OPC-Server

FSM-5000-OPC

en Technical description

Table of contents

1 Purpose

This document contains information on fire panels with OPC license and OPC Server version 2.0.x and upwards. It is about successfully configuring the panel network and the corresponding FSM-5000-OPC server to enable communication between both via a single Ethernet connection using any OPC client application. If you are using BIS 4.x as OPC client refer to the FSM-5000-OPC User Guide.
The reader must be familiar with OPC (OLE for process control) and the usage of fire alarm systems in general.

Notice!
Setting up and configuring an panel network controlled by an OPC server requires good IT knowledge.

The information refers to FSM-5000-OPC Version 2.0.x and later and supported panel software.

Figure 1.1: Panel network controlled by an OPC server with single Ethernet connection

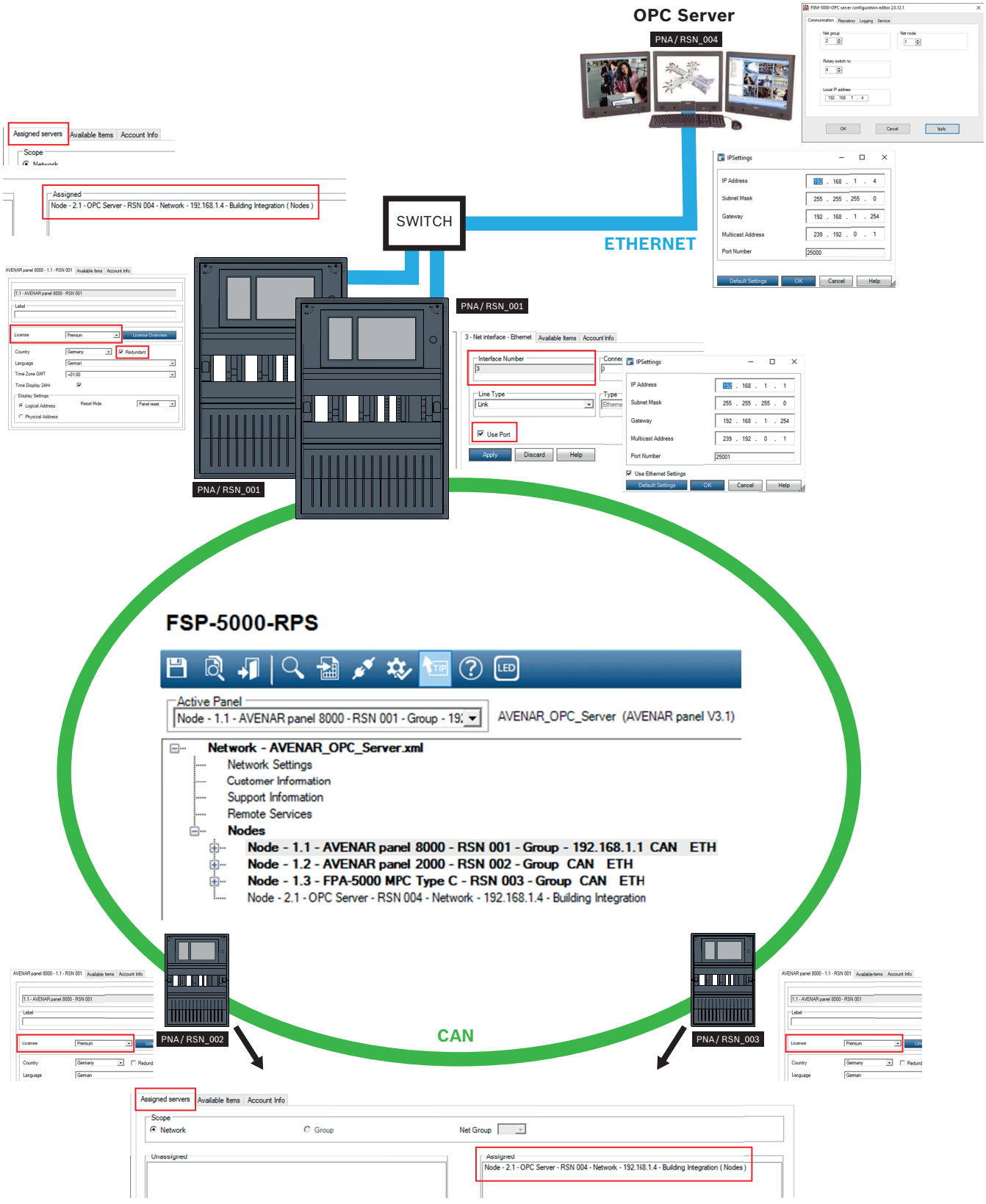

Figure 1.2: Panel network controlled by an OPC server with redundant panel

This document contains information on fire panels with OPC license and OPC Server version 2.0.x and upwards. It is about successfully configuring the panel network and the corresponding FSM-5000-OPC server to enable communication between both via a single or redundant Ethernet connection. In completing these steps successfully a functional interface is provided for a subsequent connection to BIS 4.x which functions as OPC client.

Notice!
Setting up and configuring an panel network controlled by an OPC server requires basic IT knowledge.

The information refers to FSM-5000-OPC Version 2.0.x and later and supported panel software.

