

BIS Automation Engine (AUE)



BOSCH

en Installation and Configuration

Table of contents

1	Short information	4
2	System overview	5
3	Hardware installation	6
3.1	Connection using an OVS interface converter	6
3.2	Fiber-Optic connections	12
3.3	Connecting a bus coupler	13
3.4	Connecting a video matrix	16
4	Configuring OPC-specific data for LSN systems	19
4.1	Reading LSN detector address lists	22
4.2	Automatically deleting unaccepted messages	23
5	Configuring OPC-Specific Data for FPA5000	25
5.1	FPA connection	25
5.2	Calling the OPC configuration editor	25
5.3	Required settings in the OPC configuration editor	26
5.4	Browsing FPA detectors	27
5.5	Configuring events and controls	27
6	OPC: BIS-BVIP	29
7	OPC: FPA 5000	34
7.1	Step-by-Step Configuration	34
7.1.1	FSP-5000-RPS	34
7.1.2	Panel Controller MPC-xxxx-B or MPC-xxxx-C	35
7.1.3	PC/Server	35
7.2	Usage	35
7.2.1	Start situation	36
7.2.2	Set a detector into "Walktest" and switch-off the Walktest on the panel	36
7.2.3	Create a fire alarm and reset it with OPC	36
7.3	General troubleshooting	36
8	OPC: MAP 5000	38
9	OPC: Praesideo PA system	42
9.1	Overview	42
9.2	Prerequisites	42
9.3	Data point type Call: Commands and events	44
9.4	Data point type Unit:	47
9.5	Data point type BGM channel (background music)	48
9.6	Data point type Alarm	50
9.7	Configuring the OPC server	51
10	Legacy OPC servers	52
10.1	Configuring OPC-specific data for Beckhoff servers	52
10.1.1	Detector types for Beckhoff connections	54
10.1.2	Notes on data transmission:	55
10.2	Example: Browsing an Allegiant matrix connection	55
10.3	BRS Software setup and configuration	58

1

Short information

The Automation Engine (AUE) is one of the main modules in the BIS family. It runs either as the only engine or in combination with the other engines.

Its main function is to connect, monitor and control security and safety systems, usually fire and intrusion panels. However, it is also possible to display live images in action plans or miscellaneous documents. For more complex video applications, we advise the use of the Video Engine or Bosch VMS.

2 System overview

BIS Automation Engine (AUE) provides the following functionality within BIS

- Highly sophisticated alarm and security management system for fire and intrusion panels
- Integration of public address and voice alarm systems for efficient evacuation of buildings
- Detailed monitoring of other vital systems, such as HVAC, building automation or energy management throughout a site
- Easy integration and configuration of subsystems through consistent use of world-wide OPC standards
- Automation of emergency responses to subsystem alarms through user-definable rules
- Management of operator rights to restrict visibility and control to specially authorized groups

3 Hardware installation

Several options exist for connecting system hardware to BIS:

- OVS interface converter (opto-coupler V.24 interface)
- Fiber-optic cable
- Local area network (LAN)

3.1 Connection using an OVS interface converter

OVS interface converters are the most commonly used connection when the distance between the BIS computer and the alarm system control panel is between 2m and 1000 m. The OVS converts the BIS V.24 interface signals into a 20 mA current loop.

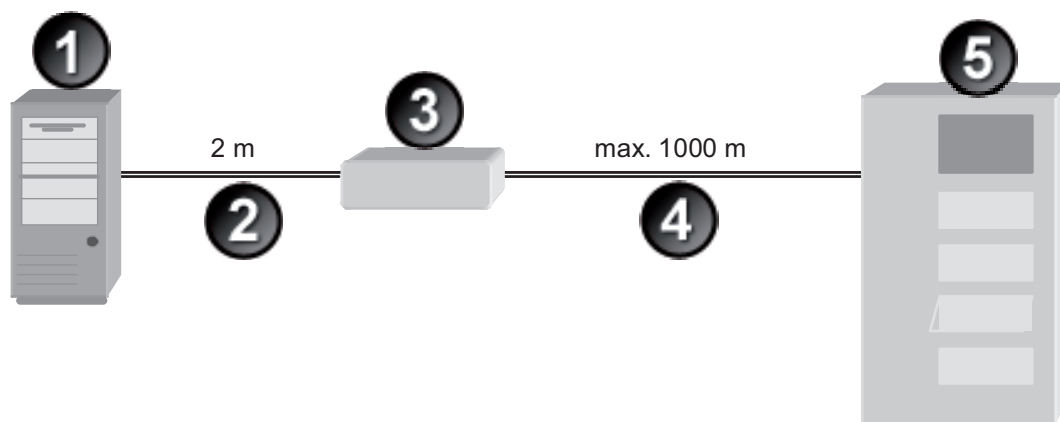


Figure 3.1: OVS Connection Diagram

#	Description
1	BIS
2	V.24 cable (2.799.382.430)
3	OVS (30.0210.8620)
4	20 mA 4-wire cable (2.798.020.102)
5	Panel

No BIS-specific modifications are necessary at the control panel alarm system, except for allowing data transmissions. All required settings are entered in the BIS user interface.

Connecting the BIS PC to the OVS

The connection between the BIS computer and the OVS is between one of the COM ports on the BIS server and the OVS V.24 port.

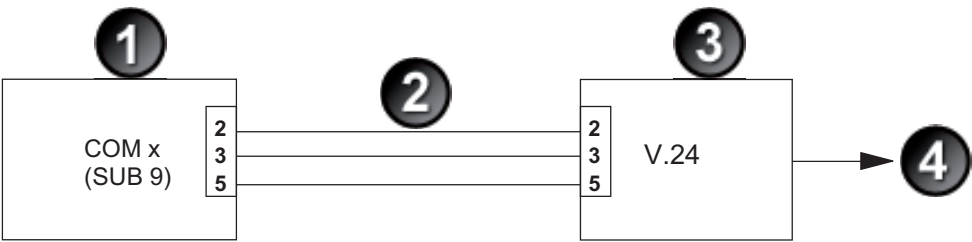


Figure 3.2: OVS to BIS PC Connection Diagram

#	Description
1	BIS
2	Standard V.24 cable
3	OVS
4	To the panel

OVS Jumper Assignments

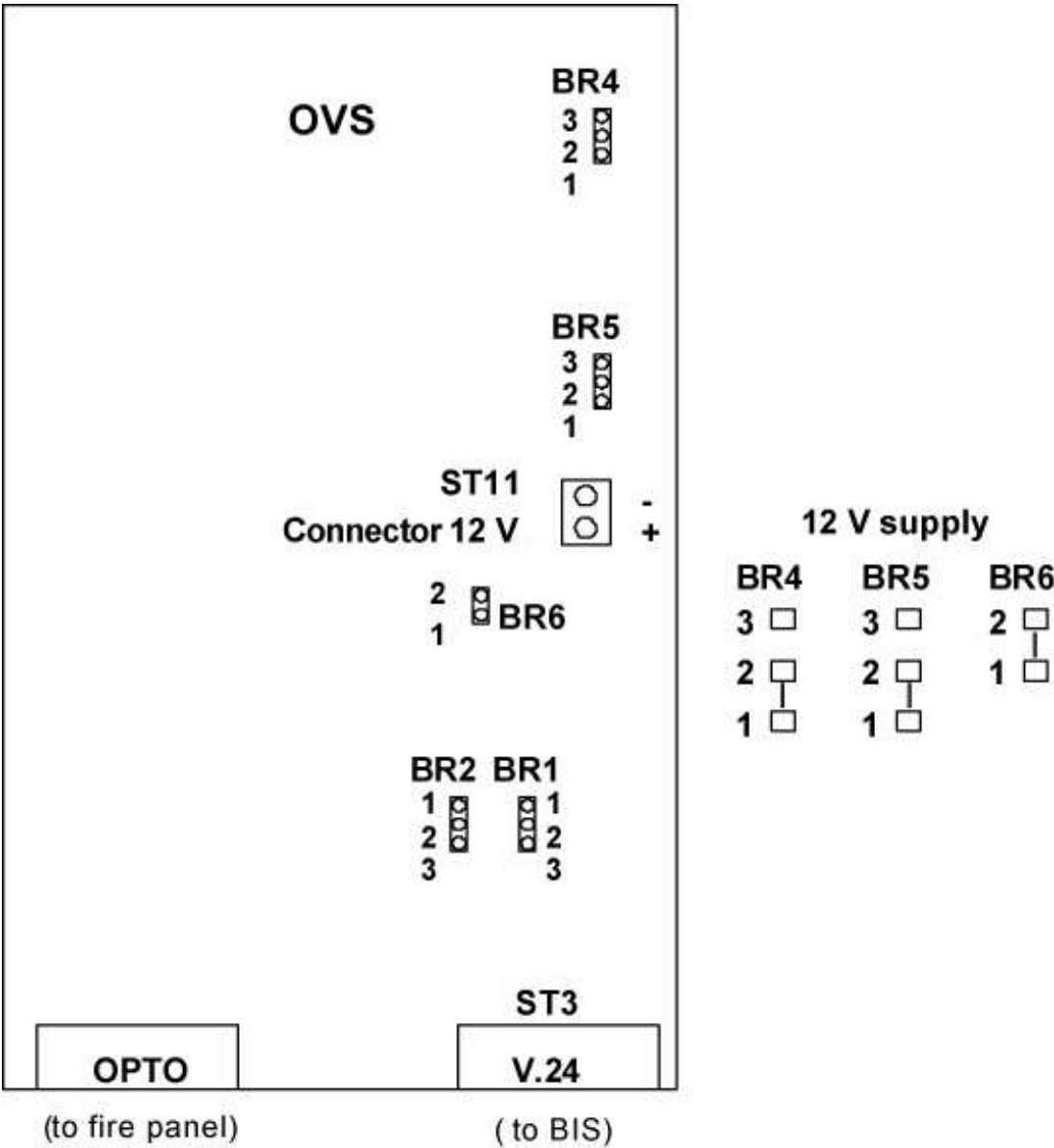


Figure 3.3: OVS Jumper Assignments

Jumpers BR1 and BR2

In order to correct any wiring errors when creating the V.24 transmitter and receiver lines, you can exchange the jumper positions of BR1 and BR2.



Figure 3.4:

#	Description
1	Transmission line

#	Description
2	Reception line

OPTO (9-pin)		V.24 (9-pin)	
Direction	Terminal	Direction	Terminal
Input +	1	Transmitter/Receiver	2
Input -	6	Receiver/Transmitter	3
Output +	5	0 V	5
Output -	9		

UGM 2020 using UESS Connection

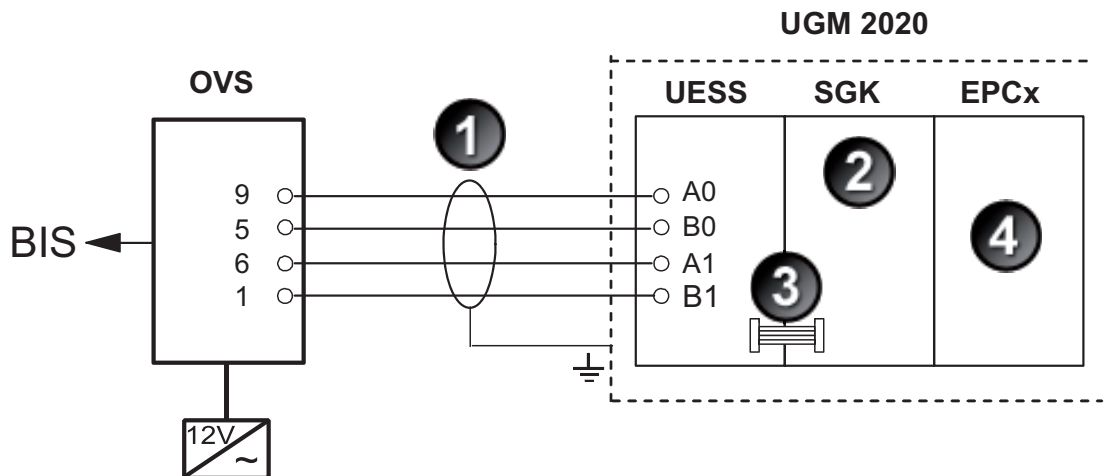


Figure 3.5: UGM 2020 Using UESS Connection Diagram

#	Description
1	20 mA interface IMPORTANT: Ground the shield only at the UGM side. Installation cable J-Y (St) Y 4x0.6mm (27.9802.0102)
2	Requires software version SKGUGM A.5 or higher
3	Ribbon cable
4	EAPS 4 or higher

Notice!

SGK Software

The standard SGK software can be used for the connection shown above. For this purpose, the definition jumpers for station A and the definition jumpers B4, B5 and B10 (= new data model/new 4a protocol) need to be set. Refer to the UGM installation manuals for more information.



UGM 2020 using UESS failsafe connection

To ensure a continued connection in the event of failure of the interface to the UGM, install a redundant connecting line between the BIS and the UGM.

Install an additional OVS line to the UGM by using an additional COM interface on the BIS computer. (Assign the second interface to the corresponding LSN-OPC servers in the configuration of BIS as well.)

The redundancy relates only to the connecting line and the processing in the UGM, but not the processing in BIS. As in the BIS system, both interfaces are handled by one process. The connection to the UGM is interrupted if this process fails.

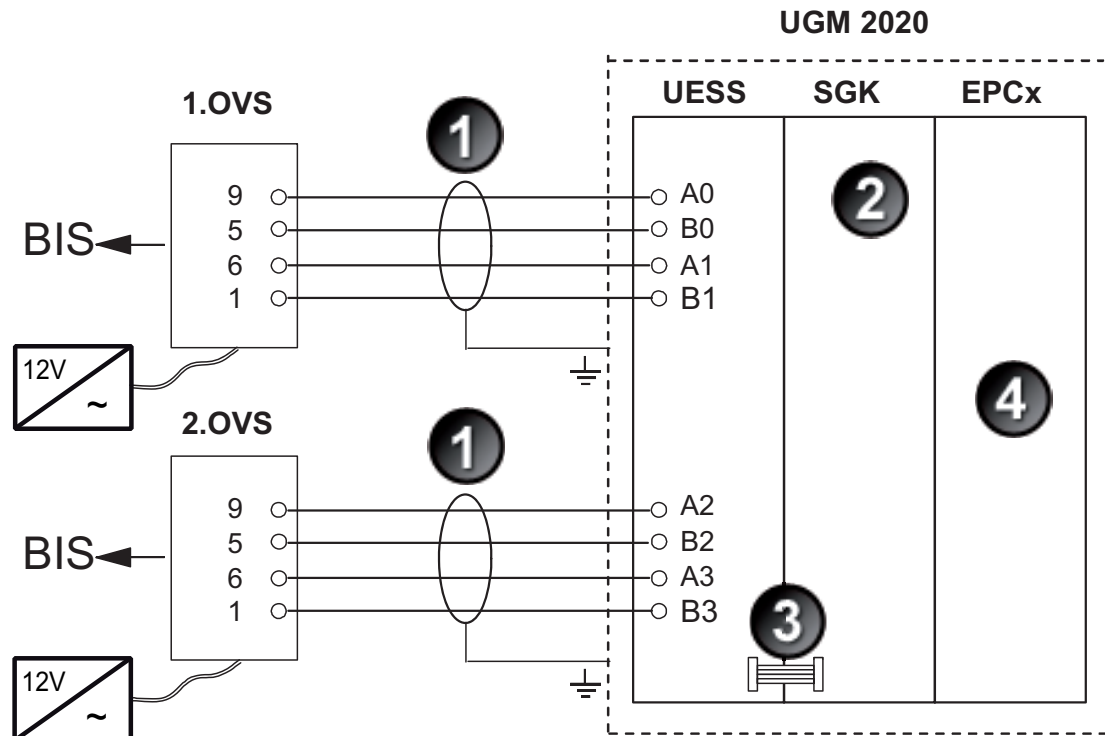



Figure 3.6: UGM 2020 Using UESS (With Redundancy) Connection Diagram

#	Description
1	20 mA interface IMPORTANT: Ground the shield only at the UGM side. Installation cable J-Y (St) Y 4x0.6mm (27.9802.0102)
2	Requires software version SKGUGM A.5 or higher
3	Ribbon cable
4	EAPS 6 or higher



Notice!

Note on second OVS

Depending on the local conditions of the UGM, the second OVS can also be connected to its own UESS. In this case, the selection of the connection points on the second UESS is the same as for the first OVS.

