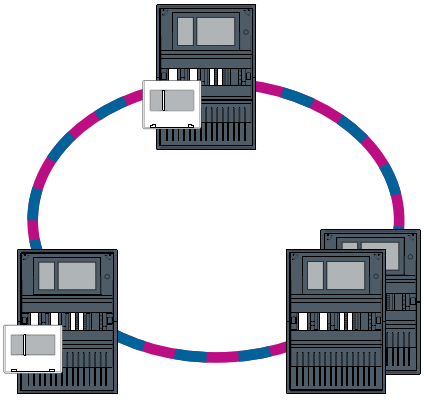
Notice!
Applicable topologies
The functionality and panel-to-panel communication is limited by the panel type. Refer to the panel specification for information on services, for number of connectable panels and for number of connectable remote keypads.



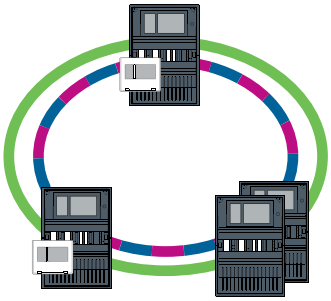
CAN loop, page 13



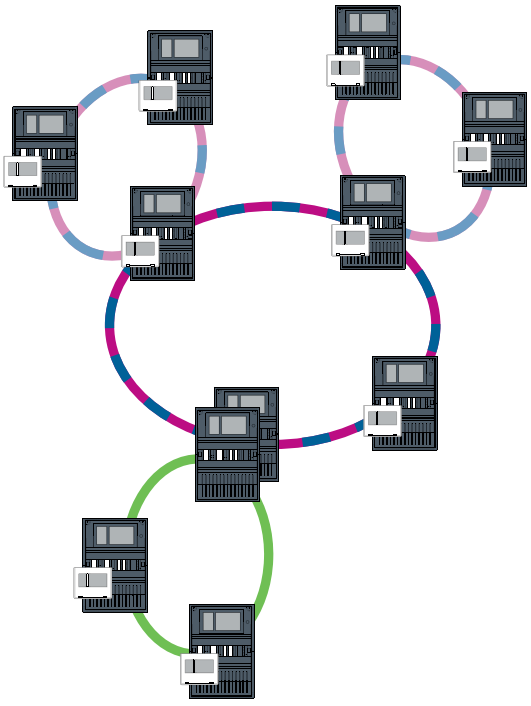
CAN loop with Ethernet segments, page 14



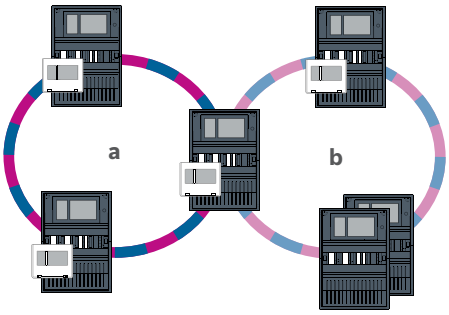
Ethernet loop, page 14



Ethernet/CAN double loop, page 14

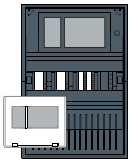
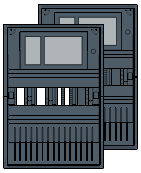
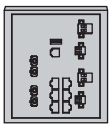


Ethernet backbone with sub-loops (Ethernet/ CAN), page 14



Connecting Ethernet loops, page 16

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 Ethernet switch each)
	Panel or redundant panel (in Ethernet topology internal Ethernet 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.
	External Ethernet switch
	Media converter
	Secure Network Gateway for Remote Services
	Building management system

Limits in network

The network contains nodes.

- A node is either a panel controller, a remote keypad or a server (BACnet server, FSI server, OPC server or UGM server).
- The number of nodes is limited to 32
- The number of logical points per network is limited to 32768.
- The number of logical points per panel operated in a network is limited to to 2048.
- The number of remote keypads that can be assigned to one panel is limited to 3.
- The number of servers that can be assigned to one panel or remote keypad is limited to:
  - 1 BACnet server
  - 2 FSI server
  - 1 OPC server
  - 2 UGM server

For further information see the system limits given in the System manual.

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, a remote keypad or a server 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 Ethernet 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 alarm 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 alarm points are connected in the sub-loop, then you have to design the panel and Ethernet network redundantly. The external Ethernet switch which connects 2 loops performs the redundancy.

Notice!
Number logical points
For a standalone panel you can connect up to 4096 logical points, even though it is designed redundantly. If the panel is included in a network, then you can connect a maximum of 2048 logical 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 Ethernet switches with RSTP enabled.
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 external Ethernet switches with RSTP enabled count as RSTP switches. Redundant panel controllers do not count as RSTP switches.
- 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 17*.
- External 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.

4.1 CAN loop

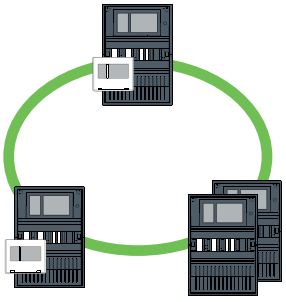


Figure 4.1: CAN loop

4.2 Ethernet loop

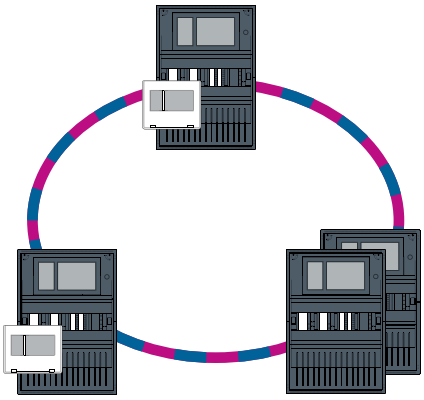


Figure 4.2: Ethernet loop

4.3 Ethernet/CAN double loop

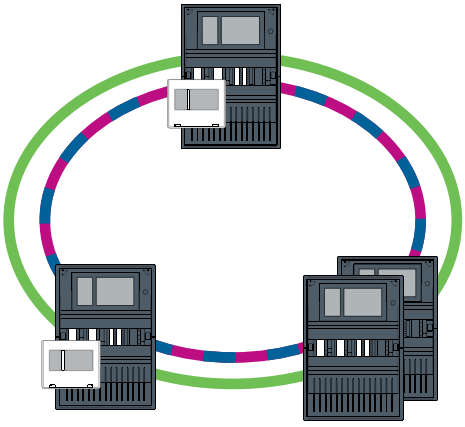


Figure 4.3: Double loop of Ethernet and CAN

4.4 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.

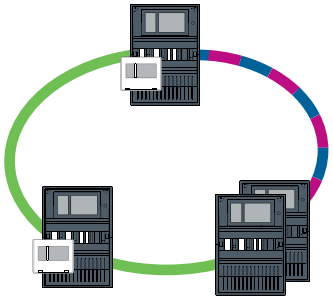


Figure 4.4: CAN loop with Ethernet segments

4.5 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 external Ethernet switches with RSTP enabled count as RSTP switches. CAN-networked panels are not counted 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 alarm 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.

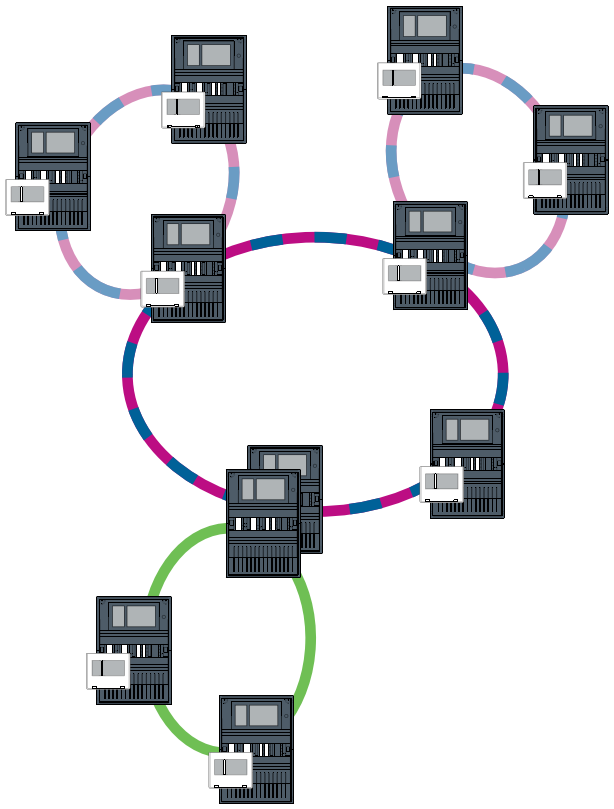


Figure 4.5: Ethernet backbone with sub-loops

4.6 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.

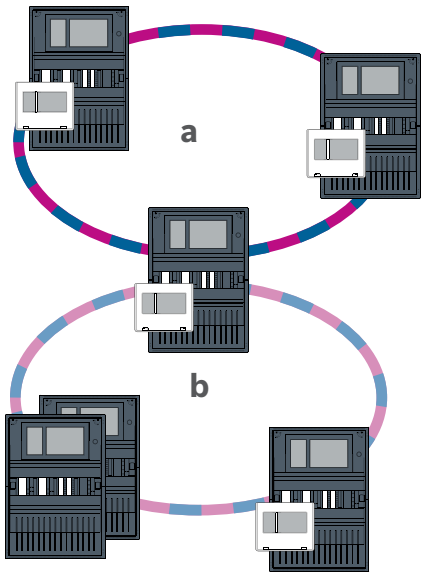


Figure 4.6: Connecting Ethernet loops via a non-redundant panel

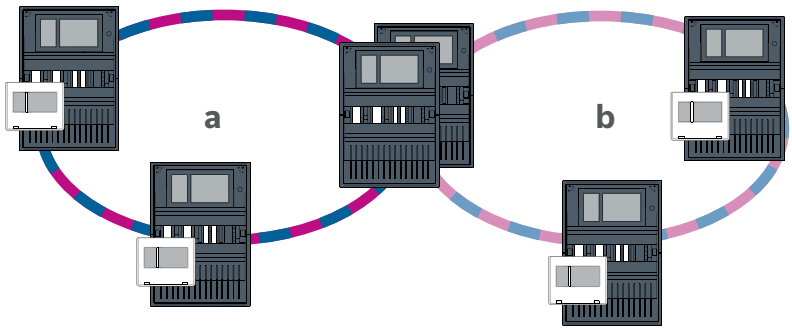


Figure 4.7: Connection Ethernet looos via a redundant panel

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

Rules for using 4 Ethernet ports

The internal switch of the panel controller has four Ethernet ports. Bosch supports only networks that are built according to the following rules in the specified order:

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 a building management system, a voice alarm system, or a hierarchy panel you have to use ETH3. You may connect an external Ethernet 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 a building management system, a voice alarm system, or a hierarchy panel.
4. If there is no panel networking via ETH1 and ETH2, then each can be used for connecting a building management system, a voice alarm system, or a hierarchy panel.

5.1 Network diameter

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

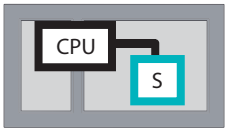
Definition

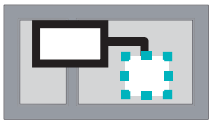
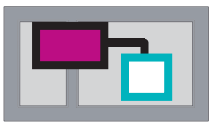
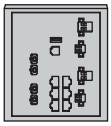
The diameter of a network corresponds to the number of RSTP switches on the longest possible section without loops between any 2 end points in the network.

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.
- Building management systems are not taken into account with respect to the diameter.

Key

	Central processor in the panel controller or in the remote keypad.
	Internal Ethernet switch with RSTP enabled 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.
	External Ethernet switch with RSTP enabled

Two connected panels form the smallest possible loop. The network diameter is two. The internal RSTP switches are between the end points.