Figure 1.3: Panel network controlled by an OPC server with single Ethernet connection

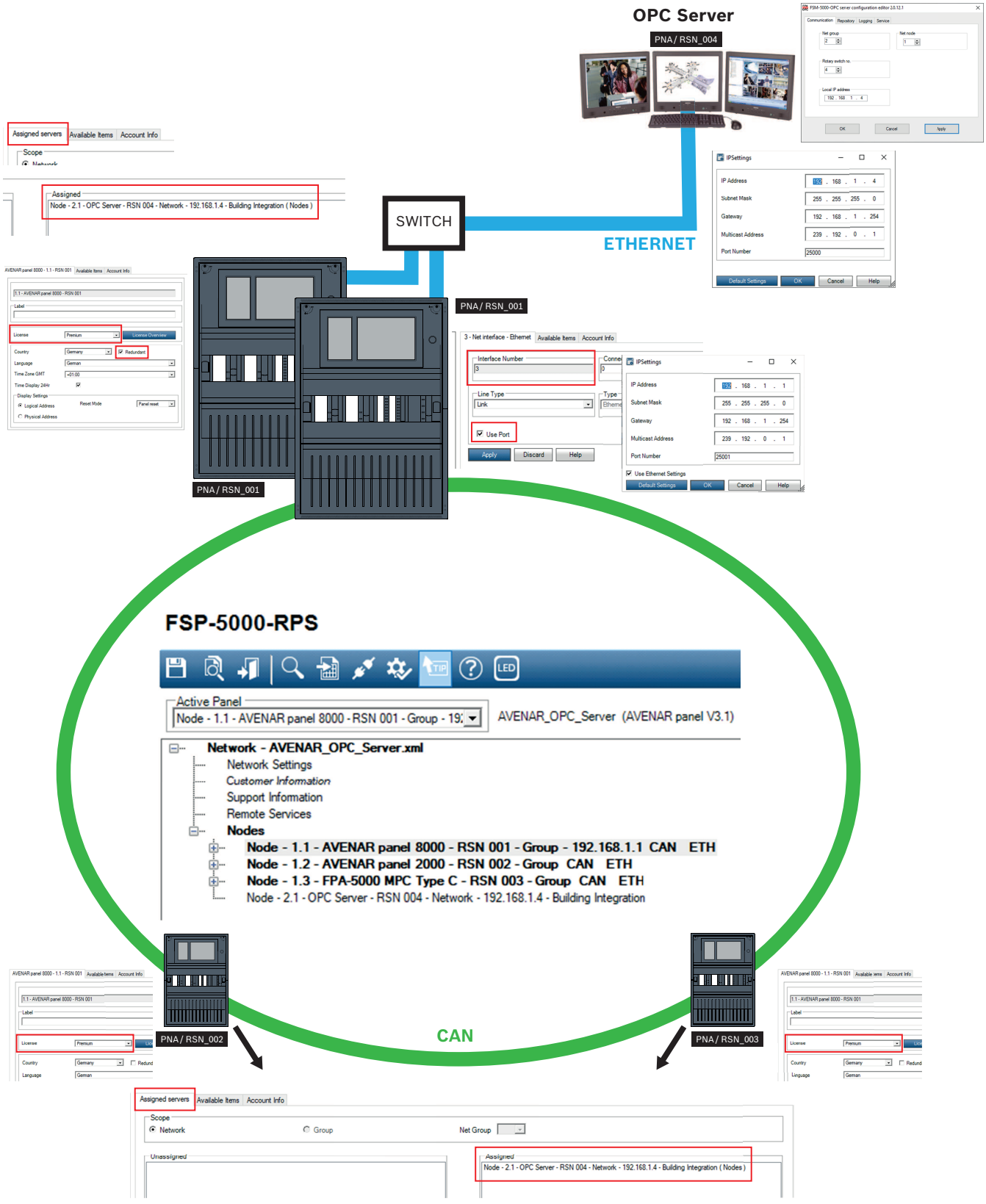

Figure 1.4: Panel network controlled by an OPC server with redundant panel

2 Preconditions

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

The following must be available to set up an OPC Server in a panel network:

- Panel with OPC license (e.g. AVENAR panel 8000 with premium license)
- Compatible FSP-5000-RPS Software
- FSM-5000-OPC Server version must be compatible to the respective panel release (Look up the compatible version in the readme file of the FSM-5000-OPC software)
- Existing Ethernet network with Cat. 5e cable
- PC to install FSM-5000-OPC on
- OPC client application (in this document the free Softing OPC Demo Client is used in the examples, see http://industrial.softing.com/en/products/functionality.html)

3 Installation

3.1 Installation of the OPC Software

Prerequisites:

– .NET Framework 4 must be installed to run FSM-5000-OPC
– Microsoft VC++ Redistributable for Visual Studio 2015 (32 bit)

Notice!
If the prerequisite software is not present, install it from the PreRequisites folder of the FSP-5000-RPS installation package or download it from http://www.microsoft.com/downloads/en/default.aspx

Task: FSM-5000-OPC is running on a PC.

1. Open the folder that contains the FSM-5000-OPC installation.
2. Click “Setup.exe” and follow the installation instructions.
3. Open the Configuration Editor:
   Start → All Programs → Bosch → FPA5000OPC-Server and run Configuration Editor
   or open Windows Explorer, navigate to
   C:\Program Files\Bosch\FPA 5000OPC-Server and run ConfigEditor.exe
4. Under the “Communications“ tab adopt the settings that were entered for the node “FPA5000 OPC Server” in the RPS configuration.
5. Configure the Windows firewall. The configuration depends on the operating system and the used firewall.
6. Restart the system.
   FSM-5000-OPC will be running after restart, indicated by a notification icon in the taskbar notification area.

Notice!
The installation of FSM-5000-OPC is only released for the Windows operating systems listed in Technical Data. For other operating systems the installation may succeed but was not tested and is therefore on your own risk.

3.2 Remote Access to the OPC Server from the Building Integration System (BIS)

Task: FSM-5000-OPC is running on a PC in your local network interconnected with the panel network. The OPC client application runs on a PC of the Building Integration System (BIS) in the same local network. It remotely accesses the FSM-5000-OPC server.