UGM 2005/2020 Using UESL Connection

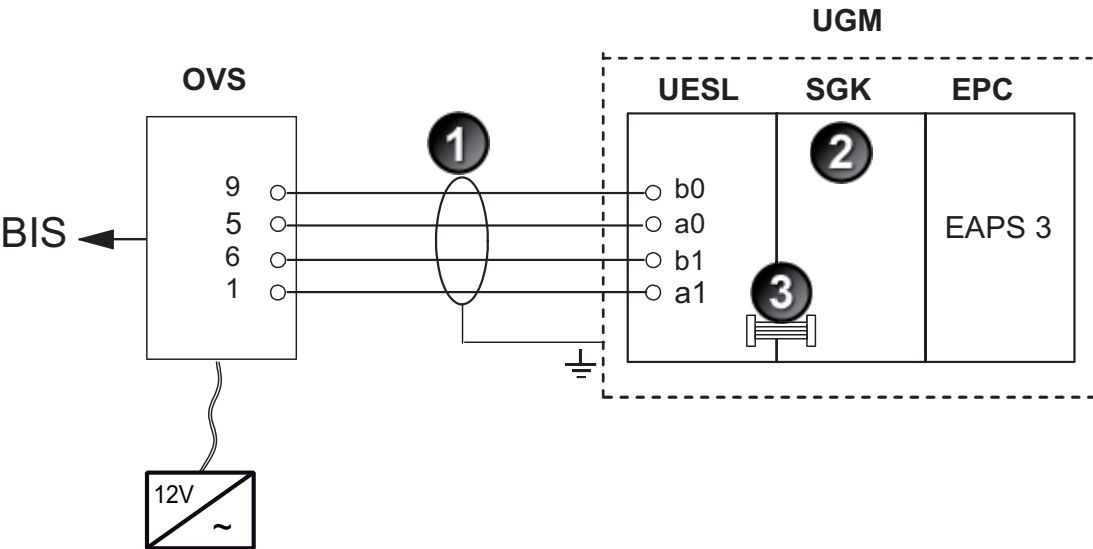


Figure 3.7: UGM 2005/2020 Using UESL Connection Diagram

#	Description
1	20 mA interface IMPORTANT: Ground the shield only at the UGM side. Installation cable J-Y (St) Y 4x0.6mm (27.9802.0102)
2	Requires software version SKGUGM A.5 or higher
3	Ribbon cable

Use the following jumpers when connecting the UGM using UESL.

EAPS Version	Jumper Settings
EPC with EAPS 5 or later	B1, B93B, B4, B5, B10
EPC with EAPS < 5	B2, B93A, B4, B5, B10
UESL Jumper Settings	

See also

- Connection using an OVS interface converter, page 6

3.2 Fiber-Optic connections

The connection of hardware systems to BIS using fiber-optic lines is recommended in all cases where high transfer rates and highest levels of immunity to faults are required over long distances.

Depending on the local conditions, with or without a main cable, one converter is required for each interface.

Notice!

Precautions for fiber-optic lines

- All voltage supplies must be switched off while installation work is performed.
- The fiber optics must be routed in a way that prevents chafing on sharp edges.
- Allow a bending radius of at least 4 cm (1.5 in.).
- When cutting fiber-optic lines, ensure that the resulting cut surfaces are smooth.
- Do not use connectors for fiber optics. Instead, connect the fiber-optic cable directly into the converter

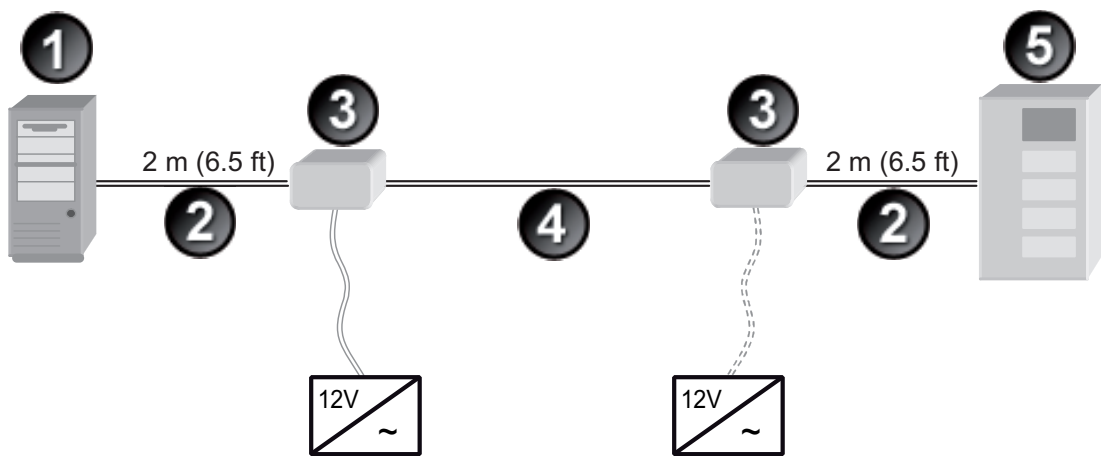


Figure 3.8: Fiber-Optic Connection Diagram

#	Description
1	BIS
2	V.24 Cable
3	Converter
4	Fiber-optic cable 27.9933.0134
5	Panel



Notice!

Connection notes
To prevent radio interference, the connecting line between the BIS PC and the converter or between the security system and the converter should be as short as possible.
On the security system side, the control center can provide the power to the fiber-optic converter.

Connection of BIS to the GO 232 Fiber-Optic Converter



Warning!

Danger of electrocution
Always disconnect the power supply before making wiring changes.

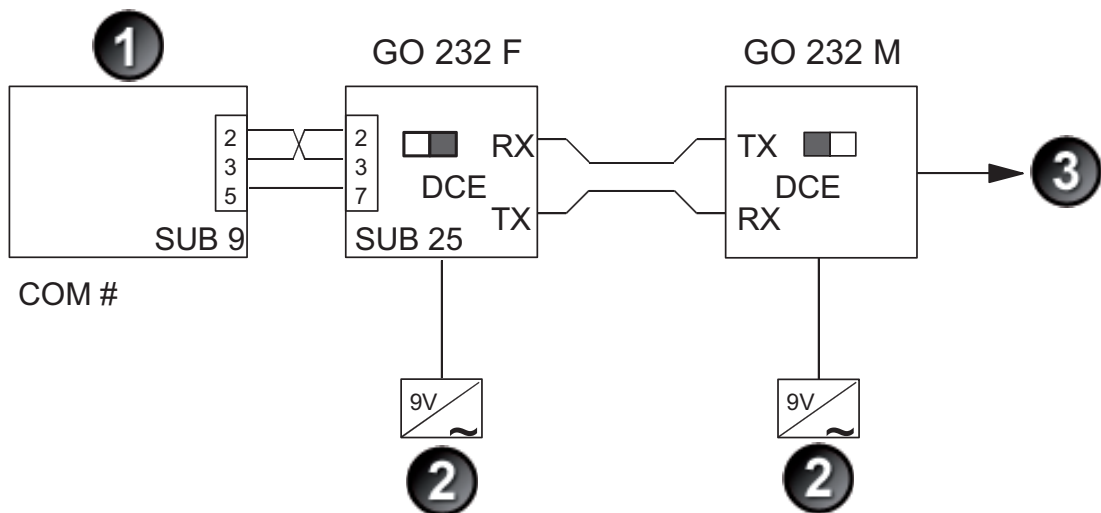


Figure 3.9: BIS to GO 232 Converter Connection Diagram

#	Description
1	System
2	Power supply
3	Panel

3.3 Connecting a bus coupler

Use a bus terminal system to connect external systems (for example, building systems, measuring systems, environmental technology, industrial installations) to BIS.
Make the connection using the relevant COM interface at the BIS computer and at the coupler element of the bus terminal system (with standard V.24 cables and, if necessary, a suitable transmission system).
The details on the following pages relate to the Beckhoff BK 8100 bus coupler with an RS-232C (V.24) interface. Use the following terminal types with the OPC server installed in the BIS server:

Terminal Type	Description
Terminal 1104	Digital input terminal with 4 inputs, 24 VDC, 3.0 ms filter.
Terminal 3202	Analog input terminal with 2 inputs.
Terminal 2134	Digital output terminal with 4 outputs, 24VDC.
Terminal 2612	Digital output terminal with 2 relay outputs, 125 VAC, 0.5 A, potential-free change-over.
Terminal 9010	Bus end terminal.
OPC Server Terminal Types	

You can use other types of couplers and terminals. In these cases, however, you must load the corresponding OPC server of the bus terminal manufacturer. For more information, refer to <http://www.beckhoff.com>.

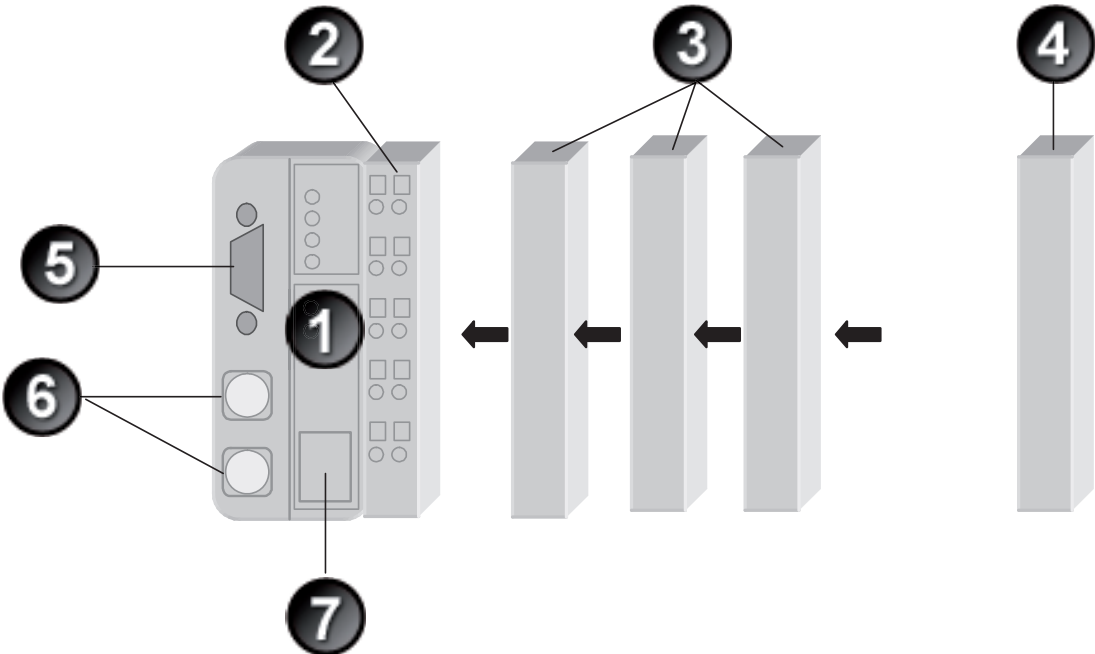


Figure 3.10: Bus Terminal System Diagram

#	Description
1	Bus coupler
2	Power supply
3	Additional terminals
4	End terminal (KL9010)

#	Description
5	Field bus connector
6	Bus address selector
7	DO NOT OPEN THIS DOOR. Opening this door voids the warranty.

Select any sequence of bus terminals at the bus coupler. You should, however, position potential-free output terminals at the end of the row. If they are not positioned at the end of the row, use a jumper connector if subsequent terminals require a voltage supply.

Every bus terminal system must have an end terminal (bus end terminal) at the end of the terminal rows.

Using the selector switch, select the station address on the bus coupler according to the configuration.



Notice!

Notice

You must configure the bus terminal system after connection. Refer to its product documentation for more information.

Several options exist for connecting the bus coupler/bus terminal system to the BIS computer:

1. OVS interface converter (opto-coupler V.24 interface)
2. Fiber-optic cable
3. Local area network (LAN) (depends on the type of bus coupler)

Connection Using OVS Interface Converter

You can use an OVS interface converter with distances of up to 1000 m (3280 ft) between the BIS computer and the bus coupler. The OVS converter converts the BIS V.24 interface signals into a 20 mA current loop.

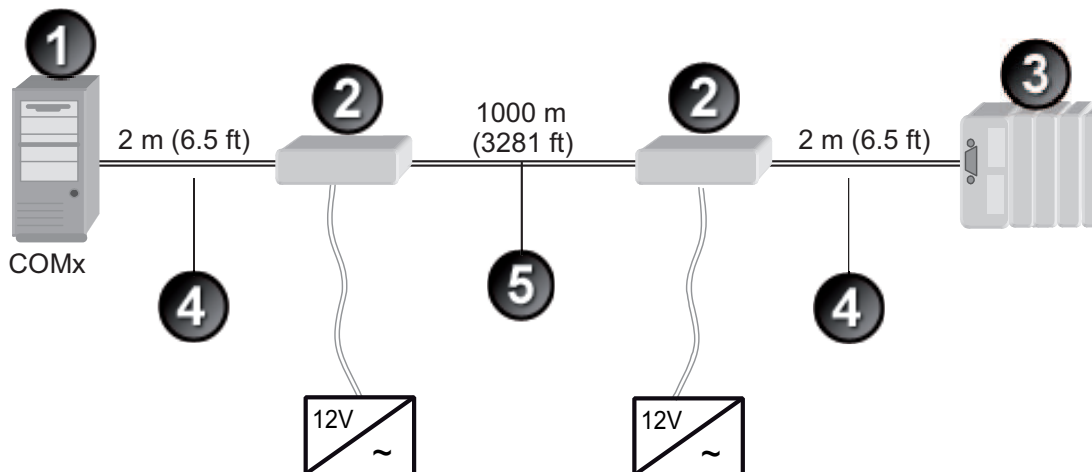


Figure 3.11: OVS Interface Converter Diagram

#	Description
1	BIS

#	Description
2	OVS (30.0210.8620)
3	Bus coupler
4	V.24 cable
5	20 mA 4-wire cable (2.798.020.102)

Refer to the manufacturer's documentation for the Beckhoff bus coupler connection settings.

In order to correct any wiring errors when creating the V.24 transmitter and receiver lines, you can exchange the jumper positions of BR1 and BR2.



Figure 3.12:

#	Description
1	Transmission line
2	Reception line

OPTO (9.pin)		V.24 (9-pin)	
Direction	Terminal	Direction	Terminal
Input +	1	Transmitter/Receiver	2
Input -	6	Receiver/Transmitter	3
Output +	5	0 V	5
Output -	9		

3.4 Connecting a video matrix

You can start control processes on the video matrix (and the cameras connected to it) by connecting a video matrix to BIS. Connect V.24 cables to a COM interface on the BIS server (using a suitable transmission system, if necessary).

All OPC servers required for LTC 8x00 video matrices are already installed in the BIS.

