



Product Handbook

security master

security master 001-0100

security master small size 001-0101

security master small size RS232 001-0102

security master Software Revision 1.5.3 LHX20 IpCam from 25.5.2008



M. S. Projekt Management und Vertrieb GmbH

Feldwicker Weg 59
46487 Wesel

support@pmv-gmbh.de
www.pmv-gmbh.de

Sales:



Elektro-Bauelemente May KG
Trabener Straße 65
14193 Berlin

Tel.: 030/7001154-0
Fax: 030/8919902

info@may-kg.com
www.may-kg.com

Important Information:

The RS232 port is only to be used to connect the LHX20 heat exchanger

No SMS messages can be sent
Despatch via GSM/GPRS modem is in preparation

Under no circumstances should cross patch cables be used to connect the sensors!

We reserve the right to make technical changes without notice

1 Table of contents

1	Table of contents	4
2	Introduction	8
2.1	Device properties	8
2.1.1	security master	8
2.1.1.1	Scope of delivery	8
2.1.2	security master small size.....	9
2.1.2.1	scope of delivery	9
2.2	Uses of the device	9
2.3	For your safety.....	10
2.4	Maintenance and cleaning	11
2.5	Environmental protection	11
2.6	Warranty	11
3	Startup procedure <i>security master</i>	12
3.1	Planning	12
3.1.1	List of sensor units.....	13
3.2	Connecting and switching on <i>security master</i>.....	15
3.2.1	Log in	17
3.2.2	Right mouse button.....	18
3.2.2.1	Inputs	18
3.2.2.1.1	Renaming.....	19
3.2.2.2	Outputs	20
3.2.2.3	Rules	20
3.2.2.3.1	Greater than.....	21
3.2.2.3.2	Equals.....	22
3.2.2.3.3	Table contains.....	23
3.2.2.3.4	Log Object.....	24
3.2.2.3.5	Delay.....	25
3.2.2.3.6	And.....	26
3.2.2.3.7	Or	26
3.2.2.3.8	Less than	27
3.2.2.3.9	Flip Flop	28
3.2.2.3.10	OnOff	28
3.2.2.4	Tables	29
3.2.2.5	Frames	30
3.2.2.6	Alarms.....	30
3.2.2.7	Add Folder	31
3.2.2.8	List view	32
3.2.2.9	Graphic view	32
3.2.3	Sensor warning and alarm displays.....	32
4	Setup security master	34
4.1	Configuration	34
4.1.1	Edit configuration	35
4.2	Users.....	37
4.2.1	Edit users.....	37

4.3	Alarms	38
4.3.1	Edit alarms.....	39
4.3.2	Save pictures	40
4.3.2.1	Without "network board"	40
4.3.2.2	With "network board".....	40
4.4	SNMP allocation	41
4.5	Clock.....	43
4.6	Internal Sensors	44
5	security master functions	45
5.1	SNMP Protocol.....	45
5.1.1	Entries in the system configuration.....	45
5.1.2	Entries in the alarm configuration	45
5.1.3	Send SNMP Traps.....	45
5.1.4	MIB Browser	47
5.1.4.1.1	Call-up values	47
5.1.5	Read data using SNMP GET	49
5.1.5.1	Load MIB.....	49
5.1.5.2	Read data	50
5.1.6	Switch digital outputs using SNMP "set"	51
5.1.6.1	Open lock.....	52
5.1.6.2	Switch digital output.....	53
5.2	Send e-mail	55
5.2.1	Entries in the system configuration.....	55
5.2.2	Entries in the alarm configuration	55
5.3	Log files.....	56
6	Setup data cupboard	57
6.1	Add sensors.....	58
6.2	Parameterise analogue input	59
6.2.1	Hysteresis	61
6.3	Parameterise digital input.....	62
6.4	Parameterise digital output	62
6.4.1	Test digital output	63
6.5	Shortcuts	64
6.5.1	Create output shortcut	64
6.5.2	Delete shortcut.....	65
6.6	IP camera.....	66
7	Peripherals	67
7.1	Analogue input module 0...10VDC [002-0109].....	67
7.2	Movement detector [002-0117]	67
7.3	Movement detector 360° [002-0192].....	67
7.4	Digital output module 4 way [002-0107]	68
7.5	Digital output module 8 way [002-0260]	68
7.6	Digital input module 4 way [002-0108].....	68
7.7	Digital input module 8 way [002-0250].....	69

7.8	Pressure sensor 0...10 bar [002-0195]	69
7.9	Shock sensor [002-0116]	69
7.10	Glass breakage sensor [002-0118]	70
7.11	IP camera [002-0140]	70
7.12	Combined sensor [002-0103]	70
7.13	Door contact for combined sensor [002-0119]	71
7.14	Combined distributor [002-0127]	71
7.15	Leakage sensor [002-0180]	71
7.16	Fan with control system [002-0150]	72
7.17	Fan with revolution logging [002-0151]	72
7.18	High-performance fan [002-0152]	73
7.18.1	Fitting the fan module	73
7.19	Supply voltage measuring adapter [002-0104]	73
7.20	Supply voltage measuring adapter 3 Phase [002-0124]	74
7.21	Supply current monitor [002-0173]	74
7.22	Peripheral bus distributor 8+2 [002-0111]	74
7.23	Smoke detector [002-0105]	75
7.24	Relay adapter AC [002-0106]	75
7.25	Oxygen sensor [002-0129]	75
7.26	Switch box 16A [002-0170]	76
7.27	Switch box 32A [002-0171]	76
7.28	Swing-arm Locking system	77
7.28.1	Locking system with keypad [002-0132, 002-01132].....	77
7.28.2	Locking system with transponder reader [002-0133, 002-01133].....	77
7.28.3	Locking system without ID module [002-0134, 002-01134].....	77
7.28.4	Keypad module [002-0130].....	78
7.28.5	Transponder reader module [002-0131]	78
7.28.6	Transponder cards [002-0858]	78
7.28.7	General	78
7.28.8	Security	78
7.29	Application	79
7.29.1	Configuration of locking system with swing-arm handle	79
7.30	Locking system with magnetic locking	80
7.31	Door locking system with magnetic clamps	80
7.31.1	Example	80
7.31.1.1	Locking system with magnetic clamp and transponder reader	81
7.32	Door locking system with magnetic clamps and automatic opening	81
7.32.1	Configuration magnetic locking system	82
7.32.2	Universal Application	83
7.33	Temperature sensor [002-0100]	84
7.34	Temperature sensor [002-0101]	84
7.35	Temperature sensor [002-0200]	84

7.36	Temperature and humidity sensor [002-0123]	85
7.37	Temperature and humidity sensor [002-0203]	85
7.37.1	Consumption monitor 16A uncalibrated [002-0181]	85
7.38	Consumption monitor 16A calibrated [002-0182]	86
7.39	Consumption monitor 32A uncalibrated [002-0183].....	86
7.40	Consumption monitor 32A calibrated [002-0184]	86
7.41	Access sensor (door contact) [002-0112].....	87
8	Special monitoring applications	88
8.1	Cooling device LHX20	88
8.1.1	Digital Interface	89
8.1.2	Signal Interfaces	89
8.1.3	Connection to the <i>security master</i>	90
8.1.4	Configuration	90
8.1.5	Log Files	91
8.1.6	RS232 Interface	92
8.1.6.1	Interface Parameters	92
8.1.6.2	Data cable	92
8.1.7	RS232 Communication	93
8.1.8	Inputs	93
8.1.8.1	Actual value display	94
8.1.8.2	Display range – limit values	94
8.1.8.3	Status display	95
8.1.8.3.1	Status 0	95
8.1.8.3.2	Status 1	95
8.1.8.4	Depiction of <i>security master</i>	96
8.1.8.5	Configuration	98
8.1.8.5.1	Alarm Alert	99
9	Service Programme	100
9.1	Sguard backup program installation	100
9.2	Device configuration backup.....	101
9.3	Restore device configuration	102
9.4	Change service (root) Password.....	103
9.5	Program updates	105

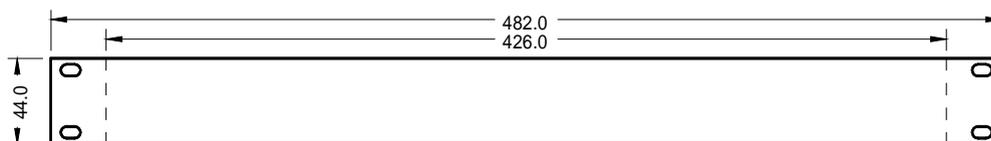
2 Introduction

2.1 Device properties

Operating temperature range	15...40°C
Maximum length of cable to the periphery	300 m
Maximum no. of peripherals per security master	100 pcs. (max. 20 per part-bus)
Maximum no. of peripherals per security master small size	40 pcs. (max. 20 per part-bus)

2.1.1 security master

Power supply connection	100...240 V AC (-10%, +6%)
Supply current	max. 1 Ampere
1 pc.	Ethernet port (10/100 MBit/sec)
5 pcs.	Interface ports for periphery
1 pc.	RS232 interface



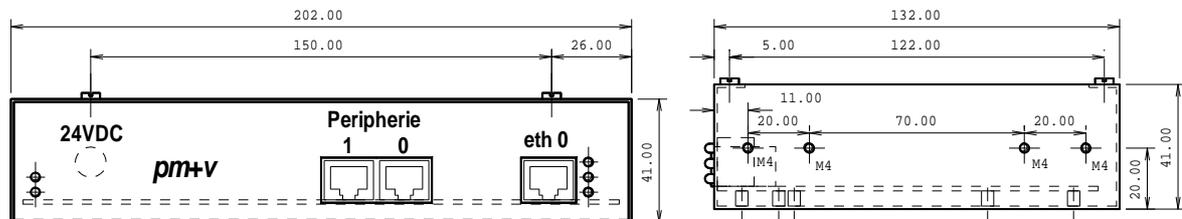
2.1.1.1 Scope of delivery

amount	description	Part No.	Notes
1 Pc.	security master	001-0100	
1 Pc.	Documentation CD		

Due to national variations no mains power cable is included with this device

2.1.2 security master small size

Power supply connection	100...240 VAC (-10%, +6%) (externes Netzteil)
Supply current	max. 1 Ampere
1 Pc.	Ethernet port (10/100 MBit/sec)
2 Pcs.	Interface ports for periphery
1 Pc.	RS232 interface



2.1.2.1 scope of delivery

amount	description	Part No.	Notes
1 Pc.	security master small size	001-0101	
1 Pc.	Mains adapter 115-230VAC/24VDC incl. power cable		
1 Pc.	19" fastening kit		
1 Pc.	Documentation CD		

2.2 Uses of the device

The **security master** is used for the monitoring of various operational parameters, such as

Movement – pressure – shock – humidity – cooling device LHX20 – customer-specific parameters
 – fan function – power supply voltage – power supply current – smoke – oxygen contents – power
 consumption – temperature – UPS – access (door contacts) – rights of access

Control of

Alarm sirens and lamps – fan function – power supply – door locking

Storage of

Alarm reports – pictures – measuring data - recording

2.3 For your safety

Ensure that the **security master** is only operated using a protective earth conductor, if not
 -an earth fault may result (indirect touching protection),
 -in the case of faults, dangerous voltages may occur.

The device is separated from the mains power supply by pulling out the plug. The socket must be close to the installation and easily accessible.

Never place objects in the openings due to risk of electrical shock.

The device may only be operated by authorised personnel.

It may not be operated anywhere in the proximity of flammable gases or vapours. The operation of electrical equipment in such an environment represents a serious safety risk. The device must not be installed, tested or operated near water. Water sprays and other liquids must not be allowed to touch the device. The device must be protected from moisture and must not be operated in a moist damp environment. Due to the inbuilt battery the device must be treated with care – avoid jerky movements and other shocks, or else a short circuit may lead to fire.

The battery in the **security master** may only be changed by qualified personnel. The **security master** contains an inbuilt (non-) replaceable lithium battery in the main board and a power cut bridging battery.

The **security master** small size contains an inbuilt (non-) replaceable lithium battery in the main board.

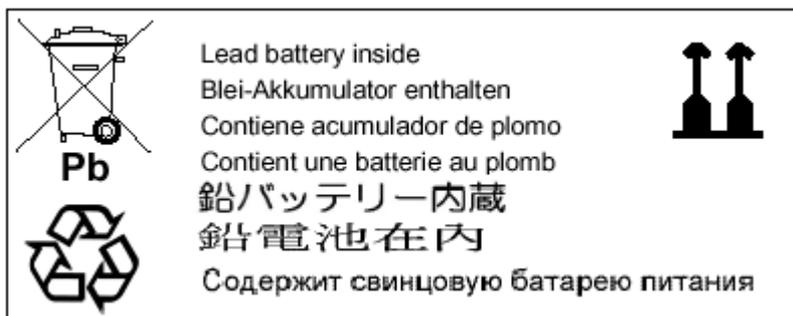
Beware:

Risk of explosion may ensue if the power cut bridging battery is improperly exchanged.

Replace using only the same type or one recommended by the manufacturer.

Dispose of old batteries according to the directions given by the manufacturer (in accordance with national regulations)

Do not open or damage batteries. Battery acid is corrosive and poisonous and harmful to the skin.



Ensure that the device is adequately cooled. Exposure to excessive ambient temperatures (>30°C) can lead to malfunctioning of the computer and a significant reduction in built-in battery and component life.

Safe operation of the *security master* and *security master small size* is only possible in conjunction with the thorough reading and observance of the user handbook and safety instructions!

Warning high voltage

Do not open the device - keep it away from children.

The device is only to be used in closed rooms for the monitoring of data cupboards.

Use only original **pm+v accessories and spare parts**.

2.4 Maintenance and cleaning

The device is maintenance-free.

Always keep the device, its connector and accessories dry and clean.

Should the device fail in spite of the most rigorous manufacturing and testing procedures, send it back in suitable packaging (keep the original packaging) to the manufacturer (**pm+v**).

2.5 Environmental protection

The device, its accessories and packaging must be disposed of in an environmentally-friendly way. Defective chargeable batteries must be recycled pursuant to Directive 91/157/EEC. Do not dispose of used batteries in household waste, fire, or water.

Do not use force to open batteries.

2.6 Warranty

We provide a warranty on **pm+v** devices in accordance with legal/country-specific terms and conditions. Damages which occur as a result of normal wear and tear, capacity overload or improper use are excluded from the terms of the warranty.

Claims can only be honoured if the device is returned to the manufacturer unopened and in suitable packaging.

3 Startup procedure *security master*

Remove the device from its transport packaging and check that the shipment is complete and undamaged.

Install the device in your data cupboard. Ensure adequate ventilation and take note of the operating temperature range of the device.

Due to national variations in equipment plug standards, no mains power cable is included as standard with the ***security master***.

The ***security master*** small size comes equipped with a power supply cable.

3.1 Planning

The distance between the two sensors with the greatest distance between them may be up to 300m.

Each of the 5 data ports is designed for the connection of 20 standard sensors. This would mean, for example, 20 temperature sensors or 20 door contacts etc.

If combined sensors are used, the quantity of the *individual* sensors is of course still counted, because combined sensors use more power and have a higher data volume.

For this reason, each sensor has a fixed number of “sensor units”. The sum of sensor units for all sensors connected to a data port may not exceed 20.

3.1.1 List of sensor units

Description	Part No.	Sensor units
Analogue input module 0...10V	002-0109	1
Movement detector (wall)	002-0117	1
Movement detector (360°)	002-0192	1
Digital output module 4 way	002-0107	4
Digital output module 8 way	002-0260	8
Digital input module 4 way	002-0108	4
Digital input module 8 way	002-0250	8
Pressure sensor 10 bar	002-0195	3
Flow-through meter 2-250 L/min	002-0194	1
Shock sensor	002-0116	1
Glass breakage sensor	002-0118	1
Combined sensor	002-0103	8
Combined distributor without temperature / humidity	002-0127	4
Combined distributor with temperature / humidity	002-0127 002-0128	6
Leakage sensor	002-0180	1
LHX20 Interface	002-0255	8
Mains supply voltage measuring adapter 1 Phase	002-0104	1
Mains supply voltage measuring adapter 3 Phase	002-0124	3
Mains supply current monitor	002-0173	4
Power box for Blade server	002-0186	9
Power monitor 3 Phase	002-0176	6
Power monitor 3 Phase 32 A	002-0188	9
Power monitor 4 Phase	002-0185	8
Smoke detector	002-0105	1
Smoke detector with VDS authorisation	002-0190	1
Relay adapter AC	002-0106	1

description	Part No.	Sensor units
Switch box 16A	002-0170	9
Switch box 32A	002-0171	9
Switch box 32A with timer function	002-0172	9
Oxygen sensor	002-0129	1
Dust sensor	002-0125	1
Keypad	002-0130	1
Temperature Sensor	002-0100	1
Temperature Sensor	002-0101	1
Temperature Sensor	002-0200	1
Temperature Sensor	002-0201	1
Temperature Sensor	002-0202	1
Temperature-humidity Sensor	002-0123	2
Temperature-humidity Sensor	002-0203	2
Transponder	002-0131	2
Door handle with keypad	002-0132	3
Door handle with keypad (Varistar)	002-1132	3
Door handle with transponder	002-0133	4
Door handle with transponder (Varistar)	002-1133	4
Door handle without ID module	002-0134	3
Door handle without ID module (Varistar)	002-1134	3
Consumption monitor	002-0181	5
Consumption monitor	002-0182	5
Consumption monitor	002-0183	5
Consumption monitor	002-0184	5
Access sensor	002-0112	1

3.2 Connecting and switching on security master



Connect the **security master** with the socket using a suitable power cable. The power socket is to be found on the back of the device.

Connect the Ethernet interface of the **security master** with your PC or laptop using a cross patch cable. If you are connecting the **security master** directly to a network, then, of course, use a normal patch cable.