Server side PC

Notice!
Consider the naming conventions for users, groups and passwords (“MgtS-Service” “BISUsers“) given in this description. The Building Integration System (BIS) internally makes use of these conventions. As BIS internally always assumes the same user and password by convention it is not necessary to logon as a distinct user or enter the password. If you remotely access the FSM-5000-OPC server with another client, you are free to choose names and a password on the server side, as long as you specify the matching logon when your client connects to the OPC server.

All of the following settings refer to the PC running the OPC server.

Notice!
The following steps are based on the Windows 10 operating system. For all other operating systems the paths to the respective dialogs might be slightly different.

Create user „MgtS-Service“ manually

1. Go to **Local Group Policy Editor** and enter the following values:
   - **Username** (case sensitive): "MgtS-Service"
   - **Password**: Please contact BIS customer support if it is the BIS client you are using.
   - **Member of group**: Administrators
   - **User must change password at next logon**: NO
   - **User cannot change password**: YES
   - **Password never expires**: YES
2. Tab **Local Security Settings**:
   - **Log on as a service**: YES
   - **Log on as a batch job**: YES

Notice!
The user name and password must be identical with the user of the login server.

Create group BISUsers manually

1. Go to **Local Users Group Policy** and enter the following value:
   - Group name (case sensitive): **"BISUsers"**
2. Add the user “MgtS-Service” to that group
3. Add the user who logs in from the operating system of the login server and who operates the ConfigurationBrowser to that group too.

DCOM-Settings for the group BISUsers

1. Click Start > Run....
2. Type dcomcnfg <ENTER>.
3. Open the tree on the left side: **Console Root** > **Component Services** > **Computers** > **My Computer**.
4. Right click on **My Computer** and choose **Properties**.
5. Choose the **COM Security** tab.
6. Add the new group “BISUsers” by using **Access Permissions** - **Edit Defaults** - **allow Local and Remote Access**.
7. Add the new group “BISUsers” by using **Launch and Activation Permissions** - **Edit Defaults** - **allow Local and Remote Launch** and **allow Local and Remote Activation**.
8. Add the new group “BISUsers” by using **Launch and Activation Permissions** - **Edit Limits** - **allow Local and Remote Launch** and **allow Local and Remote Activation**.
9. Reboot the PC.

Set Local Security Policy

Perform the following procedure to set the Local Security Policy (e.g. Windows 10):

1. Go to **Start** - **Control Panel** - **Administrative Tools**, and select **Local Security Policy**.
2. Open the tree on the left side: **Security Settings** - **Local Policies**- **Security Options**.
3. Select on the right side**: Network access: Sharing and security model for local accounts**.

4. Right click on this selection to open **Properties** and choose **Classic- local users authenticate as themselves**.
5. Close all windows and restart the PC.
6. Open **dcomcnfg** and go to **services** (Local).
7. Select **FPA5000OPCServer** - **Properties** and open the **Log-On** tab
8. Choose radio button **This Account** - **User: MgtS-Service** and the password.
9. You are requested to restart the service in order to activate the changes. Select **Stop and Start** (or **Restart**).

Client side PC

On the PC running the FSM-5000-OPC client software connect to the server with the same logon you used to start the service. This also applies if you install both on the same PC. The OPC server installation routine installs the service for the local system account by default. Change the service to “MgtS-Service” when you use the OPC server with BIS.

3.3 Backward Compatibility

There are two setup packages to provide backward compatibility.
To install the respective file

1. Go to the Compatibility folder on the setup disk
2. Double click the respective msi-file

Notice!
Only use these packages if you require compatibility with solutions designed for versions prior to version 1.1 of FSM-5000-OPC server.

3.3.1 Package: BIS600StateConversion.msi

Description: States of the OPC server mapped to an offset of 600 instead of line status designed for backward compatibility of OPC Server version 2.0.x with older clients. For instance configurations read by BIS 1.0.x requires it in order to work with the 2.0.x OPC Server.
Postcondition: Registry entry for OPC configuration set.

3.3.2 Package: LanguageDependentCommand.msi

Description: The commands are language dependent like OPC Server 1.0.x. Designed for backward compatibility of OPC Server version 2.0.x with older clients. For instance configurations read by BIS 1.0.x requires it in order to work with the 2.0.x OPC Server.
Postcondition: Registry entry for OPC configuration set.

4 Technical Interface Description

The interface description explains the OPC interface of the server.

4.1 Items

In the OPC namespaces are items representing the data.

4.1.1 Naming

The items in the DA and AE namespaces are named according to the following scheme:
<PanelGroupNumber-PanelNodeNumber>.<SIType>.<SINumber>.<SISubnumber>

4.1.2 Item Properties and Event Attributes

The table shows the relevant properties of the items:

Property Name	Property ID	Property Type	Description
Description	101	BSTR	The short text of the item.
Command	5001	BSTR	Reference to the command list in the command item
Hierarchie	5556	BSTR	

The Property Command (5001) has the value that refers to the Property ID of its type in the Command Item. For example if the item has the value 5005 for Property Command (5001) than the property 5005 of the command item represents the type of the item with the command list.

4.1.3 Types

Each item has a type. Each type has a set of commands that it supports. The description of the command could be read from the command item. Also the supported commands are provided by the entry for the type in the command item.

4.1.4 Item States

Each item has a value that represents the current state of the item. Items do not use all of the possible states. The possible states of an item depend on the item type.

State Table	OPC Server Versions	Description
See appendix A.1	1.0.x 2.0.x in backward compatibility Mode	States mapped to 600
See appendix A.2	2.0.x in standard mode	The OPC server maps all states of the panel to the BIS/ UGM2020 states (LZs).

4.1.5 Command item

The command item describes the types and the commands of the item types.