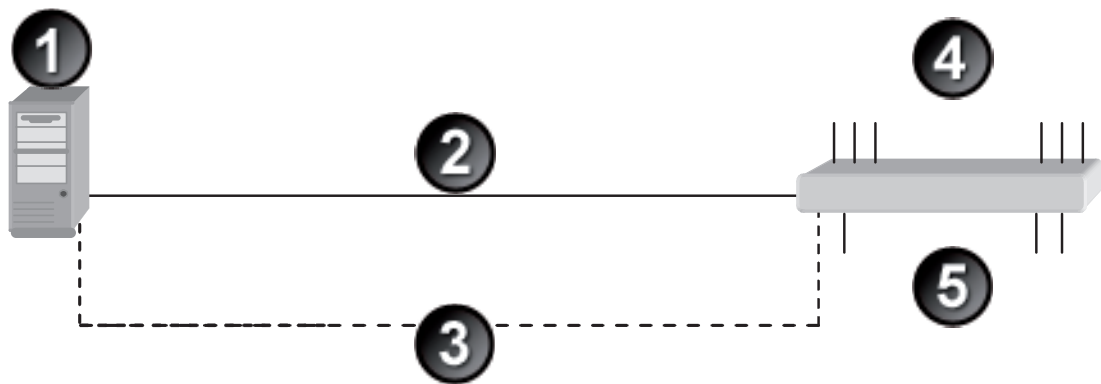


Figure 3.13: Video Matrix Connection

#	Description
1	BIS server PC
2	Serial cable
3	Optional video to IP converter (e.g. VideoJet)
4	Cameras
5	Video outputs

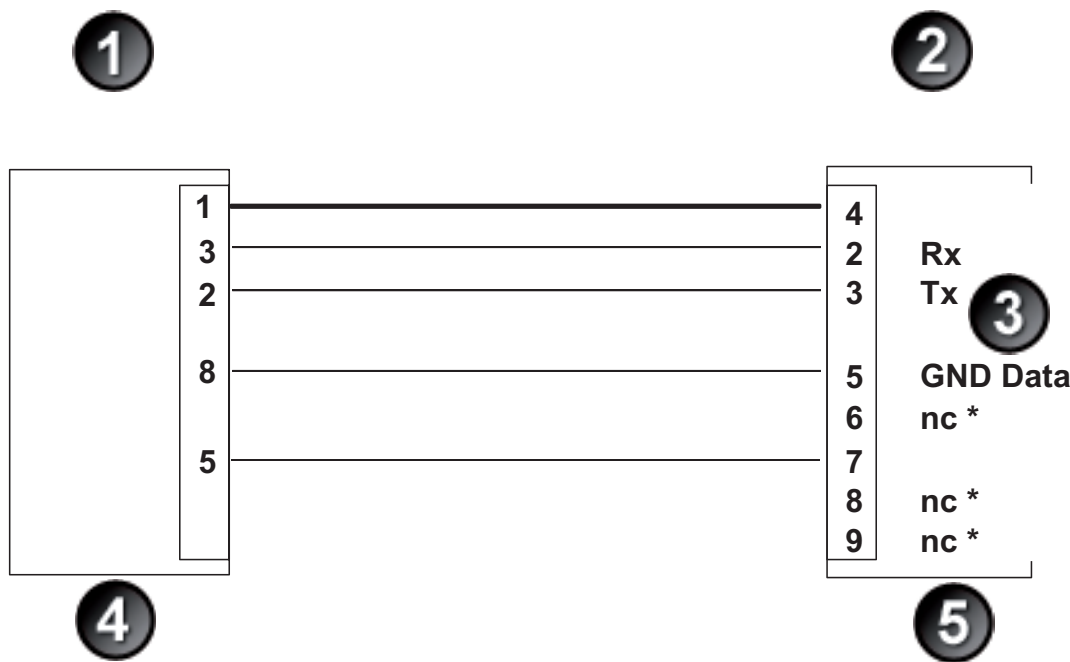







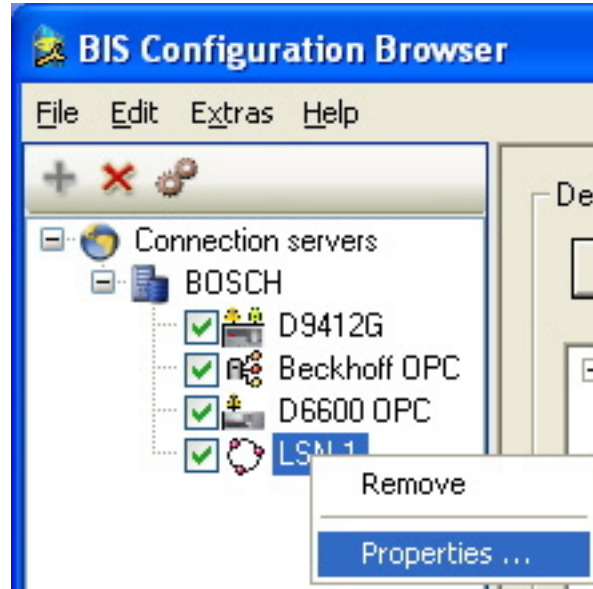
Figure 3.14: BIS Interface to LTC 8300 to 8900 Video Matrix

#	Description
	System (COM interface)
	Matrix LTC 8300 – 8900 port
	Rx = Receiver TX = Transmitter GND Data = Ground for data nc = Not connected
	SUB D 9-female
	SUB D-9 male

4 Configuring OPC-specific data for LSN systems

If, in the **Connections** Configuration Browser tab on a remote server computer, you entered **LSN** as the connection type, you must precisely define the data of this OPC server, and assign the corresponding detector addresses.

1. Right-click the LSN subsystem, then select **Properties...**



2. Define the serial port, baud rate and address offset with which the LSN system will connect.

Offsets (definition)

The **Offset** of an address is a predefined integer that can be added to the addresses of detectors belonging to a particular LSN connection. Offsets can be used to group detectors of the same LSN connection into a distinct numerical address-range, and ultimately help to clarify the origin of an alarm.

Address-offsets work as follows:

- The address offset is added to every address delivered by the LSN connection. The BIS address is calculated by adding the address offset to the address delivered from the LSN connection.

$$\text{BIS Address} = \text{LSN address} + \text{Offset}$$
- Conversely, the address offset is subtracted from every address that BIS sends to the LSN connection.

$$\text{LSN address} = \text{BIS address} - \text{Offset}$$
- Offset values can range from 0 to 2,000,000,000. If a higher number is entered it is automatically changed to the maximum.

How offsets affect existing LSN addresses

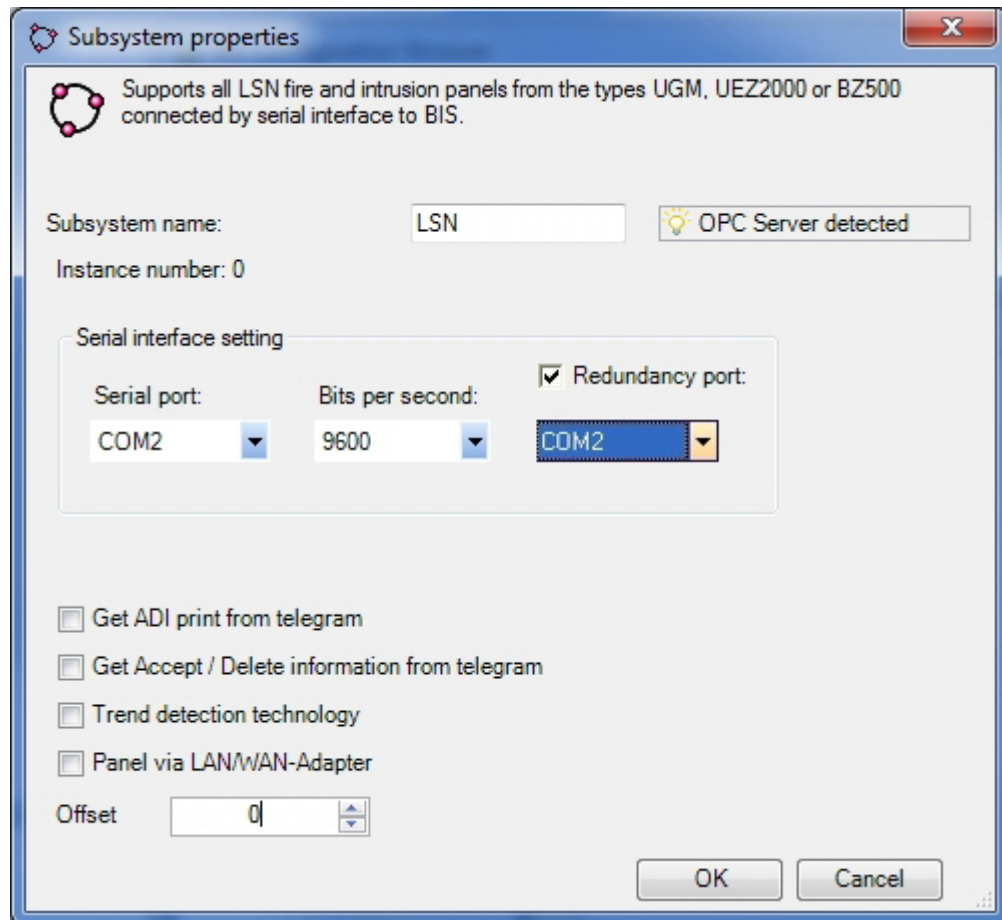
An address-offset can also be applied to an already existent LSN connection. Click **Apply** to activate the offset. The affected addresses will remain valid for all BIS functions that used them before the offset, e.g.:

- Existing associations (also known as “jobs”)
- Existing address lists
- Assignments of detectors to locations
- All addresses that will be on that LSN connection in future

Please note that, depending on the number of addresses affected, there may be a slight delay before the address offset is propagated to these other BIS functions.

How offsets affect new LSN addresses

BIS will raise an error and refuse to duplicate an address that is already in the system, so choose the offset carefully to avoid collisions of address ranges when you create new addresses, either manually/individually, or via an MPP file. See *Reading LSN detector address lists*, page 22.

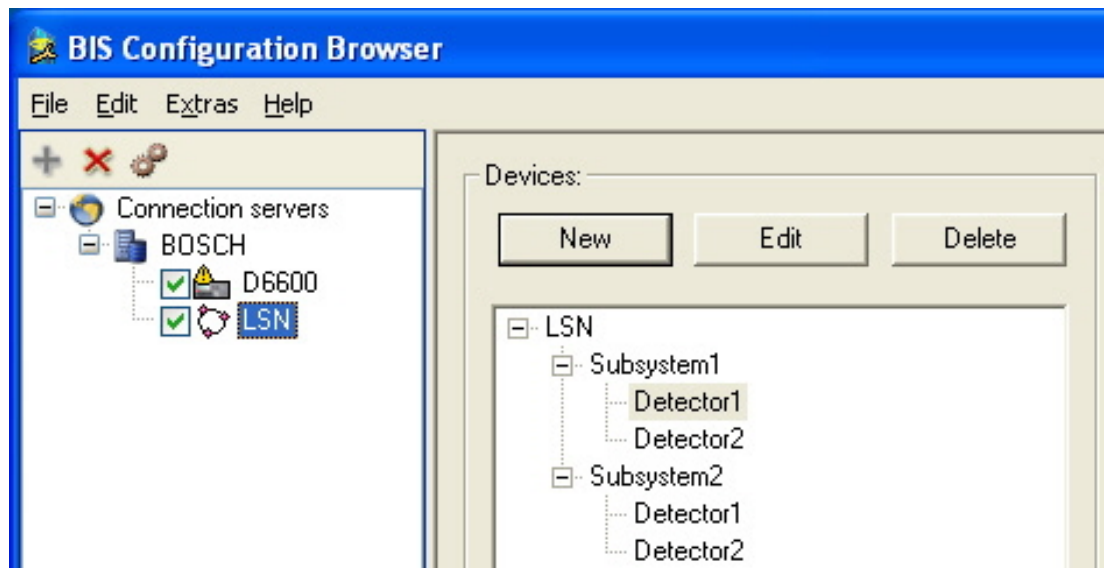


If the connected LSN system is a UGM-type system, and if connection redundancy is to be configured for this system, select the check box **Redundancy port** and choose the port number. The baud rate that you set applies to both ports. Then click **OK**.

Result: The **Subsystem properties** window closes and the offsets are listed in the **Groups** pane of the main window.

Manually modeling the detector-hierarchy of an LSN system

In the **Devices** pane click button: **New**. Select new nodes and click **New** again to create sub-nodes for them. Click button: **Delete** to remove unwanted nodes. In this way you can manually model the detector-hierarchy of the LSN system.

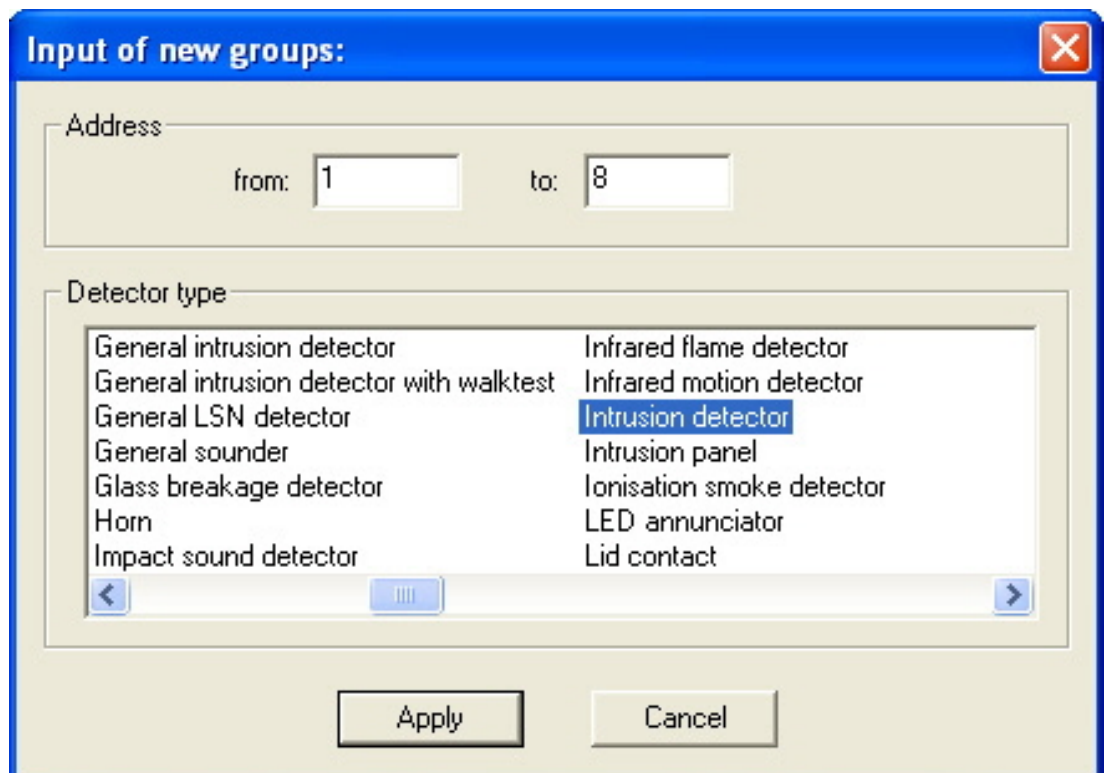


Note: for a batch-method of recreating detector hierarchies in BIS via an MPP file, see *Reading LSN detector address lists*, page 22.

Assigning detector types to detectors

With the detector selected under **Devices**, click **New** under **Groups**. Assign a **Detector type** to each detector created. The control commands and appearance are defined on the basis of the type.

Make sure the text in the **Detector type** field accurately describes the detector. The **Brief text** entered here is used by the GUI in messages sent to BIS operators.



Detector type: Intrusion detector

Brief text:

Location: BIS.Detectors without location

☐ This address signalizes malfunction of the device

✓ Apply ✗ Discard



Notice!

Assigning addresses manually is only required for OPC servers with no configuration program of their own, such as "Beckhoff" OPC servers.

In the case of OPC servers of "LSN" type, the address "0" may not be used, because this always signifies all elements of this address group.


4.1

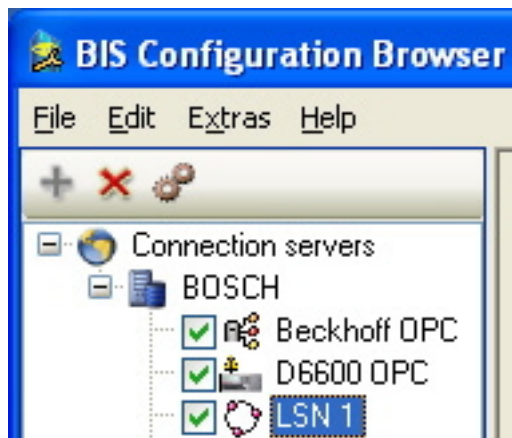
Reading LSN detector address lists

The easiest way to configure BIS with the topology of an LSN system is to read in an MPP file. This is a text file that contains the addresses of all the LSN system's detectors.

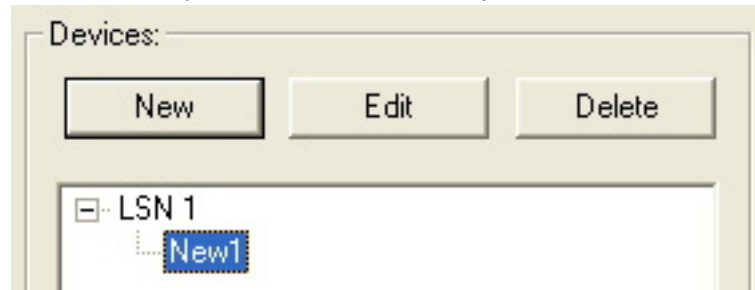
Proceed as follows to generate and read in this file:

1. Generate the MPP file using the configuration program native to your LSN system, such as WINPARA for UGM and UEZ systems, NZPARA for NZ300 systems, or the RPS (remote programming software) for MAP and FPA panels. If in doubt, consult the online help for that configuration program.
2. Copy the MPP file to the BIS server and into a directory that is accessible to the BIS application.
3. In the BIS Configuration Browser, select the **Connections** Outlook button, then select from the **Connection servers** tree the LSN subsystem from which you generated the MPP

file. If this LSN system is not yet in the tree, add it manually now (click the  button and select it from the list of OPC servers offered)



4. In the **Devices** pane, select the desired system in the device structure.



5. Click **Read detector checklists** and locate the MPP file that you generated and copied previously.
- ✓ **Result:** the detector addresses in the file appear as a hierarchy under the selected LSN system in the **Connections** dialog.

