ExCam[®] XI410

User Manual





Table of contents

1	Intro	oduction	.4
2	Тес	hnical data	.4
	2.1 2.2 2.3 2.4 2.5 2.6 2.7	Explosion protection Illustration of the model key Electrical parameters of the camera System cable SKDP03-T Optical specifications Video-technical characteristics Other technical data	.4 .5 .6 .6 .8
3	Safe	ety Instructions	.9
4	Inst	allation	11
5	Elec	ctrical connection	13
	5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8 5.8.1 5.8.2 5.8.3 5.8.4 5.8.5 5.8.6	Potential equalization	13 14 14 17 19 20 20 20 21 22 22 23
6	Net	work access and visualization	24
	6.1 6.2 6.3	Minimum system requirements	24 24 24
7	Visu	alization/ Analysis Software PIX Connect	28
	7.1 7.2 7.3 7.4	General information about PIX Connect Focusing the thermal image Adjustment of temperature range User interface	28 28 28 29
8	Clea	aning	30
9	Mai	ntenance / Modification	30
10) D	isposal / Recycling	30
11	l D	rawings & 3D models	31



Table of Figures and Charts

Table 2-1 Model key	5
Figure 2-3 Sectional view of SKDP03-T	6
Table 2-2 Measurement field and pixel size	7
Table 2-3 Other technical data	8
Table 4-1 Mounting accessories	12
Figure 5-1 ExCam XI410 Potential equalization	13
Table 5-1 Potential equalization	13
Figure 5-2 ExCam XI410 T08-VA0.4.K1.GER-N.N-xxx.N-P	14
Figure 5-3 ExCam XI410 T08-VA0.4.K1.GER-N.N-xxx.N-T	14
Figure 5-4 Video Tutorial ExTB-3	15
Figure 5-5 Pin assignment of the cable SKDP03-T	15
Table 5-2 Wire assignment of terminal box ExTB-3(SKDP03-T)	15
Figure 5-6 Wired terminal box ExTB-3	16
Figure 5-7 ExTB-3 -> Safe area	17
Figure 5-8 Plug assignment RJ45	17
Figure 5-9 Plug assignment, RJ45	
Figure 5-10 Ex-d cable selection	19
Figure 5-11 PIF connections	21
Figure 5-12 Connection of 3 PIFs	
Figure 5-13 Fail-Safe monitoring states	23
Figure 7-1 Motorized focus settings in PIX Connect Software	
Figure 7-2 Adjust temperature range	
Figure 7-3 User interface	

History of revisions

Product:	ExCam [®] XI410
Title:	User Manual for ExCam [®] XI410
DocId.	220316-PT08BA-ES-ExCam XI410_en_rev.02.docx
Author:	Eva Schneider, Grad. Eng. (UAS)
Created on:	16.03.2022

Rev.	Date	Name	Comment	Approved by
Index				
0	16.03.2022	E. Schneider	Compilation of the document	
1	11.10.2022	E. Schneider	Extension for optional accessory	
			Industrial Process Interface	
2	12.12.2022	E. Schneider	Several corrections	



1 Introduction

The ExCam XI410 is a powerful thermographic camera with an integrated infrared thermometer and motor focus for use in potentially explosive areas. It delivers excellent infrared images (384x240p) of objects in a temperature range from -20°C to 900°C. In addition, the thermal imaging camera has extensive analysis functions (e.g. thermal analysis with hot and cold spots). The ExCam XI410 cannot only see where it is hot, it can also measure the temperature exactly. When designing the ExCam XI410, our main focus was on safety, mechanical precision and high quality of stainless steel.

Like all cameras of the ExCam series, it is certified according to European regulations (ATEX) as well as international ones (IECEx). The explosion-protected housing is approved for the ATEX group II for zones 1, 2, 21 and 22 including the explosion groups IIC / IIIC. For more information please visit our website at www.samcon.eu/en

2 Technical data

2.1 Explosion protection

Identification marks	$\langle \widehat{\mathbf{Ex}} \rangle$ II 2G (zone 1 and 2)
acc. to Directive 2014/34/EU:	$\langle \widehat{\mathbf{Ex}} \rangle$ II 2D (zone 21 and 22)
Explosion protection (gas):	Ex db IIC T6 Gb
Explosion protection (dust):	Ex tb IIIC T80°C Db
Protection class camera:	IP66/68 (IEC /EN 60529)
Protection class terminal box:	IP66 (IEC /EN 60529)
Transport/storage temperature:	-40°C+70°C
Ambient temperature (EX):	-10°C+50°C
Named testing laboratory:	TÜV Rheinland (number 0035)
EU type approval certificate:	TÜV 18 ATEX 8218X (2021)
IECEx Certificate of Conformity:	TUR 18.0023X (2021)
Other certificates see:	https://www.samcon.eu/en/products/network/excam-xi410/



Attention!

The instructions stated on the type plates have to be observed!



2.2 Illustration of the model key

1)	2)	3)	4)	5)	6)	7)
Ex product-	Туре	Housing-	Temp	Cable	Cable	Optic
name		combination	range	length [m]	termin.	
ExCam XI410	T08-	VA0.4.K1.GER-	N.N-	005.N-	P-	018/029/
						053/080
	T08-	VA0.4.K1.GER-	N.N-	005.N-	Т-	018/029/
						053/080

Table 2-1 Model key

Explanations:

1)	ExCam XI 410 =	Functional camera description of the ExCam Series (technical data/ specification of the individual <u>camera module</u>)
2)	T 08 =	SAMCON Production- Type 08
3)	VA0 .4.K1.GER =	T07 ex d housing (stainless steel 1.4404) with small diameter $Ø_{VA0}$ =48mm)
	VA0. 4 .K1.GER = VA0.4. K1 .GER =	T07 VA0.4 housing with <u>maximum body length</u> (L _{.R} = 171.2mm) <u>K1</u> cable gland flange
	VA0.4.K1. GER =	Germanium sight glass, suitable for thermographic applications (MIR/ FIR)
4)	N. N =	Normal ambient temperature range ($T_{amb} > -10^{\circ}C$)
	N. N =	No high temperature battery installed ($T_{amb} < +50^{\circ}C$)
5)	005. N =	Length of the connection line in meter at delivery; 5m is the standard cable length, max. cable length is: <u>005100</u> [m]
	005. N =	Non armoured cable
6)	P =	Plug- termination (standard)
		CAT6, <u>RJ-45 plug</u> , AWG 26-22,
	TD =	Terminal Box Ex-e termination (optional)
7)	0XX =	Different optics available: 18°, 29°, 53° and 80°



2.3 Electrical parameters of the camera

Power supply of the camera:

Voltage supply:	24 V DC
Reference voltage:	10 - 30 V DC
Maximum power consumption:	2.5 W
Typical power consumption:	< 2.0 W

2.4 System cable SKDP03-T

Outside diameter:	12.40 ± 0.3 mm				
Bending radius:	$8 \text{ x} D_a$ when installed and $4 \text{ x} D_a$ after relocation				
Data line:	4 x 2 x AWG23/1 CAT.6				
Performance elements:	3G1.5 (BK-BU-GN/YE)				
Properties:	PUR halogen-free, flame-retardant, UV-re-				
	sistant, chemical resistance, shielded				

Quick link:

https://www.samcon.eu/fileadmin/documents/en/60-Assembling%26mounting/SKDP03-T_Datasheet.pdf





Figure 2-3 Sectional view of SKDP03-T

2.5 Optical specifications

A selection of lenses offers the possibility to precisely measure objects in different distances; we offer lenses for close, standard and large distances. Please note that the ExCam XI410 has a fixed optic. A change of optics is not possible. The following table shows a relationship between the measurement object distance and the pixel size on the object level.

HFOV: Horizontal field of view VFOV: Vertikal field of view DFOV: Diagonal field of view IFOV: Instantaneous field of view (size of the single pixel on object level)



53°-optic

					D	Distance to measurement object [m]							
		0,05	0,1	0,2	0,3	0,5	1	2	4	6	10	30	100
Enlargement of	HFOV		0,100	0,200	0,300	0,490	0,990	2,000	4,000	5,900	9,900	29,700	98,900
total measuring	VFOV		0,057	0,110	0,170	0,280	0,550	1,100	2,200	3,300	5,500	16,500	54,900
level [m]	DFOV		0,115	0,230	0,340	0,570	1,130	2,300	4,500	6,800	11,300	33,900	113,100
Size of the													
single pixel													
[mm]	IFOV		0,300	0,500	0,800	1,300	2,600	5,100	10,300	15,500	25,800	77,200	257,400

18°-optic

					D	istance	to measu	urement	object [n	 n]			
	0,05	0,1	0,2	0,3	0,5	1	2	4	6	10	30	100	
Enlargement of	HFOV			0,069	0,102	0,170	0,330	0,660	1,310	2,000	3,300	9,800	32,600
field at object	VFOV			0,043	0,064	0,100	0,210	0,410	0,820	1,200	2,100	6,100	20,500
level [m]	DFOV			0,081	0,120	0,200	0,390	0,780	1,550	2,300	3,900	11,500	38,500
Size of single													
pixel [mm]	IFOV			0,200	0,300	0,400	0,900	1,700	3,400	5,100	8,500	25,500	84,800