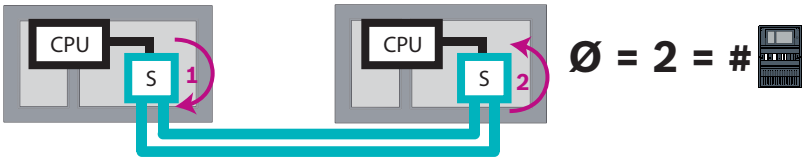


Figure 5.1: Network diameter of a loop with two panels

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

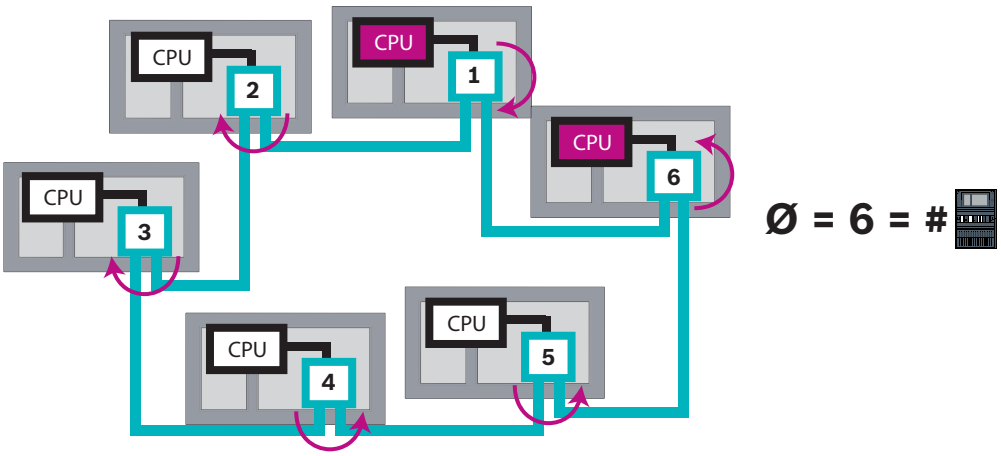


Figure 5.2: Network diameter of a loop with six panels

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

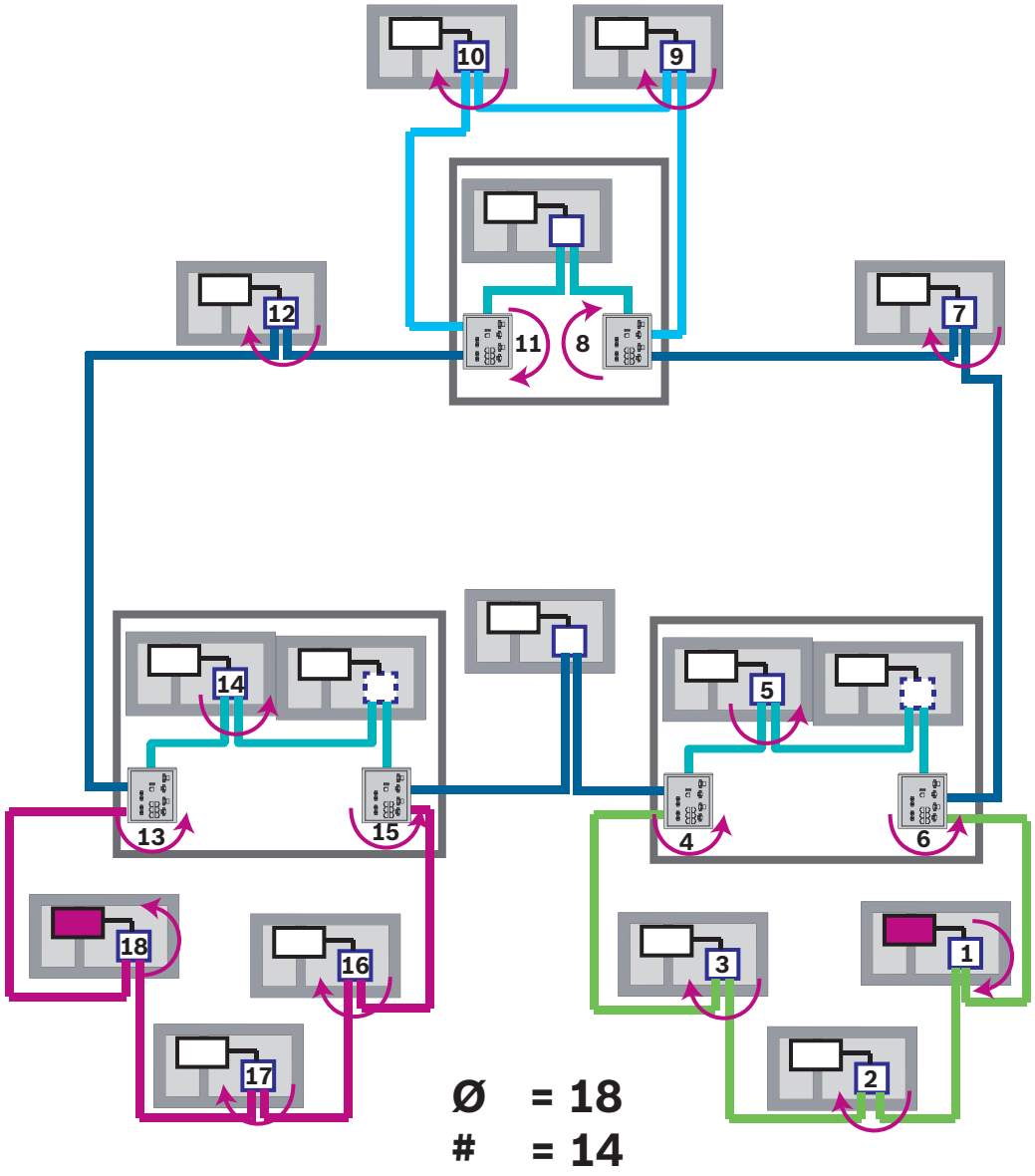


Figure 5.3: Network diameter of a backbone with sub-loops
The figure shows, for the diameter you have to find the longest path.

5.2 Cables used

Use only the following cables for Ethernet 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 - Ethernet network
Consider for Ethernet panel networks, that for installations in Germany, where compliance to VdS 2540 is required, fiber optic cable has to be used for all data transmission paths. The only exception is inside a housing.

5.3 Creating or modifying an Ethernet network

There are several procedures for creating an Ethernet network of fire alarm control panels. The two 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
The internal switch of the panel controller has four Ethernet ports. Bosch supports only networks that are built according to the following rules in the specified order:

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 a building management system, a voice alarm system, or a hierarchy panel you have to use ETH3. You may connect an external Ethernet 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 a building management system, a voice alarm system, or a hierarchy panel.
4. If there is no panel networking via ETH1 and ETH2, then each can be used for connecting a building management system, a voice alarm system, or a hierarchy panel.

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.

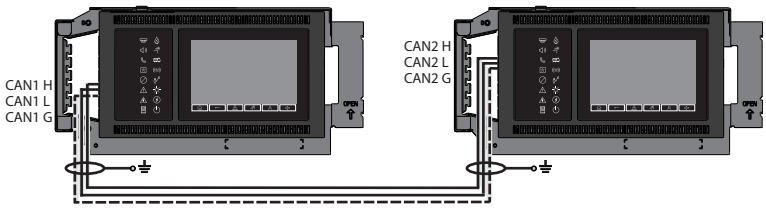


Figure 6.1: CAN connection

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.

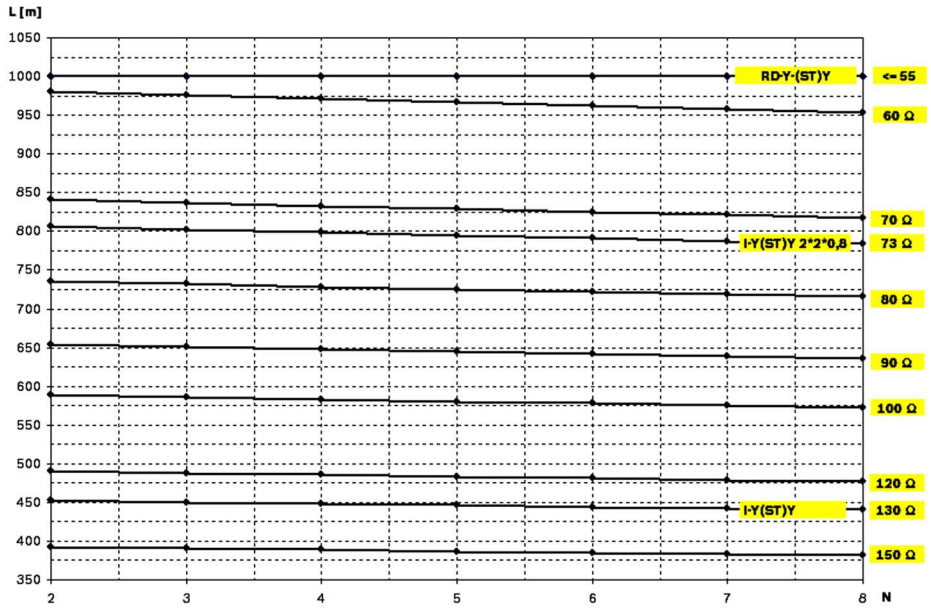


Figure 6.2: CAN network: Achievable cable length, depending on the number of nodes and the cable resistance

L = cable length in meters

N = number of nodes

6.1 Creating or modifying a CAN network

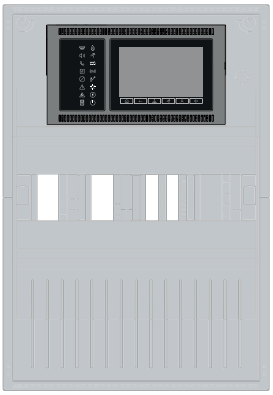
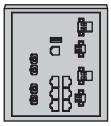
This procedure is suitable for projects involving only a small number of engineers working on the installation of the fire alarm system concurrently.

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
	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
	External Ethernet switch
	Media converter
	Secure Network Gateway for Remote Services
	Connection to building management system, voice alarm system or hierarchy panel

7.1 Panel network over Ethernet

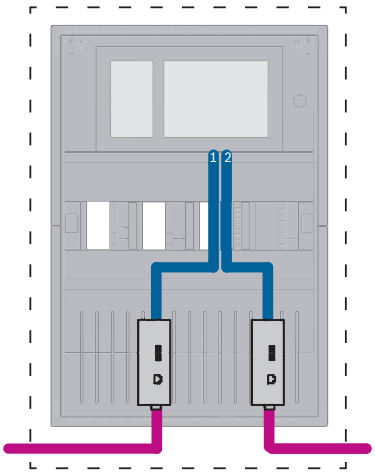


Figure 7.1: Panel network over Ethernet

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

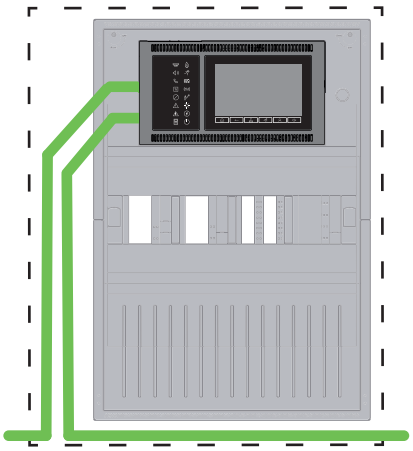


Figure 7.2: Panel network over CAN

7.3 Connect services to panel

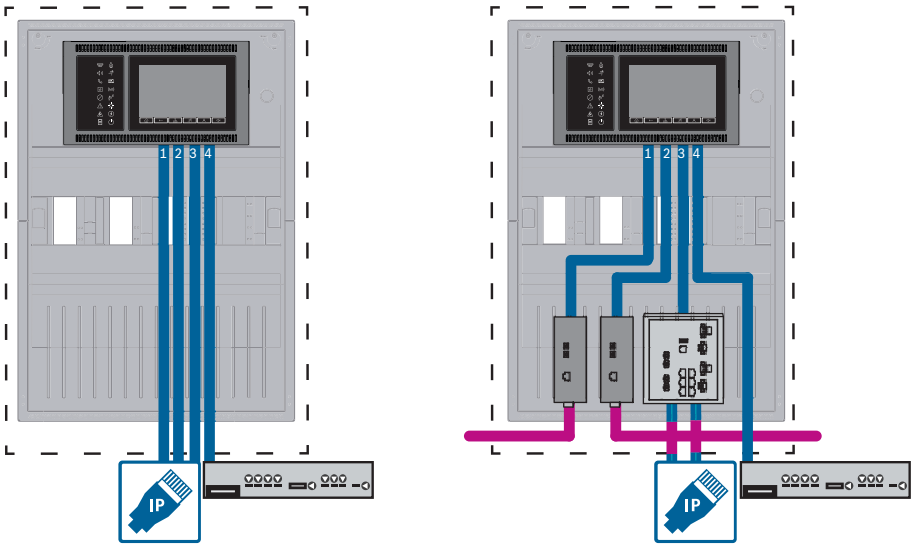


Figure 7.3: Left side: without panel network, Right side: with panel network

Only for more than two services connected to the panel, the external Ethernet switch is required.
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