4.2 Automatically deleting unaccepted messages

A UGM or other LSN system usually has its own keyboard or a fire brigade control panel. If so desired, BIS can be configured so that deleting messages on these keyboards or panels causes the deletion of the corresponding messages in BIS.



Notice!

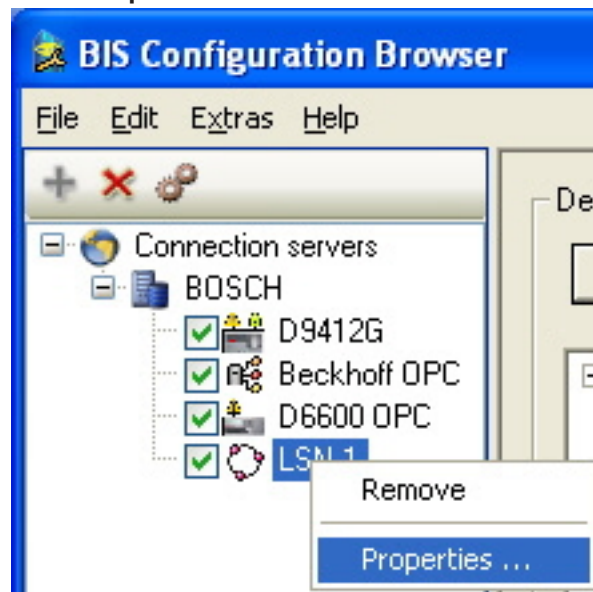
Telegrams and Messages

A **Telegram** in the context of UGM is a complex, machine-readable communication containing the alarm code, address, sub-address, time-stamp and other information.

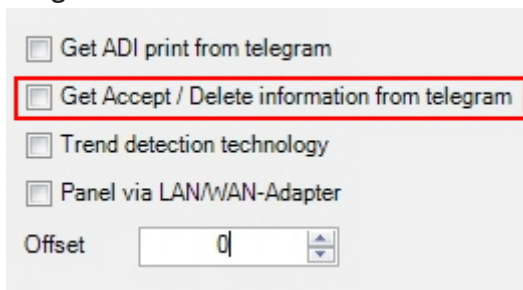
A **Message** is a human-readable extract of a Telegram.

Proceed as follows to enable or disable the automatic processing of such messages:

1. From the Configuration Browser's Connections tab, right-click the LSN subsystem and select **Properties...**



2. To enable automatic message processing, select **Get Accept/Delete information from telegram**.



The screenshot shows a configuration window with several options. The option 'Get Accept / Delete information from telegram' is highlighted with a red rectangular box. Other options include 'Get ADI print from telegram', 'Trend detection technology', and 'Panel via LAN/WAN-Adapter'. Below these options is an 'Offset' field with a value of '0' and a spin button.

3. When this box is selected, if an operator of a remote LSN subsystem deletes or accepts a message on that panel, BIS automatically deletes all messages from that LSN subsystem with the same state, provided the message has not already been accepted by the BIS operator.

BIS will not delete subsystem messages if:

- a BIS client operator has accepted the message

BIS will delete subsystem messages if:

- an action plan containing no actions is assigned to the message
- the address of the message-deletion event is 0xFFFF. In this case **all** messages from that LSN subsystem with the requested state are deleted.
- the subaddress of the message is 0x00. In this case all messages from the subaddress of an address are deleted.



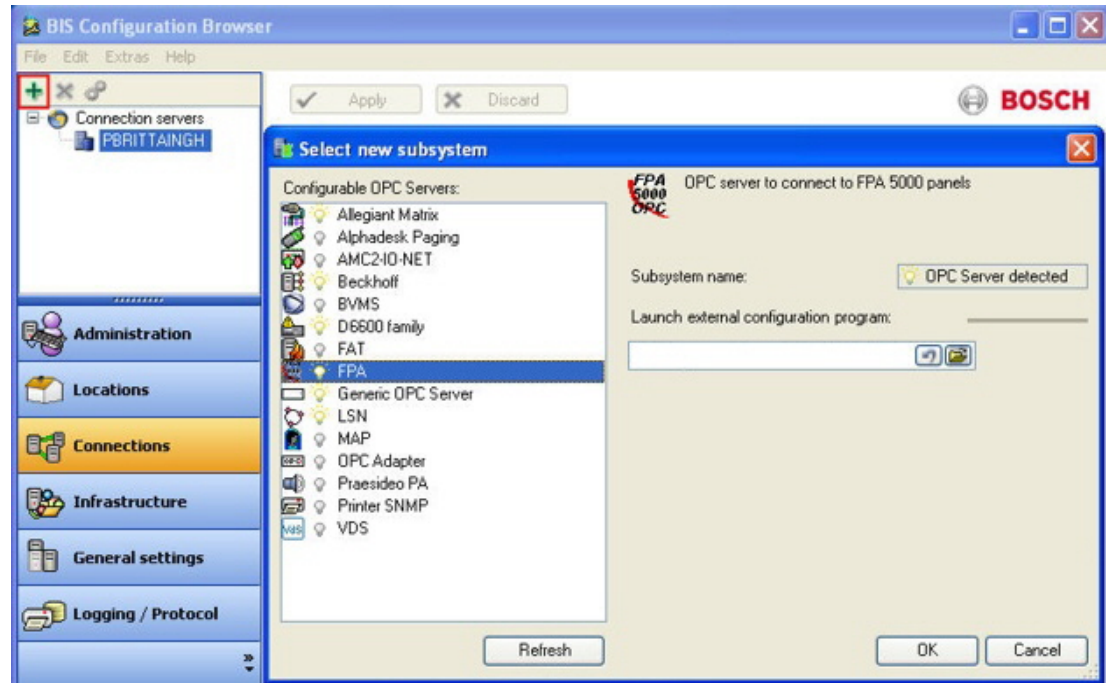
Notice!

The automatic deletion of messages is recorded in the BIS Event log.

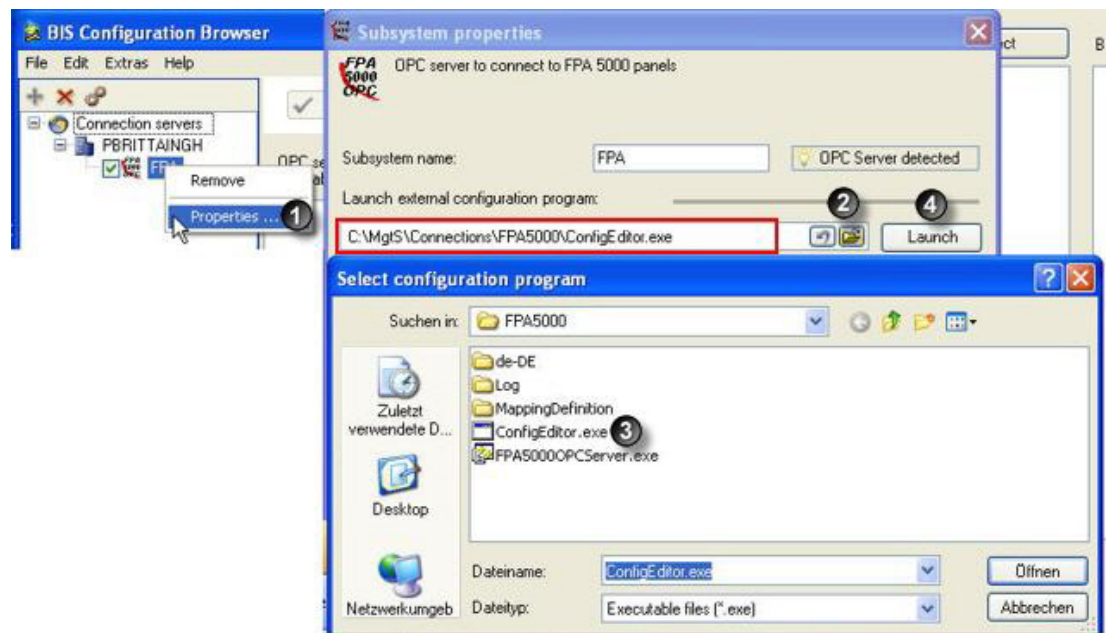
5 Configuring OPC-Specific Data for FPA5000

5.1 FPA connection

First add **FPA** as a new subsystem in the BIS Configuration Browser.



5.2 Calling the OPC configuration editor



Perform the following procedure:

1. Right-click the FPA subsystem, then select **Properties....**

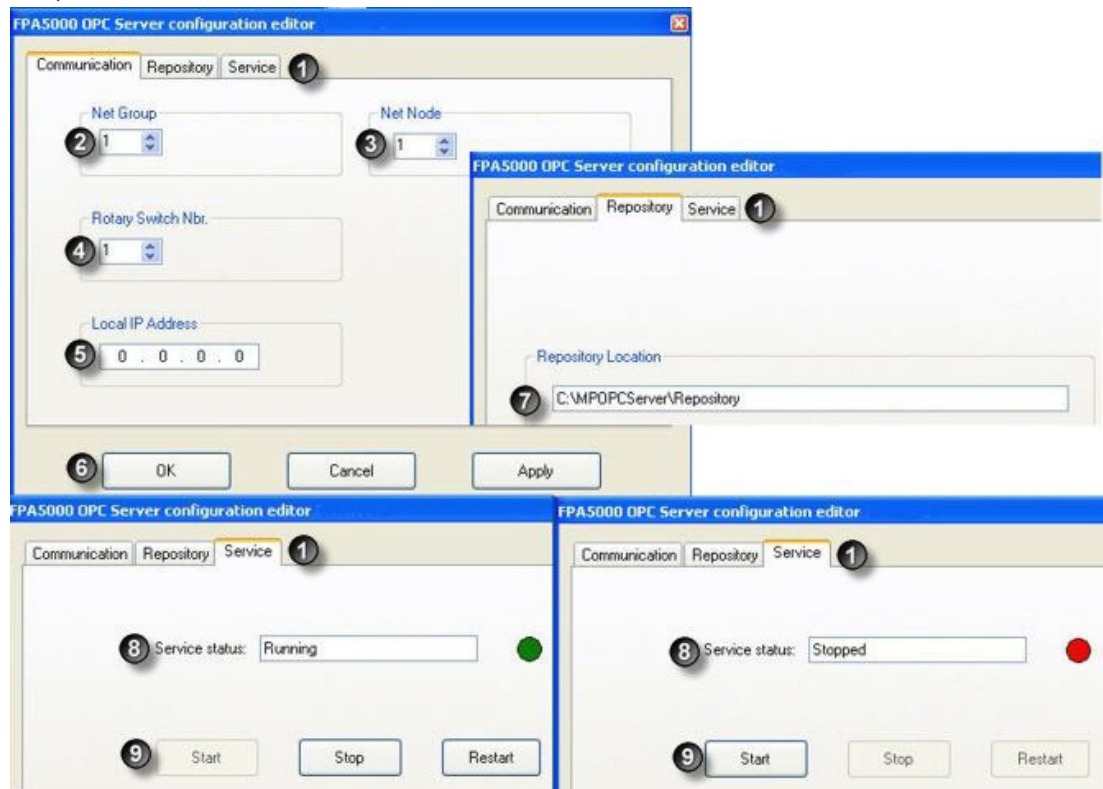
1

2. Check that the configuration program is available in the default directory. If not, select it from the FPA5000 subdirectory using path/file selectors **2** and **3**.
3. Launch configuration program **4**.

5.3

Required settings in the OPC configuration editor

Network identification, and other settings required for OPC communication with a particular FPA, are found on the editor's tabs as follows.



1	Tabs: the currently active tab is highlighted
2	Combo box for setting the FPA Net Group (1 ... 255)
3	Combo box for setting the FPA Net Node (1 ... 255)
4	Combo box for setting the FPA Rotary Switch Nr. (1 ... 232)
5	IP edit box for setting Local IP Address of OPC Ethernet Interface on the OPC server
6	OK, Cancel, Apply buttons for committing or discarding changes
7	Text box Repository Location for entering the folder of the intermediate storage of the FPA configuration

8	Status of OPC server services (as indicated by text and colored “LEDs”)
9	Command buttons for starting, stopping and restarting the OPC server

Notice!

Important



The entries in the fields **2**, **3**, **4** and **5** must match the entries in the corresponding fields of the configuration program FSP-5000-RPS.

The communication between the OPC server and FPA 5000 requires a valid ADC-5000-OPC license key to be inserted into the FPA panel controller.

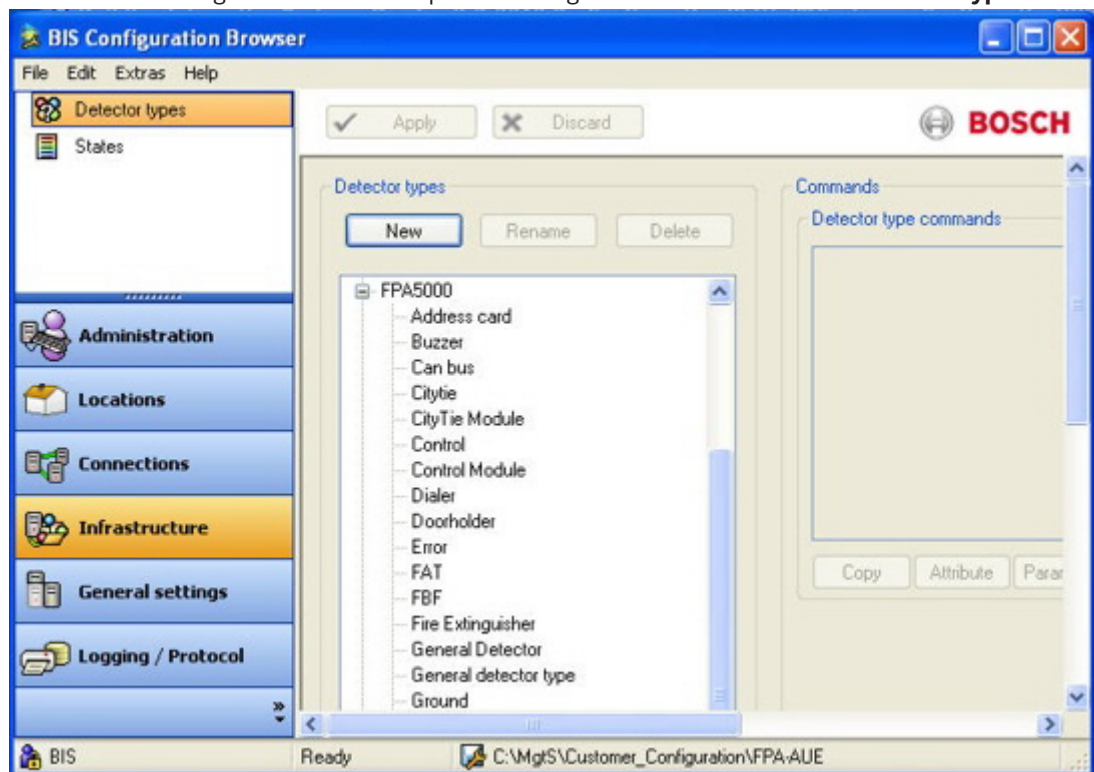
5.4 Browsing FPA detectors

After OPC configuration, configure the FPA connection in the BIS Configuration Browser. The necessary steps are described in the BIS Configuration online help under Configuration Browser tabs > **Connections and Addresses**

5.5 Configuring events and controls

Configure any FPA-specific detector types in the BIS Configuration Browser

See the BIS Configuration online help: BIS Configuration Browser tabs > **Detector types**



**Notice!****IMPORTANT**

Configuration of the FPA basic functions in the BIS Configuration Browser requires FPA5000 system knowledge. Please consult the FPA5000's own documentation.

6

OPC: BIS-BVIP

Introduction

BVIP stands for Bosch Video IP and is the name of a growing family of video products: cameras, encoders, and decoders that communicate via IP (Internet Protocol). Between them the various BVIP products provide a wide range of advanced VCA (video content analysis) features.

BVIP devices communicate with BIS via OPC. To this end BIS provides a configuration tool for locating BVIP devices on the network, sorting them, organizing them and making them available for users of the BIS Video Engine.

Adding the BVIP OPC server to BIS

Add the BVIP OPC server to your BIS configuration as you would any other OPC server. If unfamiliar with the procedure, follow the steps in this subsection:

Prerequisite: A BIS installation running in a network containing BVIP devices.