29°-optic

		Distance to measurement object [m]											
	0,05	0,1	0,2	0,3	0,5	1	2	4	6	10	30	100	
Enlargement of	HFOV		0,059	0,112	0,170	0,270	0,530	1,070	2,100	3,200	5,300	15,900	52,900
field at object	VFOV		0,036	0,068	0,100	0,160	0,320	0,640	1,300	1,900	3,200	9,500	31,700
level [m]	DFOV		0,069	0,131	0,190	0,320	0,620	1,240	2,500	3,700	6,200	18,500	61,600
Size of single													
pixel [mm]	IFOV		2,000	0,300	0,400	0,700	1,400	2,800	5,500	8,300	13,800	41,300	137,700

80°-optic

					D	istance	to measu	urement	object [n				
		0,05	0,1	0,2	0,3	0,5	1	2	4	6	10	30	100
Enlargement of	HFOV	0,084	0,160	0,320	0,480	0,810	1,600	3,300	6,500	9,800	16,600	49,900	166,400
field at object	VFOV	0,044	0,080	0,170	0,250	0,410	0,800	1,600	3,200	4,800	8,000	24,100	80,400
level [m]	DFOV	0,095	0,180	0,360	0,540	0,910	1,800	3,600	7,300	10,900	18,500	55,400	184,800
Size of single pixel [mm]	IFOV	0,200	0,400	0,800	1,300	2,100	4,200	8,500	16,900	25,500	43,400	130,000	433,200

Table 2-2 Measurement field and pixel size

For distances smaller than the minimum measuring distance (0.35m@18°/29°; 0.25m@53°; 0.2m@80°), the measuring accuracy can be outside the specification.

As an alternative to the table, you can use the Optris GmbH <u>opticcalculator</u>: <u>https://www.optris.de/optikkalkulator-fuer-waermebildkameras</u>



Or the free optris Optikkalkulator App: Optris calculator – Apps bei Google Play





2.6 Video-technical characteristics

We use the Optris Xi410 Spot-finder IR-Camera in a pressure-resistant enclosure. For details, please refer to the Product Documentation, video-technical data of optris[®]:

https://www.optris.com/xi-410



2.7 Other technical data

	Camera	Terminal box
Permissible ambient temperature	-10°C +50°C	-60°C +55°C
Protection class as per EN	IP66/68	IP66
60529/IEC 529	(Test conditions: 0.5h/8m	
	water column 5°C)	
Housing material	Stainless steel, mat. no. 1.4404	Polyester resin
Weight	About 0.93 kg	1 kg
Dimensions	D48mm x 171.2mm	145mmx145mmx71mm
		Table 2-3 Other technical data



3 Safety Instructions

Please absolutely observe the installation instruction's safety directions of the T08 ExCam series!

Quick link:

https://www.samcon.eu/fileadmin/documents/en/22-Ex-Network-Cameras/ExCam-Series-T08-EX-Installation-Manual-2020.pdf

It is absolutely mandatory to adhere to the national safety regulations and regulations for prevention of accidents, as well as to the safety instructions given below in this User Manual!



Attention!

Cameras of type T08 ExCam are not suitable for use in zones 0 and 20. The ambient temperature, temperature class and explosion group written on the enclosure nameplate must be absolutely adhered to! The customer is not allowed to make any alterations of the camera! The camera must be operated in a proper and sound condition and only in the way intended.



Attention!

Repairs may only be carried out by using original parts from the manufacturer. Repairs which affect the explosion protection may only be carried out in accordance with the nationally applied regulations and exclusively by the manufacturer.



Attention!

The alignment of the camera to intensive energy sources (e.g. devices which emit laser radiation or reflections of such equipment) can cause an irreparable defect of the infrared detector. This is also valid if the camera is switched off.



Attention!

Devices of type T08-VA0.x.K1.GER may not be used in mining/ firedamp hazard (ATEX group 1) or in areas with high risk of mechanical stress (ATEX group 2).



Attention!

Prior to installation, take external sources of heat or cold into account! The temperature ranges prescribed for storage, transport and operating must be adhered to!





Attention! Adhere to the warnings given on the nameplate:

"WARNING – DO NOT OPEN IN HAZARD AREAS"



Using the camera in explosion-protected areas with regard to temperature and dust layers is defined in the respective national regulations.



When installing the ExCam, adhere to the requirements of the EN/IEC 60079-14.



4 Installation

For commissioning and operating the camera, the relevant national regulations, as well as the generally accepted rules of technology shall prevail. Before mounting the camera, thoroughly check it for any transport damage regarding the housing and cable. Installation, electrical connection and the first commissioning must only be carried out by qualified specialists.

Work preparation:



Attention!

Prepare your work carefully and in accordance with the relevant regulations.



Attention!

Depending on classification of hazard areas, it is imperative to obtain a work approval first!

When you open the pressure-resistant enclosure under voltage, it is absolutely necessary to prevent potentially explosive atmosphere!

To ensure the best image quality delivered by the network camera, plan the installation site carefully (consider object distance or size, angle and minimum object distance to the focus).

- Use appropriate tools and aids.
- When working, ensure a safe stand.
- Make sure that any static charge is avoided.



Attention!

Please observe the national security, installation and accident prevention regulations (e.g. DIN EN 60079-14) and the safety instructions in this User Manual, as well as the ones in the Installation Guidelines!



Attention!

Adhere to the provisions of the IECEx, ATEX and EX installation instructions for mounting and starting up!

The ExCam[®] XI410 consists of a flame-proof camera housing (T08 Ex-d) and an ex-e terminal box (VA0.4-...-T) or a Plug (VA0.4-...-P). The camera is equipped with a systemcable (5 to 100 m). Mount the camera according to the desired field of view. Install the terminal box so that a good accessibility is given, in order to facilitate the electrical connection.

Drawings for drill hole patterns and further information can be viewed on our product page:





Wall bracket WMB	WALL MOUNT BRACKET WMB-VA0.x/VA1.x Wall bracket for devices of T08-VA0-series Suitable for hanging the camera on walls. Material: stainless steel 1.4404 Weight: 0.68 kg Dimensions: 80 x 100 x 205 mm
Pole adapter PMB	POLE MOUNT EXCAM VA1.x (-) Pole apter for VA wall mount Material: stainless steel 1.4404 Suitable for pole diameters between 50 and 105 mm Load-bearing capacity: 45 kg Dimensions:120x180x130 at masts of Ø 60 mm)
Hinge attachment SCH	Hinge attachment SCH-VAx.x Hinge attachment for easy mounting on round sight glasses acc. to DIN 28120/28121 or similar for VA Material: stainless steel AISI 316L/1.4404 Weight: ca. 0.04 kg Dimensions WxHxD [mm]: 29.2x40x73.1

Table 4-1 Mounting accessories



5 Electrical connection



Attention!

The electrical connection of the equipment may only be carried out by qualified and skilled personnel!



Attention!

It is absolutely necessary to ground the ExCam[®] series' housing via the PA connection.



Attention!

Please observe the national security, installation and accident prevention regulations (e.g. DIN EN 60079-14) and the safety instructions in this User Manual, as well as the ones in the Installation Guidelines!

The delivered ExCam[®] XI410 is equipped with an electrical connection cable of the type SKDP03-T. The maximum transmission range from the camera to the next active network interface is 100 m and can be specified by the client. The user is NOT authorised to carry out any electrical connection work inside the pressure-resistant enclosure (T08).

5.1 Potential equalization



Figure 5-1 ExCam XI410 Potential equalization

Potential equalization/grounding of the camera housing is absolutely necessary, in order to avoid static charges and thus the formation of sparks. For this purpose, a screw terminal is provided at the rear side's bottom (see Figure 5-1). The cross-section of the potential equalization has to comply with the National Ground Rules (at least 4mm²). Wiring table:

Potential	Colour (IEC 60757)	Cross-sec-	Comment
		tion	
PA	GN/YE	4 mm ² (rigid)	Terminal: Slotted screw M3x0.5x5 (DIN 84) with washer Ø3,2mm (DIN 125A), Keep 1.2 Nm tightening torque!

Table 5-1 Potential equalization



5.2 Variants of cable termination

Figures 5.2 and 5.3 illustrate the cable termination of the ExCam XI410.



Figure 5-3 ExCam XI410 T08-VA0.4.K1.GER-N.N-xxx.N-T

5.3 Connection work at the device (terminal box)



Attention!

Never open the Ex-e terminal box under voltage!



Attention!

Adhere to the international installation regulations for connection chambers with increased safety (Ex-e).



Attention! Adhere to attached separate User Manual for the Ex-e terminal box.

Video Tutorial:

Observe our video tutorial:

"SAMCON 01 Wiring the cable SKDP03-T to the junction box ExTB-3" <u>https://go.samcon.eu/v01</u>







Figure 5-4 Video Tutorial ExTB-3

The pin assignment of the SKDP03-T is executed in accordance with the standard EIA/TIA-568B for 24VDC, as follows:



Figure 5-5 Pin assignment of the cable SKDP03-T

Camera (Ex-d)	Colour	Terminal	Cross-sec-	Comment
(T568B)	SKDP03-T	ExTB-3	tional sur-	
	(IEC60757)		face	
SHIELD		PE	1.5 mm ²	Shield
Tx+	WH/OG	1	0.26 mm ²	Solid conductor
Tx-	OG	2	0.26 mm ²	Solid conductor
Rx+	WH/GN	3	0.26 mm ²	Solid conductor
Rx-	GN	4	0.26 mm ²	Solid conductor
(GND ISO)	WH/BU	5	0.26 mm ²	Solid conductor
(AO / RS485 B)	BU	6	0.26 mm ²	Solid conductor
(AI/DI/RS485 A)	BN	7	0.26 mm ²	Solid conductor
(n.c.)	WH/BN	8	0.26 mm ²	Solid conductor
(n.c.)		PE		
VCC	BK	9	1.5 mm ²	24VDC
GND	BU	10	1.5 mm ²	0VDC
PE/PA	YE / GN	PE	1.5 mm ²	PE

Table 5-2 Wire assignment of terminal box ExTB-3(SKDP03-T)





Figure 5-6 Wired terminal box ExTB-3

Particularly in EMC critical environments, it is necessary to make sure that the cable shield is grounded on side of the terminal block! The maximum cable length is 100 m.