Property Name	Property ID	Property Type	Description
Description	101	BSTR	Item decription

Property Name	Property ID	Property Type	Description
<ItemType1>	5001	BSTR	Command list of item type 1
...	...	...	...
<ItemTypeN>	5001 + N	BSTR	Command list of item type N

The command list of an item type is described in XML format. The possible commands of an item can be read in runtime by the OPC server after connection to the panel network.

4.1.6 Special items

For the operation of the FSM-5000-OPC server a panel with OPC license is necessary (e.g. AVENAR panel 8000 with premium license). A license can have three states:

Available	NORMAL
Running out	AC_COUNTDOWN_STARTED
Not available	AC_TAMPER

It is addressed by the item address <group of the OPC Server>.<node of the OPC Server>.SI_ADDRESSCARD.0.0.

4.2 Command handling

The possible commands with description of an item are read from the command item in XML format. To send commands to the OPC Server the command value will be written as value to the command item. The command value is also in XML format and can be derived from the command description.

4.2.1 Learning the commands

- Every item has a property 5001. The integer value of this property refers to a property index in item “CMD item” which contains the command description for the item.
- “CMD item” contains command descriptions for all items. “CMD item” is visible in the Data Access namespace.
- Items of the same type of functionality share the same command description. For example property 5027 of “CMD item” is described as “Input”. An item which has a property 5001 with a value of 5027 supports commands according to the command description of CMD#5027.
- The format of command descriptions is XML. This XML is a template for the command that will be sent back to the OPC Server. For item CMD#5027 (OPC syntax for the CMD item property with ID 5027) the value may be as following:

```
<nsPV:Commands xmlns:nsPV="file:///S3K/Proxyverwalter"
xmlns:nsMakroNotPV="file:///S3K/NichtProxyverwalter"><nsPV:Command
Name="ISOLATE_ON" Anzeigename="Isolate on" Description="Isolate a device"
OPCServerKlasse="MagicPanel OPC Server" /><nsPV:Command Name="ISOLATE_OFF"
Anzeigename="Isolate off" Description="UnIsolate a device"
OPCServerKlasse="MagicPanel OPC Server" /><nsPV:Command Name="WALKTEST_ON"
Anzeigename="Walktest on" Description="Walktest on"
OPCServerKlasse="MagicPanel OPC Server" /><nsPV:Command Name="WALKTEST_OFF"
Anzeigename="Walktest off" Description="Walktest off"
```

```
OPCServerKlasse="MagicPanel OPC Server" /><nsPV:Command Name="ACK"
Anzeigename="Acknowledge" Description="Acknowledge"
OPCServerKlasse="MagicPanel OPC Server" /><nsPV:Command Name="RESET"
Anzeigename="Reset" Description="Reset" OPCServerKlasse="MagicPanel OPC
Server" /></nsPV:Commands>
```

– The command description is a collection of <COMMAND> elements. Each element consists of a name, a display name and a description (language specific)

This is how to read all supported commands for an item. Read the OPC DA specification on how to achieve this programmatically (see www.opcfoundation.org).

4.2.2 Execution of commands

1. Create a new command in XML format. The XML command is based on the command template explained in Learning the commands. Here is an example on how to read the format. The description of this example and more examples can be found in Command Examples.

```
<nsPV:Command Name="ACK" Anzeigename="Acknowledge"
Description="Acknowledge" OPCServerKlasse="BoschFPA5000OpcServer1"
xmlns:nsPV="file:///S3K/Proxyverwalter" Sender="BIS" Adresse="Fire Panel
1-2.NAC.2"/>
```

You get the name of the command from the command description (e.g. “ACK”) and also “Anzeigename” and “Description”. The syntax of the “Address” value is described in section Naming.

The command can also contain parameters as an optional attribute but most commands do not require parameters. An exception is SET_TIME which requires five string parameters: hours, minutes, day, month, year. For details on how to pass parameters read the command description of SET_TIME:

```
<nsPV:Command Name="SET_TIME" Anzeigename="Zeit stellen" Description="Zeit
stellen" OPCServerKlasse="MagicPanel OPC Server">
<nsPV:Parameters><nsPV:Parameter ValueType="string" Name="Stunde"
Anzeigename="Stunden" Description="Stunde
2stellig"><nsMakroNotPV:ACTIVATION /></nsPV:Parameter><nsPV:Parameter
ValueType="string" Name="Minute" Anzeigename="Minuten" Description="Minuten
2stellig"><nsMakroNotPV:ACTIVATION /></nsPV:Parameter><nsPV:Parameter
ValueType="string" Name="Tag" Anzeigename="Tage" Description="Tage
2stellig"><nsMakroNotPV:ACTIVATION /></nsPV:Parameter><nsPV:Parameter
ValueType="string" Name="Monat" Anzeigename="Monate" Description="Monate
2stellig"><nsMakroNotPV:ACTIVATION /></nsPV:Parameter><nsPV:Parameter
ValueType="string" Name="Jahr" Anzeigename="Jahr" Description="Jahr
2stellig"><nsMakroNotPV:ACTIVATION/></nsPV:Parameter></nsPV:Parameters></
nsPV:Command>
```

2. Write an XML Command to the CMD item.

This is how to execute commands for an item. Refer to the OPC command specification (www.opcfoundation.org).

4.2.3 Command examples

Scenario 1: Acknowledge a report

In the following scenario the sounder 2.1 of the panel 1 in panel group 1 (“Fire Panel 1-1.NAC.2.1") will receive an acknowledge command.

<nsPV:Command Name="ACK" Anzeigename="Acknowledge" Description="Acknowledge" OPCServerKlasse="BoschFPA5000OpcServer1" xmlns:nsPV="file:///S3K/Proxyverwalter" Sender="BIS" Adresse=" Fire Panel 1-2.NAC.2"/>

If you send this command the report created for that sounder will be acknowledged if it exists.