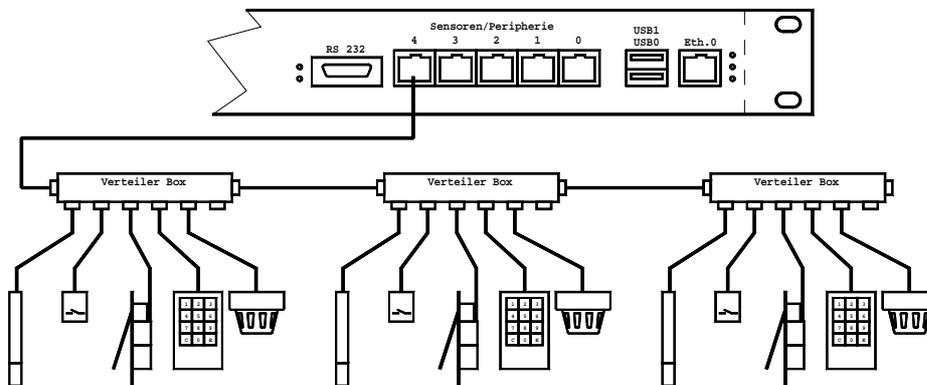
The security master is pre-set as follows:

IP-Address	192.168.0.33
Net mask	255.255.255.0
User name	peter
Password	peter

Please note that your PC or laptop must be configured for the pre-set IP range. If you are unsure consult your system administrator.

You should now attach the peripherals.

The ports are overload protected. In case of an overload the power supply to the sensors is automatically shut off.



Attachment of peripherals to the **security master**.

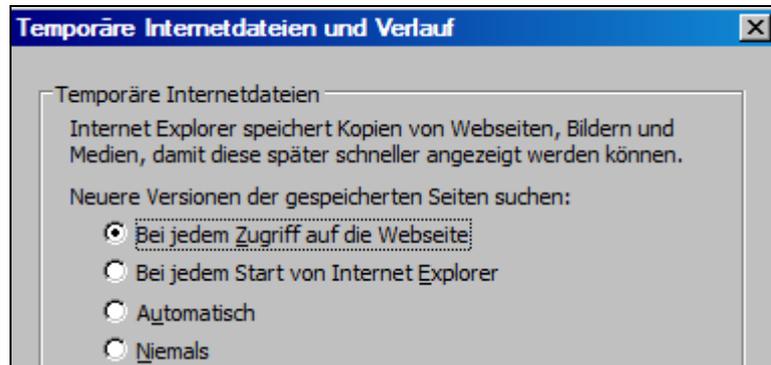
Take extreme care to ensure that the cables are not kinked, stretched or constricted.

This can lead to malfunctions in the whole bus system!

Important

Switch the **security master** on using the power switch. The red status LED will blink as long as the **security master** is not operational. As soon as it stays lit, the device is working and the sensors are being continuously interrogated.

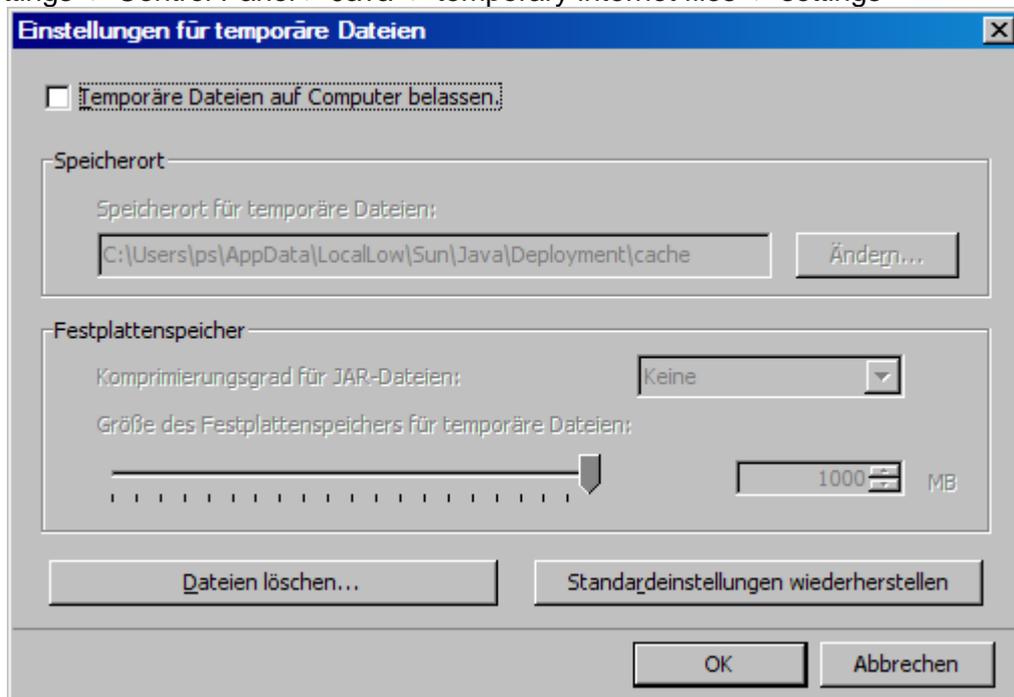
The **security master** is operated using a web browser. The web browser must support “JAVA” and Java must be activated. The connection must be direct without the use of proxy servers.



Please ensure that the browser is configured as shown.

In addition, the temporary data setting for Java must be set up.

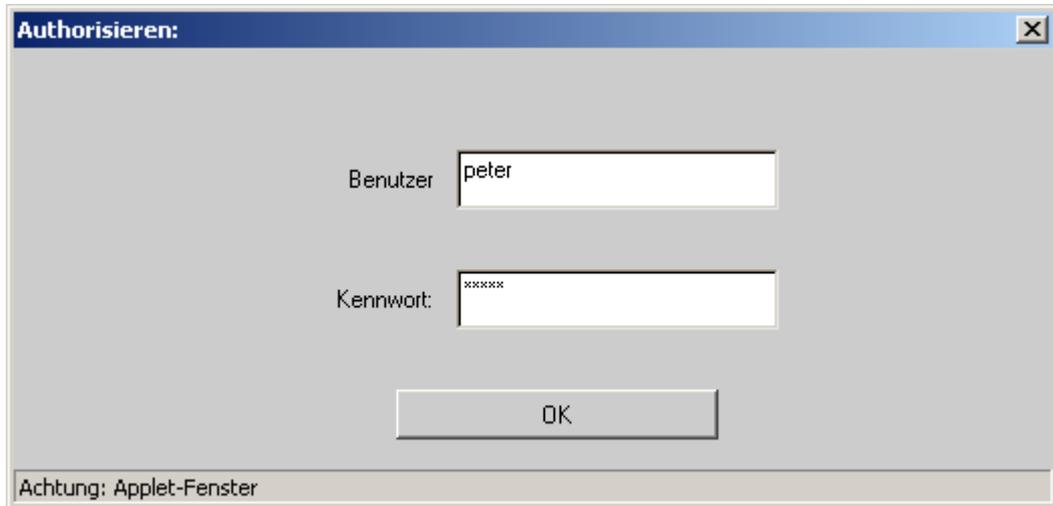
→ Settings -> Control Panel-> Java -> temporary internet files -> settings



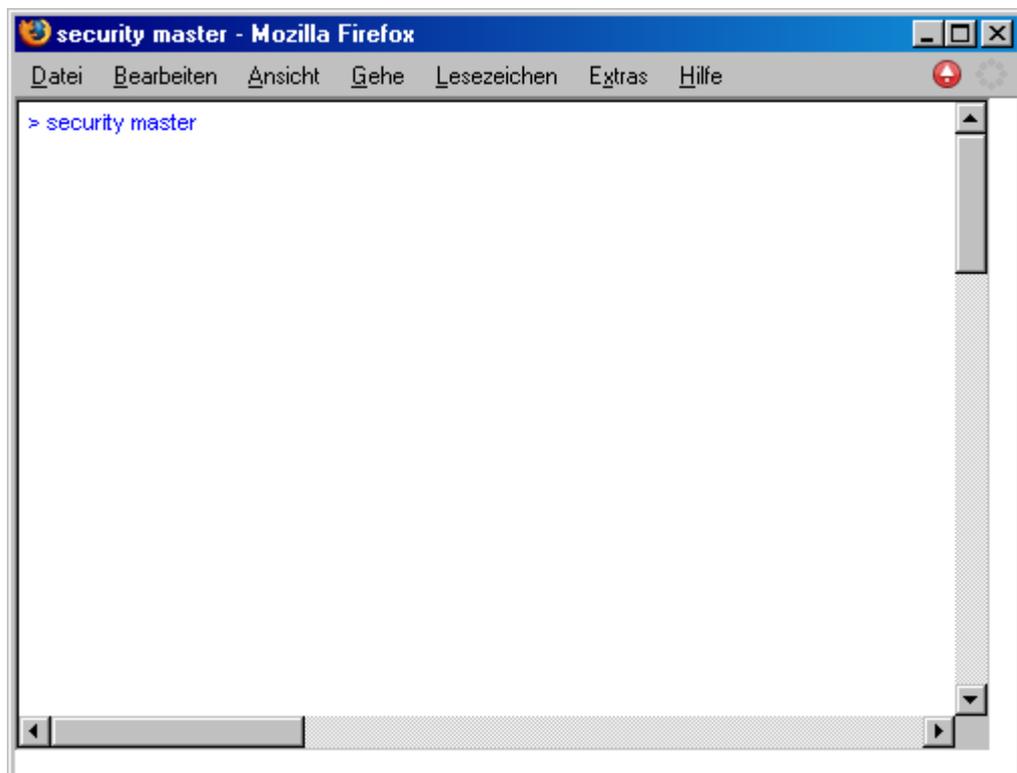
The box “Leave temporary files on the computer“ must be unchecked.

3.2.1 Log in

Open your web browser and enter 192.168.0.33 in the address bar. The **security master** will respond with the login mask.



Username: peter
 Password: peter
 ok



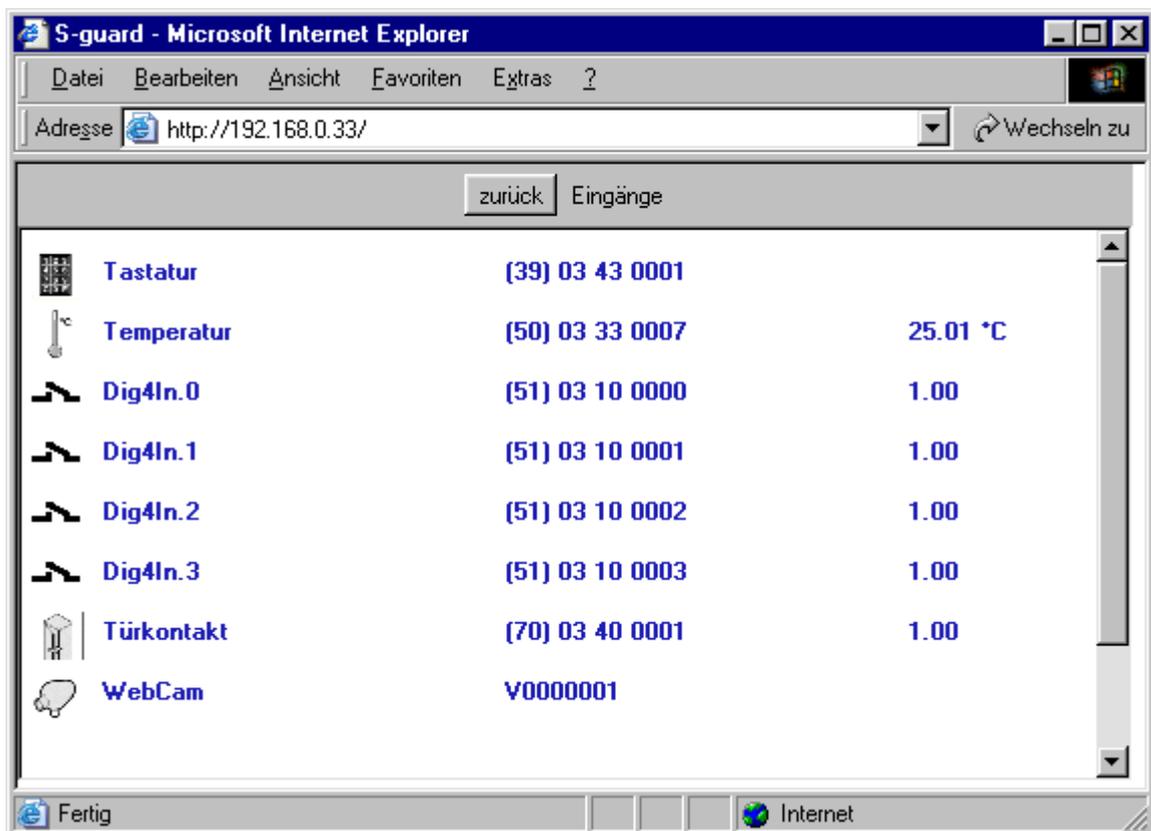
The **security master** will bring up the opening page (in the case of a new device the page will be empty)

3.2.2 Right mouse button

Upon clicking the right mouse button a menu will appear:



3.2.2.1 Inputs

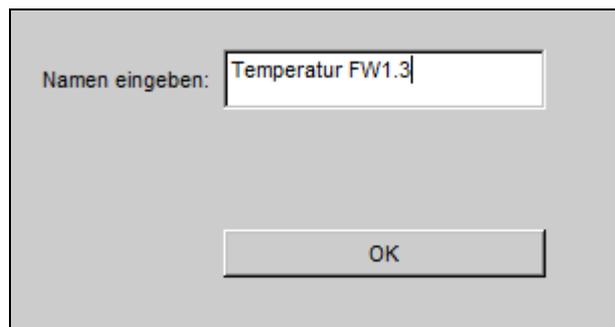
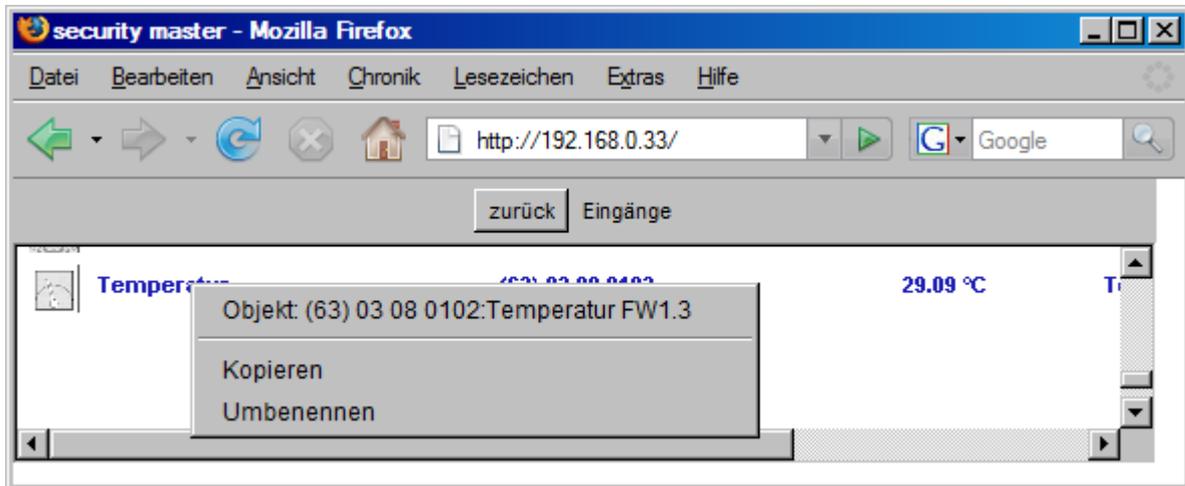


You will see a list of all connected and active input modules.

3.2.2.1.1 Renaming

Display "inputs" or „outputs“ list.

Place cursor on the appropriate sensor, right click, rename:

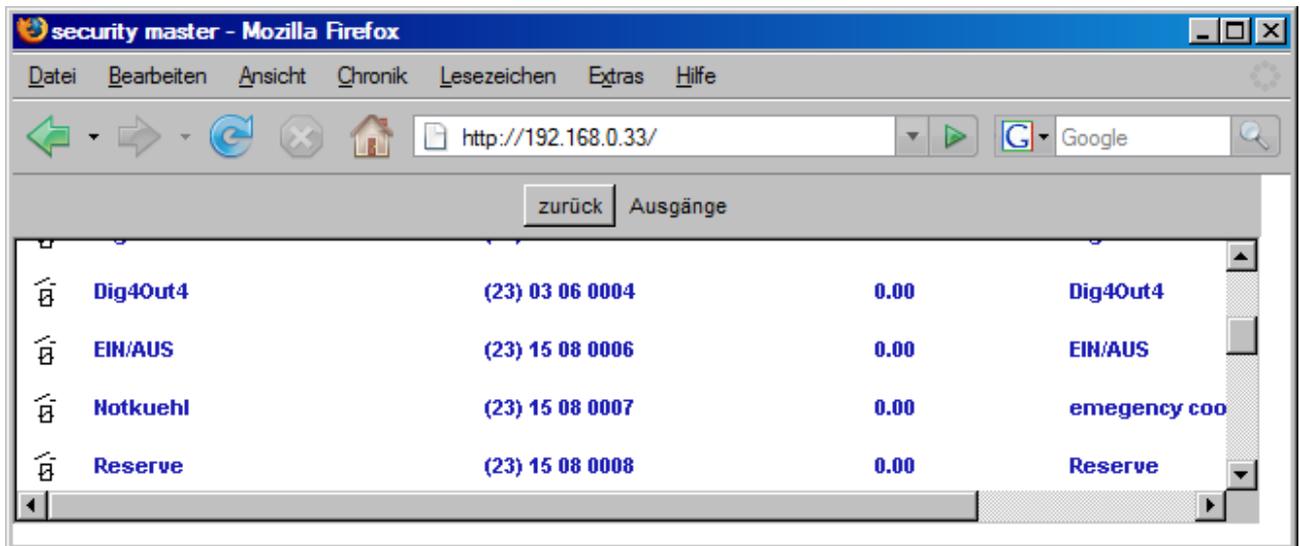


enter new name:



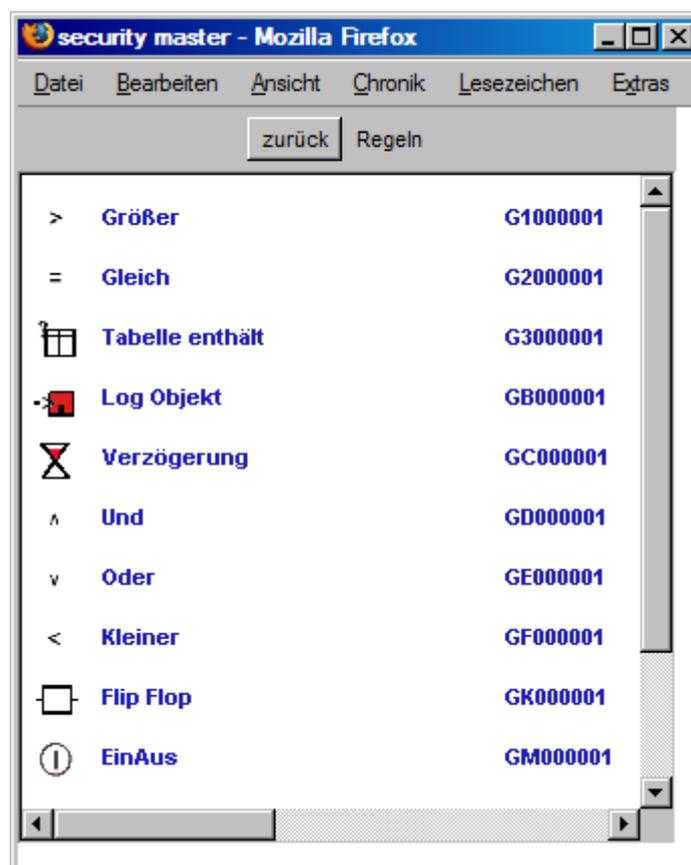
The new name is saved and will appear on every page.

