FPA-5000

FPA-5000

BOSCH

en Networking Guide

Table of Contents

1	**Safety instructions**	**5**
2	**Short Information**	**6**
3	**Ethernet networking**	**7**
3.1	Procedure	7
3.1.1	Standard procedure for smaller projects	7
3.1.2	Medium-sized and large projects	7
3.2	Special features of the FPA network	8
3.2.1	Protocols	8
3.2.2	Network diameter	9
3.2.3	Cables used	11
3.2.4	Extension of existing networks	12
3.2.5	Ethernet/IP communication	12
3.3	Ethernet topologies	13
3.3.1	Key	16
3.3.2	Ethernet loop without OPC server	17
3.3.3	Ethernet loop with OPC server	18
3.3.4	Ethernet/CAN double loop	20
3.3.5	Ethernet backbone with sub-loops (Ethernet/CAN)	21
3.3.6	Connecting Ethernet loops	23
3.4	UGM-2040 networks with dual homing	25
3.4.1	Standard Ethernet settings of FPA-5000 with UGM-2040	25
3.4.2	FPA-5000 with basic network connection to UGM-2040	26
3.4.3	FPA-5000 - UGM-2040 dual homing	27
3.4.4	Redundant FPA-5000 - UGM-2040 dual homing	27
3.4.5	FPA-5000 CAN loop - UGM-2040 dual homing	28
3.4.6	Redundant FPA-5000 CAN loop - UGM-2040 dual homing	29
3.5	Condition monitoring	30
4	**CAN networking**	**33**
5	**RPS settings**	**36**
5.1	FPA-1200/FPA-5000 network nodes	36
5.2	Line numbers	36
5.3	Switches	37
5.4	OPC servers	38
5.5	UGM-2040 servers	38
6	**Installation**	**39**
6.1	Installing media converters in the mounting frame	39
6.2	Installing media converters in PSS 0002 A/USF 0000 A	40
6.3	Settings on media converter	41
6.4	Installing switches in PSS 0002 A/USF 0000 A	42
6.5	Settings on switch	43

6.5.1 Assign IP address 44
6.5.2 Program redundancy settings 44
6.5.3 Programming the fault relay 45
6.5.4 Programming connection monitoring 45
6.5.5 QoS priority, only for UGM-2040 46
6.6 CAN network 47

7 Connections 57
7.1 Cabling of panel controller 57
7.1.1 Media converters and power supply 57
7.2 Switch with power supply and fault relay 58
7.3 Cabling of FMR-5000 remote control unit 62

A Appendix 64
A.1 Ethernet error messages 64
A.2 Non EN 54-compliant topologies 65
A.2.1 Non-redundant network with switches 65
A.2.2 Redundant RSTP network with switches 66
A.2.3 Redundant dual homing network with switches 67
A.2.4 Redundant RSTP network with switches and CAN/Ethernet loops 68

Glossary 70

Index 73

1 Safety instructions

NOTICE!
An exclusive Ethernet network is required in order to set up a central fire alarm network. For safety reasons, no networks used for any other purpose may be used in this capacity.

NOTICE!
To ensure that the network is set up in compliance with EN 54, use only components that have been approved for use in central fire alarm networks.

NOTICE!
For security reasons, do not use open access via the internet for programming and remote diagnosis. Use VPN-protected access.

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

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

2 Short Information

This document is aimed at readers with experience in planning and installing EN 54-compliant fire alarm systems and who also have additional networking knowledge.
Network topologies that are not EN 54-complaint and which require extensive knowledge of network technology are described in the appendix. These topologies are therefore only suitable for applications not compliant with any standard and require exact clarification with the customer.

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

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

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

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

NOTICE!
Dear Customer,
We work tirelessly to keep our documentation up to scratch. Should you have any suggestions, however, or if you have discovered an error, please e-mail us at ST.TechComFire@de.bosch.com.

3 Ethernet networking

3.1 Procedure

There are several procedures for creating a 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.

3.1.1 Standard procedure for smaller projects

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

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

If you configure the network settings on the control panels first, this will give you the advantage that you can then program all of the other control panels in the network from one control panel.

3.1.2 Medium-sized and large projects

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

1. Plan out the network.
2. Produce a configuration of the network without peripherals with FSP-5000-RPS.
3. Print the network information out for safe keeping, or store the information on the laptop.
4. Install the network cables and check individual sections or loops.
5. Install the panels and commission them as stand-alone panels.
6. Install the peripherals in the panels.
7. Configure each of the panels with RPS.
8. Ensure that the individual panels are working correctly.

9. Commission the individual loops of the network one after the other, according to the topology.
   Start with the backbone.
   - Produce a configuration for the backbone in RPS. Import all of the necessary panel configurations. Configure the network settings and print them out.
   - Connect all panels to the network.
   - Configure the network settings for the individual control panels directly at the panel controller as per the printout.
   - Reset each of the control panels in order to load the network configuration.
   - "PING" the neighboring panels in order to check the network.
   - Commission the entire backbone and rectify any errors.

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

3.2 Special features of the FPA network

In the panel network, the Ethernet network connections are monitored continuously. If a connection has been severed, the interruption is detected. Repaired connections are also detected.

MAC addresses

Each panel controller has three MAC addresses.
- MAC address for the host
- MAC address for network connection 1 (Eth 1)
- MAC address for network connection 2 (Eth 2)

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

3.2.1 Protocols

SNMP

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

NOTICE!