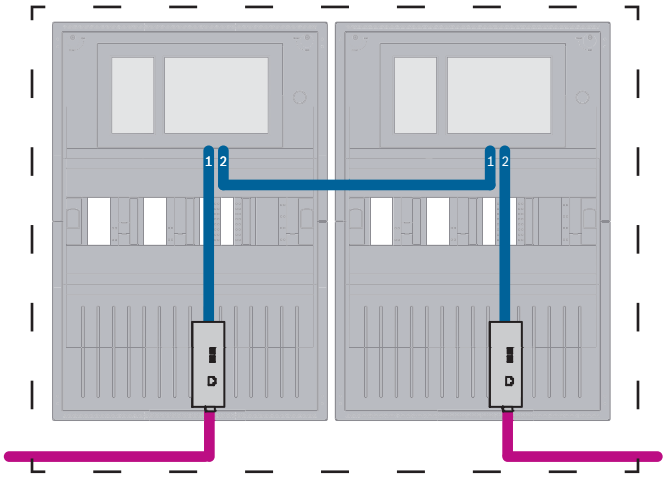


Figure 7.4: Panel network over Ethernet with redundant panels

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

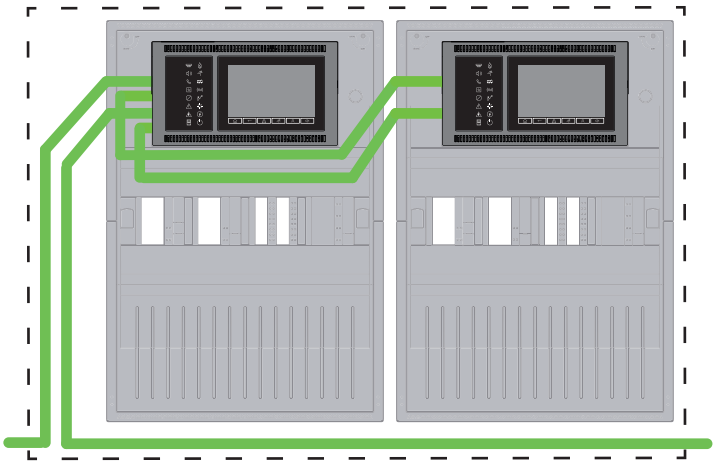


Figure 7.5: Panel network over CAN with redundant panels

7.6 Panel network over two Ethernet loops

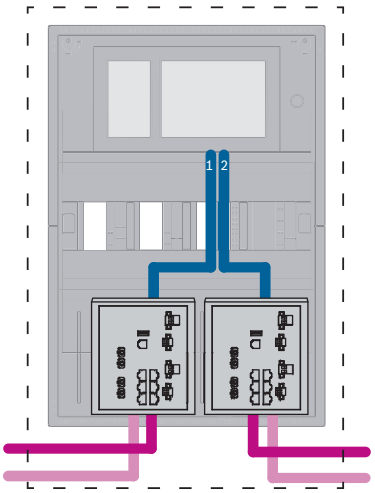


Figure 7.6: Connect Ethernet networks

7.7 Panel network over two Ethernet loops with redundant panels

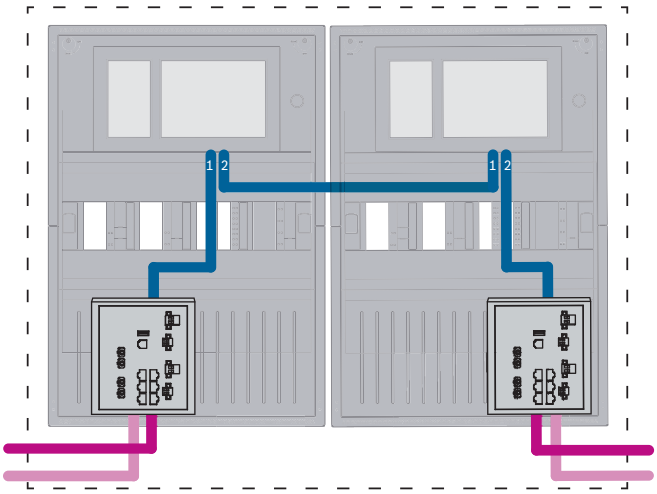


Figure 7.7: Connect Ethernet networks with redundant panels

7.8 Connect Ethernet and CAN network with redundant panels

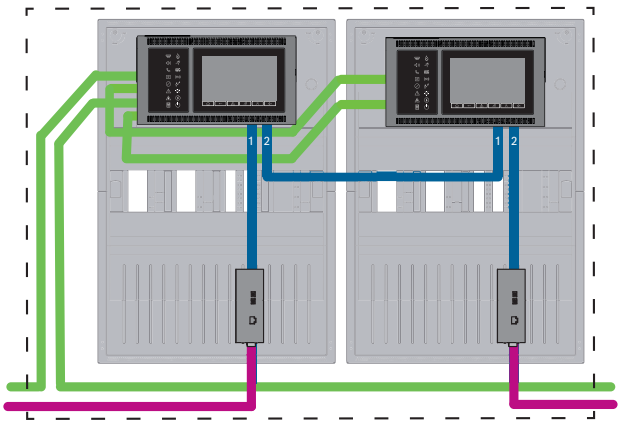


Figure 7.8: Connect Ethernet and CAN network with redundant panels

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

It is possible to connect the Secure Network Gateway to a redundant AVENAR panel.
For the following reasons, it is recommended not to connect the Secure Network Gateway to a redundant AVENAR panel but instead to an AVENAR panel without panel redundancy:

- The procedure is an interim solution.
- If connected to a building management system, the ETH3 port of the redundant panel controller must be used and configured.

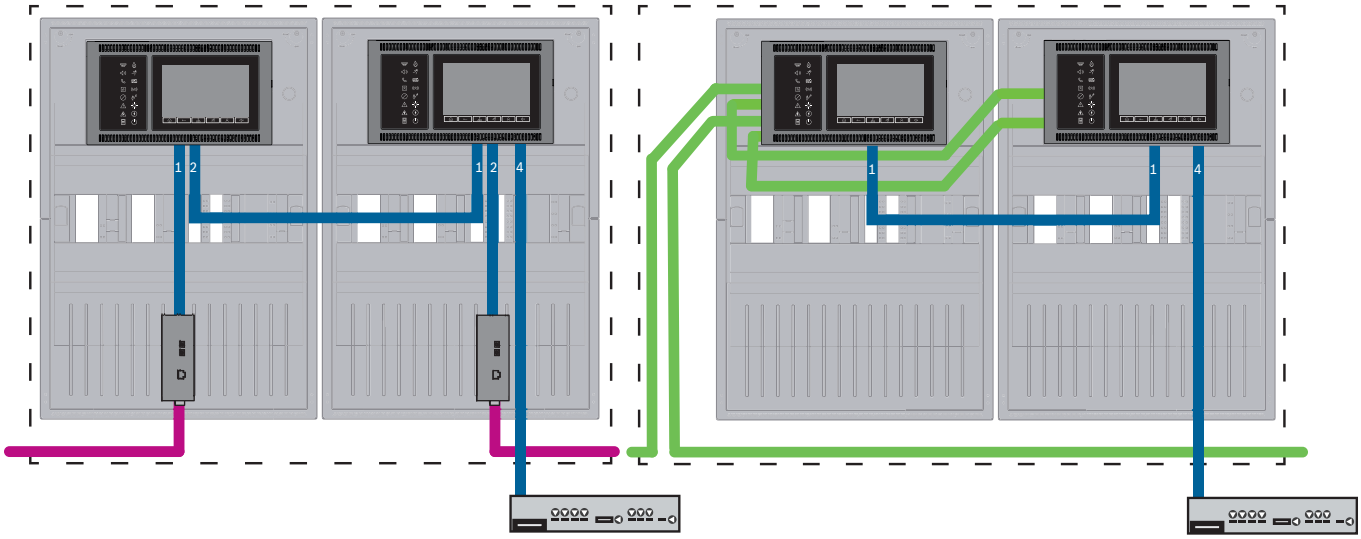


Figure 7.9: Left side: Redundant panel with Ethernet network. Right side: Redundant panel with CAN network

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.

Procedure

1. For connecting the Secure Network Gateway, connect it to the ETH4 port of the redundant panel controller.
2. In the CAN network an Ethernet cable is required from the ETH1 to the ETH1 port of the redundant panel controller. Configure the ETH1 settings in the FSP-5000-RPS **Net interface-Ethernet** window:
   - For **Line type** select **Link**
   - A line number greater than 0 in **Connected to line number** causes that the connection is supervised.
3. For both, CAN network or Ethernet network, configure the ETH4 settings in the FSP-5000-RPS **Net interface-Ethernet** window:
   - Enter 0 in **Connected to line number**.
   - Mark **Use port**.

7.10 Connect life safety services to redundant panels

You must connect life safety services to an AVENAR panel without panel redundancy:

- The interim solution for remote services is not suitable for life safety relevant connections to a voice alarm systems (VAS over IP) or to a hierarchy panel. An EN 54 certified switch connected to the main panel controller and to the redundant panel controller must be installed.

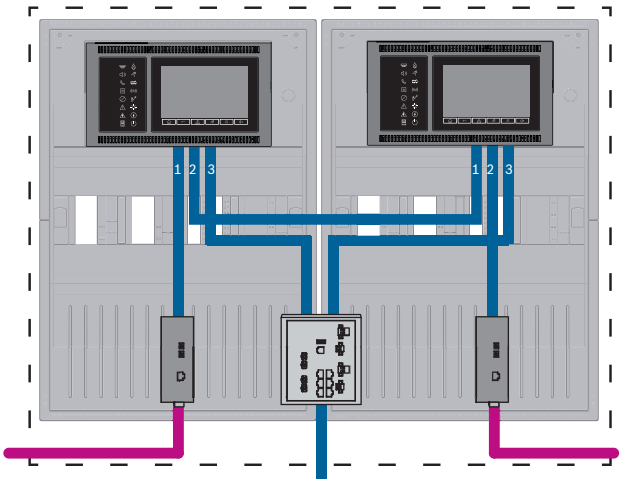


Figure 7.10: VAS and hierarchy panel interface to redundant AVENAR panel

8 Remote Services

The following services belong to Remote Services:

– Remote Alert
– Remote Maintenance

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 (Remote Assistant). Remote Services for Private Secure Network is only available in Germany with a service agreement with Bosch BT-IE.

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.

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.

8.1 Preconditions for Remote Services

8.1.1 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.
Remote Connect has to be enabled in the FSP-5000-RPS configuration of this panel.

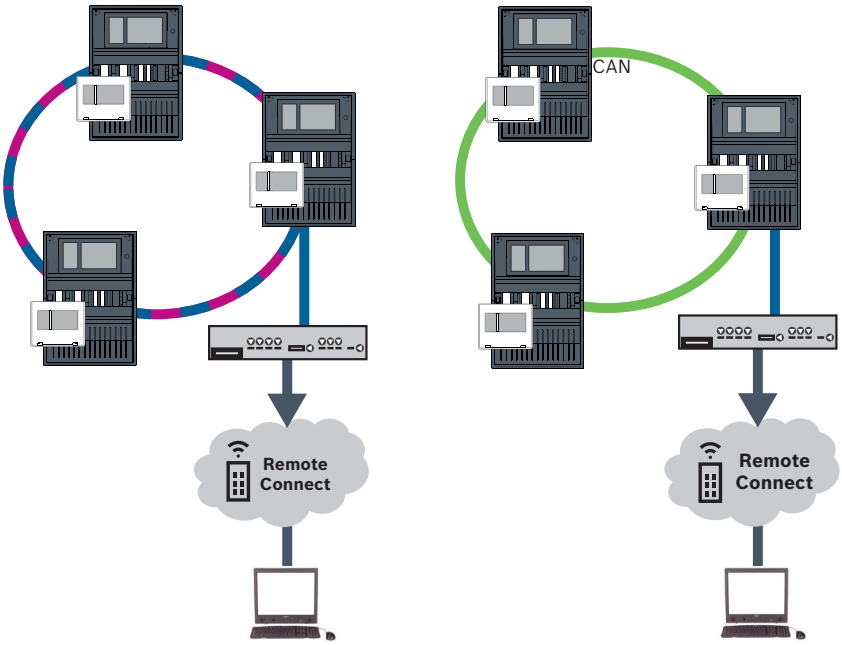


Figure 8.1: Remote Connect in an Ethernet loop | Remote Connect in a CAN loop

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

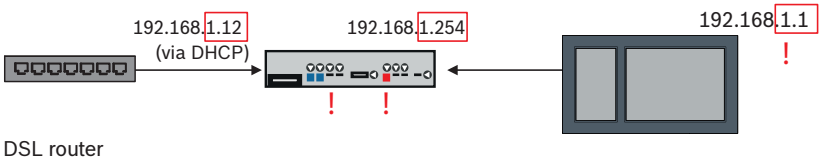
Notice!
To connect panels via FX, use media converters approved by Bosch.

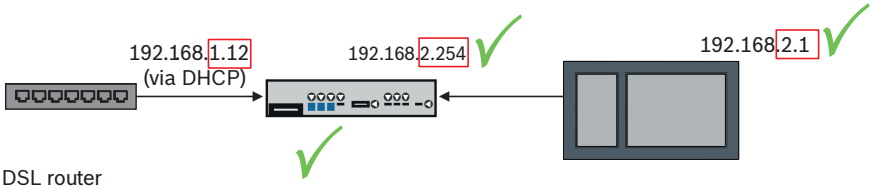
To prevent sending EN 54-2 relevant multicast traffic to the router, use the external Ethernet switch. Activate IGMP snooping of the external Ethernet switch, see the corresponding section in the Installation chapter of the networking manual.

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.

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.

8.1.2 Fire System Explorer

For using Remote Services you must be a user of a Fire System Explorer (FSE) tenant. The one unique Remote ID represents your company.



Notice!

To avoid reconfigurations or adjustments when using Remote Services, ensure that the following requirements are met:

- panel with firmware 3.1.16 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 5.12.28 or higher installed and internet access

FSE uses SingleKey ID. Find more information on the SingleKey ID page: https://singlekey-id.com

Create an FSE tenant

If you cannot use an existing FSE tenant, then you have to create one on: https://fse.bosch-nexospace.com/login/

You may have to log in or register on the SingleKey ID page.