Attention!

Finally, check your network installation.



Attention!

Cables and wires must comply with the requirements of the IEC 60079-0/1/7 & 14.



Attention!

The supply line must have a sufficient cross-section. The cable protection must comply with national and international regulations.



Example: Direct routing from ExTB-3 to safe area



5.4 Plug-assignment (RJ45)





If the cable termination uses a plug, the latter should be plugged into the RJ45 slot of the network device (PSE). Prior to connecting it to the camera, the network device (PSE) can



already be supplied with power, hence there is no "power ON" priority which has to be observed.



Attention!

Use appropriate RJ45 plugs! Check the cable shielding, cross-section and the outside diameter!



Attention!

It is imperative to ensure a correct routing of the individual wires according to the EIA/TIA-568B"

Detailed instructions on how to connect an RJ45 plug are available in our video tutorial: "SAMCON 03 Mounting and installing the RJ45 jack to SAMCON cables" <u>https://go.samcon.eu/v03</u>





Figure 5-9 Plug assignment, RJ45



5.5 Appropriate cables & cable entries

An integral part of the device safety is the correct selection of the cables, wires and cable entries.



Attention!

Cables and wires must comply with the requirements of the IEC 60079-0/1/7 & 14.



Attention!

The supply line must have a sufficient cross-section. The cable protection must comply with national and international regulations.

For non-binding configuration and planning guidelines, please visit our website:

Perhaps our video will help you: "Cables for flameproof devices in potentially explosive atmospheres" http://go.samcon.eu/video-cable-ex





Figure 5-10 Ex-d cable selection

5.6 Fusing

The power supply fusing depends on the cable cross-section and length. 300 mA mT- fuse is recommended.



Attention!

Please pay attention to the national and international regulations regarding selectivity and line protection.



5.7 Tests prior to switching on voltage



Attention!

Prior to starting the device, perform all tests as indicated by the national regulations. Furthermore, check the correct function and installation of the device in accordance with this User Manual and other applicable regulations.



Attention!

Incorrect installation or operation of the camera may lead to a loss of warranty!



Attention!

Do not switch on the camera at temperatures below 0°C!

5.8 Optional accessory: Industrial Process Interface (PIF)

An industrial process interface with 500 VACeff insulation voltage between ExCam XI and process is available for permanent monitoring of hardware and software during operation. The PIF is equipped with self-monitoring (fail-safe mode) so that states such as interruptions in the cable connection, termination of the software, etc. can be recorded and output as an alarm. The fail-safe time constant is 1.5 seconds. The PIF is not explosion-proof and may therefore only be used in safe areas.

5.8.1 Process Interface of the camera

Name	Description	Max. range / status
AI	Analog Input	0 - 10 V ¹⁾
or	Digital Input	24 V
DI	(Low-aktive = 0 0.6 V)	
AO	Analog Output	0/4 – 20 mA
	Alarm Output	0/4 – 20 mA

ExCam XI 80/410 offers the following direct In- and Outputs:

1) the AI is designed for max. 24 V, voltage level above 10 V is not interpreted

In addition the above direct in- and outputs the ExCam XI80/410 has a RS485- interface. This interface can be used to control the external, industrial PIF. When using the RS485 interfacethe direct out- and inputs are not available.

If the process interface of the camera is directly connected to external hardware (without using the supplied PIF cable) an activation of the field "Support proprietary PIF cable" in the menu Tools/ Configuration/ Device (PIF) in the PIX Connect Software is necessary.





Consider that the input of the PIF is not protected if there is a direct PIF connection! A voltage > 3 V on the INT-pin will destroy the device!

5.8.2 Pin assignment Industrial Process Interface (PIF)



GN	RS485 B
YE	RS485 A
WH	12 V
BN	GND
SHIELD	GND

Figure 5-11 PIF connections

5.8.3 Programmable functions PIF

Analog Input (AI)	Emissivity embient temperature, reference temperature, up
Analog Input (AI)	Emissivity, ambient temperature, reference temperature, un-
	committed value, flag control, triggered recording, triggered
	snapshots, triggered line-scanner, triggered event grabber,
	reset peak-/valley-hold, switch temperature range
Analog Output (AO)	Main measure area, measure area, internal temperature, flag
	status, recording status, line scan status, alarm, frame sync,
	fail-safe, external communication, autonomous status
Digital Output (DO)	Flag status, recording status, line scan status, alarm, frame
	sync, fail-safe, external communication, autonomous status



5.8.4 In- and outputs

Name	Description	Max. range ¹⁾ / status
INPUT	Analog- or digital input	0 - 10 V ²⁾
1/2/3		
AO 1/2/3	Analog output 1, 2 and 3	0 – 10 V
	Alarm output 1,2 and 3	0/4 – 20 mA
DO 1/2/3	Relay output 1,2 and 3	open/closed (red LED on)/ 030 V,
	Alarm output	400 mA
		0/4 – 20 mA
FS	Fail-safe relay	open/closed (green LED on)/ 030
		V, 400 mA

1) depending on supply voltage; for 0-10 V on the AO the PIF has to be powered with min. 12 V. 2) the AI is designed for max. 24 V, the voltage level above 10 V is not interpreted

5.8.5 Extension up to 9 outputs

The industrial PIF has a maximum of 3 analog outputs. To use up to 9 analog or alarm outputs maximum 3 PIFs can be connected. Each stackable industrial PIF must have its own RS485 address. The address must be set directly on the board. For the PIF which is the furthest away the 120R switch (TERM. –Termination) has to be set.



Figure 5-12 Connection of 3 PIFs



5.8.6 Example for a Fail-Safe monitoring



Fail-Safe monitoring states

- Breakdown of PIF power supply [1]
- [2] [3] Cable break of fail-safe cable
- Interruption of cable Xi-PIF
- [4] Malfunction of Xi
- Breakdown of Xi power supply/ Interruption of USB cable [5]
- Malfunction of PIX Connect software [6]



Fail-Safe monitoring states

- Breakdown of PIF power supply [1]
 - Cable break of fail-safe cable
 - [6] [7]

[5]

- [2] [3] Short circuit of fail-safe cable [4] Interruption of cable Xi-PIF

Malfunction of Xi

Breakdown of Xi power supply/ Interruption of USB cable Malfunction of PIX Connect software

Figure 5-13 Fail-Safe monitoring states



6 Network access and visualization

The most important procedures of initially starting the camera are described below. A detailed software description can be found on the supplied USB stick and in the Help menu in the PIX Connect software under $Help \rightarrow Documentation$. Alternatively, the software can also be downloaded from the Optris website at the following link: <u>https://www.optris.global/pix</u>

6.1 Minimum system requirements

- Windows 7, 8 or 10
- USB port
- Hard disk with min. 30 MByte free storage
- Minimum 128 MByte RAM

6.2 Set up installation / first use

All drivers are loaded automatically by the Windows operating system. No driver installation is necessary. The software starts automatically in the installed language.

- 1. Connect the supplied USB stick to your PC
- 2. Start the Setup.exe. Follow the instructions of the wizard until the installation is finished. After installation, you will find the software on your desktop (as a program icon) and in the start menu: Start \ Programs \ Optris GmbH \ PIX Connect
- 3. Select the desired language in the menu Tools \rightarrow Language

6.3 Allocating IP adress

The ExCam XI410 is designed for use in an Ethernet network and requires an IP address for access and control.

Software configurations based on OEM operating instructions (Optris)

Ethernet setup (point-to-point connection)

After you have connected the Ethernet cable to the camera and the PC, you first have to make the network settings on the PC.

The devices are delivered with the following factory settings:

- IP-address camera: 192.168.0.101
- IP-address PC: 192.168.0.100
- Port-number: 50101



To do this, go to **All Control Panel Items** and open the **Network and Sharing Center**. Go to **Ethernet**.

Control Panel Home	View your basic network infor	mation and set up connections
Change adapter settings	Nicht identifiziertes Netzwerk	Access type: No network access
Change advanced sharing settings	Public network	Connections: Ethernet
Media streaming options		
Local Area Connection St	tatus 🗾	Local Area Connection Properties
General		Networking
Connection		Connect using:
IPv4 Connectivity:	Internet	Intel(R) PRO/1000 MT Network Connection
IPv6 Connectivity:	No network access	Carferra
Media State:	Enabled	This connection uses the following items:
Duration:	00:05:48	
Speed:	1.0 Gbps	
Details		File and Printer Sharing for Microsoft Networks
		Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4)
Activity		
		Ink-Layer Topology Discovery Responder
Sent	: — Neceived	Install Uninstall Properties
Bytes: 9	96,057 29,998	Description
		Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication
Properties 😵 Dis	able Diagnose	across diverse interconnected networks.
	Close	OK Cancel

Now press Properties.