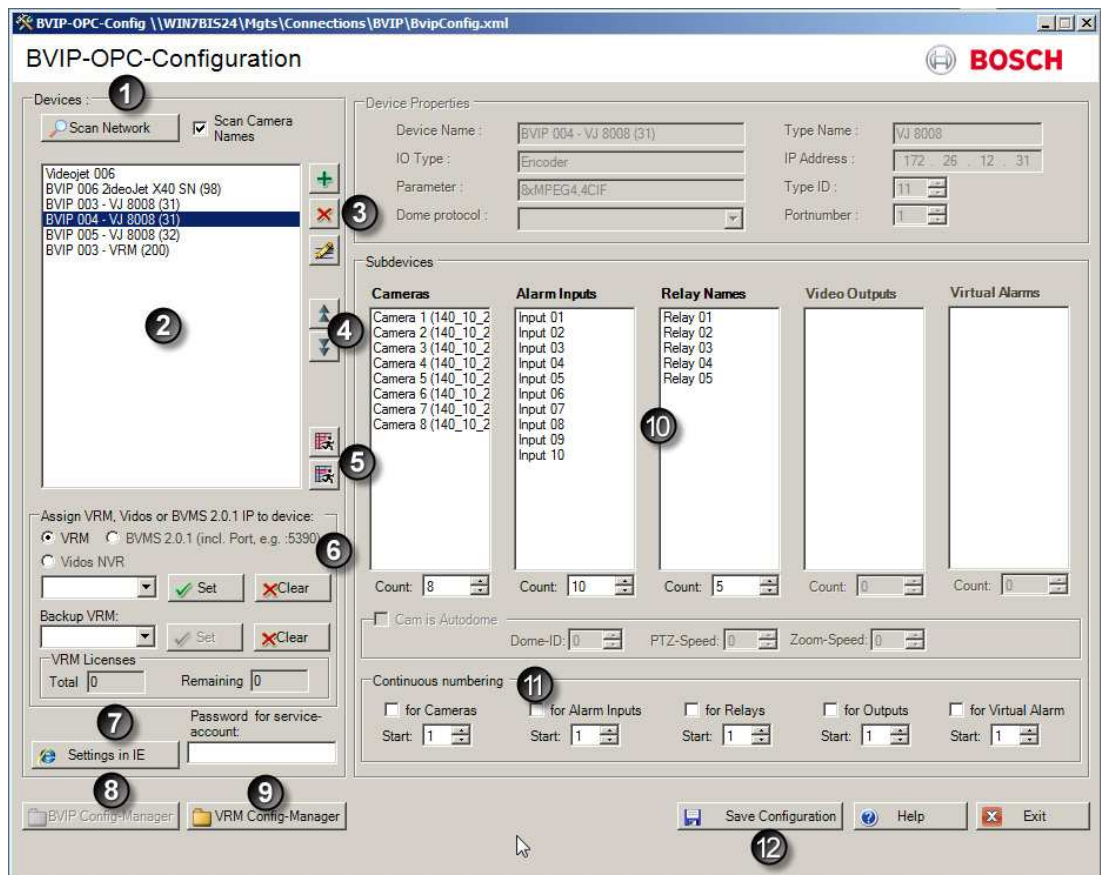
Prerequisite: A BIS configuration loaded in the BIS Configuration Browser.

1. In the BIS configuration browser select the Outlook button **Connections**
 2. In the upper left dialog pane, under **Connection servers**, right-click the login server, or the connection server where the BVIP OPC server resides, and select **Add subsystem...**
 3. From the popup dialog's list of configurable OPC servers select **BVIP Family**
 4. (Optional) Modify the Subsystem name in the textbox if desired, and
 5. Click **OK**.
- ✓ Result: Bvip (or the subsystem name you modified in the previous step) appears in the list of OPC servers.

Launching the BVIP-OPC-Configuration program

1. Right-click the **Bvip** OPC server and select **Properties...**
Result: the **Subsystem properties** dialog opens
 2. Click the **Launch** button to start the BVIP OPC configuration program
- ✓ Result: The BVIP-OPC-Configuration dialog appears

The various controls of the BVIP-OPC-Configuration dialog are explained in the graphic and table below.



1	Button to scan the network for BVIP devices	7	Button to invoke the webpage for the selected device in the IE browser. This is a superset of the features assigned by icons (5). Note that a password for the device's service account may be demanded.
2	List of BVIP devices currently added to this configuration	8 and 9	Buttons to invoke the configuration manager programs for BVIP devices and VRMs.
3	Buttons to add, remove or edit selected devices	10	Columns displaying the various cameras, inputs and outputs of the selected device.
4	Buttons to move the selected device up and down within the list.	11	A set of controls for applying a continuous numbering scheme to the BVIP devices currently added to this configuration. Continuous numbering may be requested by operators for ease-of-use.

5	The upper button invokes a dialog to add VCA features to all listed devices. The lower button invokes a dialog to add VCA features to only the selected devices (i.e. those highlighted in list (2)).	12	Buttons to save the configuration and exit the BVIP-OPC configuration tool.
6	Controls for assigning a VRM (Video Recording Manager) and a backup VRM to the selected device.		

Locating BVIP devices on the network

1. In the BVIP-OPC-Configuration dialog click the **Scan Network** button. Note that the check box **Scan Camera Names**, if selected, forces the retrieval of any names given manually to the devices. If the check box is cleared a generic naming scheme is used.

Result: The **Device Scanner** dialog appears. This dialog lists all the BVIP devices that it finds on the network. Devices that are not yet in the BVIP OPC server's device list are displayed in normal typeface with selected check boxes. Devices that have already been added are displayed in grayed-out typeface with their check boxes cleared.

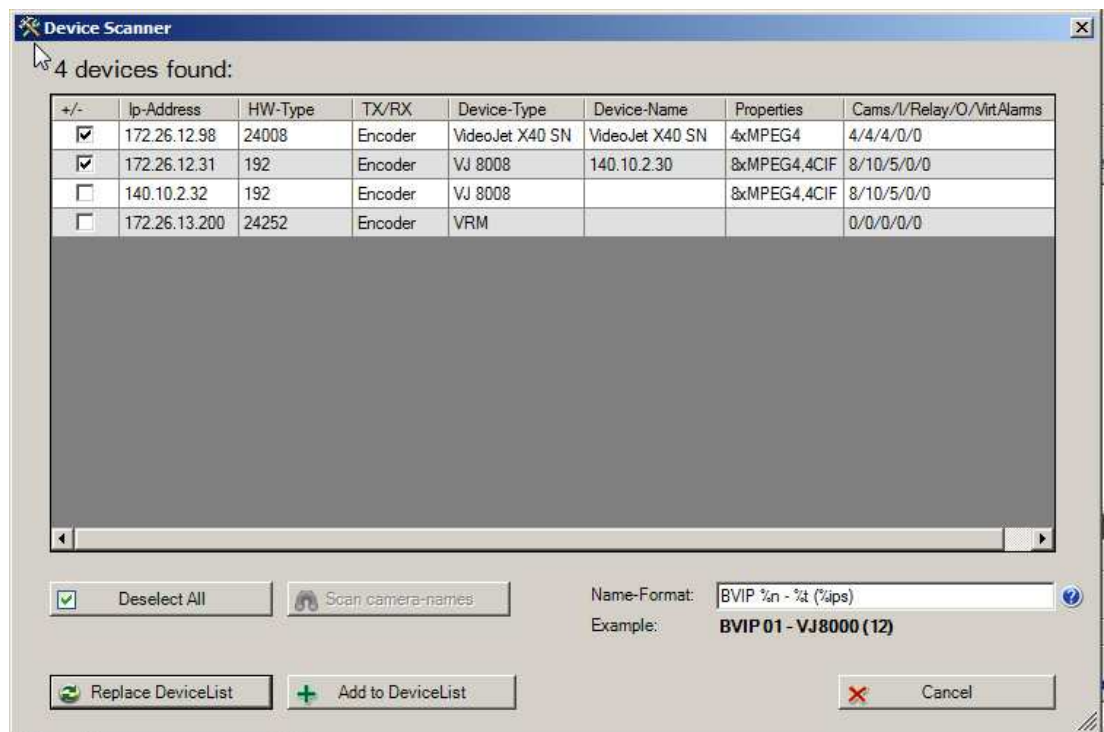


Figure 6.15: Device scanner

2. Click the button **Replace Device List** to overwrite the current device list with those whose check boxes are selected here;
Alternatively click **Add to Device List** to add them to the current device list.

Activating VCA (Video Content Analysis) for BVIP devices

You can activate video content analysis uniformly across all BVIP devices in your list, or individually for selected devices. Proceed as follows:

Prerequisite: There are BVIP devices in the list of devices in the BVIP-OPC Configuration program. See (2) in , page 30 above.

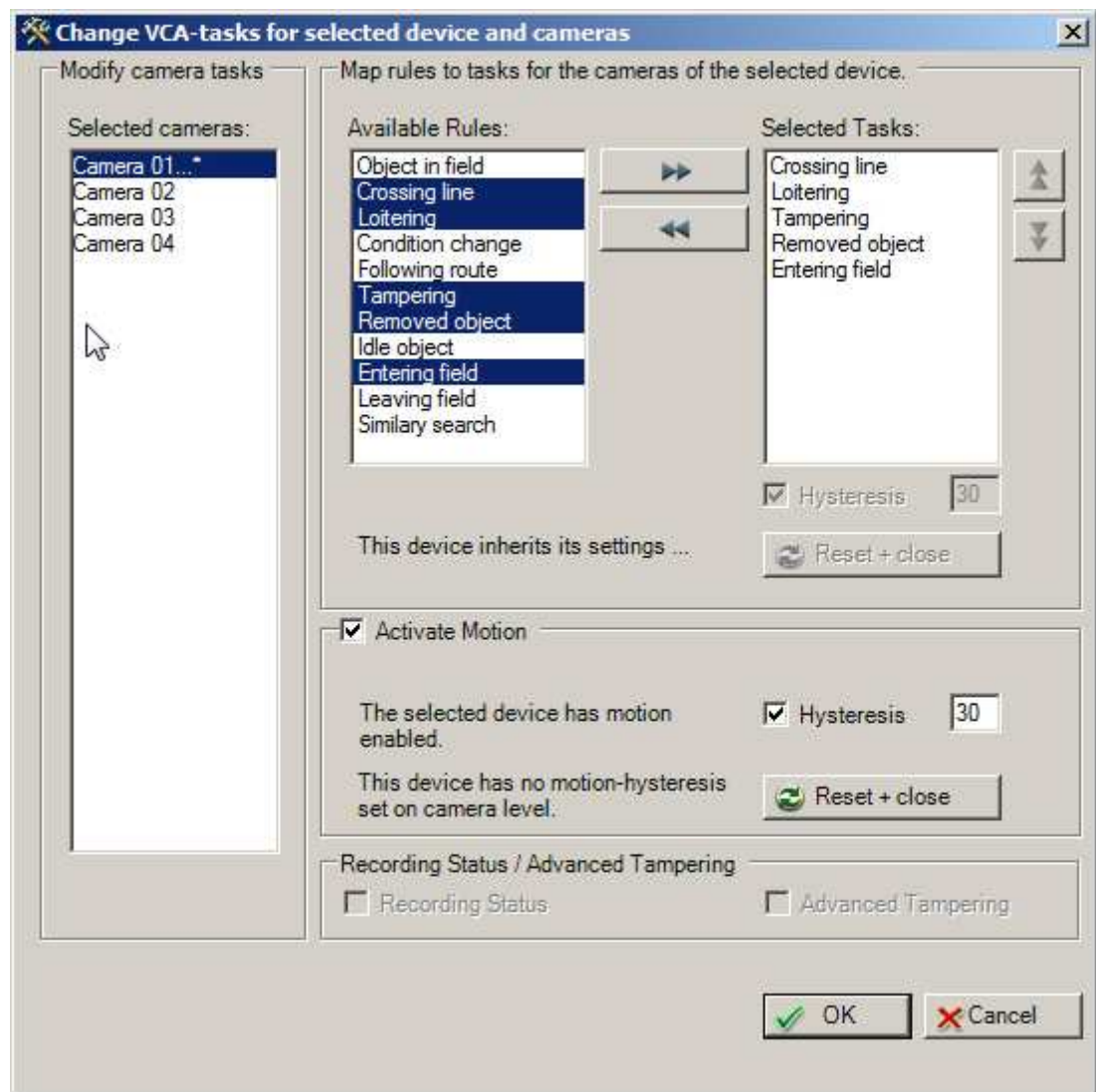


1. Click the **upper** of the two VCA buttons to add or modify VCA features for **all** devices in the list

-or-

Click the **lower** VCA button to add or modify VCA features for **only the currently selected devices**. See (5) in , page 30 above.

Result: A dialog appears for changing VCA tasks. NOTE: If you have chosen to modify the VCA features for all devices then the **Selected cameras** list will not appear in the dialog.



2. If appropriate, first select a camera from the **Selected cameras** list.
3. Next, use the horizontal double-arrow buttons to move a maximum of 8 VCA features from the **Available** to the **Selected Tasks** list.
4. Use the vertical double-arrow buttons to change the order of VCA features in the **Selected Tasks** list.

**Notice!**

Order of the selected VCA features

IMPORTANT To ensure correct functioning of the feature within Video Engine, ensure that the order of VCA features in the **Selected Tasks** list corresponds to the order defined on the configuration web-page of the camera itself.

See also

– , page 30

7 OPC: FPA 5000

Introduction

The Fire Panel 5000 system can be integrated with BIS through OPC. This section describes the prerequisites for this integration, the installation of the OPC server on the BIS server or one of its connection servers, and the configuration steps necessary within BIS.

Prerequisites for FPA 5000

- **Hardware:** A network connection to the computer where the FPA 5000 server is to run, either BIS server or one of its connection servers
- **Software:** The FPA OPC server software, available from Bosch ST technical support.
- **License:** The license code for the FPA OPC server software, available from xxx

Prerequisites for BIS

- **Hardware:** a network connection to the computer where the FPA OPC server is to run, if this is a BIS connection server
- **Software:** BIS with Automation Engine
- **Licenses:**
 - The BIS Re-fitting features specific to your version of BIS
 - Additional OPC server licence
 - Enough Bosch detector points for the proposed BIS+FPA configuration

7.1 Step-by-Step Configuration

7.1.1 FSP-5000-RPS

1. Open the FSP-5000-RPS programming software.
2. In an existing 2.x configuration select “Nodes” in the tree view and choose “Create FPA-5000 OPC- Server” in the context menu.
A new node with name FPA-5000 OPC-Server is created and a dialog box for configuration is opened.
3. Configure the OPC server node.
Enter the virtual RSN and logical node.
4. Choose **IP Settings...** to enter the IP settings dialog.
5. Edit the fields accordingly. **IP Address** and **Subnet Mask** are mandatory fields, **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 RSN and the IP address are required to configure the OPC server.

6. Confirm your changes with **OK** and leave the dialog.
7. Double-click on the FPA-5000 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 are not assigned an IP address.
10. Confirm your changes with **OK** and leave the dialog.
11. Double-click on the “FPA-5000” node, e.g. “FPA 5000 – 1.1 – RSN”
A dialog box for FPA-5000 additional configuration opens
12. Select **OPC Server** under a vacant **Inserted address card(s)** field.

**Notice!**

It is mandatory that this FPA-5000 node is then assigned to the OPC server!

13. Choose the country and the language from the list

**Notice!**

Take care about the country and language settings. BIS 2.x will display commands and detector names in the selected language.

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

7.1.2**Panel Controller MPC-xxxx-B or MPC-xxxx-C**

1. Insert the ADC-5000-OPC card into one of the vacant address card slots.
2. Go to the node that has been assigned an IP address and connect the Cat.-5 cable to the MPC-xxxx-B or MPC-xxxx-C “Ethernet” port (RJ45).

7.1.3**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\Bosch\FPA5000 OPC-Server\Log (for Windows XP, might be slightly different for other operating systems).

7.2**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 (see --- MISSING LINK ---) 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 a OPC command. Then switch the Walktest off 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” with via OPC to the panel and receive “Normal” when the detector changed back to its normal state.

7.2.1

Start situation

The panel has started and connected with the OPC server the panel is in base position without troubles or alarms.

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) the normal state for all kinds of items without activation or trouble.

7.2.2

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 Step 2: Execution of commands for more information about that).

The panel will set the detector in the administrative state “Walktest” (Compound state 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.