Scenario 2: Reset a report

<nsPV:Command Name="RESET" Anzeigename="Reset" Description="Reset" OPCServerKlasse="BoschFPA5000OpcServer1" xmlns:nsPV="file:///S3K/Proxyverwalter" Sender="BIS" Adresse="Fire Panel 1-2.Detector.1.2"/>

Scenario 3: Bypass a detector

In the following scenario the input 100.1 of the panel 11 in panel group 47 (Adresse="Fire Panel 47-11.Input.100.1"/>) will receive the command "Bypass on".

<nsPV:Command Name="Bypass on" Anzeigename="Bypass on" Description="Bypass a detector" OPCServerKlasse="MagicPanel OPC-Server" xmlns:nsPV=="file:///S3K/Proxyverwalter" Sender="BIS" Adresse="Fire Panel 47-11.Input.100.1"/>

If you send this command the input will change its state to “bypass”.

5 Step-by-Step Configuration

5.1 FSP-5000-RPS

1. Open the FSP-5000-RPS programming software.
2. In an existing configuration, click with the right mouse button on **Network line** in the tree view and choose **Create Server** > **Create OPC Server** in the context menu.
3. Configure the OPC server node.
   Enter the virtual PNA/RSN and logical node.
4. Choose **IP Settings...** to enter the IP settings dialog.
5. Edit the fields accordingly. **Line 2** and **Subnet Mask** are mandatory fields, Port Number is 25000 and **Gateway** is optional.

Notice!
The settings must match the network adapter/card settings of the computer the FSM-5000-OPC Server will be installed on!
The values of Net Group and Node Address, the PNA/RSN and the IP address are required to configure the OPC server.

6. Confirm your changes with **OK** and leave the dialog.
7. Click on the panel node that will be physically connected to the Ethernet.
   A dialog box for configuration opens.
8. Choose **IP Settings...** to enter the IP settings dialog.
9. Edit the fields accordingly. Panels not directly connected to the Ethernet have not assigned an IP address.
10. Confirm your changes with **OK** and leave the dialog.
11. Click on **Net interfaces** and on **Net interface** - **Ethernet** with the corresponding port that physically connects the Ethernet cable to the OPC server.
12. Select **Use Port** and click on **Apply**.

Notice!
Use ETH3 for connecting an OPC server. Connection via an external RSTP switch is allowed when not used for panel networking. If there is no Ethernet panel networking, then ETH1 and ETH 2 can be used for connecting an OPC server. If no connection to Remote Services is required, then ETH4 can be used for connecting an OPC server as well.

13. Choose the country and the language from the list

Notice!
Take care about the country and language settings. BIS 4.x will display commands and detector names in the selected language.

14. Confirm your settings with **OK** and leave the dialog.
15. Click on **Assigned servers**.
    A dialog box opens.
16. Assign the OPC server to the panel. Repeat this task for each node that shall transmit its states to the OPC server.

Notice!
It is mandatory that each panel node is assigned to the OPC server to be available in BIS. A premium license is required for each node to be assigned to an OPC server.

17. Confirm your changes with **OK** and leave the dialog.

5.2 Panel Controller

– AVENAR panel 8000 / 2000 with premium license: Connect the Cat.-5 cable with the Ethernet port 3 (ETH03).
– FPA-5000 (MPC-xxxxx-B or MPC-xxxx-C): Connect the Cat.-5 cable with the Ethernet port (RJ45).

5.3 PC/Server

1. Connect the Cat.-5 cable to the PC Ethernet port. Afterwards open the DOS command window and successfully “ping” the panel controller.
2. Right click on the OPC icon in the taskbar notification area and open the **Connection** dialog. A list with all identified panels and their respective connection status is displayed. If the configuration was successful, all panels which are assigned to the OPC server should have the status “connected”.
   You can also find these information in a log file, located on C:\Program Files (x86)\Bosch
3. \FPA5000 OPC-Server\Log (for Windows 10, might be slightly different for other operating systems).

6 Usage

This chapter presents a sample for a simple scenario. The intention is to give you a basic impression on how FPA5000-OPCServer is working. The scenario contains the following:

– A network configuration as described in the example in chapter Technical Interface Description.
– Additional to that we configured an LSN-Module with two rings: Ring 1 contains an automatic detector of type FAP-OTC420 (optical-thermal detector). Ring 2 contains a manual call point of type DM-210.

The item name of the automatic detector is 2.8.DETECTOR.1.1 and the name of the manual call point is 2.8.DETECTOR.2.1.
We will see how to receive item state information from the panel for both detectors and how to use commands in order to control the detectors. On OPC server side we are once more using the Softing Demo Client for demonstration. The scenario consists of two parts:
Part 1: Set the automatic detector into “Walktest” by sending an OPC command. Then switch off the Walktest on the panel and receive a “Normal” state for the Detector by OPC.
Part 2: Create a fire-alarm with the manual detector. Receive “Fire” by OPC. Send “Reset” via OPC to the panel and receive “Normal” when the detector changed back to its normal state.

6.1 Start situation

The panel has started, is in idle state without troubles or alarms and is connected to the OPC server.

1. Open the OPC client.
2. Select both detectors for watching the status and also the CMD item for sending commands.
3. Look up the state value in the table Appendix A.2 - State Table 2. Value 5 is assigned with Stand-by/Control off (LZ: GE) which is the normal state for all kinds of items without activation or trouble.

