INSTALLATION MANUAL

DiBos

BOSCH

610–4.998.137.176
Version: A5
Date: 11–2004

Safety instructions

Important Safeguards

1. **Read, Follow, and Retain Instructions** – All safety and operating instructions should be read and followed before operating the unit. Retain instructions for future reference.
2. **Heed Warnings** – Adhere to all warnings on the unit and in the operating instructions.
3. **Attachments** – Attachments not recommended by the product manufacturer should not be used, as they may cause hazards.
4. **Installation Cautions** – Do not place this unit on an unstable stand, tripod, bracket, or mount. The unit may fall, causing serious injury to a person and serious damage to the unit. Use only manufacturer–recommended accessories, or those sold with the product. Mount the unit per the manufacturer's instructions. Appliance and cart combination should be moved with care. Quick stops, excessive force, or uneven surfaces may cause the appliance and cart combination to overturn.
5. **Cleaning** – Unplug the unit from the outlet before cleaning. Follow any instructions provided with the unit. Generally, using a damp cloth for cleaning is sufficient. Do not use liquid cleaners or aerosol cleaners.
6. **Servicing** – Do not attempt to service this unit yourself. Opening or removing covers may expose you to dangerous voltage or other hazards. Refer all servicing to qualified service personnel.
7. **Damage Requiring Service** – Unplug the unit from the main AC power source and refer servicing to qualified service personnel under the following conditions:
   - When the power supply cord or plug is damaged.
   - If liquid has been spilled or an object has fallen into the unit.
   - If the unit has been exposed to water and/or inclement weather (rain, snow, etc.).
   - If the unit does not operate normally, when following the operating instructions. Adjust only those controls specified in the operating instructions. Improper adjustment of other controls may result in damage, and require extensive work by a qualified technician to restore the unit to normal operation.
   - If the unit has been dropped or the cabinet damaged.
   - If the unit exhibits a distinct change in performance, this indicates that service is needed.
8. **Replacement Parts** – When replacement parts are required, the service technician should use replacement parts specified by the manufacturer, or that have the same characteristics as the original part. Unauthorized substitutions may result in fire, electrical shock, or other hazards.
9. **Safety Check** – Upon completion of servicing or repairs to the unit, ask the service technician to perform safety checks to ensure proper operating condition
10. **Power Sources** – Operate the unit only from the type of power source indicated on the label. If unsure of the type of power supply to use, contact your dealer or local power company.
    - For units intended to operate from battery power, refer to the operating instructions.
    - For units intended to operate with External Power Supplies, use only the recommended approved power supplies.
    - For units intended to operate with a limited power source, this power source must comply with EN60950. Substitutions may damage the unit or cause fire or shock.
    - For units intended to operate at 24 VAC, normal input voltage is 24 VAC. Voltage applied to the unit's power input should not exceed 30 VAC. User–supplied wiring, from the 24 VAC supply to unit, must be in compliance with electrical codes (Class 2 power levels). Do not ground the 24 VAC supply at the terminals or at the unit's power supply terminals.
11. **Coax Grounding** – If an outside cable system is connected to the unit, ensure that the cable system is grounded. U.S.A. models only—Section 810 of the National Electrical Code, ANSI/NFPA No.70, provides information regarding proper grounding of the mount and supporting structure, grounding of the coax to a discharge unit, size of grounding conductors, location of discharge unit, connection to grounding electrodes, and requirements for the grounding electrode.

Safety instructions (continued)

12. **Grounding or Polarization** – This unit may be equipped with a polarized alternating current line plug (a plug with one blade wider than the other). This safety feature allows the plug to fit into the power outlet in only one way. If unable to insert the plug fully into the outlet, try reversing the plug. If the plug still fails to fit, contact an electrician to arrange replacement of the obsolete outlet. Do not defeat the safety purpose of the polarized plug.
    Alternately, this unit may be equipped with a 3–wire grounding plug (a plug with a third pin, for grounding). This safety feature allows the plug to fit into a grounding power outlet only. If unable to insert the plug into the outlet, contact an electrician to arrange replacement of the obsolete outlet. Do not defeat the safety purpose of the grounding plug.
13. **Lightning** – For added protection during a lightning storm, or when this unit is left unattended and unused for long periods of time, unplug the unit from the wall outlet and disconnect the cable system. This will prevent damage to the unit due to lightning and power line surges.
14. **Restricted Access Locations** are required for the installation.

FCC & ICES Information

(U.S.A. and Canadian Models Only)

This device complies with part 15 of the FCC Rules. Operation issubject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules and ICES–003 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer, or an experienced radio/TV technician for help.

Intentional or unintentional changes or modifications, not expressly approved by the party responsible for compliance, shall not be made. Any such changes or modifications could void the user's authority to operate the equipment.

The user may find the following booklet, prepared by the Federal Communications Commission, helpful: How to Identify and Resolve Radio–TV Interference Problems. This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004–000–00345–4.

Safety instructions (continued)

For Indoor Product

1. **Water and Moisture** – Do not use this unit near water – for example, in a wet basement, in an unprotected outdoor installation, or in any area classified as a wet location.
2. **Object and Liquid Entry** – Never push objects of any kind into this unit through openings, as they may touch dangerous voltage points or short out parts that could result in a fire or electrical shock. Never spill liquid of any kind on the unit.
3. **Power Cord and Power Cord Protection** – For units intended to operate with **230VAC**, **50Hz**, the input and output power cord must comply with the latest versions of IEC Publication 227 or IEC Publication 245.
   Power supply cords should be routed so they are not likely to be walked on or pinched. Pay particular attention to location of cords and plugs, convenience receptacles, and the point of exit from the appliance.
4. **Overloading** – Do not overload outlets and extension cords; this can result in a risk of fire or electrical shock.

For Rack–Mount Product

1. **Ventilation** – This unit should not be placed in a built–in installation or rack, unless proper ventilation is provided, or the manufacturer’s instructions have been adhered to. The equipment must not exceed its maximum operating temperature requirements.
2. **Mechanical Loading** – Mounting of the equipment in a rack shall be such that a hazardous condition is not achieved due to uneven mechanical loading.

ATTENTION
OBSERVE PRECAUTIONS
FOR HANDLING
ELECTROSTATIC
SENSITIVE DEVICES

WARNING: Electrostatic–sensitive device. Use proper CMOS/MOSFET handling precautions to avoid electrostatic discharge.

NOTE: Grounded wrist straps must be worn and proper ESD safety precautions observed when handling the electrostatic–sensitive printed circuit boards.

CAUTION: Lithium Battery

Danger of explosion if battery is incorrect replaced. Replace only with the same or equivalent type recommended by the manufacturer.
Dispose of used batteries according to the battery manufacturer’s instructions.

Cover Removal

WARNING: Removal of the cover should only be performed by qualified service personnel – not user serviceable. The unit should always be unplugged before removing the cover and remain unplugged while the is removed.

Safety instructions (continued)

Safety Precautions

<table>
<tr><td>⚡</td><td><b>CAUTION
RISK OF ELECTRIC SHOCK.
DO NOT OPEN!</b></td><td>⚠</td></tr>
<tr><td colspan="3"><b>CAUTION: TO REDUCE THE RISK OF ELECTRIC SHOCK, DO NOT REMOVE COVER (OR BACK). NO USER SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.</b></td></tr>
</table>

⚡ This symbol indicates the presence of uninsulated ”dangerous voltage” within the product’s enclosure. This may constitute a risk of electric shock.

⚠ The user should consult the operating an maintenance (servicing) instructions in the literature accompanying the appliance.

⚠ **Attention:** Installation should be performed by qualified service personnel only in accordance with the National Electrical Code or applicable local codes.

⚡ **Power Disconnect.** Units with or without ON–OFF switches have power supplied to the unit whenever the power cord is inserted into the power source; however, the unit is operational only when the ON–OFF switch is in the ON position. The power cord is the main power disconnect for all units.

TABLE OF CONTENTS

Section Page

Table of Contents (continued)

Section Page

1 Introduction

1.1 System Description

The video system is a digital monitoring system with which video images can be saved on location in order to transmit and evaluate them anyplace you designate regardless of distance and location.
The image data delivered by the video system also permits statements about the size of the danger and developments before and after the event.

1.2 Uninterruptible Power Supply

As an electronic device, the video system reacts sensitively to suddenly–occurring voltage spikes, voltage drops, and voltage failure.
To avoid damage to the electronic components, to avoid data loss, and to ensure proper operation, the installation of an uninterruptible power supply UPS is recommended.

Depending on the stability of the mains, the following UPS types are recommended:

- Mains with voltage spikes and voltage failure:
  the use of an offline UPS is sufficient.
- Mains with voltage spikes, voltage failure, and **voltage drops**:
  the use of an online UPS is recommended.

For 1 DiBos, a UPS with at least 300 VA is required. If additional devices (e.g. monitors, subsystems) are also protected, the performance of the UPS must be increased accordingly.

1.3 Recommended Virus Scanners/Firewalls

Windows® XP embedded is the operating system of the video system. The use of a virus scanner and a firewall is recommended.

Virus Scanners
The following virus scanners are approved for the video system. They are organized according to their capability.

1. Trend Micro PC–cillin Internet Security 5.1
2. Norton AntiVirus 2004
3. McAfee VirusScan 8.0

Note:

- Always use the most current virus update.
- The real–time virus scanner must be activated. Only thus can sufficient protection against viruses be achieved. This has no effect on the system's performance.
- All partitions on the hard disk that contain saved images must be excluded from the scanning procedure.
- Scanning of the C drive, with the exception of the partitions that contain the images, should occur time–controlled. During the scanning of the C drive, the system's performance is reduced noticeably and thus the image repeat and image storage rates.
  The loss of individual images cannot be ruled out.

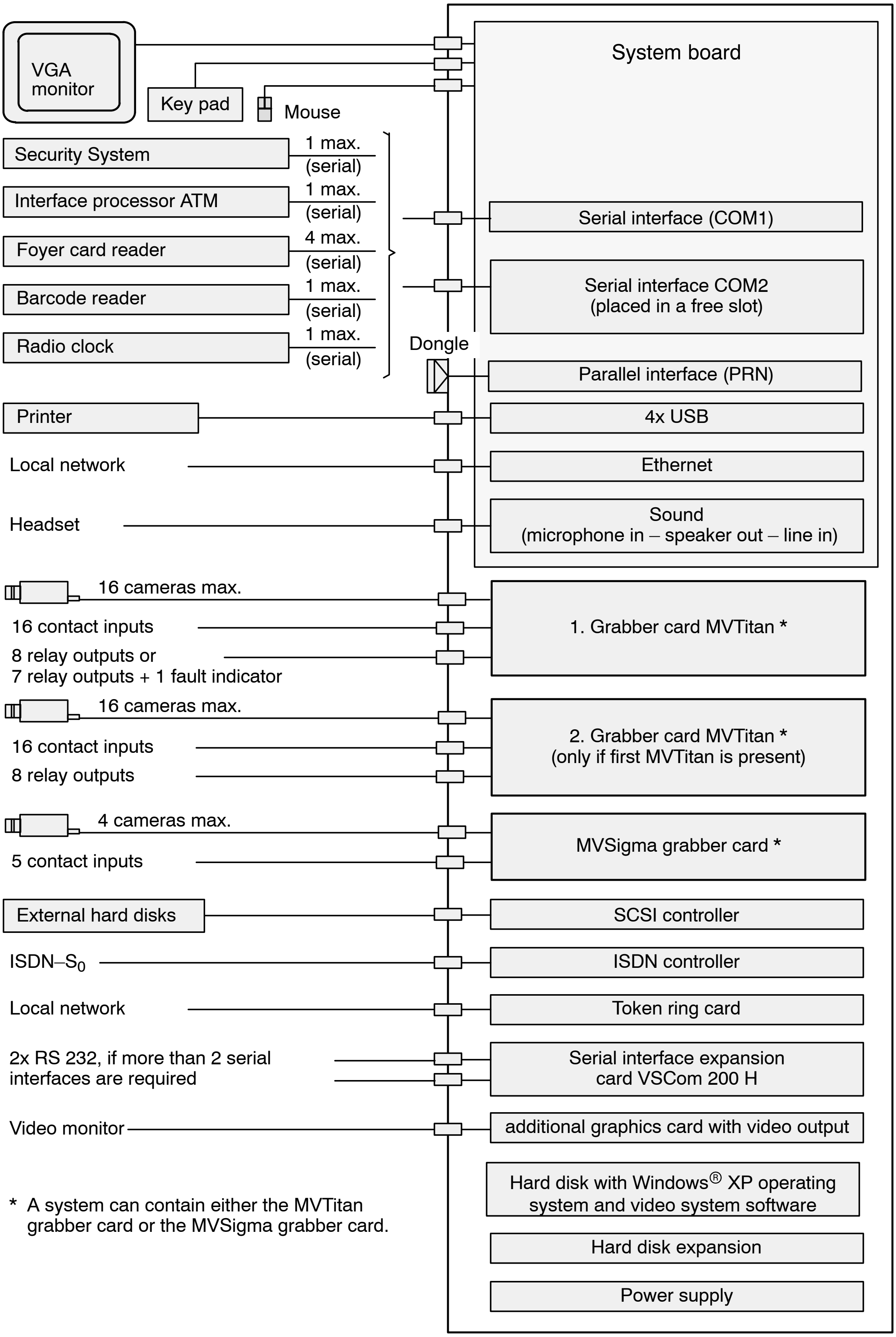
Firewall
The firewall integrated into Windows® XP embedded is not activated by default. It can be activated if necessary.
With the virus scanners listed above, only Trend Micro PC–cillin Internet Security includes an integrated firewall. With Norton AntiVirus 2004 and McAfee VirusScan 8.0, you must purchase the firewall separately.
The following open ports are required:

- Port 80: only for Web servers
- Port 1147: only for network connection DiBos–DiBos
- Port 1148: only for network connection DiBos–DiBos and encrypted data transmission

Note:
always use the most current version of the firewall.

Introduction (continued)

1.4 Component Overview



* A system can contain either the MVTitan grabber card or the MVSigma grabber card.

Introduction (continued)

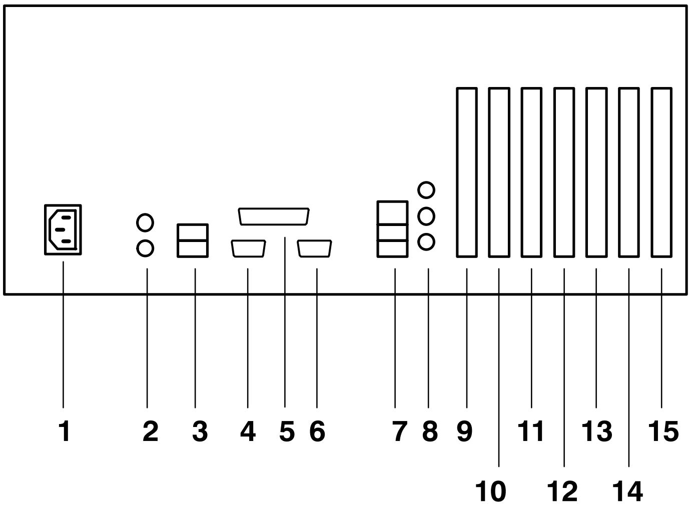
1.5 Laws/Norms/Guidelines

Electromagnetic compatibility (EMC)	USA	FCC Part 15, Class B
	EU	EMC directive 89/336/EWG
	– Fault broadcast	EN 61000–6–3
	– Interference immunity	DIN EN 50130–4 To fulfill DIN EN 50130–4, DiBos must be operated with a UPS.
Electrical security	USA	UL listed (E183863–A1–UL–2)
	EU	EN 60950–1
Climate check	Germany	VdS guideline 2110
Monetary institutions (Banks)	Germany	Accident prevention “cash register” regulations (BGV C9) Note during the installation/configuration of the system according to accident prevention “cash register” regulations the SP9.7/5 ”Installation Notes for Optical Room Monitoring Systems” (ORÜA).
Guarantee		
Duration	3 years	

2 Computer Slots

Installation of the internal hardware components of the computer may only be performed by the video system manufacturer. Any field configuration changes to the internal hardware will void the system warranty.

Rear view:



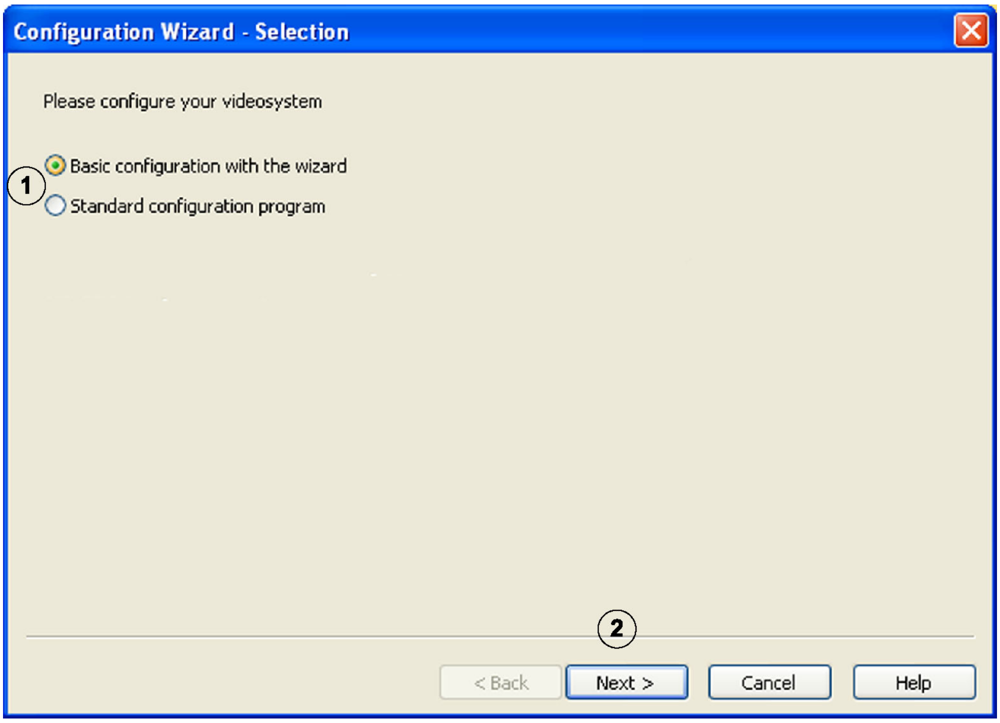
1	=	Power supply
2	=	Keyboard – mouse
3	=	2x USB 2.0
4	=	Serial interface COM1 (COM2 in another empty slot)
5	=	Parallel interface (PRN)
6	=	Monitor
7	=	USB 2.0 – USB 2.0 – Ethernet (RJ45)
8	=	Microphone in (mono) – speaker out – line in
9	=	Additional graphics card with TV output
10	=	1. MVTitan or MVSigma grabber card
11	=	2. MVTitan grabber card (only if first grabber card is present)
12	=	SCSI controller
13	=	ISDN card or modem 56 k
14	=	Token ring network card
15	=	Interface expansion card VSCom 200 H or watchdog V–DOG

Note:
if necessary, the interface card VSCom 200 H should be placed in a free slot.

3 Quick installation

For information about the device connections, please see Chapter 2.

1. Connect the mouse and keyboard (put ferrite on the cables).
2. Plug the 26–pin D–sub plug of the grabber cable on the corresponding plug of the grabber card.
3. Connect the cameras to the grabber cable. On each cable there is a plastic ring with a printed number. This number stands for the video input, e.g. “1” for video input 1.
4. Connect the contact inputs (alarm inputs) and relay outputs to the grabber cable.
5. Switch all connected devices on.
6. Plug the network cable into the video system.
7. Switch the video system on. The switch is on the back side. The system will then boot up automatically and stop at the setup assistant.
8. If you do not yet have experience with the system, select the “Create basic configuration with help of the assistant” option. With a few clicks of the mouse, you will have a basic configuration. The system automatically recognizes the connected video hardware (cameras, grabber).
   Note: after the basic configuration, expansions must be executed in the standard (expert) configuration (see Chapter 6.2).



Configuration Wizard - Selection

Please configure your videosystem

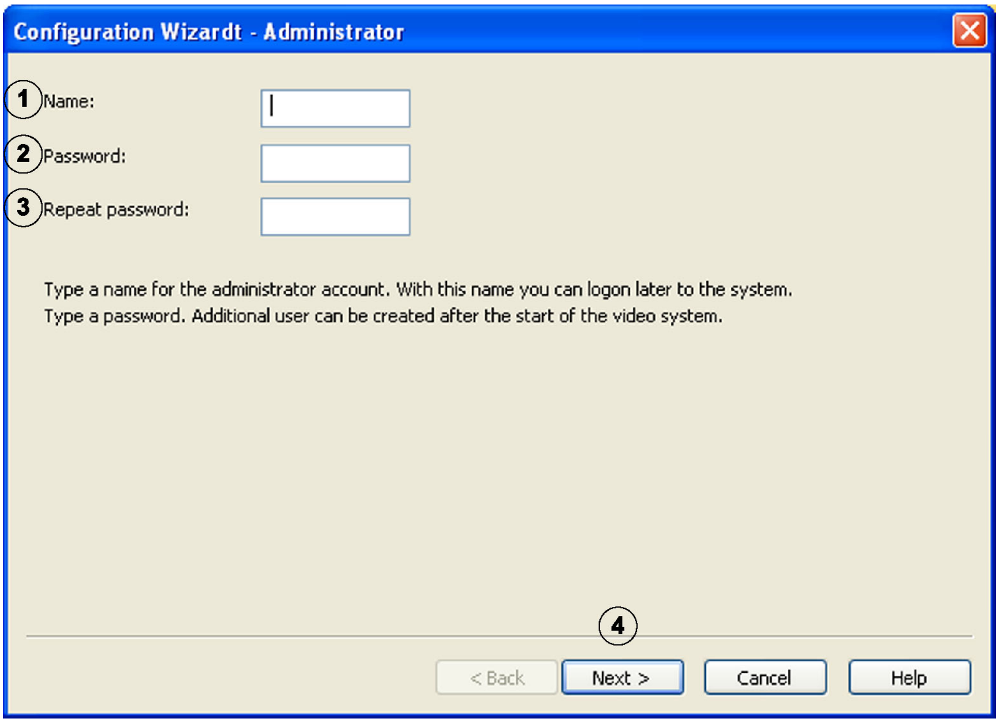
● Basic configuration with the wizard
○ Standard configuration program

Carry out your selection as follows:

No.	Name	Description
1	Basic configuration with the wizard	**Select this function to start the Assistant.**
	Standard configuration program	With this function, you start Expert Configuration (see Chapter 6.2).
2	Next	Click on **Next** to continue.

Quick installation (continued)

Logon as administrator



Type a name for the administrator account. With this name you can logon later to the system.
Type a password. Additional user can be created after the start of the video system.

No.	Name	Description
1	Name	Enter the name here. You have to logon in the video system with this name in the future to operate the system. The user given here receives administrator rights, i.e. rights with which she/he can perform all system functions. However, the name can be changed later. Please take note of the following information for instructions on how to do this:
2	Password	Enter the password here. Entering a password is optional. This is recommended, however, to prevent unauthorized access by others.
3	Repeat password	Enter the password again for security purposes.
4	Next	Click on **Next** to continue.

Note: You will enter Expert Configuration as follows after successfully concluding Basic Configuration.

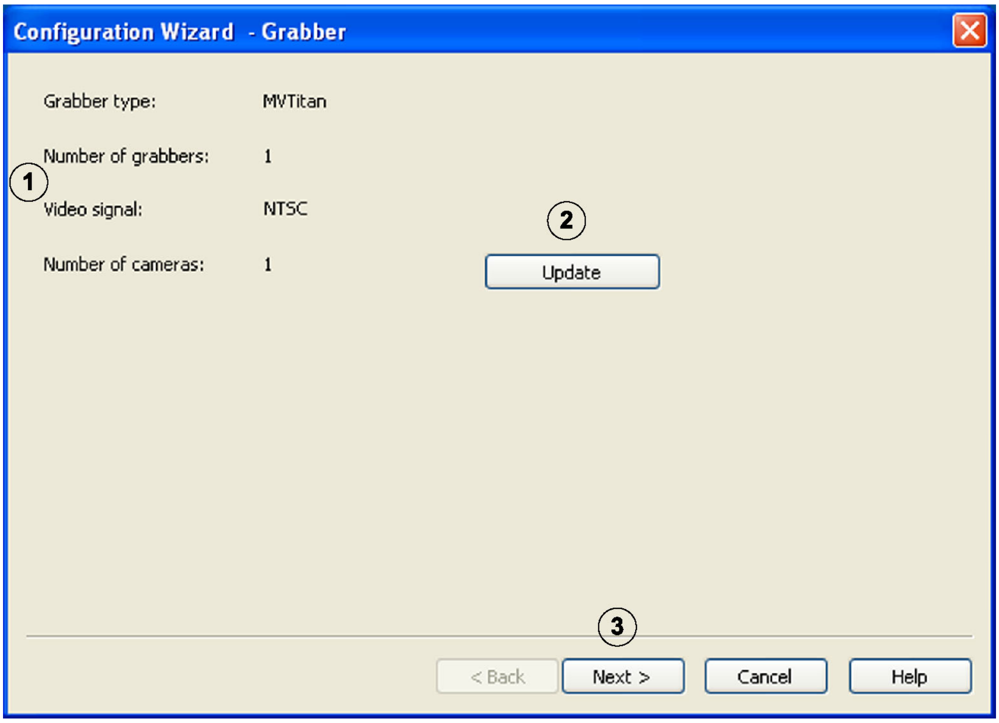
– Start the system. This will take you to the live image.

– In Live Image, select the **System/Configuration** menu. This will then take you to Expert Configuration.

– Select the **User management/user** menu in the configuration. The name and password can be changed here. You can also specify additional users here.

Quick installation (continued)

Display of the existing hardware



Configuration Wizard - Grabber

Grabber type: MVTitan

Number of grabbers: 1

Video signal: NTSC

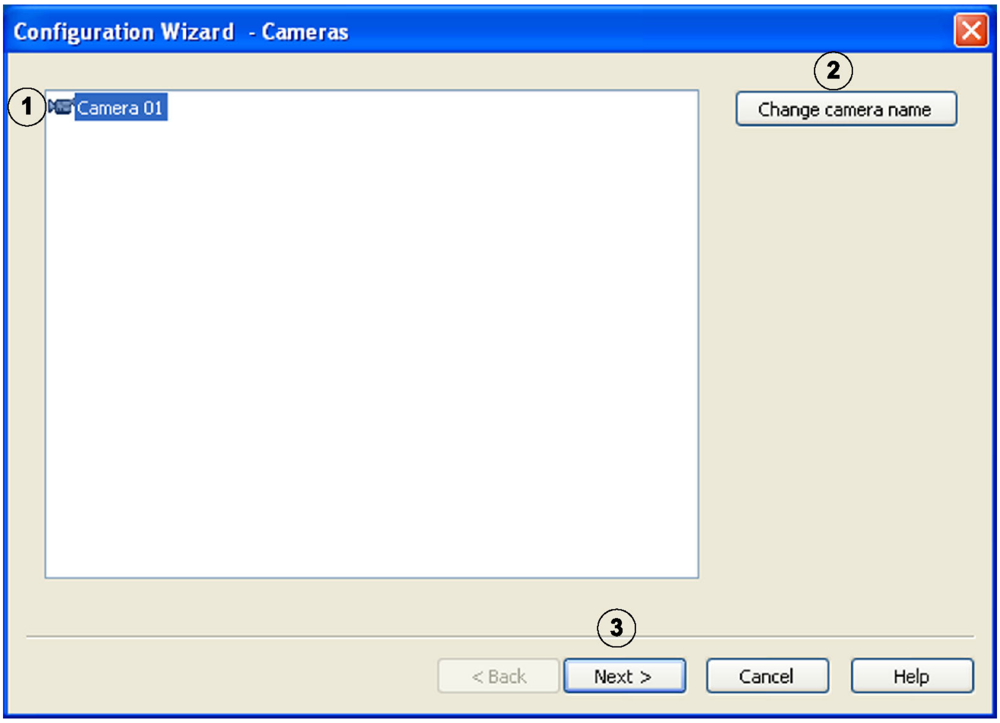
Number of cameras: 1

The existing video hardware is displayed in this dialog box.

No.	Name	Description
1	Grabber type: Number of grabbers: Video signal: Number of cameras:	The built–in grabber type is displayed. Either MVTitan or MVSigma. The number of built–in grabbers is displayed. The video norm used by the connected cameras is displayed automatically. The number of connected cameras is displayed.
2	Update	If a camera is put into operation after Basic Configuration has been started, this can be included by clicking on **Update**.
3	Next	Click on **Next** to continue.

Quick installation (continued)

Changing the camera name

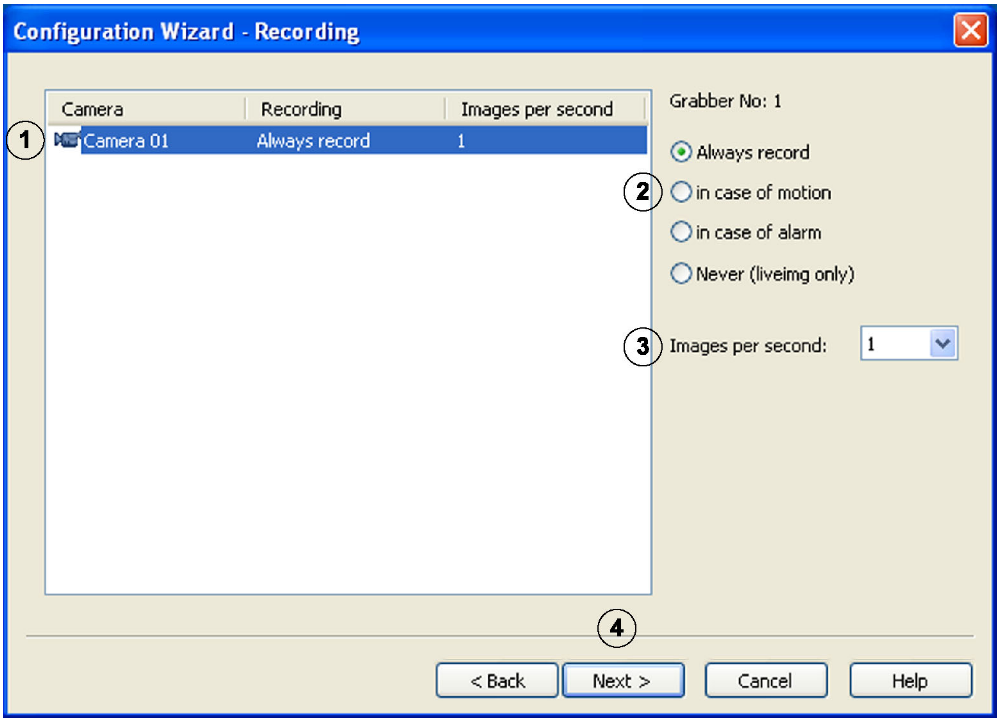


You can change the camera name in this dialog box.

No.	Name	Description
1		Click on the camera whose name you wish to change. The selection is displayed in color.
2	Change camera name	Click on **Change camera name**. You can now change the name of the selected camera.
3	Next	Click on **Next** to continue.

Quick installation (continued)

Select storage method


Configuration Wizard - Recording

Camera	Recording	Images per second
Camera 01	Always record	1

Grabber No: 1

- ◉ Always record
- ○ in case of motion
- ○ in case of alarm
- ○ Never (liveimg only)

Images per second: 1

You can determine the following for each camera in this dialog box:

- if a recording (storage of images) should take place and
- how many images per camera should be displayed.

The system automatically determines the type of recording for each camera. The system will thus create a storage job with the following settings:

- Recording: Always record
- Images per second: 1

You can change this standard setting as follows:

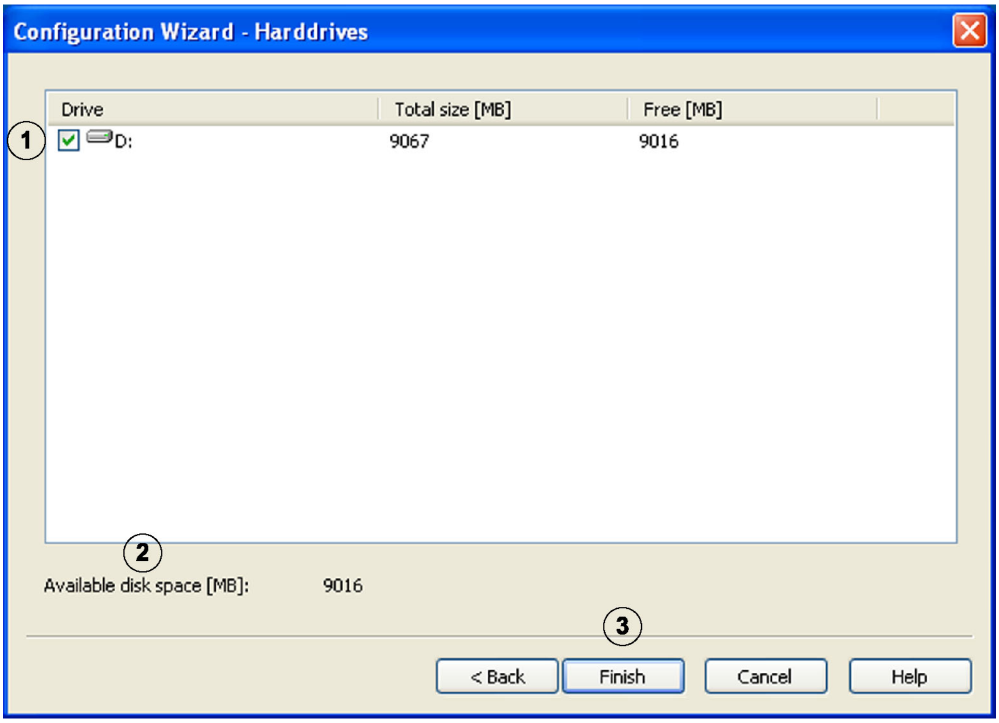
No.	Name	Description
1		Click on the camera whose setting you wish to change. The selection is displayed in color.
2	Grabber no.: x	Select when a recording should occur for each camera.
	Always record	The camera always records.
	In case of motion	The camera starts recording as soon as a movement occurs. The area of the camera image to be monitored can be drawn in Expert Configuration (menu **Hardware**/**Framegrabber**/**Cameras**, **Setup** buttons).
	In case of alarm	The camera records as soon as the corresponding alarm input of the frame grabber triggers (e.g. Camera 1 corresponds to Detector 1).
	Never (liveimg only)	No recording occurs. Only a camera live image is displayed.

Quick installation (continued)

3	Images per second	Enter the number of images per second that are to be recorded in the **Images per second** box. **Note:** The system checks the plausibility of the configured recording rate here.
4	Next	Click on **Next** to continue. **Note:** If a second MVTitan grabber is available, the dialog box for the second grabber will be displayed again after confirming with **Next** . Change the standard settings here as well if necessary.

Quick installation (continued)

Select the drive for storage and finish Basic Configuration.



Drive	Total size [MB]	Free [MB]
☑ D:	9067	9016

Available disk space [MB]: 9016

In this dialog box, select the drive for storage of the image data.

No.	Name	Description
1	 ☑ D:\ □ D:\	The List field contains all hard drives and network drives known to the system at the start of Basic Configuration. Both the total size and free storage capacity in MByte is shown. The drive is activated. The drive is not activated.
2	Available disk space (MB):	The total size of the memory capacity for the activated drives is displayed in Mbytes.
3	Finish	Click on **Finish** to accept the entries and finish Basic Configuration. The video system is subsequently started. Log on with your user name and password and make further modifications in Expert Configuration if necessary. **Note:** At least 1 drive must be selected so that the configuration can be finished.

Quick installation (continued)

Note:
When finishing Basic Configuration, the system proceeds according to the following convention:

- A ring archive is created for each camera (this can be overwritten).
- The size of the archives is generated according to the formula “available disk space: total number of cameras”. All selected system partitions are used for the available memory capacity, with the exception of system partition (C:).
- A storage job with x number of images per second is created for each camera.
- If the trigger is the result of movement, the entire contents of the image are evaluated as an area to be monitored.