3.2.2.2 Outputs



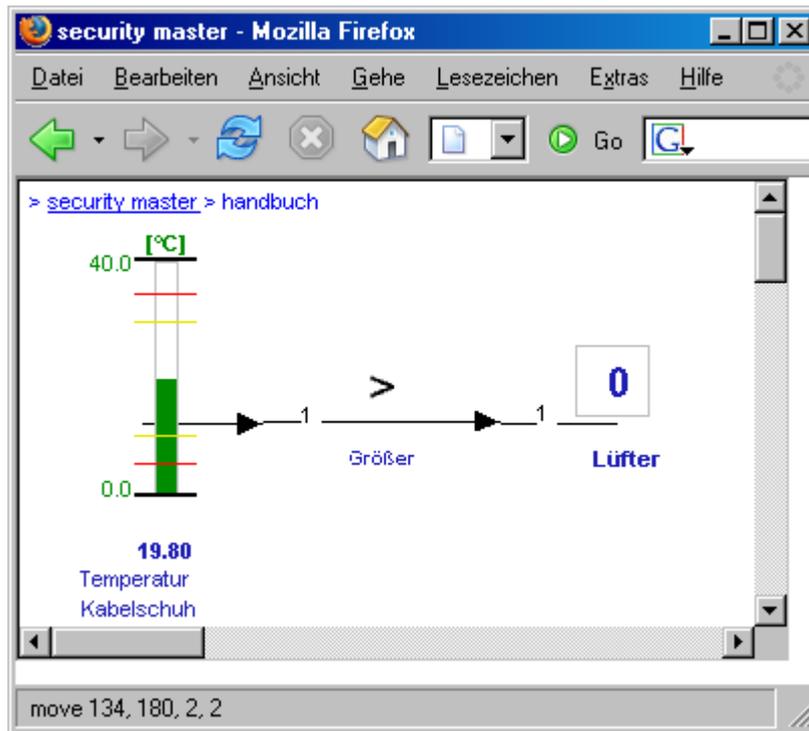
You will see a list of all active output modules connected to the **security master**. This example shows a 4 way digital output module.

3.2.2.3 Rules



You will see a list of all rules and computer statements stored in the **security master**. These serve to create logic operations between recorded data and the actions resulting from them. Take note in the use of logic operations of the logical conditions of the input and output variables. If, for example, an input with the condition “0” is supposed to execute a switching function, it must in some cases be negated (with the aid of the “equals function”) in order to generate the necessary condition “1”.

3.2.2.3.1 Greater than



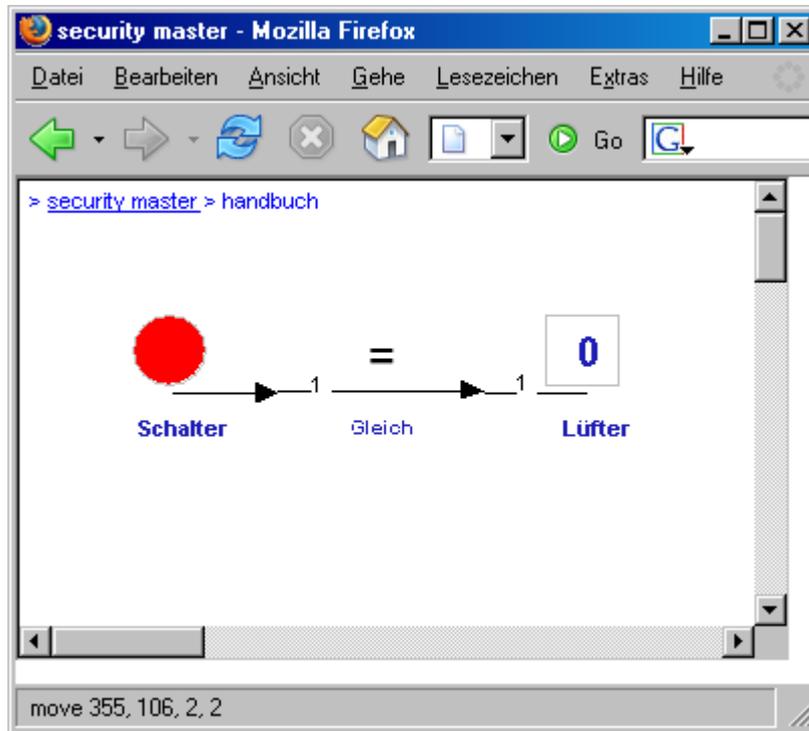
In this example, the “greater than” rule serves to control the function of a fan in the case where a particular temperature is exceeded.

The screenshot shows a dialog box titled "Regeleigenschaften". It contains two input fields: "Vergleichswert:" with the value "25" and "Hysterese:" with the value "1". Below these fields is an "OK" button. At the bottom of the dialog, it says "Java Applet Window".

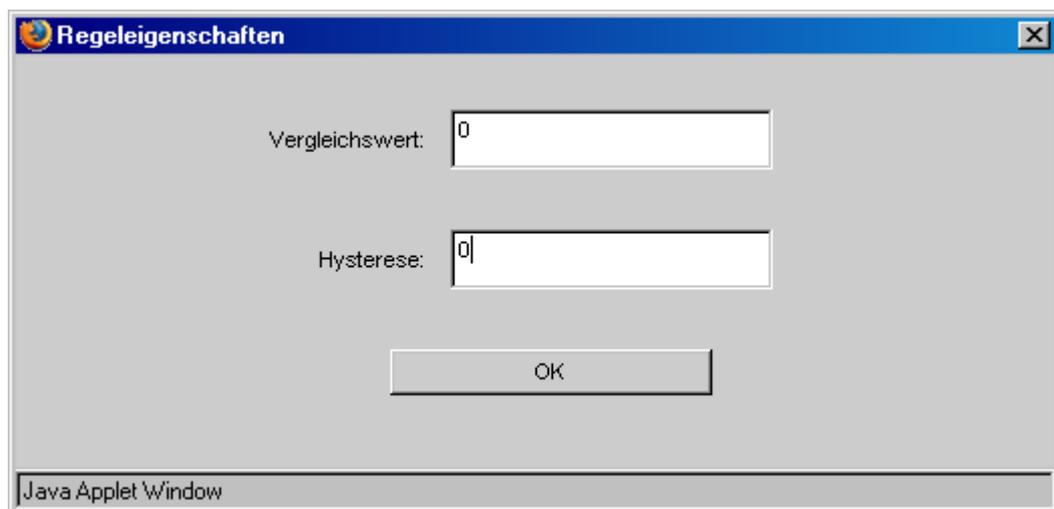
If the temperature of 25°C is exceeded the fan is switched on.

3.2.2.3.2 Equals

With the “equals” rule, an output function can be generated when a particular value is attained.



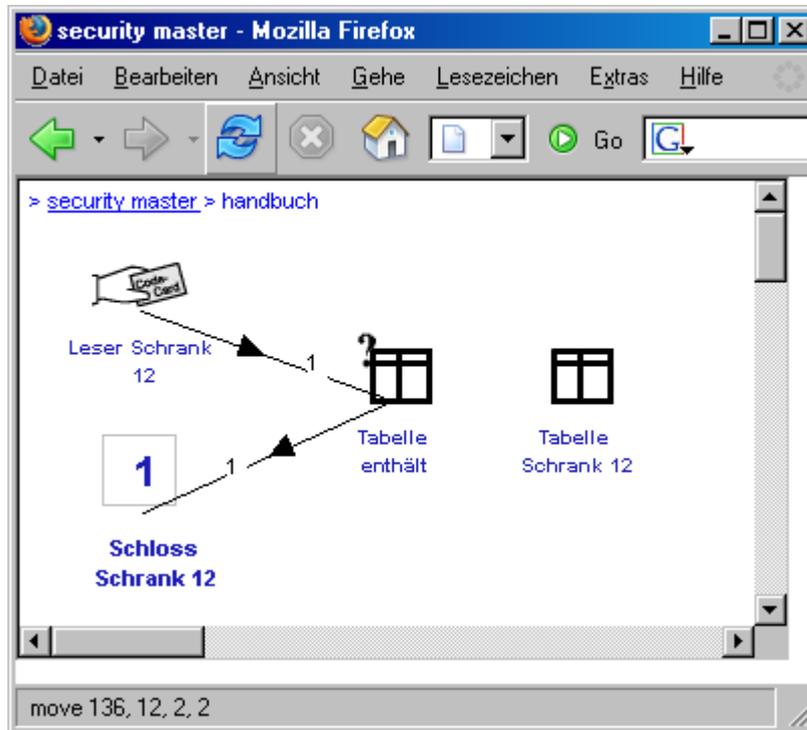
This function makes sense with analogue and digital inputs. In the case of digital variables this function can be used as an inverter. For this the reference value is set to “0”.



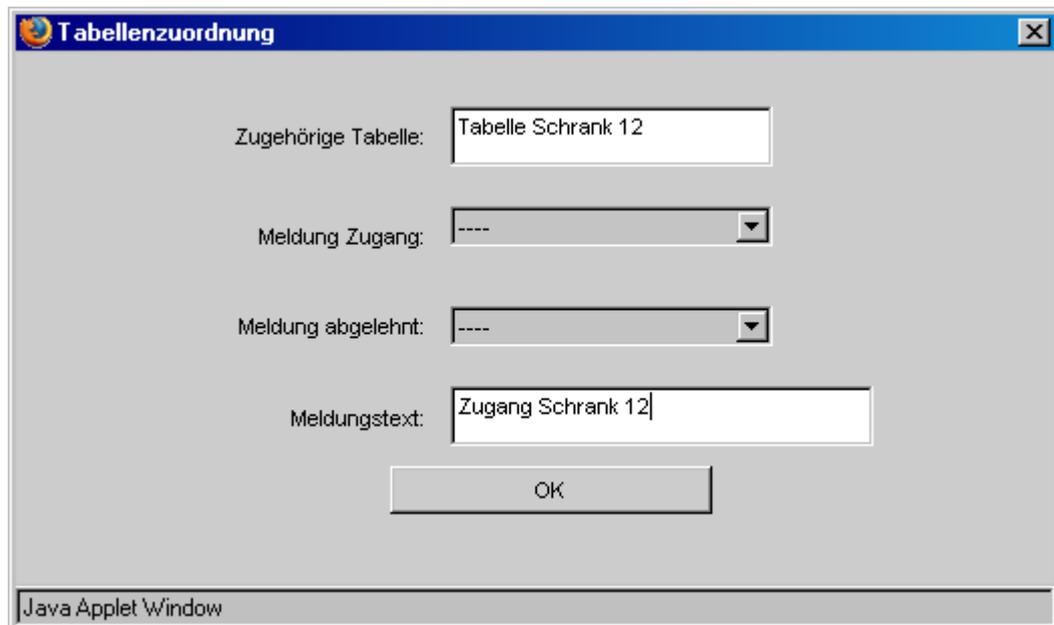
Inverter

3.2.2.3.3 Table contains

This function is needed to create a short cut to a table which contains the list of those with authorised access.

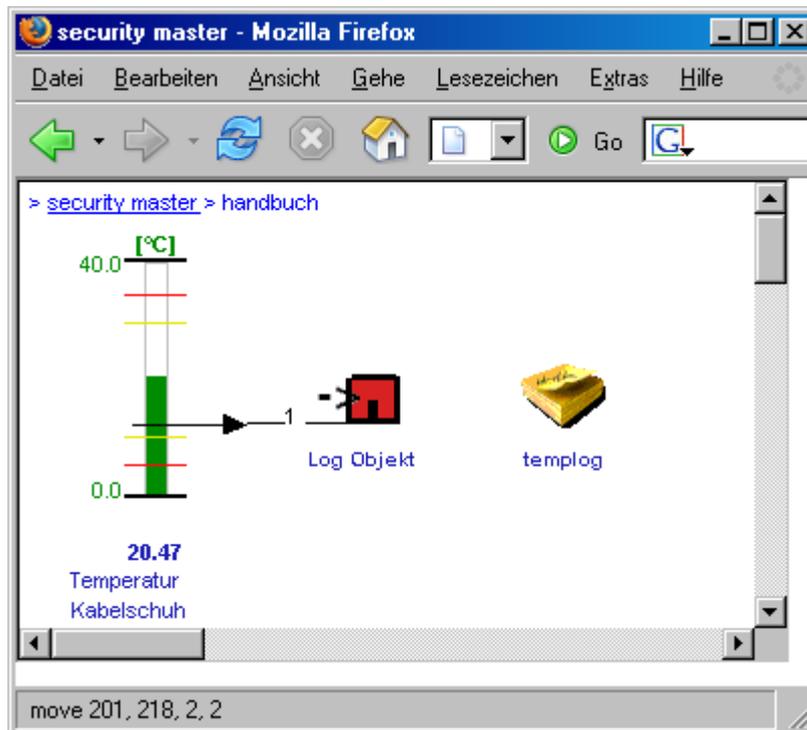


When a card is read, the “table contains” rule looks in the table to see if the card code is stored there. If yes, the lock is opened; if not, access is refused.



The name of the associated table is stored under “properties”.

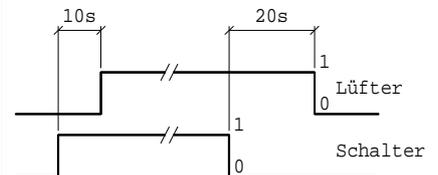
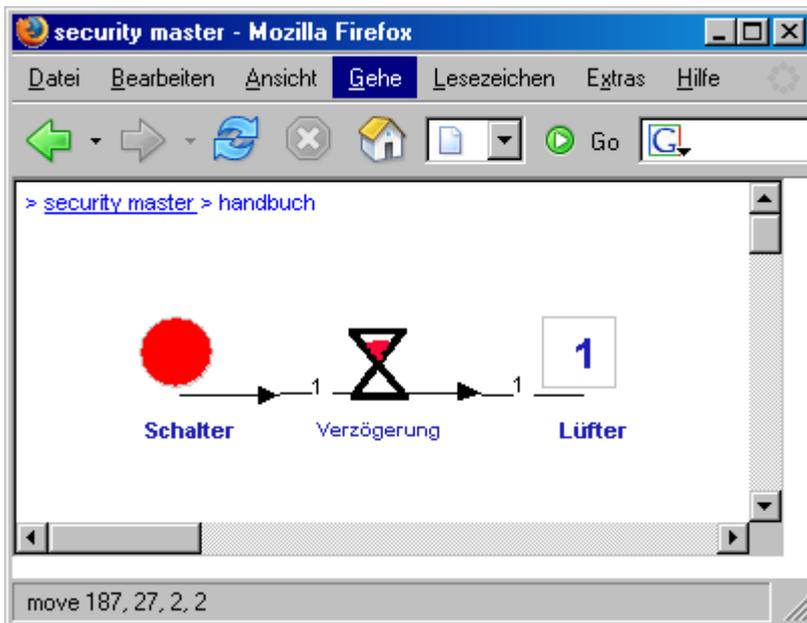
3.2.2.3.4 Log Object



With the aid of the „log object“ rule, 4 readings can be logged at the same time. Here the temperature readings are continuously saved in the “templog” file.

The log file and log parameters are defined under “properties“

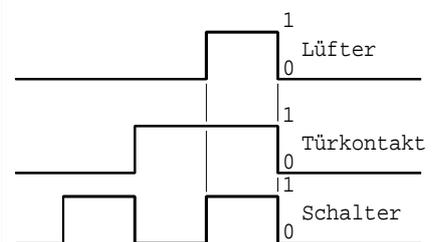
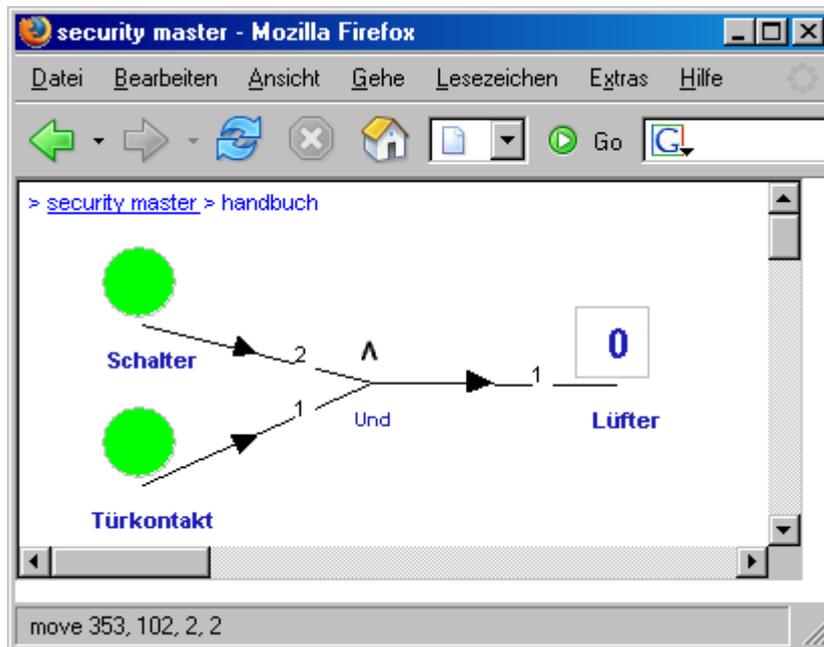
3.2.2.3.5 Delay



This rule can be used to implement a delay in switching on or off. The rule can be parameterised under “properties”

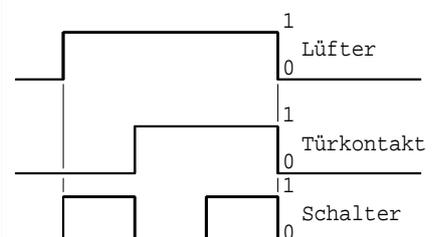
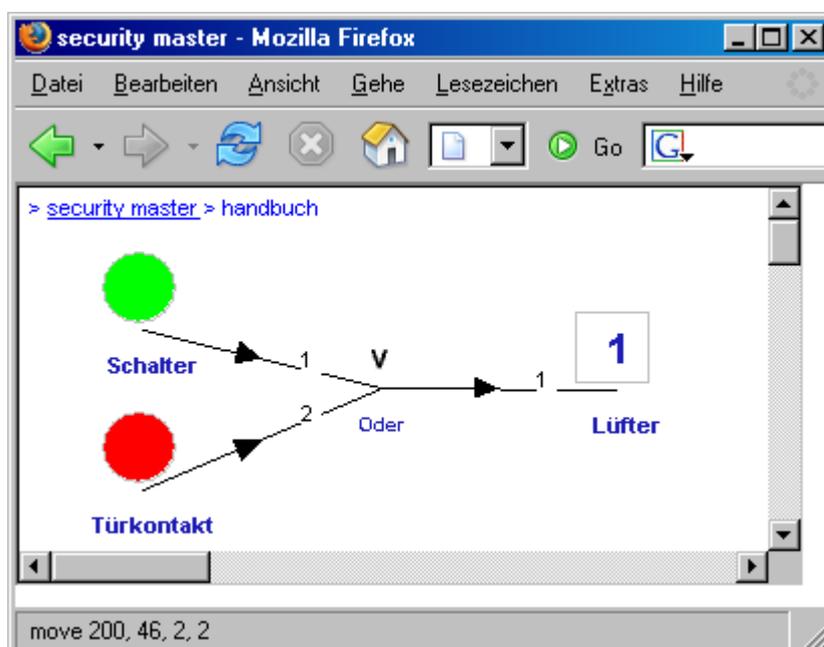
In this example the output of the delay element is switched on with a switching-on delay of 10 seconds and switched off again with a delay of 20 seconds after the output is switched off. The “off” condition is condition “0”.