You may have to accept the terms of contract and the data privacy conditions.

FSE sends you an email to the provided address containing an activation link.

For creating a new FSE tenant contact the customer support.

Logging into an existing FSE tenant

You got an invitation e-mail.

1. Click the activation link in the invitation e-mail.
2. Select the tenant into whom you want to log in. The systems of the tenant are shown.

Order licenses

Each system requires its own license. Automatic assignment is recommended.

- To order a 1-year license from Bosch Fire Alarm Systems write an e-mail to the order desk. You have to include the unique Remote ID of the tenant. If you need licenses for several tenants, you have to write for each tenant one e-mail.

You receive for each order e-mail an invoice e-mail to the address provided. With the next login into the tenant the licenses are available in the corresponding Remote ID account. If the **Auto-Renew** function is on, then a valid license will automatically assigned as soon as a matching license is available. Besides the **Auto-Renew** function, an user with administrator access can also assign a **Backup License** to a system with a running license. This license is assigned as soon as the current license expires.

Assign license

If you have to assign a license manually, for example if the **Auto-Renew** function is off, proceed as follows:

1. Click the key icon for managing licenses.
2. You assign an available license by opening the three dot menu next to the license and selecting **Assign to a system**. Or, you click **Systems**, select a system, and select **Assign license** from the three dot menu next to the system.
3. The license and the system size has to match:
   S License (Small system) for a system with less than 254 points

M License (Medium system) for a system with 254 - 2000 points
L License (Large system) for a system with more than 2000 points

4. **Auto-Renew** on is recommended.
5. Click **Assign License**.

The list of licenses and the list of systems is updated.

Connect to FSP-5000-RPS

For the connection to FSP-5000-RPS you have to create an access token.

1. In FSE, click your user name and select **Create access token**.
2. Start FSP-5000-RPS.
3. Click the settings icon and select **Options**.
4. In the **Settings** window, select **Remote Services**.
5. Under **Account,** enter your FSE e-mail address and your FSE password and continue with **OK**.
6. In the **Configurations** window, select your system.
7. In the navigation tree, select **Remote Services**.
8. Select **Fire System Explorer** from the **Access type** drop down list.
9. Copy the generated access token:

– into **User token** if you are working on your personal computer
– otherwise into **One time token**.

8.2 Remote Alert

Through Remote Alert, a panel pushes relevant status information.
Transferred data are analyzed with Remote Alert. In case of an unexpected event, the user will be informed via E-Mail about the received alerts.
Remote Alert is also available for Private Secure Network.
Part of Remote Alert is the **Remote Fire Safety** application. The app allows users to receive instant push notifications on their mobile devices for alarms and system warnings.
The user can also access historical notifications that can be shared via email or messenger service.
Additionally, the app provides updates on system status including health, connectivity, license validity, and if a fire panel firmware update is required.
The app can be downloaded for free: https://play.google.com/store/apps/details?id=com.bosch.remote_fire_safety&gl=EN or https://apps.apple.com/de/app/remote-fire-safety/id1557422840

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 user interface, you can conduct walk tests.

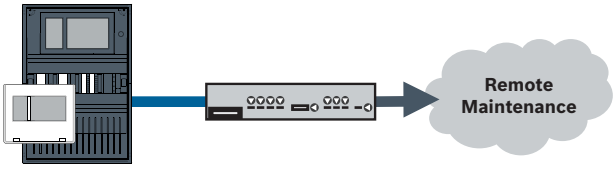


Figure 8.2: Remote Maintenance

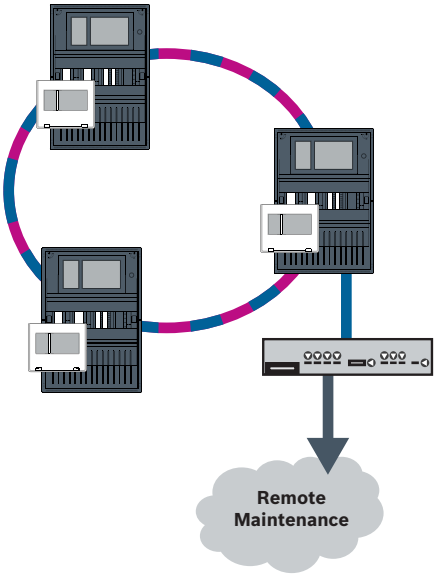


Figure 8.3: Remote Maintenance

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 collects data of relevant LSN devices and functional modules. The data are analyzed and visualized for maintenance activities.

8.4 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).

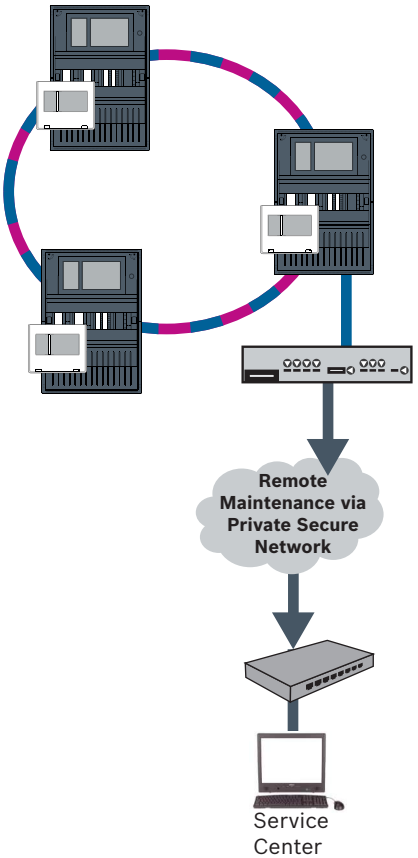


Figure 8.4: Remote Maintenance for Private Secure Network

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. 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 are the same on the panel controllers, the FSP-5000-RPS, and the external Ethernet switch.

9 Building management system

The panel controller equipped with a premium license can be connected to a building management system via an Ethernet interface using one of the following servers:

- FSI server: FSI (Fire System Interface) is a Bosch proprietary communication protocol. A Software Development Kit (SDK) is available for a tailor made integration.
- OPC server: OPC (OLE for Process Control) is a standardized communication protocol compliant with Building Integration System (BIS).
- BACnet server: BACnet (Building Automation and Control Network) is a standardized communication protocol specifically for connection to a third party building management system.

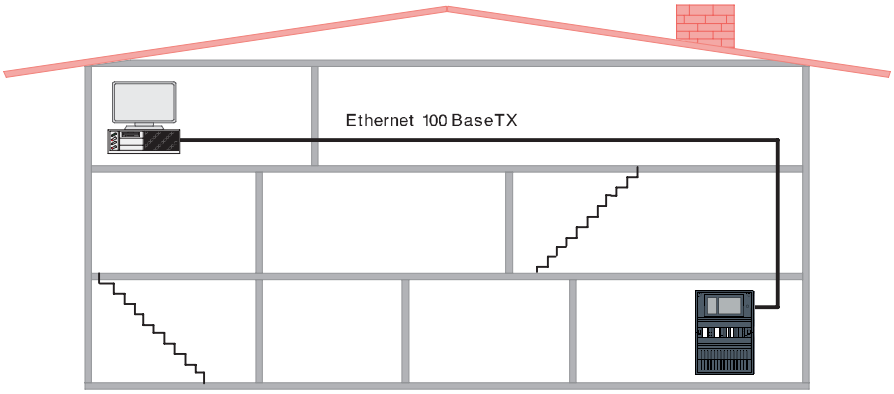


Figure 9.1: Connection to building management system

When connecting to a building management system with 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?

Notice!
When connecting the building management system, observe the safety instructions in *Safety, page 5*.

Configuration in FSP-5000-RPS
A server (OPC server, BACnet server, FSI server) must be created in FSP-5000-RPS programming software to make a connection to a building management system.
You must perform the following settings in both the FSP-5000-RPS software and the server:
Program the Logical node address (**Net group** and **Net node**), the Physical node address (**PNA/RSN**) and IP Settings (**IP address** and **Port**).
Bosch recommends to use port 25000 for an OPC server and port 25001 for a BACnet server or a FSI server.

You must assign a server to each panel or remote keypad from which statuses should be transmitted. The number of servers that can be assigned to one panel or remote keypad is limited to:

– 1 BACnet server
– 2 FSI server
– 1 OPC server
– 2 UGM server

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

External Ethernet switch for connecting a building management system must be programmed separately

Program the IP address and redundancy settings of the external Ethernet switch, see *Configure external Ethernet switch, page 44*. 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 external Ethernet switch are identical.

Switches for connecting a building management system and the second loop must be programmed separately

Program the IP address and redundancy settings of the external Ethernet switch, see *Configure external Ethernet switch, page 44*. 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 *External Ethernet switch, page 52*.
Make sure that the RSTP settings in the panel controllers, in FSP-5000-RPS and in the external Ethernet switch are identical.
Change the RSTP priority for the switches for connecting the two loops, as they belong to the backbone.

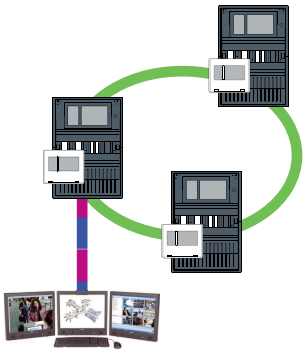
The server must be programmed separately

Program the Logical node address (**Net group** and **Net node**), Physical node address (**PNA/ RSN**) and IP Settings (**IP address** and **Port**).
Bosch recommends to use port 25000 for the Ethernet interface between the fire panel and the server.
Make sure that the settings in the FSP-5000-RPS programming software and in the server are identical.

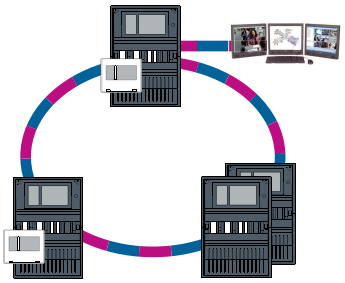
Notice!
For detailed information about the installation and configuration of the BACnet or OPC server, refer to the their manuals available in the online catalog at www.boschsecurity.com. The manual of the FSI server can be found on the extranet (access rights required).

Topologies with building management system

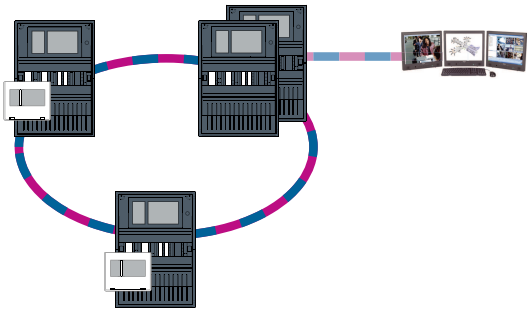
The building management system may be connected via an Ethernet cable (copper) or fiber optic cable.



CAN loop with building management system

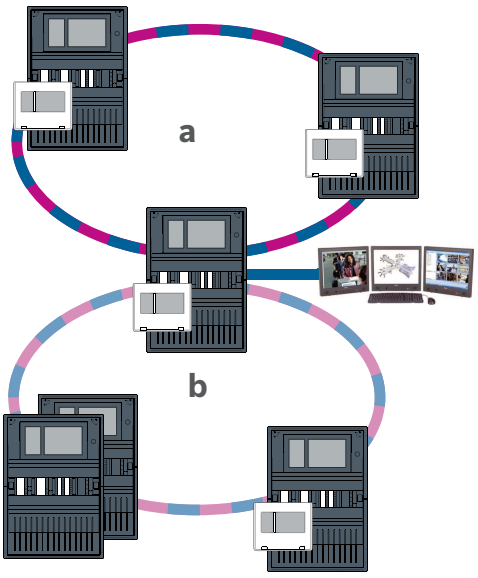


Ethernet loop with building management system

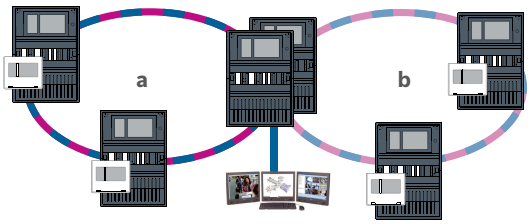


Ethernet loop with building management system to redundant panel

In the following topologies, loop a is the backbone. Loop b is the sub-loop.



Connecting Ethernet loop via a non-redundant panel



Connecting Ethernet loop via a redundant panel

10 Smart Safety Link

This chapter specifies the technical solution for a secure Ethernet interface between Bosch fire panels and Bosch voice alarm systems.
Smart Safety Link is the most reliable and secure interface to combine a fire detection and a voice alarm system (VAS). Smart Safety Link offers exceptional flexibility and options for expandability.