4 Connections

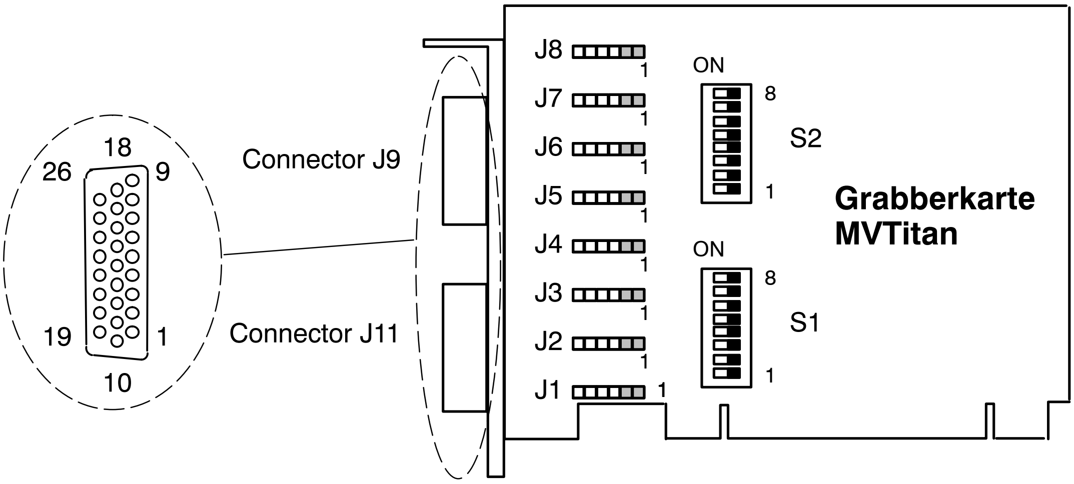
This section describes the following connections/installation:

- Grabber card MVTitan/MVSigma
- Ethernet/token ring
- ISDN controller
- Interface expansion card VSCom 200 H
- SCSI controller
- Monitor, keyboard, mouse
- External hard disks
- B&W, CCVS and Y/C cameras
- V–DOG and tamper contact
- Software dongle and printer
- Fault indicator
- Automatic teller machine
- Bar code reader
- Programming the foyer card reader MINITER RS 485
- Radio clock DCF 77
- Web Connection for Access Via Browser
- Modem
- Security systems:
  - NZ 500/BZ 500
  - BZ 500
  - AZ 1010/NZ 1008
  - NZ 1012/BZ 1012
  - BZ 1012
  - NZ 1060
  - BZ 1060
  - UEZ 1000
  - UEZ 2000
  - UGM 2020
  - Bosch D9000

Connections (continued)

4.1 Grabber Card MVTitan (max. 2)

May only be executed by authorized trained personnel!



Pin Assignment connector J9/J11

	Connector J11		Connector J9		J11/J9	
Pin	Assignment	Setting	Assignment	Setting	Color	BNC
1	+12 V	–	+12 V	–	w	–
2	Video input 1	S1–1	Video input 9	S2–1	–	V1
3	Video input 2	S1–2	Video input 10	S2–2	–	V2
4	Video input 3	S1–3	Video input 11	S2–3	–	V3
5	Video input 4	S1–4	Video input 12	S2–4	–	V4
6	Alarm input 1	–	Alarm input 9	–	br	–
7	Alarm input 2	–	Alarm input 10	–	gn	–
8	Relay 3a	J3	Relay 7a	J7	yw	–
9	Relay 4a	J4	Relay 8a	J8	gr	–
10	GND	–	GND	–	pk	–
11	Alarm input 5	–	Alarm input 13	–	blu	–
12	Alarm input 6	–	Alarm input 14	–	rd	–
13	Alarm input 7	–	Alarm input 15	–	bk	–
14	Alarm input 8	–	Alarm input 16	–	vio	–
15	Relay 1b	–	Relay 5b	–	gr/pk	–
16	Relay 2b	–	Relay 6b	–	rd/blu	–
17	Relay 3b	–	Relay 7b	–	w/gn	–
18	Relay 4b	–	Relay 8b	–	br/gn	–
19	Alarm input 3	–	Alarm input 11	–	w/yw	–
20	Alarm input 4	–	Alarm input 12	–	yw/br	–
21	Video input 5	S1–5	Video input 13	S2–5	–	V5
22	Video input 6	S1–6	Video input 14	S2–6	–	V6
23	Video input 7	S1–7	Video input 15	S2–7	–	V7
24	Video input 8	S1–8	Video input 16	S2–8	–	V8
25	Relay 1a	J1	Relay 5a	J5	w/gr	–
26	Relay 2a	J2	Relay 6a	J6	gr/bn	–

Connections (continued)

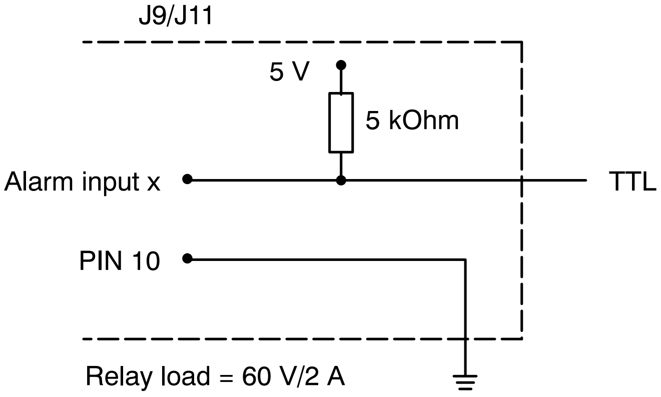
Relay output

J1 to J8	
Position 1 –2	Relay contact N/O contact
Position 2 –3	Relay contact N/C contact
Position 4 –5	Common
Position 5 – 6	not occupied

Video input termination

S1, S2	
off	Input not terminated
on	Terminated with 75 Ohm (delivery state)

Alarm input connection:



Note:

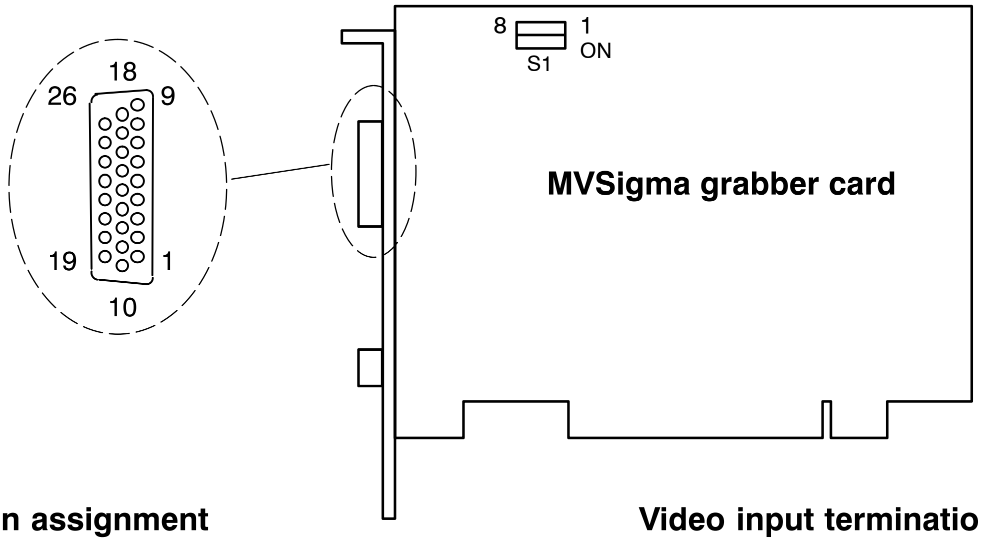
Video input 1 – 16

- 1 input per B&W and CCVS camera
- 2 inputs per Y/C camera

Connections (continued)

4.2 Grabber Card MVSigma

May only be executed by authorized trained personnel!



Pin assignment

Pin	26–pin connector Assignment	Color	BNC
1	+12 V DC	w	–
2	Video input 1	–	V1
3	Video input 2	–	V2
4	Video input 3	–	V3
5	Video input 4	–	V4
6	Used	–	–
7	Used	–	–
8	Alarm input 1	yw	–
9	Alarm input 2	gr	–
10	Used	–	–
11	Alarm input 3	blu	–
12	Used	–	–
13	Used	–	–
14	Used	–	–
15	Used	–	–
16	Alarm input 4	rd/blu	–
17	Earth alarm inputs	w/gn	–
18	Alarm input 5	br/gn	–
19	Not used	–	–
20	Not used	–	–
21	Not used	–	–
22	Not used	–	–
23	Not used	–	–
24	Not used	–	–
25	Not used	–	–
26	Not used	–	–

Video input termination

S1–1, S1–2, S1–3, S1–4	
off	Input not terminated
on	Terminated with 75 Ohm (delivery state)

4.3 Connection to a Token Ring or Ethernet Network

May only be executed by authorized trained personnel!

In addition to the Ethernet connection on–board, there is an optional token ring card available.

Note:
Only the card type Madge Token Ring Smart 16/4 PCI Ring Node may be used.

Installation and configuration of the token ring card

1. Switch off the computer and disconnect the network plug.
2. Install the network card in the appropriate computer slot (see Section 2).
3. Switch the computer on. The network card will be recognized and installed automatically by the system.

Integration into a customer network with dynamic assignment of IP addresses (for Ethernet and token ring)

In the delivery state, DHCP is activated. If, however, you have switched over to a fixed IP address and you would like to return to a dynamic distribution of the IP addresses (DHCP), then activate DHCP as follows.

1. Log on as the Administrator.
2. Adapt the TCP/IP address as follows:
   - Select ”Start → Control Panel→ Network Connections.”
   - Double–click on ”Local Area Connection → General”.
   - On the following dialog box, select the ”Internet Protocol (TCP/IP)” option and click the ”Properties” button.
   - Activate the ”Obtain IP address automatically“ option button and confirm by clicking ”OK”.
3. Adapt the computer names as follows:
   Select ”Start → Control Panel → Performance and Maintenance→ System→ Computer Name→ Change” and make the following entries for
   ”Computer name: <Computer name><Computer number>”
   ”Workgroup: <Computer name>_NETWORK”
4. Confirm your entries by clicking ”OK”.
5. Restart the computer.

Connections (continued)

Integration into a customer network with static assignment of IP addresses (for Ethernet and token ring)

Ask the system administrator for the IP and subnet address and proceed as follows:

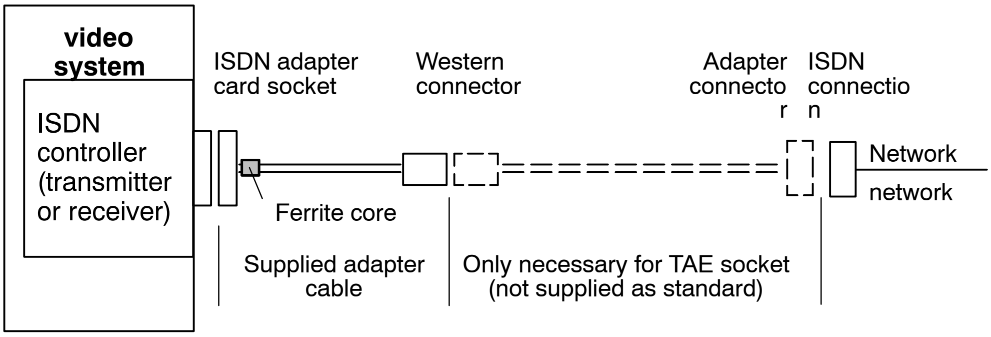
1. Log on as the Administrator.
2. Adapt the TCP/IP address as follows:
   - Select ”Start → Control Panel→ Network and Internet Connections”.
   - Double–click on ”Local Area Connection”.
   - On the following dialog box, select the ”Internet Protocol (TCP/IP)” option and click the ”Properties” button.
   - Activate the ”Use the following IP addresses“ option button and enter the IP and subnet mask:
     ”IP address: x . y . z . computer number”
     x: like other computers
     y: like other computers
     z: last two digits of the dongle number
     Computer number: consecutive number of the computer
     ”SubNet address: e.g. 255 . 255 . 0 . 0” (remains the same)
     Confirm by clicking ”OK”.
3. Adapt the computer name as follows:
   Select ”Start → Control Panel →Performance and Maintenance→ System→ Computer Name→ Change” and make the following entries for
   ”Computer name: <Computer name><Computer number>”
   ”Workgroup: <Computer name>_NETWORK”
4. Confirm your entries by clicking ”OK”.
5. Restart the computer.

4.4 Connecting the ISDN Controller

May only be executed by authorized trained personnel!

The ISDN connection is established via a supplied adapter cable (with Western connector) to the S_o interface of the computer.

Note:
Only use the card type Fritz! Card PCI V2.0.



For installation of the ISDN card the computer must have an ISDN connection and the card must be installed in the computer. Use the drivers provided.

For data transfer the connection must support the EURO ISDN (DSS1) protocol. For S_o connections in PABXs this must be enabled first in the PABX. Also, the data service must be enabled in incoming and outgoing direction. The video system is configured for EURO ISDN as standard when supplied. For further details, see section 7.4.

ISDN socket TAE 8 to S_o interface of the video system
(9–pin Sub–D socket)

Sub–D socket	TAE 8 Connector	Function
1 –		
2 – SR1–	**– 4 (b1)**	**Transmitter wire**
3 – SR2+	**– 3 (a1)**	**Transmitter wire**
4 – SX1–	**– 6 (a2)**	**Receiver wire**
5 – SX2–	**– 5 (b2)**	**Receiver wire**

ISDN socket IAE (RJ 45) to S_o interface of the video system
(9–pin Sub–D socket)

Sub–D socket	IAE connector	Function
1 –		
2 – SR1–	**– 5 (b1)**	**Transmitter wire**
3 – SR2+	**– 4 (a1)**	**Transmitter wire**
4 – SX1–	**– 3 (a2)**	**Receiver wire**
5 – SX2–	**– 6 (b2)**	**Receiver wire**

4.5 Connecting the VSCom 200 H (Interface Expansion)

May only be executed by authorized trained personnel!

Note:
only use the VSCom 200 H PCI card.

The interface expansion card is retrofitted as follows.

1. Switch off the computer and install the interface expansion card in the appropriate computer slot (see Section 2).
2. Reboot the computer.
3. Log on as the Administrator.
4. The system recognizes the interface expansion card automatically.

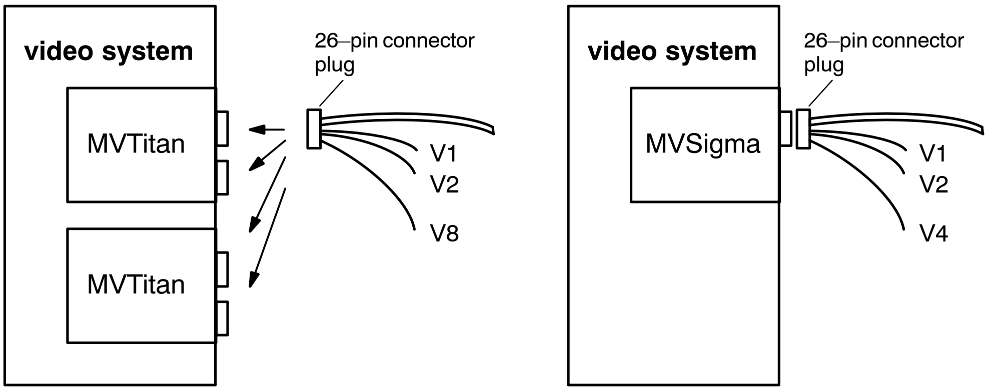
4.6 Connecting External Hard Disks

A SCSI controller must be installed in order to connect the external hard disk housing.
For information about the type and number of hard disks that may be connected, see the price list.

Note:
The Adaptec SCSI card 29160 may be used as the SCSI controller or the LSI Logic 160 MB Ultra Wide 68 PIN HD SYM 21040.

4.7 Connecting the Cameras

Note that one input is needed per B&W and CCVS camera and two inputs per Y/C camera.



Connection of	MVTitan Connector J11	 Connector J9	MVSigma
B&W and CCVS cameras	Camera 1 – V1 Camera 2 – V2 I I Camera 8 – V8	Camera 9 – V1 Camera 10 – V2 I I Camera 16 – V8	Camera 1 – V1 I I Camera 4 – V4
Y/C cameras	Camera 1 – V1/V5 Camera 2 – V2/V6 Camera 3 – V3/V7 Camera 4 – V4/V8	Camera 5 – V1/V5 Camera 6 – V2/V6 Camera 7 – V3/V7 Camera 8 – V4/V8	—

MVTitan: Maximum number of cameras per plug (J11 or J9) for mixture

B&W or CCVS	Y/C
8	—
6	1
4	2
2	3
—	4

Note:

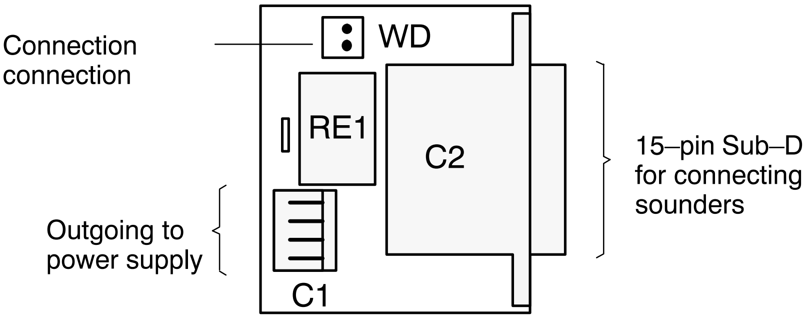
- Switch off the computer to connect the cameras.

4.8 Connecting the V–DOG and Tamper Contact

May only be executed by authorized trained personnel!

The module is used to monitor the tamper contact and power supply of the power unit. For signaling, a sounder can be connected.

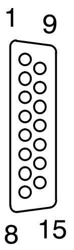
V–DOG



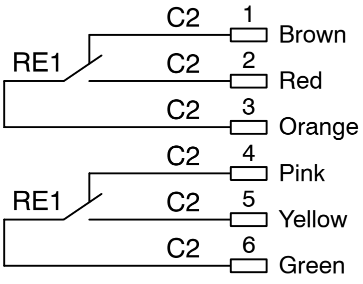
Installation:

A 15–pin MIDI extension cable is provided to connect a sounder to a C2 connector.
If necessary, remove the female connector from the MIDI cable and isolate the cable ends.

C2



C2 connector assignment



PC switched off
(disconnected
from power)

MIDI cable assignment

1	Brown	10	not occupied
2	Red	11	
3	Orange	12	
4	Pink	13	
5	Yellow	14	
6	Green	15	
7	not occupied		
8			
9			

4.9 Connecting the Software Dongle and the Printer

The programs are protected against unauthorized use by a dongle. The system cannot be operated without this dongle. The dongle must be connected to the **PRN** interface (LPT1) on the system board and remains there throughout operation. The dongle must be plugged in before switching the system on.

A printer must be connected via the USB interface so as not to hinder the reading out of program information from the dongle.

4.10 Connecting a Fault Indicator

A fault indicator (sounder) can be connected to relay 4 of the 1st MVTitan grabber card (must be activated in the configuration under **Hardware**/ **Connections**).

The following events will be signaled by the fault indicator:

- Images may be lost because the alarm archive is full
- The free disk space is not sufficient for the programmed total size of the archives
- The camera is not transmitting a video signal
- The database server could not record all images
- The grabber process does not answer in the prescribed time (timeout)
- The programmed holidays/special days are not released in the hardlock
- The programming for the serially–connected security system has been deleted by a software update
- System overload
- The directory could not be deleted from the database server
- Cannot create and write logbook
- The images could not be recorded by the database server
- The backup medium is full
- A timed backup could not be executed because a search macro was not found
- The programmed number of grabbers does not match the actual hardware configuration
- 5% of the hard disk is not free
- The database server is not started

4.11 Connecting the ATM via the Interface Processor (Serial)

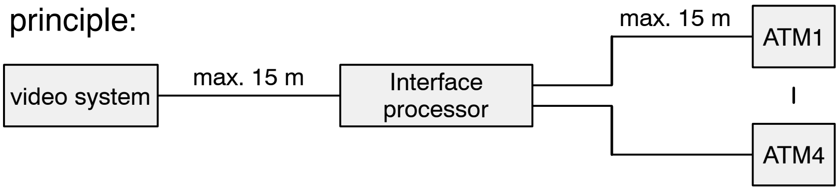
A maximum of 4 automatic teller machines or three automatic teller machines and 1 access control system can be connected to the video system via an interface processor.
The following ATM interfacing variants are available:

- **Method 1:**

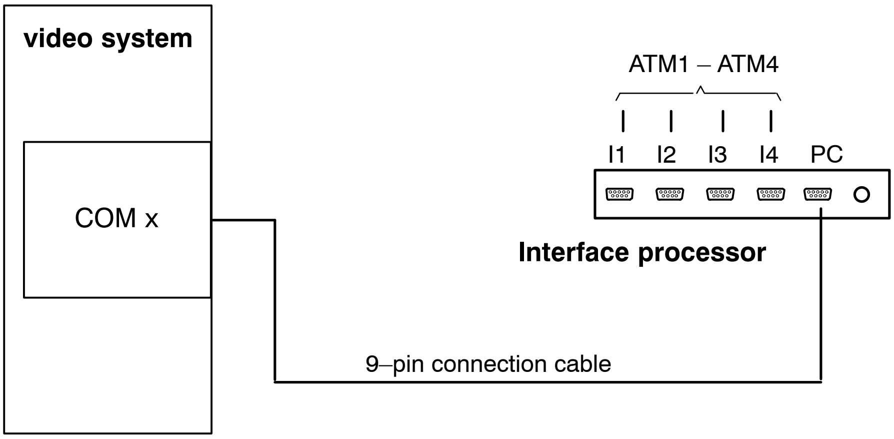
  Problem:
  The automatic teller machines (ATMs) are not located far from the video system. The distance between the video system and interface processor and between the interface processor and an ATM should be less than 15 m.

  Solution:
  The individual ATMs are linked directly to the interface processor by specific interfaces.
  The distance between the video system and the interface processor and the interface processor and the ATMs is max. 15 meters.

Connection principle:



Detailed connection:



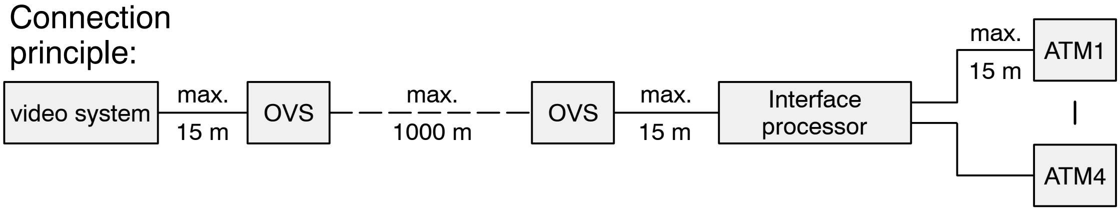
Connections (continued)

- **Method 2:**

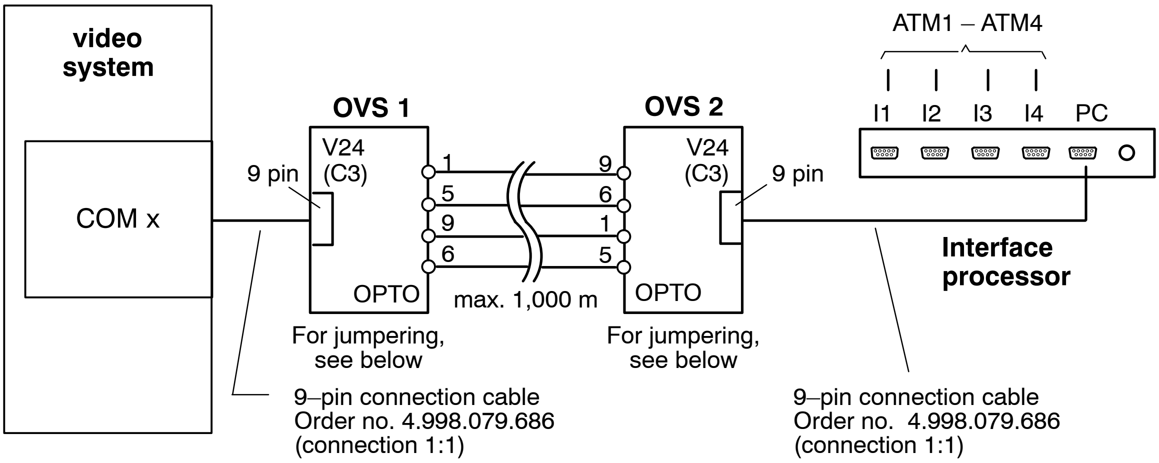
  Problem:
  The automatic teller machines (ATMs) are located further away from the video system. The distance between the video system and interface processor and between the interface processor and an ATM cannot be less than 15 m.
  However, the ATMs are close enough to one another for them all to be connected to the interface processor so that the distance between the interface processor and each ATM is less than 15 m.

  Solution:
  The individual ATMs are linked directly to the interface processor by specific interfaces. Two OVS are required between the video system and the interface processor to increase the range.

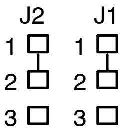
Connection principle:



Detailed connection:



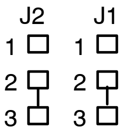
Jumpering of OVS 1:



C3:
Pin 2 = transmitter line
Pin 3 = receiver line

For assignment of OVS see Section 4.18.1

Jumpering of OVS 2:



C3:
Pin 2 = receiver line
Pin 3 = transmitter line

For assignment of OVS see Section 4.18.1

Note:
By changing jumper J1 and J2 in the OVS it is possible to mix up the transmitter and receiver lines (see above).

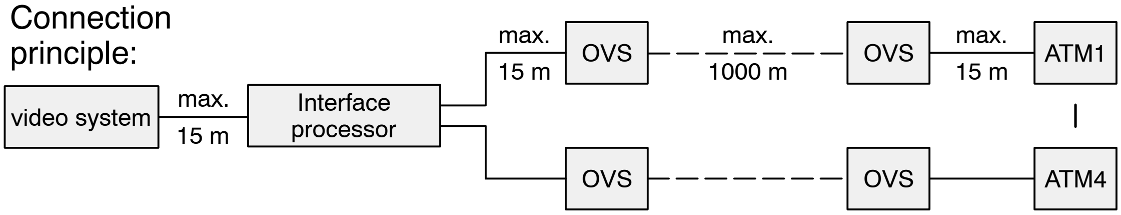
Connections (continued)

- **Method 3:**

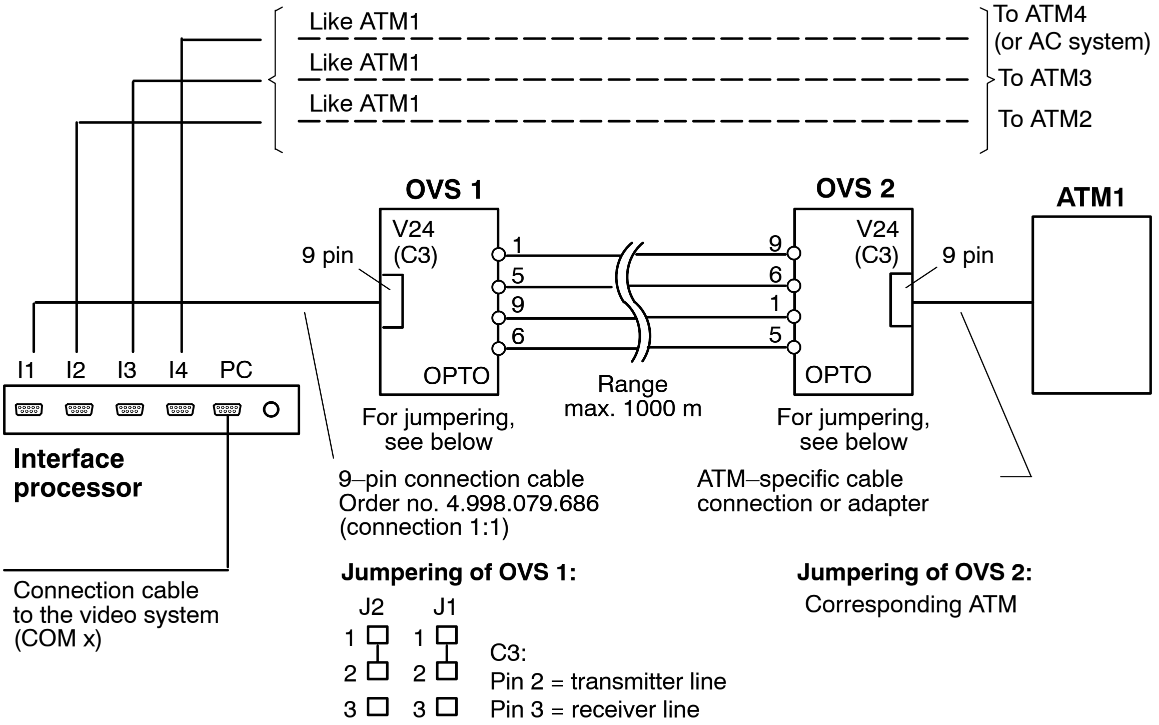
  Problem:
  The automatic teller machines (ATMs) are located further away from the video system. The distance between the video system and interface processor and between the interface processor and an ATM cannot be less than 15 m.
  However, the ATMs are not close enough to one another for them all to be connected to the interface processor so that the distance between the interface processor and each ATM is less than 15 m.

  Solution:
  The interface processor is connected directly to the video system.
  To increase the range, two OVS units are required between the interface processor and each ATM.

Connection principle:



Detailed connection:



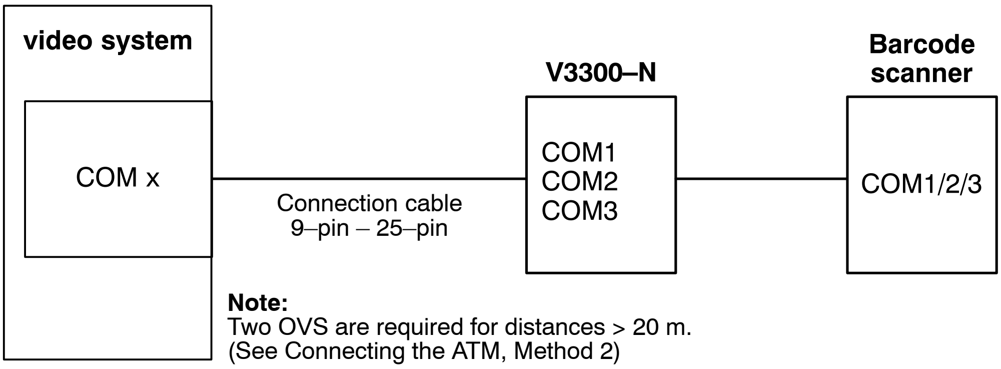
For assignment of OVS see Section 4.18.1

Note:
By changing jumper J1 and J2 in the OVS it is possible to mix up the transmitter and receiver lines.

4.12 Connecting the Barcode Reader

4.12.1 Barcode Reader V3300–N

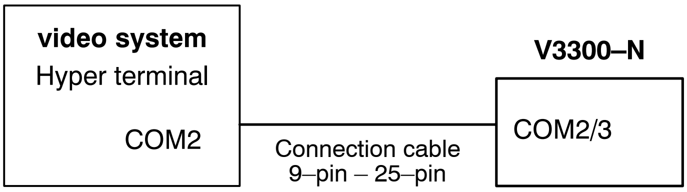
Only the barcode readers listed below should be used. With other types of barcode readers, you must check whether their protocol matches that of the video system.



Note:
Two OVS are required for distances > 20 m.
(See Connecting the ATM, Method 2)

To operate the VS3300–N, you must change some settings. A preconfigured hyperterminal program, which can be called up from the diskette under Windows ® XP by typing in ”VISOLUX SCANNER.ht,“ is used as the program editor for the V3300–N.

Programming the V3300–N
The V3300–N can only be programmed on its internal COM2 or COM3 interface; this must be done before calling up the video system program. Connect the V3300–N to the COM2 interface of the video system as follows.



Certain settings are necessary on the V3300–N itself in order to program it. The following list gives you a brief summary. For more details, please refer to the listed sections of the V3300–N manual.

- Activating programming mode
  → see ”Setup Mode” Section
- Setting the baud rate, number of data bits, number of stop bits, and parity
  → see ”Changing Baud Rate”, ”Changing Number of Data Bits”, ”Changing Stop Bits” and ”Changing Parity” Sections

Connections (continued)

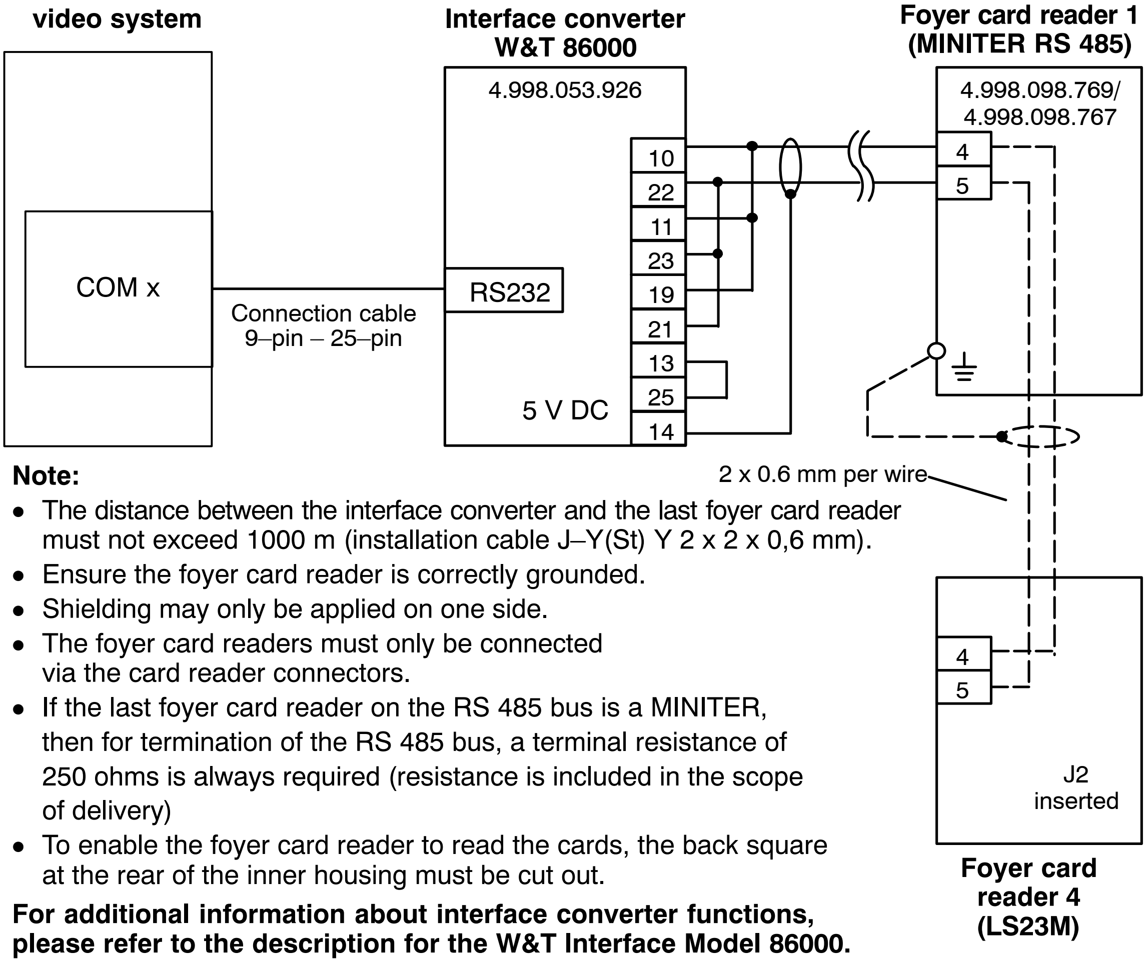
- Selecting communication protocol
  Use the default protocol.
  → see ”Communications Protocol” Section
- Hide own device address
  The device address must not be transmitted because it is not evaluated in the video system and unnecessarily reduces the available memory capacity for the barcode reader data to be saved in live image.
  → see ”Transmitting own device address” Section
- Hiding sequence ID
  The sequence ID must not be transmitted for the same reasons as above.
  → see ”Transmitting Sequence ID” Section
- Deactivating the beeper
  The beeper must be deactivated because high scan frequencies cause data transfer errors when it is activated.
  → see ”Activating beeper after receiving data” Section
- Defining transmit header
  Set STX as the header.
  → See ”Defining Transmit Header” Section
- Defining transmit trailer
  Set CR, LF as trailers.
  → See ”Defining Transmit Trailer” Section
- Enabling interface
  Enable the interface used by the V3300–N.
  → see ”Enabling/Disabling Interface” Section
- Enabling codes
  Enable the codes that are used. The maximum code length is 17 characters.
  → see ”Enabling/Disabling Codes” Section
- Saving programming
  Before finishing the programming, you must store the set parameters using the ”Save” command and then press ”ESC”. The V3300–N then exits programming mode and restarts automatically. The device is ready to operate when ”READY TO READ” appears on the display.