6.2 Set a detector into “Walktest” and switch-off the Walktest on the panel

Send the following command line to the panel:

```
<nsPV:Command Name="WALKTEST_ON" Anzeigename="Walktest on"
Description="Walktest on" OPCServerKlasse="BoschFPA5000OpcServer1"
xmlns:nsPV="file:///S3K/Proxyverwalter" Sender="BIS" Adresse="Fire Panel
2-8.Detector.1.1"/>
```

(See *Execution of commands, page 16* Step 2: Execution of commands for more information about that).
The panel will set the detector into the administrative state “Walktest” (Compound state set to Walktest/Normal). You will not see a status report for this on the main dialog, but you can see it by entering the status menu.
After sending the command and receiving the new item state, the Softing demo client shows: According to the state table value “37” stands for Maintenance - Stand-by/Control Off.

6.3 Create a fire alarm and reset it with OPC

Now press the button on the manual call-point. The panel controller displays a fire alarm on 2.8.DETECTOR.2.1. On the OPC client:
The value 16 stands for Ext-Fire (LZ: F1) -compare with Appendix A.2 - State Table 2
After unlocking the latch on the manual call point, send the following OPC command to the panel:

```
<nsPV:Command Name="RESET" Anzeigename="Reset" Description="Reset"
OPCServerKlasse="BoschFPA5000OpcServer1" xmlns:nsPV="file:///S3K/
Proxyverwalter" Sender="BIS" Adresse="Fire Panel 2-8.Detector.2.1"/>
```

The detector returns to normal state and the fire alarm disappears from the panel display.

7 Troubleshooting

If the configuration of the FSM-5000-OPC server doesn't work in the panel network try the following:

- Confirm on the panel controller that the IP address is assigned and "ping" the OPC server.
- If the Ping request is answered but the configuration still doesn't work please check
  - all settings on the panel,
  - all settings in the FSM-5000-OPC Configuration Editor,
  - the Ethernet adapter settings in the Window's System Configuration.
- De-activate firewall
- Follow these steps:
  - Stop OPC (see "Service" tab in Configuration Editor)
  - Delete bin file(s) under C:\MPOPCServer\Repository
  - Start OPC → A new file per node will be created.
- If no elements are shown, check whether the Repository folder exists and whether it contains a bin file for each node. The files are located under C:\MPOPCServer \Repository.
- On the MPC panel controller go to **Diagnostics** - **Network** - **Routing table.**
  A table with routing information is displayed. All networked nodes that can be reached via the panel and that are recognized within the system network are displayed under Node. Aside the respective interfaces via which the connected network nodes are connected to the panel are displayed. If the OPC server configuration is correct there must be an entry under **Node** with the RSN of the OPC server node and the interface "UDP tunnel".
- Make sure that the panel controller does not show any troubles which could concern the OPC server node or the network communication in general.
- Verify that you have a panel controller with OPC license.

7.1 Update of Configuration Cache in OPC Server

1. Determine the directory with the cache files in the configuration directory.
2. Delete the cache files for the panel(s) in the determined directory. The cache file name corresponds to the panel group and node number. The schema is MP<group>_<node>.bin, e.g. panel 1.1 has the cache file MP1_1.bin.
3. Disconnect the connection between OPC server and panel. A connection error is shown on the panel.
4. Reconnect OPC server and panel. Reset the trouble messages on the panel.
5. After some time the cache files are recreated for the reconnected panels in the determined directory. After creation of the cache files, the panel items are published via OPC.

Start browsing the OPC server to see the new configuration.

7.2 FSM-5000-OPC Server Tracing

The tracing of the OPC Server is possible on two levels. The first level is the application, the second is the FPA-5000 network.

7.2.1 Application Tracing

Change the trace level of FSM-5000-OPC server.

1. Start Windows Registry Editor with „regedit.exe" at command line.
2. Navigate in the registry editor to the key:
   HKEY_LOCAL_MACHINE\Software\Bosch\FPA_5000_OPC\Global

3. Here you find a value with the name „TraceLevel“. The data value of this entry can have two valid entries as described below. You can change the value by double click.

TraceLevel value	Description
Info	Default setting, strongly recommended in normal operation mode
Verbose	Used to get traces for support cases, must not be used in normal operation mode

- Restart the OPC Server to apply the change of TraceLevel.

7.2.2 Network Tracing

Follow the instructions of section Application Tracing but set the value for the key “TraceLevelNetStack” to “Verbose”.
Restart the OPC Server to apply the change.

7.3 Workaround if FSM-5000-OPC Server Installation of OPCEnum didn’t work

If the FSM-5000-OPC server setup does not properly install the OPCEnum service which is used by OPC clients to enumerate available OPC servers use the following workaround to fix this.
Precondition: The required files have been copied to your system by the MSI installer during FSM-5000-OPC server setup:

- Uninstall OPC server with the following script:

```
@echo off
regsvr32 /u /s "%CommonProgramFiles%\OPC Foundation\Bin\OpcDxPs.dll"
regsvr32 /u /s %WINDIR%\system32\opcbc_ps.dll
regsvr32 /u /s %WINDIR%\system32\opccomn_ps.dll
regsvr32 /u /s %WINDIR%\system32\opchda_ps.dll
regsvr32 /u /s %WINDIR%\system32\opcproxy.dll
regsvr32 /u /s %WINDIR%\system32\opcSec_PS.dll
regsvr32 /u /s %WINDIR%\system32\opc_aeps.dll
"%CommonProgramFiles%\OPC Foundation\Install\OpcCustomInstaller" /Uninstall
```

- Now re-install the server with the following script:

```
@echo off
regsvr32 /s "%CommonProgramFiles%\OPC Foundation\Bin\OpcDxPs.dll"
regsvr32 /s %WINDIR%\system32\opcbc_ps.dll
regsvr32 /s %WINDIR%\system32\opccomn_ps.dll
regsvr32 /s %WINDIR%\system32\opchda_ps.dll
regsvr32 /s %WINDIR%\system32\opcproxy.dll
regsvr32 /s %WINDIR%\system32\opcSec_PS.dll
regsvr32 /s %WINDIR%\system32\opc_aeps.dll
"%CommonProgramFiles%\OPC Foundation\Install\OpcCustomInstaller" /Install
```