Now select **Internet Protocol Version 4 (TCP** / IPv4) in the properties window and then go to **Properties** again.

Internet Protocol Version 4 (TCP/IPv4	4) Properties
General	
You can get IP settings assigned aut this capability. Otherwise, you need for the appropriate IP settings.	omatically if your network supports to ask your network administrator
Obtain an IP address automatic	ally
— Use the following IP address: —	
IP address:	192.168.0.100 2.
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	/i/
Obtain DNS server address aut	omatically
O Use the following DNS server ac	ddresses:
Preferred DNS server:	
Alternate DNS server:	• • •
Validate settings upon exit	Advanced
	OK Cancel

In the register card **General**, activate the check box

"Use the following IP address". Now enter a user-defined IP address for

your PC (192.168.0.100). This must be identical to the address set in the PIX Connect software.

Then close the window with **OK**. The network settings on the PC are complete.



Start the PIX Connect software and activate the **Ethernet** function. To do this, go to **Devices** and **Enable Ethernet** in the menu.



Make sure that all three networks (Domain, Private, Public) are allowed in the Windows Firewall window to ensure a connection to the device

Windows Defender Firewall has blocked some features of USB IR Camera Software (NET 4.5, () on all public, private and domain networks. Image: Software (NET 4.5, v120) Image: Software (NET 4.5, v120) Path: C: Uprogram files (x86) (pptris gmbh/pix connect/imager.exe USB IR Camera Software (NET 4.5, v120) to communicate on these networks: Image: Domain networks, such as a workplace network Private networks, such as my home or work network Private networks, such as my home or work network Private networks, such as my home or work network Private networks, such as my home or work network Private networks, such as my home or work network Private networks, such as a workplace network Private networks, such as a workplace network Private networks, such as a my home or work network Private networks, such as my home or work network Private networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an appot through a firewall? Allow programs to communicate through Windows Firewall Tools Help Allowed programs and features: Plane the inks of allowing a program to communicate? Nume the tricks of nallowing a program to communicate? Planemet Voume Management	Windows Defender Firewall has blocked some features of USB IR Camera Software (.NET 4.5, t) on all public, private and domain networks. Image: Software (.NET 4.5, v120) Image: Software (.NET 4.5, v120) Private networks Image: Software (.NET 4.5, v120) Image: Software Networks, such as my home or work network Image: Software Networks, such as my home or work network Image: Software Networks, such as my home or work network Image: Software Networks, such as my home or work network Image: Software Networks, such as my home or work network Image: Software Networks, such as my home or work network Image: Software Networks </th <th>Windows Se</th> <th>- and for a set</th> <th></th> <th></th> <th></th> <th></th> <th>^</th>	Windows Se	- and for a set					^
bious Defender Firewall has blocked some features of USB IR Camera Software (.NET 4.5, c) on all public, private and domain networks. Name: USB IR Camera Software (.NET 4.5, v120) Publisher: Unknown Path: C:\program files (x86)\optris gmbh\pix connect\imager.exe vUSB IR Camera Software (.NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Private networks, such as my home or work network Private networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel + System and Security + Windows Firewall + Allowed Programs • 4 Search C Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Name the risks of allowing an app through a firewall? I codd, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Name To make through Protocol ShiMP Trap Wear USB R Camera Software (.NET 4.2, .90) Wear USB R Camera Software (.NET 4.5, .912) Wart USB Redirector WWart	<pre>boys Defender Firewall has blocked some features of USB IR Camera Software (.NET 4.5, b) on all public, private and domain networks.</pre>	Wind app	ows Defend	ler Firewall has blo	ocked som	e features o	f this	
a) on all public, private and domain networks. Name: USB IR Camera Software (.NET 4.5, v120) Publisher: Unknown Path: C:\program files (x86)\optris gmbh\pix connect\jmager.exe VUSB IR Camera Software (.NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Private networks, such as my home or work network Private networks, such as my home or work network Private networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel • System and Security • Windows Firewall • Allow access Cancel Control Panel • System and Security • Windows Firewall • Allowed Programs • 4y Search CC Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings What are the risks of allowing a program to communicate? Name Domain Home/Work (Private) Public Name Numeers Control Application Name Remote Re	a) on all public, private and domain networks. Name: USB IR Camera Software (.NET 4.5, v120) Publisher: Urknown Path: C:\program files (x86)\optris gmbh\pix connect\jmager.exe vUSB IR Camera Software (.NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Private networks, such as my home or work network Private networks, such as my home or work network Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel > System and Security > Windows Firewall > Allowed Programs	dows Defende	er Firewall has blo	ocked some features of US	SB IR Camera S	oftware (.NET 4	.5,	
Name: USB IR Camera Software (NET 4.5, v120) Publisher: Unknown Path: C:\program files (x86)\pptris gmbh\pix connect\imager.exe vUSB IR Camera Software (NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Private networks, such as my home or work network Private networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel > System and Security > Windows Firewall > Allowed Programs \$ \$ search C Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Image Control Panel > Secure Socket Tunneling Protocol Secure Socket Tunneling Protocol Image Remote Access Image Control Application Vest use Remote Control Application Image Remote Control Service Image Remote Control Service Visit USB Redirector Image Remote Control Service Image Remote Control Service Visit USB Redirector Image Remote Control Service Image Remote Control Service Visit USB Redirector Image Remote Control Service Image R	Name: USB IR Camera Software (NET 4.5, v120) Publisher: Unknown Path: C:\program files (x86)\optris gmbh\pix connect\jmager.exe vUSB IR Camera Software (NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Domain networks, such as my home or work network Private networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Cancel Control Panel + System and Security + Windows Firewall + Allowed Programs 49 Search C Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Image: Change settings Name Domain Home/Work (Private) Public Image: Change settings What are the risk of allowing a program to communicate? Image: Change settings Image: Change settings Weat USB Records Control Application Image: Change settings Image: Change settings Image: Change settings Veater to risks of allowing a program to control Application Image: Change settings Image: Change settings Image: Change settings Veater to Volume Management <td< td=""><td>0) on all public</td><td>, private and dor</td><td>main networks.</td><td></td><td></td><td></td><td></td></td<>	0) on all public	, private and dor	main networks.				
Publisher: Unknown Path: C: \program files (x86) \pptris gmbh\pix connect\jmager.exe UUSB IR Camera Software (.NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Private networks, such as a workplace network Public networks, such as my home or work network Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel + System and Security + Windows Firewall + Allowed Programs Control Panel + System and Security + Windows Firewall + Allowed Programs Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings Allowed programs and features: Name Memote Access Control Application Remote Volume Management Remote Remote Volume	Publisher: Unknown Path: C: \program files (x86) \pptris gmbh \pix connect\jmager.exe VUSB IR Camera Software (.NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Private networks, such as my home or work network Private networks, such as my home or work network Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security): tare the risks of allowing an app through a firewall? Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Program > Communicate? Moved programs and features:		Name:	USB IR Camera Softwa	are (.NET 4.5, 1	v120)		
Path: C:\program files (x86)\optris gmbh\pix connect\jmager.exe USB IR Camera Software (NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Private networks, such as my home or work network Private networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security): tare the risks of allowing an app through a firewall? Control Panel + System and Security + Windows Firewall + Allowed Programs Security Total and Security + Windows Firewall + Allowed Programs Security Total and Security + Windows Firewall + Allowed Programs Security Total and Factures: What are the risks of allowing a program to communicate: Moved programs to communicate through Windows Firewall Allowed programs and features: What are the risks of allowing a program to communicate: Name Domain MemetVock (Private) Public Notived programs and features: Sign Parme Software (INT 20, v00) Sign Parme Software (INT 20, v00) Wat USB Redirector Wat USB Redirector	Path: C: (program files (x86) (optris gmbh/pix connect/jmager.exe USB IR Camera Software (NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Private networks, such as my home or work network Private networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security): tare the risks of allowing an app through a firewall? Control Panel • System and Security • Windows Firewall • Allowed Programs Control Panel • System and Security • Windows Firewall • Allowed Programs Control Panel • System and Security • Windows Firewall • Allowed Programs Control Panel • System and Security • Windows Firewall • Allowed Programs Control Panel • System and Security • Windows Firewall • Allowed Programs Control Panel • System and Security • Windows Firewall • Allowed Programs Control Panel • System and Security • Windows Firewall • Allowed Programs Control Panel • System and Security • Windows Firewall • Allowed Programs Control Panel • System and Security • Windows Firewall • Allowed Programs Control Panel • System Control Security • Control Security		Publisher:	Unknown				