4.12.2 Barcode reader DOUBLE–X–LR

Contact Product Service Video of the video system manufacturer for connection of a barcode reader DOUBLE–X–LR.

4.13 Connecting Foyer Card Reader MINITER RS 485

The foyer card reader MINITER RS 485 is connected via a serial interface. A maximum of four foyer card readers can be connected in series. The foyer card reader LS23M and the foyer card reader MINITER RS 485 can be operated on the same serial bus. Please note that the foyer card reader LS23M should preferably be installed as the last bus element.

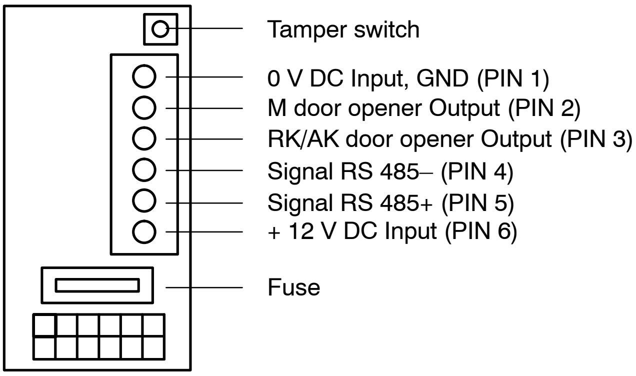


Note:

- The distance between the interface converter and the last foyer card reader must not exceed 1000 m (installation cable J–Y(St) Y 2 x 2 x 0,6 mm).
- Ensure the foyer card reader is correctly grounded.
- Shielding may only be applied on one side.
- The foyer card readers must only be connected via the card reader connectors.
- If the last foyer card reader on the RS 485 bus is a MINITER, then for termination of the RS 485 bus, a terminal resistance of 250 ohms is always required (resistance is included in the scope of delivery)
- To enable the foyer card reader to read the cards, the back square at the rear of the inner housing must be cut out.

For additional information about interface converter functions, please refer to the description for the W&T Interface Model 86000.

MINITER RS 485 contact assignment


Tamper switch
0 V DC Input, GND (PIN 1)
M door opener Output (PIN 2)
RK/AK door opener Output (PIN 3)
Signal RS 485– (PIN 4)
Signal RS 485+ (PIN 5)
+ 12 V DC Input (PIN 6)
Fuse

Programming the foyer card reader MINITER RS 485

Programming is carried out using MINITER RS 485 software. This can be installed on a service laptop or on a video system.
Proceed as follows:

1. Start the programming software and select RS 485 operation.
2. Select the COM port to which the foyer card readers are connected via the “Interface” menu item.
   Even if several foyer card readers MINITER RS 485 are to be programmed for the first time, only one foyer card reader should be connected during programming. This is because the foyer card reader will assign all the card readers with the same bus address by default.
3. Select the “MINITER → Read/Identify Miniter” menu and click “Identification of all activ addresses”.
   “Address: 48” and “Protocol: Bosch” is displayed.
4. Select foyer card reader number 48 and confirm your selection with ”OK”.
5. Click “Read Miniter” and enter “Password: 991357”. Confirm with ”OK”.
6. The foyer card reader addresses must be specified as follows:
   Foyer card reader no. 1 = address 48
   Foyer card reader no. 2 = address 49
   Foyer card reader no. 3 = address 50
   Foyer card reader no. 4 = address 51
   For operation, the other parameters must be set as follows:
   - Door opening time: optional
   - Door opener with buzzer: optional
   - Door opener interval tone: optional
   - Monitoring module: no
   - Password: 991357
   - Signal chipcard: no
   - Send start character: no
   - Data on display: no
   - Evaluate track 2: yes
   - Evaluate track 3 or 1: yes
   - Open door on fault: no
   - Protocol: Bosch
   - Bloc list: optional
   - Data length track 2: 18 (for credit cards)
   - Data length track 3/1: 26 (for EC cards)

Connections (continued)

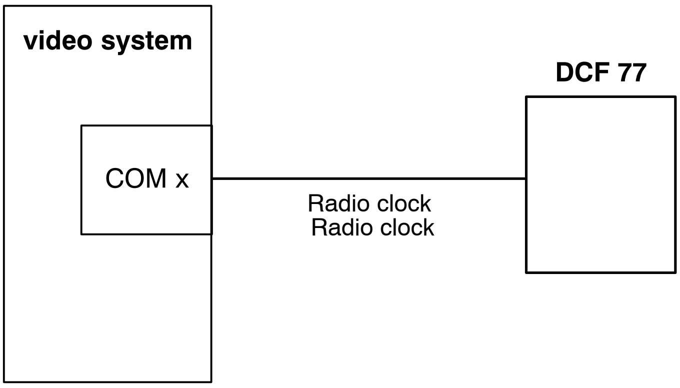
7. Set different authorization for credit cards (track 2) and EC cards (track 3), so that access can be gained to the foyer card reader if the connection between the video system and the Miniter is interrupted (see operating instructions for Miniter RS 485).
   Otherwise in normal operation the video system takes over access authorizations.
8. Save the file via the "File → Save as" menu under the name "DiBos_foyer_card_reader_x" (x = 1 .. 4).
9. Select "File → Exit".
10. Select the "MINITER → Write Miniter" menu and select and open the "DiBos_foyer_card_reader_x" file.
    The new and current address of the foyer card reader is displayed.
11. Confirm the address with "OK".
12. Click "Write file in Miniter" and confirm this by entering the old password.
    System confirmation is given when programming has been completed successfully.

4.14 Connecting Radio Clock DCF 77

May only be executed by authorized trained personnel!

The connection must be made to a serial interface.

Note:
Only the radio clock NeoClock DCF 77 should be used.



The interface expansion card is retrofitted as follows.
Use the supplied installation CD.

1. Connect the radio clock to the serial interface.
2. Log on as the Administrator.
3. Enter the settings for the interface in use.

Baud:	2400
Data bits:	8
Parity:	None
Stop bits:	2
Protocol:	None

4. Insert the installation CD.
5. Call up ”Setup.exe” in the Windows® XP Explorer.
6. Select ”Install server” and click ”Next”.
7. Select the destination directory for the programs.
   Click ”Next”, if you want to use the default path or click ”Browse” to select another one.
8. Follow the on–screen instructions.
9. Once installed, configure the ”Time Synchronization” program.
   - Select ”Start → Control Panel →System”.
   - Select the ”Hardware” tab and click ”Device Manager”.
   - In the tree structure, open the entry ”Ports” with a double click and select the ”Port settings” tab.
   - Double–click on the appropriate interface, e.g. ”COM 1”, to open its properties field.

Connections (continued)

10. Make the following settings in the configuration menu:

Language:	”German”
Port:	”COM x” (interface in use)
Synchronization:	”Automatic”.
Time lag:	Select ”0” (hours) and ”Daylight saving time”
License:	Enter serial number and activation code (Please note these entries are case sensitive)

    Click ”Save”.
11. Click ”Yes” in the information window to start the ”Time Synchronization” service.
    Note:
    A timer appears in the Windows® XP task bar (at the bottom edge of the screen). This confirms that the ”Time Synchronization” program has started.
    The color of the timer depends on the status of the receiver.

Yellow:	Program starting (takes up to three minutes)
Red:	No synchronization or installation error
Green:	The system timer is synchronized correctly with the receiver.
12. End the ”NeoClock Time Server” service as follows:
    - Select ”Control Panel → Administrative Tools→ Services”.
    - Select the ”NeoClock Time Server” service and click ”Close” to exit the service.
    - Deactivate the service by selecting the start type ”Deactivated” and confirm with ”OK”.
    - Confirm with ”OK” and close the ”Services” dialog box and the Control Panel.
13. Reboot the PC.
14. The ”NeoClock Time Server” program must not be configured; instead TARDIS should be used. (Program used to synchronize video systems in a network; contact Product Service Video of the video system manufacturer.)
15. Follow the operating instructions for NeoClock XP to position the clock (available as a PDF file on the CD).

4.15 Web Connection for Access Via Browser

May only be executed by authorized trained personnel!

The master disk contains the preinstalled Web application for accessing the image archive via the browser. The Web application needs port 80 and is activated by default. Should access via http be hindered, the World Wide Web Publishing service must be deactivated.

Activating/deactivating the Web application:

You must have administrator rights to carry out the following steps:

1. Log on as the Administrator.
2. Select ”Start → Control Panel”.
3. Double–click the ”Administrative Tools” icon.
4. Double–click the ”Internet Information Services” icon.
5. Open the tree structure under ”Internet Information Services” until you see the entry ”Default Web Site”.
6. Select the entry ”Default Web Site”.
7. Start the service with the button ”▶”
   or
   stop the service with the button ”■”.

4.16 Connecting a Modem

May only be executed by authorized trained personnel!

You must have administrator rights to carry out the following steps:

4.16.1 Selecting and Installing the Modem

Notes for selecting the modem:

- Internal PCI modems, serially–connected modems, and modems connected via USB can be used as long as they are supported by Windows® XP.
- Protocols V.90 and V.34 must be supported.
- Regulations of the relevant country must be observed (particularly with regard to operation in the telephone network, interference suppression, electrical safety and fire prevention).
- Compatible with the features of the national telephone networks.
- The special characteristics of company private telephone systems must be observed (e.g. deactivating dial tone recognition, tone or pulse dialing).

Installing the modem

Install the modem according to the supplied manufacturer documentation. Under Windows® XP, many modem types are recognized automatically. Nevertheless, you should take the special features of the installation into consideration (example: if the modem does not recognize a telephone system's dial tone, the option ”Wait for dial tone before dial” must be selected.

Decrease Timeout Value for Outgoing Connections

1. From the Windows ® XP desktop, select ”Start → Control Panel”.
2. From the ”Control Panel” folder, select the ”Phone and Modem Options” icon.
3. On the ”Phone and Modem Options” dialog field, click the ”Modems” tab.
4. From the list box, select the installed modem and click the ”Properties” button.
5. On the ” ... Properties” dialog, click the “Advanced” tab and then click the “Change Default Preferences ...” button.
6. On the “General” page, under “Cancel the call if not connected within .. seconds,” change the value from “60” to “15.”
7. Confirm the open dialog fields with ”OK”.

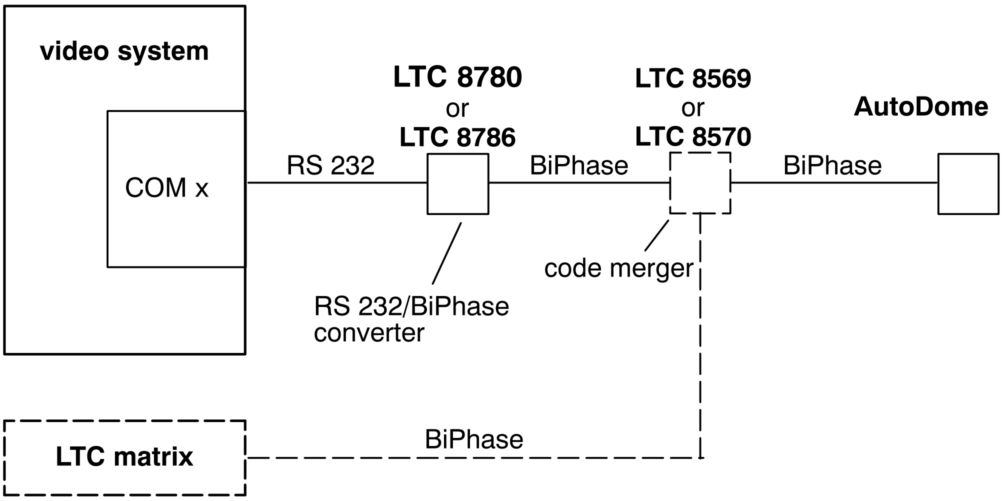
Enable dial–in (if incoming calls should be accepted)

1. From the Windows ® XP desktop, select ”Start → Control Panel”.
2. From the ”Control Panel” folder, select the ”Network Connections” icon.
3. In the ”Network Connections” folder, under ”Network Tasks”, click the ”Create a new connection” icon.
4. On the ”New Connection Wizard” dialog box, click the ”Next” button.
5. On the ”Network Connection Type” wizard page, select the option ”Set up an advanced connection” and click the ”Next” button.
6. On the ”Advanced Connection Options” wizard page, select the ”Accept incoming connections” option and click the ”Next” button.
7. On the ”Devices for Incoming Connections” wizard page under ”Connection Devices”, select the previously–installed modem and place a checkmark next to this entry. Click the “Next” button
8. On the ”Incoming VPN Connection” wizard page, activate the ”Do not allow virtual private connections” option and click the ”Next” button.
9. Create the new user as follows:
   - On the ”User Permissions” wizard page, click the ”Add” button and enter the following on the ”New User” dialog box:
   - User name: ‘RasUser8B19’
   - Full name: leave empty
   - Password: Enter password (can be changed later via the DiBos interface)
   - Confirm password: Enter the password again
   - Confirm with ”OK”.
   - On the wizard page, make sure that there is a checkmark next to the newly–created user ”RasUser8B19”.
   - Click the “Next” button.
10. Set the settings for the network protocol as follows:
    - On the ”Networking Software” wizard page, select the ”Internet protocol (TCP/IP)” entry from the list box and make sure that there is a checkmark next to this entry.
    - Click on ”Properties” and make sure that in the ”Incoming TCP/IP–Properties” dialog box, the option ”Allow callers to access my local area network” is not selected and that the option ”Assign TCP/IP addresses automatically using DHCP” is selected. Confirm with ”OK”.
    - Click the “Next” button on the wizard page.
11. On the ”Completing the New Connection Wizard” wizard page, click ”Finish”.

Connections (continued)

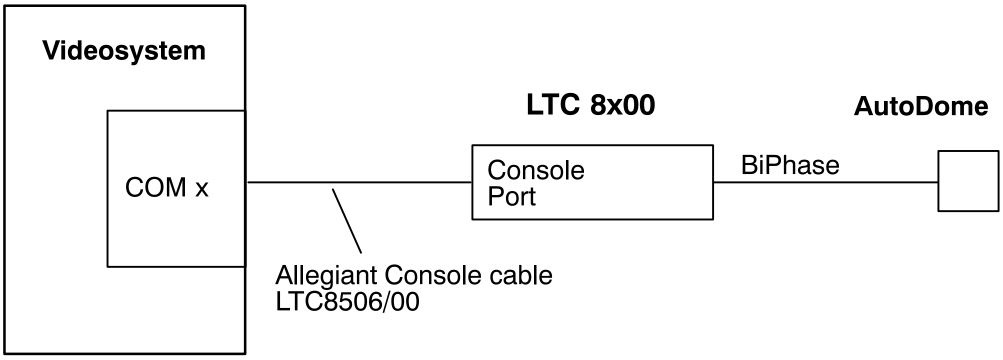
4.17 Connecting AutoDome/SAE–Dome

• Connecting AutoDome



Note: Additionally a code merger LTC 8569 or LTC 8570 is needed, if a PTZ shall be controlled from the video system and a Bosch LTC matrix.

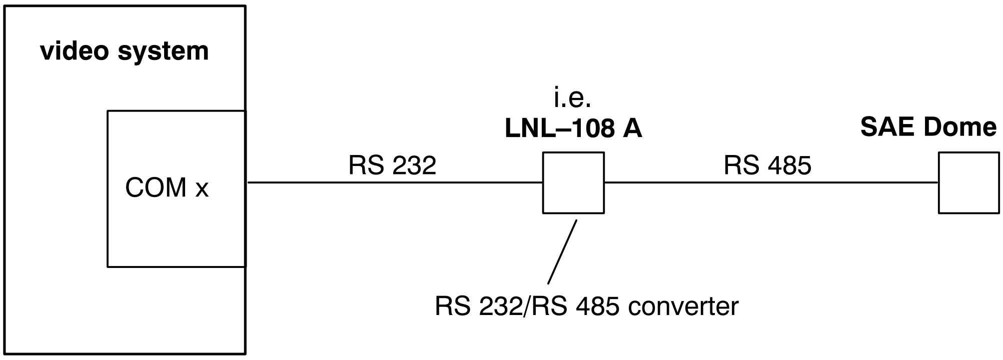
• Connecting AutoDome via matrix



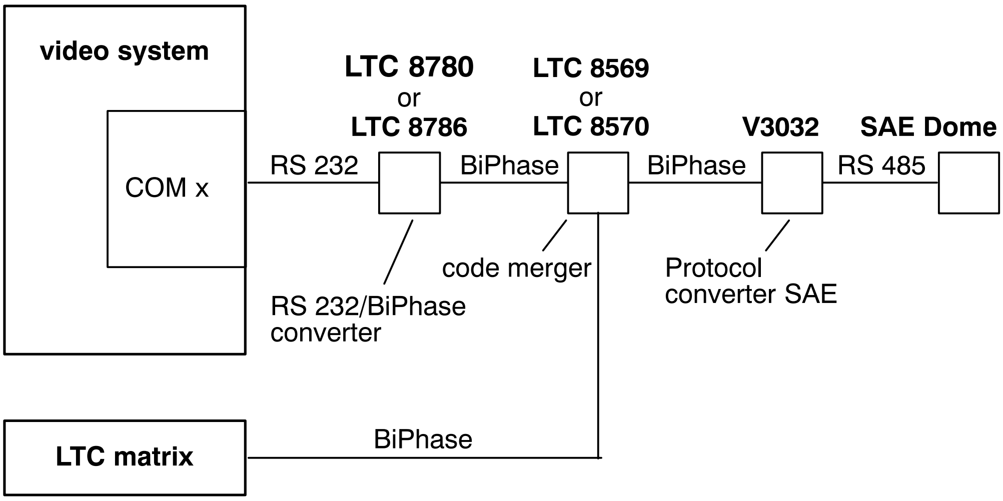
Hinweis: Valid CCL commands can be configured in the DiBos. Then you can send these pre–configured commands manually to the Allegiant matrix

Connections (continued)

• Connecting SAE Dome directly



• Connecting SAE Dome with V3032 Biphase interface

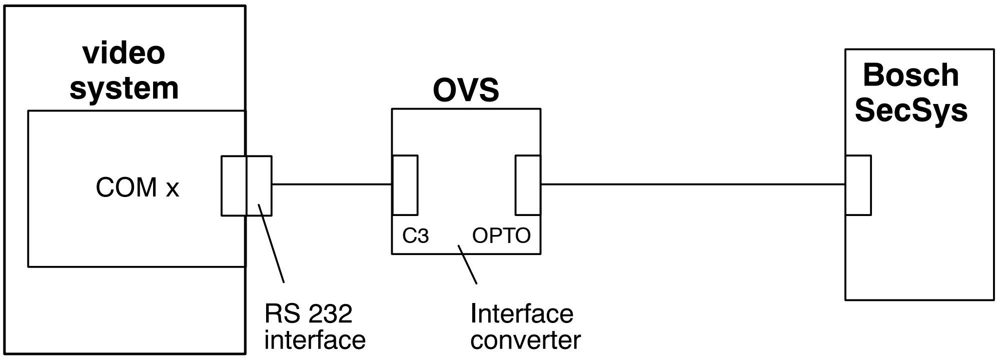


Note: Additionally a code merger LTC 8569 or LTC 8570 is needed, if a PTZ shall be controlled from the video system and a Bosch LTC matrix.

4.18 Connecting a Security System

4.18.1 General remarks

The video system is connected to a SecSys via an RS 232 interface at COM x, e. g. by connecting an interface converter OVS in between.



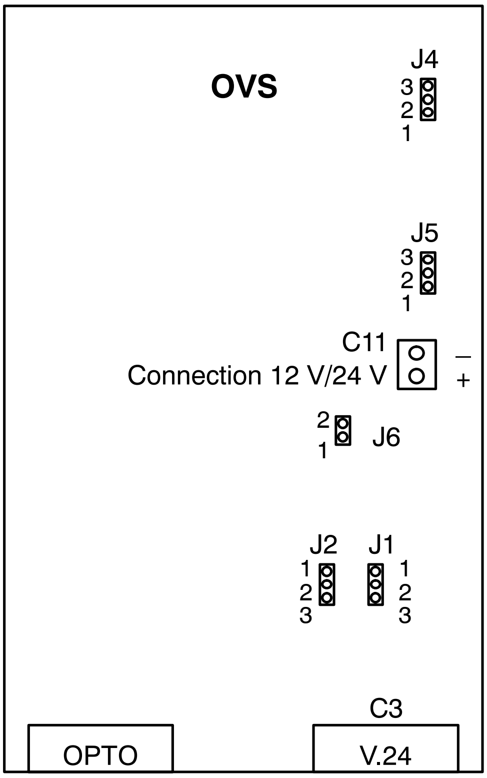
No specific alarm modifications are necessary on the security system for connection to the video system. A suitable interface module is required. All settings are made via the video system user interface:

Data transmission must be enabled in the SecSys and the SecSys must be equipped with a suitable interface module (see Connections).

With the OVS it is possible to compensate any differences in the transmitter and receiver line assignments of the devices on the V.24 side of the link. To do this change the jumpers J1 and J2.

Connections (continued)

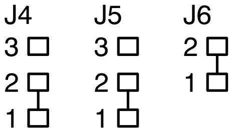
Jumper assignment for interface converter OVS



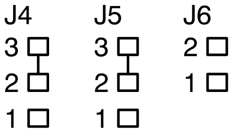
Attention:

Remove the OVS network plug before opening the device !

For power supply of 12 V/24 V

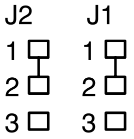


For a power supply of 230 V



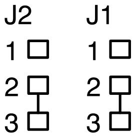
Replacing transmitter and receiver lines

Variant 1:



C3:
Pin 2 = transmitter line
Pin 3 = receiver line

Variant 2:



C3:
Pin 2 = receiver line
Pin 3 = transmitter line

Connector assignment for OPTO

Direction	Connection
Input –	1
Input +	6
Output +	5
Output –	9

Connector assignment for V.24 (C3)

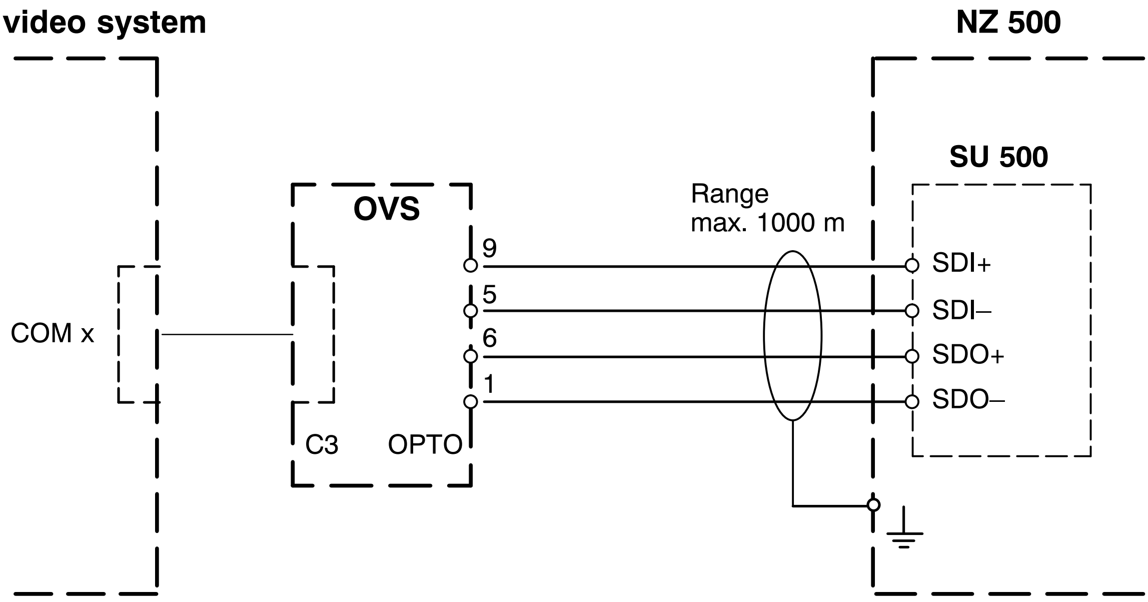
Direction	Connection
Transmitter/Receiver *	2
Receiver/Transmitter *	3
0 V	5

* Depends on J1/J2

Note:
Telecommunications cable type J–Y(St)Y 2x2x0,6 is recommended for cabling. Ground the cable shield at the center end to prevent earth currents.

Connections (continued)

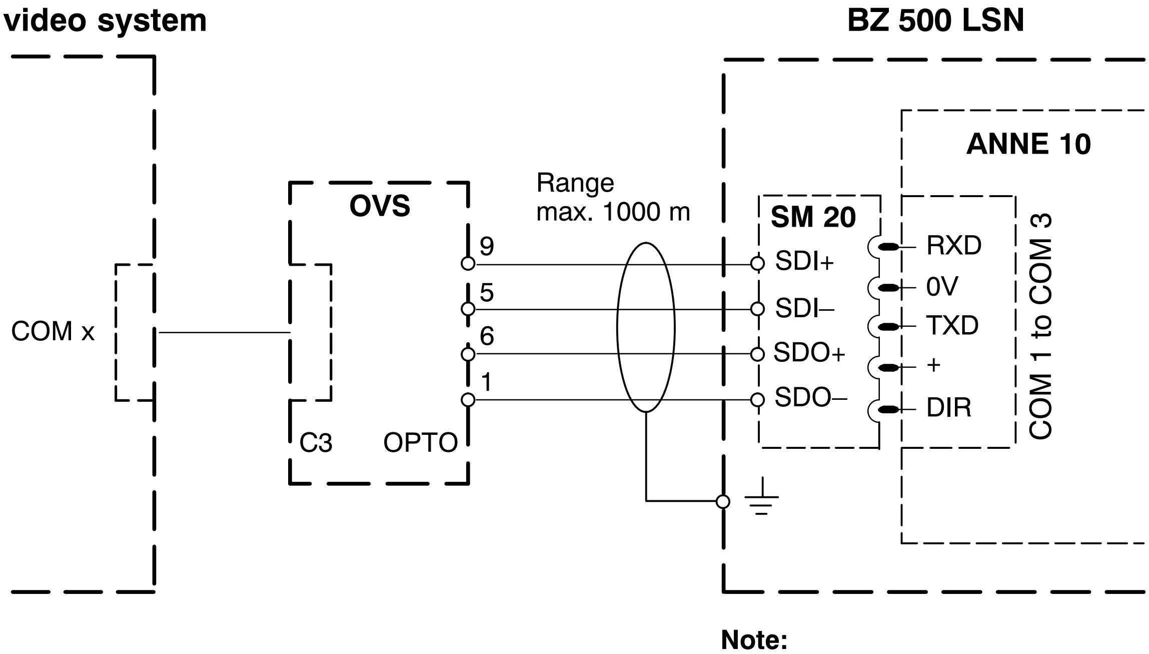
4.18.2 Connecting to NZ 500 (20 mA)



Only connect shield to NZ 500.
Installation cable J–Y (St) Y 2x2x0,6

SU 500:
J1 inserted (1200 bit/s)

4.18.3 Connecting to BZ 500 (20 mA)



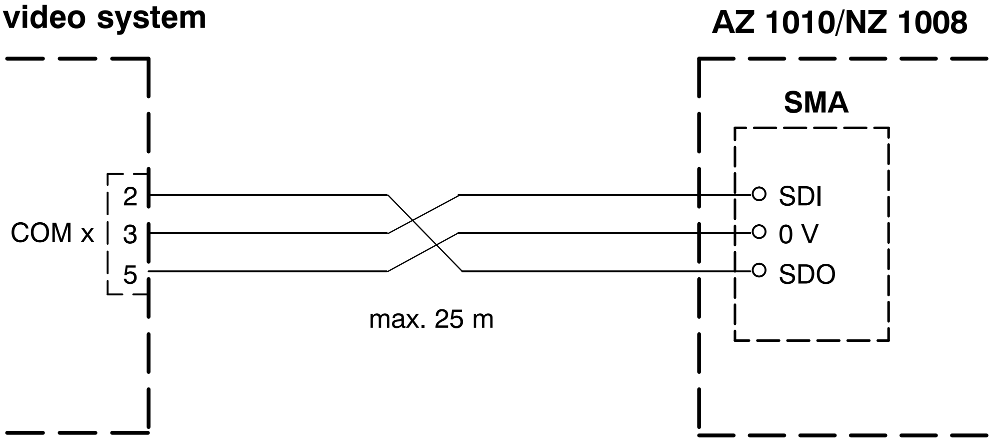
Only connect shield to BZ 500.
Installation cable J–Y (St) Y 2x2x0,6

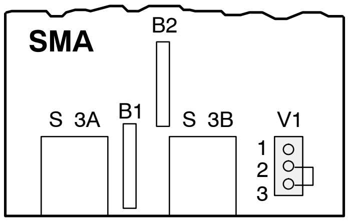
Note:
COM 2 and COM 3 only with
ERSE 10 interface module

Connections (continued)

4.18.4 Connecting to AZ 1010/NZ 1008

- **V.24 Connection to AZ 1010/NZ 1008**



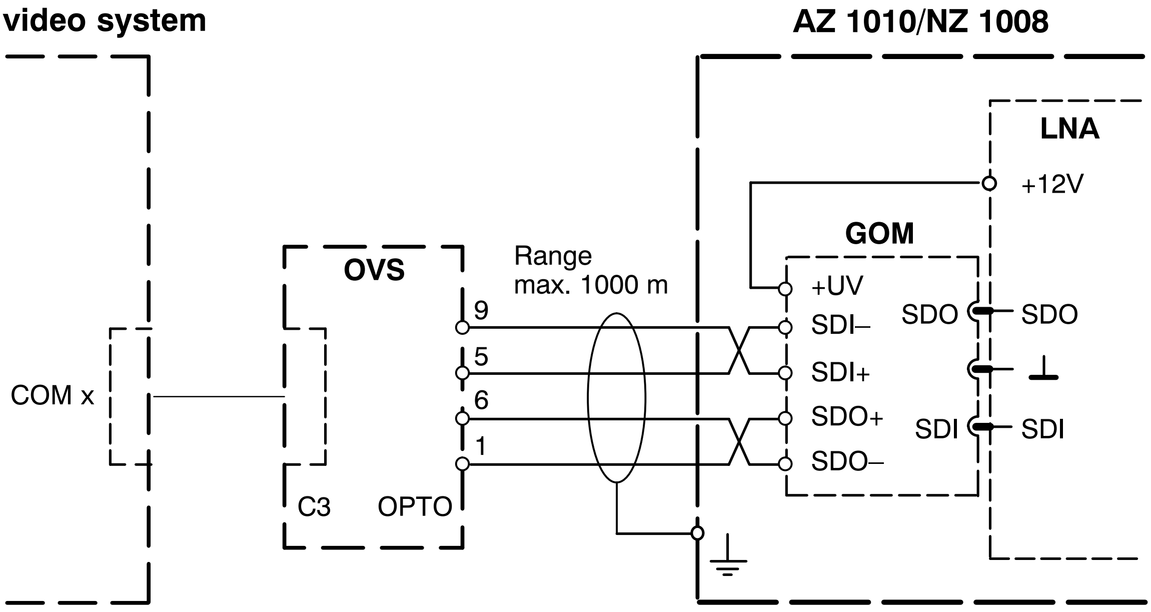


Connection to the AZ 1010/NZ 1008 must be programmed at the center

Jumper assignment (V) on the SMA

Jumper V1 set to 2/3
Level for V.24 interface

- **20 mA connection to AZ 1010/NZ 1008**



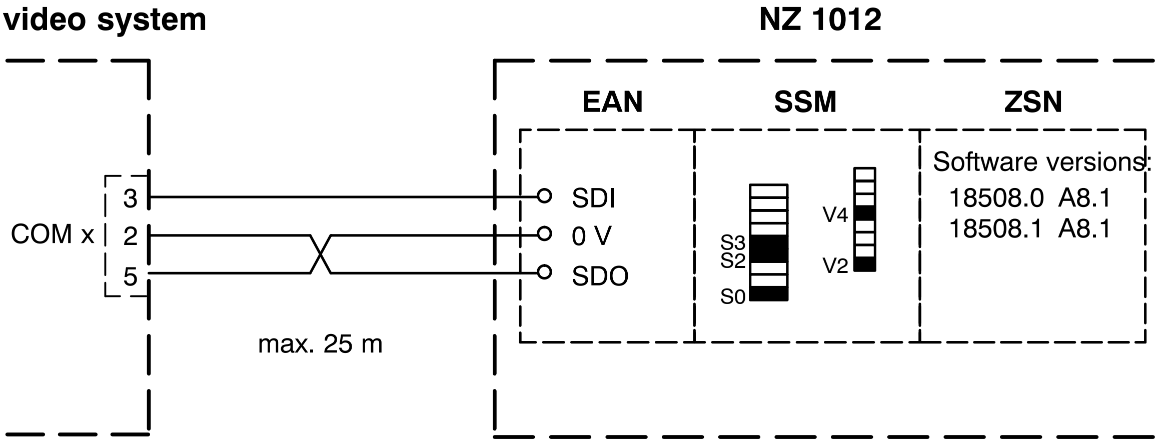
Jumper assignment (V) on the SMA

Jumper V1 set to 1/2
Level for V.24 interface

Only connect shield to AZ 1010/NZ 1008.
Installation cable J–Y (St) Y 2x2x0,6

4.18.5 Connecting to NZ 1012

• V.24 connection to NZ 1012

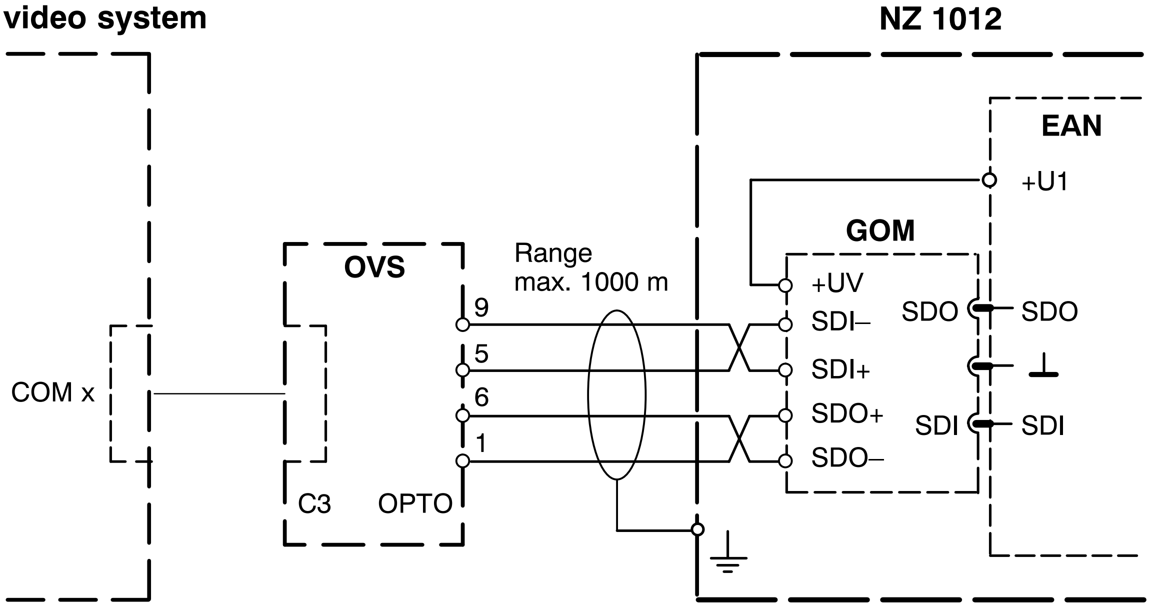


Dip–Fix switches (S) and jumpers (V) on SSM

Interface 1:			**Interface 2:**		
S0	On:	1200 baud	S4	On:	1200 baud
S1	Off:	Video system	S5	Off:	Video system
S2	On:	Transmit priority for NZ 1012	S6	On:	Device is connected
S3	On:	Device is connected	S7	On:	Transmit priority for NZ 1012
V2, V4	Inserted:	V.24 interface	V12, V14	Inserted:	V.24 interface

Note: Connection to interface 2 is possible.