The FPA panel network uses the following SNMP password: PUBLIC

LLDP

LLDP is a basic protocol standardized by the IEEE that is used to share network information between neighboring devices. This information is
- provided as part of the SNMP data and
- displayed via the panel controller as part of the network diagnostic data.

RSTP

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

The protocol is used for exactly this purpose in the FPA-5000 network.

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

Dual homing

Dual homing ensures that one connection is always active for a network device. The second connection is deactivated. If the first connection fails, the second one is activated.
Dual homing is only intended for a redundant connection to the UGM-2040.

3.2.2 Network diameter

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

Definition

The diameter of a network corresponds to the number of RSTP switches on the longest possible section without loops between any two end points in the network.
The following must be taken into account in relation to a FPA-RSTP Ethernet network:

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

Key

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

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

Figure 3.1 Network diameter of a loop with 2 panels

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

Figure 3.2 Network diameter of a loop with 6 panels

In the case of complex topologies consisting of a backbone and sub-loops that are connected to each other via RSTP switches not integrated into the MPC, the RSTP switches must also be included.

Figure 3.3 Network diameter of a backbone with sub-loops

Figure 3.3 shows that the longest path must always be found for the diameter.

3.2.3 Cables used

Use only the following cables for networking:

- Ethernet cable

  Ethernet patch cable, shielded, CAT5e or better.

  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.

3.2.4 Extension of existing networks

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

3.2.5 Ethernet/IP communication

In the panel network, the Ethernet interface and IP protocols are used for different services. These services are panel networking over IP, OPC servers, and condition monitoring. The Ethernet interface can be disabled completely or its use disabled only for panel networking over TCP/IP. Disabling the interface or panel networking over TCP/IP may be necessary if the panels are networked via CAN.

Enabling services

- OPC servers
  Add an OPC server to the RPS configuration
- Condition monitoring
  Activate the relevant check box in RPS
- Panel networking over TCP/IP
  In RPS, enable panel-to-panel communication in the Ethernet network

  Disable panel communication over TCP/IP if the Ethernet interface of the panel controller is to be used only for communicating with an OPC server or for condition monitoring. This is important because data could otherwise be transferred over the Ethernet unintentionally.

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

3.3 Ethernet topologies

Topologies

The following topologies are possible:

Ethernet loop without OPC server, *Page 17*
Ethernet loop with OPC server, *Page 18*

Ethernet/CAN double loop, *Page 20*

Ethernet backbone with sub-loops, *Page 21*

Connecting Ethernet loops, *Page 23*

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

NOTICE!
For each panel, a maximum of 512 detection points may be connected according to EN 54-2. If this number is exceeded, the panel must be designed redundantly. For technical reasons, a maximum of 2032 detection points can then be connected.

NOTICE!
If the panel acts as an interface with a CAN sub-loop, this panel must then also be designed redundantly according to EN 54-2 if more than 512 detection points are connected in the sub-loop.
This restriction does not apply in an Ethernet sub-loop, as the switches to connect the two loops perform the redundancy.

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

NOTICE!
The requirements of EN 54-13 for data transmission paths can only be met with fiber optic cable connections for Ethernet.
Connections within a housing may be established with Ethernet cables.

NOTICE!
Switches and media converters in Ethernet networks must be installed in FPA-5000 housings. Installation outside of the FPA-5000 housing is not compliant with EN 54.

NOTICE!
To ensure that the network is set up in compliance with EN 54, use only components that have been approved for use in central fire alarm networks.

NOTICE!
Networks with more than 20 RSTP switches or a diameter greater than 20 require special settings.
The standard setting for the IP configuration is only designed for networks with a maximum of 20 RSTP switches or a maximum network diameter of 20.

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

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

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

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

- IP settings
  - IP address 192.168.1.x
    The last digit of the IP address in the standard settings is always identical to the RSN set on the panel controller.
  - Network screen 255.255.255.0
  - Gateway 192.168.1.254
  - Multicast address 239.192.0.1
  - Port number 25001 - 25008 (only the first port can be set; 8 consecutive ports are always used)

- RSTP parameters (redundancy settings)
  - Bridge Priority 32768
  - Hello Time 2
  - Max. Age 20
  - Forward Delay 15

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

Settings for loops with more than 20 RSTP switches
If there are more than 20 RSTP switches in the network, you must adjust the RSTP settings on the panel controller and in the programming software. In-depth knowledge of networks is required for this. The panel controllers and RSTP switches are regarded as RSTP switches. Redundant panel controllers are not regarded as RSTP switches, as the switch contained within these is not operated as an RSTP switch.

Parameters
- A maximum of 32 nodes can be used in a loop.
- The diameter of the network must not be greater than 32, see *Section 3.2.2 Network diameter, page 9*
- The Ethernet transmission sections outside of the FPA housing must be designed as fiber optic cable connections.
- Owing to system constraints, a maximum of one panel only and three FMR-5000s can be used in a network in the case of the FPA-1200.
- Switches and media converters must not be used outside of FPA housings.

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

Additional information when using the OPC server
If you are using OPC servers in your network, these servers must be added to the RPS programming software.
You must perform the following settings in both the RPS software and on the OPC server:
- Network nodes
- Network group
- RSN
- IP Address
- Port

The OPC server uses port 25000 as standard.