7.4 No state changes are transmitted for the panel network

1. Check the IP connection to the panel network e.g. ping the panel IP address.

2. Check your settings in ConfigEditor, particulary the PNA/RSN configured for the OPC Server. If the PNA/RSN configured on the server (ConfigEditor) does not match the PNA/RSN configured for the OPC server in the programming software FSP-5000-RPS the panel will not attach to the OPC server.
3. Ensure that you have an OPC license. If your system runs out of the license free time (48 hours) the license item will change its status to “tamper” and the panel network quits sending the status.
4. Check that the Firewall is turned off or required ports are unblocked.

7.4.1 Remote Access does not work

1. Take care that the Windows Firewall on the system that runs the OPC Server is deactivated. Also check that the server systems firewall does not block the remote connection.
2. Check that the client can find the server computer in your network (IP settings, DNS, Workgroup settings). In order to check this you may temporarily configure a public folder share at the server system (See Windows Help on this topic. Open the Windows Explorer on the client. Click on Network > Workgroup - the server has to be visible there. Note: You don’t need file sharing for OPC at all. This is only a test whether the server is visible.) or you may enter ping <name_of_server_computer>at the command line of the client.
3. Proof consideration of configuration steps described in chapter Remote Access to the FSM-5000-OPC Server from the Building Integration System (BIS).
4. Use the Softing Demo client (“Run as a different user” with the correct account) and check whether you get access to the OPC Server. DA V2 shall show FPA5000OPC. Select it and select group. After that you should be able to browse with “DA items”.
5. If it is not working at all, check that you got a TCP/IP connection to the remote system (e.g. with “ping”).
6. Check that the client can connect with FPA5000OPCServer when it runs local on the remote system (e.g. use the Softing Demo Client for proofing it). If this doesn’t work, fix this problem first (see also chapter Workarounds for known Problems).

7.4.2 No state changes are transmitted for the panel network

1. Check the IP connection to the panel network e.g. ping the panel IP address.
2. Check your settings in ConfigEditor, particulary the PNA/RNS configured for the OPC Server. If the PNA/RSN configured on the server (ConfigEditor) does not match the PNA/RSN configured for the OPC server in the programming software FSP-5000-RPS the panel will not attach to the OPC server.
3. Ensure that you have a panel controller with OPC license. If your system runs out of the license free time (48 hours) the license item will change its status to “tamper” and the panel network quits sending the status.
4. Check that the Firewall is turned off or required port (Port Number 25000) is unblocked.
5. Verify in the FSP-5000-RPS that the OPC-Server is assigned to the desired panel. This means the OPC-Server is part of the list of "Assigned servers" of the panel.

8 Technical data

Supported OPC standards:

– DA 2.0
– AE 1.01

Other Standards

– “BIS Common Requirements” (Bosch standard).

Supported operating systems:

– Windows 10 (64 bit)
– Windows 2012 Server
– Windows 2016 Server

Limits

For each panel approximately 2000 OPC items can be created in maximum configuration.

Memory

For configuration data caching a file with approximately 200kb is stored for each panel in the repository folder.

Licensing

Each panel requires a Premium license to be assigned to an OPC server.

Additional Information

LAN Technology Specifications:

Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	8ß2.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/ EW	300 meters 300m MMF/ 10km SMF 10km/40km 300m/10km/40km

Guide to Ethernet Coding

10	at the beginning means the network operates at 10Mbps.
BASE	means the type of signaling used is baseband.
2 or 5	at the end indicates the maximum cable length in meters.
T	at the end stands for twisted-pair cable.
X	at the end stands for full duplex-capable cable.
FL	at the end stands for fiber optic cable.

For example: 100BASE-TX indicates a Fast Ethernet connection (100 Mbps) that uses a twisted pair cable capable of full-duplex transmissions.

Cable Grade Capabilities

Cable Name	**Makeup**	**Frequency Support**	**Data Rate**	**Network Compatibility**
Cat-5	4 twisted pairs of copper wire -- terminated by RJ45 connectors	100 MHz	Up to 1000Mbps	ATM, Token Ring,1000Base-T, 100Base-TX, 10Base-T
Cat-5e	4 twisted pairs of copper wire -- terminated by RJ45 connectors	100 MHz	Up to 1000Mbps	10Base-T, 100Base-TX, 1000Base-T
Cat-6	4 twisted pairs of copper wire -- terminated by RJ45 connectors	250 MHz	1000Mbps	10Base-T, 100Base-TX, 1000Base-T

9 Appendices

9.1 Appendix A.1 - State Table 1

OPC Item Value	Internal Panel Compound State	Description
600	Invalid	
601	Normal	
602	Fault	
603	Fire	
604	Fire Pre	1st state AND / Cross zoning
605	Fire verify	Alarm Verification
606	Heat	
607	Supervisory	Supervisory Error
608	Smoke	
609	Activate	
610	Activation failed	
611	Tamper	
612	Cover open	Cover is open
613	Paper out	Paper is out
614	Threshhold Alarm	1st stage fire, threshold
615	Trouble light	Light trouble, e.g. C-Sensor of a combined detector not working
616	Panel Restart by Watchdog	Panel restarted by watchdog
617	On	
618	Off	
619	Pollution	
620	Pollution light	
621	Monitor	
622	Water	
623	Power Fail	
624	Manual Alarm	
625	Fire PAS	PAS (Wait for acknowledge)
626	Fire PAS	PAS (Investigate)
627	Address card change	Address card changed