3.2.2.3.6 And



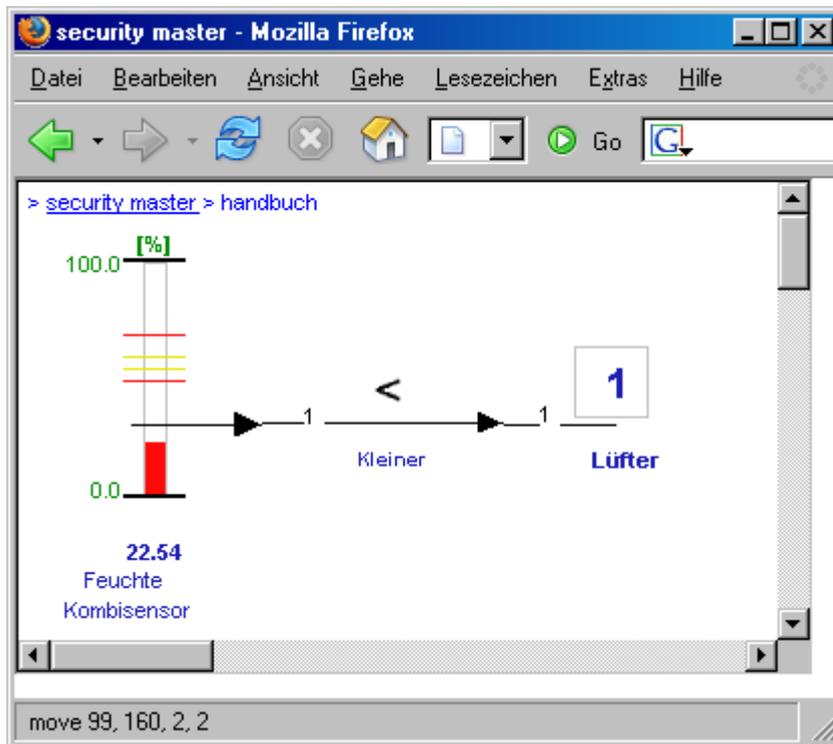
With the aid of the “and” rule, 2 inputs can be (logically) connected with each other. The fan is only switched on when both switches are set at “1”.

3.2.2.3.7 Or

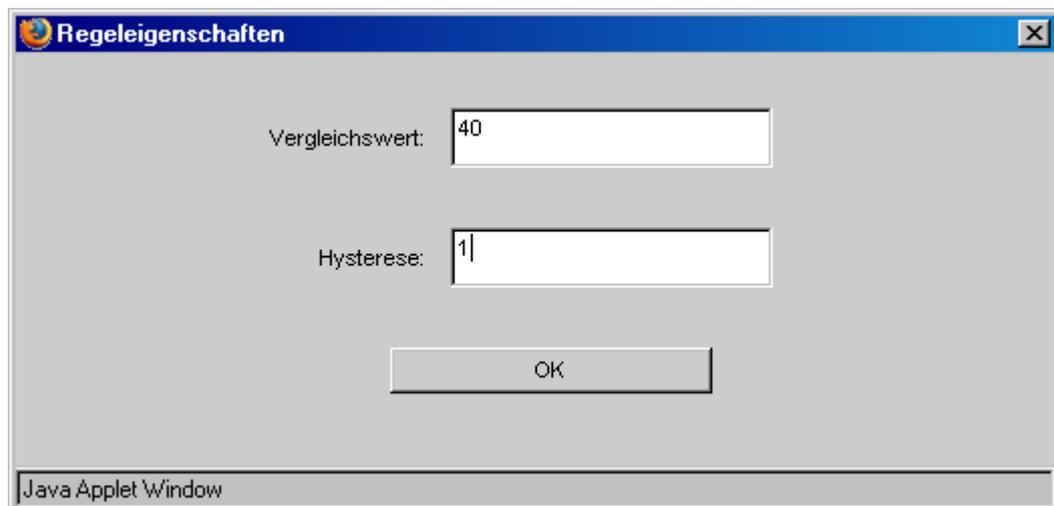


The fan is switched on when one or other of the switches is at “1”, or when both switches are at “1”.

3.2.2.3.8 Less than



In this example, the “less than“ rule serves to control a fan when the air humidity value falls below a certain limit.



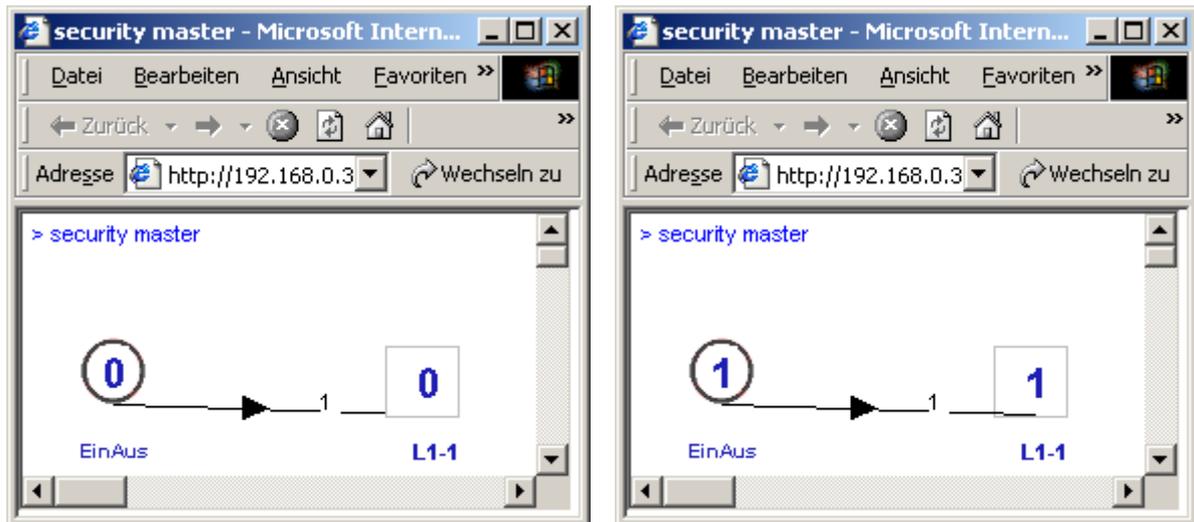
If the relative humidity value falls to 40% below a certain limit a fan is switched on.

3.2.2.3.9 Flip Flop

This function contains an RS Flip Flop.

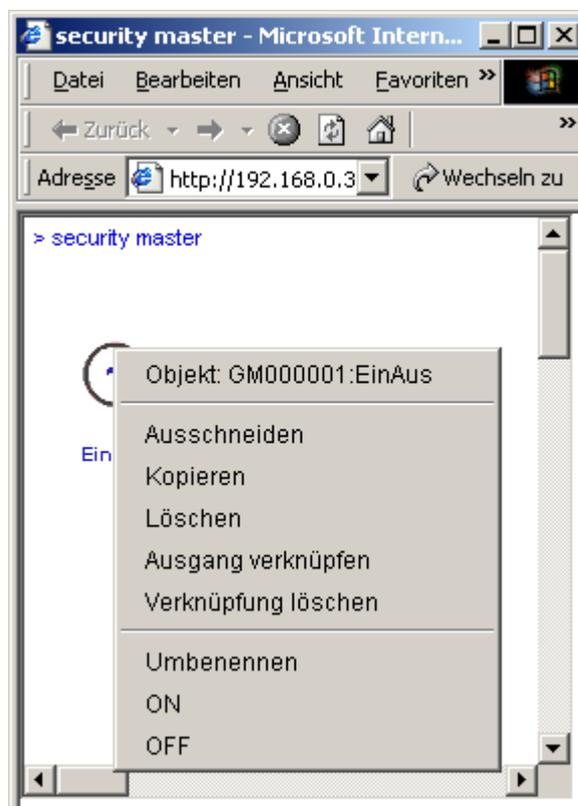
This function is linked to 2 input signals. One input signal sets the flip flop. With the help of the second input signal it is reset.

3.2.2.3.10 OnOff



With the help of the OnOff function, outputs can be activated via the user interface.

Right mouse button:



Control of the OnOff function

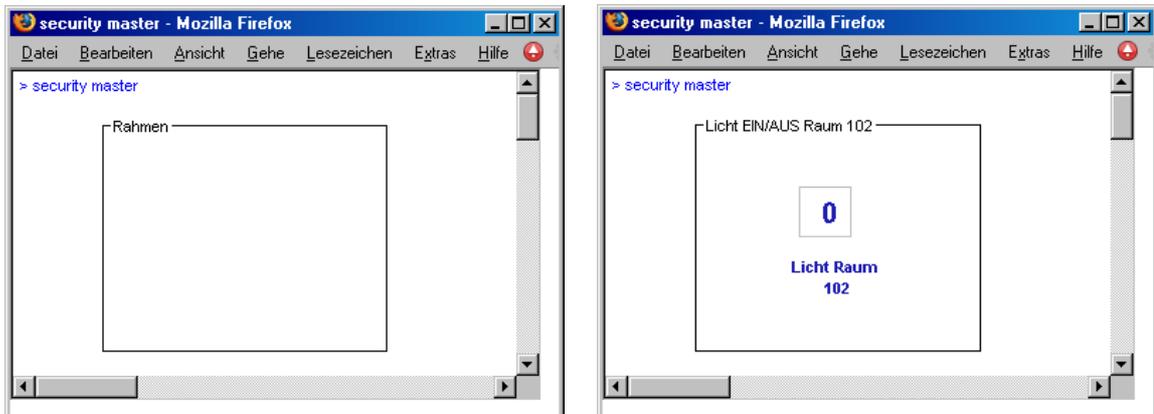
3.2.2.4 Tables



Overview of all the tables and system components stored in the **security master**.

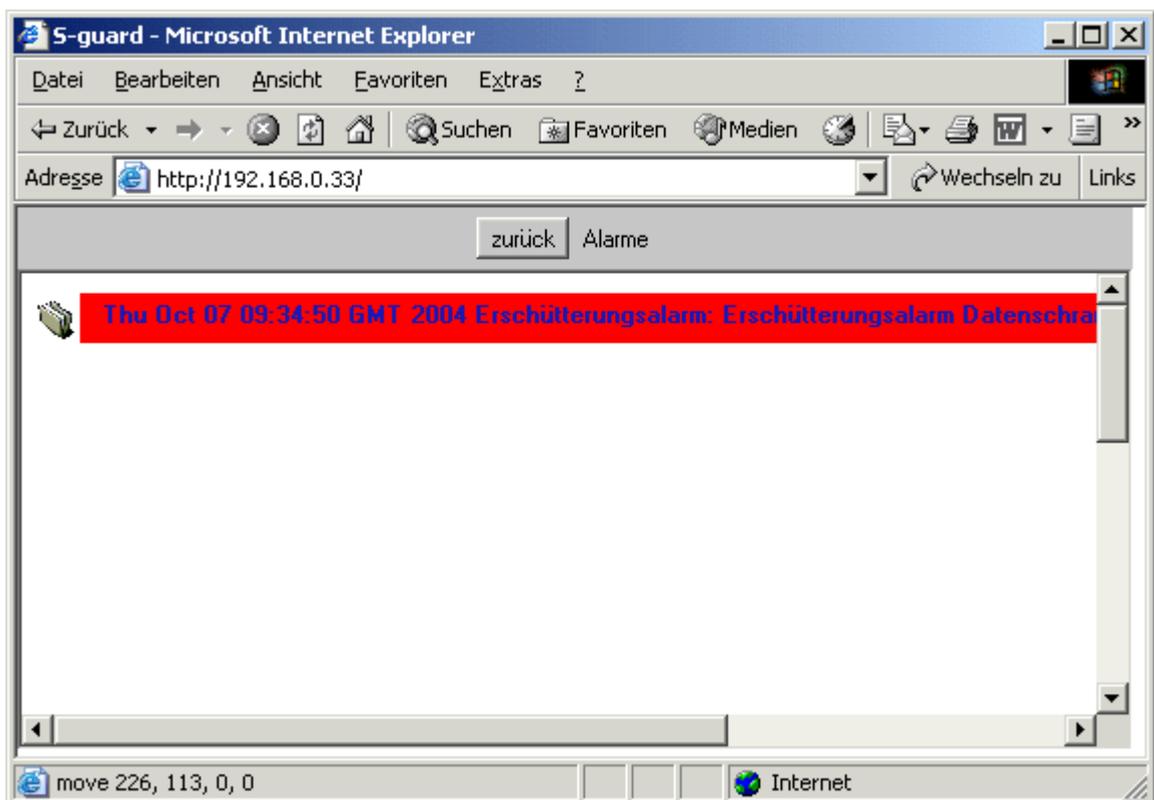
Table	For example, access codes are stored here for the locking system.
Alarms	Individual alarms are defined here which can be used in sensor configuration
Configuration	The security master's Configuration data are defined here
users	User names and passwords are stored here
Log file	Shortcuts to log files are created here
clock	The system clock is displayed here
Internal Sensors	Some internal sensor readings are displayed here
Alarm page	Here the accumulated alarm records are shown (see "alarms")
Webcam Log	Here the pictures from the IP camera are stored. In the case of internal storage the last 15 series of 6 pictures per camera can be viewed. If the pictures are stored on a network board then all of them can be viewed
SNMP allocation	Here the connected sensors are allocated to the ports (1-100)

3.2.2.5 Frames



A frame can be inserted to make the groupings clearer. The frame can be renamed.

3.2.2.6 Alarms



Alarms configured for the alarm page are displayed here.

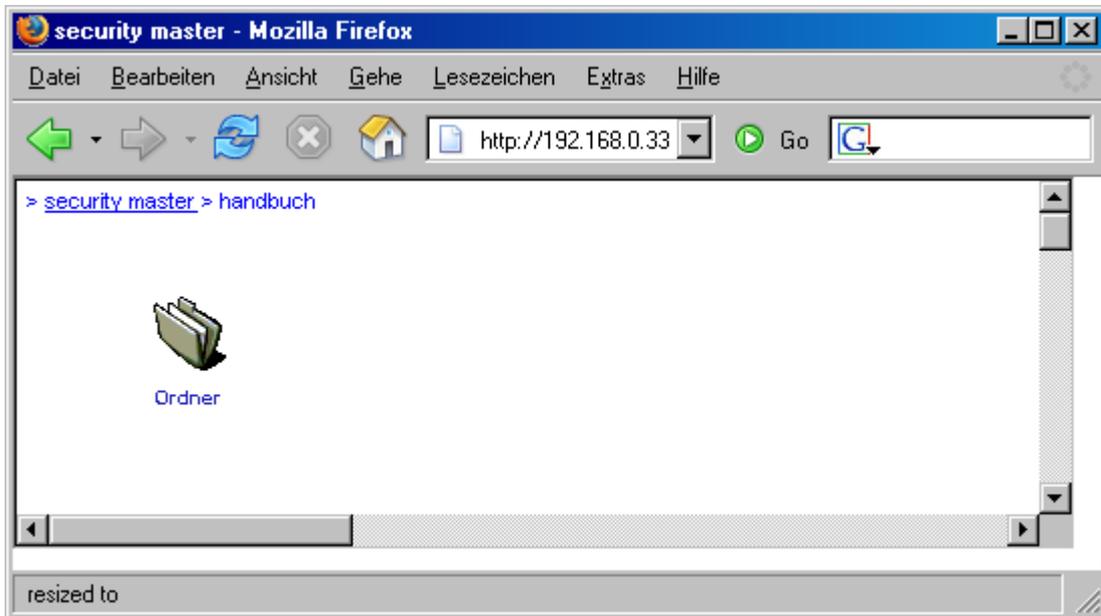
Used in conjunction with alarm monitoring, this page gives detailed information about any recorded alarms.

It is important that the alarm records contain all the information which is necessary in order quickly to process them. This means that the information must be very detailed, especially in the case of complex applications.

Using the right mouse button it is possible to delete single alarms or all alarms from this view. To delete an alarm, double click on it.