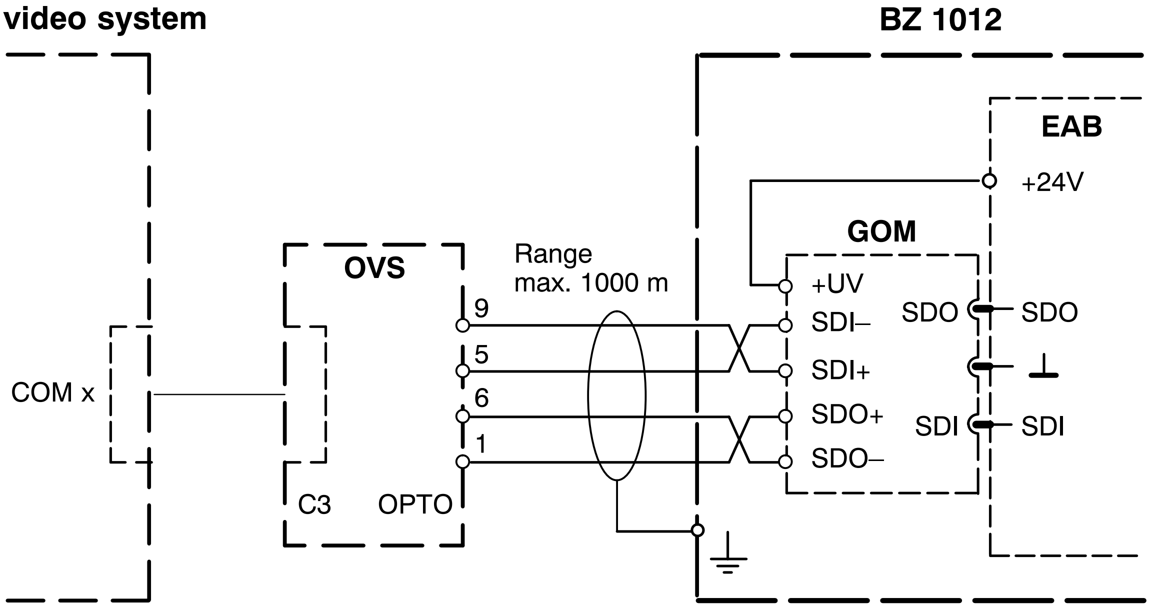
• 20 mA connection to NZ 1012



Insert SSM jumpers at ”20 mA”.

Connections (continued)

4.18.6 Connecting to BZ 1012 (20 mA)

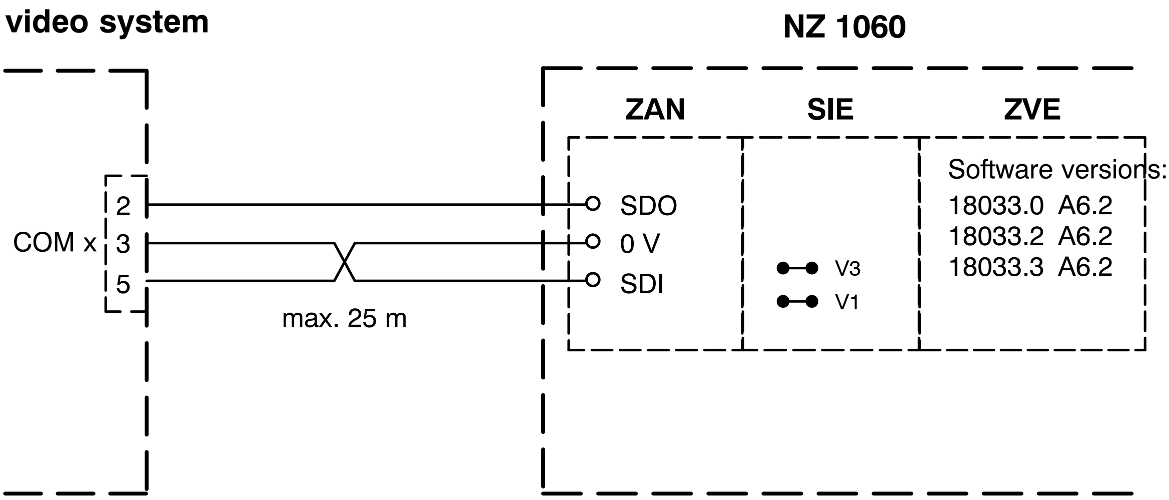


Insert SSM jumpers at ”20 mA”.

Connections (continued)

4.18.7 Connecting to NZ 1060

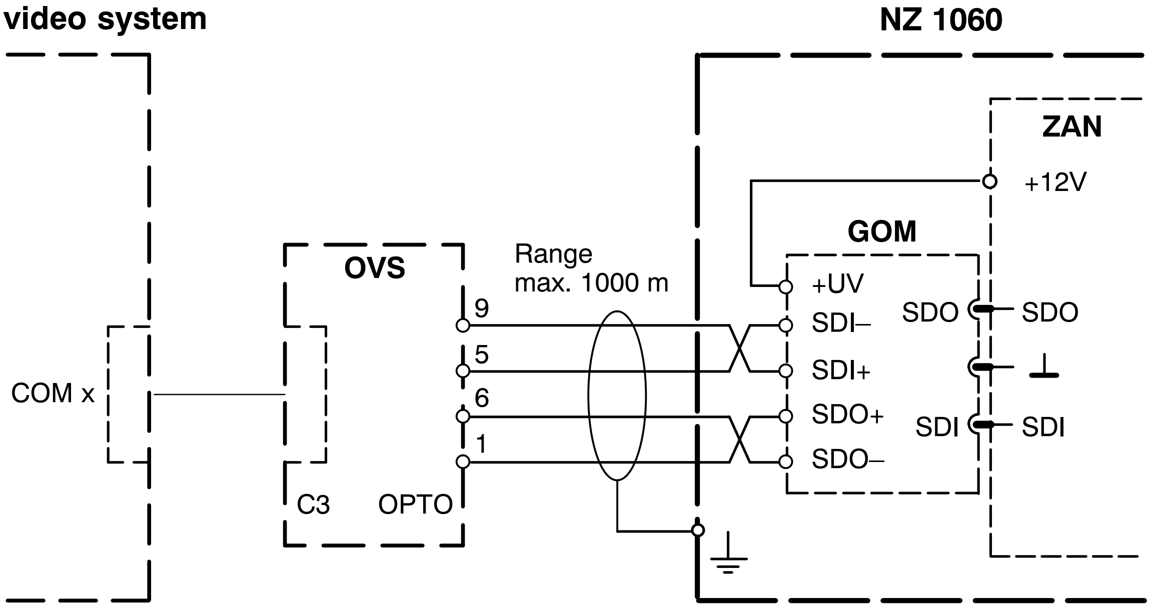
• V.24 connection to NZ 1060



Note:
It is preferable to use interfaces 6 through 9, but connection to interfaces 2 through 5 is also possible depending on the project.

Program the appropriate interface to AUX (1200 baud), insert jumpers on SIE (V1, V3) for V.24 interface.

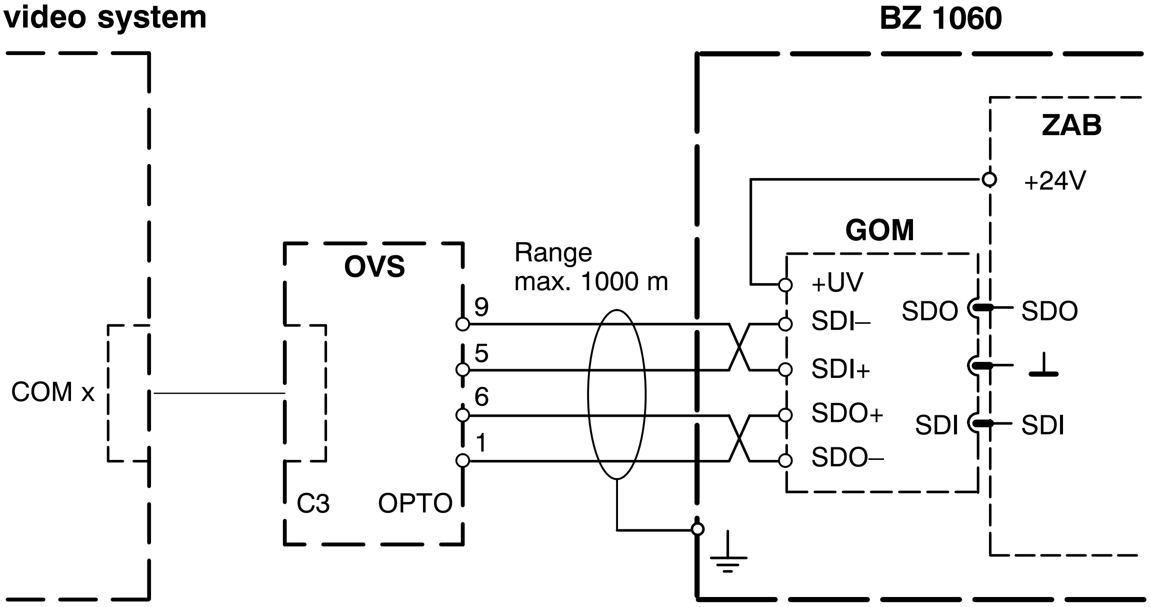
• 20 mA connection to NZ 1060



It is preferable to use interfaces 6 through 9, but connection to interfaces 2 through 5 is also possible depending on the project.
Program the appropriate interface to AUX (1200 baud), insert jumpers on SIE (V2, V4) for 20 mA interface.

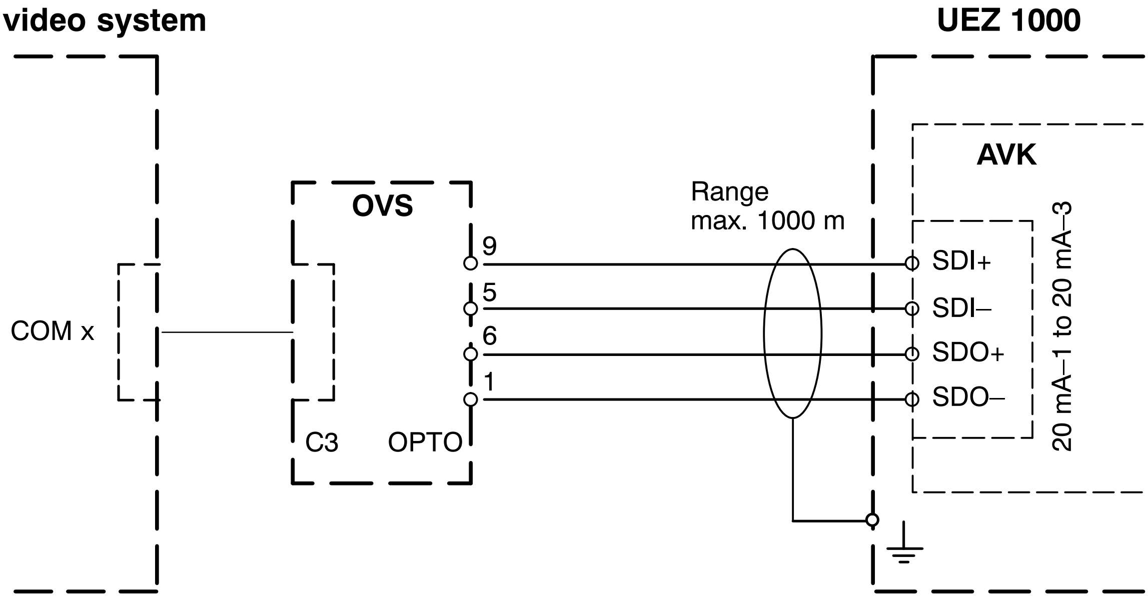
Connections (continued)

4.18.8 Connecting to BZ 1060 (20 mA)



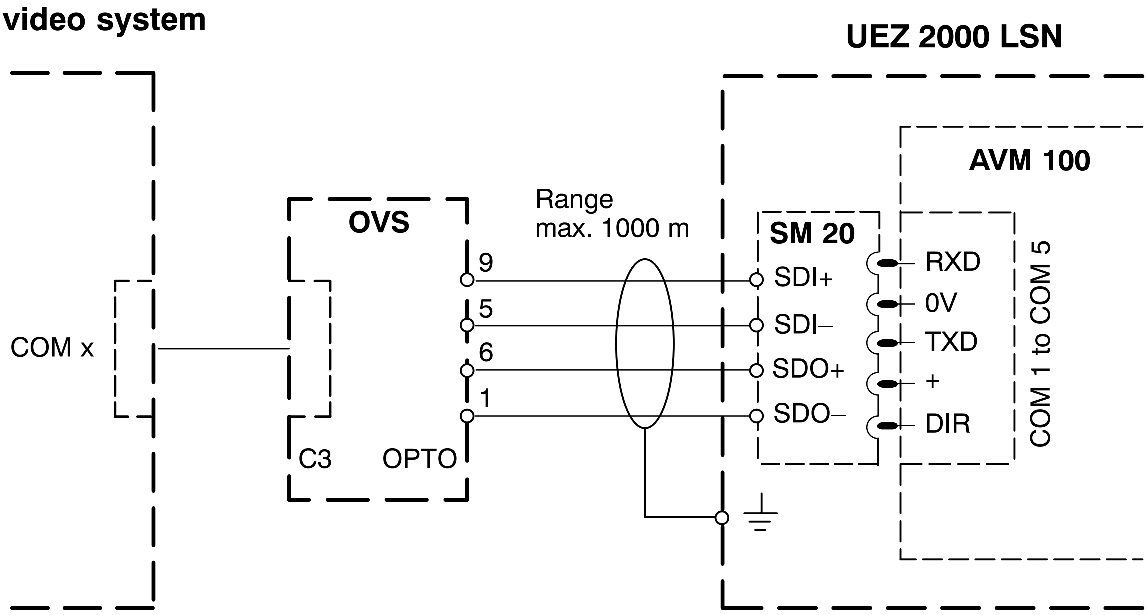
It is preferable to use interfaces 6 through 9, but connection to interfaces 2 through 5 is also possible depending on the project.
Program the appropriate interface to AUX (1200 baud), insert jumpers on SIE (V2, V4) for 20 mA interface.

4.18.9 Connecting to UEZ 1000 (20 mA)



Only connect shield to UEZ 1000.
Installation cable J–Y (St) Y 2x2x0,6

4.18.10 Connecting to UEZ 2000 (20 mA)



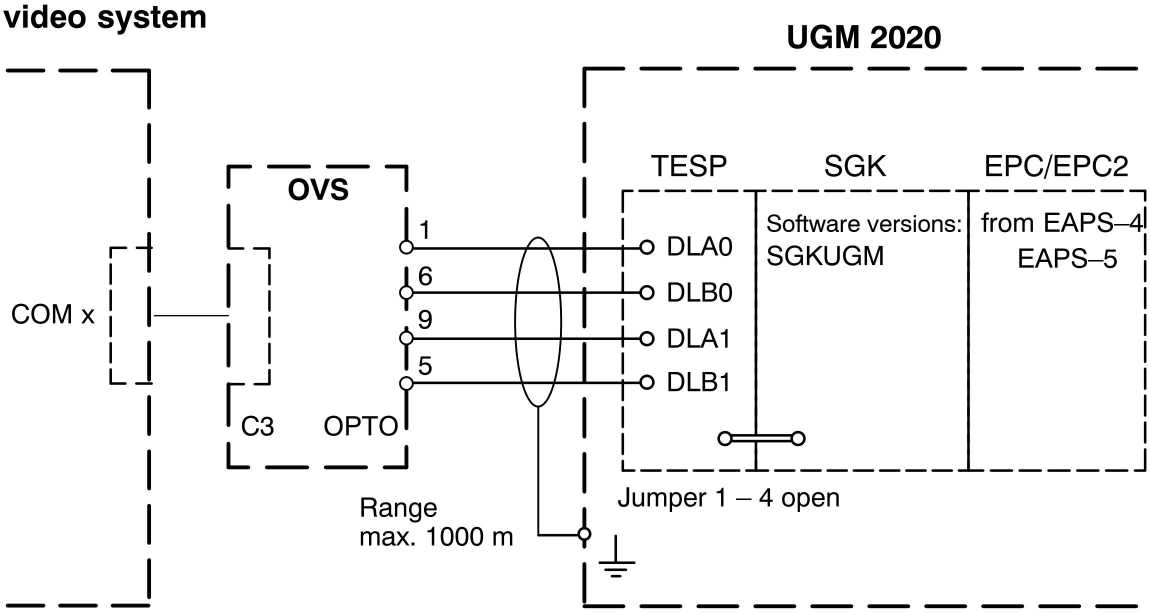
Only connect shield to UEZ 2000.
Installation cable J–Y (St) Y 2x2x0,6

Note:
COM 4 and COM 5 only with
SEMO1 interface module

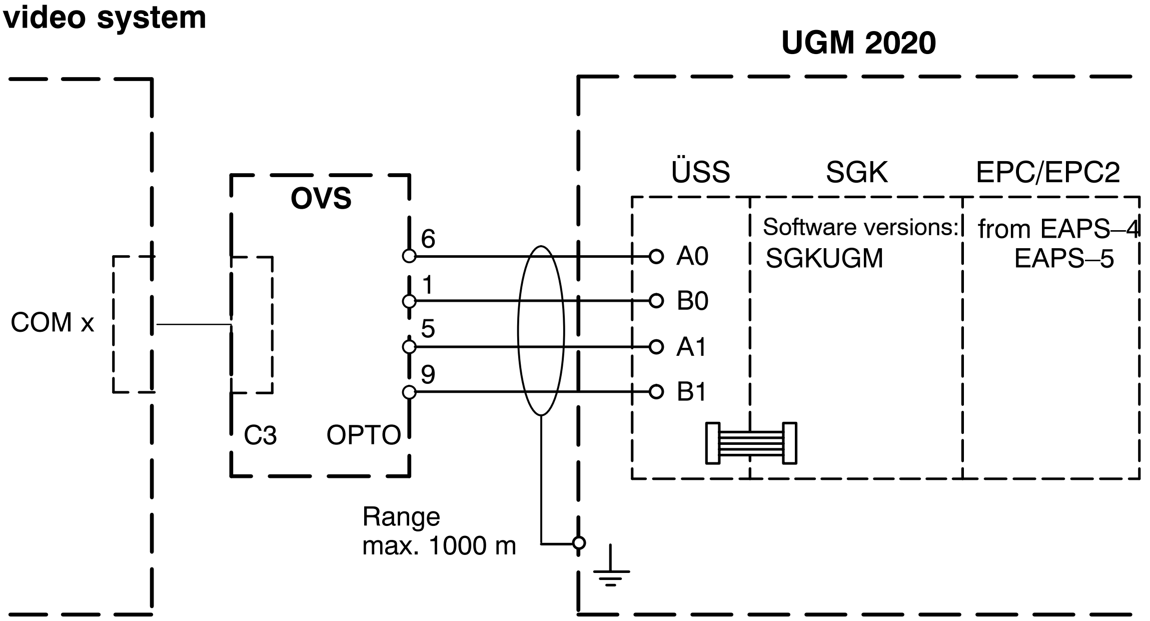
Connections (continued)

4.18.11 Connecting to UGM 2020

• 20 mA connection to UGM 2020 or TESP (by telephony)

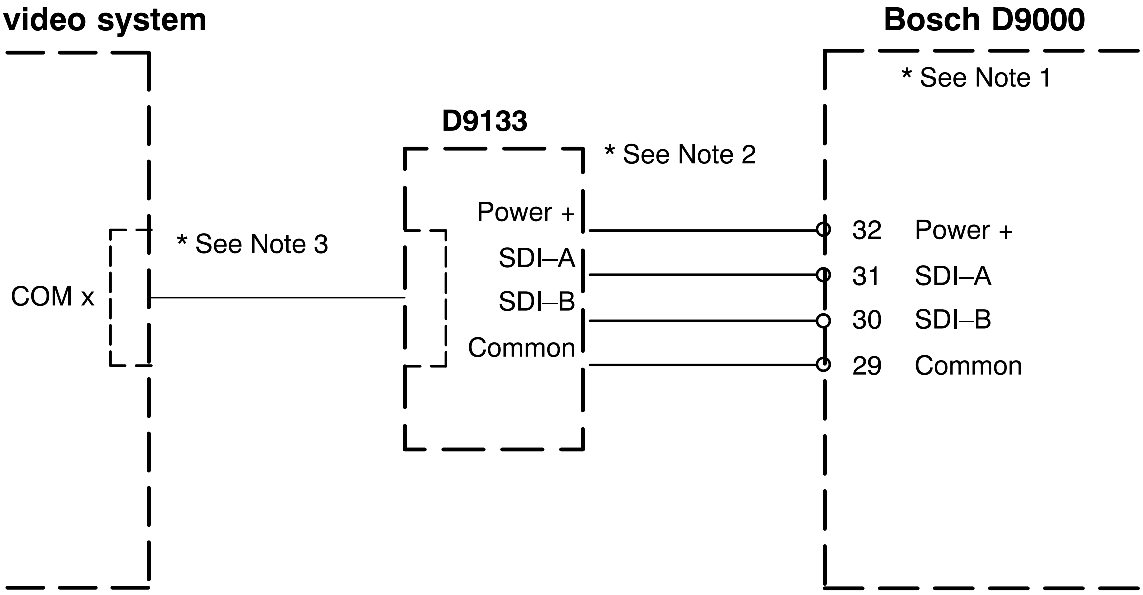


• 20 mA connection to UGM 2020 via UESS



Connections (continued)

4.18.12 Connecting to Bosch D9000 Series



The video system is triggering in case of
- Unacknowledged alarm point status
- Unacknowledged supervised point status
- Unacknowledged trouble point status

Note:

1. Panel firmware must be version 6.3 or higher. Refer to panel installation instructions for additional information. Some panel programming is required (see section on SDI Automation).
2. D9133 (not included) module must be set for adress 80. Only one D9133 per panel is allowed. Refer to D9133 installation instructions for additional information.
3. Connection of D9133 to DiBos is accomplished using a null modem cable ”DB9F” (not included). Additional programming is required in the DiBos to use the alarm panel for job activation. Refer to the installation instructions for DiBos, under the Section for Configuration of Security System inputs.

5 XP Administration

5.1 Changing from video system to XP administrator level

May only be executed by authorized personnel!

Proceed as follows in order to change from the video system to the XP administrator level.

1. End the operating procedure in the video system (”*System* → *Exit system*” menus).
2. In Windows® XP click the ”*Start* → *Log Off”* menu. The Windows log-off dialog will appear.
3. Press the right Shift key and click the *Log Off* button. Here, hold the right Shift key down until the Windows logon screen appears.
4. Log on with the following user name.
   - *AdministratorDe* for the German version of the operating system
   - *AdministratorEn* for the English version of the operating system
   - *AdministratorEs* for the Spanish version of the operating system
   - *AdministratorFr* for the French version of the operating system

   Please do not use the user *Administrator* any longer!
   For security reasons, you must ask the “Product Service Video” of the video system manufacturer for the password. Then, for security reasons, change this password.

5.2 Log on as Windows® XP user

To log on in Windows® XP as a user of the operating system, proceed as follows.

1. In Windows® XP click the ”*Start* → *Log Off”* menu. The Windows log-off dialog will appear.
2. The system will log on automatically as DiBos user.
   - *dibosDe* for the German version of the operating system
   - *dibosEn* for the English version of the operating system
   - *dibosEs* for the Spanish version of the operating system
   - *dibosFr* for the French version of the operating system

   For security reasons, you must ask the “Product Service Video” of the video system manufacturer for the password. Then, for security reasons, change this password.

Warning:

an automatic start, e.g. after a power failure, only occurs as preset user.

6 Configuration

If you are starting the video system for the first time, a dialog box appears with the following configuration possibility:

- **Basic configuration with the wizard**
  The basic configuration is intended for inexperienced users. With the help of a setup assistant, you will create a basic configuration of the system with a few clicks of the mouse. The system automatically recognizes the connected video hardware (cameras, grabber).
  If more extensive configuration is necessary, this occurs with the help of the standard (expert) configuration since the basic configuration is only called automatically on the first start of the system. If later you would like to go from the standard configuration to the basic configuration, this is only possible with a loss of the configuration data and the saved video images.
- **Use standard configuration program**
  The standard configuration (expert configuration) is intended for users who have a certain amount of experience with the system. If you select the standard configuration, you will see a dialog box “Setup Assistant Administrator” in which you must enter your name and password (you must use this name/password to log onto the system for the first time). After confirmation of your entries, you will reach the standard configuration.
  Proceed as described above by clicking the individual menu items and making the corresponding settings.

You will find operating instructions for both types of configuration-*online*, that is, directly in the system. For this call up the online help by pressing the “F1” key or clicking the “Help” button.

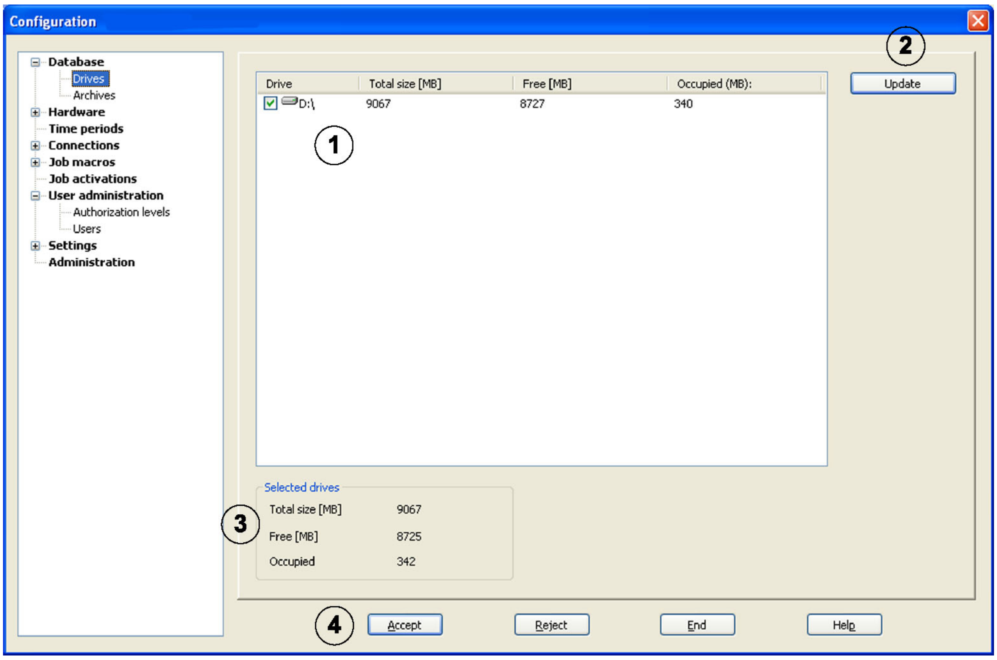
6.1 Basic configuration

For more information on this, please see Section 3.

6.2 Standard configuration (expert configuration)

6.2.1 Configuration Drives

(Database/drives menu)



Drive	Total size [MB]	Free [MB]	Occupied (MB):
☑ D:\	9067	8727	340

Selected drives

Total size [MB]	9067
Free [MB]	8725
Occupied	342

This dialog box shows you an overview of the hard drives and network drives available.

No.	Name	Description
1		The list box contains all hard drives and network drives that are known to the system at the start of configuration. The total size, the free memory capacity and the occupied memory capacity are shown in Mbytes. The drives that are listed can be activated or deactivated.
	☑ D:\	The drive is activated.
	□ D:\	The drive is not activated.
2	Update	If an additional drive is activated during the configuration, it can be accepted into the list box by clicking **update**.
3	Selected drives	The total size of the memory capacity, the free memory capacity and the occupied memory capacity are shown in Mbytes for the activated drives.
4	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

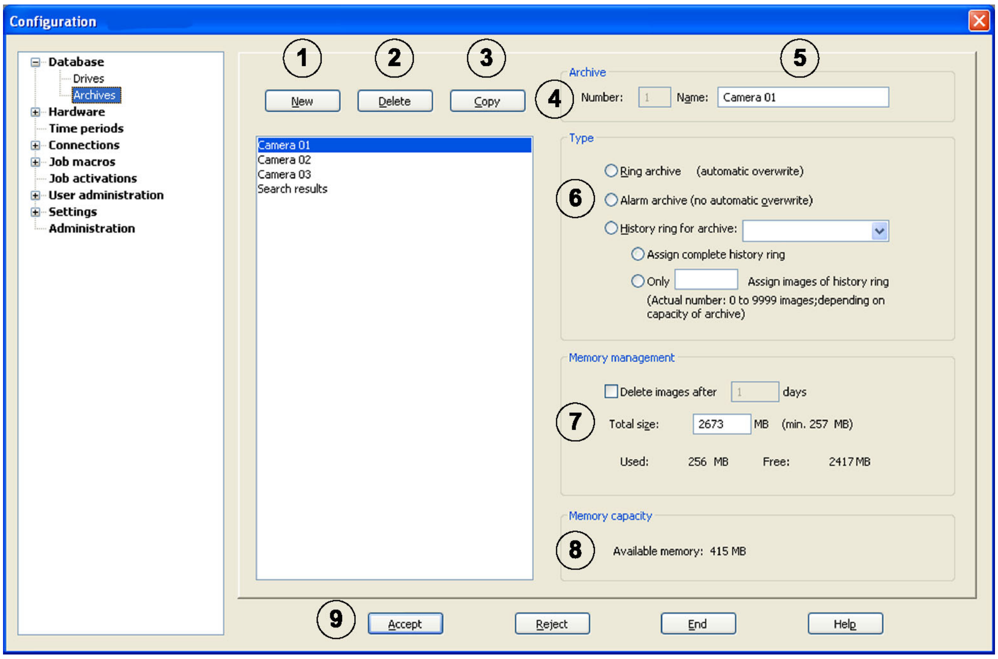
Note: **Several drives can be made available for archives. In this case, the archive images are evenly distributed amongst the activated drives.**

Note: **The external SCSI drives must be activated before starting up the PC.**

Configuration (continued)

6.2.2 Configuration Archives

(Database/archives menu)



Camera 01
Camera 02
Camera 03
Search results

Archive
Number: 1 Name: Camera 01

Type
○ Ring archive (automatic overwrite)
○ Alarm archive (no automatic overwrite)
○ History ring for archive:
○ Assign complete history ring
○ Only Assign images of history ring
(Actual number: 0 to 9999 images;depending on capacity of archive)

Memory management
□ Delete images after 1 days
Total size: 2673 MB (min. 257 MB)
Used: 256 MB Free: 2417 MB

Memory capacity
Available memory: 415 MB

The archives presented in the overview box are located on the activated drives. The archives partition the drives into individual areas so that the saved images can be found more quickly during image searches. Images and search results are stored in the archives.

No.	Name	Description
1	New	Creates a new archive. Click on **New** and designate the name of the archive in the input box **Name** (5**)**
2	Delete	Deletes an existing archive. Choose an archive in the list box and click on **Delete**. The archive is deleted when you confirm the warning message.
3	Copy	Copies an existing archive. Choose an archive in the list box and click on **Copy**. The archive is copied and can be adapted quickly.
4	Archive Number	The system assigns a (system) number to the archive. It is used for internal identification in case there are archives with the same name. Each archive receives the next highest number or the next number in the sequence if an archive is deleted. Search results always have the number 255.
5	Archive Name	Displays the name of the archive (can be changed).

Configuration (continued)

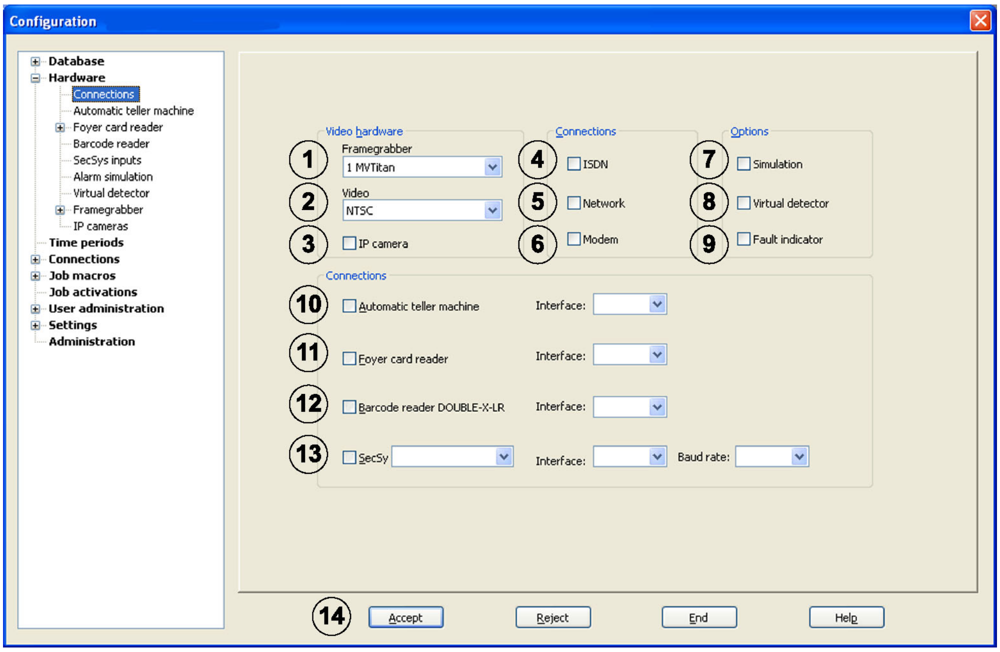
6	Type	Select an archive type. **For most applications, it is advisable to set up a separate archive for each camera. This enables a fast search in the image archive later.**
	Ring archive	**Ring archive**: The images are saved one after the other. If the ring archive is full, the storage process begins all over again. The oldest images are overwritten. A history ring can be assigned to a ring archive so that the images that triggered the alarm are also saved.
	Alarm archive	**Alarm archive**: The alarm archive contains the images recorded after triggering of the alarm. The alarm archive is not overwritten. A history ring can be assigned to an alarm archive so that the images that triggered the alarm are also saved.
	History ring	**History ring**: The images are saved one after the other. If the history ring is full, the storage process begins all over again. The oldest images are overwritten. A history ring must be assigned to a ring or alarm archive. Because of the way the history ring works, no rapidly repeating triggers may be allocated to it, as is the case for example with sensor cameras, PIR movement detectors and door contacts. The usage of pre–alarm images is recommended for rapidly repeating triggers. Pre–alarm images can be set–up in **Job macros/save**.
	History ring for archive x:	Select the archive to which the history ring should be assigned.
	Assign complete history ring	The history ring will be assigned completely to an alarm or ring archive.
	only assign x history ring images	Only the number of images entered will be assigned to an alarm or ring archive.
		Notes: The purpose of the history ring is to save a detector's images only when at rest. If a significant event occurs, e.g. a hold–up alarm, the images from the history ring are copied into the assigned alarm or ring archive. This process enables a quick reconstruction of the event because the alarm archive assigned contains the images that triggered the alarm as well as the images after the hold–up.
7	Memory management Delete images after x days	If necessary, activate function and input number of days. Deletion always occurs at midnight. "1" means that the saved images will still be deleted at midnight on that same day.
	Total size	Total size of the archive in MB. The used and free memory space in the archive is immediately shown underneath.