7.2.3

Create a fire alarm and reset it with OPC

Now we are pressing the button on the manual call-point. FPA5000 displays an fire alarm on 2.8.DETECTOR.2.1. So do 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 we 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"/>
```

After that the state of the detector returns to normal again and the fire report vanish from the panel display:

7.3

General troubleshooting

If the configuration of the FSM-5000-OPC server doesn’t work with the FPA-5000 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 OPC card is detected by panel:

Choose in the start menu of the panel controller: **Diagnostics - Hardware - Address cards**

8 OPC: MAP 5000

Introduction

The Modular Alarm Platform (MAP) 5000 system can be integrated with BIS through OPC. This section assumes a working MAP 5000 and describes the prerequisites for the integration, the configuration of MAP 5000 for use with BIS, the installation of the OPC server on the BIS server or one of its connection servers, and the configuration steps necessary within BIS.

Prerequisites for MAP 5000

- **Hardware:** A network connection to the computer where the MAP OPC server is to run, either BIS server or one of its connection servers
- **Software:** The MAP OPC server software, available from Bosch ST technical support.
- **License:** The license code for the MAP OPC server software, as purchased from Bosch.

Prerequisites for BIS

- **Hardware:** a network connection to the computer where the MAP OPC server is to run, if this is a BIS connection server
- **Software:** BIS with Automation Engine
- **Licenses:**
 - The BIS Re-fitting features specific to your version of BIS
 - Additional OPC server licence
 - Enough Bosch detector points for the proposed BIS+MAP configuration

Configuring MAP 5000 for use with BIS

Three basic steps need to be performed within MAP, using MAP's RPS (remote programming software):

1. Each MAP's internal BIS user needs to be activated.
2. Each MAP panel needs its own IP address
3. Each MAP panel involved needs to export its detector and its area configurations; that is, each panel needs to generate 2 XML files.

Notice!



Detector points' areas and names.

When configuring MAP, ensure that all detector points are assigned to areas. Otherwise they will not be visible to BIS.

BIS requires unique detector names, although MAP does not. Therefore configure your MAP with unique names if you want to integrate it in a BIS system.

Activating the MAP-internal BIS user.

1. Start the MAP RPS software and open the **Hardware Manager**
2. In the hardware hierarchy, select a MAP panel you wish to integrate with BIS.
3. In the main dialog pane, under the rubric for BIS settings:
 - enter the user code for the MAP internal BIS user. The factory default is 000003
 - Note:** accept the default value if provided
 - select the check box to activate BIS programming

Assigning an IP address to the MAP panel

4. Start the MAP RPS software and open the Hardware Manager
5. In the main dialog pane, under the rubric for the MAP panel, enter an IP address for the panel
6. Click menu: **Review > Network setup** and enter the IP address, subnet mask, and standard gateway for the panel.

Exporting
(publishing) the
panel
configuration

7. In the MAP RPS software click **RPS Menu Button > Publish**
8. Browse a directory in which to store the panel configuration files, and click **OK**
9. Two files are written to that directory. These files :
 - `Id_all_cfg_001.xml`, containing the IDs of all detector points
 - `Area_cfg_001.xml`, containing the assignments of IDs to areas
 -

Installing the MAP OPC server

Prerequisites

The MAP OPC server is installed on the BIS server or one of its connection servers. The following are required:

- **Hardware:** 1.6 GHz CPU and 2 GB RAM
- **Software:**
 - Windows 7 32 bit or Windows XP 32 bit
 - Windows Installer v3.1 or higher
 - .NET Framework v3.5 SP1 or above
 - OPC core components

Installation steps

1. Right-click the file `MapOPCSetup.msi` and select **Run as Administrator**. Click **Next**.
2. In the ensuing dialog do the following:
 - Enter the folder where the MAP OPC server should be installed and
 - Select the radio button **Everyone**.
3. Click **Next** and wait for the installation to finish. Then close the dialogs.

Verifying correct installation of the MAP OPC server

Check the installation log

1. In the installation folder of the MAP OPC server (which you entered above) open the file `install.log` in a text editor.
2. Verify that the body lines begin with the success code 0. These lines confirm, for example, that the user `mgts-service` exists, and has the correct write-permissions. If there are non-zero return codes then proceed to the next section “Checking the DCOM parameters of the MAP OPC server”, else proceed to “Configuring the Windows Service MAP Communication”.

Note: If the user `mgts-service` does not exist before installation of the OPC server, then `MapOPCSetup.msi` creates it with the default password **mgts**. In this case a 2 appears at the beginning of the line. This is no cause for concern, and you may proceed to “Configuring the Windows Service MAP Communication”.

Checking the DCOM parameters of the MAP OPC server

Note: This section may be skipped if the lines of the `install.log` file are prefixed only with the success code 0.

1. Click the Windows **Start** button and search for `dcomcnfg.exe`. Execute this program
2. In the left pane navigate as follows: **Console Root > Component Services > Computers > My Computer > DCOM Config**
3. In the central pane find the MAP OPC server, right-click and select **Properties**
4. On the **Security** tab, make sure that all permissions (Launch and Activation, Access and Configuration) are set to **Customize**
5. On the **Identity** tab, select the radio button **This user** and enter the username and password of the `mgts-service` user. If the user has just been created by the installation program then the password is **mgts**.

Configuring the Windows Service MAP Communication to start automatically

Note: This is a mandatory post-installation step.

The MAP Communication Service is part of the MAP OPC server and is responsible for communication with the MAP panel.

1. Click the Windows **Start** button and search for `dcomcnfg.exe`. Execute this program
2. In the left pane navigate as follows: **Console Root > Services (Local)**
3. In the central pane find the MAP Communication Service, right-click and select **Properties**
4. On the **General** tab, set the **Startup type** to **Automatic**
5. Start the service manually if required immediately. Else the service will only be started automatically upon rebooting the computer.

Configuring the OPC server

The following steps are mandatory.

Setting the start parameters.

1. In the MAP OPC installation folder copy the configuration files `Id_all_cfg_001.xml` and `area_cfg_001.xml`, which were published by (i.e. exported from) MAP's remote programming software (RPS). Paste the two files into the `RPS_config` subfolder of the installation folder. If multiple MAPs are to be connected, create numbered subfolders of `RPS_config` and copy the file-pair from each MAP into its own subfolder.
For example, two valid paths could be:
`\RPS_config\1\Id_all_cfg_001.xml` and `\RPS_config\2\Id_all_cfg_001.xml`
where each of these files was generated by a different MAP and contains that MAP's configuration.
2. In the MAP OPC installation directory right-click and start the program `StartparametersEditor.exe` as Administrator
3. Click menu: **File > Open** and select `Startparameters.xml` from the same directory
4. On the **Panels** tab for the first MAP 5000 to be integrated enter the following information
 - Panel name
 - Panel serial number
 - Panel IP address
 - Panel user ID
 - Panel Realtime port (default 6793)
 - Panel user DB port (default 6794)
 - The directory where the copies of the published XML files reside.
5. On the **States** tab change the IDs of the following states to be compatible with BIS
 - Change **tamper internal** to 1550 or 1243
 - Change **walk test** to 2014 or 1866
 - Change **installer mode** to 1242
6. On the **License Key** tab enter your product code. Without such a code the OPC server will shut down after 90 minutes.
7. On the Settings tab you may alter the following parameters if desired:
 - **Reconnection:** the number of attempts that should be made to reestablish a lost OPC connection. The value 0 (zero) means infinite retries.
 - **Connection polling time:** the amount of time to wait between connection retries.
 - **Ignore value:** The number of connection retries before generating an error message
8. If another panel is to be integrated, click menu **Panels > Add panel** and repeat steps 4 through 7.

Configuring BIS for use with MAP 5000

The configuration within BIS consists of three steps. Perform all three:

- Adding to BIS the new states provided by the MAP OPC server

- Connecting the MAP OPC server to BIS
- Adding to BIS the detectors made available through the MAP OPC server

Adding to BIS the new states provided by the MAP OPC server

1. Start the BIS Configuration Browser on the configuration that is to include MAP 5000
2. Click **Infrastructure > States**
3. Add a new State-list with the following entries. This is more convenient than adding the states individually, as state-lists can be used in BIS Jobs, Associations and If-Then rules)

State	Description	Priority
5000	Bypass	20
5001	Verification	18
5002	Installer mode	18
5003	Disabled	19
5004	ready to arm	49
5005	ready to disarm	48
5006	notready to arm	50
5007	walk test	18
5008	Antimask	18

Connecting the MAP OPC server to BIS

1. Click **Connections > Connection servers**
2. Right-click the connection server to which the MAP is connected and select **Add connection.**
3. Select MAP from the ensuing dialog and confirm with **OK**

Adding to BIS the detectors made available by the OPC server

1. Back in the main BIS dialog click the **Connect** button. The left column becomes populated with all the devices connected to the MAP OPC server.
2. Right-click the MAP object in the left column and select **Add.**
3. Confirm in the ensuing popup that you wish to load the detector type definitions from the server.

Note: Bosch recommends that you store the detector point addresses of the MAP in a BIS Address List.

1. In the BIS Configuration Browser click **General Settings > Address Lists.**
2. Right-click the MAP panel and select **New.** Give the list the name MAP.
3. Add the range of states from the right-hand dialog pane.
4. Save the configuration

Save and load the configuration to use the MAP 5000 OPC server within BIS.

9 OPC: Praesideo PA system

Praesideo from Bosch is a full-featured, digital public address (PA) and emergency sound system. The PA system is crucial to the successful evacuation of buildings and safe, efficient control of human crowds.

Integration with BIS provides a direct link to the systems which detect threats to those crowds, and helps to save lives by faster, clearer, more informative and better-directed communication.

9.1 Overview

Praesideo is integrated into BIS via its own OPC server.

When integrated, the BIS operator can perform the following Praesideo operations from within BIS:

- Initiate public address announcements
- Direct announcements to the zones affected by a threat, depending on the information collected by fire alarms and other detectors.
- Track all actions taken and the course of the evacuation in the BIS event log.

Software versions supported:

Software	Versions
OPC-DA (Data Access)	V1.0A, V2.05, V3.0
OPC-AE (Access and Events)	V1.10
BIS	V2.3 and higher

9.2 Prerequisites

Setting up the software

1. Install BIS including Automation Engine (AUE)
2. Login as **MgtS-Service**
 - Note: if the user name **MgtS-Service** is not available for login, remove it from the Windows local security policy **Deny logon locally**
3. Check the configuration and connectivity of the Network Controllers (NCO)
 - set the IP address of the NCO using NCO's control button
 - ping the Praesideo NCO to check connectivity
 - log on to the Praesideo NCO via its web interface
 - Make sure you can see the names of NCOs, connected units (e.g. amplifiers), zones and audio inputs,
4. Set up prerequisite software Praesideo core and Praesideo Open Interface (POI) on the BIS server
 - install Praesideo core from the following folder on the BIS installation medium: _Install\AddOns\BIS\PraesideoOPC\
 - install Praesideo Open Interface from the same folder
5. Set up the OPC server
 - **Important note:** If you are performing a BIS update, make a backup first of the Praesideo configuration file.
 - Install the Praesideo OPC server from the Praesideo installation medium

- Click **Start > Run > dcomcnfg** and set the dcomcnfg identity of PraesideoProxy to **MgtS-Service**
- Configure the OPC server by running the following file:
<installation drive>:\MgtS\Server\Praesideo Proxy\PraesideoProxyCfg.exe

**Notice!**

IMPORTANT: Always keep an up-to-date backup of the Praesideo configuration file

To retain across BIS upgrades your configuration of Praesideo devices, you will need to copy this backup to the Praesideo directory after the BIS upgrade. A BIS upgrade installation does NOT do this automatically.