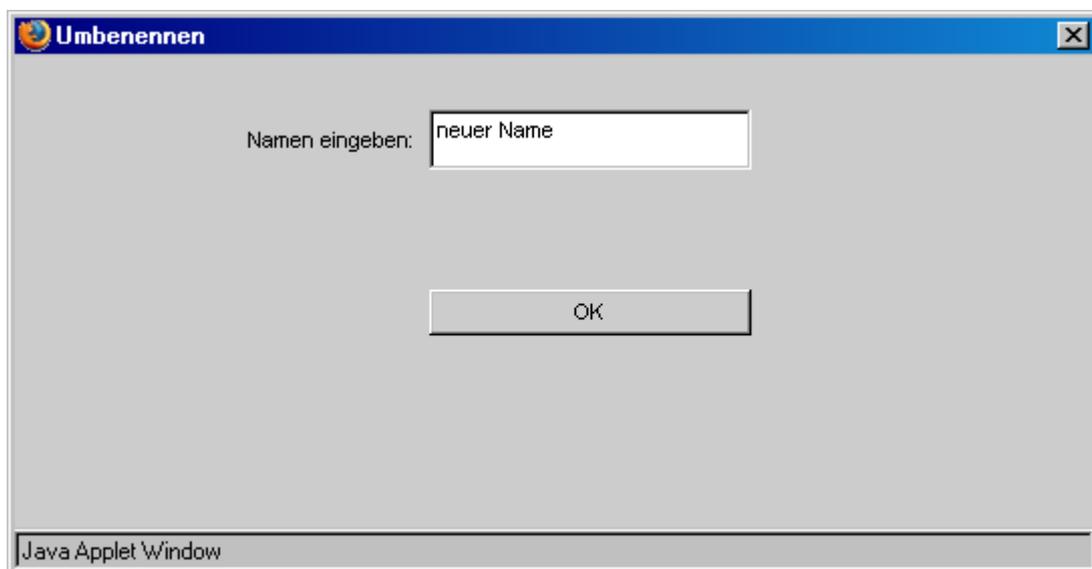
It is also possible to delete all alarms simultaneously.

3.2.2.7 Add Folder



This function is used to add a new folder to the current mask. The folder can be freely placed and renamed.

Right mouse button-> add folder-> left mouse button-> OK



Cursor on the folder-> right mouse button-> rename-> left mouse button -> enter new name -> OK

3.2.2.8 List view

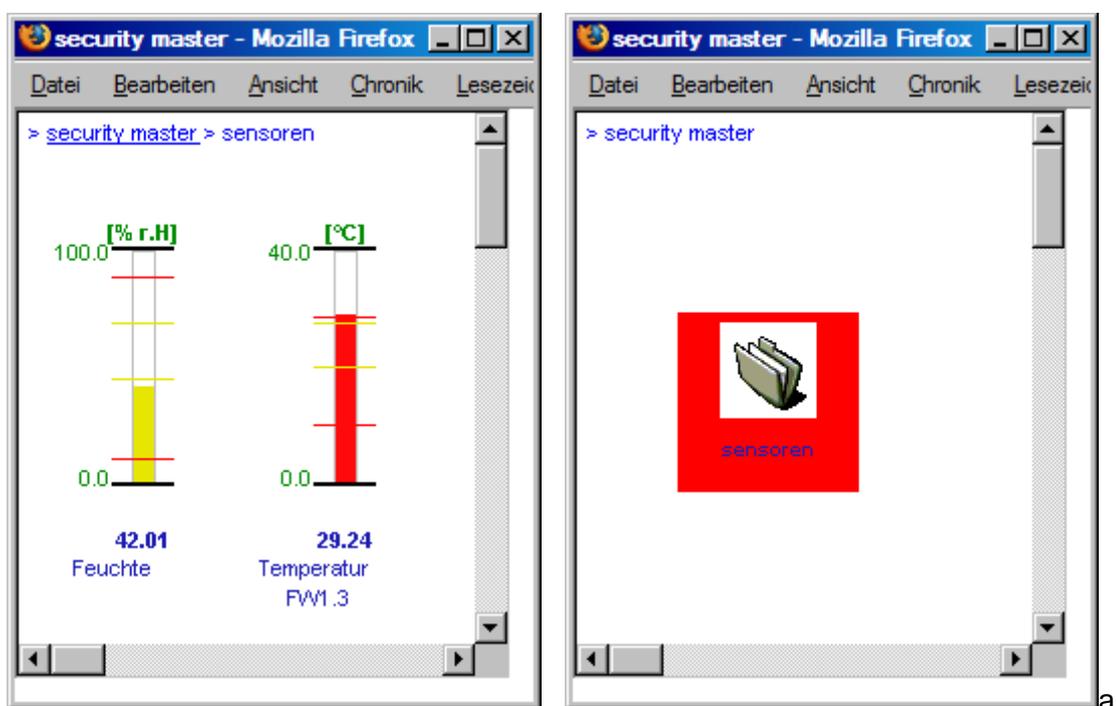
The folders and peripheral modules are listed.

3.2.2.9 Graphic view

The folders are displayed in a graphic and can be freely placed using the mouse. This display format may be clearer.

3.2.3 Sensor warning and alarm displays

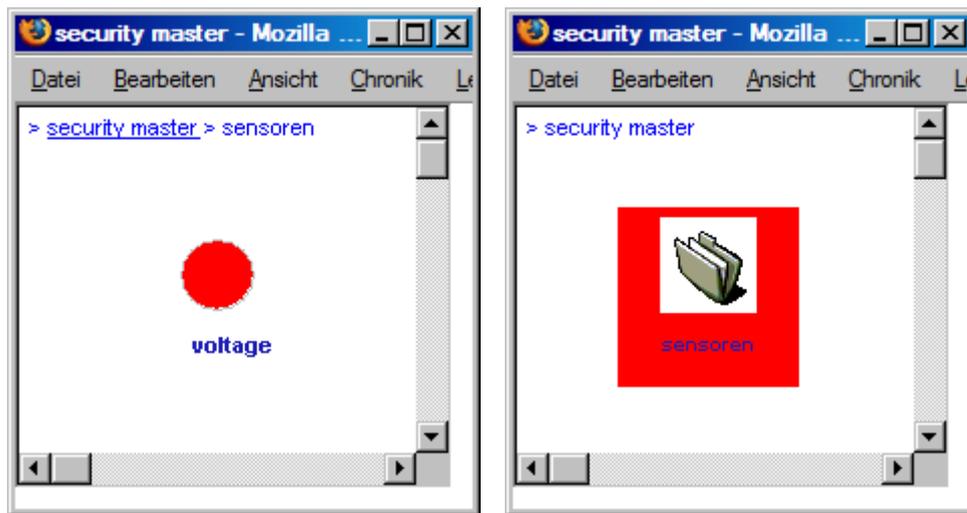
Analogue sensors switch to **warning condition** if the upper warning limit is exceeded, or if a value falls below the lower warning limit. The display bar then turns yellow. An **alarm condition** is indicated when the bar turns red.



Once a sensor has exceeded the upper alarm limit or the value has fallen below the lower limit the bar turns red, as does the superordinate folder.

A yellow folder colour is to be taken as a warning, and a red folder colour as an alarm. If the folder contains several different elements then the folder turns red if at least one subordinate sensor switches into alarm condition (also if a subordinate folder turns red). If none of the sensors are in alarm condition the folder turns yellow provided at least one subordinate sensor is in warning condition.

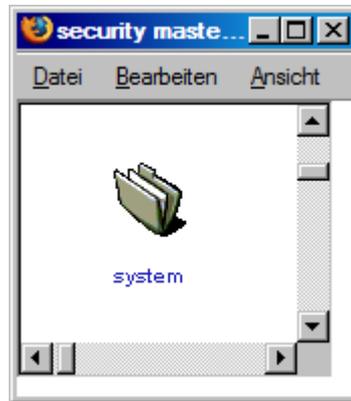
The folder colours do not depend on the definition of the alarms. They depend solely on the condition of the sensors. Whether alarms are sent or not, or whether they appear on the alarm page, is a matter of separate configuration.



In the case of digital sensors it is possible under “Properties“ to select how the superordinate folder should behave. That means it is a matter of choice whether the open or the closed condition should be signalled as red or green.

4 Setup security master

Firstly you can create a “system“ directory. This directory can be used to file and to edit all system parameters.



Add and rename folders.

4.1 Configuration

The configuration editing is now copied into the system folder.

Switch to „system“ directory.

Right mouse button -> tables -> configuration -> paste > place icon



4.1.1 Edit configuration

The screenshot shows a Java Applet window titled "System Konfiguration:". The window contains the following fields and controls:

- IP Adresse:** Text input field containing "192.168.0.33".
- SNMP community:** Text input field containing "public".
- Netzmaske:** Text input field containing "255.255.255.0".
- SMTP Server IP:** Text input field containing "192.168.0.41".
- Gateway:** Text input field containing "192.168.0.1".
- E-mail Absender:** Text input field containing "peter@secmaster.com".
- Netzwerk: (USER PASSWORD //IP/PATH):** Three adjacent text input fields, all empty.
- Logdatei für System Alarme:** A dropdown menu with "system" selected.
- Modem Amtsvorwahl:** Text input field, empty.
- Submaster:** A dropdown menu, empty, with "neu" and "löschen" buttons to its right.
- IP-Adresse vom Zeitserver (NTP):** Text input field, empty.
- IP Kamera:** A dropdown menu, empty, with "neu" and "löschen" buttons to its right.
- Lokale Logdateien löschen:** A button at the bottom left.
- Auslieferungszustand herstellen und neu starten:** A button at the bottom right.
- V 1.5.3 LHX20 IpCam** and **OK** buttons at the bottom center.

The status bar at the bottom of the window reads "Java Applet Window".

Here the specified system parameters can be defined.

System Configuration

IP Address	Here you define the device's IP address. This IP address does not take effect immediately. The security master must be rebooted for this to happen.
Net mask	Here you define the device's net mask.
Gateway	Here you define the device's gateway
Network board	Here you define the hard disk on which the log file readings and pictures on this security master are to be filed. For this a folder has to be released for sharing on the relevant server, or on your PC. USER PASSWORD //IP/Path (SMB Protocol) USER user of your PC PASSWORD Password of your PC (non-readable) IP IP Address of your PC Path Directory on your PC
IP Address of timeserver (NTP)	The system time on the security master is regularly synchronised with the timeserver indicated here (NTP). The timeserver is interrogated each time the security master is switched on and every 60 minutes thereafter.
Delete local log files	When this button is activated all log data in the security master are deleted. Any pictures from an IP camera which may have been stored are also deleted.
SNMP community	Here you define the device's SNMP community.
SMTP Server	Here you define the IP address of the e-mail server to which the e-mails generated by the device are to be sent.
E-Mail sender	Here you define the sender identity that appears when this device sends e-mails.
Log file for system Alarms	Here you define which alarms are to be set off when system alarms occur. System alarms are triggered for example when a sensor or access to the network board is lost.
Submaster	Here you define the IP addresses of all security masters which are to be shown on the user interface of this device.
IP camera	Here the access data for the IP camera are given. A maximum of 2 cameras may be connected.
Reset to factory settings and restart	The device is reset to the factory settings. All data are deleted. The IP address remains unchanged.

4.2 Users

Now the user access editing is copied to the system folder.



4.2.1 Edit users

neu

löschen

Kennwort

öffnen

Administrator

A new user is added. He can have administrator rights or just the rights to open directories.

Username: test

Password: secret

As soon as a user with Administrator rights is added the factory setting (username: peter, password: peter) is deactivated. Access is then only possible for those set up as Administrators!!!

4.3 Alarms

Initially, alarms are defined which can then be activated in the case of particular events or where limit values are exceeded etc.

First, the alarm editing is copied into the system folder.



Alarm Configuration

Trap Type	Here you set the Trap Type [0...255]
Trap	Here the IP addresses are defined to which the traps are sent
E-mail	Here you enter the e-mail addresses of all users who are to be informed when alarms are activated
SMS	via GSM (GPRS in preparation)
Log files	Here you enter the names of the log files in which the alarm protocols are to be saved.
add alarm to the alarm page	Here you can activate the display of individual alarms on the alarm page
Log the images	Here you can determine if pictures from the IP camera should be saved in the case of this particular alarm.
Signal after [s]	Here you can set a time delay. Once this time has elapsed an alarm signal is activated.
repeat Signal after [s]	If an alarm condition still applies once this time has elapsed a further alarm signal is activated
Do not repeat Signal after [s]	Once an alarm signal has been activated no further signal is activated within the period of time defined here.

Attention

Conflicts can occur between the settings „repeat signal after“ and „do not repeat signal after“. For this reason only one of these settings should ever be used.

4.3.1 Edit alarms

Here the individual alarms are defined.

The screenshot shows a Java Applet window titled 'Alarme' with a close button in the top right corner. The window contains the following configuration options:

- Konfiguration für Alarme:** A dropdown menu showing 'Temperatur ALARM'. To its right are two buttons: 'neu' and 'löschen'.
- Trap:** A dropdown menu showing '192.168.0.39'. To its right are two buttons: 'neu' and 'löschen'.
- Typ:** A text input field containing the number '6'.
- Email:** A dropdown menu showing 'peter@sm.com'. To its right are two buttons: 'neu' and 'löschen'.
- SMS:** An empty dropdown menu. To its right are two buttons: 'neu' and 'löschen'.
- Logdateien:** A dropdown menu showing 'templog'. To its right are two buttons: 'neu' and 'löschen'.
- Signalisieren nach [s]:** A text input field containing '0'.
- Nochmal signalisieren nach [s]:** A text input field containing '0'.
- Nicht nochmal signalisieren in [s]:** A text input field containing '0'.
- Alarm der Alarmseite hinzufügen
- Log the images
- OK** button

At the bottom of the window, it says 'Java Applet Window'.

Example of a temperature alarm.

4.3.2 Save pictures

The saving of pictures is set in the alarm configuration.

The option "log the images" must be activated for the corresponding alarm.

When an alarm signal is activated the 6 available pictures are saved. As a rule these will be pictures from the time window directly before the alarm event.

This interval can be adapted so that pictures from the relevant time window can be saved.

By the use of the option "signal after [s]" in alarm configuration, the time window can be moved back.

If, for example, the value of 3 s is entered here, the time window is moved back by 3 seconds, and, as a rule, 3 pictures from before and 3 from after the point of triggering of the alarm are saved.

By varying this parameter the time window for the saving of series of pictures can be moved back almost indefinitely.

4.3.2.1 Without "network board"

If, during the configuration, no path is entered for a "configuration", the pictures series are saved in case of an alarm in the **security master** itself.

A maximum of 15 picture series of 6 pictures each per camera is saved. Once this maximum has been reached the oldest series of pictures are overwritten.

To view the picture series, the "webcamlog" table must be copied onto the desired page. By double clicking on the symbol the list of picture series is displayed from which the desired picture series can be selected.

If a network board is entered in the configuration the picture series are saved on the "network board". All picture series are then saved and can be viewed. No older picture series are overwritten.

4.3.2.2 With "network board"

If the path to a network board is defined (see also "configuration" chapter), a "saveimages" subdirectory must be created in the directory which the **security master** is to access. In the case of an alarm the **security master** automatically saves the pictures in this directory. The picture series are continuously saved.

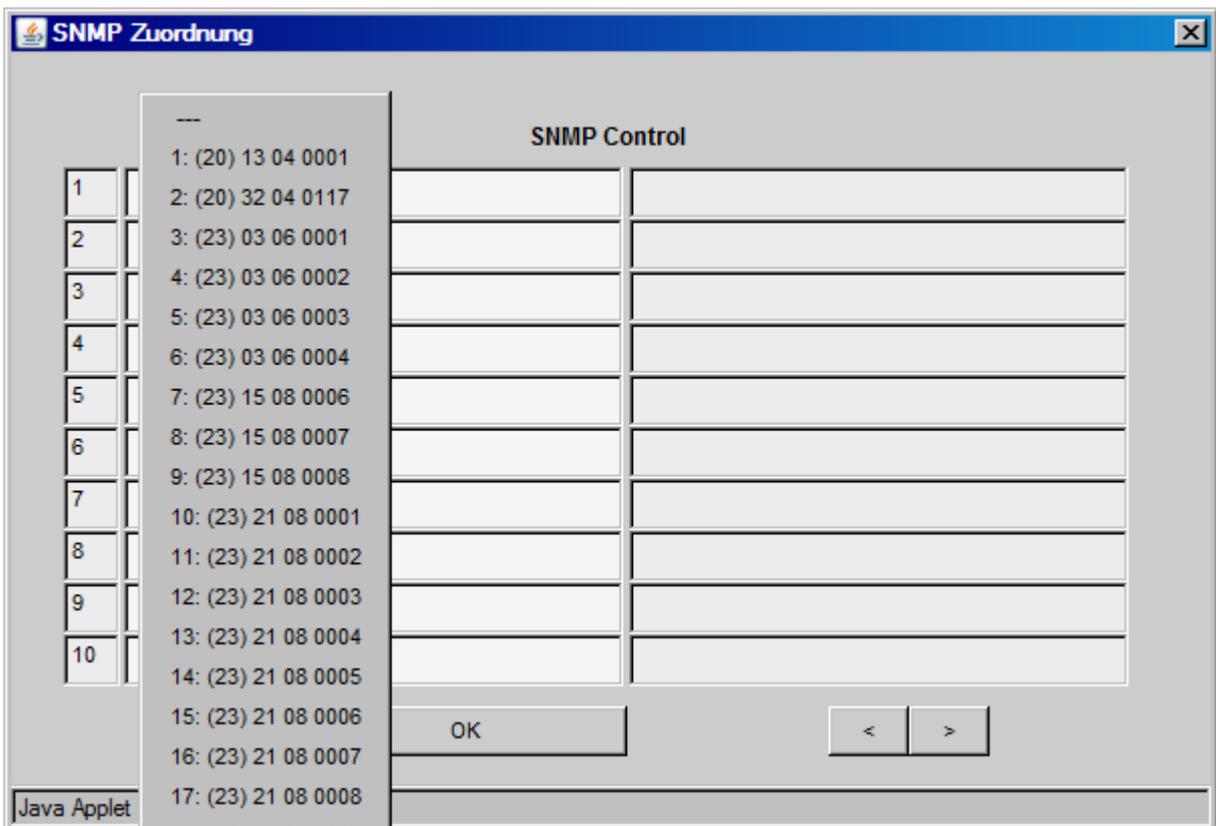
The selection and display of picture series is executed as before using the **security master**. The pictures are in any case also available for further evaluation on the network board.

4.4 SNMP allocation



SNMP allocation -> right mouse button -> "properties"





Place cursor on the desired port and click right mouse button.
 A list appears of the serial numbers of all connected inputs.
 Highlight, left mouse button, the serial number of the sensor is entered into the field.
 The name of the sensor is transferred into the right-hand field.