NOTICE!
FSP-5000-RPS programming software:
Please note that you must assign the OPC server to each network node from which statuses are to be transmitted.

3.3.1 Key

Icon	Description
	TX Ethernet cable (copper)
	FX Ethernet cable (fiber optic cable)
	TX or FX Ethernet cable
	CAN-Bus
	FPA-5000/FPA-1200/FMR-5000
	FPA-5000 redundant
	RSTP switch
	Media converter

3.3.2 Ethernet loop without OPC server

For this configuration, the notes, settings, parameters and features specified in *Section 3.3 Ethernet topologies, page 13* apply.

Figure 3.4 Ethernet loop without OPC server

Key, see *Section 3.3.1 Key, page 16*

3.3.3 Ethernet loop with OPC server

For this configuration, the notes, settings, parameters and features specified in *Section 3.3 Ethernet topologies, page 13* apply.
The information given here expands on *Section 3.3 Ethernet topologies*.

The switch for connecting the OPC server must be programmed separately.
Program the IP address and redundancy settings of the switch, see *Section 6.5 Settings on switch, page 43*. As the switch is installed in the immediate vicinity (without intermediate space), the power supply does not have to be designed redundantly and the fault outputs are therefore not used.
Make sure that the RSTP settings in the panel controllers, RPS programming software and switch are identical.

The OPC server must be programmed separately.
Program the IP address, network nodes, network group and RSN, see *Section 5.4 OPC servers, page 38*.
The OPC server uses port 25000 as standard.
Make sure that the settings in the RPS programming software and OPC server are identical.

Parameters

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

Figure 3.5 Ethernet loop with OPC server to non-redundant panel

Key, see *Section 3.3.1 Key, page 16*

Figure 3.6 Ethernet loop with OPC server to redundant panel

Key, see *Section 3.3.1 Key, page 16*

3.3.4 Ethernet/CAN double loop

For this configuration, the notes, settings, parameters and features specified in *Section 3.3 Ethernet topologies, page 13* apply.

Figure 3.7 Double loop of Ethernet and CAN

Key, see *Section 3.3.1 Key, page 16*

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

For this configuration, the notes, settings, parameters and features specified in *Section 3.3 Ethernet topologies, page 13* apply.
The information given here expands on *Section 3.3 Ethernet topologies*.

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

Please note that with this topology you are required to determine the network diameter, see *Section 3.2.2 Network diameter, page 9*. Only RSTP devices are included in the network diameter, CAN-networked panels are disregarded.

NOTICE!
If the panel acts as an interface with a CAN sub-loop, this panel must then also be designed redundantly according to EN 54-2 if more than 512 detection points are connected in the sub-loop.
This restriction does not apply in an Ethernet sub-loop, as the switches to connect the two loops perform the redundancy.

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

NOTICE!
For all panels and switches in the backbone, set a higher RSTP priority than in the sub-loops. This 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 loops are part of the backbone!
Use a RSTP priority of 16384 in the backbone.

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

Settings for loops with more than 20 RSTP devices
Panel controllers connected via CAN are not regarded as RSTP switches when determining the network diameter.

The switches for connecting the OPC server and the sub-loops must be programmed separately.
Program the IP address and redundancy settings of the switches, see *Section 6.5 Settings on switch, page 43*. For this topology, the fault outputs of the switch only have to be used if you have designed the power supply for the switch redundantly or there is a switch-to-switch connection, see *Section 7.2 Switch with power supply and fault relay, page 58*.
Make sure that the RSTP settings in the panel controllers, RPS programming software and switch are identical.

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

The OPC server must be programmed separately.

Program the IP address, network nodes, network group and RSN, see *Section 5.4 OPC servers, page 38*.

The OPC server uses port 25000 as standard.

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

Parameters

– The OPC server may be connected via an Ethernet cable or fiber optic cable

Figure 3.8 Ethernet backbone with sub-loops

Key, see *Section 3.3.1 Key, page 16*

3.3.6 Connecting Ethernet loops

For this configuration, the notes, settings, parameters and features specified in *Section 3.3 Ethernet topologies, page 13* apply.
The information given here expands on *Section 3.3 Ethernet topologies*.

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

Additional settings
This topology is a special instance of the Ethernet backbone with sub-loops, see *Section 3.3.5 Ethernet backbone with sub-loops (Ethernet/CAN), page 21*. 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.

The switches for connecting the OPC server and the second loop must be programmed separately.
Program the IP address and redundancy settings of the switch, see *Section 6.5 Settings on switch, page 43*. For this topology, the fault outputs of the switch only have to be used if you have designed the power supply for the switch redundantly, for connections see *Section 7.2 Switch with power supply and fault relay, page 58*.
Make sure that the RSTP settings in the panel controllers, RPS programming software and switch are identical.
Change the RSTP priority for the switches for connecting the two loops, as they belong to the backbone.

The OPC server must be programmed separately.
Program the IP address, network nodes, network group and RSN, see *Section 5.4 OPC servers, page 38*.
The OPC server uses port 25000 as standard.
Make sure that the settings in the RPS programming software and OPC server are identical.

Parameters
– The OPC server may be connected via an Ethernet cable (copper) or fiber optic cable
In these examples, loop a is the backbone. Loop b is the sub-loop.