Configuration (continued)

	Used	The available memory is indicated. If the total of all configured archives exceeds 90% of the entire available memory, a message appears. A reserve of at least 10% must be remain.
8	Memory capacity	System memory available
9	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

6.2.3 Configuration of hardware connections

(Hardware/connections menu)



Framegrabber: 1 MVTitan

Video: NTSC

You can set–up numerous hardware options in this dialog box. Select the hardware either by clicking on the arrow pointing downwards and making the selection or by activating—clicking—the relevant control box in front of the hardware. Click once more for deactivation.

☑	Control box is activated. Hardware is selected.
□	Control box is not activated. Hardware is not selected.

The settings on this hardware page should not normally be changed unless there are expansions. If changes are actually required, they can only be carried out by authorized persons or after consultation with the technical support department.

No.	Name	Description
1	Framegrabber	1 MVTitan: The system contains one MVTitan Grabber. 2 MVTitan: The system contains two MVTitan Grabbers. 1 Sigma: The system contains one MVSigma Grabber.
2	Video signal	PAL or NTSC
3	IP cameras *	A maximum of 16 network cameras can be connected.

* See section 6.2.15 for additional information. Contact Bosch Security for an IP camera compatibility list.

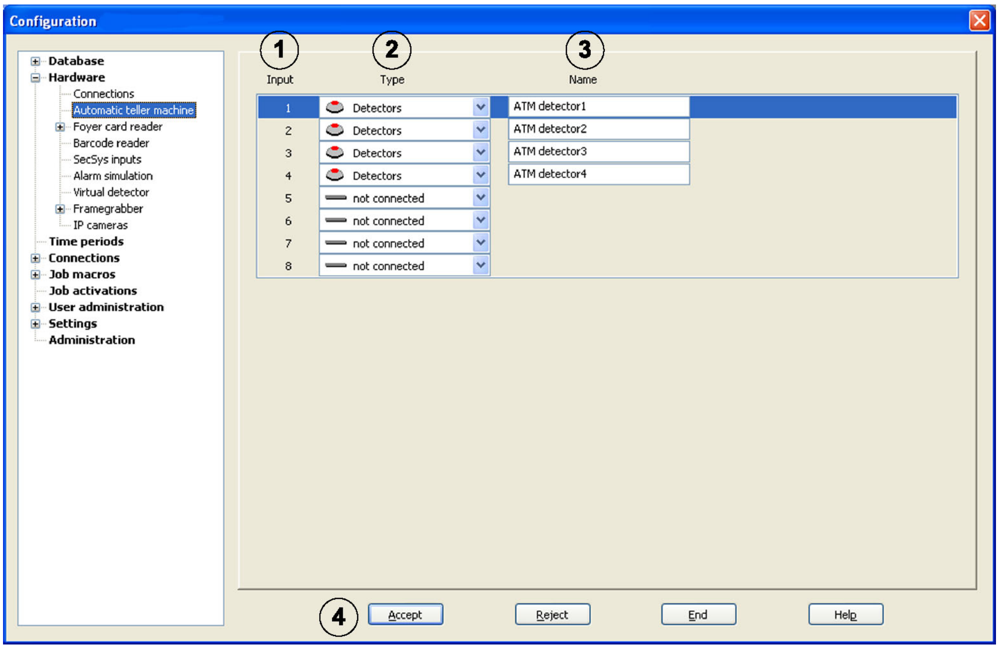
Configuration (continued)

4	ISDN*	When connecting to other systems of this type via ISDN
5	Network	When connecting to other systems of this type via a network
6	Modem*	For modem connections A RAS capable modem must be connected and RAS service must be installed.
7	Simulation	Support for four alarm inputs that can be simulated for triggering test alarms or for the application of a job such as “burning a CD” for example.
8	Virtual detector	The virtual detectors offer the same functionalities as the other detectors in the system. They provide inputs that can be used to carry out jobs in the video system. In contrast to other units, virtual detectors are not physical hardware. Virtual detectors can be used by other software programs to communicate with the video system. A maximum of 32 virtual detectors are available.
9	Fault indicator	For internal error identifier. The fault indicator always uses relay 4 of the 1st MVTitan. The events that lead to triggering of the fault indicator can be found in chapter 4.10.
10	Automatic teller machine*	Connection of a maximum of 4 automatic teller machines each with 2 alarm inputs.
11	Foyer card reader*	Connection of a maximum of 4 foyer card readers.
12	Barcode reader*	Connection of one barcode reader.
13	SecSys *	Connection of a security system.
14	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

* Option

6.2.4 Configuration of automatic teller machine (option)

(Hardware/automatic teller machine menu)



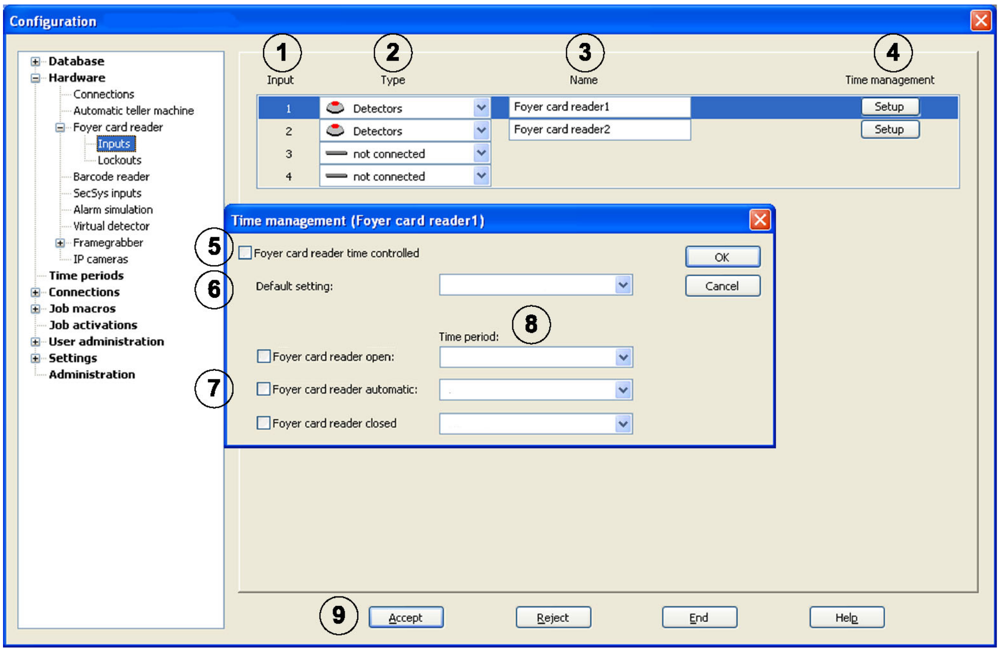
Input	Type	Name
1	Detectors	ATM detector1
2	Detectors	ATM detector2
3	Detectors	ATM detector3
4	Detectors	ATM detector4
5	not connected	
6	not connected	
7	not connected	
8	not connected	

A maximum of 4 automatic teller machines each with 2 alarm inputs can be connected (must be activated under Hardware/Connections). These inputs, which have to be supported by the video system, must be configured as detectors.

No.	Name	Description
1	Input	Click on the relevant ATM input. The selected line is activated.
2	Type Detectors not connected	Click on the arrow pointing downwards in the **Type** column and select whether a detector (contact) should be configured or not. Input is interpreted. Input is not interpreted. Assignment of the inputs: Input 1 + 2 = automatic teller machine 1 Input 3 +4 = automatic teller machine 2 Input 5 +6 = automatic teller machine 3 Input 7 +8 = automatic teller machine 4 Inputs 1, 3, 5, 7 normally activate the portrait camera and inputs 2, 4, 6, 8 activate the money withdrawal camera.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen. The alarm input is now known to the system under this name.
4	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

6.2.5 Configuration of the foyer card reader inputs (option)

(Hardware/foyer card reader/inputs menu)



Input	Type	Name	Time management
1	Detectors	Foyer card reader1	Setup
2	Detectors	Foyer card reader2	Setup
3	not connected		
4	not connected		

□ Foyer card reader time controlled

Default setting:

Time period:

□ Foyer card reader open:

□ Foyer card reader automatic:

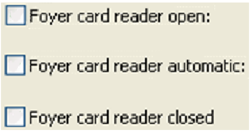
□ Foyer card reader closed

A maximum of 4 foyer card readers can be connected, with each foyer card reader supporting one alarm input (must be activated under Hardware/Connections). These inputs need to be configured as detectors.

The number of foyer card readers configured must match the number of foyer card readers connected.

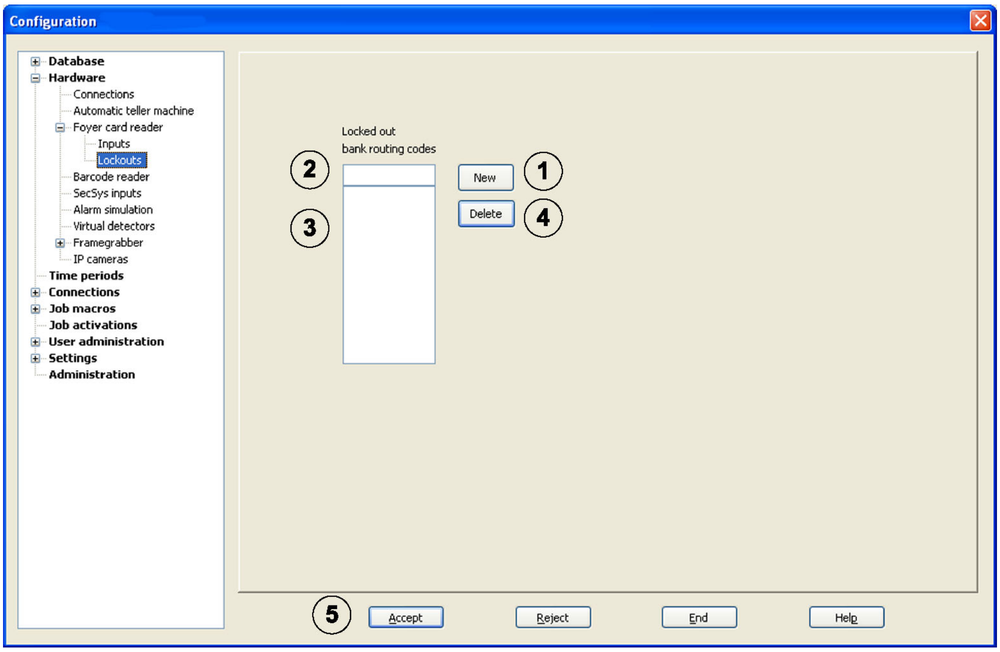
No.	Name	Description
1	Input	Click on the corresponding input. The selected line is activated.
2	Type Detectors not connected	Click on the arrow pointing downwards in the **Type** column and select whether the foyer card reader should be activated or not. A foyer card reader will be connected to the input. No foyer card reader will be connected to the input.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen. The input is now known to the system under this name.
4	Time management Setup	Click on **Setup** in the **Time management** column if you want to enter time management information for the foyer card reader. If not, then continue with item 9. **Note:** Only possible if a time period was specified on the **Time periods** menu.

Configuration (continued)

5	Foyer card reader time controlled	Activate **Foyer card reader time controlled** and implement the following settings.
6	Default setting	Click on the arrow pointing downwards in the **Default setting** list box and select the default setting the foyer card reader should have.
	Foyer card reader open	– The foyer is always open.
	Foyer card reader automatic	– Access is only valid with an EC card or credit card. Cards from specified banks can be locked out here.
	Foyer card reader closed	– The foyer is always closed.
7	 □ Foyer card reader open: □ Foyer card reader automatic: □ Foyer card reader closed	You have determined the default setting of the foyer card reader in the preceding item. If necessary, activate the corresponding item as well if this default setting needs to be time–limited.
8	Time period	Enter the time period within which the time limitation is to be in effect (q. v. configuring Time periods).
9	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

6.2.6 Configuration of the foyer–card reader lockouts (option)

(Hardware/foyer card reader/lockouts menu)



In this dialog box it is possible to lockout certain bank routing codes, i.e. EC cards that correspond to the locked out entries have no access authorization. Access is denied by the foyer–card reader. The basic setting of the foyer–card reader must be set to “Foyer–card reader automatic.”

Entering lockouts

No.	Name	Description
1	New	Click on **New**.
2	Locked bank reference numbers	Enter the bank reference number to be locked in the text box. It is possible to use wildcards (? or *) in any combination. For this, heed the following note and the examples. Once entered, the bank reference number is included in the list field (3).
5	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

Deleting lockouts

No.	Name	Description
3	Locked bank reference numbers	Select the lockout you wish to delete from the list box.
4	Delete	Click on **Delete**. The lockout is deleted.
5	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Note:
With the wildcards, you must heed the following meanings:

- ? Any character or no character may appear at the exact position of the question mark.
- * A sequence of any characters (one character and more) or no character may appear at the exact position of the asterisk.

Example:

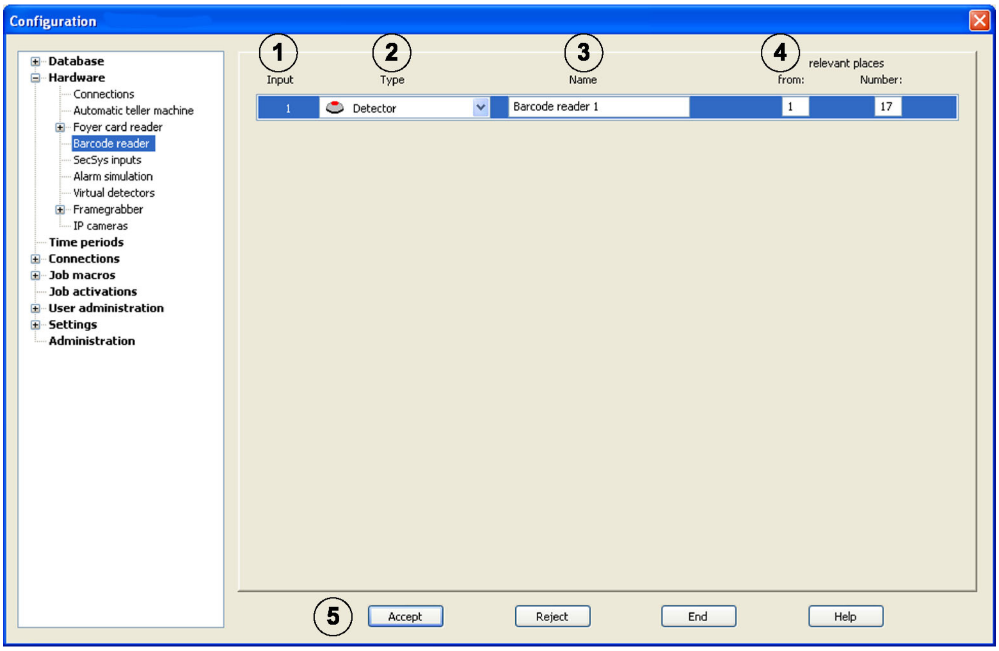
12**?**78*4	locks the bank reference code	12**1**78**3**4 or 12**0**78**12345667**4 or 12**8**784 (if for * no character) etc.
43*	Locks out the bank reference code	43 or 43**6574** or etc.

Exception:

*	locks **all** bank reference codes

6.2.7 Configuration of barcode reader (option)

(Hardware/barcode reader menu)



Input	Type	Name	relevant places from:	Number:
1	Detector	Barcode reader 1	1	17

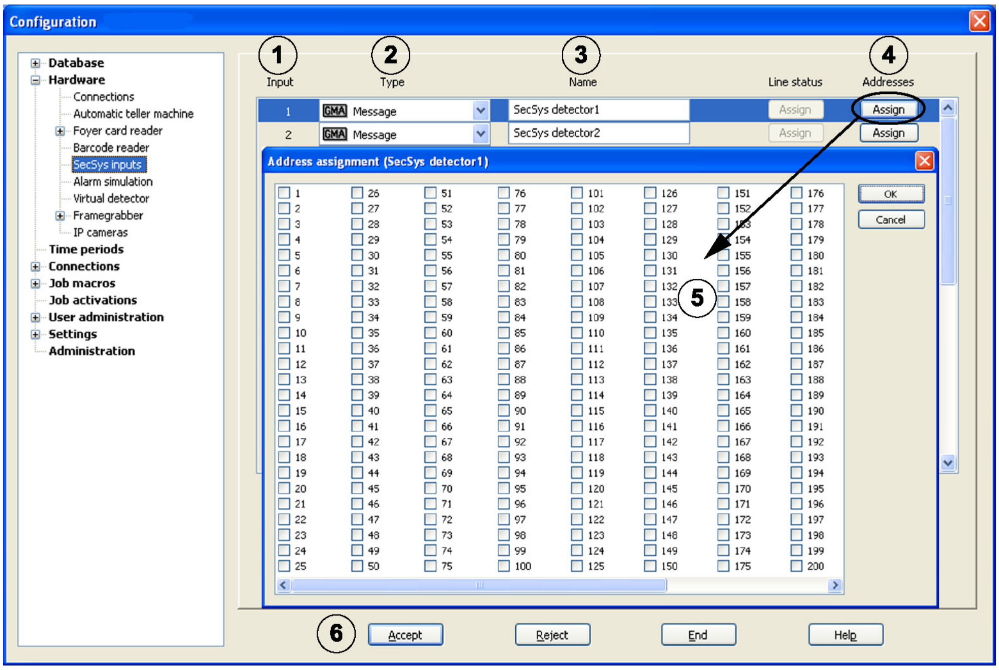
You can connect a barcode reader (must be activated under Hardware/Connections). The barcode reader supports the output of a scanner. This input, which is supported by the video system, needs to be configured as a detector.

No.	Name	Description
1	Input	Click the input of the barcode reader. The line is activated.
2	Type	Click on the arrow pointing downwards in the **Type** column and select whether the barcode reader should be activated or not.
	Melder	A barcode reader will be connected to the input.
	nicht belegt	No barcode reader will be connected to the input.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen. The input is now known to the system under this name.
4	relevant places	
	from	– Enter the position of the barcode number here from where the barcode reader is to begin checking (counting starts from the left).
	Number	– Enter the number of places to be checked.
5	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

6.2.8 Configuration of security system inputs for Bosch D9000 Series (option)

(Hardware/SecSys inputs menu)



Input	Type	Name	Line status	Addresses
1	GMA Message	SecSys detector1	Assign	Assign
2	GMA Message	SecSys detector2	Assign	Assign

□ 1	□ 26	□ 51	□ 76	□ 101	□ 126	□ 151	□ 176
□ 2	□ 27	□ 52	□ 77	□ 102	□ 127	□ 152	□ 177
□ 3	□ 28	□ 53	□ 78	□ 103	□ 128	□ 153	□ 178
□ 4	□ 29	□ 54	□ 79	□ 104	□ 129	□ 154	□ 179
□ 5	□ 30	□ 55	□ 80	□ 105	□ 130	□ 155	□ 180
□ 6	□ 31	□ 56	□ 81	□ 106	□ 131	□ 156	□ 181
□ 7	□ 32	□ 57	□ 82	□ 107	□ 132	□ 157	□ 182
□ 8	□ 33	□ 58	□ 83	□ 108	□ 133	□ 158	□ 183
□ 9	□ 34	□ 59	□ 84	□ 109	□ 134	□ 159	□ 184
□ 10	□ 35	□ 60	□ 85	□ 110	□ 135	□ 160	□ 185
□ 11	□ 36	□ 61	□ 86	□ 111	□ 136	□ 161	□ 186
□ 12	□ 37	□ 62	□ 87	□ 112	□ 137	□ 162	□ 187
□ 13	□ 38	□ 63	□ 88	□ 113	□ 138	□ 163	□ 188
□ 14	□ 39	□ 64	□ 89	□ 114	□ 139	□ 164	□ 189
□ 15	□ 40	□ 65	□ 90	□ 115	□ 140	□ 165	□ 190
□ 16	□ 41	□ 66	□ 91	□ 116	□ 141	□ 166	□ 191
□ 17	□ 42	□ 67	□ 92	□ 117	□ 142	□ 167	□ 192
□ 18	□ 43	□ 68	□ 93	□ 118	□ 143	□ 168	□ 193
□ 19	□ 44	□ 69	□ 94	□ 119	□ 144	□ 169	□ 194
□ 20	□ 45	□ 70	□ 95	□ 120	□ 145	□ 170	□ 195
□ 21	□ 46	□ 71	□ 96	□ 121	□ 146	□ 171	□ 196
□ 22	□ 47	□ 72	□ 97	□ 122	□ 147	□ 172	□ 197
□ 23	□ 48	□ 73	□ 98	□ 123	□ 148	□ 173	□ 198
□ 24	□ 49	□ 74	□ 99	□ 124	□ 149	□ 174	□ 199
□ 25	□ 50	□ 75	□ 100	□ 125	□ 150	□ 175	□ 200

The serial connection of a Bosch D9000 Series SecSys allows for many SecSys inputs to be assigned to each video system input.

Note: Function must be activated under Hardware/Connections.

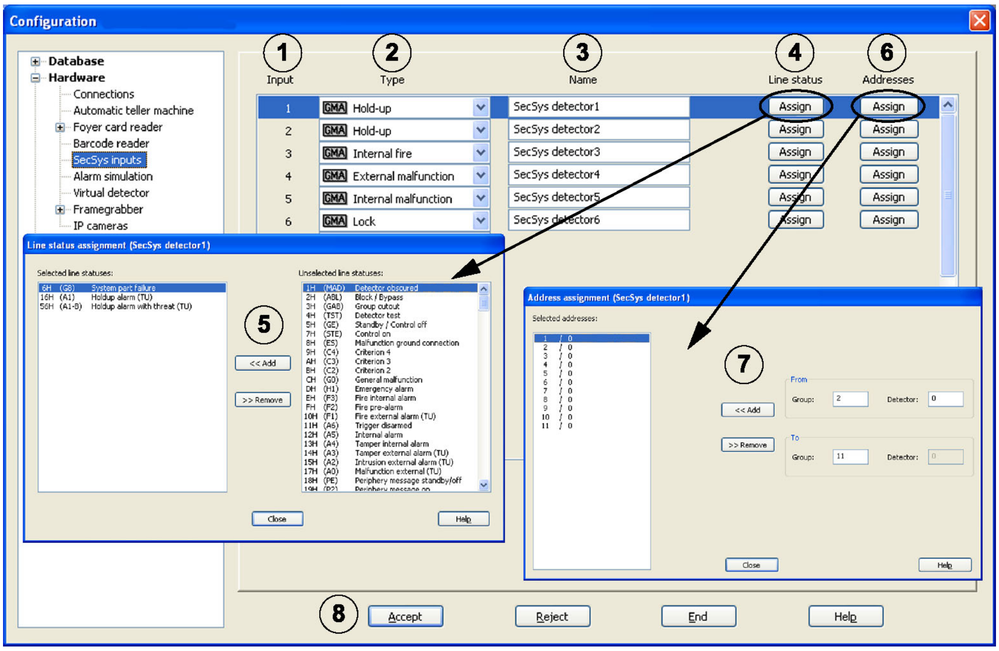
No.	Name	Description
1	Input	Click on the corresponding input. The selected line is activated.
2	Type	Click on the arrow pointing downwards in the **Type** column and select whether the input should be configured or not.
	GMA Message	Input is interpreted.
	not connected	Input is not interpreted.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen. The input is now known to the system under this name.
4	Addresses Assign	Click on **Assign**in the column **Addresses** if you would like to assign certain SecSys addresses to the input.

Configuration (continued)

5	“Assignment of addresses” dialog box	Select the SecSys addresses that you would like to assign to the input and click **OK**.
	☑	The address is assigned to the input.
	□	The address is not assigned to the input.
6	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

6.2.9 Configuration of security system inputs for Bosch alarm systems – excluding D9000 Series (option)

(Hardware/SecSys inputs menu)



Input	Type	Name	Line status	Addresses
1	GMA Hold-up	SecSys detector1	Assign	Assign
2	GMA Hold-up	SecSys detector2	Assign	Assign
3	GMA Internal fire	SecSys detector3	Assign	Assign
4	GMA External malfunction	SecSys detector4	Assign	Assign
5	GMA Internal malfunction	SecSys detector5	Assign	Assign
6	GMA Lock	SecSys detector6	Assign	Assign

Line status assignment (SecSys detector1)

Selected line statuses:

```
6H   (G8)    System part failure
16H  (A1)    Holdup alarm (TU)
56H  (A1-B)  Holdup alarm with threat (TU)
```

<< Add >> Remove

Unselected line statuses:

```
1H   (MAD)   Detector obscured
2H   (ABL)   Block / Bypass
3H   (GAB)   Group cutout
4H   (TST)   Detector test
5H   (GE)    Standby / Control off
7H   (STE)   Control on
8H   (ES)    Malfunction ground connection
9H   (C4)    Criterion 4
AH   (C3)    Criterion 3
BH   (C2)    Criterion 2
CH   (G0)    General malfunction
DH   (H1)    Emergency alarm
EH   (F3)    Fire internal alarm
FH   (F2)    Fire pre-alarm
10H  (F1)    Fire external alarm (TU)
11H  (A6)    Trigger disarmed
12H  (A5)    Internal alarm
13H  (A4)    Tamper internal alarm
14H  (A3)    Tamper external alarm (TU)
15H  (A2)    Intrusion external alarm (TU)
17H  (A0)    Malfunction external (TU)
18H  (PE)    Periphery message standby/off
19H  (P2)    Periphery message on
```

Close Help

Address assignment (SecSys detector1)

Selected addresses:

```
1  / 0
2  / 0
3  / 0
4  / 0
5  / 0
6  / 0
7  / 0
8  / 0
9  / 0
10 / 0
11 / 0
```

<< Add >> Remove

From – Group: 2 Detector: 0

To – Group: 11 Detector: 0

Close Help

The serial connection of a SecSys allows up to 16 input types to be defined which, when they occur, trigger an alarm in the system.

Each input type is assigned line statuses as the default, but these can be adapted for specific projects in LSN security systems. In addition, security system addresses can also be assigned to any input type.

Note: Function must be activated under Hardware/Connections.
LSN security systems are not yet available in the United States.

No.	Name	Description
1	Input	Click on the corresponding input. The selected line is activated.
2	Type	Click on the arrow pointing downwards in the **Type** column and select the input type.
	GMA Hold-up	The input type, e.g. hold–up, is activated.
	not connected	The input type is not activated. Note: Certain line statuses are assigned to each input as the default. This assignment can be changed for LSN security systems.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen. The input is now known to the system under this name.

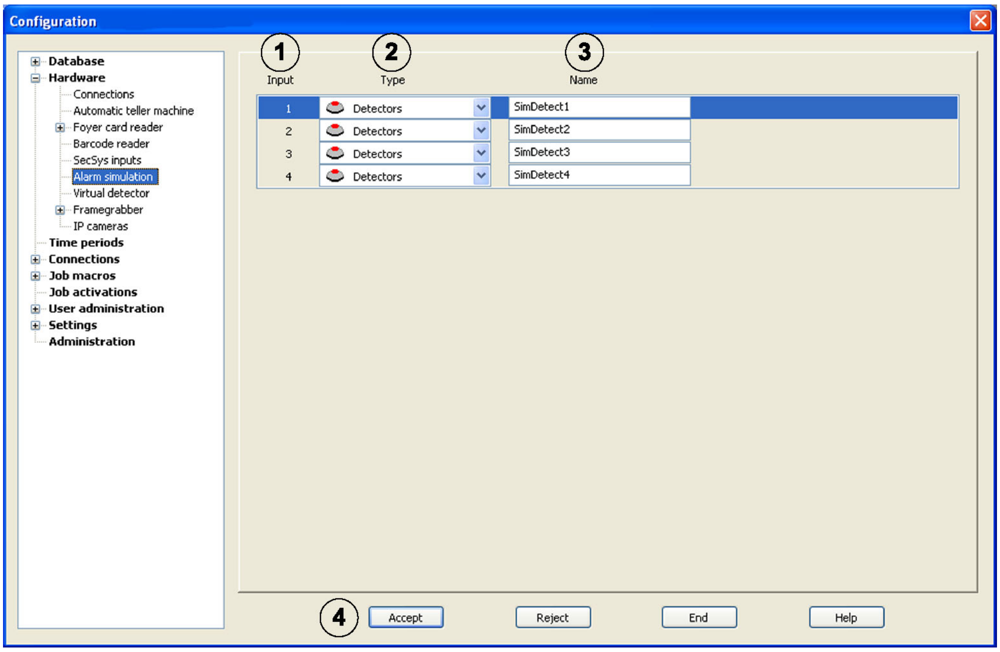
Configuration (continued)

4	Line status	Click on **Assign**, in the **Line status** column if you would like to change or view the standard assignment of the line status (only for LSN security systems).
5	"Assignment of line statuses" dialog box	To add line statuses, select the line status on the right and click on **Add**. To remove line statuses, select the line status on the left and click on **Remove**. Confirm with **Close**. The line statuses on the left are assigned to the SecSys input.
6	Addresses	Click on **Assign**in the column **Addresses** if you would like to assign certain SecSys addresses to the input.
7	"Assignment of addresses" dialog box	To add addresses, put the addresses into the input boxes **from group ... detectors ..** and **to group .. detectors ..** and click on **Add**. To remove addresses, select the addresses to be removed on the left and click on **Remove**. Confirm with **Close**. The addresses on the left are assigned to the SecSys input.
8	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

6.2.10 Configuration of alarm simulation

(Hardware/alarm simulation menu)



Input	Type	Name
1	Detectors	SimDetect1
2	Detectors	SimDetect2
3	Detectors	SimDetect3
4	Detectors	SimDetect4

The video system supports 4 alarm inputs, which can be simulated for triggering test alarms.

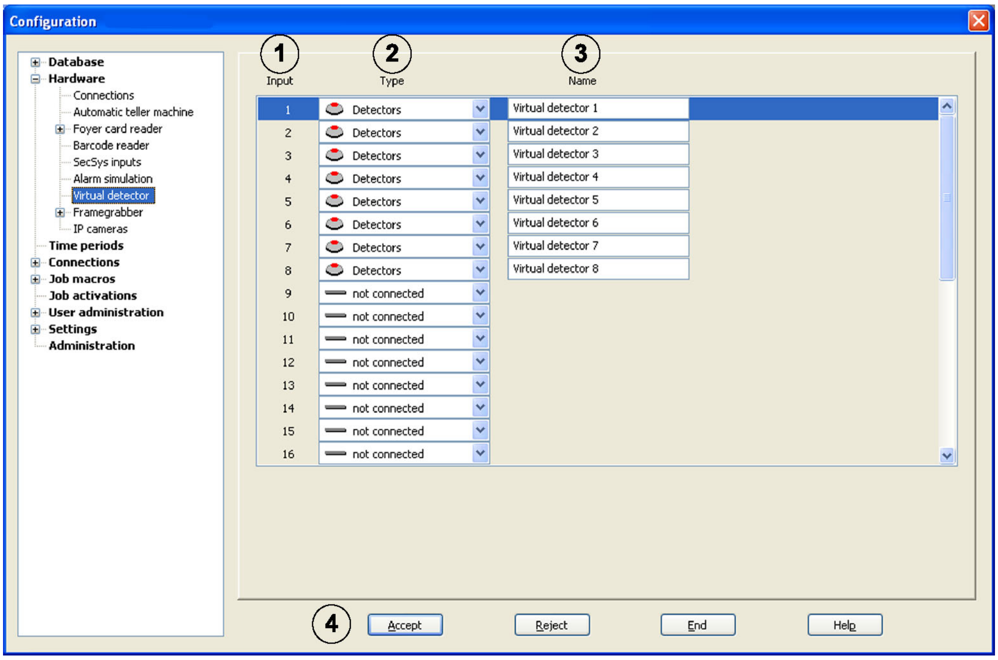
Note: Function must be activated under Hardware/Connections.

No.	Name	Description
1	Input	Click on the corresponding input. The selected line is activated. Please ensure that input 1 corresponds to the button Alarm 1, input 2 corresponds to the button Alarm 2, etc.
2	Type	Click on the arrow pointing downwards in the **Type** column and select whether the test alarm input should be configured or not.
	Detectors	The input should be used for alarm simulation.
	not connected	The input should not be used for alarm simulation.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen.
4	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

6.2.11 Configuration of virtual detectors

(Hardware/virtual detector menu)



Input	Type	Name
1	Detectors	Virtual detector 1
2	Detectors	Virtual detector 2
3	Detectors	Virtual detector 3
4	Detectors	Virtual detector 4
5	Detectors	Virtual detector 5
6	Detectors	Virtual detector 6
7	Detectors	Virtual detector 7
8	Detectors	Virtual detector 8
9	not connected	
10	not connected	
11	not connected	
12	not connected	
13	not connected	
14	not connected	
15	not connected	
16	not connected	

The virtual detectors offer the same functionalities as the other detectors in the system. They provide inputs that can be used to carry out jobs in the video system. In contrast to other units, virtual detectors are not physical hardware. Virtual detectors can be used by other software programs to communicate with the video system. A maximum of 32 virtual detectors is available.

Note: Function must be activated under Hardware/Connections.

No.	Name	Description
1	Input	Click on the corresponding input. The selected line is activated.
2	Type Detectors not connected	Click on the arrow pointing downwards in the **Type** column and select whether the input should be configured or not. The input is to be used as a virtual detector. The input is not to be used as a virtual detector.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen.
4	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

Note: External software can communicate with the virtual detectors via a COM interface (COM stands for Component Object Model).
For a simple connection, please see a type library (VirtualInputs.tlb) in the installation directory of the video system.

The COM interface provides the following functions:

```
HRESULT SwitchOn(SHORT inputNr);
HRESULT SwitchOnWithData(SHORT inputNr,VARIANT vZeit, VARIANT vTransactionNr, VARIANT vATMNr,
                         VARIANT vBankCode, VARIANT vAccountNr, VARIANT vAmount, VARIANT
                         vAlarmId);
HRESULT SwitchOnWithAlarmId(SHORT inputNr, VARIANT vAlarmId);
HRESULT SwitchOff(SHORT inputNr);
```

The data types have the following format:

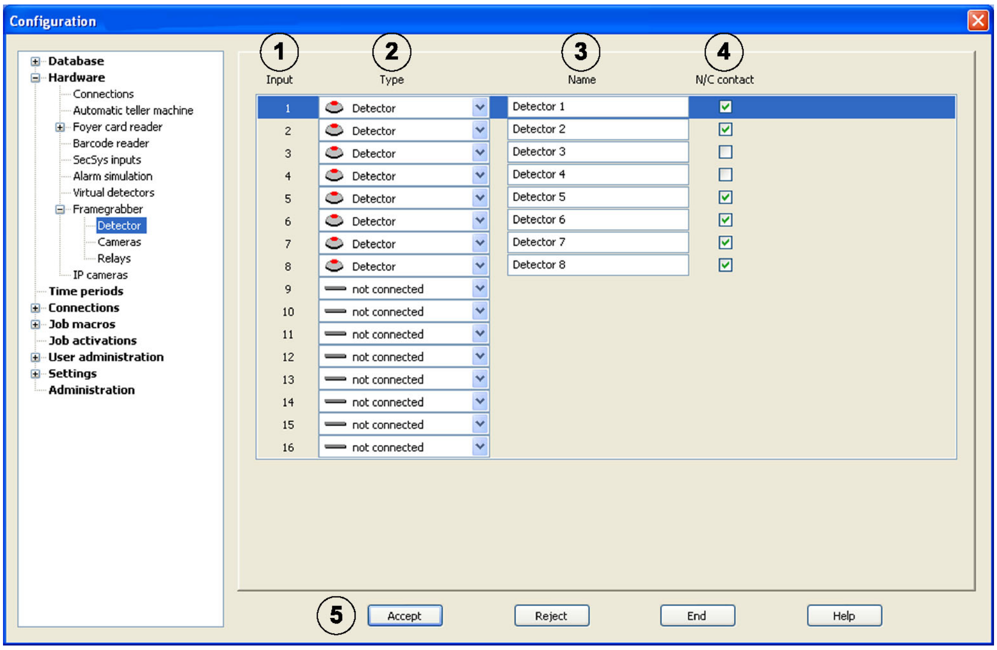
Name	Type	Length	Application
inputNr	SHORT		Detector number whose status is to be changed.
vZeit	VARIANT (String/number)	4	Indicates the time from unsynchronized external systems (e.g. GAA). (hh:mm)
vTransactionNr	VARIANT (String/number)	4	Transaction number
vATMNr	VARIANT (String/number)	6	Automated teller machine number
vBankCode	VARIANT (String/number)	8	Bank routing number
vAccountNr	VARIANT (String/number)	10	Account number
vAmount	VARIANT (String/number)	4	Amount (entire number)
vAlarmId	VARIANT (String/number)	8	Alarm Id

Searches for these boxes can be done using the browser interface or the search dialog in the image archive.