After installing the Praesideo software the configuration file is located by default in:

<installation drive>:\MgtS\Server\Praesideo Proxy\

- Check the correct functioning of the OPC server
 - Start the Softing OPC client (<installation drive>:\MgtS\Tools\Softing\SOClient.exe)
 - Connect to the Praesideo OPC
 - Add all items
 - Ensure the state of the zone(s) is **10009** (= free) or **10011** (= background music)
 - Start a call using Praesideo hardware, e.g. a call station and its key-pad, to the same zone(s)
 - Ensure the state of the zone(s) is **10010** (= in use) for as long as the call is active
 - **Notes** for more recent versions of Praesideo OPC, e.g. 4.2.1.0:
All NCO related items show value '0' if only Data Access (DA) part of Praesideo OPC is connected
To monitor real-time values, the Alarm and Events (AE) part of the Praesideo OPC must be started as well.
- Connect BIS to OPC server
 - Add new Praesideo states to BIS configuration (Configuration Browser > **Infrastructure > States**) OR load a configuration that already contains these states
 - Add connection in Configuration Browser > **Connections > Generic OPC > Praesideo 30 DA+AE**
 - connect to the OPC server and add all addresses you require into the BIS configuration
- Test run: Start a prerecorded message from NCOs internal flash disk using the BIS client:
 - Right-click and select the command **Start** on any Call item, e.g. Call_0, Call_1.
 - Specify parameters. For test purposes use:
Routing: (names of a zone or zones that you have already configured in Praesideo)
Priority: 100
Partial: 1
StartChime: 2-tone chime
EndChime: 2-tone chime
LiveSpeech: 0
AudioInput: 0
Messages: (the name of a message that you have already recorded in Praesideo)
Repeat: 1 (repeat the message once)
 - In the BIS client observe the state changes of this Call item and the zones addressed
 - Wait till announcement is over or cancel call by right-clicking the Call item and selecting "abort".

9. Test run. Start a live call from any audio input (e.g. call station) using the BIS client
 - Select right-click command “Start” for any call item.
 - Specify parameters from the test run in the previous step:

Routing: (names of a zone or zones that you have already configured in Praesideo)

Priority: 100

Partial: 1

StartChime: 2-tone chime

EndChime: 2-tone chime

LiveSpeech: 1

AudioInput: (the audio-input name of your call station)

Messages: , (that is, a single comma, meaning no prerecorded messages)

Repeat: 0
 - In the BIS client observe the state changes of this Call item and the zones addressed
 - Stop the transmission of live speech by right-clicking the Call item and selecting "stop".

9.3 Data point type Call: Commands and events

The number of Call items available to the BIS/Praesideo system is fixed in the configuration file of the OPC server. Their names consist of a string plus an incremental suffix, e.g. Call_1, Call_2 etc.

Sending commands

To send a command to a Praesideo Call item from the BIS client, Device overview:

1. Right click the Call item
 2. Add the name of the command and the parameters via the **Parameter Entry** dialog box
 3. The parameters for the commands **Add to**, and **Remove from** can be left empty if you do not wish to add or remove target zones
 4. Pre-recorded calls reset automatically when they finish.
- Live calls require a **Stop** or **Abort** command, otherwise the audio input channel remains open and the zones continue to hear whatever is spoken near the microphone.

Data point type	Commands	Description
Call	Start	Creates and starts a call
	Stop	Finishes the call and adds the end chime
	Abort	Cuts the call off immediately and plays no end chime
	Add to	Adds resources (typically zones or zone groups) to a call in real time. Added zones start to hear the call from the moment the command is successfully issued.
	Remove from	Removes resources (typically zones or zone groups) from a call in real time. Removed zones stop hearing the call from the moment the command is successfully issued.
	Reset	Resets the state of a Call item to Inactive
	Start Extended Call	Creates and starts a call with extended attributes (see below for Properties and event attributes for extended calls)

Tab. 9.1: Calls/Commands

States

The Call items can be in any of the states listed below. These are then reflected in the **Device overview** in the BIS client UI.

Inactive is the default state. Call items are set to Inactive when they have completed successfully. This Call item can then be reused.

The state names that end in the word **faulty** indicate that at least part of the Call has failed.

The **Reset** command sets the state of a Call from any state to **Inactive**.

Data point type	States	Description
Call	Inactive	The default state. The Call item is ready for use
	Start	The Call item initializes and plays the start chime
	Start faulty	At least one of the Call's resources is unreachable
	Messages	The Call item carries a pre-recorded message
	Messages faulty	At least one of the Call's resources is unreachable
	Live Speech	The Call item carries live speech from an operator
	Live Speech faulty	At least one of the Call's resources is unreachable
	End	The Call item is terminating
	End faulty	At least one of the Call's resources is unreachable

Tab. 9.2: Calls/States

Properties and event attributes

The following is a list of the parameters that can modify commands to Call items. Start a command on a call item by right clicking it in the **Device overview** in the BIS client. Add the parameters in the **Parameter entry** pop-up box.

Data point type	Item properties and event attributes	Description
Call	Property name	Data type, description
	Routing	Names of zone groups, zones and control outputs (Item IDs without network controller ID) where the call is targeted (comma separated list without blanks)
	Priority	Call priority. Default priority is 100. Calls with a priority over 223 become emergency calls and supersede all others.
	Partial	1 = Partial: make the call even if not all zones are available. 0= Not partial: all zones must be available before making the call
	StartChime	Name of the start chime
	EndChime	Name of the end chime
	LiveSpeech	Whether the call contains a live announcement
	AudioInput	Name of audio input channel for live announcement. Typically this is the microphone on the call station unit.

Data point type	Item properties and event attributes	Description
	Messages	Names of pre-recorded messages separated by commas. A comma alone signifies absence of pre-recorded messages
	Repeat	Number of times a call should be repeated. 0 = play the message only once.

Tab. 9.3: Calls/Properties and event attributes**Properties and event attributes for extended calls**

The following is a list of the parameters for an extended call. Start a command on a call item by right clicking it in the **Device overview** in the BIS client. Add the parameters in the Parameter entry pop-up box.

Data point type	Item properties and event attributes	Description
ExtendedCall	Property name	Data type, description
	Routing	Names of zone groups, zones and control outputs (Item IDs without network controller ID) where the call is targeted (comma separated list without blanks)
	Priority	Call priority. Default priority is 100. Calls with a priority over 223 become emergency calls and supersede all others.
	OutputHandling	0= Not partial: all zones must be available before making the call 1 = Partial: make the call, even if not all zones are available. 2 = Stacked : extend partial calls with replays to previously unavailable zones
	StackingMode	0 = Wait for all zones to become available before starting replay 1 = Start replay for individual zones as soon as each becomes available
	StackingTimeout	Number of minutes for a stacked call to wait for available resources. 0 = wait indefinitely, i.e. no timeout 1-255 minutes
	StartChime	Name of the start chime
	EndChime	Name of the end chime
	LiveSpeech	Whether the call contains a live announcement
	AudioInput	Name of audio input channel for live announcement. Typically this is the microphone on the call station unit.
	Messages	Names of pre-recorded messages separated by commas. A comma alone signifies absence of pre-recorded messages

	Repeat	Number of times a call should be repeated. 0 = play the message only once.
	CallTiming	0 = Immediate, broadcast when the call is started 1 = Time-shifted, broadcast when the original call is finished 2 = Monitored, broadcast when not cancelled within 2 seconds after the monitoring phase has finished
	PreMonitorDest	The destination zone of the pre-monitor phase of a pre-monitored call
	LiveSpeechAtt	The attenuation to be used for the audio input during the live speech phase. Range 0..60 dB.
	StartChimeAtt	The attenuation to be used for the chime generator during the start chime phase. Range 0..60 dB.
	EndChimeAtt	The attenuation to be used for the chime generator during the end chime phase. Range 0..60 dB.
	MessageAtt	The attenuation to be used for the message generator during the prerecorded message phase. Range 0..60 dB.

Tab. 9.4: Extended calls/Properties and event attributes

9.4 Data point type Unit:

Units are the hardware in the Praesideo network. Typical examples are

- Network controller (NCO)
- Power amplifier
- CobraNet expanders
- OMNEO expanders
- Call station

...plus various channels and interfaces. For instance, the Network controller (NCO) typically uses a hardware unit known as a call stacker. The call stacker temporarily stores calls until their intended target zones become available to play them. Communication with call stackers is invisible to the user, who addresses only the NCO.

The BIS operator monitors Units for faults, or sends one of the following commands:

Sending commands

Data point type	Commands	Description
Unit	Reset fault	Parameter: The Event ID of the POI diagnostic event
	Resolve fault	Parameter: The Event ID of the POI diagnostic event
(CobraNet and OMNEO expanders only)	Disable	Puts the unit in state DisabledByUser , regardless of its real state
(CobraNet and OMNEO expanders only)	Enable	Undoes the DisabledByUser state

Data point type	Commands	Description
(Network controller only)	Cancel all calls	Deletes from the connected call stacker all waiting calls that came from my call station, so that they cannot be played or re-played. Aborts the call if it is playing at this moment.
(Network controller only)	Cancel last call	Deletes from the connected call stacker the last call that came from my call station, so that it cannot be played or re-played. Aborts the call if it is playing at this moment.
(Network controller only)	Reconnect	Disconnect and connect again to the network controller (refresh connection)

Tab. 9.5: Units/Commands

States

There exists a very large number of states, mostly with self-explanatory names, that are specific to the various unit types. A full list can be found in the Praesideo documentation and in the Praesideo configuration tool with its corresponding XML file. The states are visible to the BIS operator in the **Device overview** of the BIS client.

The most important states to monitor are the following

Data point type	States	Description
Unit	UnitConnected	The unit is connected to the network. This is the standard error-free state.
	UnitNotConnected	The unit is not connected to the network
	...	

Tab. 9.6: Units/States

9.5 Data point type BGM channel (background music)

Preparation

1. Configure a BGM channel in Praesideo
 2. Add this BGM channel to the OPC configuration using the Praesideo configuration tool
<installation drive>:\MgtS\Server\Praesideo Proxy\PraesideoProxyCfg.exe
 - Open Tab: **Device**
 - Navigate to the desired NCO
 - Right-click the NCO for a context menu, and add a datapoint of type **BGM Channel**. The name of the channel is best copied and pasted from the web interface of the NCO.
 3. In BIS (re-)browse the OPC server to make the BGM channel available in BIS
- Note:** A BIS address representing a BGM channel will have no state (always shows **Unknown**) and a detector type of **BGM channel**

Sending commands

Send commands from the BIS client by right-clicking the sub-address of the BGM channel below the `PraesideoProxy30.NCO<nnn>` (where `<nnn>` is the numerical ID of the NCO). The command parameters are

- **Routing:** a comma-separated list of names of zone groups or zones to which the BGM is to be directed.
If this parameter contains only a comma then all zones are muted.
- **Volume:** an integer representing the volume. The maximum value is 0 (audible at standard volume) and the minimum value is -96 dB (mute)

Data point type	Commands	Description
BGM channel	Set routing	Broadcasts the selected BGM channel only to the zones and zone groups in the parameter Routing (see above) Zones included in the parameter will start receiving BGM immediately and get the state Backgroundmusic . Zones not included in the parameter will stop receiving the selected BGM immediately (if they are playing it) and get the state Free .
	Add routing	Broadcasts the selected BGM channel additionally to the zones and zone groups in the parameter Routing (see above) Zones included in the parameter will start receiving BGM immediately and get the state Backgroundmusic . Zones not included in the parameter will continue in their current state, e.g. playing other than the selected BGM channel.