Figure 3.9 Connecting Ethernet loop via a non-redundant panel

Figure 3.10 Connecting Ethernet loop via a redundant panel

Key, see *Section 3.3.1 Key, page 16*

3.4 UGM-2040 networks with dual homing

The topologies to be installed and the network settings to be programmed can be obtained from your UGM-2040 planner.

UGM-2040 topologies

Connection to switches in the UGM-2040.

1. FPA-5000 via Ethernet to UGM (max. 512 detectors per panel)
2. FPA-5000 via redundant Ethernet to UGM (max. 512 detectors per panel)
3. Redundant FPA-5000 via redundant Ethernet to UGM (more than 512 detectors)

NOTICE!
All FPA panel controllers and UGM servers must be located in the same subnetwork. However, each FPA configuration must have a different multicast address.

NOTICE!
RSTP is not permitted in applications with UGM-2040 with dual homing.

NOTICE!
Use only media converters to connect the FPA-5000/FPA-1200 via FX.

NOTICE!
Due to the technical restriction on the number of detectors in the panel network, a maximum of 2032 detection points may be used for each redundant panel.

3.4.1 Standard Ethernet settings of FPA-5000 with UGM-2040

In the standard settings of the FPA-5000, both the FSP-5000-RPS programming software and the control unit adopt the set RSN as the last number of the IP address.
You can deviate from the standard values specified here depending on the configuration required.

NOTICE!
- Correct setting of the RSN on the panel controllers and in the FSP-5000-RPS programming software is a requirement for a run-capable network.
- The IP address, network screen and gateway form a common subnetwork of all connected Ethernet devices.
- The multicast address and port number separate the FPA networks.

When connecting the FPA-5000 to the UGM-2040, you only have to perform Ethernet network settings on the connection panel.

- IP settings
  - IP address 192.168.1.x
    The last digit of the IP address in the standard settings is always identical to the RSN set on the panel controller.
  - Network screen 255.255.255.0
  - Gateway 192.168.1.254
  - Multicast address 239.192.0.1
  - Port number 25001

- Redundancy settings:
  - None, with basic network connection for FPA-5000.
  - Dual homing, for FPA-5000 with redundant network connection.

You can deviate from the standard values specified here depending on the configuration required.

The following applies to the nth RPS configuration or the nth FPA network:

- IP settings
  - IP address 192.168.n.x

    The last digit of the IP address (x) in the standard settings is always identical to the RSN set on the panel controller.

    The RPS configuration/FPA network (n) determines the penultimate digit of the IP address.
  - Network screen 255.255.0.0
  - Gateway 192.168.n.254
  - Multicast address 239.192.0.n
  - Port number 25001+n*10
- Redundancy settings:
  - None, with basic network connection for FPA-5000.
  - Dual homing, for FPA-5000 with redundant network connection.

3.4.2 FPA-5000 with basic network connection to UGM-2040

Figure 3.11 Non-redundant panels to UGM-2040

NOTICE!
Please note that the connection to the UGM is established without redundancy of the transmission path. Please check that this setup is permissible for your application.

Parameters

- The panels connected to the UGM-2040 must not communicate with each other. Each panel therefore requires a separate multicast address and a dedicated port number range.
- Each panel needs a separate RPS configuration.
- Owing to system constraints, a maximum of one panel only and three FMR-5000s can be used in a network in the case of the FPA-1200.

Features

- The network is EN 54-compliant.
- RSTP may not be used.

3.4.3 FPA-5000 - UGM-2040 dual homing

Figure 3.12 Non-redundant panels to UGM-2040 with dual homing

NOTICE!
Please note that the panel controller is not designed redundantly. Please check that this setup is permissible for your application.

Parameters

- The panels connected to the UGM-2040 must not communicate with each other. Each panel therefore requires a separate multicast address and a dedicated port number range.
- Each panel needs a separate RPS configuration.
- Owing to system constraints, a maximum of one panel only and three FMR-5000s can be used in a network in the case of the FPA-1200.

Features

- The network is EN 54-compliant.
- RSTP may not be used.

3.4.4 Redundant FPA-5000 - UGM-2040 dual homing

Figure 3.13 Redundant panels to UGM-2040 with dual homing

Parameters

- The panels connected to the UGM-2040 must not communicate with each other. Each panel therefore requires a separate multicast address and a dedicated port number range.
- Owing to system constraints, a maximum of one panel only and three FMR-5000s can be used in a network in the case of the FPA-1200.
- Several RPS configurations in the same physical network require different multicast addresses and port number ranges.

Features

- The network is EN 54-compliant.
- RSTP may not be used.

3.4.5 FPA-5000 CAN loop - UGM-2040 dual homing

Figure 3.14 Non-redundant panel with CAN loop to UGM-2040 with dual homing

NOTICE!
Please note that the panel controller is not designed redundantly. Please check that this setup is permissible for your application.

Parameters

- The CAN loops connected to the UGM-2040 must not communicate with each other. Each CAN loop therefore requires a separate multicast address and a dedicated port number range.
- A maximum of 32 nodes can be used with an RPS configuration.
- CAN connections can be established as cable or fiber optic cable connections.
- Several RPS configurations in the same physical network require different multicast addresses and port number ranges.
- Owing to system constraints, a maximum of one panel only and three FMR-5000s can be used in a network in the case of the FPA-1200.