Example: Virtual detector via Web browser
http://”IP adress”/VirtualInputSrv.asp?inputNr=”x”&action=on

6.2.12 Configuration of detector inputs

(Hardware/Frame grabber/Detector menu



Input	Type	Name	N/C contact
1	Detector	Detector 1	☑
2	Detector	Detector 2	☑
3	Detector	Detector 3	☐
4	Detector	Detector 4	☐
5	Detector	Detector 5	☑
6	Detector	Detector 6	☑
7	Detector	Detector 7	☑
8	Detector	Detector 8	☑
9	not connected		
10	not connected		
11	not connected		
12	not connected		
13	not connected		
14	not connected		
15	not connected		
16	not connected		

With this dialog box you can activate and deactivate the contact inputs of the grabber card and select the stable state. A maximum of 8 or 16 contact inputs can be connected to each MVTitan grabber card and a maximum of 5 contact inputs can be connected to each MVSigma grabber card. A maximum of 2 MVTitan or a maximum of 1 MVSigma can be installed.

Note: If a sensor camera is configured, the associated detector input is used as a sensor input. The detector input is no longer available as an alarm input.

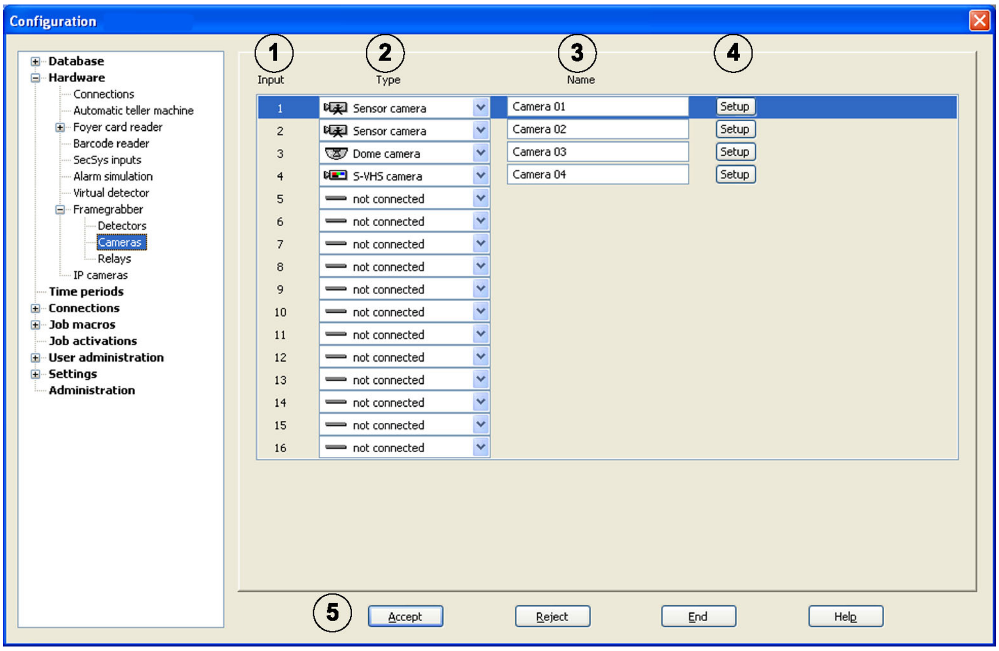
No.	Name	Description
1	Input	Click on the corresponding input. The selected line is activated.
2	Type Detectors ▾ not connected ▾	Click on the arrow pointing downwards in the **Type** column and select whether the input should be configured or not. Input is interpreted as an alarm input. Input is not interpreted as an alarm input.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen.

Configuration (continued)

4	Open contact	Determine whether the alarm input should be an open or closed contact.
	☑	The input is an open contact.
	□	The input is a closed contact.
5	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

6.2.13 Configuration of cameras

(Hardware/Frame grabber/camera menu)



Input	Type	Name	
1	Sensor camera	Camera 01	Setup
2	Sensor camera	Camera 02	Setup
3	Dome camera	Camera 03	Setup
4	S-VHS camera	Camera 04	Setup
5	not connected		
6	not connected		
7	not connected		
8	not connected		
9	not connected		
10	not connected		
11	not connected		
12	not connected		
13	not connected		
14	not connected		
15	not connected		
16	not connected		

With this dialog box you can select which camera you would like to activate and which camera type it should be.
A maximum of 8 or 16 cameras can be connected to each MVTitan grabber card and a maximum of 4 cameras can be connected to each MVSigma grabber card. A maximum of 2 MVTitan or a maximum of 1 MVSigma can be installed.

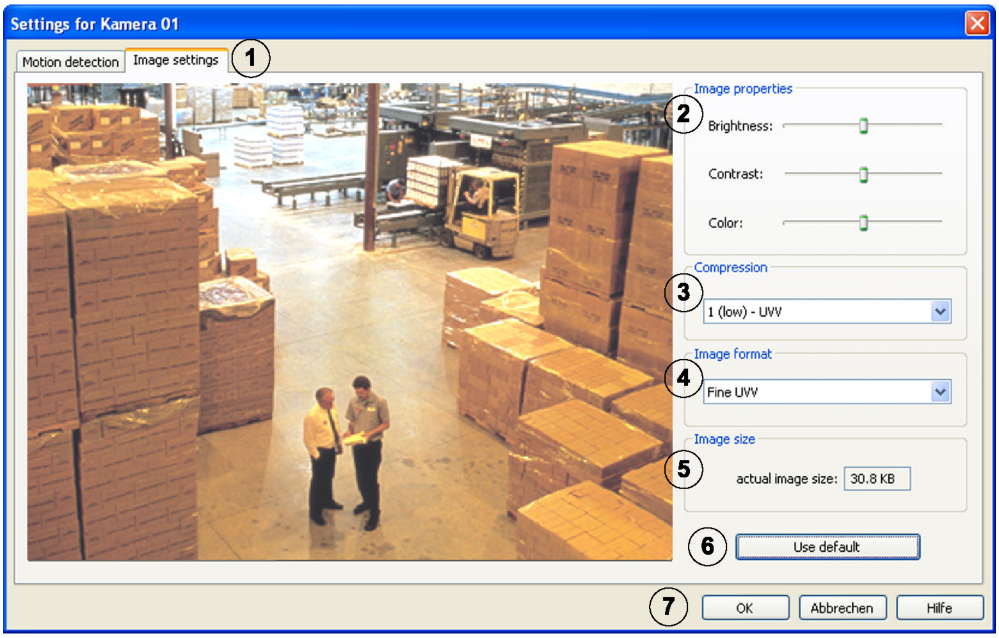
No.	Name	Description
1	Input	Click on the corresponding camera input. The selected line is activated.
2	Type	Click on the arrow pointing downwards in the **Type** column and select the camera type. You can choose from: PAL camera, SVHS camera, sensor camera, or dome camera. **Information regarding the SVHS cameras:** Each SVHS camera uses 2 inputs. The layout of the inputs can be seen in chapter 4.1. **Information concerning sensor cameras:** Each sensor camera uses one detector input in the **Frame grabber/detector** menu; e.g. detector input 2 is automatically used when the sensor camera has been configured to input 2. This means that when all cameras are configured as sensor cameras, physical contact is no longer available.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen.

Configuration (continued)

4	Setup	These settings can be set individually for each camera. They will remain saved until a change is carried out. Click on **Setup** to do the following: – change the image settings such as brightness, contrast, color and compression for all camera types; – in addition with sensor cameras the areas to be monitored must be drawn in and the sensitivity set – and implement the interface settings, camera positions and camera controls for dome cameras. The individual setup settings are explained in a subsequent section.
5	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

Image settings for all camera types

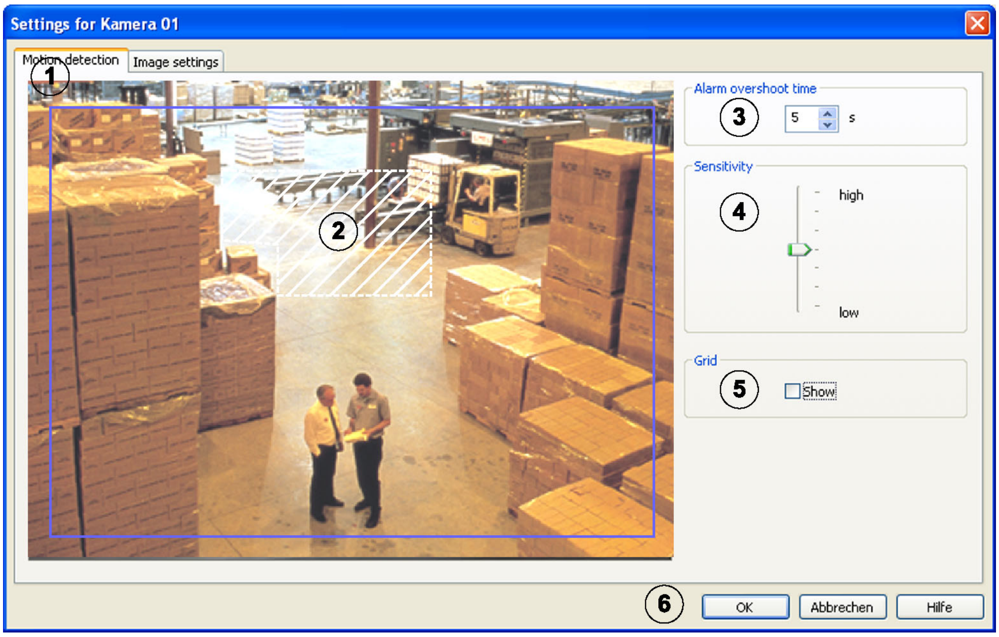


Implement the setting for each camera as required.

No.	Name	Description
1	Image settings	Click on **Image settings**.
2	Image properties	Set the brightness, contrast and color. You can view the result of the setting in the camera image next to it.
3	Compression	Set the compression here. Values between 1 and 5 are possible, whereby 1 is the lowest compression (that is, the best image quality) and 5 the highest compression (that is, the worst image quality).
4	Image format	Set the resolution. You can choose between fine and coarse. Only every second pixel (quarter image) is used for coarse resolution.
5	Image size	The image size is displayed here. It is dependent on the previously selected settings.
6	Use default	Click on **Use default** when you would like to call up the default settings. Default: Average for brightness, contrast and color. 1 (low) for compression. Fine for image format.
7	OK	Click **OK** to confirm the entries.

Configuration (continued)

Set the monitoring area for the sensor camera (movement detection)



Implement the setting for each camera as required.

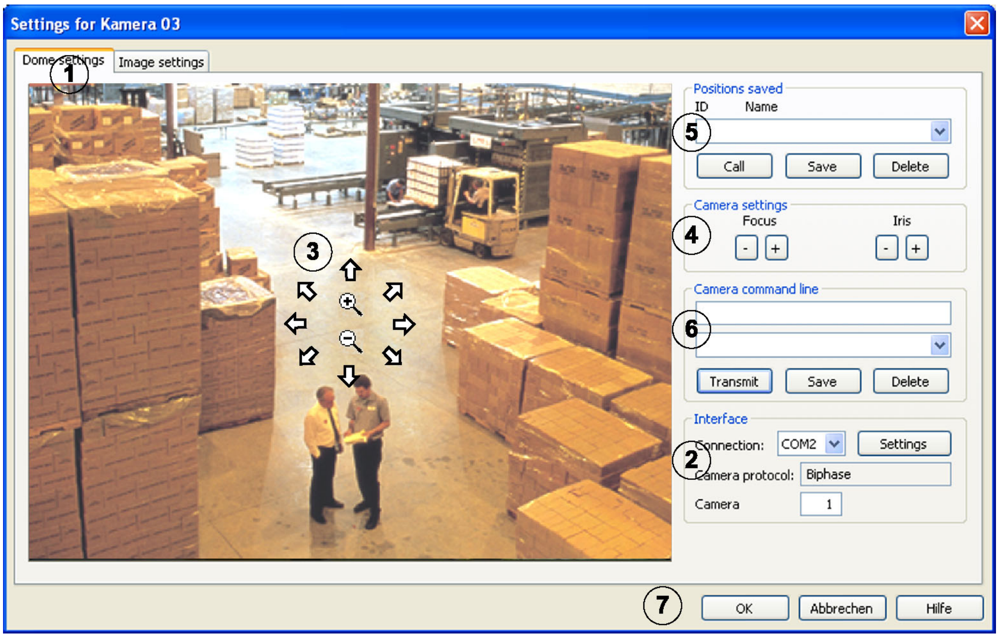
No.	Name	Description
1	Motion detection	Click on **Motion detection**. The entire image content within the blue area is sensitive at first; i.e. content is monitored for movement. If you want to limit the area to be monitored, carry out the next step.
2	Within the blue area Clicking with the left mouse button or Dragging an area with the left mouse button pressed down Clicking with the right mouse button or Dragging an area with the right mouse button pressed down	A minus sign appears next to the mouse cursor, which indicates that the selected area is not sensitive and thus not evaluated upon movement detection. **Non–sensitive areas are shown shaded.** A plus sign appears next to the mouse cursor, which indicates that the selected area is sensitive again and that evaluation will occur upon movement detection. **Sensitive areas are shown not shaded.**
3	Alarm overshoot time	Enter the time for which the detector input is to stay in alarm status after an alarm occurs. **Note:** A recording job must be linked to the detector input.

Configuration (continued)

4	Sensitivity	Change the sensitivity if the results of the movement detection are not satisfactory.
	high	The sensitivity is higher; i.e. smaller texture changes (outlines, brightness, movement) are necessary to trigger an alarm.
	low	The sensitivity is reduced; i.e. bigger texture changes (outlines, brightness, movement) are necessary to trigger an alarm.
5	Grid	When **Grid** is activated, an image is blended into the grid. The size of the sensitive/not sensitive areas displayed is based on the grid.
6	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

Set dome cameras



Settings for Kamera 03

Connection: COM2

Camera protocol: Biphase

Camera 1

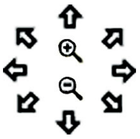
Implement the setting for each camera as required.

No.	Name	Description
1	Dome settings	Click on the **Dome settings** tab.
Creating interface settings		
2	Interface	The settings for the interfaces have to be carried out first. Additional dome setting can only be set after this.
	Connection	Click on the arrow pointing downwards and select the interface.
	Settings	Click on **settings** and then enter the setting for the COM interface (bits per second, data bits, stop bits, parity, camera log). The settings depend on the camera type. Please see the manual for the matrix for more information.
	Camera Protocol	The entry occurs automatically if you have previously entered the settings.
	Camera	Give the address of the camera. The address is setup in the camera.

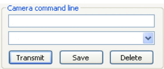
Configuration (continued)

Saving camera positions

You can set the positions of dome cameras to which you can automatically swivel time and time again. Users can quickly select these positions in the live image, provided they are authorized to do this.

3	This is how you control the camera.	**This is how you swivel the camera:**
		Move the mouse cursor into the camera image until the direction arrow points in the direction in which you want to swivel the camera. Then press the left mouse button. The camera swivels in the direction of the arrow with the speed increasing the further you move the arrow outwards (with the mouse button held down). **This is how you zoom:** Move the mouse cursor into the center of the camera image until the magnifying glass appears with a plus or minus sign. You can zoom the camera by clicking the left mouse button.
	⊕	The camera moves closer to the object.
	⊖	The camera moves away from the object.
4	Camera settings	Implement the following settings.
	Focus	Sharpness of the image and
	Aperture	Brightness
5	Positions saved	
	ID Name	Click on the arrow pointing downwards in the **ID name** text box and select a number that has not been used if you want to save a position or select a previously saved position if you want to change it. **Note:** A previously saved camera position can be displayed by selecting it in the **ID Name** text box and clicking on **Display** . The saved position is deleted via **Delete** .
	Save	Click on **Save** , enter a logical name in the open dialog box, and confirm it. A message appears that the scene has been saved. The name is imported into the **ID Name**text box. When this name is selected, the camera automatically moves to this camera position.

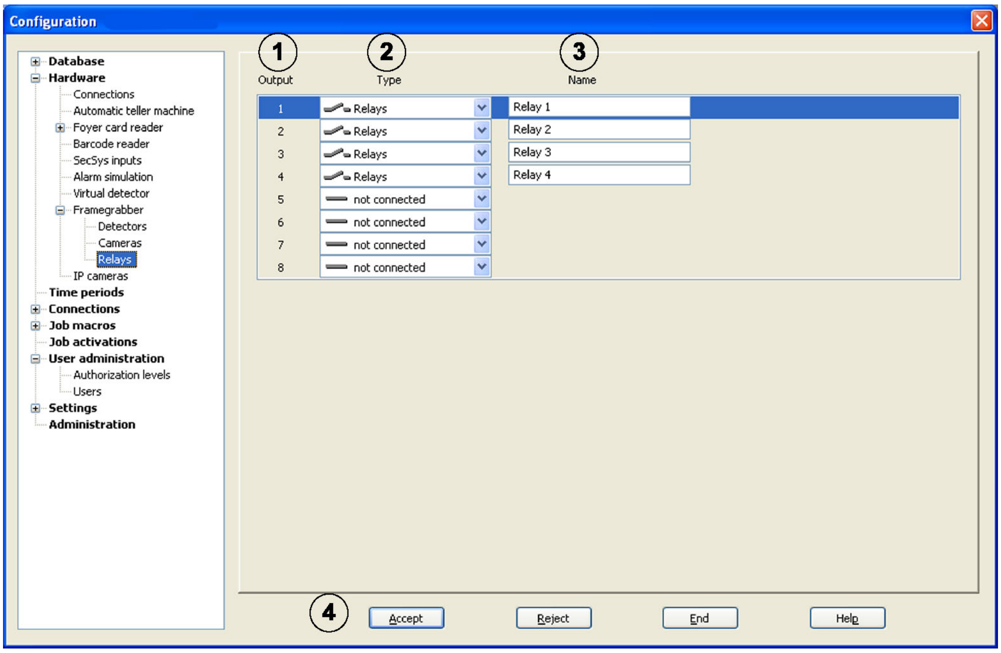
Configuration (continued)

Entering control commands via the command line Here using the command line you can specify different settings for dome cameras or matrixes that you can call up automatically again and again. For more information about which commands are possible, see the operating instructions for the camera or matrix in question. The operator can select these commands quickly in the live image if these have been released for the operator's authorization.		
6	Camera command line	
	 	Click on the arrow pointing downwards in the **Camera command line** option group and select a number that has not been used if you want to save a position or select a previously saved position if you want to change it. Enter the command in the command line (via the line with the down arrow). **Note:** You can perform a command for checking by clicking on **Transmit** . The saved command is deleted via **Delete** .
	Save	Click on **Save**, enter a logical name in the open dialog box, and confirm it. A message appears that the command has been saved. The name is imported. Selecting this name causes the camera to automatically carry out the command.
Accepting entries		
7	OK	Click **OK** to confirm your entries.

Example: Matrix: CCL command
LCM+ 2 1
(that is, switch Camera 2 to Monitor 1)

6.2.14 Configuring relays

(Hardware/Frame grabber/Relays menu)



Output	Type	Name
1	Relays	Relay 1
2	Relays	Relay 2
3	Relays	Relay 3
4	Relays	Relay 4
5	not connected	
6	not connected	
7	not connected	
8	not connected	

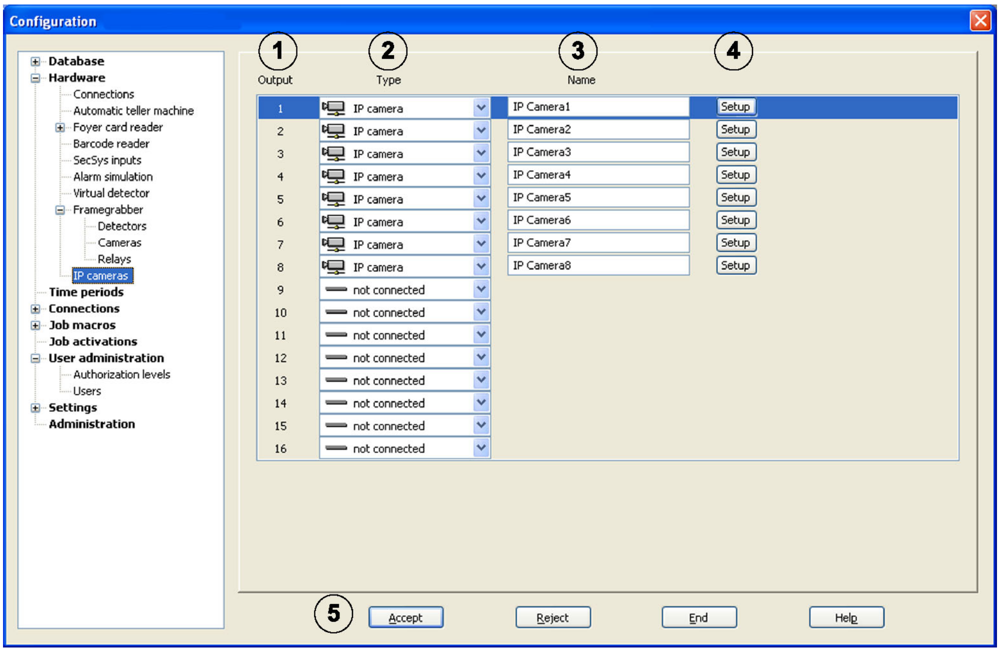
A maximum of 4 or 8 relay outputs can be connected to each MVTitan grabber card. With the MVSigma grabber card, no relays can be connected. A maximum of 2 MVTitan can be installed.
The relays can be activated locally using a remote station or via a browser.

No.	Name	Description
1	Input	Click on the corresponding relay output. The selected line is activated. Please be aware that relay output 4 might already be in use. This is the case when a fault indicator has been selected in the **Connections** menu. In this case, the system automatically uses relay output 4 of the 1st MVTitan with the fault indicator.
2	Type Relays not connected	Click on the arrow pointing downwards in the **Type** column and select whether the relay output should be activated or not. The relay output is activated. The relay output is not activated.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen.
4	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

6.2.15 Configuring IP cameras

(Hardware/IP cameras menu)



Output	Type	Name	
1	IP camera	IP Camera1	Setup
2	IP camera	IP Camera2	Setup
3	IP camera	IP Camera3	Setup
4	IP camera	IP Camera4	Setup
5	IP camera	IP Camera5	Setup
6	IP camera	IP Camera6	Setup
7	IP camera	IP Camera7	Setup
8	IP camera	IP Camera8	Setup
9	not connected		
10	not connected		
11	not connected		
12	not connected		
13	not connected		
14	not connected		
15	not connected		
16	not connected		

A maximum of 16 IP cameras (network cameras) can be connected. The IP cameras can also be connected to the available cameras through Frame grabber.
Only those cameras with which JPEG images can be called up via the http protocol can be used as IP cameras.

Note: Function must be activated under Hardware/Connections.

No.	Name	Description
1	Input	Click on the corresponding output. The selected line is activated.
2	Type IP camera not connected	Click on the arrow pointing downwards in the **Type** column and select whether the output should be used by an IP camera or not. The output is being used by an IP camera. The output is not being used.
3	Name	Place the cursor in the **Name** column and enter the name. Any name can be chosen.

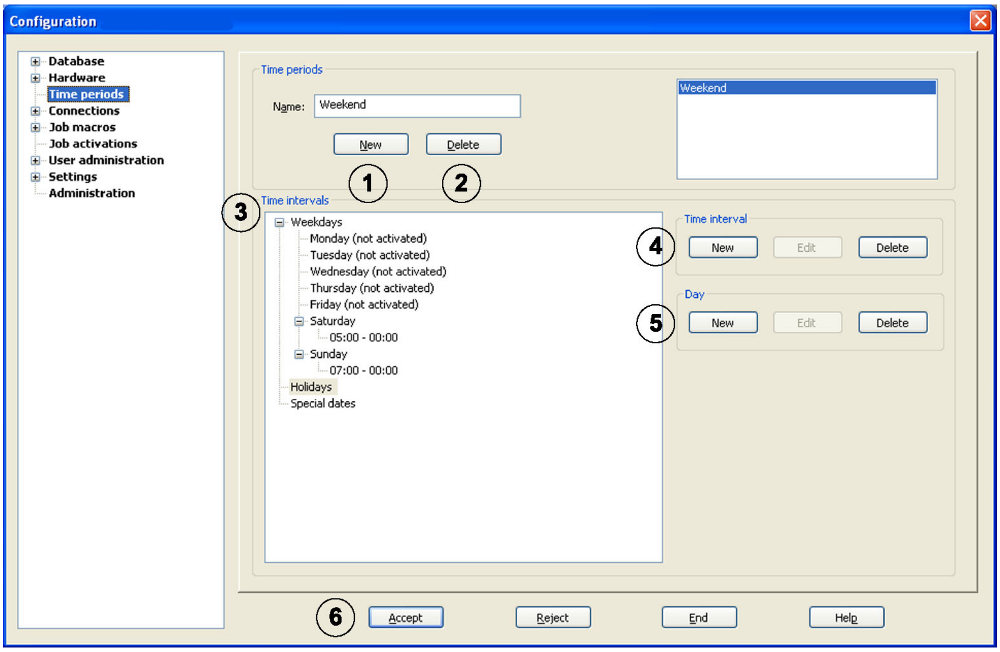
Configuration (continued)

4	Setup	Click on **Setup** and implement the settings for each camera. Enter the following – Address (URL) of the camera under which JPEG images can be called up. **Note:** If you click on **Display** , you can check to see whether the URL entered is correct. In this case the camera image appears. **Note:** Axis: http://”IP–address”/jpg/image.jpg Mobotix: http://”IP–address”/record/current.jpg – User name and password for the cameras; these are required for registration (e.g. Mobotix banking camera) – Activate images per second **Note:** This function should always be activated when the camera delivers the same image repeatedly upon repeated requests, even though no new image was grabbed. Thus the network load can be minimized during live image display.
5	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

6.2.16 Configuring time periods

(Time periods menu)



To ensure that jobs are activated at specific times, you can define different times for specific events, such as triggering a save job at certain times.

No.	Name	Description
1	New	Creates a time period. Click on **New** and enter the actual name in the **Name** input box.
2	Delete	Deletes a time period. In the overview (in the right side of the dialog box), select the time period that you wish to delete and click on **Delete**.
3	Time intervals	Choose the day and continue with steps 4 and 5.
	Weekdays	– Monday through Sunday
	Holidays	– Holidays. Holidays can be adapted for particular countries (see **Administration** Menu).
	Special dates	– Days that can be selected at will.
		Warning: The system evaluates the entries according to priority. If entries assigned to a particular day are contradictory, the entry with the higher priority is always in effect. – Special dates (highest priority) – Holidays (average priority) – Weekdays (lowest priority)

Configuration (continued)

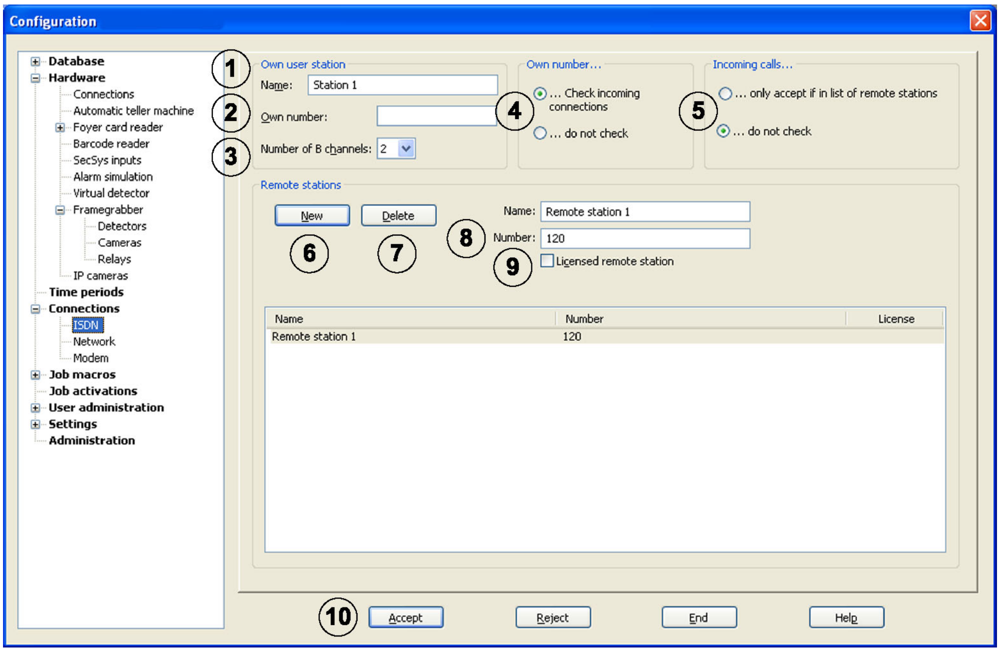
4	Time interval	The times (from ... to) for the selected weekdays, holidays and special dates can be entered here.
	New	A new time can be entered.
	Edit	An existing time can be changed.
	Delete	Deletes the time periods of the selected day.
5	Day	The holidays and special dates are selected here. **Note:** Activation only occurs on the selected day if a time interval is assigned. If there is no time interval, no activation occurs.
	New	A new day can be selected.
	Edit	An existing day can be changed.
	Delete	Deletes the selected day.
6	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Note:
You have to assign a time period to a job in the **Job Activations** menu.

Configuration (continued)

6.2.17 Configuration of the ISDN connections (option)

(Connections/ISDN menu)



Own user station

Name: Station 1

Own number:

Number of B channels: 2

Own number...

● ... Check incoming connections

○ ... do not check

Incoming calls...

○ ... only accept if in list of remote stations

● ... do not check

Remote stations

Name: Remote station 1

Number: 120

□ Licensed remote station

Name	Number	License
Remote station 1	120	

In this menu, define your own user station (local computer) and the remote stations so that you are able to establish a connection to a remote station when continuing the configuration process and/or to allow a connection to your own user station.

Note: Function must be activated under Hardware/Connections.

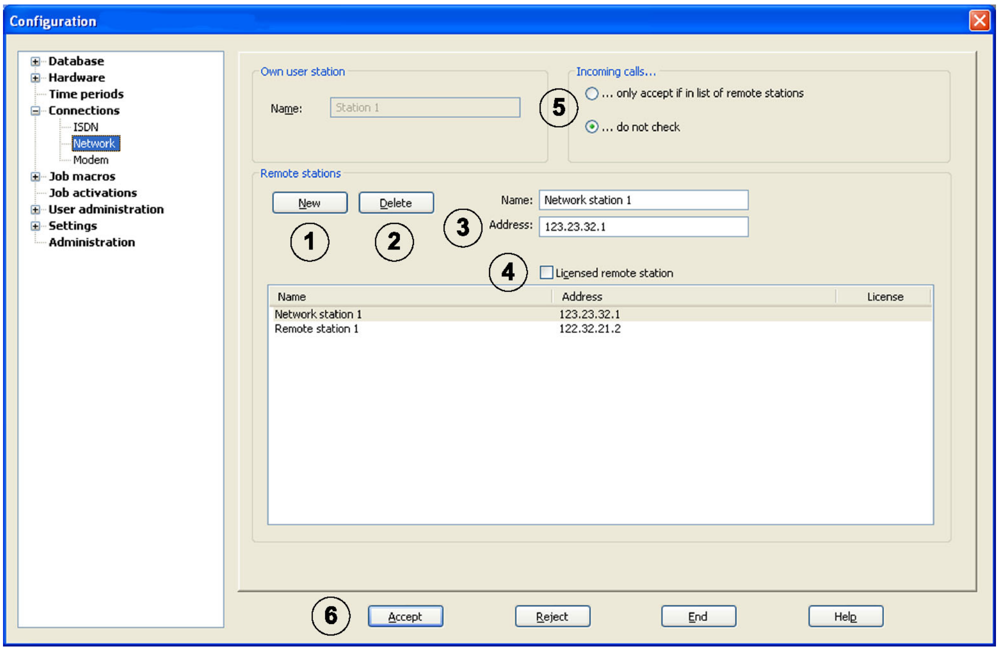
No.	Name	Description
1	Name	Enter the locale computer name in **Name** of the options group **Own user station**. Note: In the live image, the local computer name is displayed in the last line of the **Connection** menu.
2	Own number	Enter the complete telephone number of your own user station into the entry box **Own number**. In the case of PABXs, which make an assignment to the number called, it is easier to just enter an “A”.
3	Number of B channels	Enter the number of B channels in the entry box Number of B channels.
4	Own number .. Check incoming connections .. do not check	Activate the corresponding option –if the system is to check whether the number entered matches your own number. The connection is only made if they match. – if the system should not check whether the number entered matches your own number. Can be selected if there is only one additional connection. In this case, your own number does not have to be entered.

Configuration (continued)

5	Incoming calls .. only accept if in list of remote stations .. do not check	Activate the corresponding option –if the system should check whether the calls are coming from a configured remote station. The connection is only made if they match. –if the system is not to perform any check.
6	New	Creates a new connection to a remote ISDN remote station. Click on **New** and enter the actual name of the remote station (the computer name) in the **Name** input box.
7	Delete	Deletes the connection to a remote ISDN remote station. In the overview (in the lower portion of the dialog box), select the remote station that you wish to delete and click on **Delete**.
8	Number	Enter the complete telephone number of the remote station in the entry box **Number** . If your own user station is located at a PABX, you must enter a digit (usually a “0”) before the number of the remote station in order to reach the outside line.
9	Licensed remote station	Activate **Licensed remote station** for projects that require this, e.g. for a Rubin K1 as a remote station (optional).
10	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

6.2.18 Configuring network connections

(Connections/network menu)



Own user station

Name: Station 1

Incoming calls...

○ ... only accept if in list of remote stations

● ... do not check

Remote stations

Name: Network station 1

Address: 123.23.32.1

□ Licensed remote station

Name	Address	License
Network station 1	123.23.32.1	
Remote station 1	122.32.21.2	

In this dialog box you can determine the video systems to which—via the network—a two–way connection should be connected.

Note: Function must be activated under Hardware/Connections.

No.	Name	Description
1	New	Creates a new connection to a remote network remote station. Click on **New** and enter the actual name of the remote station (the computer name) in the **Name** input box.
2	Delete	Deletes the connection to a remote network remote station. In the overview (in the lower portion of the dialog box), select the remote station that you wish to delete and click on **Delete**.
3	Address	Enter the TCP/IP address of the remote station or the computer name (e.g. for DHCP) in the **Address** input box.
4	Licensed remote station	Activate **Licensed remote station** for projects that require this, e.g. for a Rubin K1 as a remote station (optional).