	Remove routing	Stops broadcasting the selected BGM channel to the zones and zone groups in the parameter Routing (see above) Zones included in the parameter will stop receiving the selected BGM immediately (if they are playing it) and get the state Free Zones not included in the parameter will continue in their current state, e.g. playing other than the selected BGM channel.
	Toggle routing	Toggles the membership of zones in the routing of a BGM channel 1) When none of the zones in the routing parameter belongs to the BGM channel, then all of them get added to it. 2) Otherwise: ...a) the zones in the routing parameter that belong to the BGM channel get removed from it (receiving the state Free); and ...b) any other zones in the routing parameter get ignored.
	Set volume	Parameter: Volume (integer) between 0 (zero) and -96 (minus 96)

Data point type	Commands	Description
	Increment volume	(no parameter) increases volume by 3 dB per invocation
	Decrement volume	(no parameter) decreases volume by 3 dB per invocation
	Increment channel volume	(no parameter) increases channel volume by 3 dB per invocation
	Decrement channel volume	(no parameter) decreases channel volume by 3 dB per invocation

Tab. 9.7: BGM channel/commands

**Notice!**

BIS does not show which BGM channel is being played in which zone

Workaround: Use the **Set routing** command to overwrite the statuses of all zones together.

9.6 Data point type Alarm

Alarms in Praesideo can come from two sources, which are OPC alarm items in BIS.:

- **Fault:** a hardware fault in the Praesideo system or alternatively a fault forwarded by external hardware. The latter is also known as a **user-injected** fault.
- **Emergency:** a Call that is broadcast with a priority greater than **223**.

An **Emergency** alarm puts the Praesideo system into **Emergency** mode: the Praesideo LED shines red, BGM is turned off and no low-priority calls can be made.

In the cases of both **Fault** and **Emergency** alarms the corresponding Alarm data point goes from **Inactive** to **Active** state, and requires manual intervention from the operator.

- If the operator gives the **Acknowledge** command, the alarm goes to the **Acknowledged** state.
- If the operator gives the **Reset** command, the alarm reverts to the **Inactive** state.

States

Alarms can be in any of three states:

Data point type	States	Description
Alarm	Active	The alarm has been triggered
	Inactive	(the default state)
	Acknowledged	The alarm was triggered and has now been acknowledged by an operator.

Tab. 9.8: Alarm/states

Sending commands

Send commands from the BIS client by right-clicking the alarm in the **Device overview** and selecting one of the following:

Data point type	Commands	Description
Alarm	Acknowledge	Confirms that the operator has noted the alarm and is initiating countermeasures.
	Reset	Turns off the alarm if its cause has been removed.
	Reset alarm extended	(Emergency only) Resets the emergency alarm. The command has a parameter AbortEvacCalls which specifies whether or not currently running evacuation priority calls must be aborted. True = abort, False = do not abort.

Tab. 9.9: Alarm/commands

9.7

Configuring the OPC server

The Praesideo OPC server needs to be configured manually to reflect those parts of the Praesideo system that are of interest to the BIS System.

- The configuration of the Praesideo system, with the names of all its components, can be read from the Praesideo system's web interface.
- Configure the OPC server using the tool: C:\MgtS\Server\Praesideo Proxy \PraesideoProxyCfg.exe which has its own documentation.

Procedure: In the Praesideo system's web interface, find the items that you wish to monitor or control from BIS. Copy and paste them into the configuration tool.



Notice!

IMPORTANT: Always keep an up-to-date backup of the Praesideo configuration file

To retain across BIS upgrades your configuration of Praesideo devices, you will need to copy this backup to the Praesideo directory after the BIS upgrade. A BIS upgrade installation does NOT do this automatically.

After installing the Praesideo software the configuration file is located by default in:

<installation drive>:\MgtS\Server\Praesideo Proxy\

10

10.1

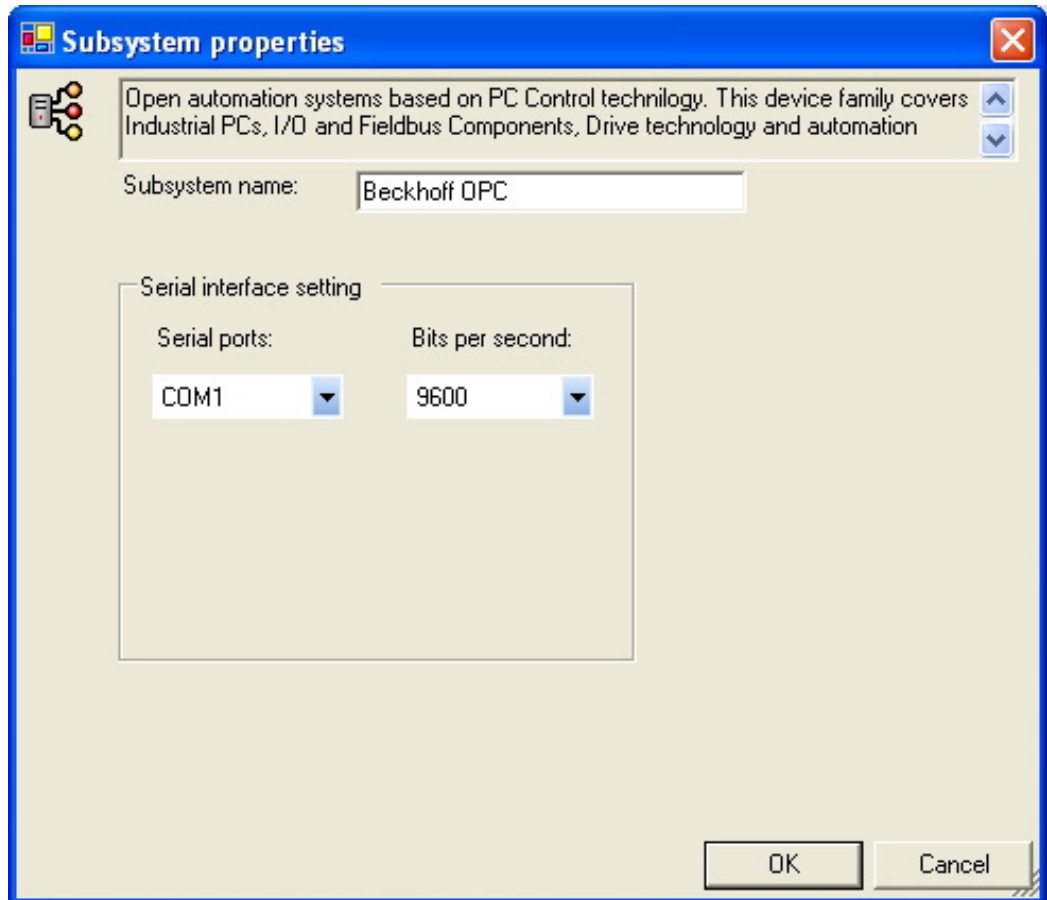
Legacy OPC servers

Configuring OPC-specific data for Beckhoff servers

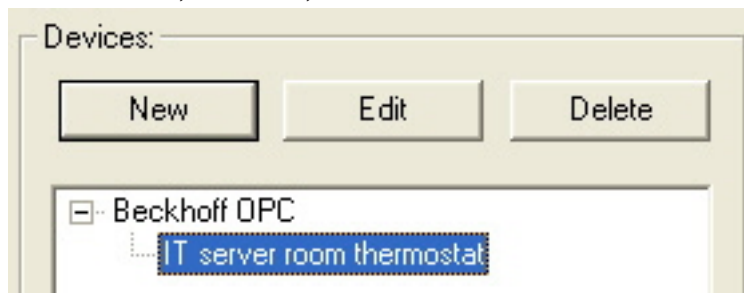
BIS provides a Beckhoff Modbus serial driver which can control one serial unit.

If, on the **Connections** Configuration Browser tab on a remote server computer, you entered **Beckhoff OPC** as the connection type, you must precisely define the data of this OPC server and assign the corresponding addresses.

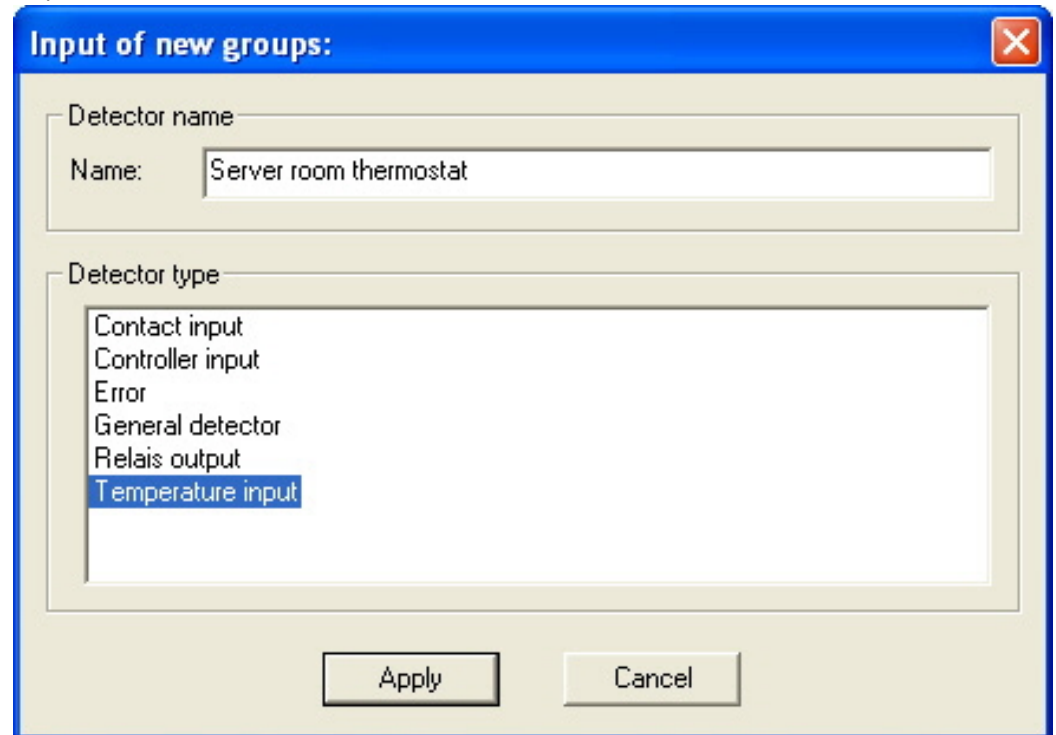
1. Define which serial port and baud rate the Beckhoff server will use, then click **OK**.



2. Under **Devices**, click **New**, then name the device.



- Under **Address**, click **New**, then name the detector and select its type. Click **Apply**. On the left side of the dialog box, create the device structure of the system and assign the required addresses.



- In the device structure, you can also create "virtual" sub-devices—devices that do not represent a separate unit in the device structure because they are part of a system. In the case of very complex connections, this can make the address structure easier to understand.
- In contrast to **virtual OPC servers**, which are created for processes, and which function without their own addresses and hardware, virtual connections are a convenient way of representing and identifying addresses which actually exist.

6. Enter all other parameters of the Beckhoff server interface accordingly (see Detector Types for Beckhoff Connections below).

☐ This address signalizes malfunction of the device

Detector

Temperature input

Brief

Mode:

Input

Ch. type:

digital

Value range: of:

0

to:

1

Logical no.
at bus:

0

Bit pos.:

1

Loc

BIS.Detectors without location

design of fieldbus component:

Calculate



Notice!
Characters not allowed in OPC server addresses
asterisk (*)
question mark (?)
The period (.) may only be used as a separator (for example, "35.2")

10.1.1

Detector types for Beckhoff connections

ContactIn Detector Type

Item	Description
ContactIn detector type	Digital input module (8x module of binary digital inputs)
Mode	Input
Channel type	Digital
Start byte	Position of contact module on the field bus (input devices), according to manufacturer's specification (1 byte, starting at "0")
End byte	Position of contact module on the field bus (input devices), according to manufacturer's specification (1 byte, starting at "0")

Item	Description
Bit position	1 through 8

ControllerIn Detector Type

Item	Description
ControllerIn detector type	Analog input module
Mode	Input
Channel type	Analog
Start byte	Position of the analog input module on the field bus (input devices), according to manufacturer's specification (1 byte)
End byte	Position of the analog input module on the field bus (input devices), according to manufacturer's specification (1 byte)
Bit position	---

TemperatureIn Detector Type

Analog input module. Values similar to **ControllerIn** detector type, but with different possible value ranges.

RelayOut Detector Type

Item	Description
RelayOut detector type	Digital output module (8x module of binary digital outputs)
Mode	Output
Channel type	Digital
Start byte	Position of relay module on the field bus (output devices), according to manufacturer's specification (1 byte, starting at "0")
End byte	Position of relay module on the field bus (output devices), according to manufacturer's specification (1 byte, starting at "0")
Bit position	1 through 8

10.1.2

Notes on data transmission:

The following conditions apply:

Analog Terminal: One analog input/output occupies 1 byte, which is one logical position (for example, an analog terminal with two inputs occupies the logical positions 0 and 1).

Digital Terminal: One digital input occupies 1 bit (for example, eight digital inputs is 1 byte, which is also one logical position).

The transmission sequence always starts with 2 x analog (that is, positions 0 and 1 are reserved for analog terminals).


Use the function **Structure of terminal bus** -> **Calculate** to read out and display the structure. The lower part of the dialog shows whether errors were detected in the configured structure.

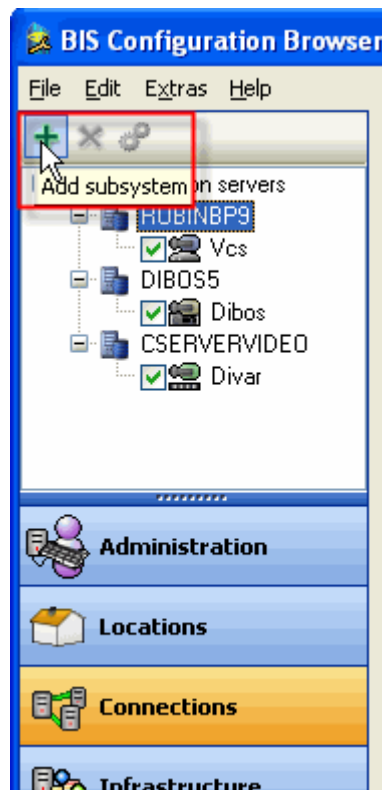
10.2

Example: Browsing an Allegiant matrix connection

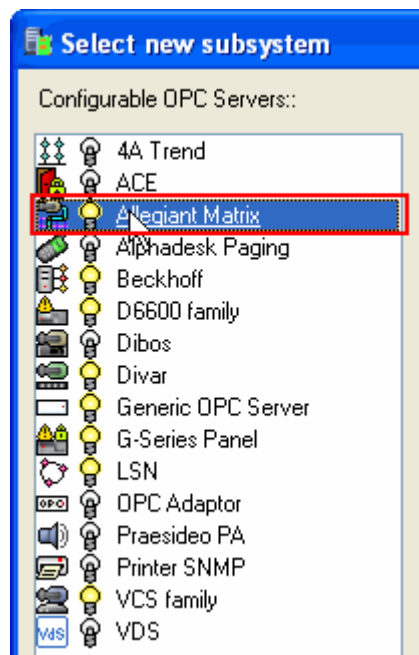
The following example shows the browsing of an Allegiant matrix connection:

Procedure

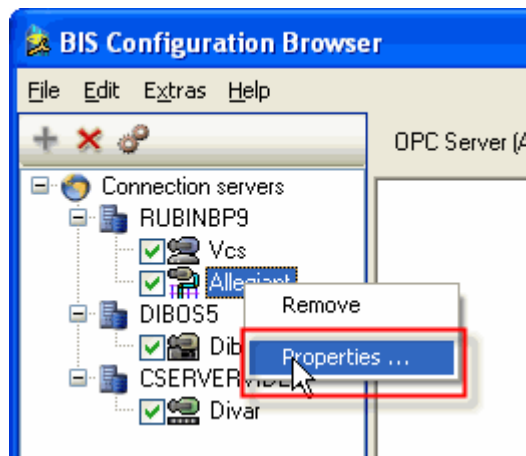
1. In the Configuration Browser select **Connections** and select the server where the video subsystem resides. Click  and select **Add subsystem**



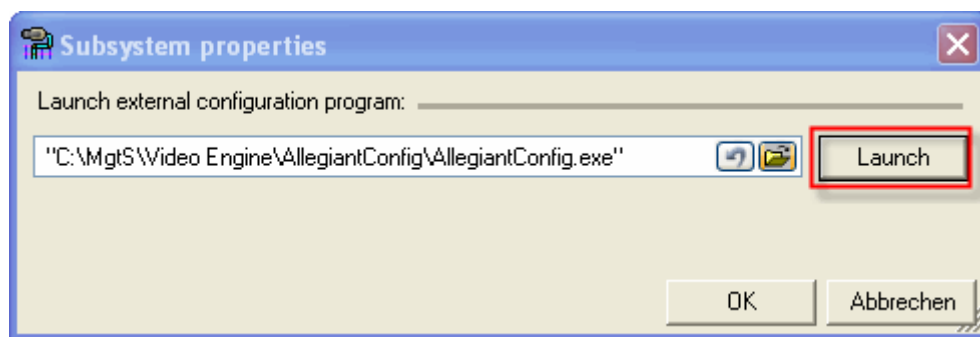
2. In the subsystem selection window, select Allegiant Matrix and confirm with **OK**.



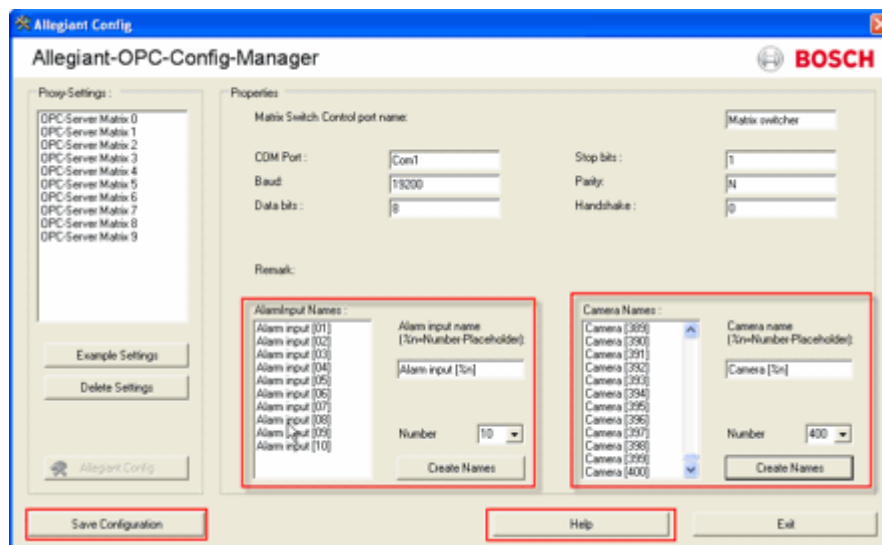
3. In the connections list, right click **Allegiant** and select **Properties**.



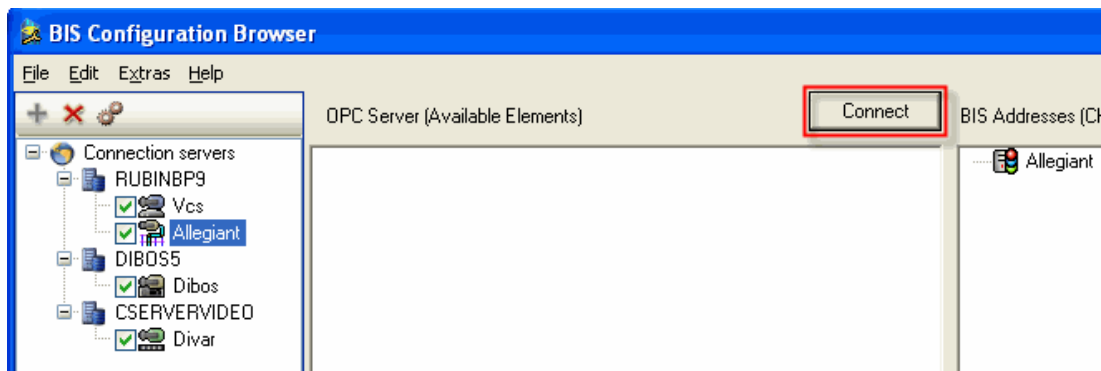
4. Launch the configuration program.



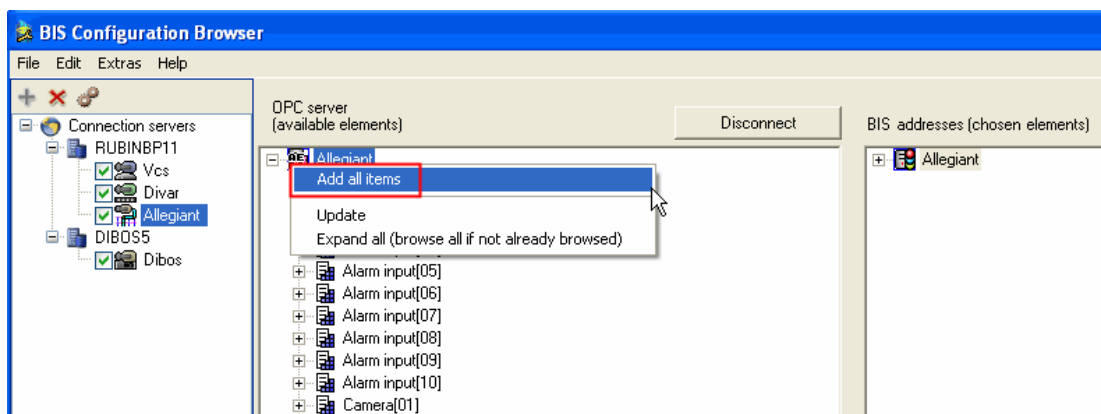
5. **Effect:** the Allegiant-OPC-Config-Manager opens



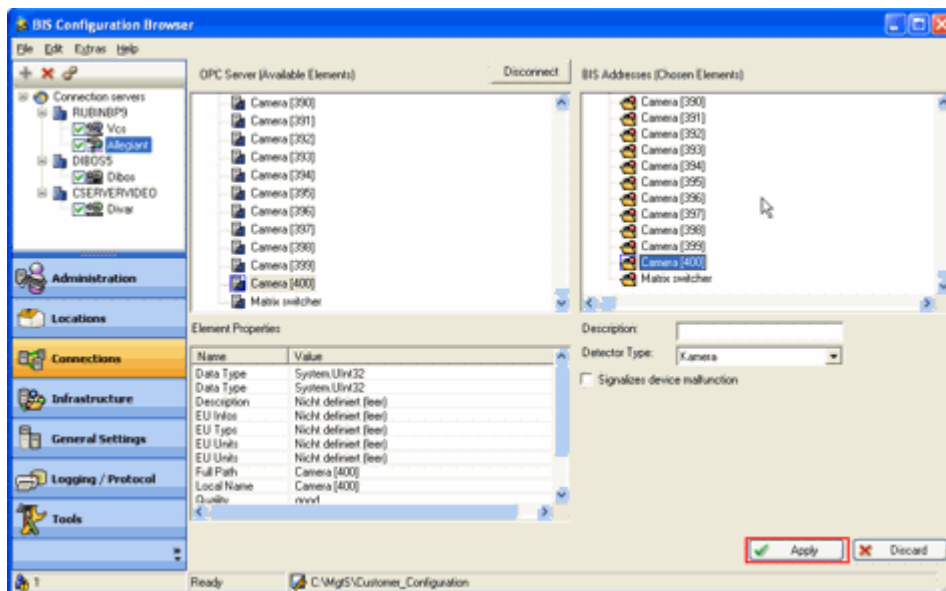
6. Click the **Connect** button to find existing OPC servers



7. Right-click **Allegiant** and select **Add all items**



8. **Effect:** All entries are listed.



9. Confirm with the **Apply** button.



10.3

BRS Software setup and configuration

This section describes how to set up the Bosch Recording Station (BRS) OPC server to work with BIS Automation Engine (AUE) and BIS Video Engine (VIE).

Prerequisite software

Procedure

1. Connect the BRS hardware dongle to the desired computer
2. Ensure that a separate data partition is available to accommodate the recordings. BRS will not write to a system partition.
3. Set up BRS software:
 - Invoke `setup.exe` from the BRS installation medium
 - When prompted for the installation type, select **BRS Software Receiver**
 - Restart the computer
4. Set up the OPC server
 - Install OPC server from the BRS installation medium `OPCVideoServer.exe`
 - Restart the computer
5. Configure BRS
 - Start BRS (**Start > Programs > BRS**)
 - Click **System > Configuration Wizard**
 - Adjust basic settings (time, time zone, IP address)
 - Assign password for user Administrator
 - Click **System > Configuration > Users**
 - Add new user `a:a` with authorization level **Normal**. BIS will connect via this user name.
 - Click **System > Configuration > Video and audio connections**
 - Click **Add** to add cameras of the supported types, e.g. JPEG or MPEG4 IP cameras
 - Click **Edit** to configure the camera settings (device type, IP address, name, channel)
 - Close configuration wizard and check whether pictures from cameras are available
6. Make video pages available for Video Engine (VIE)
 - make sure IIS is installed on the BRS computer
 - Open **Control Panel > (Performance and maintenance) > Administrative tools > IIS**
 - Right click **Default Web Site**, select **Properties**
 - On in tab **Home Directory** assign `C:\Program Files\BRS\Web\aspx` as the local path
7. Set up the connection to BIS
 - Ensure that the Windows firewall is disabled on the BRS computer.
 - Add the IP address of the BRS computer to the local host table on the BIS server, if no name server is in operation.
 - Ensure that the BRS computer is available on the network: Ping the BRS computer by its name.
 - Right-click the BIS Manager on BIS server, select **Run as** and select user **MgtS-Service**. **Note:** If the BIS Manager will not run under **MgtS-Service**, ensure that the user is not listed under the local security policy **Deny logon locally**.
 - In the BIS Configuration Browser: **Administration > Server structure > Connection server** create a connection to the computer on which the Software BRS is running.
 - Add a connection to the OPC server BRS on this connection server, connect to it and add all items.
 - In the BIS Configuration Browser select **Tools > VIE Configuration > BRS-Accounts**.
 - Configure BIS to use the user `a:a` to log into BRS.
8. Test BRS functionality in BIS
 - Log on to the BIS client
 - Open Video Engine

- Right click on any Camera in Device Overview + select "Live image"
 - Affirm if you are prompted to install Dibos8.cab. It contains necessary codecs and controls
9. Configure BRS for automatic startup
 - add BRS (Start-> Programs-> BRS) to Startup folder
 10. – Ensure that your designated default user logs on automatically. E.g on Windows XP:
 - Click **Start > Run** and type CONTROL USERPASSWORDS2. Click **OK**.
 - From the list select the account which is to log on automatically.
 - Clear the check box **Users must enter a user name and password to use this computer**, and click **OK**
 - Type the user account password and complete the process.
 11. Disable screen saver on the BRS computer

Troubleshooting:

If after changing a BRS configuration the Video Engine displays a black frame we recommend restarting the BRS computer.

Bosch Sicherheitssysteme GmbH

Robert-Bosch-Ring 5

85630 Grasbrunn

Germany

www.boschsecurity.com

© Bosch Sicherheitssysteme GmbH, 2016