628	Not enough address space	Address card changed and now there are less addresses licensed than points configured
629	Address card tamper	The countdown after address card removal is finished, addresses are to be switched off
630	Fire internal	Internal fire, results from a usage type “FIRE_INT”
631	Error	Indicates an invalid value for a logical state since INVALID is used elsewhere in the system
632	Unknown	For state stor use only
633	internal use	Wild card
634	Configuration mismatch	Mismatch of network configuration (topology information)
635	Unknown item	Unconfigured item i.e. network node detected
636	Missing	Configured item i.e. network node NOT detected, for internal items currently trouble used
637	Incompatible software	Incompatible software detected for nodes in network
638	Incompatible network protocol	Incompatible network protocol version detected for nodes in network
639	internal use	
640	internal use	
641	Walktest Normal	
642	Walktest Fault	
643	Walktest Activate	
644	Walktest Activation failed	
645	Walktest On	
646	Walktest Off	
647	Walktest Alarm	
648	Bypass Normal	
649	Bypass Fault	
650	Bypass Activate	
651	Bypass Isolated Activation failed	
652	Bypass Alarm	
653	Isolate Normal	
654	Isolate Fault	
655	Isolate Activate	

656	Isolate Activation failed	
657	Isolate Alarm	
658	Normal Day Mode	
659	Fault Day Mode	
660	Alarm Day Mode	

Tab. 9.1: Appendix A.1 - State Table 1

9.2 Appendix A.2 - State Table 2

OPC Item Value	Description	LZ Name
0	Missing Zone	FG
1	Detector masking	MAD
2	Fade-out/Skip	ABL
3	Zone switch off	ABS
4	Detector test	TST
5	Stand-by/Control off	GE
6	Breakdonw centr. part	G8
7	Control On	STE
8	Malfunction ground	ES
9	Criterion -4	K4
10	Criterion -3	K3
11	Criterion -2	K2
12	Malfunction generic	G0
13	Emergency alarm	H1
14	Int-Fire	F3
15	Pre-Fire	F2
16	Ext-Fire (TU)	F1
17	Trigger disarmed	A6
18	Intern-Alarm	A5
19	Int-Sabotage	A4
20	Ext-Sabotage (TU)	A3
21	Ext-Intrusion (TU)	A2
22	Hold-up Alarm (TU)	A1

23	Ext-Malfunction.(TU)/Ext-Fire. (TU)	A0
24	Stand-by/Off	PE
25	On	P2
26	Acknowledgement	P3
27	Malfunction	P4
28	Malfunction power supply	P5
29	Switch Off	P6
30	Alarm verification	TEL
31	Address Blocking	ASP
32	Triggering generic	R-FG
33	Maint.-Stand-by OMM	R-GE
34	Maint.-Light Pollution	R-G0
35	Maint.-Heavy Pollution	R-G2
36	Maint.-Alarm OMM	R-AL
37	Maint.-Stand-by/Control Off	R-GE
38	Maint.-Breakdown Centr. Part	R-G8
39	Maint.-Control On	R-STE
40	Maint.-Malfunction Ground	R-ES
41	Maint.-Criterion-4	R-K4
42	Maint.-Criterion -3	R-K3
43	Maint.-Criterion -2	R-K2
44	Maint.-Malfunction	R-G0
45	Maint.-Emergency Alarm	R-H1
46	Maint.-Int-Fire	R-F3
47	Maint.-Pre-Fire	R-F2
48	Maint.-Ext-Fire	R-F1
49	Maint.-Triggering	R-A6
50	Maint.-Intern Alarm	R-A5
51	Maint.-Alarm Thermo (UGM)	R-A4
52	Maint.-Alarm Optics (UGM)	R-A3
53	Maint.-Ext-Intrusion (UGM)	R-A2
54	Pollution (UGM)	R-A1
55	Maint.-Malfunction-Ext	R-A0
56	Stand-by R-R/Max (UGM)	R-PE

57	Stand-by ThermoMax (UGM)	R-P2
58	Stand-by Optics (UGM)	R-P3
59	Alarm Pre-Level (UGM)	R-P4
60	Fire-Int Thermo (UGM)	R-P5
61	Fire-Int Optics (UGM)	R-P6
62	Fire-Ext Thermo (UGM)	R-TEL
63	Fire-Ext Optics (UGM)	R-ASP
64	Stand-by R-R/Max	GE-TD
65	Stand-by TMax	GE-TM
66	Stand-by Optics	GE-O
67	Stand-by Combi	GE-K
68	Light Pollution	V2
69	Heavy Pollution	V1
70	Heavy Pollution (Qty.)	V0
71	Alarm Pre-Level Ion	AV-I
72	Alarm Pre-Level Optics	AV-O
73	Alarm Pre-Level Thermo	AV-T
74	Alarm Pre-Level Combi	AV-K
75	Maint.-Alarm Optics	R-F1-O
76	Maint.-Alarm Thermo	R-F1-T
77	Maint.-Alarm Combi	R-F1-K
78	Fire-Ext Opt	F1-O
79	Fire-Ext Thermo	F1-T
80	Fire-Ext Combi	F1-K
81	Call Fire Brigade	FWR
82	Fire-Pre (TU)	F2-E
83	Fire-Int Opt	F3-O
84	Fire-Int Therm	F3-T
85	Fire-Int Combi	F3-K
86	Hold-up alarm with menace (TU)	A1-B
87		
88	Stand-by Day/Internal	T-GE
89	Periph. Control On	P8
90	Light Malfunction	G1

91	Line Malfunction	G2
92	End of Paper	PA
93	Triggering Disarmed	A7
94	Mains	Fault
95	Battery	Fault

Tab. 9.2: Appendix A.2 - State Table 2

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

202010071035