The bi-directional data communication establishes a supervised connection between the fire detection panel and the VAS. Both the fire panel and the VAS indicate a fault message when the connection is interrupted. In case of an interrupted connection, the user can start the evacuation of the complete building manually by using a call station of the VAS. An interruption of the interface does not lead to an automatic evacuation of the building. When the interface is re-established, the fire panel automatically re-synchronizes the current alarm state with the VAS. In case of a fire condition, the fire panel can automatically start voice announcements using virtual VAS triggers that are activated by rules which are configured in FSP-5000-RPS. The fire panel generates a supervisory message when an evacuation event is started from the VAS. A malfunction on the VAS will generate a fault message on the user interface of the fire panel. Through the graphical user interface of AVENAR panel the operator has the possibility to silence the announcements of the fire panel. The operator can request a status overview of all virtual triggers. Each virtual trigger can be marked with an unambiguous label containing the location and message type. A clearly distinctive color is reflecting the condition of each virtual trigger. An operator with L2 user rights can start and stop the voice announcement in the selected virtual trigger manually.
PAVIRO or Praesideo can be connected to AVENAR panel without data encryption.
Due to its networked topology PRAESENSA requires an interface with encrypted data communication. Only use AVENAR panel running on panel controller firmware version 4.x to connect with PRAESENSA.
Smart Safety Link over Ethernet was introduced in panel controller firmware version 2.11 and FSP-5000-RPS version 4.3.

Notice!
Voice alarm system connected to AVENAR panel
Each fire panel which is physically connected to a voice alarm system via Smart Safety Link needs a premium license.

10.1 One direct VAS interface

The fire panel and voice alarm system can be connected by one single TX Ethernet cable.

Notice!
VdS 2540
When connecting a voice alarm system to a panel using Smart Safety Link the system must be installed in the same room as the fire panel and positioned directly adjacent to it. Otherwise, the requirements of VdS 2540 regarding data transmission paths are not fulfilled.

10.1.1 Praesideo and PAVIRO

AVENAR panel can be directly connected to the dedicated Open Interface Ethernet port of the system controller of Praesideo (PRS-NCO-3) or PAVIRO (PVA-4CR12).
Use the Open Interface for a single panel or for a panel network.

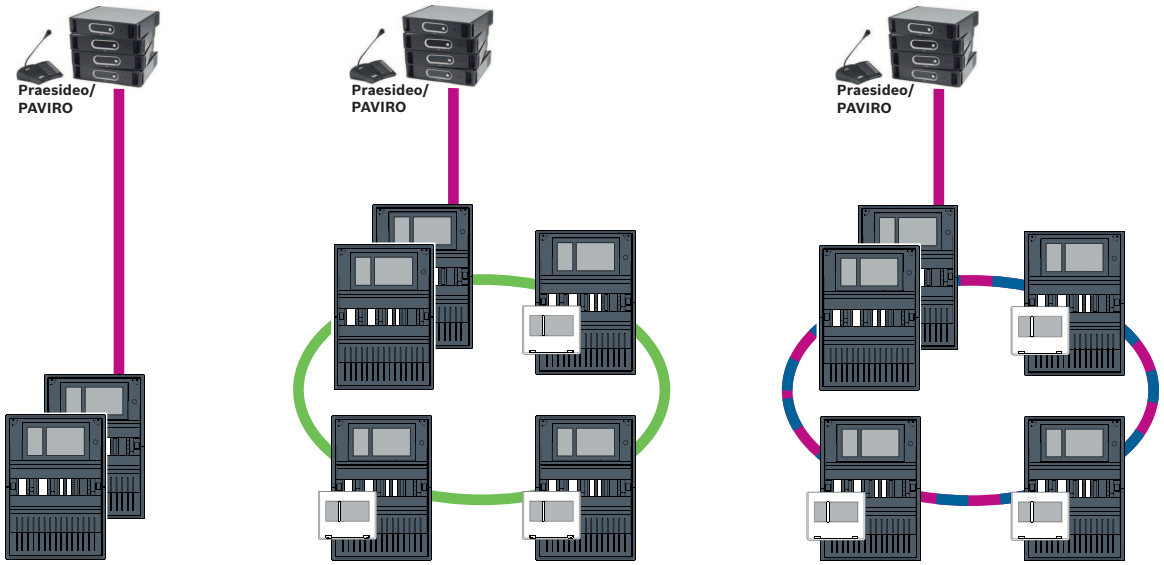


Figure 10.1: One direct Praesideo|PAVIRO interface

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).

10.1.2 PRAESENSA

PRAESENSA is a networkable voice alarm system using an IP-network for audio and control. Always connect AVENAR panel through a PRA-ES8P2S Ethernet switch, 8xPoE, 2xSFP to PRAESENSA.

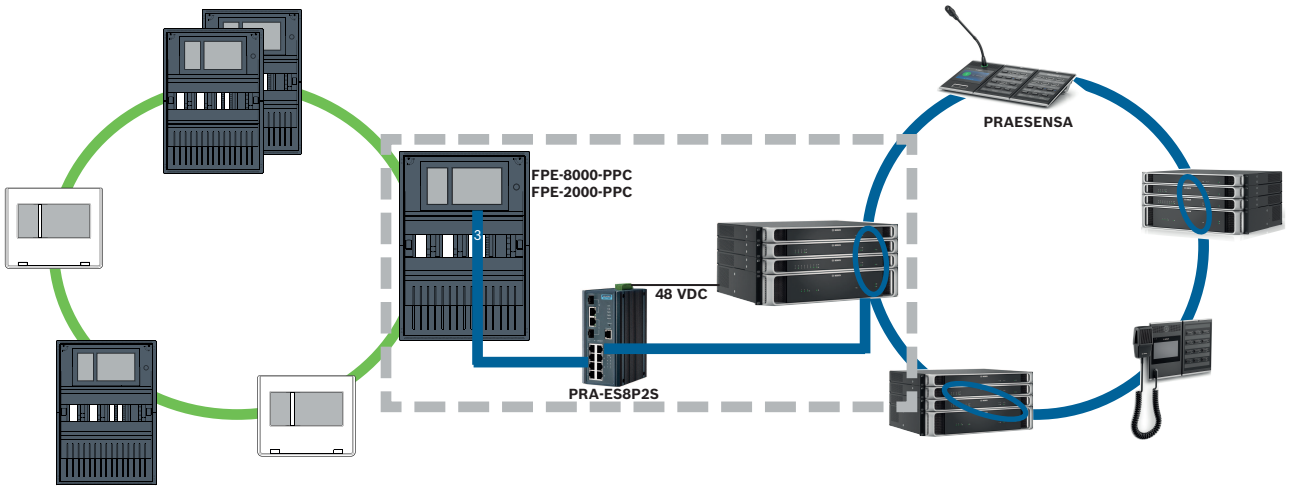


Figure 10.2: PRAESENSA to AVENAR panel

Notice!

PRAESENSA to AVENAR panel

- Use PRA-ES8P2S exclusively for Smart Safety Link. Besides the PRA-SCL System controller do not connect other PRAESENSA equipment to the Ethernet ports of the Ethernet switch, 8xPoE, 2xSFP. Do not use the Ethernet switch, 8xPoE, 2xSFP for connection to a building management system, hierarchy panel, Secure Network Gateway for Remote Services, etc.
- Use a panel containing only one panel controller to connect with PRAESENSA using Smart Safety Link. Smart Safety Link to PRAESENSA is not yet compatible with panel controller redundancy. The panels in the network that are not directly connected to PRAESENSA may contain panel controller redundancy.
- Use CAN-Bus topology for the panel network. Do not use an Ethernet panel network.
- All AVENAR panel and all AVENAR keypad 8000 in the network must run with panel firmware 4.x.

Procedure

1. Mount the PRA-ES8P2S Ethernet switch in the PRAESENSA rack. Install PRA-SCL flush to AVENAR panel, in one single room. Do not mount the PRA-ES8P2S Ethernet switch in the AVENAR panel enclosure.
2. PRAESENSA must supply the power for PRA-ES8P2S.
3. Configure the PRA-ES8P2S Ethernet switch:
   – only allow unicast communication between FPE-8000-PPC and PRAESENSA Controller
   – block all multicast communication
   – disable RSTP
4. Check the mode of PRAESENSA, it must run in DHCP mode. Zeroconf mode is not supported when using Smart Safety Link.
5. Connect the PRAESENSA Controller by a single Ethernet cable (RSTP disabled).
6. For the Smart Safety Link configuration of AVENAR panel, select **Encrypted VAS over IP** in FSP-5000-RPS.

10.2 Multiple direct VAS interfaces

In a CAN network, each fire panel can be connected to one voice alarm system. Apply the direct interface connection as specified in *One direct VAS interface, page 37*.

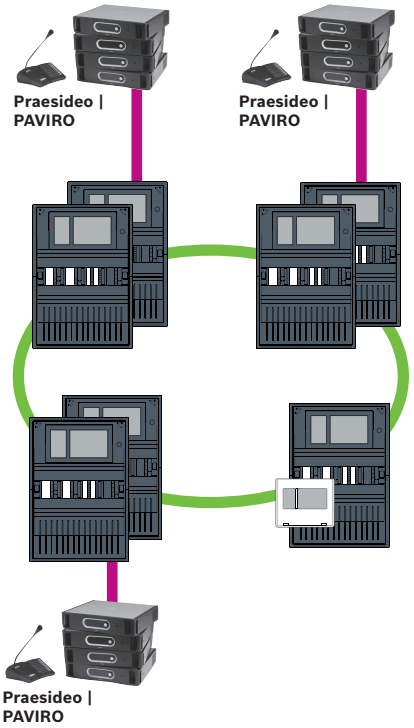


Figure 10.3: Multiple direct VAS interfaces

For each node, for which you want to deactivate panel networking over IP, perform the following procedure in FSP-5000-RPS:

1. Select the node for deactivating panel networking.
2. Select **Use Ethernet settings**.
3. Deselect **Panel networking over IP**.
4. Click **Apply** .

10.3 VAS integrated in Ethernet panel network

If Praesideo and PAVIRO are integrated in panel networks, then the voice alarm system have a redundant transmission path. The redundant transmission path allows that the fire alarm panel and the voice alarm system are installed in separate rooms.
Currently it is not possible to integrate PRAESENSA into an Ethernet panel network.

Notice!
VdS 2540
When connecting a voice alarm system to a panel using Smart Safety Link the system must be installed in the same room as the fire panel and positioned directly adjacent to it. Otherwise, the requirements of VdS 2540 regarding data transmission paths are not fulfilled.

Notice!
VdS 2540 - Ethernet network
Consider for Ethernet panel networks, that for installations in Germany, where compliance to VdS 2540 is required, fiber optic cable has to be used for all data transmission paths. The only exception is inside a housing.

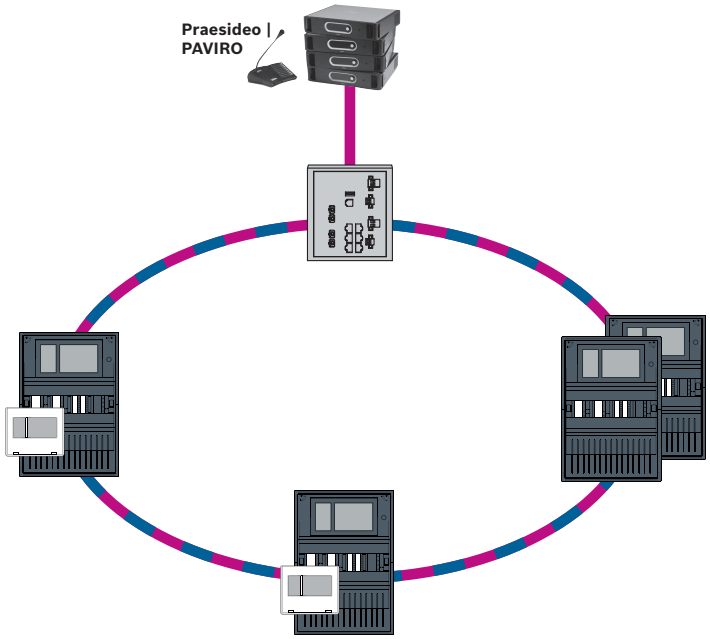


Figure 10.4: VAS integrated in Ethernet panel network

To prevent sending EN 54-2 relevant multicast traffic to the router, use the external Ethernet switch. Activate IGMP snooping of the external Ethernet switch, see the corresponding section in the Installation chapter of the networking manual.

The fire alarm system must supply the power for the external Ethernet switch.

11 Hierarchy panel

An UGM server server must be created in FSP-5000-RPS programming software to make a connection to a hierarchy panel.

You must perform the following settings in both the FSP-5000-RPS software and the hierarchy panel: Program the Logical node address (**Net group** and **Net node**), the Physical node address (**PNA/RSN**) and IP Settings (**IP address** and **Port**).

Bosch recommends to use port 25001 for the Ethernet interface between the fire panel and the hierarchy panel.

You must assign a server to each panel or remote keypad from which statuses should be transmitted. The number of servers that can be assigned to one panel or remote keypad is limited to:

- 1 BACnet server
- 2 FSI server
- 1 OPC server
- 2 UGM server

Notice!

All panel controllers and hierarchy panel 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.

In order to connect a panel to the hierarchy panel, you must simulate the physical structure of the network in FSP-5000-RPS. This also includes the line numbers between the connecting panel controller and the switches of the hierarchy panel.