Configuration (continued)

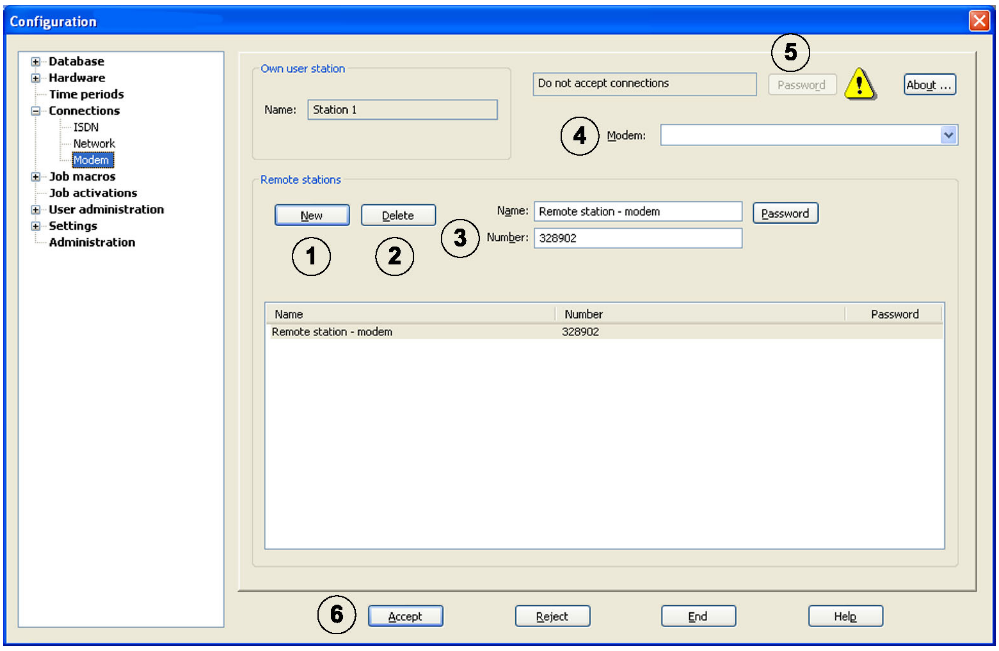
5	Incoming calls .. only accept if in list of remote stations .. do not check	Activate the corresponding option – if the system should check whether the calls are coming from a configured remote station. The connection is only made if they match. – if the system is not to perform any check.
6	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Note: The number of accessible remote stations can be viewed in the dongle. For manual connection setup, only the number of released connections is offered.

Configuration (continued)

6.2.19 Configuring modem connections

(Connections/modem menu)



Name: Station 1

Do not accept connections

Name: Remote station - modem

Number: 328902

Name	Number	Password
Remote station - modem	328902	

In this dialog box you can determine the video systems to which—via the modem—a two–way connection should be connected.

In order to ensure that a configuration can be performed, an RAS–capable modem* must be connected and RAS service must be installed. If no RAS–capable modem is connected or no RAS service is installed, the following note symbol and a button with additional information appear.

Note: Function must be activated under Hardware/Connections.

No.	Name	Description
1	New	Creates a new connection to a remote modem remote station. Click on **New** and enter the actual name of the remote station (the computer name) in the **Name** input box.
2	Delete	Deletes the connection to a remote modem remote station. In the overview (in the lower portion of the dialog box), select the remote station that you wish to delete and click on **Delete**.
3	Number	Enter the complete telephone number of the remote station in the entry box **Number** . If your own user station is connected to a PABX, you must enter a digit (usually a “0”) before the number of the remote station in order to obtain the exchange line.

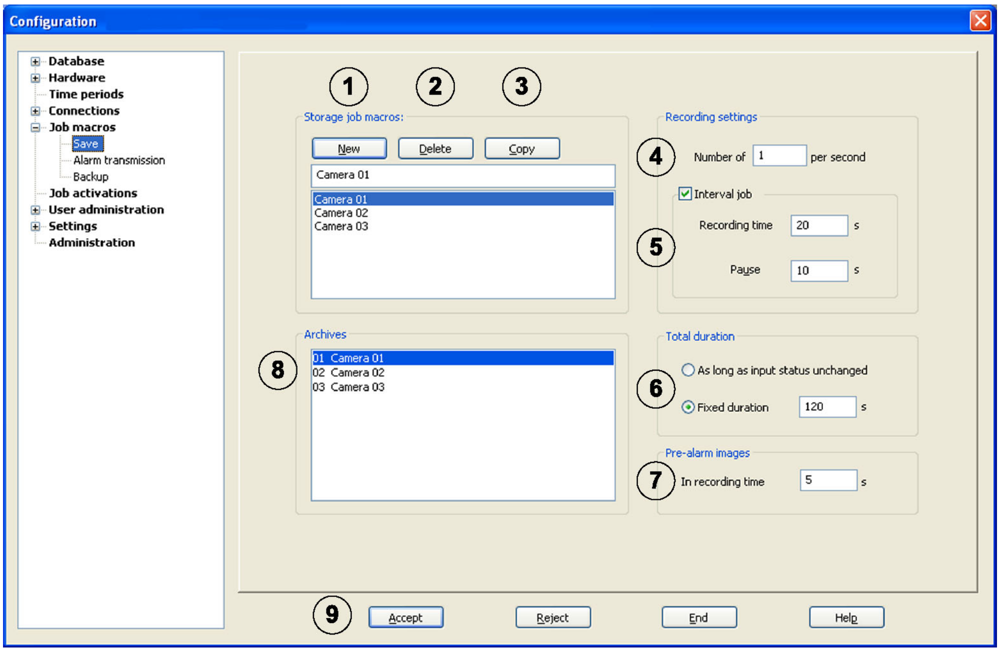
* See Section 4.16.1 for additional information.

Configuration (continued)

4	Modem	Select the connected modem in the **Modem** list box.
5	Password	Click Password in order to change the RAS password for incoming calls.
6	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

6.2.20 Configuring storage job macros

(Job macros/save menu)



Camera 01

Camera 01
Camera 02
Camera 03

Number of 1 per second

☑ Interval job

Recording time 20 s

Pause 10 s

01 Camera 01
02 Camera 02
03 Camera 03

○ As long as input status unchanged

● Fixed duration 120 s

In recording time 5 s

Job macros, e.g. saving images automatically (so–called storage job macros), define sequences (jobs) that should either run continuously or when an alarm is triggered. These jobs, which are only defined once, can then be used for variable alarm triggers and cameras.

No.	Name	Description
1	New	Creates a new storage job macro. Click on **New** and enter the name in the input box.
2	Delete	Deletes an existing storage job macro. Select a storage job macro in the list box and click on **Delete**. The storage job macro will be deleted.
3	Copy	Copies an existing storage job macro. Select a storage job macro in the list box and click on **Copy**. The storage job macro is copied and can be adapted quickly.
4	Number of images	Enter the number of images to be recorded per second in the **Number of images** input box. **Note:** The system does not check the plausibility of the configured images here. Please check this yourself.
5	Interval job	Activate **Interval job** if recording is not to be continuous, but intermittent recordings are needed. If this is the case, enter:
	Recording time	The duration of a recording.
	Pause	The time between recordings

Configuration (continued)

6	Total duration As long as input status unchanged Fixed duration	Activate the corresponding option – if recording (with possible pauses) should be repeated as long as the input status of the alarm input exists. Recording does not end until the input status is changed. – If the entire duration of recording should be restricted to the time you enter.
7	Pre–alarm images In recording time	Enter the time for which the system is to save images before an alarm. A time from “0” to “10” seconds can be entered. In contrast to the history ring, pre–alarm images can be used for rapidly repeating triggers. Note: The system saves continuous images from the particular camera in the working memory. Only in the event of an alarm does the system write these images from the last x seconds automatically into the camera’s alarm archive. The images are then assigned before alarm images. This allows you to subsequently look at events leading to the alarm and the events after the alarm in the image archive. One image is saved per second of pre–alarm here, i.e. for 0 seconds no image, for 1 second one image, for 2 seconds 2 images, etc.
8	Archives	Select the archive list or archives in which the images are to be saved.
9	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

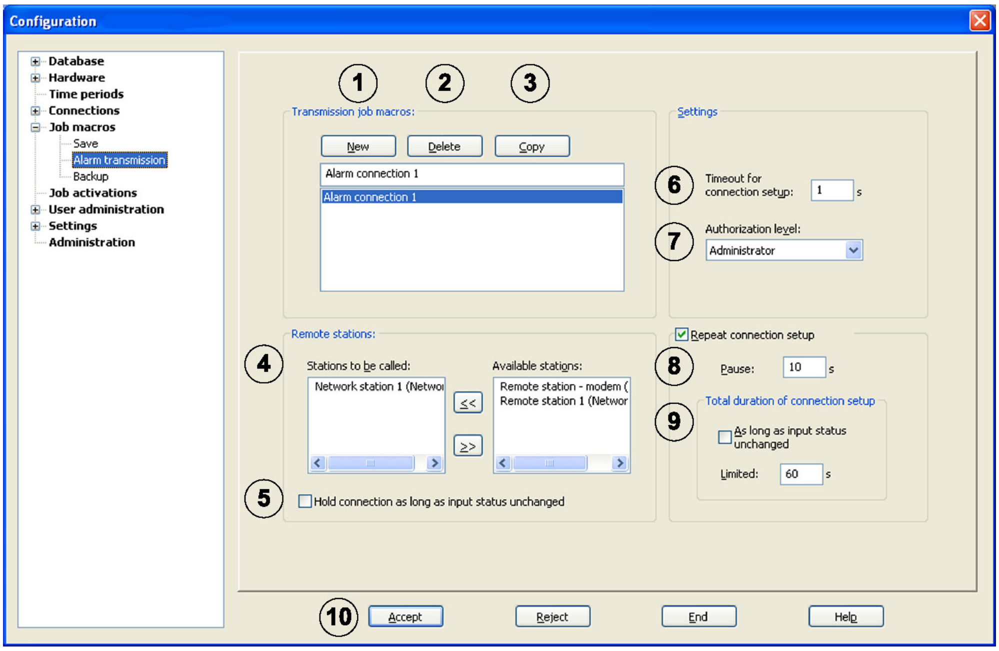
Note: If the job macro is assigned to various cameras in the**Job activations** menu, all images will be stored in a common archive.

Note: If more than one target archive is assigned to a job macro, the same image will be written in all archives.

Note: A job macro must be configured before activating a job.

6.2.21 Configuring alarm transmission job macro

(Job macros/alarm transmission menu)



Transmission job macros:
Alarm connection 1
Alarm connection 1

Settings
Timeout for connection setup: 1 s
Authorization level: Administrator

Remote stations:
Stations to be called: Network station 1 (Netwo
Available stations: Remote station - modem (
Remote station 1 (Networ

□ Hold connection as long as input status unchanged

☑ Repeat connection setup
Pause: 10 s
Total duration of connection setup
□ As long as input status unchanged
Limited: 60 s

Job macros define sequences (jobs) that should either run continuously or when an alarm is triggered. These jobs, which are only defined once, can then be used for variable alarm triggers and cameras.
In the event of an alarm, the station issuing the alarm establishes a connection to a configured remote station. A separate connection window from the station issuing the alarm is opened in the live image of the remote station, and the images of the cameras assigned to this job macro are displayed in the remote station. Activation of the job macro occurs in the **Job activation** menu.

Before you begin the alarm transmission job macro:

- Activate the **ISDN** and/or **Network**checkbox in the **Hardware/Connections** menu.
- Define your own user station and the remote stations in the **Connections/ISDN** and/or **Connections/network** menu.

Configuration (continued)

Configuring an alarm transmission job macro:

No.	Name	Description
1	New	Creates a new transmission job macro. Click on **New** and enter the name in the input box.
2	Delete	Deletes an existing transmission job macro. Select a transmission job macro in the list box and click on **Delete**. The transmission job macro will be deleted.
3	Copy	Copies an existing transmission job macro. Select a transmission job macro in the list box and click on **Copy**. The transmission job macro is copied and can be adapted quickly.
4	Remote stations	
	Available stations	This list box contains all remote stations known in the system.
	Stations to be called	This list box contains the stations that should be called by this job macro. The job macro should create a connection to these stations. During selection, proceed as follows: Select the station and possible spare stations, to which a connection should be established, from the list box of available stations and click the <<button. The selected stations are added to the list box of stations that are to be called. **Note:** Please note that the system processes the stations that are to be called from top to bottom if no connection can be established with the top station. This means that the remote station at the top must be the station that you wish to communicate with first. The other stations are spare stations.
5	Hold connection as long as input status unchanged	Activate this function when the connection should only exist as long as the input status is unchanged. If the input status changes and the function is activated, the connection will be disconnected.
6	Timeout for connection setup	Enter the time within which an attempt should be made to establish a connection to the relevant station. **Note:** If the total time of the connection setup to a remote station has elapsed (and the triggering criteria still exists and item 5 is selected), an attempt to set up a connection to the next station in the list is started automatically, using the same settings.

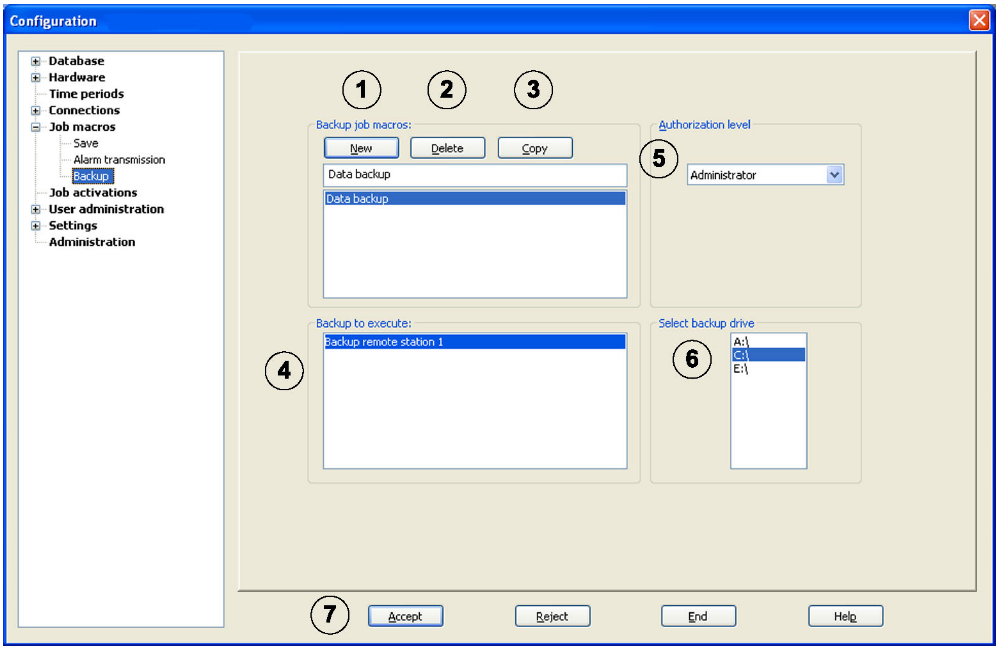
Configuration (continued)

7	Authorization level	Select the authorization level. This job macro will only be available to the user with the authorization level selected. **Note:** The name and connection password for the authorization level (from the **User management/authorization levels** menu, **Connection password**button) have to match each other in the local station and in the station that is to be called. The individual releases of authorization level, e.g. released cameras, archives..., can vary however. You can then receive the releases of authorization level in the remote station when logging into the remote station.
8	Repeating the connection	If a number of attempts are made, in the event that establishing a connection to all the remote stations in the list fails, then activate this function and
	Pause	enter the time after which a new log–in attempt should be made.
9	Total duration of connection setup	Activate the corresponding option
	As long as input status unchanged	–if recording (with possible pauses) should be repeated as long as the input status of the alarm input exists. Recording does not end until the input status is changed.
	Fixed duration	– If the entire duration of recording is restricted to the time you enter.
10	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

6.2.22 Configuring backup job macro

(Job macros/backup menu)



Backup job macros: Data backup

Data backup

Authorization level: Administrator

Backup to execute: Backup remote station 1

Select backup drive: A:\ C:\ E:\

Job macros define sequences (jobs) that should either run continuously or when an alarm is triggered. These jobs, which are only defined once, can then be used for variable alarm triggers and cameras.
For back job macros, the current day’s images can automatically be saved to a network drive for example. Activation of the job macro occurs in the **Job activation** menu.

Before you begin the backup job macro:
Before you can setup a backup job macro in the configuration, you have to create a search macro in the image archive and save. Set the criteria in this search macro that is to be used when searching for images. This search macro is assigned to a backup job macro when configuring (see in no. 4: “Configuring backup job macro”).

This is how you can create a search macro:

- Call up the image archive.
- Select the **Database/search dialog (Single images)** menu.
- Define the time, camera number, archives and remote stations for the search macro in this dialog box.
- Click on the **Search macros** tab in the dialog box in the upper left side and select the command **Save** .
- Enter a name for the search macro and confirm with **OK**. This saved search macro appears in the configuration and can be selected.
- Leave the image archive and call up the configuration via the **Configuration** menu. You can now create a backup job macro.

Configuration (continued)

Configuring a backup job macro:

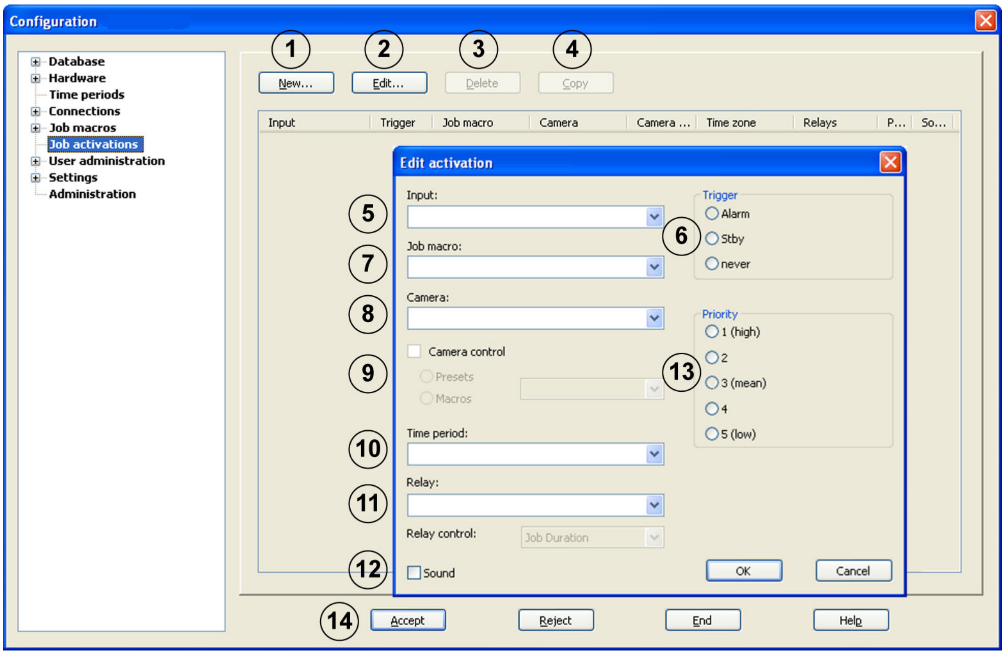
No.	Name	Description
1	New	Creates a new backup job macro. Click on **New** and enter the name in the input box.
2	Delete	Deletes an existing backup job macro. Select a backup job macro in the list box and click on **Delete**. The backup job macro will be deleted.
3	Copy	Copies an existing backup job macro. Select a backup job macro in the list box and click on **Copy**. The backup job macro is copied and can be adapted quickly.
4	Backup to execute	Select the search macro in the list. The result of this search macro will then be saved upon activation of the backup job macro.
5	Authorization level	Select the authorization level for archive access during backup from the list.
6	Selecting backup drive	Select the drive. The data will be transferred to this drive.
7	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Note: A time–controlled backup can only be linked to one alarm status. To do this, select a detector input that is always in alarm. A time period and a backup job macro have to be assigned to this detector input.

Note The use of a SIM detector is only recommended if the backup is to be done manually. A SIM detector is not suitable for an automatic time–controlled backup because the alarm status will not be maintained if system is reset.

6.2.23 Configuration of job activations

(Job activations menu)



Any number of system reactions for the alarm inputs can be specified in this menu. A job activation is absolutely necessary in order to ensure that camera images are saved.

No.	Name	Description
1	New	Creates a new job activation. Click on **New** and make your entries in the dialog box that opens.
2	Edit	For editing an existing job activation. Select a job activation in the list box and click on **Edit**. You can now change the existing inputs.
3	Delete	Deletes an existing job activation. Select a job activation in the list box and click on **Delete**. The job activation is deleted.
4	Copy	Copies an existing job activation. Select the job activation in the list box and click on **Copy**. The job activation is copied and can be adapted quickly.
5	Input	Select the input.

Configuration (continued)

6	Trigger	Select the triggering criteria that are to trigger the job activation.
	Alarm	The job is activated as soon as the alarm input is triggered.
	Stby	The job is activated as long as the input is in standby mode. Can be used for history recording.
	Never	The job is not activated.
7	Job macro	Select the job macro that is to be implemented.
8	Camera	Click on the camera that is to be used for recording or transmission.
9	Camera control	Select **Camera control** if you want to control a camera. You can choose between previously saved presets or marcos.
	Presets	Click on **Presets** and select the preset in the List field (refer to page 89 to see how to save camera presets).
	Macros	Click on **Marcros** and select a marco in the List field (refer to page 90 to see how to save macros).
10	Time period	Select the time period within which the input status is to lead to an activation. **Note:** Once the time period has elapsed, no activation occurs. The end of a time period also ends a job.
11	Relays	If necessary, select the relay that is to be controlled and assign this relay
	Relay control	at **Relay control** one of the following statuses: Job start, job duration or job end. **Note:** The relay is controlled for approximately one second with job start and job end. Job duration so long as job exists.
12	Sound	Activate this function as required.
	☑	When starting a job, an audible sound sequence is played (can be set separately for each job activation). If several jobs are assigned to one input, it is possible to play the signal sound once only. History jobs can thus be specifically indicated (audibly).
	□	When starting a job, no audible sound sequence is played. This allows for silent alarms to be triggered in the case of a holdup.

Configuration (continued)

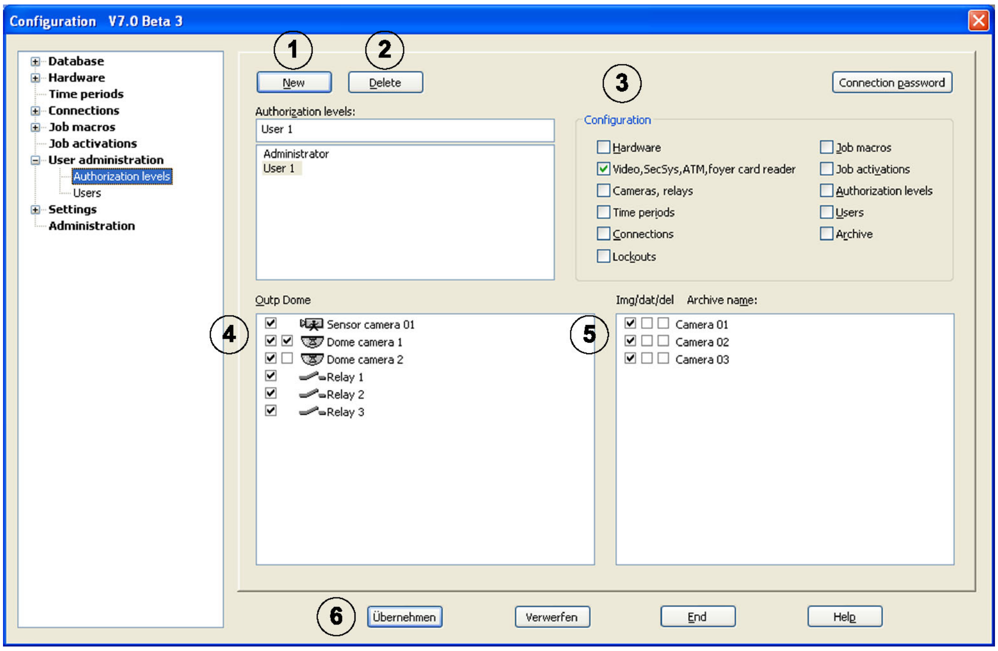
13	Priority	Determine the priority of the job. Priority 1 (high) to priority 5 (low). **Note:** A priority can only be specified in connection with a job macro.
14	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Note:
The inputs must be defined in the following menus:
For detector inputs, see the **Hardware/framegrabber/detectors** menu.
For the foyer card reader input, see the **Hardware/foyer card reader** menu.
For automatic teller machine inputs, see the **Hardware/automatic teller machine** menu
For SecSys inputs (statuses), see the **Hardware/SecSys inputs** menu.
For alarm simulation inputs, see the **Hardware/alarm simulation** menu.
Inputs of the virtual detectors see **Hardware/Virtual Detectors** menu
For the barcode reader input, see the **Hardware/barcode reader** menu.

Note:
A time–controlled backup can only be linked to one alarm status. To do this, select a detector input that is always in alarm status. This detector input has to be assigned a time period and a backup job macro.

6.2.24 Configuration of authorization levels

(User management/authorization levels menu)



Authorization levels: User 1

Administrator
User 1

Configuration

□ Hardware	□ Job macros
☑ Video,SecSys,ATM,foyer card reader	□ Job activations
□ Cameras, relays	□ Authorization levels
□ Time periods	□ Users
□ Connections	□ Archive
□ Lockouts	

Outp Dome

☑ Sensor camera 01
☑ ☑ Dome camera 1
☑ □ Dome camera 2
☑ Relay 1
☑ Relay 2
☑ Relay 3

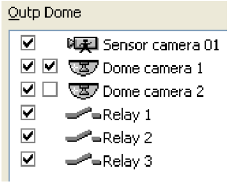
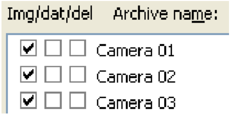
Img/dat/del Archive name:

☑ □ □ Camera 01
☑ □ □ Camera 02
☑ □ □ Camera 03

You can create different authorization groups in this menu if you have administrator rights. These so–called authorization levels enable you to determine what the user is allowed to do in the system. The *Administrator* authorization level has all rights, and this is configured before delivery from the plant.

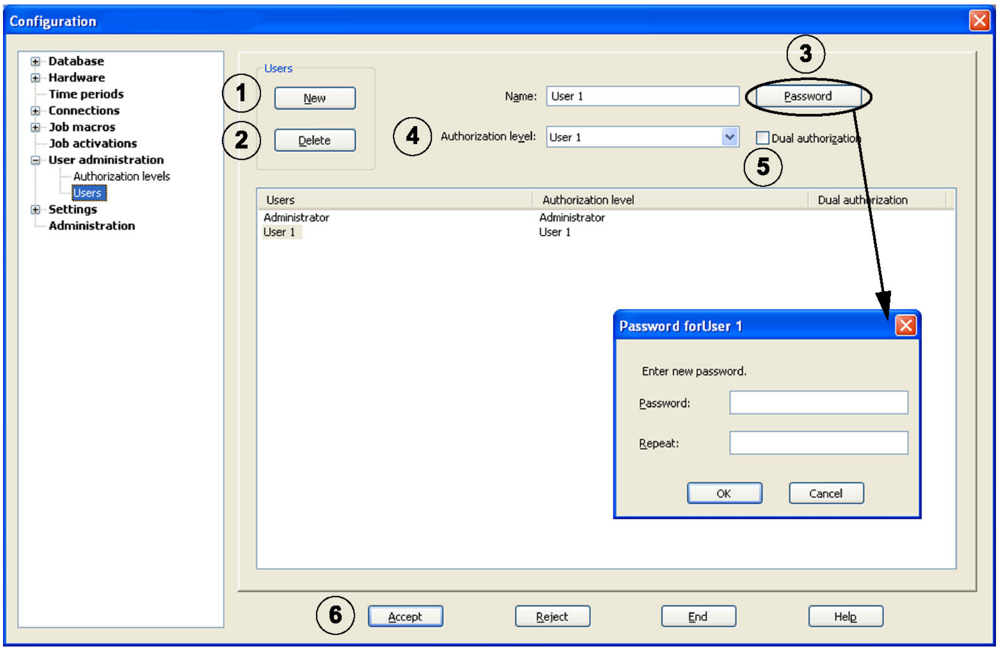
No.	Name	Description
1	New	Creates a new authorization level. Click on **New** and enter the name in the input box.
2	Delete	Deletes an existing authorization level. Select an authorization level in the list box and click on **Delete**. The authorization level is deleted.
3	Configuration	Activate the check boxes in front of the functions in which the person with this authorization level is allowed to implement configuration.

Configuration (continued)

4	Outp Dome  Outp Dome ☑ Sensor camera 01 ☑ ☑ Dome camera 1 ☑ □ Dome camera 2 ☑ Relay 1 ☑ Relay 2 ☑ Relay 3	Activate the check boxes of those elements (cameras, relays) that are to be available for the person with this authorization level. In the case of dome cameras, a 2nd column with a check box is also displayed. The check boxes in front of the elements stand for: Left column: In the live image, the user is only shown the cameras and relays for which the check box is activated. Right column: In the live image, the user can only control the cameras for which the check box is activated. **Note:** The video system only offers the video hardware that is already configured. If new components are set up, access to them must subsequently be configured for all authorized users.
5	Img dat del  Img/dat/del Archive name: ☑ □ □ Camera 01 ☑ □ □ Camera 02 ☑ □ □ Camera 03	By activating the check box, you can select the access rights for the authorization levels in the relevant archives. The activated check boxes in front of the elements stand for: Image In the image archive, the user sees only the archives for which the checkbox is activated. Dat The stored images, together with the supplementary data (e.g. date, time, ATM data) can be searched for, viewed, evaluated, copied and printed. Del The contents of the archives can be deleted.
6	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

6.2.25 Configuration of the users

(User management/user menu)



Name: User 1

Authorization level: User 1

Users	Authorization level	Dual authorization
Administrator	Administrator	
User 1	User 1	

Password forUser 1

Enter new password.

Password:

Repeat:

To protect access to system components and data, operating procedures can only be carried out by logged–on users. Each user is assigned an authorization level for the work he/she needs to carry out (also see configuration of authorization levels).

Additionally, the logon procedure of a user can be protected by a password. This password is only evaluated with local logon procedures. For remote logons, the authorization password is evaluated. With remote login procedures, the password of the authorization levels is evaluated.

Note: **You should definitely protect the *Administrator* authorization level with a password. Please ensure that this password in only known to those persons responsible for this video system.**

No.	Name	Description
1	New	Creates a new user. Click on **New** and enter a user name in the **Name** input box.
2	Delete	Deletes an existing user name. In the overview (in the lower portion of the dialog box), select the user name that you wish to delete and click on **Delete**.
3	Password	Click on **Password** and enter a password for the user. Confirm your entries.
4	Authorization level	Click on the arrow pointing downwards in the list box and select an authorization level for the user.

Configuration (continued)

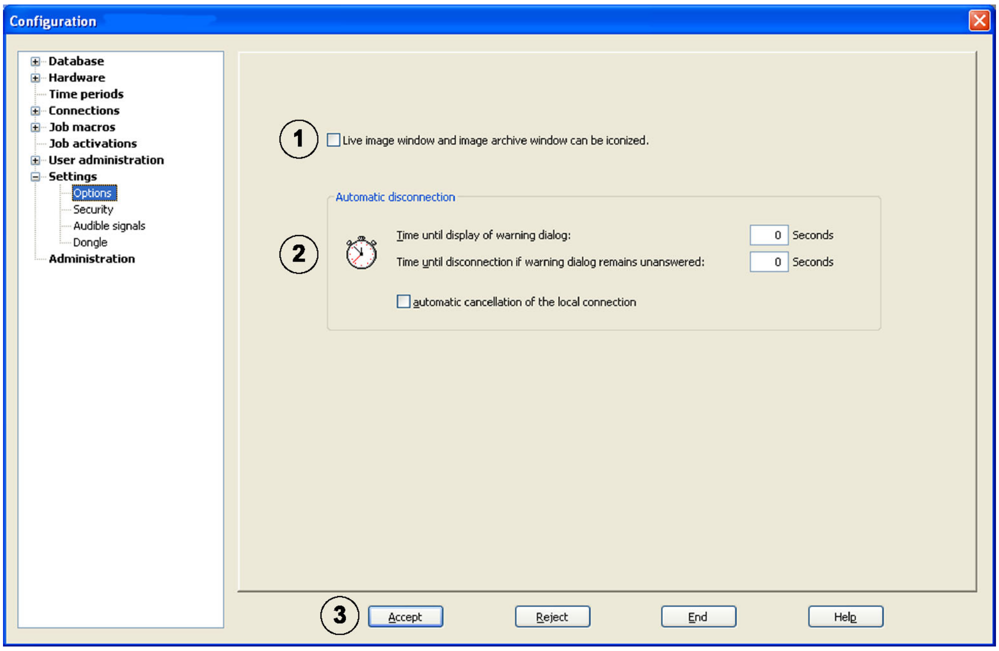
5	Dual authorization	Activate the function when the user is only allowed to login to the system together with another user.
6	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Note: There is no limit to the number of users that can be set up.
The user password is only valid for the logon procedure of a local user.
The authorization *Administrator* can only be given by other administrators.

Configuration (continued)

6.2.26 Configuration of options

(Settings/options menu)



1 □ Live image window and image archive window can be iconized.

Automatic disconnection

2 Time until display of warning dialog: 0 Seconds

Time until disconnection if warning dialog remains unanswered: 0 Seconds

□ automatic cancellation of the local connection

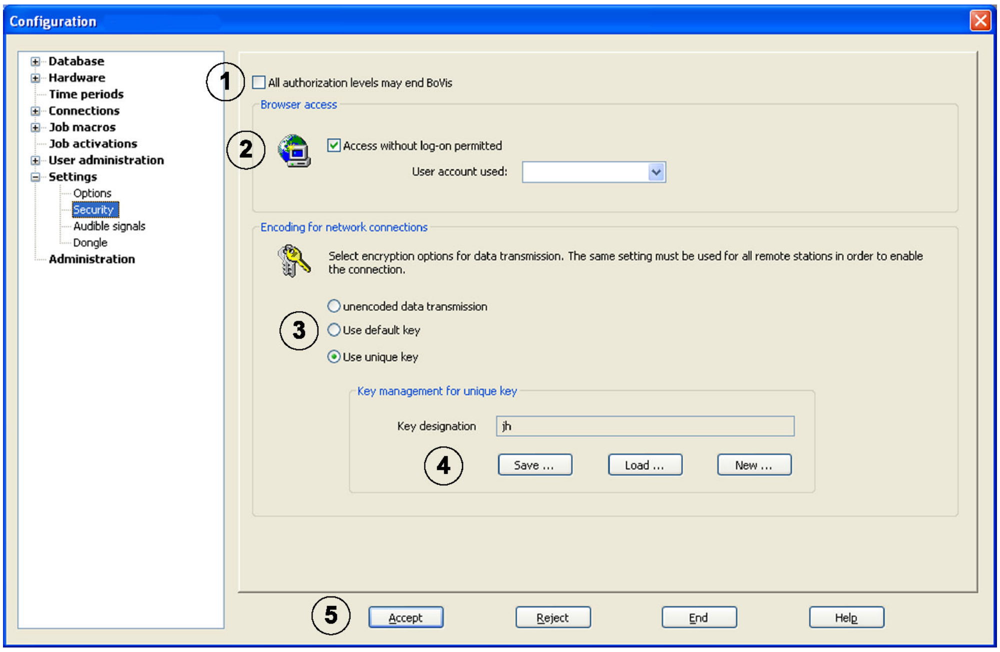
This dialog box enables you to implement optional settings for the live image, the image archive and for an automatic disconnection.

No.	Name	Description
1	Live image window and image archive window can be iconized	Here you can choose whether the ability to iconize the live image and image archive windows should an option. Changes are taken over only after restarting DiBos.
2	Automatic disconnection	For ISDN and network connections and local live image, you can
	Time until display of warning dialog	– enter the time after which a warning dialog is to be displayed and, in addition,
	Time until disconnection if warning dialog remains unanswered	– the time after which there is to be a cancel if the warning dialog remains unanswered (value 0 means no cancel).
	Automatic cancellation of the local connection	If the local connection (the local live image) is also to be automatically cancelled after the pre–set time, activate the check box (it can be useful to save bandwidth with the grabber).
3	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

6.2.27 Configuration of security settings

(Settings/security menu)



☐ All authorization levels may end BoVis

Browser access

☑ Access without log-on permitted

User account used:

Encoding for network connections

Select encryption options for data transmission. The same setting must be used for all remote stations in order to enable the connection.