USB IR Camera Software (.NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Private networks, such as my home or work network Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel > System and Security > Windows Firewall > Allowed Programs < 49 Search Ci Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed program and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Remote Control Application Teamviewer Remote Control Application Teamviewer Remote Control Application Teamviewer Remote Control Service WWRT USB Redirector WWRT USB Redirector	USB IR Camera Software (NET 4.5, v120) to communicate on these networks: Domain networks, such as a workplace network Private networks, such as my home or work network Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel + System and Security + Windows Firewall + Allowed Programs • 4 Security Control Panel + System and Security + Windows Firewall + Allowed Programs Order Because these networks to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings What are the risks of allowing a program to communicate? Allowed programs and features: Name Volume Management Domain Home/Work (Private) Public Doubling and Remote Control Application Determineter Remote Control Service WW&T Netzwerkgeräte verwalten WW&T USB Redirector WW&T USB Re		Path:	C:\program files (x86)	\optris gmbh \pi	x connect\image	r.exe	
Domain networks, such as a workplace network Private networks, such as my home or work network Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Control Panel System and Security Windows Firewall Control Panel System and Security Windows Firewall Allowed Programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public ShiMP Trap UsB IR Camera Software (NET 20, 90) Wart Netzwerkgeräte verwalten Wart USB Redirector Network USB Redirector Network USB Redirector Details Remove	Domain networks, such as a workplace network Private networks, such as my home or work network Private networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel + System and Security + Windows Firewall + Allowed Programs • 4• Security Control Panel + System and Security + Windows Firewall + Allowed Programs • 4• Security Control Panel + System and Security + Windows Firewall + Allowed Programs • 4• Security Control Panel + System and Security + Windows Firewall + Allowed Programs • 4• Security Control Panel + System and Security + Windows Firewall + Allowed Programs Control Panel + System and Security + Windows Firewall + Allowed Programs Control Panel + System and Security + Windows Firewall + Allowed Programs Control Panel + System and Security + Windows Firewall + Allowed Programs Control Panel + System and Security + Windows Firewall + Allowed Programs Control Panel + System and Security + Windows Firewall + Allowed Programs Control Panel + System and Security + Windows Firewall + Allowed Programs Control Panel + System and Security + Vindows Firewall + Allowed Programs Control Panel + System and Security + Vindows Firewall Control Panel + System and Security + Vindows Firewall Control Panel + System and Security + Vindows Firewall Control Panel + System and Security + Vindows Control Panel + System and Security + Vindows Control Panel + System and Security + Vindows Control Panel + System Remote Control Application Control Panel + System Remote Control Service Cont	w USB IR Cam	era Software (.N	ET 4.5, v120) to commun	icate on these	networks:		
Private networks, such as my home or work network Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel • System and Security • Windows Firewall • Allowed Programs • 49 Search Cl Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Nummer Volume Management Remote Volume Management Remote Volume Management Remote Volume Management Water the risks of allowing rotocol Secure Socket Tunneling Protocol Stander Control Application Water Netwer Remote Control Application Water Netwerkgeräte verwalten Water USB Redirector Water USB Redirector Water USB Redirector	Private networks, such as my home or work network Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel + System and Security + Windows Firewall + Allowed Programs 	Domain net	tworks, such as a	workplace network				
Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel System and Security Windows Firewall Allow programs to communicate through Windows Firewall Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings What are the risks of allowing a program to communicate? Name Domain Home/Work (Private) Public Remote Volume Management Routing and Remote Access Succur Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application SNMP Trap Walk Tusks Redirector WikkT USB Redirector WikkT USB Redirector Nume Remove	Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel + System and Security + Windows Firewall + Allowed Programs • 4• Search C Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Name Domain Home/Work (Private) Public Remote Volume Management Remote Volume Management Remote Volume Management Remote Volume Management Remote Control Application Teamwiewer Remote Control Application We&T USB Redirector W&W To USB Redirector W&W To USB Redirector W&W To USB Redirector MW&T USB Redirector MW	Private net	works, such as m	ny home or work network				
Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an apo through a firewall? Centrol Panel System and Security Windows Firewall Allowed Programs Centrol Panel System and Security Windows Firewall Allowed Programs Centrol Panel System and Security Windows Firewall Allowed Programs Centrol Panel System and Security Windows Firewall Centrol Panel System and Security Windows Firewall Allowed Programs Centrol Panel System and Security Windows Firewall Centrol Panel System and Security Windows Firewall Centrol Panel System and Security Secure Centrol Panel System and Security Windows Firewall Centrol Panel System and Security Windows Secure Centrol Panel System and Security Secure Centrol Panel System and Secure Sec	Public networks, such as those in airports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel • System and Security • Windows Firewall • Allowed Programs • 49 Search © Control Panel • System and Security • Windows Firewall • Allowed Programs Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Sourd Software (NET 20, 900) Som Prap Software (NET 20, 900) We&T USB Redirector We&T USB Redirector Allow another program. Allow another program. Control Panel • System and Security • Public • Control Panel • Software (NET 20, 900) Control Panel • Control Service Control Panel • Control Panel • Control Panel • Control Panel • Control Panel • Control Panel • Control Panel • Control Pane	Finalene	anoins, sourias ii	ly nome of work network				
Public networks, such as those in arports and correct shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall > Allowed Programs Control Panel > System and Security > Windows Firewall To add, change, or remove allowed programs and ports, click Change settings Change setings Change settings Change settings Change setting	Dubic networks, such as those in arports and coffee shops (not recommended because these networks often have little or no security) tare the risks of allowing an app through a firewall? Control Panel > System and Security > Windows Firewall > Allowed Programs							
tare the risks of allowing an app through a firewall? Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Control Panel Control Panel Control Panel System and Security Control Panel Control Panel Control Panel System and Security Control Panel Control	tare the risks of allowing an app through a firewall? Image: Second	Public netw	orks, such as the	ose in airports and coffee	shops (not rec	ommended		
t are the risks of allowing an app through a firewall? Control Panel • System and Security • Windows Firewall • Allowed Programs Control Panel • System and Security • Windows Firewall • Allowed Programs	tare the risks of allowing an app through a firewall? Image: Second	because th	ese networks oft	ten have little or no securi	ity)			
tare the risks of allowing an app through a firewall? Control Panel > System and Security > Windows Firewall > Allowed Programs	tare the risks of allowing an app through a firewall?							
Cancel Control Panel * System and Security * Windows Firewall * Allowed Programs Cancel Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Rewords Volume Management Image and Remote Access Image and Remote Access Image and Remote Access Styler Teamviewer Remote Control Application Image and Remote Access Image and Remote Access Image and Remote Access Wat Tusts Redirector Wat TUSB Redirector Image and Remove Image and Remove	Control Panel System and Security Windows Firewall Allowed Programs Image: Security Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Momed programs and features: Mame Domain Home/Work (Private) Public Remote Volume Management Image: Domain Image: Domain Image: Domain Image: Domain Scure Socket Tunneling Protocol Image: Domain	at are the risk	s of allowing an a	on through a firewall?				
Control Panel * System and Security * Windows Firewall * Allowed Programs Cancel Control Panel * System and Security * Windows Firewall * Allowed Programs Search C Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Change settings: Allowed programs and features: Name Domain Home/Work (Private) Public (Private)	Name Domain Home/Work (Private) Public Control Panel * System and Security * Windows Firewall * Allowed Programs Image: Security Image: Security Tools Help Allow programs to communicate through Windows Firewall Control Panel * System and Security * Windows Firewall Control Panel * System and Security * Windows Firewall Allow programs to communicate through Windows Firewall Control Panel * Sign of allowing a program to communicate? What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Revoite Volume Management Image: Socket Tunneling Protocol Image: Socket Tunneling Protocol Image: Socket Tunneling Protocol SINMP Trap Image: Socket Tunneling Protocol Image: Socket Tunneling Protocol Image: Socket Tunneling Protocol Secure Socket Tunneling Protocol Image: Socket Tunneling Protocol <th></th> <th></th> <th>and a set of the set of the set of the</th> <th></th> <th></th> <th></th> <th></th>			and a set of the set of the set of the				
Allow access Cancel Control Panel * System and Security * Windows Firewall * Allowed Programs Search C Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Image settings Allowed programs and features: Image ment Remote Volume Management Image ment Routing and Remote Access Image ment Standard Remote Control Application Image ment Viss Remote Control Application Image ment W&T to turneing Protocol Image ment Viss Redirector Image ment W&T Netzwerkgeräte verwalten Image ment W&T USB Redirector Image ment Wat Tusts Redirector Image ment Image ment Image ment Image ment Image ment Image ment Image ment Image ment Image ment<	Control Panel • System and Security • Windows Firewall • Allowed Programs • • Search C Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Routing and Remote Access Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Service Wat Tusb Redirector Wat USB Redirector Wat USB Redirector Remove Allow another program.							
Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Search C Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Routing and Remote Access Secure Socket Tunneling Protocol SMMP Trap Teamviewer Remote Control Application Feamviewer Remote Control Service VUSB IR Camera Software (NET 2.0, v90) Swnoidewer, exe Wart Netzwerkgeräte verwalten Wart USB Redirector Wart SB Redirector Wart USB Redirector Details Remove	Control Panel							-
Control Panel > System and Security > Windows Firewall > Allowed Programs ✓ Search C Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Routing and Remote Access Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Service Yuncviewer, exe W&XT Netzwerkgeräte verwalten W&XT USB Redirector W&XT USB Redirector W&XT USB Redirector 	Control Panel System and Security Windows Firewall Allowed Programs Control Panel System and Security Windows Firewall Search C Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Routing and Remote Access Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Application Teamviewer Remote Control Service WuSt Netzwerkgeräte verwalten Wu&T USB Redirector Wu&T USB Redirector Allow another program				Allo	w access	Cancel	
Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Remote Volume Management Image: Control Application Routing and Remote Access Image: Control Application Secure Socket Tunneling Protocol Image: Control Application Teamviewer Remote Control Application Image: Control Service W&XT USB IR Camera Software (.NET 2.0, v90) Image: Control Service W&XT USB Redirector Image: Control Service Marcoiewer.exe Image: Control Service Marcoiewer.ex	Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Remote Volume Management Image: Change Settings Secure Socket Tunneling Protocol Image: Change Settings Starwiewer Remote Control Application Image: Change Settings W&R Toss Remote Software (NET 2.0, v90) Image: Change Settings W&W TUSB Redirector Image: Change Settings W&W TUSB Redirector Image: Change Settings Allow another program. Allow another program.				Allo	waccess	Cancel	
Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Remote Volume Management Image: Click Change Settings Routing and Remote Access Image: Click Change Settings Secure Socket Tunneling Protocol Image: Click Change Settings Image: Trap Image: Click Change Settings Image: Trap Image: Click Change Settings Image: Volume Management Image: Click Change Settings Image: Secure Socket Tunneling Protocol Image: Click Change Settings Image: Sinther Remote Control Application Image: Click Change Settings Image: Vulse IR Camera Software (.NET 2.0, v90) Image: Vulse Remote Control Service Image: Wat Tusts Redirector Image: Vulse Redirector Image: Wat Tusts Redirector Image: Vulse Redirector Image: Wat Tusts Redirector Image: Vulse Remove	Tools Help Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Image: Classical Colspan="2">Image: Classical Colspan="2">Classical Colspan="2">Classical Colspan="2">Classical Colspan="2">Classical Colspan="2">Classical Colspan="2">Classical Colspan="2">Classical Colspan="2">Classical Colspan= Classical Colspan="2">Classical Colspan="2">Classical Colspan="2">Classical Colspan="2">Classical Colspan= Classical Colspan="2">Classical Colspan= Classical Colspan="2">Classical Colspan= Classical Colspan="2">Classical Colspan="2">Classical Colspan="2">Classical Colspan= Classical Colspan="2">Classical Colspan="2" Classical	Control Papel	Surtem and Securit			w access	Cancel	nch Ce
Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and pots, click Change settings. What are the risks of allowing a program to communicate? Image: State and State a	Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate?	Control Panel 🕨	System and Securit	y ▶ Windows Firewall ▶ Allo	wed Programs	w access	Cancel	rch Co
Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Older Control Management Older Control Secure Socket Tunneling Protocol Older Control Application Older Teamviewer Remote Control Application Older Control Service Older Volume Remote Control Service Older Volume Remote Control Service Older Volumer Remote Older	Allow programs to communicate through Windows Firewall To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Routing and Remote Access Secure Socket Tunneling Protocol SNIMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Service VISB IR Camera Software (.NET 2.0, v90) W&T USB IR Camera Software (.NET 2.0, v90) W&T USB Redirector W&T USB Redirector W&T USB Redirector W&T USB Redirector M&T USB Redirector MT Teamviewer Remove	Control Panel Tools Help	System and Securit	:y ▶ Windows Firewall ▶ Allo	wed Programs	w access	Cancel	rch Co
To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Pomain Home/Work (Private) Public Remote Volume Management Routing and Remote Access Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Application Teamviewer Remote Control Service VUSB IR Camera Software (.NET 2.0, v90) VVV VV VVCviewer.exe VVncviewer.exe VVNCVIEWER.ex	To add, change, or remove allowed programs and ports, click Change settings. What are the risks of allowing a program to communicate? Allowed programs and features: Name Obmain Home/Work (Private) Public Remote Volume Management Routing and Remote Access Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Service USB IR Camera Software (.NET 2.0, v90) Wacriewer.exe W& T USB Redirector W& T USB Redirector W& T USB Redirector W& T USB Redirector M& T USB Redir	Control Panel → Tools Help	System and Securit	y ▶ Windows Firewall ▶ Allo	wed Programs	w access	Cancel	rch Co
What are the risks of allowing a program to communicate? Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Image: Domain Image: Domain Home/Work (Private) Public Remote Volume Management Image: Domain Home/Work (Private) Public Image: Domain Home/Work (Private) Public Remote Volume Management Image: Domain Home/Work (Private) Public Image: Domain Home/Work (Private) Public Routing and Remote Access Image: Domain Home/Work (Private) Public Image: Domain Home/Work (Private) Image: Domain Home/Work (Pr	What are the risks of allowing a program to communicate? Change settings Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Routing and Remote Access Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Service USB IR Camera Software (.NET 2.0, v90) Wat Netzwerkgeräte verwalten W&T USB Redirector W&T USB Redirector W&T USB Redirector Mathematical Remove Allow another program.	Control Panel ♪ Tools Help	System and Securit	y ► Windows Firewall ► Allo	wed Programs	ewall	Cancel	rch Co
Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Image: Domain Image: Domain Image: Domain Routing and Remote Access Image: Domain Image: Domain Image: Domain Secure Socket Tunneling Protocol Image: Domain Image: Domain Image: Domain Secure Socket Tunneling Protocol Image: Domain Image: Domain Image: Domain Teamviewer Remote Control Application Image: Domain Image: Domain Image: Domain W USB IR Camera Software (.NET 2.0, v90) Image: Domain Image: Domain Image: Domain W&T Netzwerkgeräte verwalten Image: Domain Image: Domain Image: Domain Image: Domain W&T USB Redirector Image: Domain Image: Domain Image: Domain Image: Domain Image: Domain M&T USB Redirector Image: Domain Image:	Allowed programs and features: Name Domain Home/Work (Private) Public Remote Volume Management Image: scale sc	Control Panel ► Tools Help T	System and Securit Allow programs	y Windows Firewall Allo to communicate through move allowed programs and po	wed Programs	ewall	Cancel	rch Co
Allowed programs and features: Name Domain Home/Work (Private) Public	Allowed programs and features: Name Domain Home/Work (Private) Public	Control Panel Tools Help	System and Securit Allow programs to add, change, or rer	y Windows Firewall Allo to communicate through move allowed programs and po	wed Programs	ewall ettings.	Cancel	rch Co
Name Domain Home/Work (Private) Public	Name Domain Home/Work (Private) Public	Control Panel → Tools Help T T	System and Securit Now programs o add, change, or rer Vhat are the risks of a	y Windows Firewall Allo to communicate through move allowed programs and po illowing a program to communi	wed Programs h Windows Fir nts, click Change se icate?	ewall	Cancel	rch Co
Image: Remote Volume Management Routing and Remote Access Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Image: Teamviewer Remote Control Service Image: Volume Remote Remote Control Service Image: Volume Remote Remote Control Service Image: Volume Remote Remote Remote Control Service Image: Volume Remote Re	Image: Construct of the second sec	Control Panel → Tools Help T V	System and Securit Allow programs to add, change, or rer Vhat are the risks of a Allowed programs a	y → Windows Firewall → Allo to communicate throug move allowed programs and po illowing a program to communi and features:	wed Programs h Windows Fir nts, click Change se icate?	ewall ettings.	Cancel	rch Co
Routing and Remote Access Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Service USB IR Camera Software (.NET 2.0, v90) Vocviewer.exe Vocviewer.exe W&T Netzwerkgeräte verwalten W&T USB Redirector W&T USB Redirector Details	Routing and Remote Access Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Service Y USB IR Camera Software (.NET 2.0, v90) Y we y Workiewer.exe Y uncviewer.exe W&T Netzwerkgeräte verwalten W&T USB Redirector W&T USB Redirector W&T USB Redirector Details Remove	Control Panel Tools Help T V	System and Securit Allow programs to add, change, or rer Vhat are the risks of a Allowed programs a Name	y Windows Firewall Allo to communicate through move allowed programs and po illowing a program to communi ind features:	eved Programs wed Programs h Windows Fir rts, click Change se icate? Domain	ewall ettings.	Cancel	rch Cc
Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Service USB IR Camera Software (.NET 2.0, v90) Vocviewer.exe Vocviewer.exe Vocviewer.exe W&T Netzwerkgeräte verwalten W&T USB Redirector W&T USB Redirector W&T USB Redirector	Secure Socket Tunneling Protocol SNMP Trap Teamviewer Remote Control Application Teamviewer Remote Control Service USB IR Camera Software (.NET 2.0, v90) WUSB IR Camera Software (.NET 2.0, v90) Workiewer.exe Workiewer.exe Workiewer.exe W&T Netzwerkgeräte verwalten W&T USB Redirector W&T USB Redirector W&T USB Redirector Details Remove	Control Panel Tools Help T V	System and Securit Allow programs to add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume	y Windows Firewall Allo to communicate through move allowed programs and po illowing a program to communi ind features: Management	wed Programs h Windows Fir nts, click Change se icate? Domain ☑	ewall ettings.	Cancel	rch Co