Features

- The network is EN 54-compliant.

– RSTP may not be used.

3.4.6 Redundant FPA-5000 CAN loop - UGM-2040 dual homing

Figure 3.15 Redundant panel with CAN loop to UGM-2040 with dual homing

NOTICE!
According to EN 54-2, a maximum of 512 detection points per panel (2032 in the case of a redundant panel) may be used. Due to the technical restriction on the number of detectors in the panel network, a total of no more than 32,512 detection points may be used for each CAN loop.

Parameters

– The CAN loops connected to the UGM-2040 must not communicate with each other. Each CAN loop therefore requires a separate multicast address and a dedicated port number range.
– A maximum of 32 nodes can be used with an RPS configuration.
– CAN connections can be established as cable or fiber optic cable connections.
– Several RPS configurations in the same physical network require different multicast addresses and port number ranges.
– Owing to system constraints, a maximum of one panel only and three FMR-5000s can be used in a network in the case of the FPA-1200.

Features

– The network is EN 54-compliant.
– RSTP may not be used.

3.5 Condition monitoring

NOTICE!
Ethernet connections used only to transfer condition monitoring data may be designed both as Ethernet cables and fiber optic connections. Please note the maximum cable permitted lengths.

NOTICE!
The connection used for condition monitoring must be without reverse capacitance.

NOTICE!
Please note that condition monitoring data is transferred in unencrypted form.

NOTICE!
FSP-5000-RPS programming software:
Please note that you must enable condition monitoring in each network node from which statuses are to be transmitted.

In the RPS programming software, you can temporarily start up condition monitoring for one month. This can be useful for troubleshooting, for example, and works without authentication of the condition monitoring system server. After a month, the function switches itself off again automatically.
For condition monitoring, you must enter the server IP address and port of the condition monitoring system server in the RPS programming software. Assign a unique Panel Network ID to the network.

Condition monitoring in the Ethernet network

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

The switch for connecting the condition monitoring system server must be programmed separately.

Program the IP address and redundancy settings of the switch, see *Section 6.5 Settings on switch, page 43*. As the switch is installed in the immediate vicinity (without intermediate space), the power supply does not have to be designed redundantly and the fault outputs are therefore not used.

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

Condition monitoring in the CAN network

Because condition monitoring data can be transferred only over the Ethernet network, each panel in a CAN network must be connected to the router for data transfer purposes.

NOTICE!
As CAN network traffic is not transferred through the Ethernet connection, you must switch off panel networking over IP in the RPS programming software.
If this is not switched off, the network will not be compliant with EN 54.

4 CAN networking

Up to 32 panel controllers, remote keypads and OPC servers can be combined to form a network.
Depending on the intended application, different panel controllers and remote keypads can be divided into groups and defined as network nodes or local nodes. As a rule, within any given group, only the status of control panels within the defined group can be displayed. The status of all control panels can be displayed and/or processed from network nodes, irrespective of the group to which the panels belong.
The panels can be networked redundantly as a loop via CAN1 and CAN2.

FOC networking

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

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

Loop topology

- In loop topology, the CAN cable is always routed from a CAN1 terminal to a CAN2 terminal [CAN1 ⇒ CAN2].
  A CAN segment thus consists of two bus users. The cable length depends on the cable cross-section.
- Due to the maximum of 32 nodes and the maximum cable length of 1000 m between nodes, a system can be installed with a total cable length of 32 km.

Networking of panels and remote keypads

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

Topology		FPA-1200	FPA-5000
	Standalone panel	Possible	Possible
	Standalone panel, redundant	Not possible	Possible
	Loop	1 FPA-1200 + max. 3 FMR-5000	Max. 32 FPA-5000/FMR-5000
	Loop with redundant panel	Not possible	Max. 32 FPA-5000/FMR-5000 + redundant FPA-5000
Refer to the limits determined by the network topology. **As the FPA-1200 is not operated as the redundant panel, DIP 6 on FPA-1200-MPC is not functional!**			

Limits in network

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

Networked panels and remote keypads are known as "nodes".

- The number of detection points in a network is limited to 32,512.
- The number of detection points per panel operated in a network is limited to 2032.
- The number of nodes per system depends on the type of topology.
  A node is either an MPC Panel Controller or an FMR-5000 Remote Keypad.
- The number of nodes in loop topology is limited to 32.
- The number of nodes per CAN segment is limited to eight.
  A CAN segment is the physical connection of a CAN line.
- Up to three remote keypads to a specific panel can be directly assigned to the network using the FSP-5000-RPS Programming Software.

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

Cable type for networking

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

The maximum permitted cable length depends on the loop resistance of the cable used and on the number of communicating nodes (see *Figure 4.1*).

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 (see *Figure 4.1*).

Figure 4.1 Achievable cable length, depending on the number of nodes and the cable resistance

L = cable length in meters

N = number of nodes

5 RPS settings

You can program the entire FPA 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 FPA fire alarm control panels 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.

5.1 FPA-1200/FPA-5000 network nodes

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

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

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

5.2 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 a 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.

Figure 5.1 Example of a network and the possible line numbering

5.3 Switches

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

5.4 OPC servers

If you are using OPC servers in your network, these servers must be added to the RPS programming software.
You must perform the following settings in both the RPS software and on the OPC server:

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

The OPC server uses port 25000 as standard.