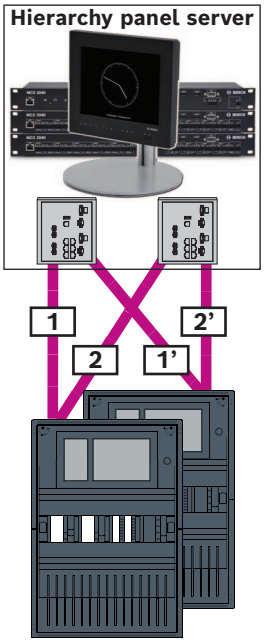


Figure 11.1: Example of line numbering for the hierarchy panel

12 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 external 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.

12.1 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 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.

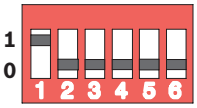
Notice!
Use only the following cables for networking:
Ethernet cable
Ethernet patch cable, shielded, CAT5e or better.
Note the minimum bending radii specified in the cable specification.
Fiber optic cable
Multi-mode: fiber optic Ethernet patch cable, duplex I-VH2G 50/125µ or duplex I-VH2G 62.5/125µ,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

12.2 Installing external Ethernet switch BRS20



Warning!
Risk of eye injury
When media converters are used, laser light may be emitted from the optical ports or from the ends of connected fiber-optic cables.
Do not look into the laser beam with the naked eye or with optical instruments, for example a microscope.
If you do not obey this warning, eye injury can occur at distances less than 100 mm.
Laser classification: Class 2M laser diode
Wavelength: 650 nm
Output power: Less than 2 mW
Standard: IEC 60825-1

Mandatory settings
Configure external Ethernet switch, page 44
Configuration-specific settings
Configure RSTP, page 45
Enable QoS priority, page 45
Activate IGMP snooping, page 45
Configure fault relays, page 45
Configure connection monitoring, page 46
Optional settings
Configure security settings, page 46
Configure system information, page 46
Change IP address, page 46
See also
- Installation manual of the Mounting kit for external Ethernet switch FPM-5000-KES
- User manual of the manufacturer

12.2.1 Configure external Ethernet switch

Preconditions
- Laptop is connected to the network.
- HiView software is installed on the laptop.

Assign IP address using HiView
1. Open the HiView software.
2. Go to the **Discovery** tab.
3. Click **Refresh** to scan the network for all available switches.
4. Double-click the switch you want to program.
5. Assign an IP address and net mask to the switch.



Notice!
For the device part of IP addresses, use numbers greater than 200 for switches, if your network configuration allows this.
This creates a clear separation from the host identifier of an IP address.
Example: Assign switch 192.168.1.201 to a panel with IP address 192.168.1.1.

Log in to the web interface
1. Log in using the manufacturer's default credentials:
   User: admin
   Password: private
2. When prompted, enter a new password with a minimum of eight characters.

Save settings in NVM (Non-Volatile Memory)
In order to save the IP address or any other configuration, follow these steps:

1. Click ⓒ to apply the settings.
2. To save the settings permanently in NVM:
   Go to **Basic Settings** → **Load/Save**.
   Click the **Save** icon in the top right corner.
3. The configuration is now saved and will remain available after the device restarts.

12.2.2 Configure RSTP

AVENAR panel uses Rapid Spanning Tree Protocol (RSTP) as the redundancy protocol. RSTP is enabled by default on the external Ethernet switch.
This procedure is only required for networks with more than 20 RSTP switches.

Procedure

1. Go to **Switching** → **L2-Redundancy** → **Spanning Tree** → **Global** → **Bridge configuration.**
2. Configure the following parameters on the switch and all panels:
   - **Bridge Priority:** 32768 (no change)
   - **Hello Time:** 2 s (no change)
   - **Forward Delay:** set to 25 s (default: 15 s)
   - **Max Age:** set to 40 s (default: 20 s)
   - **Tx holds:** 10 (no change)
3. Click ⓒ and save settings to the NVM.

12.2.3 Enable QoS priority

This procedure is required when the external Ethernet switches are used for communication between fire panel networks and the UGM-2040.
Procedure

1. Go to **Switching** → **QoS/Priority** → **Port Configuration**.
2. For all ports that connect the panel network to the UGM-2040, set the **Trust mode** to **trustIPDsc.**
3. Click ⓒ and save settings to the NVM.

12.2.4 Activate IGMP snooping

This procedure is required for systems that include voice alarm systems. It prevents EN 54-2-relevant multicast traffic from reaching other systems.

Procedure

1. Go to **Switching** → **IGMP Snooping** → **Global**.
2. Set **Operation** to **On**.
3. Go to **Switching** → **IGMP Snooping** → **Configuration**.
4. Set **Maximum Response Time** to **3 seconds**.
5. Activate **VLAN ID 1**.
6. Go to **Switching** → **IGMP Snooping** → **Querier**.
7. Set **Operation** to **On.**
8. Set **Query Interval** to **4 seconds**.
9. Go to **Switching** → **IGMP Snooping** → **Multicast**.
10. Enable **Discard** for packets with **unknown multicast addresses**.
11. Ensure **Send to Query and Registered Ports** is selected.
12. Click ⓒ and save settings to the NVM.

12.2.5 Configure fault relays

Preconditions

Configure the fault relay only if at least one of these conditions is true:

- There is a connection between two switches.
- The switch has a redundant power supply.

Procedure

1. Go to **Diagnostics** → **Status Configuration** → **Signal Contact** → **Signal Contact 1**.
2. In the **Global** tab, set the **Configuration** to **Device Status**.
3. Go to **Diagnostics** → **Status Configuration** → **Device Status**.
4. In the **Global** tab, enable these parameters under **Monitor**:
– **Power Supply 1**
– **Connection errors**
5. Disable all other parameters.
6. Click ⓒ and save settings to the NVM.

12.2.6 Configure connection monitoring

This procedure is required when the switch fault relay is used.

Procedure

1. Go to **Diagnostics** → **Status Configuration** → **Device Status.**
2. Select the **Global** tab.
3. Enable **Monitor** for **Connection errors**.
4. Select the **Port** tab.
5. For each port to be monitored, enable **Propagate connection error**.
6. Click ⓒ and save settings to the NVM.

12.2.7 Configure security settings

To improve protection against unauthorized access and to secure configuration data, you can apply the following optional settings.

Disable HiDisovery protocol

1. Go to **Basic Settings** → **Network** → **Global**.
2. Under **HiDiscovery** set **Operation** to **Off**.
3. Click ⓒ and save settings to the NVM.

Enable configuration encryption

1. Go to **Basic Settings** → **Load/Save**.
2. Under **Enable configuration**, click **Set a password**.
3. Enter a password with a minimum of eight characters.
4. Select **Save configuration afterwards** and click **OK**.
5. Click ⓒ and save settings to the NVM.

12.2.8 Configure system information

System information can optionally be configured to help identify your switch more quickly.

Procedure

1. Go to **Basic Settings** → **System.**
2. Set the system name, location, and contact person.
3. Click ⓒ and save settings to the NVM.

12.2.9 Change IP address

You have the option to change the IP address.

Procedure

1. Go to **Basic Settings** → **Network** → **IPv4**.
2. Set these values:
– **IP address assignment:** Local
– **IP address:** for example 192.168.1.201
– **Network screen:** for example 255.255.255.0
– **Gateway:** for example 192.168.1.254.
If the switch does not need a gateway, use 0.0.0.0.
3. Click ⓒ and save settings to the NVM.

12.3 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
– 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

– 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, 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.

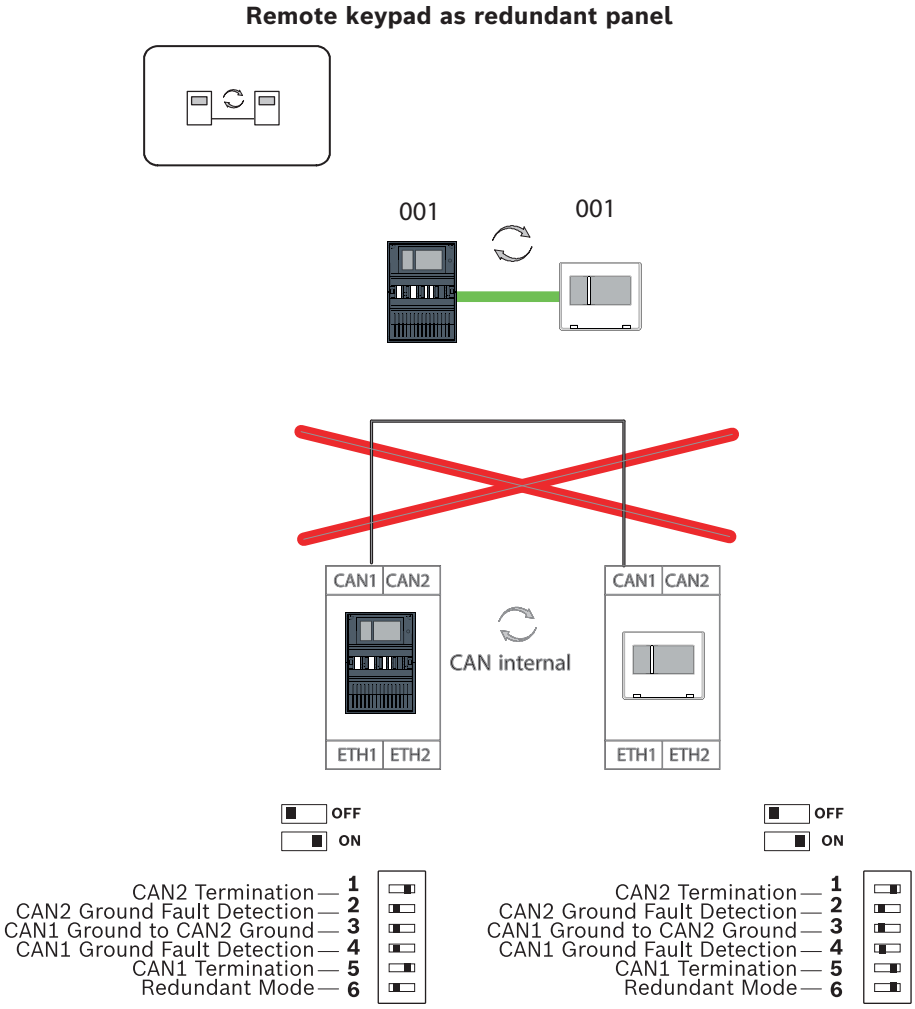


Figure 12.1: DIP switch settings for remote keypad as redundant panel

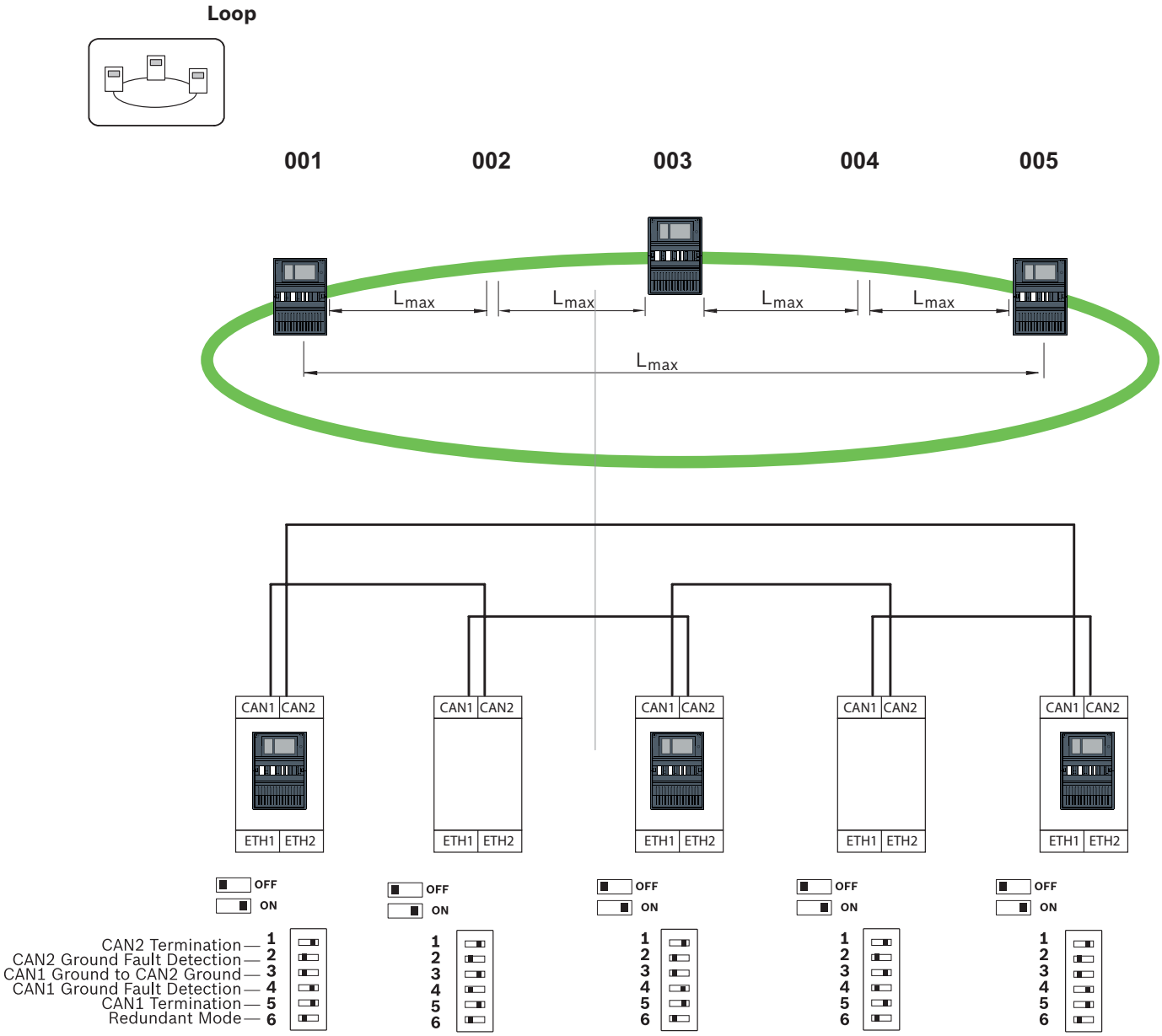
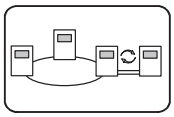