SNMP Trap Image: Control Application Teamviewer Remote Control Service Image: Control Service USB IR Camera Software (.NET 2.0, v90) Image: Control Service USB IR Camera Software (.NET 2.0, v90) Image: Control Service USB IR Camera Software (.NET 2.0, v90) Image: Control Service USB IR Camera Software (.NET 2.0, v90) Image: Control Service USB IR Camera Software (.NET 2.0, v90) Image: Control Service Use vacuum reservice Image: Control Service Vocuiewer.exe Image: Control Service Vocuiewer.exe Image: Control Service Vw&T Netzwerkgeräte verwalten Image: Control Service W&T USB Redirector Image: Control Service Image: Control Service Image: Contr	SNMP Trap Image: Control Application Teamviewer Remote Control Service Image: Control Service USB IR Camera Software (.NET 2.0, v90) Image: Control Service USB IR Camera Software (.NET 2.0, v90) Image: Control Service USB IR Camera Software (.NET 2.0, v90) Image: Control Service USB IR Camera Software (.NET 2.0, v90) Image: Control Service USB IR Camera Software (.NET 2.0, v90) Image: Control Service Use Voicewer.exe Image: Control Service Vincviewer.exe Image: Control Service Vw&T Netzwerkgeräte verwalten Image: Control Service Vw&T USB Redirector Image: Control Service Image: Control Service Image	Control Panel Tools Help 7 V	System and Securit Allow programs to add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Remote Volume	y → Windows Firewall → Allo to communicate througl move allowed programs and po illowing a program to communi and features: Management mote Access	♦ Allo wed Programs h Windows Fir nts, click Change se icate? Domain ♥	ewall ettings.	Cancel	rch Co
Teamviewer Remote Control Application Teamviewer Remote Control Service USB IR Camera Software (.NET 2.0, v90) Vocviewer.exe vncviewer.exe W&T Netzwerkgeräte verwalten W&T USB Redirector W&T USB Redirector W&T USB Redirector	Image: Control Application Image: Control Service Image: Control Service Image: Control Service Image: Contre <td>Control Panel → Tools Help 7 V</td> <td>System and Securit Allow programs of o add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Remote Volume Renuting and Rer Secure Socket T</td> <td>ty Windows Firewall Allo to communicate through move allowed programs and po illowing a program to communi and features: Management mote Access unneling Protocol</td> <td>wed Programs h Windows Fir orts, click Change se icate? □ □</td> <td>ewall ettings.</td> <td>Cancel</td> <td>rch Cc</td>	Control Panel → Tools Help 7 V	System and Securit Allow programs of o add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Remote Volume Renuting and Rer Secure Socket T	ty Windows Firewall Allo to communicate through move allowed programs and po illowing a program to communi and features: Management mote Access unneling Protocol	wed Programs h Windows Fir orts, click Change se icate? □ □	ewall ettings.	Cancel	rch Cc
Image: Second	Image: Control Service Image: Control Service Image: Control Servi	Control Panel → Tools Help 7 V	System and Securit Allow programs to add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Remote Volume Secure Socket T SNMP Trap	ty Windows Firewall Allo to communicate througl move allowed programs and po illowing a program to communi and features: Management mote Access unneling Protocol	Wed Programs H Windows Fir rts, click Change se icate? Domain I I I I I I I I I I I I I I I I I I	ewall ettings.	Cancel	rch Cc
U USB IR Camera Software (.NET 2.0, v90) U vncviewer.exe vncviewer.exe V w&T Netzwerkgeräte verwalten W&T USB Redirector W&T USB Redirector W&T USB Redirector Details Remove	Image: Second of Service Image: Second of Service Image: Second of Second of Service Image: Second of Second o	Control Panel → Tools Help 7 V	System and Securit Allow programs o add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Routing and Rer Secure Socket T SNMP Trap V Teamviewer Rer	ty → Windows Firewall → Allo to communicate througl move allowed programs and po illowing a program to communi and features: Management mote Access 'unneling Protocol mote Control Application	Wed Programs Windows Fir rts, click Change se icate? Domain	ewall ettings.	Cancel	rch Cc
W USB IR Camera Software (.NET 2.0, V90) W W W W voriewer.exe Image: Imag	Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90) Image: Software (.NE1 2.0, v90)	Control Panel → Tools Help / T	System and Securit Allow programs o add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Routing and Rer Secure Socket T SNMP Trap Teamviewer Rer	ty → Windows Firewall → Allo to communicate througl move allowed programs and po illowing a program to communi and features: Management mote Access 'unneling Protocol mote Control Application mote Control Application	Allo wed Programs h Windows Fir rts, click Change se icate? Domain	ewall ettings.	Cancel	rch Cc
Wexcriewer.exe Image: Constraint of the second	Image: Second	Control Panel Tools Help V	System and Securit Allow programs o add, change, or rer vhat are the risks of a Allowed programs a Name Remote Volume Routing and Rer Scure Socket T SNMP Trap Teamviewer Rer Framviewer	ty Windows Firewall Allo to communicate through move allowed programs and po illowing a program to communi and features: Management mote Access unneling Protocol mote Control Application mote Control Service	Allo wed Programs h Windows Fir rts, click Change se icate? Domain V C V V V	ewall ettings.	Cancel	rch Cc
Image: Second	✓ vncviewer.exe □ ✓ ✓ W&T Netzwerkgeräte verwalten □ ✓ ✓ W&T USB Redirector ✓ □ ✓ W&T USB Redirector □ ✓ ✓ W&T USB Redirector □ ✓ ✓ Betails Remove Allow another program	Control Panel Tools Help V	Allow programs o add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Routing and Rer Secure Socket T SNMP Trap Teamviewer Rer Teamviewer Rer USB IR Camera S	ty Windows Firewall Allo to communicate through move allowed programs and po illowing a program to communi and features: Management mote Access 'unneling Protocol mote Control Application mote Control Service Software (.NET 2.0, v90)	Allo wed Programs h Windows Fir rts, click Change se icate? Domain C C V	ewall ettings.	Cancel Change setting Public	IS
W&T Netzwerkgeräte verwalten Image: Constraint of the second	W&T Netzwerkgeräte verwalten Image: Constraint of the second	Control Panel Tools Help V	System and Securit Allow programs o add, change, or rer Vhat are the risks of a Allowed programs a Mame Remote Volume Remote Volume Renoting and Rer Secure Socket T SNMP Trap Teamviewer Rer Teamviewer Rer USB IR Camera S Support Secure Secu	ty → Windows Firewall → Allo to communicate througl move allowed programs and po illowing a program to communi and features: Management mote Access 'unneling Protocol mote Control Application mote Control Service Software (.NET 2.0, v90)		ewall ettings.	Cancel	rch Cc
W&T USB Redirector Image: Construction of the second sec	W&T USB Redirector Image: Constraint of the second sec	Control Panel Tools Help V	System and Securit Allow programs o add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Remote Volume Renuting and Rer Secure Socket T SNMP Trap Teamviewer Rer Canviewer Rer W USB IR Camera S Sociever exe Vncviewer.exe	ty → Windows Firewall → Allo to communicate througl move allowed programs and po illowing a program to communi and features: Management mote Access 'unneling Protocol mote Control Application mote Control Service Software (.NET 2.0, v90)	Allo Wed Programs h Windows Fir orts, click Change se icate? Domain V U V V V V V V V V V V V	ewall ettings.	Cancel	rch Cc
W&T USB Redirector W&T USB Redirector	W&T USB Redirector W Wat USB Redirector Details Remove Allow another program	Control Panel Tools Help V	System and Securit System and Securit Ilow programs o add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Routing and Rer Secure Socket T SNMP Trap Teamviewer Rer Teamviewer Rer D USB IR Camera S Noncviewer.exe W& Thetzwerker	ty → Windows Firewall → Allo to communicate througl move allowed programs and po illowing a program to communi and features: a Management mote Access 'unneling Protocol mote Control Application mote Control Service Software (.NET 2.0, v90) geräte verwalten	Allo wed Programs h Windows Fir rts, click Change se icate? Domain V V V V V V V C C C C C C	ewall ettings.	Cancel	rch Cc
Details Remove	Details Remove	Control Panel Tools Help V	System and Securit Allow programs o add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Routing and Rer Secure Socket T SNMP Trap Teamviewer Rer Constructioner Secure Construction of the secure Secure Construction of the secure Secure Construction of the secure Se	ty Windows Firewall Allo to communicate through move allowed programs and po illowing a program to communi and features: Management mote Access 'unneling Protocol mote Control Application mote Control Service Software (.NET 2.0, v90) geräte verwalten ector	Allo wed Programs h Windows Fir rts, click Change se icate? Domain V V V V V V V V V V V V V	ewall ettings.	Cancel	rch Cc
Details Remove	Details Remove Allow another program	Control Panel Tools Help V	System and Securit Allow programs o add, change, or rer vhat are the risks of a Allowed programs a Name Remote Volume Routing and Rer Secure Socket T SNMP Trap Teamviewer Rer Greativiewer Rev	ty Windows Firewall Allo to communicate through move allowed programs and po illowing a program to communi and features: Management mote Access 'unneling Protocol mote Control Application mote Control Service Software (.NET 2.0, v90) geräte verwalten ector octor	Allo wed Programs h Windows Fir rts, click Change se icate?	ewall ettings.	Cancel	rch Cc
Allow as the stresses	Allow another program	Control Panel Tools Help V	System and Securit Allow programs of o add, change, or rer Vhat are the risks of a Allowed programs a Name Remote Volume Routing and Rer Secure Socket T SNMP Trap Teamviewer Rer Teamviewer Rer Teamviewer Rer USB IR Camera S NMP Trap Teamviewer Rer Was Netzwerke Was Netzwerke Was Netzwerke Was USB Redin Was USB Redin	ty Windows Firewall Allo to communicate through move allowed programs and po illowing a program to communi and features: Management mote Access 'unneling Protocol mote Control Application mote Control Service Software (.NET 2.0, v90) geräte verwalten ector ector ector	Allo wed Programs h Windows Fir nts, click Change se icate? Domain V V V V V V V V V V V V V	ewall ettings.	Cancel	rch Cc
Allow another brodram	Anow another program	Control Panel Tools Help V	System and Securit Allow programs i o add, change, or rer Vhat are the risks of a Allowed programs a Mame Mame Remote Volume Rer Secure Socket T SNMP Trap Teamviewer Rer Teamviewer Rer Teamviewer Rer Streamviewer Rer Streamviewer Rer WISB IR Camera S Swocyjewer, exe Wast Netzwerke W&T Netzwerke W&T USB Redin	ty → Windows Firewall → Allo to communicate througl move allowed programs and po illowing a program to communi and features: → Management mote Access `unneling Protocol mote Control Application mote Control Service Software (.NET 2.0, v90) geräte verwalten ector ector	Allo Wed Programs h Windows Fir orts, click Change se icate? Domain V V V V V V V V V V V V V	ewall ettings.	Cancel	rch Cc