○ unencoded data transmission

○ Use default key

● Use unique key

Key management for unique key

Key designation: jh

You have the option of implementing security settings in this dialog box, e.g. browser access, or encoding for network connections.

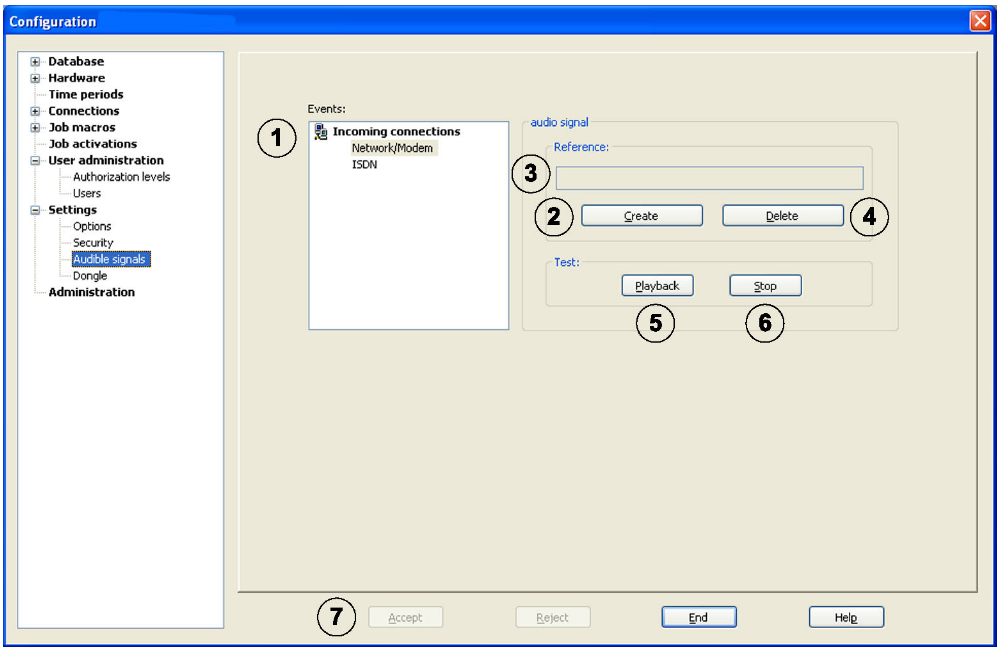
No .	Name	Description
1	All authorization levels may end DiBos	Activate the check box if all users should receive authorization to end the system.
2	Browser access Access without log–on permitted User account used	With browser access via network. – Activate the check box if access to the system is to be allowed via the browser (without logon). – In the list box, select the user for whom this access is used.
3	Encoding for network connections Unencoded data transmission Use default key Use unique key	You can select the encoding options for data transmission. The same setting must be used for all stations in order to enable the connection. – The data transmission occurs unencrypted, e.g. for an application on the network. – A default key, which is the same for all video systems, is used. It is already present on all systems and is activated when this function is selected. – A unique key is generated. This key must be loaded on all the other video systems (see item 4).

Configuration (continued)

4	Key management for unique key	This item is only to be carried out if you want to use a unique key.
	New	– **Generating a unique key:** Click on **New** and enter a name for the encoding. Click on **OK** to confirm. Warning: The current encoding will be overwritten.
	Save	– **Saving a unique key:** It is advisable to save the generated key onto a floppy disk immediately and to keep it in a safe place, as this key must be loaded for the other video systems. To do this, insert a diskette and click on **Save**. Select drive letter A and click on **Save**again.
	Load	– **Loading a unique key:** Insert a diskette and click on **Load**. Select the file and click on **Open**.
		– **Deleting a unique key:** If you generate a new key or load a new key, the system automatically replaces the current key with the new key.
5	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

6.2.28 Configuration of audio signals

(Settings/audio signals menu)



In this dialog box, you can allocate different audio signals to incoming messages from network / modem and ISDN connections. This gives you a differentiation option.

Assigning an audio signal to a connection:

No.	Name	Description
1	Incoming connections	Select the connection to which you wish to assign an audio signal.
2	Create	Click on **Create** thereby opening the window within which you then select the wav file you wish to assign to the connection. Click on **Open** to accept the file.
3	Reference	The wav file is displayed to you in the **Reference** text box located there.
5	Playback	If you want to hear the file for testing purposes, click on **Playback**.
6	Stop	Clicking on **Stop** ends the playback.
7	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

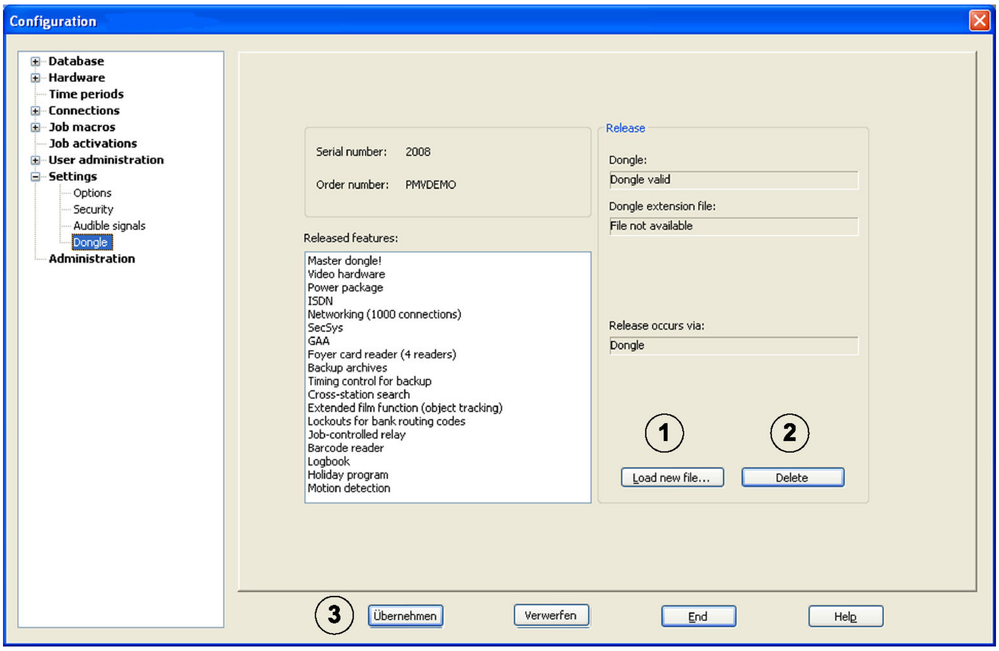
Deleting an audio signal:

No.	Name	Description
1	Incoming connections	Select the connection whose audio signal you wish to delete.
3	Reference	The wav file is displayed to you in the **Reference** text box located there.
4	Delete	Click on **Delete**. The reference to the wav file is deleted.
7	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

6.2.29 Configuration of the dongle

(Settings/dongle menu)



Serial number: 2008

Order number: PMVDEMO

Released features:

Master dongle!
Video hardware
Power package
ISDN
Networking (1000 connections)
SecSys
GAA
Foyer card reader (4 readers)
Backup archives
Timing control for backup
Cross-station search
Extended film function (object tracking)
Lockouts for bank routing codes
Job-controlled relay
Barcode reader
Logbook
Holiday program
Motion detection

Release

Dongle: Dongle valid

Dongle extension file: File not available

Release occurs via: Dongle

In this dialog field, you can see the serial and job numbers, the approved system performance features and the approved status of the hardware dongle and the hardware dongle extension file.
The hardware dongle expansion file contains system performance features acquired subsequently. To activate these system performance features, the file must be loaded. The hardware dongle expansion file always relates to a particular dongle (specify dongle and order number).

Loading a new dongle file:

No.	Name	Description
1	Load new file	Click on **Load new file**to load a new file. Import the data from a diskette for example. The currently existing file is overwritten.
3	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

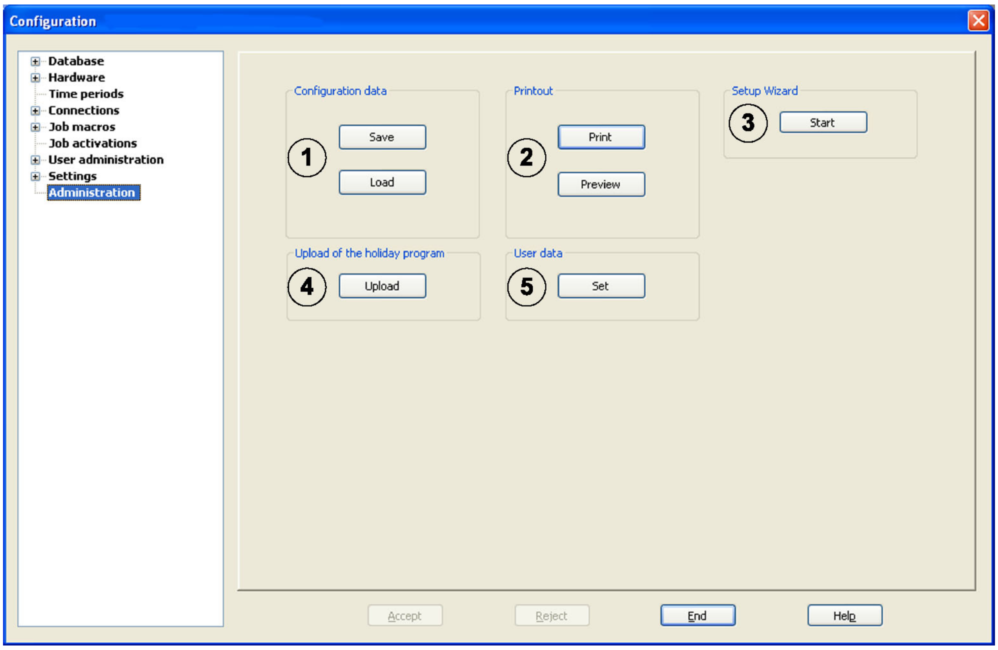
Deleting an existing dongle file:

No.	Name	Description
2	Delete	Click on **Delete**, to delete the existing dongle file.
3	Accept	Click on **Accept**. If you have made incorrect inputs, click on **Reject** and start over.

Configuration (continued)

6.2.30 Administration configuration

(Administration menu)



This dialog box contains the following options:

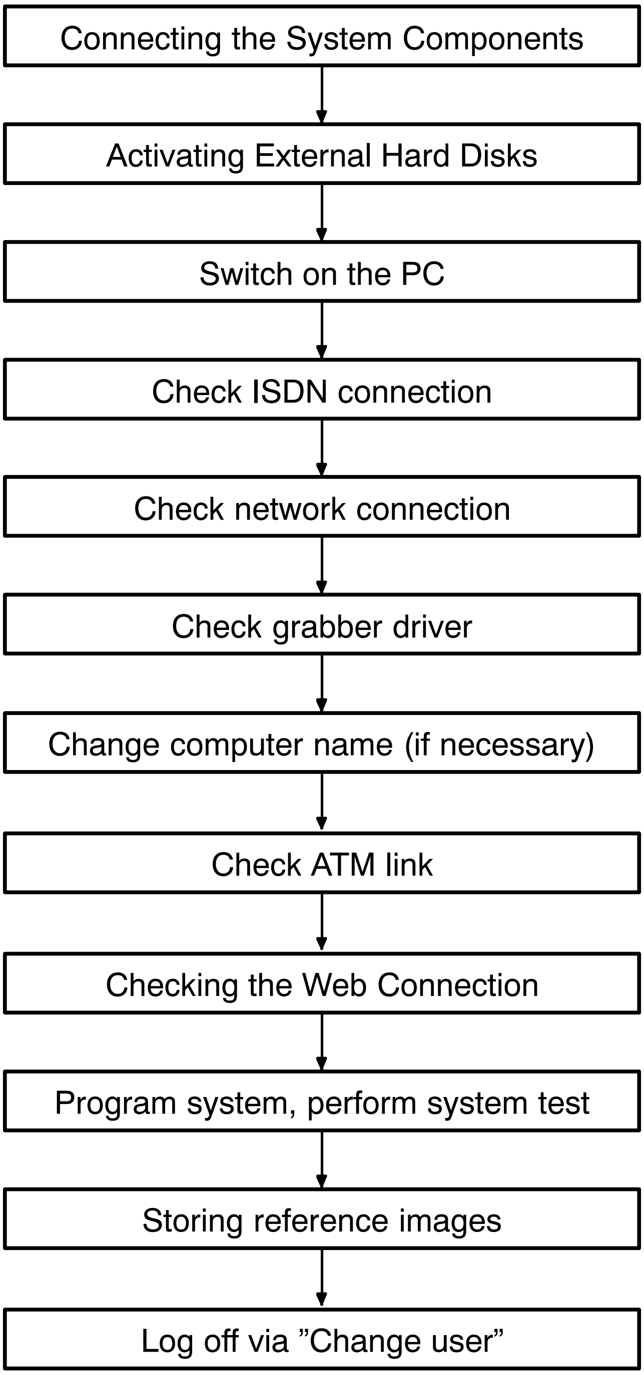
No.	Name	Description
1	Configuration data	
	Save	The configuration can be saved on the network drive or data medium. **Note:** For security reasons, the configuration should always be saved on an external data medium.
	Load	A new configuration can be loaded. The new configuration overwrites the current one.
2	Printout	
	Print	The configuration is printed.
	Preview	The configuration is shown as a preview.
3	Setup Wizard	It is possible to re–configure the system.
	Start	Click **Start**. Note, however, that if you do this, the configuration and image data will be deleted. During reconfiguration, you can select from – a basic configuration with which you create a basic configuration of the system with just a few mouse clicks, which you can then complete or – the standard configuration (expert configuration), with which you must enter the complete configuration. All settings and all image archives must be deleted before a re–configuration can be carried out. The system does this automatically after you have confirmed a warning message.

Configuration (continued)

4	Upload of the holiday program	You have the option here to adapt the holidays for the time program according to specific countries. The adjustment must be made in the*Holidays.xml* file.
	Upload	Click on **Upload** and answer the warning message with **Yes** if the current file is to be overwritten or with **Cancel** if you want to change the file. **Note:** Save the *Holidays.xml* file in Explorer, before you change it in Editor.
5	User data Set	Click on **Set**. You will see an entry box where you can enter information about the system documentation (e.g. contract number, customer).

7 Startup

Proceed as follows to start up the computer:


Connecting the System Components
Activating External Hard Disks
Switch on the PC
Check ISDN connection
Check network connection
Check grabber driver
Change computer name (if necessary)
Check ATM link
Checking the Web Connection
Program system, perform system test
Storing reference images
Log off via ”Change user”

7.1 Connecting the System Components

See Section 4.

7.2 Activating External Hard Disks

External hard disks must be activated before starting up the PC.

7.3 Switching On the PC (Startup)

1. Switch on the computer and the monitor.
   The computer carries out its startup procedure and automatically starts the video system. The startup procedure is complete when the log on dialog box of the video system appears. The video system is already running in the background.
2. Log on as the Administrator.

Note:

The system can be started from the Windows® XP level by clicking on the ”Start → All Programs → DiBos” menu.

7.4 Checking the Optional ISDN Connection

General requirements

For data transfer via ISDN, the connection must support the DSS1 protocol. For S_0 connections in PABXs this must be enabled first in the PABX. The data service also has to be enabled in both directions (incoming and outgoing) for this connection.

Requirements for the video system

Check whether the ISDN driver has started.
Proceed as follows:

1. Start your PC and open the live image.
2. Exit the video system as the Administrator.
3. Select ”Start → Control Panel→ Performance and Maintenance → System”.
4. Select the ”Hardware” tab.
5. Click the ”Device Manager” button.
6. In the tree structure, open the ”Network Adapter” directory by double–clicking on it.
7. Double–click on the entry ” AVM ISDN –Controller Fritz Card PCI V2.0”.
   The status of the driver is displayed in the ”Device status” field.
8. You can restart with ”Start → All Programs → DiBos”.

7.5 Checking the Optional Network Connection

Networking details

The following details are required from the network operator for starting up and checking the network:

- IP address
- Subnet mask
- (Gateway)

Notes for checking the network

Use the following test programs to start up and check the network:

1. Select ”Start → All Programs → Accessories → Command prompt” .
2. The following commands are available:

   ping
   This command is only available if the TCP/IP protocol is installed.

   ping localhost
   This program checks communication with its own computer. Networking is a requirement for token ring.

   ping <Name of remote station> or
   ping <TCP/IP address of the remote station>
   This program checks communication with the remote station.

   arp –a
   The program displays other computers after contact has been established with them.

   ipconfig
   Displays all current TCP/IP network configuration values
   (IP address, subnet mask, standard gateway)

   tracert <Name of the remote station>
   This program determines the route to a destination.

   net view
   Shows all available remote stations.

7.6 Checking the Grabber Driver

Make sure the grabber driver has started.

1. Start up your computer as far as the live image.
2. Exit the video system as the Administrator.
3. Select ”Start → Control Panel” and click ”Sounds, Speech, and Audio Devices.” On the Properties dialog box that opens, select the ”Hardware” tab and click on ”MVTitan” in the list. The display ”Device status: the device is operational” shows you that the grabber driver is started.
4. You can restart via ”Start → All Programs → DiBos”.

7.7 Changing the Computer Name

Change the name of the local computer if necessary:

1. Change from the video system level to the Administrator level (see Section 5.1).
2. Select ”Start → Control Panel →Performance and Maintenance→ System→ Computer Name→ Change” and make the following entries for

”Computer name:	<Computer name><Computer number>”
”Workgroup:	<Computer name>_NETWORK”
3. Click ”OK” again.
4. Log on as a Windows® XP user (see Section 5.2).

7.8 Checking the Optional ATM Connection

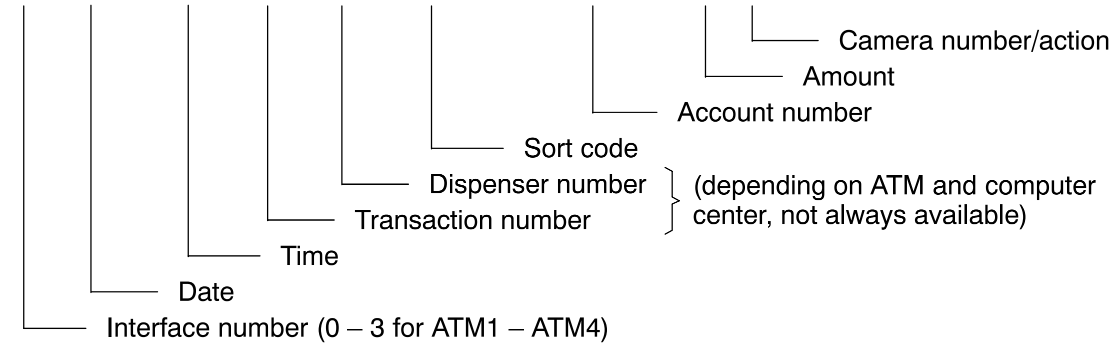
The data telegram between the video system and ATM can be checked using the ”Hyper Terminal” program in Windows® XP.

- Start the program via the ”Start → All Programs → Accessories → Communications → Hyper Terminal” menus.
- After startup enter a name (test name) in the dialog box and confirm your entry.
- In the next dialog box select the interface to which the interface processor is connected (input box ”Connect using”). Confirm with ”OK”.
- Enter the following parameters:
  - Baud: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
    Confirm the entries with ”OK”.
- From the ”File → menu, select Properties → Settings → ASCII–Settings” and activate the ”Append line feeds to incoming line ends” check box. Confirm with ”OK”.

Programming of the Hyper Terminal is now complete. The data can be evaluated.

Data telegram between video system and interface processor:

Telegram	Remarks
■1■280897■1318■08896■ ■ ■ ■ ■1■■	Card in ATM
■1■280897■1318■08896■ ■82054135■0532037398■ ■ ■■	Card recognized by ATM
■1■280897■1318■08896■ ■82054135■0532037398■220■ ■■	Amount entered
■1■280897■1318■08896■ ■82054135■0532037398■220■2■■	Take money
■1■280897■1318■08896■ ■82054135■0532037398■220■ ■■	Money withdrawal
■1■280897■1318■08896■ ■82054135■0532037398■220■ ■■	End of transaction


Camera number/action
Amount
Account number
Sort code
Dispenser number
Transaction number
(depending on ATM and computer center, not always available)
Time
Date
Interface number (0 – 3 for ATM1 – ATM4)

Note:
Action 1 = message ”Card in ATM”
Action 2 = message ”Take money”
Some ATMs display a message as soon as the card is inserted, but without a sort code and account number. Other ATMs only display a message when the sort code and account number have been read and the pin has been correctly entered.

7.9 Checking the Optional Web Connection

Check whether access can be obtained after activating the web application whether access can actually occur.

Proceed as follows:
1. Start the web browser (Internet Explorer 5.x and later or Netscape Navigator 7.x and later).
2. In the browser enter the address ”http://hostname”.
   Either the IP address or the name of the computer, on which the web server is installed, can be entered as the ”host name” .
   The log on screen of the Web application for the video system is displayed once the connection has been established. You can now log on.

7.10 System Test

After programming, check the basic functions required by the customer to ensure that they have been correctly set.

7.11 Storing reference images

Create a directory for storing reference images, e.g. ”C:\Reference images”. Save an image of the best quality per camera in this directory (”Image <Camera no>.JPG”) and print the images out two times apiece.

7.12 Log off

When you exit the system, make sure you leave the status as unoperated.
- Log off in the user interface of the video system via the ”System → Change user” menu.
  The log on dialog box appears to log on again.
  The system continues to run unoperated in the background.

8 Fault Indication/Correction

This section contains notes on faults that may occur when first starting up or during operation.
If you cannot determine the cause of the fault, please contact ”Product Service Video” of the video system manufacturer.

Fault	Possible Cause	Remedy
Next to the symbols for the grabber’s inputs and outputs, a “?” appears.	The grabber driver has not started, the grabber card or the signal connector is faulty.	Restart the driver, replace the grabber card or check the signal connector.
All SecSys inputs are longer than 10 s in alarm state.	Interface malfunction with SecSys.	Correct interface malfunction.
Message ”Hardlock not found”	Hardlock (dongle) missing or feature is not enabled.	Insert hardlock or add feature.
Fault indicator, error message		
– Video signal of a camera missing	–	– Check video signal
– Alarm memory (tee–off) is full	–	– Manually delete alarm images
– Hard disk is full	– 50 MB or more not available on any drive	– Connect external hard disks or check programming
– Images cannot be written	– Images are written in too many archives	– Adjust Recording
Software feature is not functioning	Check that the hardlock has been enabled	Enable hardlock is visible in the ”?” –> ”About” menu
The external hard disks are not being detected by the system	– Terminator missing	– Insert terminator
	– The hard disk ID has been assigned twice	– Assign the hard disk IDs in ascending order
	– The hard disks are not formatted	– Use the hard disk manager to format the hard disks in NTFS.
No ISDN connection	– The connection password of the transmitter and the receiver are not the same	– Check the connection password
	– Incorrect protocol set	– Select the correct protocol (EURO–ISDN) via an ISDN–PCI Setup.

9 Maintenance and Service

9.1 Maintenance Tasks to be Carried Out

Perform the following maintenance tasks:

- On the video system itself:
  - Check all cable connections are secure
  - Check the fan and clean it if necessary
  - Clean the screen if it is dirty
  - Check the system time and correct it if necessary
- Check the quality (e.g. focus, brightness, contrast) of the last five images stored for each camera.
- Randomly check the images saved in the archives (e.g. for image quality and additional data).
- Activate at least once by a SecSys (if connected) or a directly connected contact.
  Check the images saved in the archives and then delete them.
- Check the utilization of the alarm tee–offs. Images of the tee–off may be deleted by agreement with the customer.
- Clean all freely accessible cameras and lenses as well as dome cameras and front screens of outdoor cameras. Check the connecting cables and connectors.
- Compare the reference images printed or saved during installation of the system with the live images of the corresponding cameras in terms of their direction. The customer is responsible to the Verwaltungs–Berufsgenossenschaft (BGV) (German administrative professional association) for the set picture detail.
- According to UVV Kassen a functional test has to be done at least once every month (UVV Kassen = German for Accident Prevention Regulation for Banks). Ensure the SP 9.7/7 (Requirements of optical room surveillance systems).
- Check the customer's printer (1 printout).
- Set up a test connection for ISDN.
- For ATM link:
  - check the connecting cables on the interface processor and OVS
  - check the transfer of transaction data
  - check the display of access control data (connecting cables for access control)
- Document all work carried out in the logbook.

Attention:

All work carried out on the system that can interfere with recording may only be carried out after consulting the customer. With regard to UVV–related equipment (UVV = German for Accident Prevention Regulation for Banks), it is best to do such work outside of opening hours.

Replace the system (without the dongle) in the event of a fault. The video system manufacturer will provide loan equipment for the interim period.

Maintenance work to be carried out by the user

The user is responsible for:

- Replacing the toner cartridge of laser printers
- Refilling printer paper or the paper tray of the video printer
- Replacing the ink cartridge of ink–jet printers.

9.2 Software update

Software installation is carried out by the Windows® XP Administrator.

9.3 Error Forwarding

Three methods are pre–configured and provided as examples. The ”error_forwarding.cmd” file contains calls for all methods.
”error_forwarding.cmd”:

With ”net send”:	rem Send messages to other computers on the network rem net_send.cmd %1 %2 ”COMPUTER NAME”
With Outlook: [1] [2]	rem Use Outlook to send an e–mail (does not work with Outlook Express)* rem wscript outlook_mail.vbs %1 %2 ”mail@adress.com”
With SMS: [2]	rem Send an SMS rem wscript MessageMaster_sms.vbs %1 %2 ”0172 . . . ”

[1] Not possible with Outlook Express

[2] Check with national service providers whether software can be used

The fault transmission applies also for relay 4 if this was specified in the configuration (Hardware/Connections menu). For information about the events that trigger a fault transmission, please see the Chapter 4.10.

9.3.1 Sending a Message in the Windows Network Using ”net send”

The Windows® XP command ”net send” sends messages to other computers on the network. Please refer to the Windows® XP online help for a detailed description of the command. If the addressed computer cannot be reached or is not switched on, the message is lost.
To activate this method, ”rem” must be removed from the following line in the ”error_forwarding.cmd” file:

rem net_send.cmd %1 %2 ”COMPUTER NAME”

. The computer name of the addressed computer must be entered in place of ”COMPUTER NAME”.

9.3.2 Sending an E–mail Using Outlook

If Outlook is installed on the computer, an e–mail can be sent in the event of a fault (not possible with Outlook Express).
To activate this method, ”rem” must be removed from the following line in the ”error_forwarding.cmd” file:

rem wscript outlook_mail.vbs %1 %2 ”mail@address.com”

The e–mail address of the receiver must be entered in place of ”mail@customer.com”.

9.3.3 Sending an SMS

If the computer is connected via an ISDN or analog modem with the telephone network, an SMS can be sent (not possible with T–DSL).
To activate this method, ”rem” must be removed from the following line in the ”error_forwarding.cmd” file:
rem wscript MessageMaster_sms.vbs %1 %2 ”0172 . . . ”
. The telephone number of the SMS receiver must be entered in place of ”0172 . . . ”. For telephone numbers in the D2 network, ”+49” must be entered in place of the ”0”.
The SMS is sent using the ”MessageMaster” program. As every network operator uses their own method to receive SMS messages via modem, the ”MessageMaster” program of the network operator must be informed of this. This is done using the ”MMCFG.exe” configuration program.

Proceed as follows:

1. Execute the ”MMCfg.exe” file.
2. Select the ”Message–Master Modem/ISDN” entry from the list box and click ”Config.”.
3. Make the following entries in the ”Configuration” dialog box:
   - Select the modem in the ”Device” option group.
   - Click on the ”Defined services” tab and select the telephone number of the appropriate network operator.
     All available network operators are stored in the ”Services.inf” file. These can be loaded by clicking ”From File...”. Ensure that some of the network operators between the analog modem and the ISDN modem are different. Depending on the modem connected, either ”D1 Alpha Service (D)” or ”D1 Alpha Service ISDN (D)” should be selected, whereby only one service can be selected.
4. Confirm with ”OK”.

9.3.4 Testing Error Forwarding

Configuration of error forwarding can be tested using the ”test_error_forwarding.cmd” file, without the video system generating a fault message. A fault with fault number 1 and fault text ”DiBos Fault Test” is generated.

9.4 Troubleshooting

The following faults have to be rectified if necessary:

- Counter light
  If recordings show impairment due to counter light, either block out the light source, e.g. through curtains on windows or shades on lights, or change the location of the camera.
- Reflections
  If the optical room surveillance system is installed inside special glazing to hinder bullets or break–in attempts, the lighting may produce unfavorable reflections. These are stronger as the intensity of the light inside the glazing becomes higher. Reflections of this kind can be reduced if the area outside the glazing is lit better and the cameras are positioned nearer to the glazing. Reflections can often be avoided by darkening light sources behind or next to the camera. If these measures do not help matters, a polarizing filter can be placed in front of the lens.
- Focus
  When checking the recordings, make sure that persons and objects inside the area of surveillance are in good focus.
  The gray or ND filter can be used in front of the lens to improve the focus.
- Dirt
  The quality of recordings is often impaired by dirt on the lens or the screen of the enclosure.

Functional interference can often be eliminated by:

1. Disconnecting and reestablishing the local or remote connection in the video system program
2. Exiting the program followed by a restart
   or
3. A warm start or switching the system off and back on (waiting approximately 20 s in between)

If this does not result in normal operation, check the programming.

If the fault cannot be rectified, the system must be replaced.

10 Technical data

Video System in 19” Housing

Operating system	Windows® XP
Hard disk	120 GB minimum
RAM	256 MB DDR
Video	AGP (on–board)
Network	Ethernet (on–board)
Sound	on–board
Connections (on rear)	see Section 2
Expansion slots	From left to right: • One slot for AGP graphics card • 6 slots for 32–bit PCI cards
Mouse/keyboard	Mouse/keyboard with mini DIN connection
Power unit	
• Input voltage	100 ... 120 V AC and 200 ... 240 V AC at 50/60 Hz (manual switchover)
• Power consumption	Approximately 100 W (typical)
• Power supply	Approximately 465 W
Storage temperature	233 K ... 343 K (–40° C ... 70°C)
Relative humidity in storage	8% ... 80% (relative humidity)
Operating temperature	278 K ... 313 K (5° C ... 40°C)
Relative humidity in operation	15% ... 80% (relative humidity)
Weight	Approximately 27 lb / 12 kg (without keyboard/monitor)
Dimensions (W x H x D)	Approximately 19,1 x 7,1 x 21,2 in / 48,5 x 18 x 54 cm (with dongle)

Technical Data (continued)

Grabber card MVTitan	max. 2x
Video inputs	16
Contact inputs	16 (either N/C contact or N/O contact)
Relay outputs	8 (or 7x output and 1x fault indicator for 1st grabber card)
Compression rate	Can be set between 10 ... 30 Kbytes
Image file capacity	Depending on compression Standard size approximately 15 KB UVV size approximately 28 KB (UVV = German for Accident Prevention Regulations for Banks)

Grabber card MVSigma	max. 1x
Video inputs	4
Contact inputs	5 (either N/C contact or N/O contact)
Compression rate	Can be set between 10 ... 30 Kbytes
Image file capacity	Depending on compression Standard size approximately 15 KB UVV size approximately 28 KB (UVV = German for Accident Prevention Regulations for Banks)

11 End user license agreement (EULA)

You have acquired a device (DiBos) that includes software licensed by Bosch Security Systems from Microsoft Licensing Inc. or it's affiliates ("MS"). Those installed software products of MS origin, as well as associated media, printed materials, and "online" or electronic documentation Windows®XP are protected by international intellectual property laws and treaties. The SOFTWARE is licensed, not sold. All rights reserved.

IF YOU DO NOT AGREE TO THIS END USER LICENSE AGREEMENT ("EULA"), DO NOT USE THE DEVICE OR COPY THE SOFTWARE. INSTEAD; PROMPTLY CONTACT BOSCH SICHERHEITS–SYSTEME GMBH FOR INSTRUCTIONS ON RETURN OF THE UNUSED DEVICE(S) FOR A REFUND. **ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON THE DEVICE, WILL CONSTITUTE YOUR AGREEMENT TO THIS EULA (OR RATIFICATION OF ANY PREVIOUS CONSENT).**

GRANT OF SOFTWARE LICENSE. This EULA grants you the following license

- You many use the SOFTWARE only on the DEVICE.
- **NOT FAULT TOLERANT.** THE SOFTWARE IS NOT FAULT TOLERANT. BOSCH SECURITY SYSTEMS HAS INDEPENDENTLY DETERMINED HOW TO USE THE SOFTWARE IN THE DEVICE, AND MS HAS RELIED UPON BOSCH SECURITY SYSTEMS TO CONDUCT SUFFICIENT TESTING TO DETERMINE THAT THE SOFTWARE IS SUITABLE FOR SUCH USE.
- NO WARRANTIES FOR **THE SOFTWARE. THE SOFTWARE is provided "AS IS" and with all faults. THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY, AND EFFORT (INCLUDING LACK OF NEGLIGENCE) IS WITH YOU. ALSO, THERE IS NO WARRANTY AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE SOFTWARE OR AGAINST INFRINGEMENT**. IF YOU HAVE RECEIVED ANY WARRANTIES REGARDING THE DEVICE OR THE SOFTWRE, THOSE WARRANTIES DO NOT ORIGINATE FROM, AND ARE NOT BINDING ON, MS.
- **Note on Java Support.** The SOFTWARE may contain support for programs written in Java. Java technology is not fault tolerant and is not designed, manufactured, or intended for use or resale as online control equipment in hazardous environments requiring fail–safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of Java technology could lead directly to death, personal injury, or severe physical or environmental damage. Sun Microsystems, Inc. has contractually obligated MS to make this disclaimer.
- No Liability for Certain Damages. **EXCEPT AS PROHIBITED BY LAW, MS SHALL HAVE NO LIABILITY FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES ARSISING FROM OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE SOFT–WARE. THIS LIMITATION SHALL APPLY EVEN IF ANY REMEDY FAILS OF ITS PURPOSE. IN NO EVENT SHALL MS BE LIABLE FOR ANY AMOUNT IN EXCESS OF U.S. TWO HUNDRED FIFTY DOLLARS (U.S.$250.00).**

End user license agreement (continued)

- **Limitations on Reverse Engineering, Decompilation, and Disassembly.** You may not reverse engineer, decompile, or disassemble the SOFTWARE, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.
- **SOFTWARE TRANSFER ALLOWED BUT WITH RESTRICTIONS.** You may permanently transfer rights under this EULA only as part of a permanent sale or transfer of the Device, and only if the recipient agrees to this EULA. If the SOFTWARE is an upgrade, any transfer must also include all prior versions of the SOFTWARE.

- **SOFTWARE TRANSFER ALLOWED BUT WITH RESTRICTIONS.** You may permanently transfer rights under this EULA only as part of a permanent sale or transfer of the Device, and only if the recipient agrees to this EULA. If the SOFTWARE is an upgrade, any transfer must also include all prior versions of the SOFTWARE.

Notes

Notes

Bosch Security Systems,Inc.
850 Greenfield Road
Lancaster, PA 17601 U.S.A.
Tel: 800–326–3270
Fax: 1–717–735–6560

Bosch Security Systems B.V.
P.O. Box 80002, 5600 JB
Eindhoven
The Netherlands
Tel: 31 40 278 1222
Fax: 31 40 278 6668

Bosch Security Systems Pte Ltd
38C, Jalan Pemimpin
Singapore 577180
Republic of Singapore
Tel: 65 (6) 319 3486
Fax: 65 (6) 319 3499

BOSCH