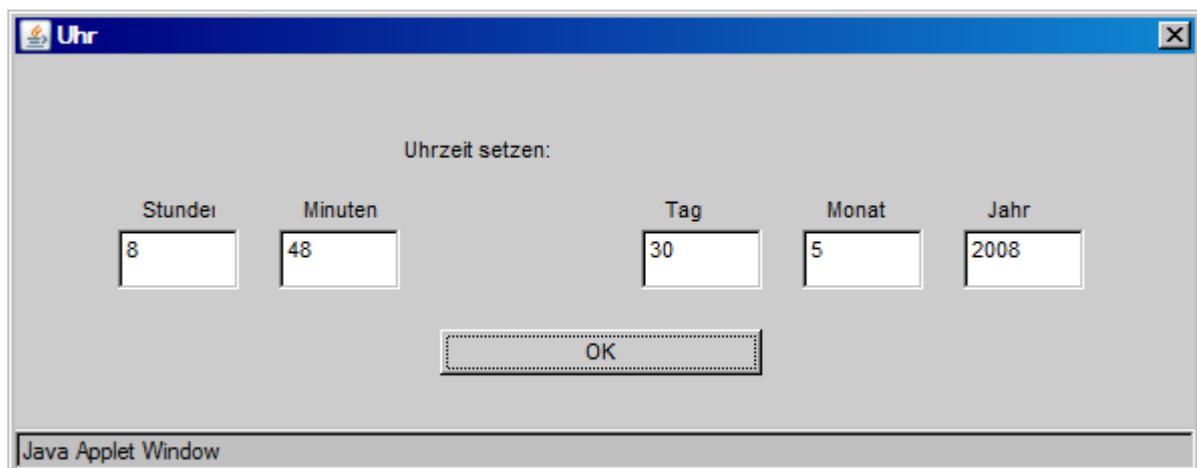
Now, using the MIB, the data from the sensors defined here can be read. Both Inputs and also the status of outputs can be read.

SNMP Control		
1	(20) 13 04 0001	doorlock front
2	(20) 32 04 0117	doorlock rear
3	(23) 03 06 0001	Dig4Out1
4	(23) 03 06 0002	Dig4Out2
5	(23) 03 06 0003	Dig4Out3
6	(23) 03 06 0004	Dig4Out4
7	(51) 04 08 0201	UPS 1 alarm
8	(51) 04 08 0202	diginp 1
9	(51) 04 08 0203	diginp 2
10	(51) 04 08 0204	diginp 3

4.5 Clock

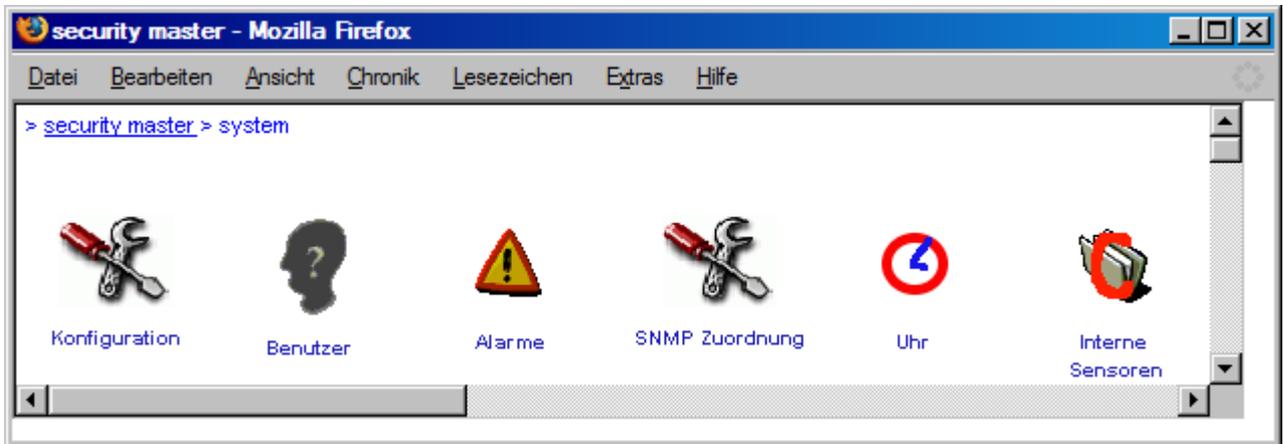


clock -> right mouse button -> "Properties"

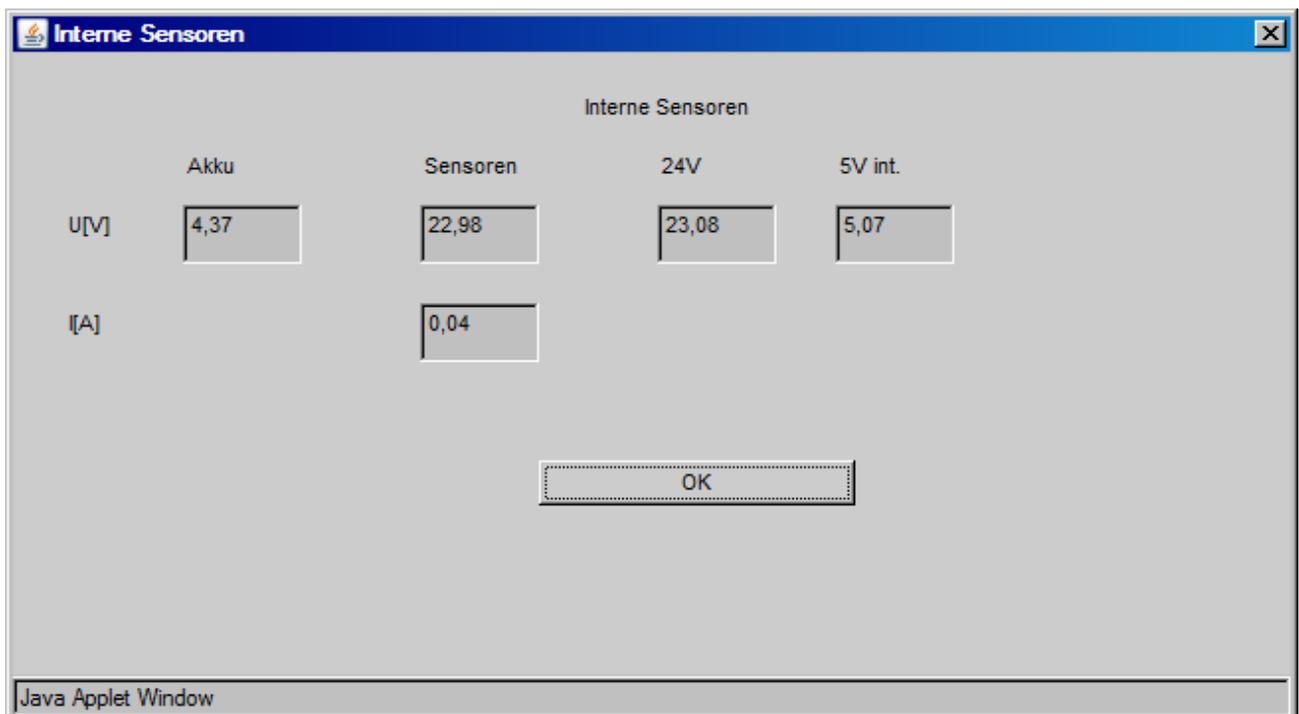


Here time and date settings can be changed.

4.6 Internal Sensors



Internal sensors -> right mouse button -> "Properties"



Here some parameters are displayed: for example, to enable recognition of overload in the power supply of the data bus.

5 security master functions

5.1 SNMP Protocol

The **security master** supports the sending of SNMP traps for all input modules, as well as for digital outputs.

The SNMP “get” function can be used for all connected sensors and actuators.

Digital outputs can also be switched using the SNMP “set” function. This includes the activation of the electromechanical locking functions.

5.1.1 Entries in the system configuration

The “SNMP community” must be entered into the system configuration.

5.1.2 Entries in the alarm configuration

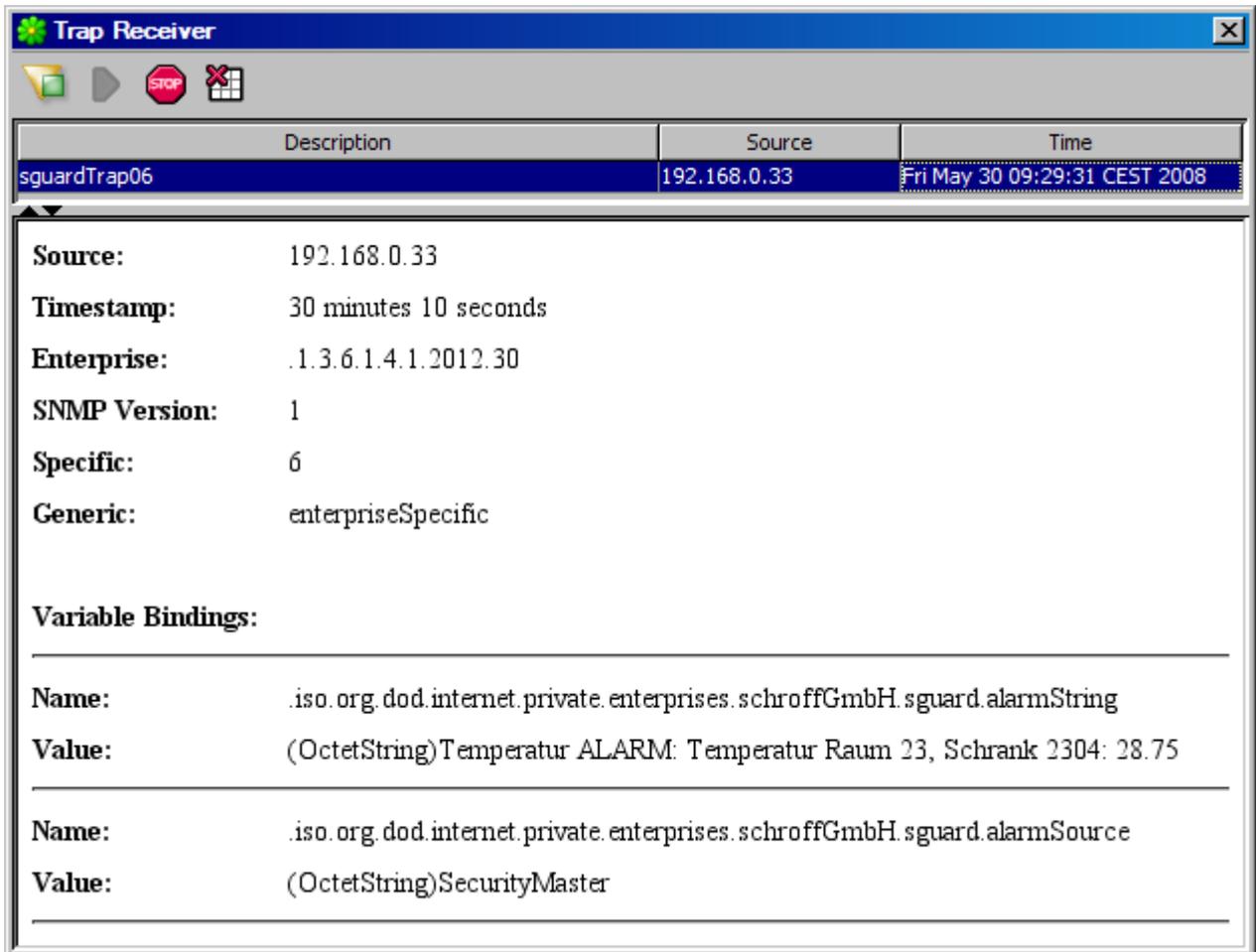
“Trap type” and recipient IP addresses must be entered in the alarm configuration.

5.1.3 Send SNMP Traps

With the aid of the SNMP protocol, SNMP traps can be sent. The trap recipients must be defined in the alarm configuration.

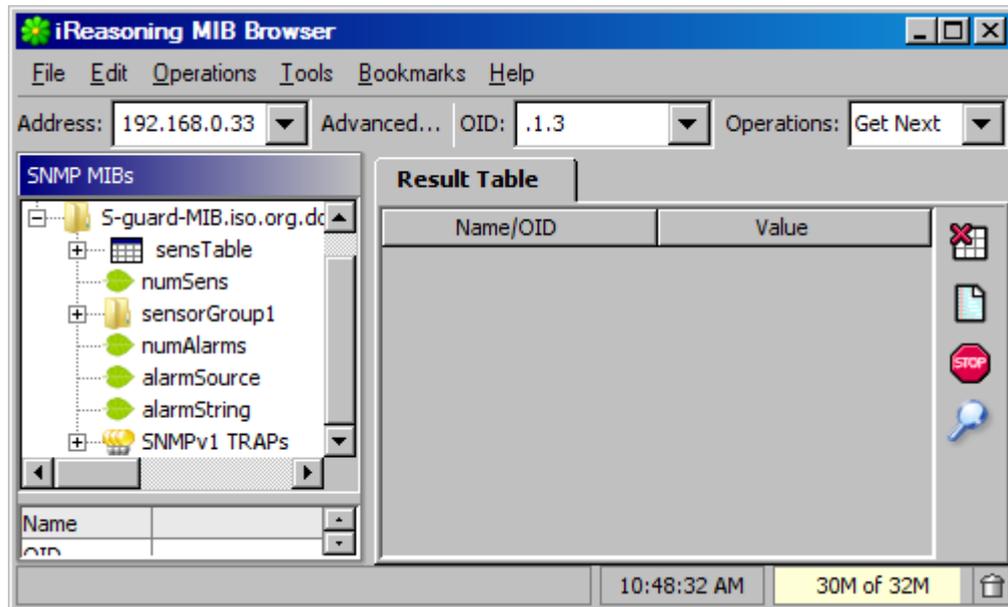
In this example, when a “temperature alarm” is triggered, an SNMP type 6 trap is sent to IP address 192.168.0.42.

The traps can be received using an “SNMP Trap Watcher”.



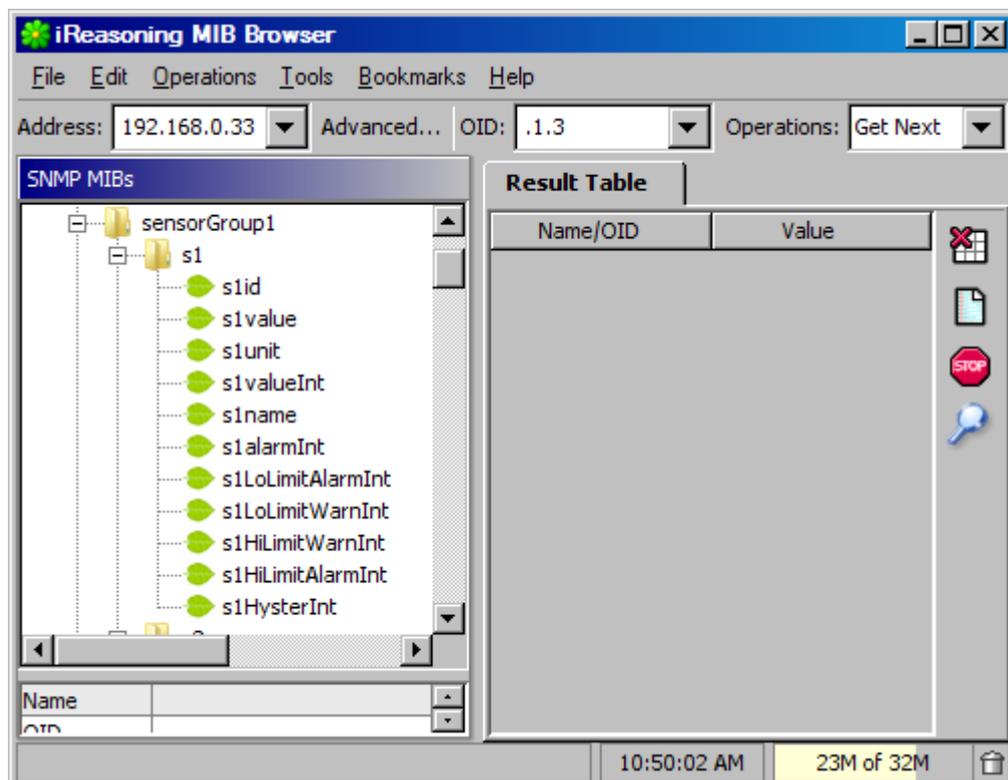
“Temperature alarm“ trap has arrived.

5.1.4 MIB Browser



The “sensTable“ administers a dynamic MIB.
 Under “sensorGroup1” 100 logical ports are available.
 Under “numAlarms” the number of alarms notifications accumulated but not yet acknowledged can be called up. This means that, when the value is 0, **no new** alarms have been recorded.

5.1.4.1.1 Call-up values



Call-up values

Id	Identification (Ser.-No.) of the sensor
value	value
unit	Reading unit
valueInt	value as integer
name	Name of the sensor
alarmInt	<p>Condition of the sensor (analogue sensor)</p> <ul style="list-style-type: none"> -1 Port not yet initialised (no value) 1 lower red zone 2 lower yellow zone 3 green zone 4 upper yellow zone 5 upper red zone <p>Condition of the sensor (Digital sensor)</p> <ul style="list-style-type: none"> -1 Port not yet initialised 1 green zone 5 red zone
LoLimitAlarmInt	Lower alarm limit
LoLimitWarnInt	Lower warning limit
HiLimitWarnInt	Upper warning limit
HiLimitAlarmInt	Upper alarm limit
HysterInt	Hysteresis as integer

Thus all necessary values are made available to a management system, so that own monitoring and alarming functions may be carried out.

5.1.5 Read data using SNMP GET

5.1.5.1 Load MIB

In order to be able to read data via SNMP, the MIB (Management Information Base) of the **security master** must be made available to the MIB browser or management system used.