With the option "**port no. assign automatically**" a port number is assigned automatically.

If several cameras with different port numbers are connected and communication is to take place with a specific camera, the corresponding camera can be determined by reacting to port number.

The authorizations of programs can also be activated retrospectively in the Windows firewall settings of the PC (Windows firewall and allow a program or feature through Windows Firewall).

The port range used should be between **49152** ... **65535**. When using other ports, it is possible that these are already reserved or assigned.

When using several XI80 cameras in one network, pay attention to the data rate:

- Switch with 100Mbits/s: approx. 17 devices (XI80)
- Switch with 1000Mbits/s: approx. 170 devices (XI80)

In addition to the data rate, you should also pay attention to the PC performance. A separate instance is required for each device used.

The device is now ready for the Ethernet connection and is listed in the menu **Devices**. The camera is identified by a network symbol and the network address and port number. Select the device. A connection to the device is established and the temperature measurement can begin.

To change the corresponding address settings, go to **Devices** and Ethernet Settings **(TCP/IP) Settings** in the menu.

The address for the device is assigned under **Device address**. This must have a different address (last block) to the other participant (e.g. PC) (**Send to address** (local computer)). It is important that the network part (first three blocks) must be identical for both addresses. The address range of the individual blocks can be between 0 and 255.

In addition, a separate port number must be configured. The selected number can be between 1 and 65535.





If you cannot assign the IP address, it may be necessary to check the firewall settings!



7 Visualization/ Analysis Software PIX Connect

7.1 General information about PIX Connect

The configuration menu of the web surface allows an intuitive navigation and offers several configuration possibilities. For detailed documentation and information how to use the web interface, please see the Optris PIX Connect Operator's Manual or visit the following website:

https://www.optris.com/xi-410



The radiometric processing of the image data enables subsequent detailed image analysis with the convenient PIX Connect software.

7.2 Focusing the thermal image

To make sure that the focus of thermal channel is adjusted correctly the motorized focus can be adjusted in the PIX Connect software (Menu \rightarrow View/ Windows/ Distance or over the icon $\stackrel{\longrightarrow}{\longrightarrow}$). Adjustment to the left = near, adjustment to the right = infinite.

Distance		E
0	44,2	œ

Figure 7-1 Motorized focus settings in PIX Connect Software

7.3 Adjustment of temperature range

Set the temperature range that suits you in the field at the bottom left.

27,0	-20°C 100°C
26,0	0°C 250°C
24,0	150°C 900°C
PI400/450 #17030008 29° -20°C 100°C	200°C 1500°C

Figure 7-2 Adjust temperature range



7.4 User interface



There are many possibilities within the user interface.

Figure 7-3 User interface

- 1. IR-Live view from the camera
- 2. Temperature profile: Temperature distribution on a maximum of two lines, which can be positioned anywhere in the image in terms of size and position.
- 3. Digital display group: Possible display of all temperatures from e.g. defined measuring fields, cold spots, hot spots, temperature at the mouse pointer, the internal temperature and the chip temperature. Alarm Settings: Bar with graphical representation of a defined lower temperature threshold (blue arrow) and an upper threshold (red arrow). The color of the digits of the displayed temperature changes to RED when the upper alarm value is exceeded and to BLUE when it falls below.
- 4. Temperature of measure area: Analyses the temperature according to the selected shape of the field, e.g. the mean value of the rectangle. This value is also shown in the live image (top right) and in the digital display.
- 5. Reference bar: Shows a color scale with the corresponding temperature values.
- 6. Temperature-time diagram: Shows the temperature curve over time for the selected ROI (region of interest).
- 7. Histogram: Statistical distribution of individual temperature values in the image.
- 8. Automatic / manual scaling of the reference bar and thus the displayed temperature range: Man., </> (min, max), 1 σ : 1 sigma, 3 σ : 3 sigma, OPT: Optimized palette
- 9. Distance Function: Adjusting the motor focus to focus the image
- 10. Menu and toolbar (icons)
- 11. Symbol for switching the individual palette views in the reference bar.
- 12. Status bar: Serial number, optics, temperature range, mouse cursor position, device frame rate/display frame rate, emissivity, ambient temperature, flag status



There are also many helpful video tutorials for the PIX-Connect software from Optris

https://www.youtube.com/results?search_query=optris+pix+connect+software

Configure your device according to your individual requirements.

8 Cleaning

Dirt on the viewing window must be removed as it can falsify the result of the temperature measurement. For regular cleaning, never use cleaning agents containing solvents (neither for the optics nor for the housing). Loose particles can be blown away with clean compressed air (Attention in dust-explosive environments). The sight glass can be cleaned with a soft, damp microfibre cloth (moistened with water) or a lens cleaner (e.g. Purosol or B+W Lens Cleaner).

9 Maintenance / Modification

The applicable regulations for the maintenance and servicing of electrical devices in potentially explosive atmospheres must be adhered to.

The required maintenance intervals are specific to the individual devices. The operating company has to determine these intervals depending on the application parameters. The maintenance tasks especially include examination of parts on which the ignition protection depends (e.g., proper condition of the casing, seals and cable entry points). If maintenance measures are necessary they have to be initiated and/or executed.

Repairs may only be carried out with original parts of SAMCON Prozessleittechnik GmbH. Damaged pressure-resistant housings have to be replaced completely. In case of doubt, send the part in question back to SAMCON Prozessleittechnik GmbH.

Reparations concerning the explosion protection must only be carried out in accordance with nationally applied regulations by SAMCON Prozessleittechnik GmbH or by an authorised electrical technician authorised by SAMCON Prozessleittechnik GmbH. Rebuilding of or alterations to the devices are not permitted.

10 Disposal / Recycling

When disposing of the device, nationally applicable regulations must be observed. This Document is subject to alterations and additions.



11 Drawings & 3D models

All drawings, 3D models, certificates and other information are available in the download area of the product page on our website:

https://www.samcon.eu/en/products/network/excam-xi410/

Analog Ex Cameras (CVBS)		
Network Ex Cameras (TCP/IP)		
ExCam IPP1275	$E_{\rm V}C_{\rm O}m^{\rm B}$ VI/10	
ExCam IPM3016		
ExCam IPM114v		
	World`s smallest explosion proof spot-finder thermographic camera	
SuGam ID01645	Thermal imaging camera with auto-focus and infrared thermometer	
Excam IPQ1645	The ExCam XI410 is a powerful thermographic camera with an integrated infrared thermometer and motor	
ExCam IPQ1615 (DLPU)	focus for use in potentially explosive areas. It delivers excellent infrared images (384x240p) of measurement	
ExCam IPQ1785	objects in a temperature range from -20°C to 900°C. In addition, the thermal imaging camera has a software with extensive analysis functions (e.g. thermal analysis with bot and cold spots). The Evcam XI410 can not on	
ExCam IPP5655	see where it is hot, it can also measure the temperature exactly. Like all cameras in the ExCam series, it is	
ExCam IPQ6075	certified according to European regulations (ATEX) as well as international ones (IECEx). These certificates an	
ExCam IPQ6075-MKII	further documents can be found in the download area.	
ExCam IPP1280 (thermal)	Features.	
ExCam XI80 (thermal)	Ocrtification for Hazardous Areas (ATEX & IECEX)	
ExCam XI410 (thermal)	Ultra-Compact and Leightweight Thermal Imaging Camera with integrated IR-Thermometer	
Modular Ex Cameras	Thermal Technology with 384x240p Resolution	
Robust Cameras (non-ex)	Exact Temperature Measurement from -20°C to 900°C	
(our Individual Camera (BTO)	♦ Thermal Sensitivity NETD 0.08°C	
Four Individual Camera (DTO)	Imager with Motor-Focus	
Ex-u camera Ericiosures	Four Optics available	
Lonnection Systems	Autonomous Operation with Automatic Spot Finder	
Cables for Ex-Areas	Automatic Calibration	
Mounting Systems	 Single-Cable-Solution (Ethernet, Power, I/O) 	
Wash and Wipe Equipment	Protection Level of IP66/68 (IEC 60529)	
Software	Software with extensive Analysis-Functions	
ownloads:	Extensive Accessories	
Comparison Chart		
Datasheet		
Jsermanual 20 Madel	Rugged measuring thermal camera with ATEX and IECEx-certification	
Drawings	Besides the European regulations (ATEX), the ExCam series is also certified according to international	
x Installation Manual	regulations (IECEX). The housings' certification comprises ALEX group II (Gas and Dust) for zone 1, 2 as well at and 22 including the explosion groups IIC / IIIC with a high risk of mechanical threat. In addition, certification	
ATEX Type Examination	be extended at any time to cover different markets.	
U Dec. of Conformity	During the ExCam XI410's development stage the focus was clearly laid on security aspects as well as	
Basic Principles Temp.	mechanical precision and high-quality stainless steels.	

If you wish additional technical information, please contact us at: support@samcon.eu



Schillerstrasse 17, 35102 Lohra-Altenvers, Germany www.samcon.eu, info@samcon.eu Phone: +49 6426 9231-0, fax: - 31