NOTICE!
FSP-5000-RPS programming software:
Please note that you must assign the OPC server to each network node from which statuses are to be transmitted.

5.5 UGM-2040 servers

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

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

Figure 5.2 Example of line numbering for the UGM-2040

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

6 Installation

Checklist

Before starting with the installation of the FPA-5000 panel network, please review all of the points set out below.

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

DANGER!

Laser light.

Do not look directly into the beam with the naked eye or with visual instruments of any kind (e.g. magnifying glass, microscope). Failure to observe this notice poses a danger to the eyes at a distance of less than 100 mm. The light emerges at the visual terminals or at the end of the fiber optic cables connected to these. CLASS 2M light-emitting diode, wavelength 650 nm, output < 2 mW, in accordance with DIN EN 60825-1:2003-10.

6.1 Installing media converters in the mounting frame

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

Figure 6.1 Installation of FPM-5000-KMC bracket in mounting frame

Figure 6.2 Installation of media converters in the FPM-5000-KMC bracket

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

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

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

Figure 6.3 Installation of FPM-5000-KES bracket in housings

Figure 6.4 Installation of media converters in the FPM-5000-KES bracket

6.3 Settings on media converter

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

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

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

NOTICE!
Use only the following cables for networking:

- Ethernet cable
  Ethernet patch cable, shielded, CAT5e or better.
  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
  Please note the minimum bending radii specified in the cable specification.

NOTICE!
Please refer to the installation guides for the mounting kits for information on how to install media converters in the housings of the FPA-5000/FPA-1200.
FPM-5000-KMC (F.01U.266.845) or 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 follows:

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

6.4 Installing switches in PSS 0002 A/USF 0000 A

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

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

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

Figure 6.5 Installation of FPM-5000-KES bracket in housings

Figure 6.6 Installation of switches in the FPM-5000-KES bracket

6.5 Settings on switch

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

NOTICE!
Please refer to the manufacturer's user guide for an exact description of the installation and configuration of the switches.
As of the present date (03/2012) , the following access data are valid:
– User: admin
– Password: private

Use a browser to call up the configuration user interface for the switches.
You must perform the following settings in the switch:
– Assign IP address
– Program redundancy settings
– Program fault relay (optional)
– Program connection monitoring (optional)

6.5.1 Assign IP address

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

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

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

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

6.5.2 Program redundancy settings

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

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

6.5.3 Programming the fault relay

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

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

Use a browser to go to the configuration user interface for the switch.
Under **Diagnosis -> Detection Contact** in the **Detection Contact 1** tab, set the **Mode Detection Contact** to **Device Status**.
Under **Diagnosis -> Device Status** in the **Monitoring** field, set the following values:
- **Power Supply Unit 1**: Monitor
- **Connection Error**: Monitor

All other settings must be set to Ignore.

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

Click on "**Write**".

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

6.5.4 Programming connection monitoring

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

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

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

6.5.5 QoS priority, only for UGM-2040

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

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

6.6 CAN network

Networking and Interfaces

The panel controller has

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

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

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

▶ the network is designed for multiple building connections (e. g. there must be no technical interference due to differences in grounding potential);

▶ the bandwidth of the bus users is sufficient for the network.

Figure 6.7 MPC, USB and RS232 interfaces

Figure 6.8 MPC connection to BIS via OPC server

Addressing and Settings in the Network

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

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

The panels and remote keypads are identified in the network by a unique address. This address is set on the rotary switches and is known as the rotary switch number (RSN) (see the figures in the circle on the circuit diagrams). The rotary switches are located on the rear of the panel controller (see *Figure 6.9*).

Note the address on the sign below the rotary switches (see *Figure 6.9*, step 2).

The DIP switches are located on the rear of the panel controller (see *Figure 6.9*).

Mark the selected setting on the sign above the DIP switches (see *Figure 6.9*, step 4).

NOTICE!

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

Addressing and Configuration of MPC Panel Controller

Figure 6.9 MPC Panel Controller, addressing

Figure 6.10 MPC Panel Controller, network connections

Standalone Panel and Redundant Standalone Panel

Figure 6.11 Standalone panel (regular and redundant): Configuration in network

Loop

Figure 6.12 Loop topology

Loop with redundant panel

Figure 6.13 Loop topology with redundant panel

Bus

Figure 6.14 Bus Topology

Bus with Redundant Panel

Figure 6.15 Bus topology with redundant panel

Bus with Redundant Network

Figure 6.16 Bus topology with redundant network

Bus with Redundant Network and Redundant Panel

Figure 6.17 Bus topology with redundant network and redundant panel

7 Connections

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

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

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

7.1 Cabling of panel controller

7.1.1 Media converters and power supply

Connection of media converters

NOTICE!
Please note the direction of transmission of the FOC fibers when connecting the FX cabling of the media converters.

Figure 7.1 Connection of media converter to the power supply and panel controller

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

7.2 Switch with power supply and fault relay

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

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

NOTICE!

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

– There is a connection between two 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 MPC.

Figure 7.2 Connection of switch to the power supply and panel controller

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

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

NOTICE!
In the case of a redundant panel controller, the IOP module must not be located on the PRS 0002 A panel rail short. The panel rail short must not be fitted with modules.