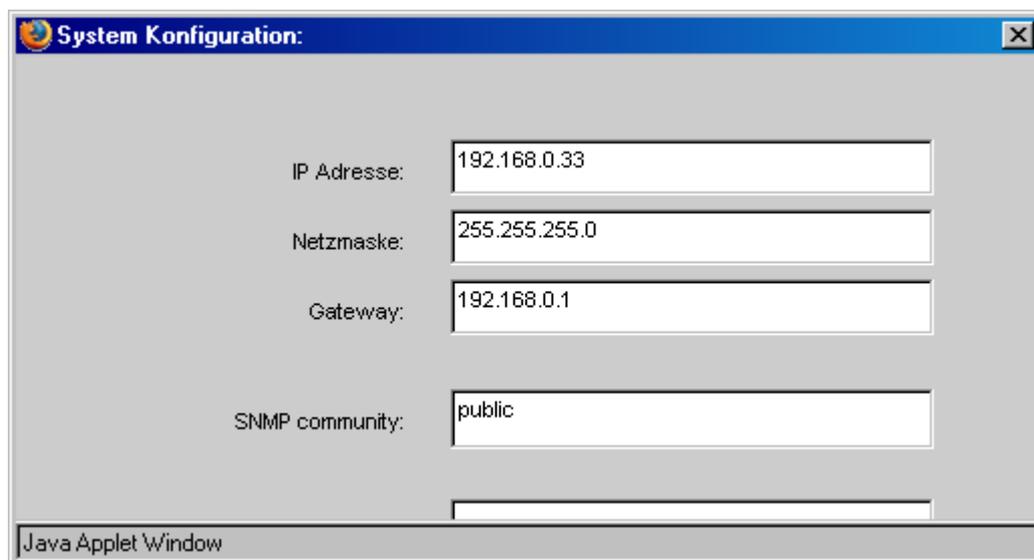
The MIB of the **security master** is to be found in a directory in the **security master** and is to be loaded and saved with the web browser of the **security master** and used with a suitable SNMP management system:

[http://IP-Address-of the -security master/secmaster.mib](http://IP-Address-of-the-security-master/secmaster.mib)

Delivery condition:

<http://192.168.0.33/secmaster.mib>

The SNMP community is set up in the system configuration. If no particular security measures are necessary, the usual setting is, for example, "public".



The screenshot shows a Java Applet Window titled "System Konfiguration:". It contains four input fields for configuration:

IP Adresse:	192.168.0.33
Netzmaske:	255.255.255.0
Gateway:	192.168.0.1
SNMP community:	public

At the bottom of the window, it says "Java Applet Window".

SNMP community is „public“

5.1.5.2 Read data

In order to read data from the device using “Get”, it is first necessary to connect each sensor to a logic port using SNMP allocation.

The data from the connected sensors which have been entered in the SNMP allocation can then be read.

The screenshot shows the iReasoning MIB Browser interface. The top bar includes a menu (File, Edit, Operations, Tools, Bookmarks, Help), an Address field (192.168.0.33), an OID field (3.6.1.4.1.2012.30.3.13.11.0), and an Operations dropdown (Walk). The main area is divided into two panes: 'SNMP MIBs' on the left and 'Result Table' on the right. The 'SNMP MIBs' pane shows a tree structure with 'sensorGroup1' expanded to show 's1' and its sub-objects. The 'Result Table' pane displays a list of objects and their values.

Name/OID	Value
s1id.0	4
s1value.0	1
s1unit.0	
s1valueInt.0	1000
s1name.0	doorlock front
s1alarmInt.0	-1
s1LoLimitAlarmInt.0	0
s1LoLimitWarnInt.0	0
s1HiLimitWarnInt.0	0
s1HiLimitAlarmInt.0	0
s1HysterInt.0	0
s2id.0	u
s2value.0	1
s2unit.0	
s2valueInt.0	1000
s2name.0	doorlock rear
s2alarmInt.0	-1
s2LoLimitAlarmInt.0	0
s2LoLimitWarnInt.0	0
s2HiLimitWarnInt.0	0
s2HiLimitAlarmInt.0	0
s2HysterInt.0	0
s3id.0	#
s3value.0	
s3unit.0	
s3valueInt.0	0
s3name.0	Di4Out1

Below the tree view, a table shows details for the selected object 's1':

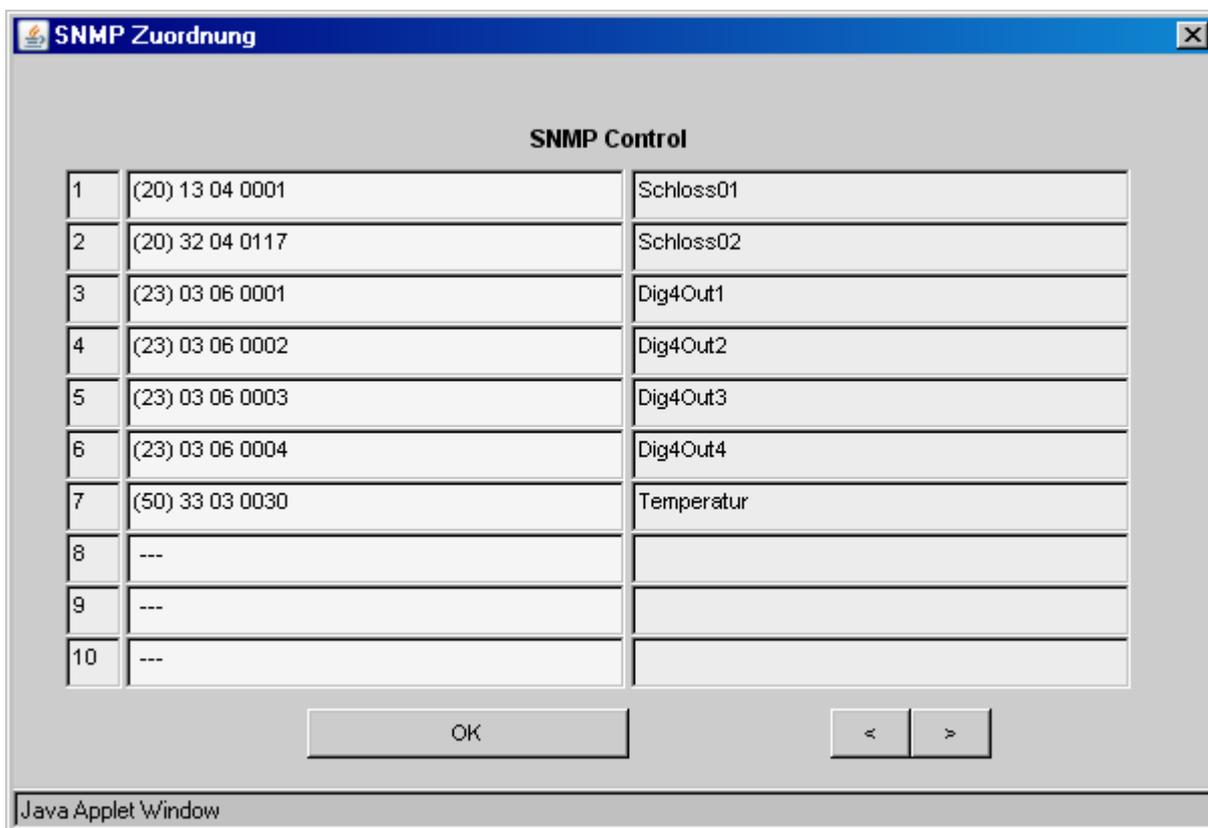
Name	s1
OID	.1.3.6.1.4.1.2012.30.3.1
MIB	S-guard-MIB
Syntax	
Access	
Status	
DefVal	

The status bar at the bottom shows the URL: .iso.org,dod.internet.private.enterprises.schroffGmbH.sguard.sensorGroup1.s13..., the time 11:05:01 AM, and the page number 28M of 34M.

5.1.6 Switch digital outputs using SNMP “set”

First the associated MIB must be loaded and program version 1.3.30 or higher must be installed on the **security master**.

The locks and digital outputs are defined in the SNMP allocation as described earlier.

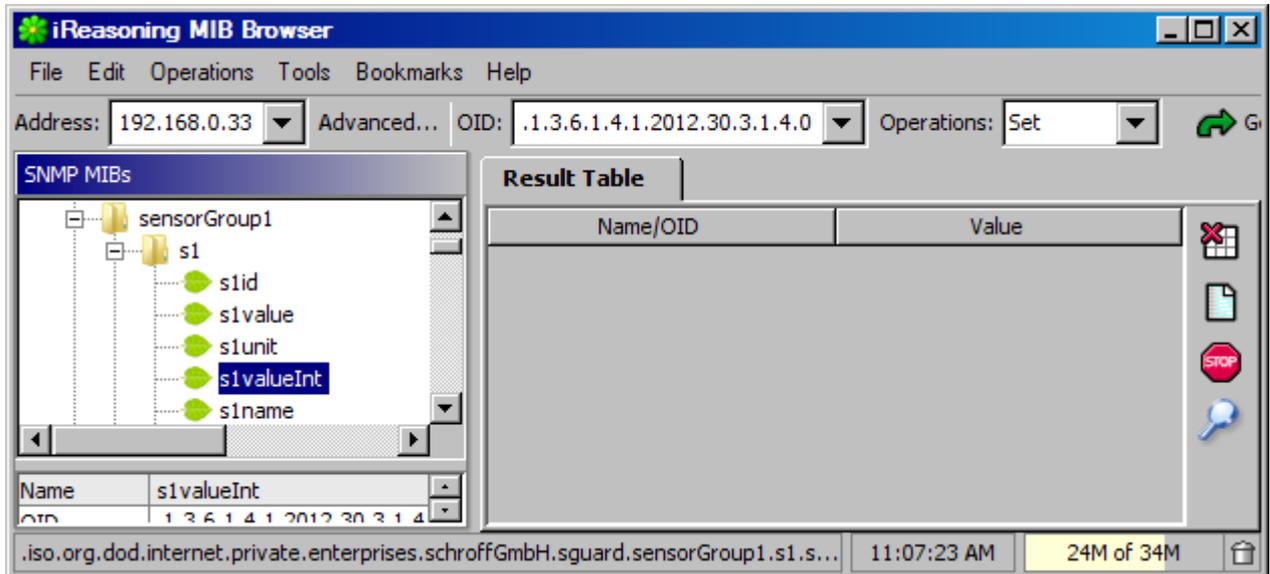


2 locks, 4 digital outputs and 1 temperature sensor are connected.

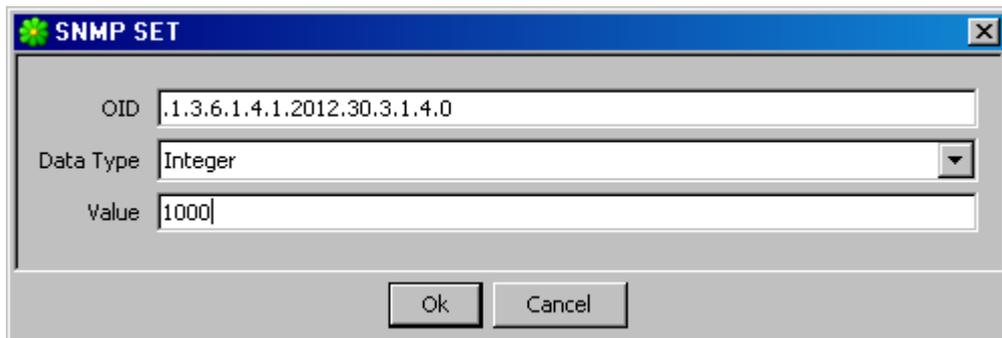
In the case of locks, “valueInt” can be set to open the doors. With digital outputs, “valueInt” can be set and reset.

valueInt = 1000 lock is opened or digital output is set,
valueInt = 0 digital output is reset.

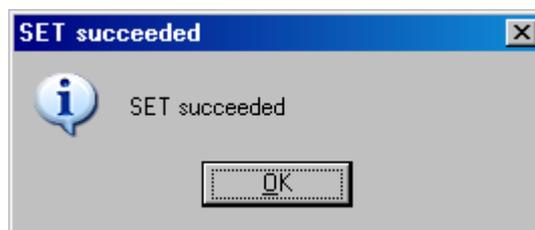
5.1.6.1 Open lock



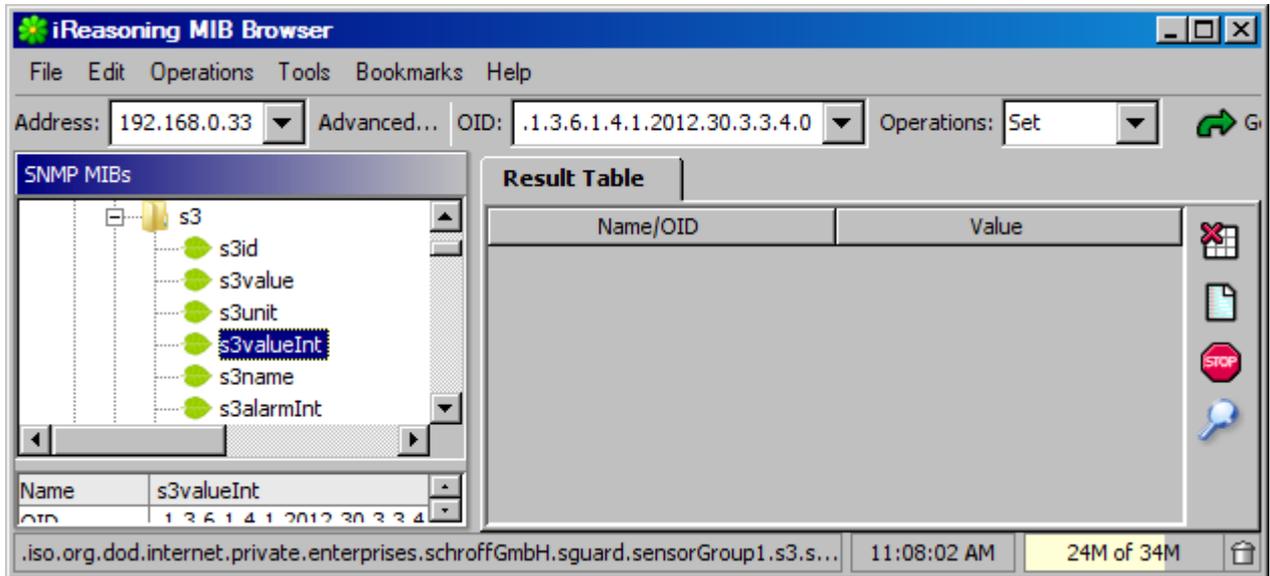
A lock is allocated to s1.
 "s1valueInt" is authorised for read-write.



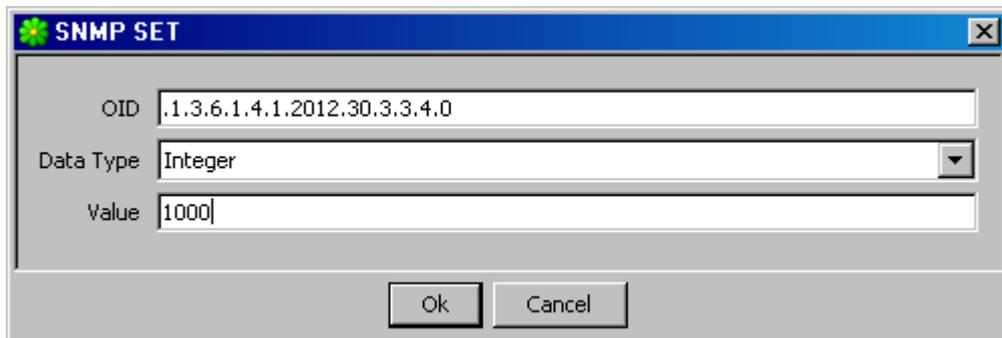
SNMP set is initialised. The value 1000 is entered. Ok -> the lock is opened.



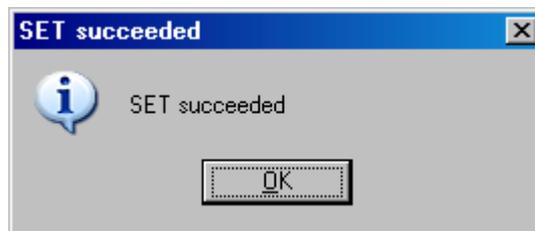
5.1.6.2 Switch digital output

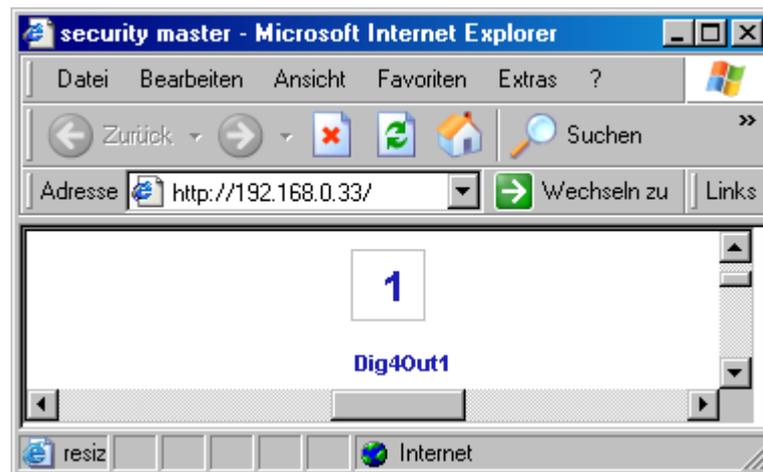


A digital output is allocated to s3.
 "s3valueInt" is authorised for read-write.

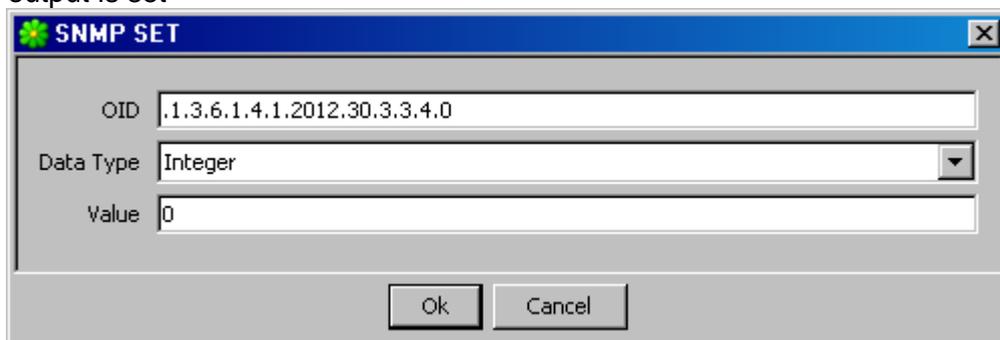


SNMP set is initialised. The value 1000 is entered. Ok -> the digital output is set.