Figure 12.2: DIP switch settings for loop

Loop with remote keypad as redundant panel



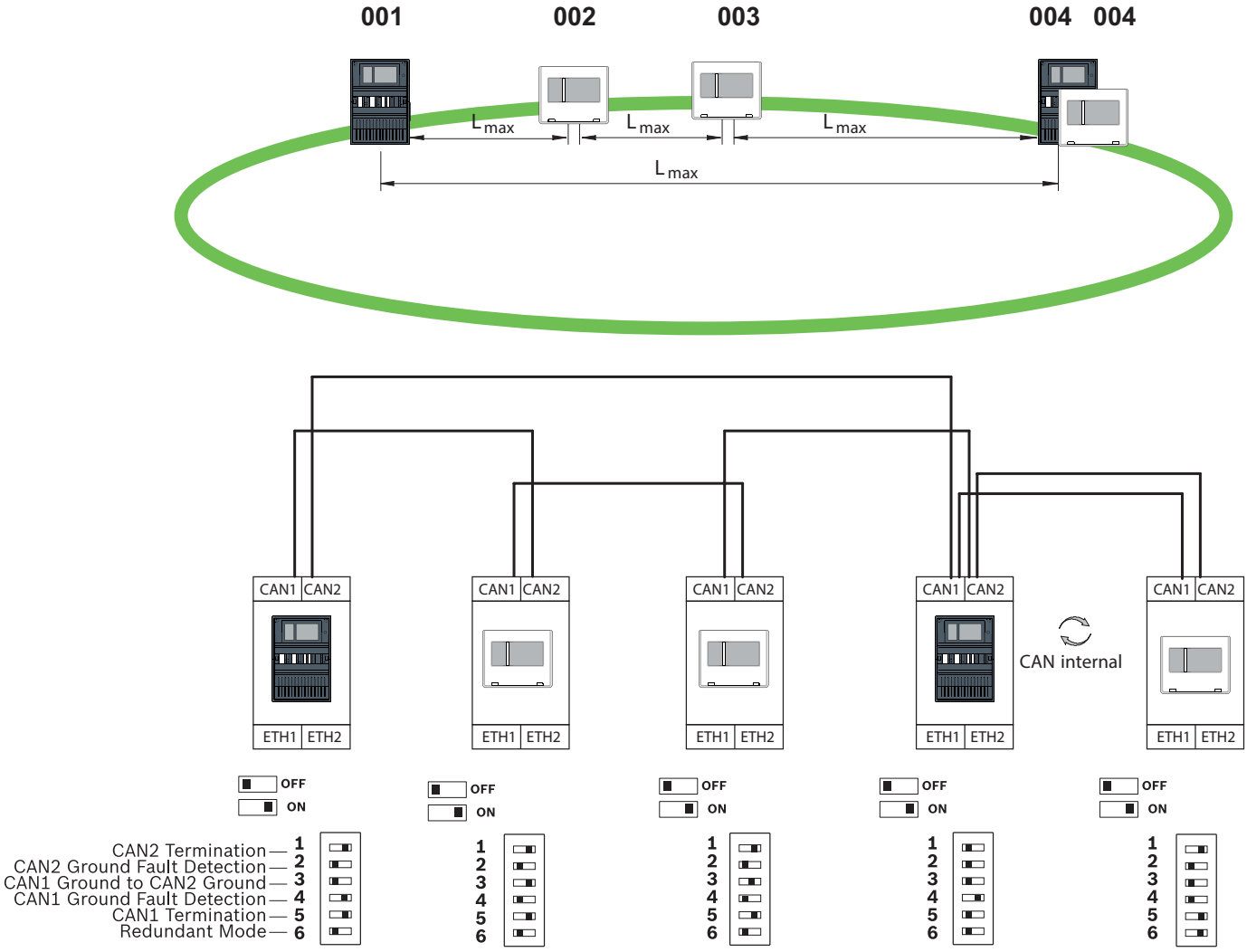


Figure 12.3: DIP switch settings for loop with remote keypad

13 Ethernet cabling

To create an EN 54-2-compliant system, connect the external Ethernet 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 external Ethernet switches use the 24 V output of either the Battery controller module or FPP-5000 External power supply.
- If you have connected a redundant power supply or are creating a switch-to-switch connection, then the fault outputs of the external Ethernet 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 Ethernet 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.

13.1 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.

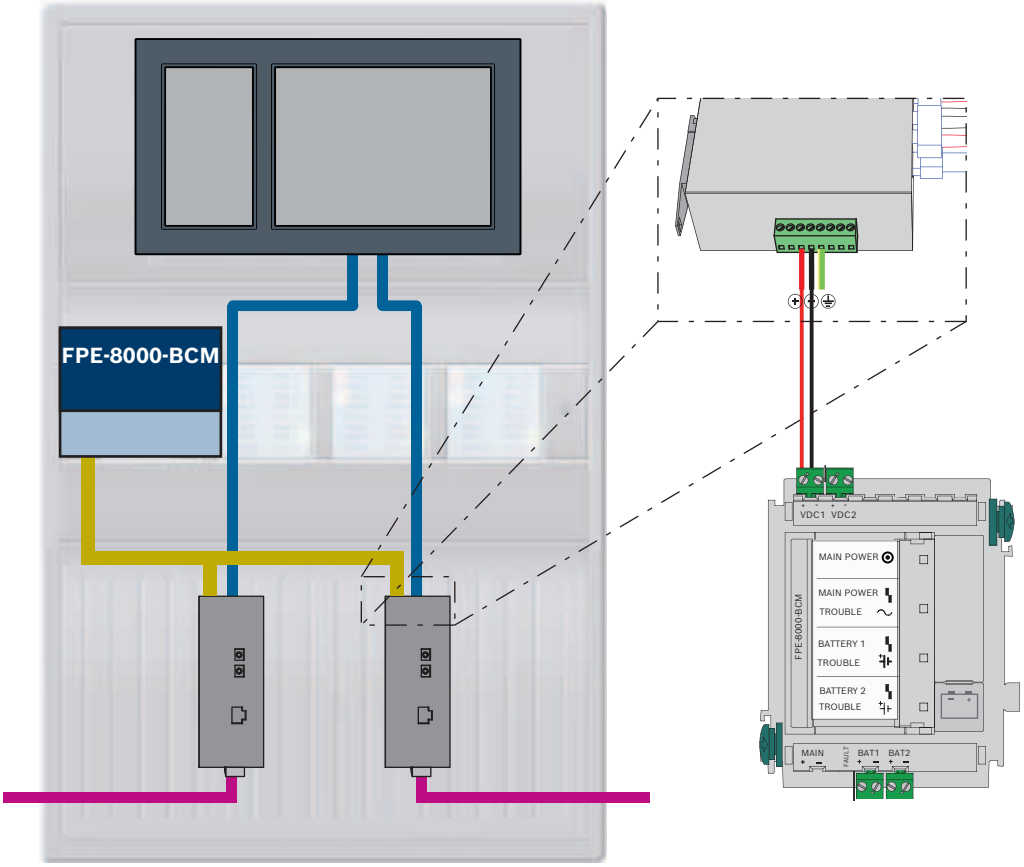


Figure 13.1: Connection of media converter to power supply and to panel controller IN1/IN2

Icon	Description
	TX Ethernet cable (copper)
	FX Ethernet cable (fiber optic cable)
	Power supply
	Transmission of fault

Icon	Description
	Media converter

13.2 External 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:

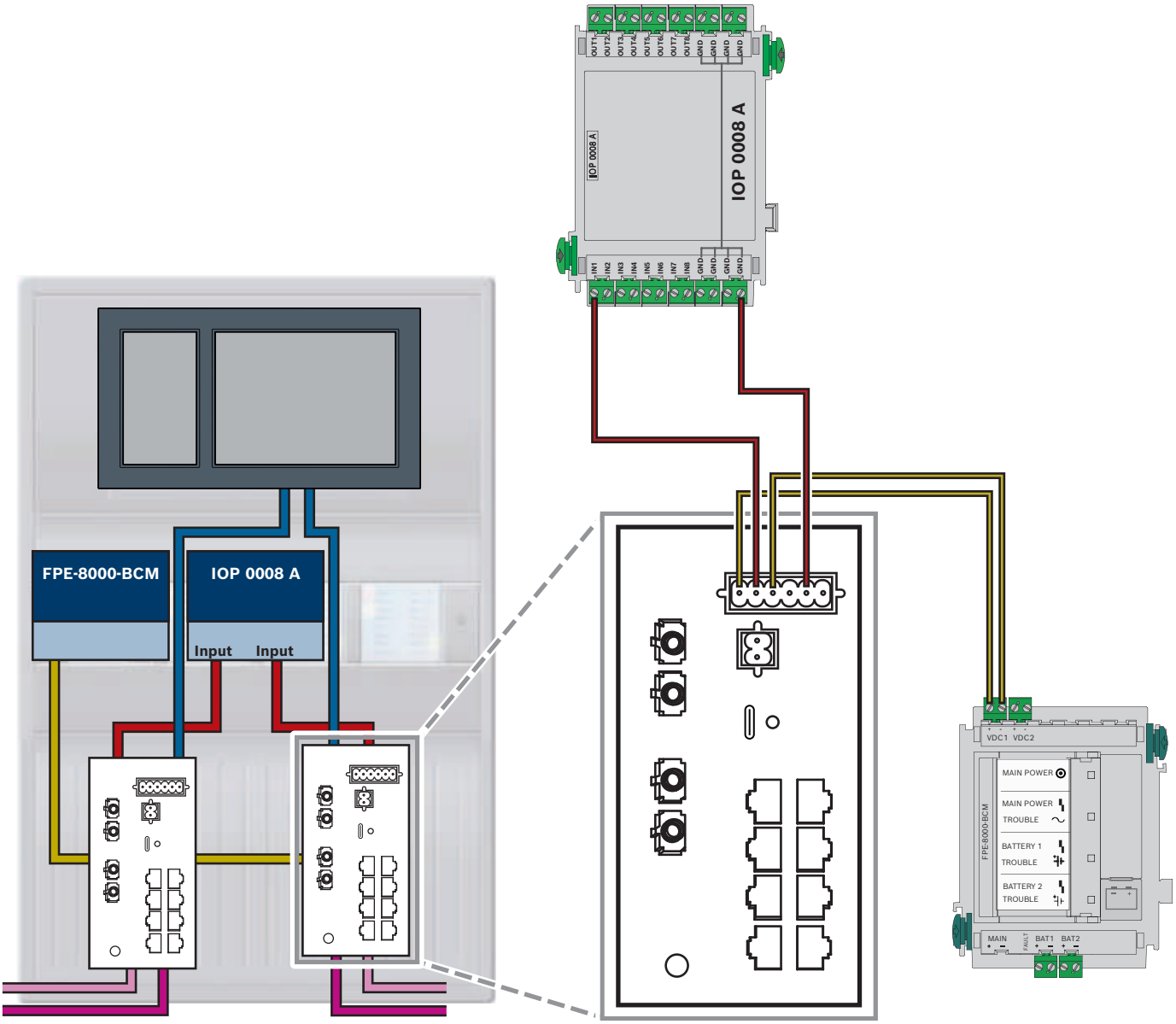


Figure 13.2: Connection of switch to the power supply and IOP

Icon	Description
	TX Ethernet cable (copper)
	FX Ethernet cable (fiber optic cable)
	Power supply
	Transmission of fault
	External Ethernet switch