Figure 7.3 Connection of switch to the power supply and IOP

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

7.3 Cabling of FMR-5000 remote control unit

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

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

NOTICE!
Use only media converters to connect a FMR-5000 remote control unit to an Ethernet panel network.
The use of switches is not permitted for the remote control unit.

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

Figure 7.4 Cabling of remote control unit

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

A Appendix

A.1 Ethernet error messages

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

Physical address	Logical address	Error message	Description and possible cause
Group faults relating to general network malfunction			
135.0.1.0	Network 1.0	Allgemeine Netzwerk Störung	There is an incompatible version of the panel network software. There are two different software versions
Group faults relating to network			
135.0.6.1	Network 2.1	Doppelte IP Adresse	An IP address has been assigned twice.
135.0.6.2	Network 2.2	IP Einstellungen	The IP configuration of the reporting panel is different to the RPS configuration
135.0.6.3	Network 2.3	Redundanz Einstellungen	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 Bus 1 Störung	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 Bus 2 Störung	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 Line 1 - Störung	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 Line 2 - Störung	Data transmission to Ethernet line 2 is restricted. Possible causes include: cable breaks, cable not connected, cable interference.

A.2 Non EN 54-compliant topologies

NOTICE!
Non EN 54-compliant topologies are not supported.

A.2.1 Non-redundant network with switches

NOTICE!
This network is not EN 54-compliant.

NOTICE!
This network topology must only be installed and set up by persons with in-depth knowledge of networks.

NOTICE!
The network must not use layer 3 switches.

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

Parameters
- A maximum of 32 nodes may be used in a network.
- The Ethernet transmission sections can be designed as fiber optic cable connections.
- A maximum of one panel only and 3 FMR-5000s can be used in a network in the case of the FPA-1200.

Features
- The network is not EN 54-compliant.

A.2.2 Redundant RSTP network with switches

NOTICE!
This network is not EN 54-compliant.

NOTICE!
This network topology must only be installed and set up by persons with in-depth knowledge of networks.

NOTICE!
The network must not use layer 3 switches.

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

Parameters
- A maximum of 32 nodes may be used in a network.
- The diameter of the network must not be greater than 32, see *Section 3.2.2 Network diameter, page 9*
- The Ethernet transmission sections can be designed as fiber optic cable connections.
- A maximum of one panel only and 3 FMR-5000s can be used in a network in the case of the FPA-1200.
- The network must be RSTP-compliant according to 802.1D-2004.

Features
- The network is not EN 54-compliant.
- The network uses RSTP.

A.2.3 Redundant dual homing network with switches

NOTICE!
This network is not EN 54-compliant.

NOTICE!
This network topology must only be installed and set up by persons with in-depth knowledge of networks.

NOTICE!
The network must not use layer 3 switches.

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

Parameters
- A maximum of 32 nodes may be used in a network.
- The diameter of the network must not be greater than 32, see *Section 3.2.2 Network diameter, page 9*
- The Ethernet transmission sections can be designed as fiber optic cable connections.
- A maximum of one panel only and 3 FMR-5000s can be used in a network in the case of the FPA-1200.

Features
- The network is not EN 54-compliant.
- The network uses dual homing.

A.2.4 Redundant RSTP network with switches and CAN/Ethernet loops

NOTICE!
This network is not EN 54-compliant.

NOTICE!
This network topology must only be installed and set up by persons with in-depth knowledge of networks.

NOTICE!
The network must not use layer 3 switches.

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

Parameters
- A maximum of 32 nodes can be used in a network including CAN loops.
- The diameter of the network must not be greater than 32, see *Section 3.2.2 Network diameter, page 9*
- The Ethernet and CAN transmission sections can be designed as fiber optic cable connections.
- A maximum of one panel only and 3 FMR-5000s can be used in a network in the case of the FPA-1200.
- The network must be RSTP-compliant according to 802.1D-2004.

Features
- The network is not EN 54-compliant.
- The network uses RSTP.

FPA-5000/
FMR-5000
CAN
FPA-5000/
FMR-5000
FPA-5000
OPC-Server
FPA-5000
FX
FPA-5000/
FMR-5000
FPA-5000/
FMR-5000
FPA-5000
FX
FPA-5000/
FMR-5000
FPA-5000/
FMR-5000

Glossary

D

Dual homing	Redundancy technology whereby one device uses a primary/active connection and a secondary/standby connection to connect a network. If the primary connection fails, the secondary connection is used.

E

Ethernet	Ethernet is also referred to as LAN technology. All devices connected in a local area network (LAN) can share data in the form of data packages.
Ethernet port	A communication channel that performs the assignment of the connections and data between server and client programs. Ports allow several connections to be established between the same server and client, for instance, and enable these connections to be supplied with data.
Ethernet/IP	This term is used to identify the FPA-5000 new network function as a holistic entity. Not to be confused with Ethernet Industrial Protocol (EIP).

F

Full duplex	A transmission mode in which a device can transmit and receive data simultaneously.

H

Half duplex	A transmission mode in which a device can transmit and receive data alternately.

I

IP	Abbreviation for Internet Protocol. Network protocol that displays the protocol range that facilitates internet networks. The task of the IP is to transport data packages from a transmitter via several networks to a receiver. It forms the basis of the internet.
IP address	Internet Protocol address. Every device that is connected to an IP network is given a numerical address and is consequently able to share data.
IP gateway	Node points (hosts) that connect various networks to each other. They can also use different protocols to do this.
IP host	IP-capable network device that is connected to an IP network.
IP multicast	A method for forwarding IP data packages to a group of interested receivers. This method is geared towards the use of receiver groups whereby it is not essential for the identity of each receiver to be known. Multicast uses the available network infrastructure extremely efficiently, as only one data package has to be sent, even if a large number of receivers is being addressed.
IP netmask	Multiple-digit binary number that divides an IP address into a network identification and host identification part. It is usually specified in 4 decimal numbers that are separated by decimal points. Each decimal number represents 8 bits (e.g. 255.255.252.0).
IP packet	Basic element of internet data communication; consists of header data (information of an IP package relevant to the protocol) and the payload.

IP router	This is a device that forwards data packages between computer networks.
IP subnetwork	Subnetwork within a larger network. A subnetwork is defined in the network identification part of an IP address.
IPv4	Internet Protocol version 4. The first version to be used worldwide. In future it will be replaced with IPv6 for internet use.

L

LAN	Local Area Network. This is a network that connects devices within a confined geographical area.
LLDP	Link Layer Discovery Protocol. LLDP is a basic protocol used by network devices to display its identity, capabilities and neighbors in a IEEE 802 LAN. You can identify devices within a network and determine the network topology.

M

MAC	Media Access Control. A level within an Ethernet device that provides a standardized interface.
MAC Address	Media Access Control address. A 6-byte address that identifies an Ethernet device or logical group. The address area should not be ambiguous worldwide: an Ethernet device manufacturer retains certain address areas that it can assign uniquely to each device manufactured and delivered.
Multicast address	Data packages can be sent to a number of receivers simultaneously. The address range for this is IPv4 224.0.0.0 to 239.255.255.255.

Q

QoS	Quality of Service. Within the network technology, this term defines the quality of services. In IP networks the following parameters are usually recorded within the quality of service: package loss rate, latency and data throughput.

R

Redundant Ethernet	Ethernet networks do not allow loops in the Ethernet topology. A loop would allow Ethernet frames to move round the network endlessly. Redundant Ethernet-based networks therefore require protocols that manage the infrastructure and detect and rectify errors therein. Such protocols include STP and the Rapid Spanning Tree Protocol.
RSN	
RSTP	Rapid Spanning Tree Protocol. RSTP is an improvement on the STP protocol. Redundant paths in local networks can be deactivated and reactivated again. It is faster than STP .

S

SNMP	Simple Network Management Protocol. Network management protocol that allows remote monitoring, diagnosis and configuration of devices within a network. Network elements are monitored and controlled by a central station.

STP	Spanning Tree Protocol. STP is a protocol that was developed in order to avoid loops in an Ethernet network. It deactivates redundant connections in order to create a network with a tree structure. If there is a failure or fault in active connections, the protocol can reactivate redundant connections.
Switch	A distributor that forwards Ethernet frames between at least two Ethernet ports. It selectively chooses the correct Ethernet connection on the basis of the destination address in the Ethernet frame. A synonym for "network switch" or "multi-port network switch".

T

TCP	Transmission Control Protocol. This is a connection-based transport protocol. The transmitter and receiver are in virtual contact through constant check messages during data transmission.
TCP port number	A TCP port number is used to identify an end point on an IP device, generally a server service or client communication handle. Please note that a TCP port number is in principle comparable to the UDP port number, but they are technically different.

U

UDP	User Datagram Protocol. This is part of the IP protocol suite and ensures connectionless, non-reliable communication between IP end points. The information in a UDP protocol header is only used by the end points.
UDP port number	A UDP port number is used to identify an end point on an IP device, generally a server service or client communication handle. Please note that a UDP port number is in principle comparable to the TCP port number, but they are technically different.

V

VPN	Virtual private network. A VPN is a network that uses the data transfer service of another (public) network to establish a private network. It is often used to facilitate a private LAN via a public internet infrastructure using encrypted connections.
VPN router	VPN routers are devices that transfer packages between private networks via a different (public) network.
VPN tunnel	A VPN tunnel is the data path between VPN routers that use a public network for this purpose, generally the public internet. A VPN tunnel is generally encrypted.

Index

A
Addressing 48
    rotary switch 48
B
Bus topology 48
C
CAN interface 33
D
DIP switches 48
Dual homing 9
E
Ethernet topologies 13
Ethernet, standard settings 14
F
Fiber optic cables
    EKS 33
L
Limits
    Network 34
LLDP 8
Loop topology 48
M
MAC address 8
N
Network
    Addressing 51
    Cable 34
    Cable length 35
    Cabling 34
    Fiber optic cable 33
    Limits 34
    Panel controller 47
Network diameter 9
Networking 33, 48
    Bus topology 48
    Cable length 34
    Fiber optic cable 33
    Loop topology 34, 48
    Panel controller 47
P
Panel controller
    Networking 47
Parameters
    RSTP 15
R
Redundancy
    Addressing 48
Redundant 48
Rotary switch 48
Rotary switch number (RSN) 48
RSTP 8
    Parameters 15
S
Standard settings, Ethernet 14
T
topologies, Ethernet 13
Topology
    Bus 48
    Loop 48

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com
© Bosch Sicherheitssysteme GmbH, 2012