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

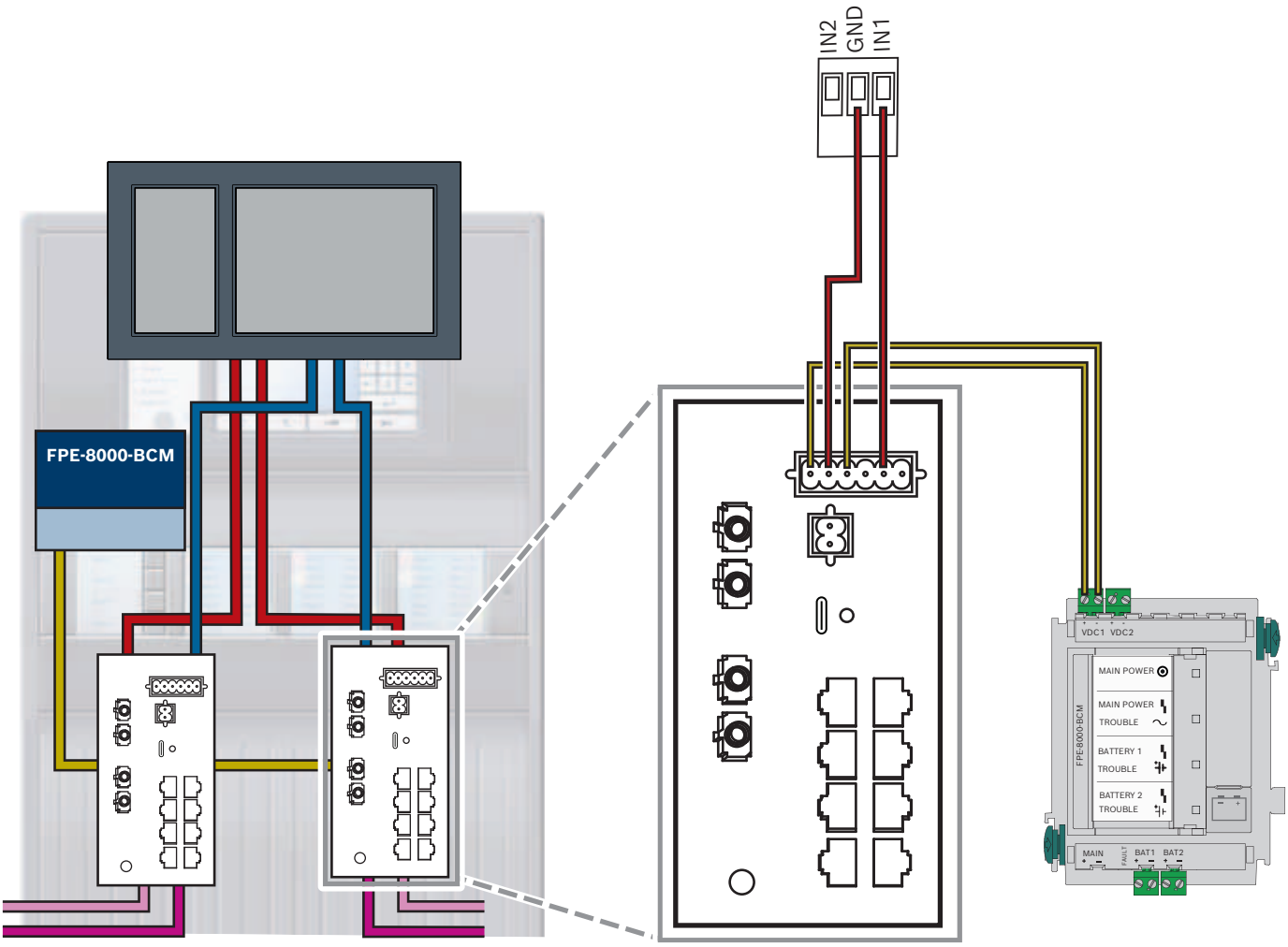


Figure 13.3: Connection of switch to the power supply and to the panel controller

Icon	Description
	TX Ethernet cable (copper)
	FX Ethernet cable (fiber optic cable)
	Power supply
	Transmission of fault
	External Ethernet switch

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

13.3 Remote keypad

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

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.

Connection to remote keypad (VdS 2540 compliant)
In the following the FPP-5000 External power supply is used for powering the remote keypad. The connection to the network is established via 2 media converters in a PSS 0002 A or USF 0000 A.

Notice!
The FPP-5000 External power supply and an additional housing for media converters must be mounted flush with the remote keypad. The power supply wires of the remote keypad and of the media converter are not monitored for creeping short circuit and creeping open and must therefore be installed in housings that are mounted flush with the housing of the remote keypad.

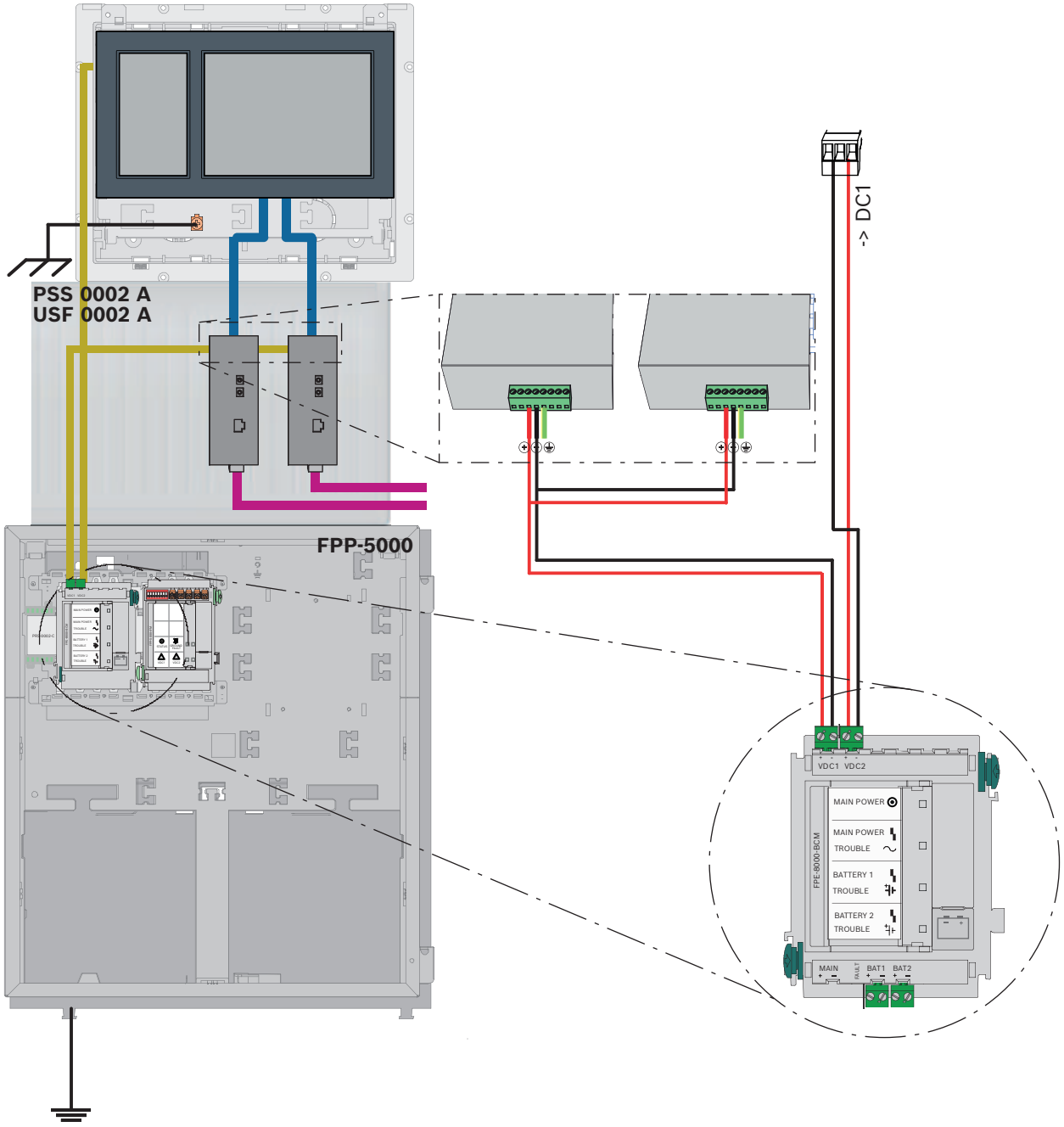


Figure 13.4: Cabling of Remote keypad

Icon	Description
	TX Ethernet cable (copper)
	FX Ethernet cable (fiber optic cable)
	Power supply
	Media converter

14 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.

14.1 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 nodes
  - Set the Physical node address (**PNA/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 building management system, the voice alarm system, the hierarchy panel 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.

14.2 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.

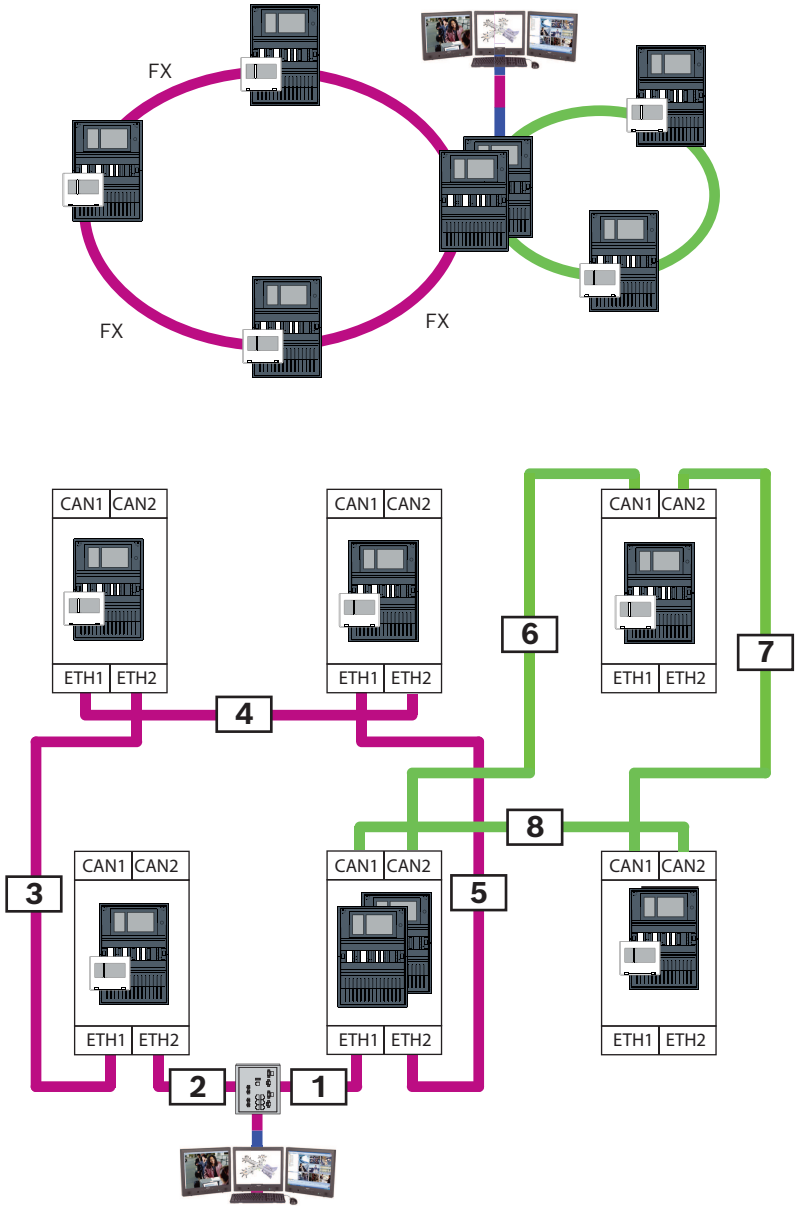


Figure 14.1: Example of a network and the possible line numbering

14.3 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.

15 Appendix

15.1 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			

Physical address	Logical address	Error message	Description and possible cause
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.
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

A

Addressing
- Physical node address 11

B

Building management system 8, 34, 47
Building management system, Topologies 35, 36

C

CAN interface 47
CAN network 8
CAN topologies 9

E

Ethernet interface 47
Ethernet network 8
Ethernet topologies 9
Ethernet, standard settings 12

F

Fire System Explorer 31
FSE 31
FSE tenant 31

L

License for Remote Services 31
Limits
- Network 11

M

MAC address 17
Maximum limits 11

N

Network
- Cable 21
- Cabling 21
- Limits 11
- Panel controller 47

Network diameter 17
Networking
- Cable length 21
- Loop topology 21

Networking over CAN 8
Networking over TCP/IP 8

P

Panel controller
- Networking 47

Parameters
- RSTP 13

PAVIRO 8, 37
Physical node address 11
Praesideo 8, 37

R

Redundancy
- Addressing 11

Remote Alert 32
Remote Connect 28
Remote Maintenance 32, 33
- for Private Secure Network 33

Remote Services 28
- Connect Secure Network Gateway 29
- Connect to FSP-5000-RPS 32
- Fire System Explorer 31
- FSE 31
- FSE tenant 31
- License 31
- Separating sub-networks 30

RS232 interface 47
RSTP parameters 13

S

Secure Network Gateway 28, 29
Services 8
Standard settings, Ethernet 12

T

Topologies 35, 36
Topologies, CAN 9
Topologies, Ethernet 9
Topologies, with Building management system 35, 36

U

USB interface 47

V

Voice alarm system 37

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Platz 1
D-70839 Gerlingen
Germany
www.boschbuildingtechnologies.com
© Bosch Sicherheitssysteme GmbH, 2026

Building solutions for a better life

202604021427