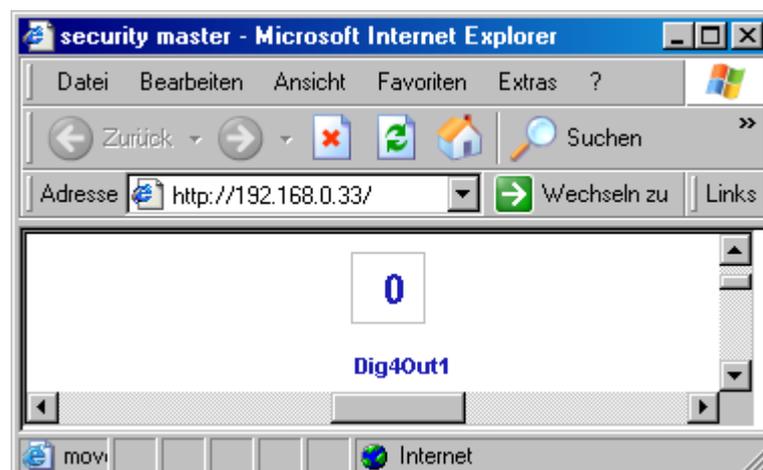
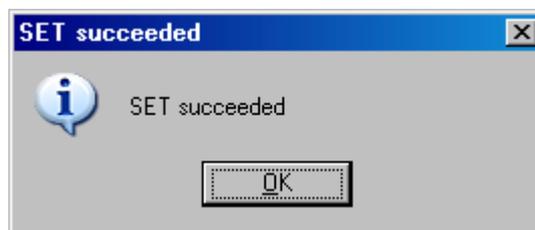




The digital output is set



SNMP set is initialised. The value 0 is entered. Ok -> the digital output is reset.



The digital output is reset again.

5.2 Send e-mail

5.2.1 Entries in the system configuration

SMTP Server:
E-mail sender:

The screenshot shows a window titled "System Konfiguration:" with the following fields:

- IP Adresse: 192.168.0.33
- SNMP community: public
- Netzmaske: 255.255.255.0
- SMTP Server IP: 192.168.0.41
- Gateway: 192.168.0.1
- E-mail Absender: peter@secmaster.com

System entries for e-mail despatch: SMTP server and sender. The IP address of the sending device is automatically attached as a link to every sent e-mail. After receiving the e-mail it is thus possible to communicate directly to the corresponding device using this link.

5.2.2 Entries in the alarm configuration

E-mail recipient:

The screenshot shows a window titled "Konfiguration für Alarme:" with the following configuration:

- Alarm Name: ALARM Netzspannung
- Trap: (empty)
- Typ: 0
- Email: peter@elektrik.de

Buttons for "neu" and "löschen" are present for each configuration row.

If "power supply voltage ALARM " is triggered, the recipient peter@elektrik.de receives an e-mail of notification.

The screenshot shows a field labeled "Meldung bei Alarm:" containing the text: "Unterspannung L1, Bismarckstrasse 19, 2. Etage, Raum 21, Schrank 4"

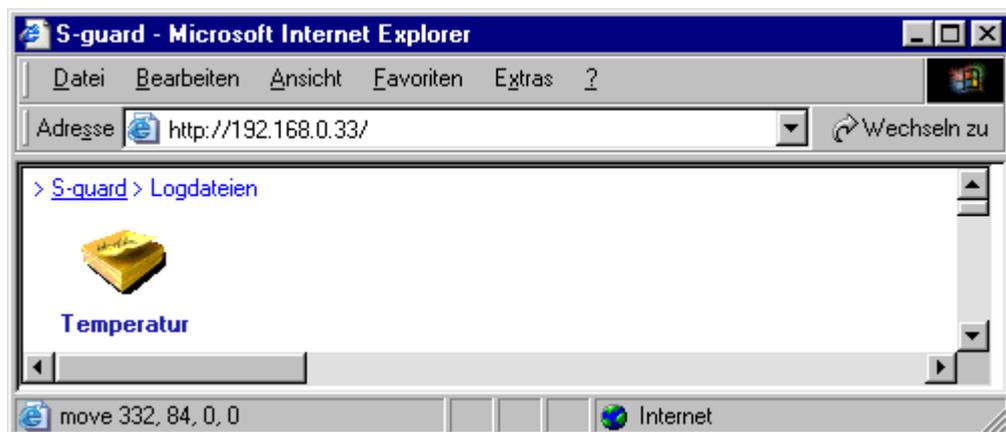
5.3 Log files

Log files are generated in order to record alarm and warning alerts. The “Alarm definition” function is used to define whether alerts are saved in the log file. In this example, alarm and warning alerts are to be saved in the “temperature” log file.



Left mouse button -> Tables

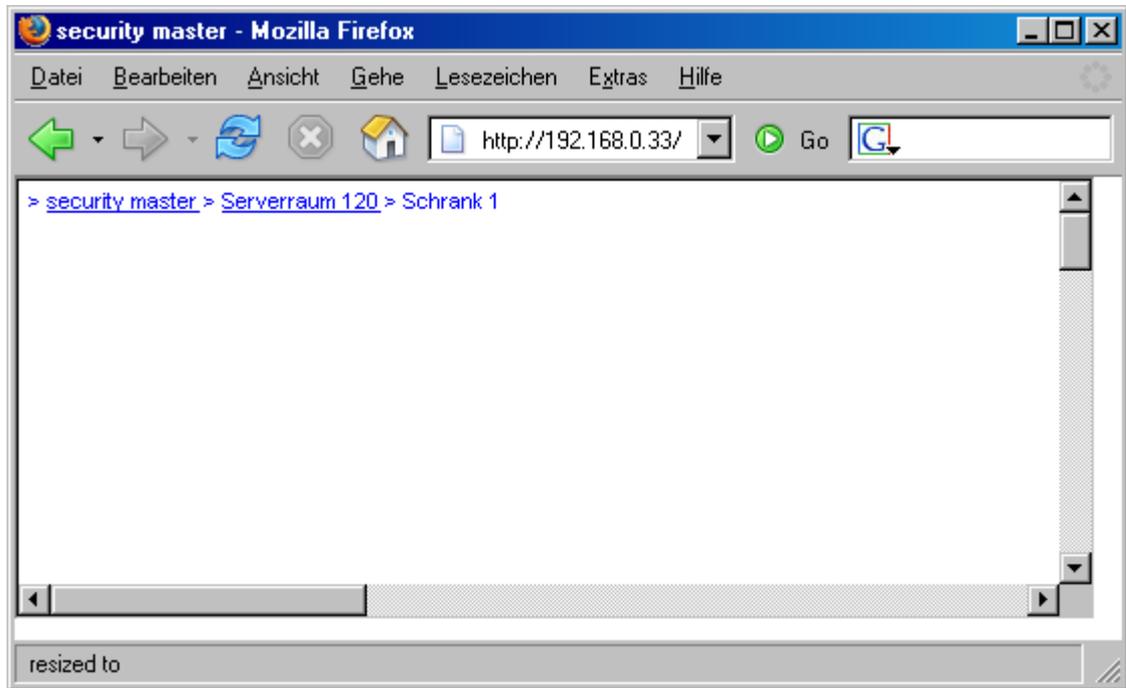
Select the log file with the mouse -> right mouse button -> copy



Paste and rename the log file with the mouse.

Log files can be defined using the “alarm definition” function. Here one of the names defined is entered: in this case, “temperature”.

6 Setup data cupboard



First you should plan the display structure and define the structure of the subdirectory.

Please remember to create backup copies of the configuration and any further changes, so that any changes can be traced easily and reversed if need be. For this you should use the program "S-guard backup" on the enclosed CD.

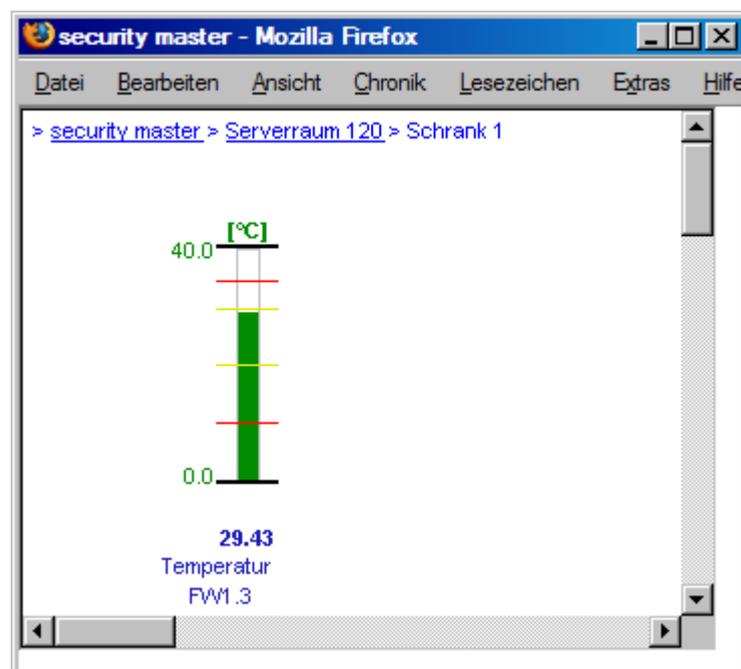
6.1 Add sensors



Menu item "inputs" is selected



Highlight sensor -> right mouse button -> copy



The sensor has been added and can be positioned.

6.2 Parameterise analogue input

Highlight sensor with the mouse -> right mouse button ->-Properties

The sensor has 5 fields of operation, which can be freely defined within the operational limits of the sensor using 4 parameters. A hysteresis can also be displayed

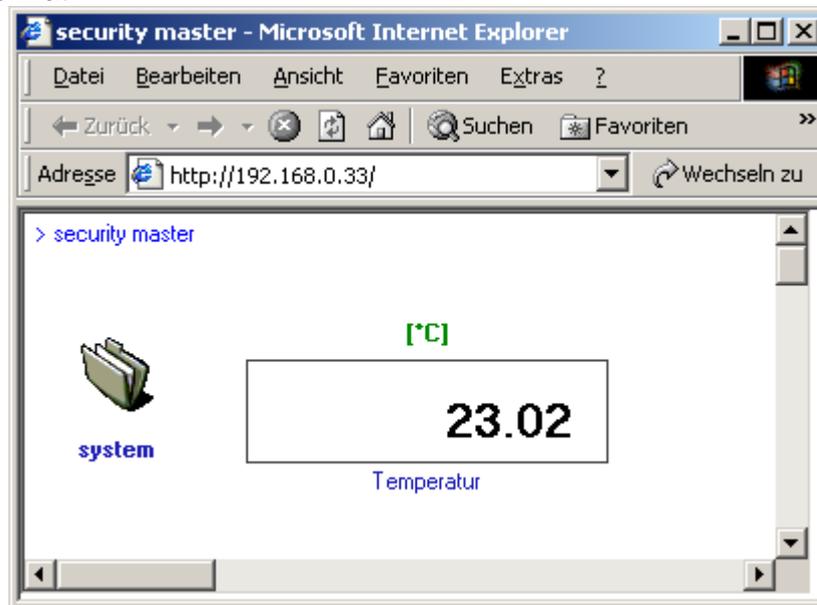
upper alarm limit	35°C
upper warning limit	30°C
lower warning limit	10°C
lower alarm limit	5°C
Hysteresis	0.1°C

Alarm alerts can be activated for the individual fields as required (the alarms are defined in the alarm directory and can be copied to here).

At the same time the display range can also be shown: in this case 0°C (lower limit) to 40°C (upper limit).

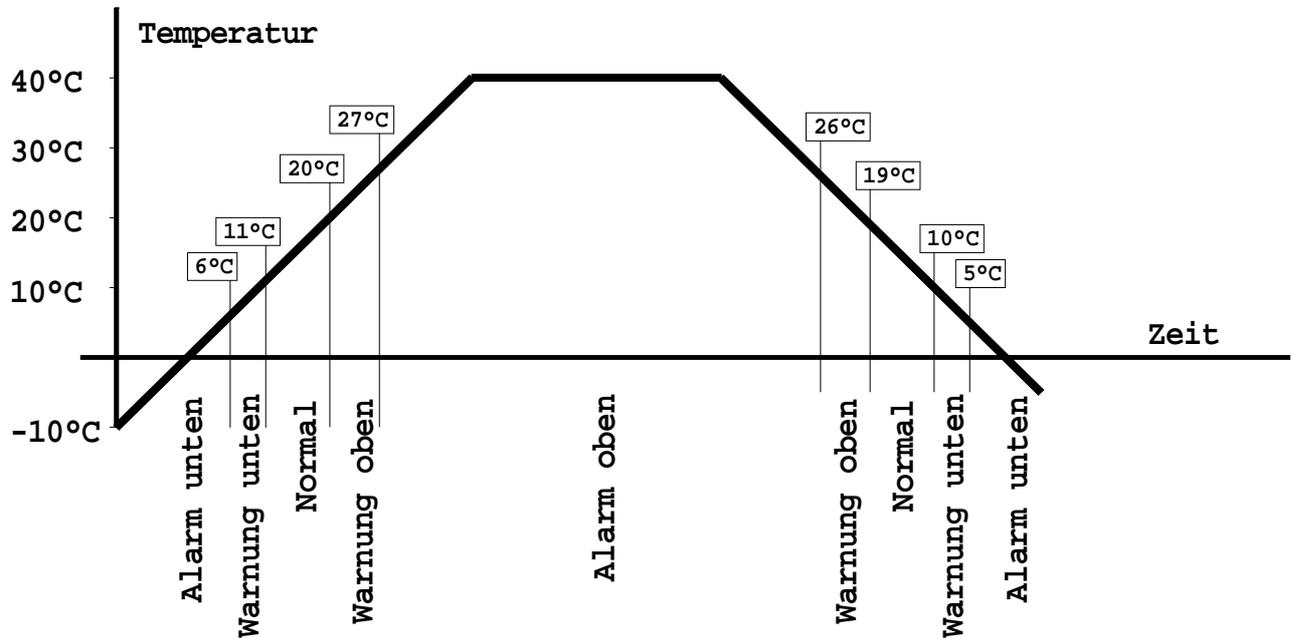
Now the alarm alert can be defined which is to be generated by this sensor: “temperature 01, room 120, data cupboard 01”. This alert will always be displayed or sent when this sensor generates an alarm signal or alert.

In this mask the control element „numeric“ can be found. If the box is ticked here the display is shown in digital format.



6.2.1 Hysteresis

The use of a hysteresis is intended to prevent the constant generation of alerts with every small fluctuation within the limit range. An example is used to explain this function.



	limit	Limit exceeded
Lower alarm limit + Hysteresis	$5^{\circ}\text{C} + 1^{\circ}\text{C} = 6^{\circ}\text{C}$	Lower alarm -> lower warning
Lower warning limit + Hysteresis	$10^{\circ}\text{C} + 1^{\circ}\text{C} = 11^{\circ}\text{C}$	lower warning -> Normal
Upper warning limit	$>20^{\circ}\text{C}$	Normal -> upper warning
Upper alarm limit	$>27^{\circ}\text{C}$	upper warning -> upper alarm
Upper alarm limit - Hysteresis	$27^{\circ}\text{C} - 1^{\circ}\text{C} = 26^{\circ}\text{C}$	upper alarm -> upper warning
Upper warning limit - Hysteresis	$20^{\circ}\text{C} - 1^{\circ}\text{C} = 19^{\circ}\text{C}$	upper warning -> Normal
Lower warning limit	$<10^{\circ}\text{C}$	Normal -> lower warning
Lower alarm limit	$<5^{\circ}\text{C}$	lower warning -> Lower alarm

In this way this sensor is configured and ready for operation. If it is now copied into other directories, the configuration data are also copied.

The “copy“ und “paste“ buttons make it possible to copy the configuration of an analogue sensor into another sensor of the same type.

Correspondingly, as depicted here, other analogue transmitters are also connected and configured.

6.3 Parameterise digital input

Alarm geschlossen:	Tuer zu
Alarm offen:	Tuer offen
Anzeige Farbe geschlossen:	<input checked="" type="checkbox"/> grün
Meldung des Alarms:	Raum 102, Schrank 1 vorn
Farbe übergeordneter Ordner:	Rot wenn offen

The colour of the superordinate folder makes it possible to define the signalisation independently of the actual condition.

6.4 Parameterise digital output

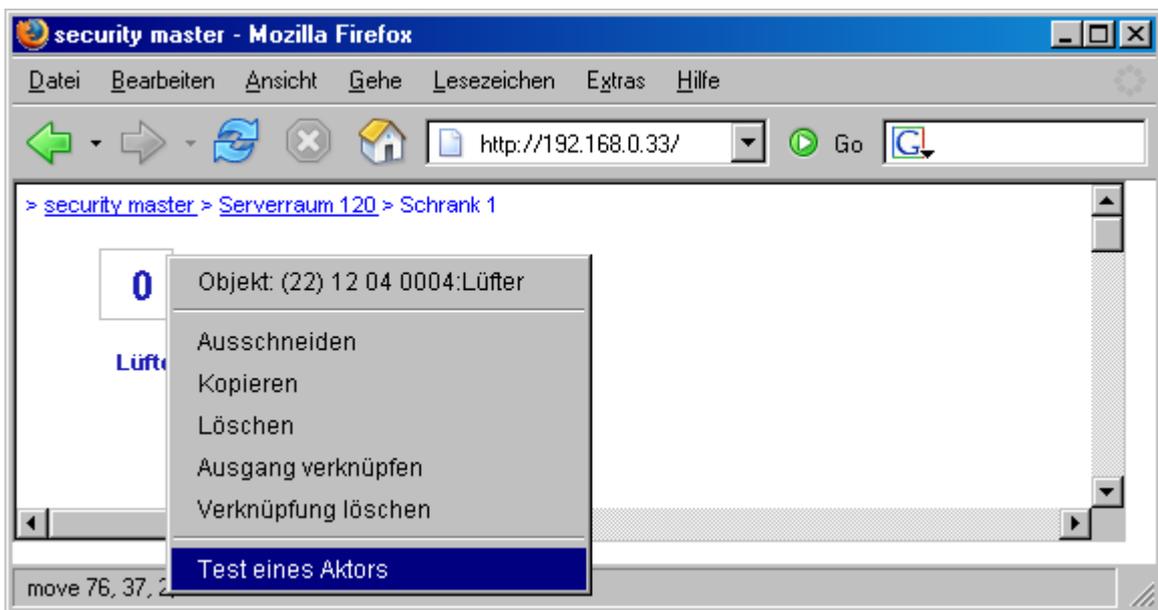
Alarm geschlossen:	Warnung
Alarm offen:	normal
Meldung des Alarms:	RZ1, Schrank 212, Lüfter 2

Here alarms can be selected for both conditions, and "alarm alert" entered.

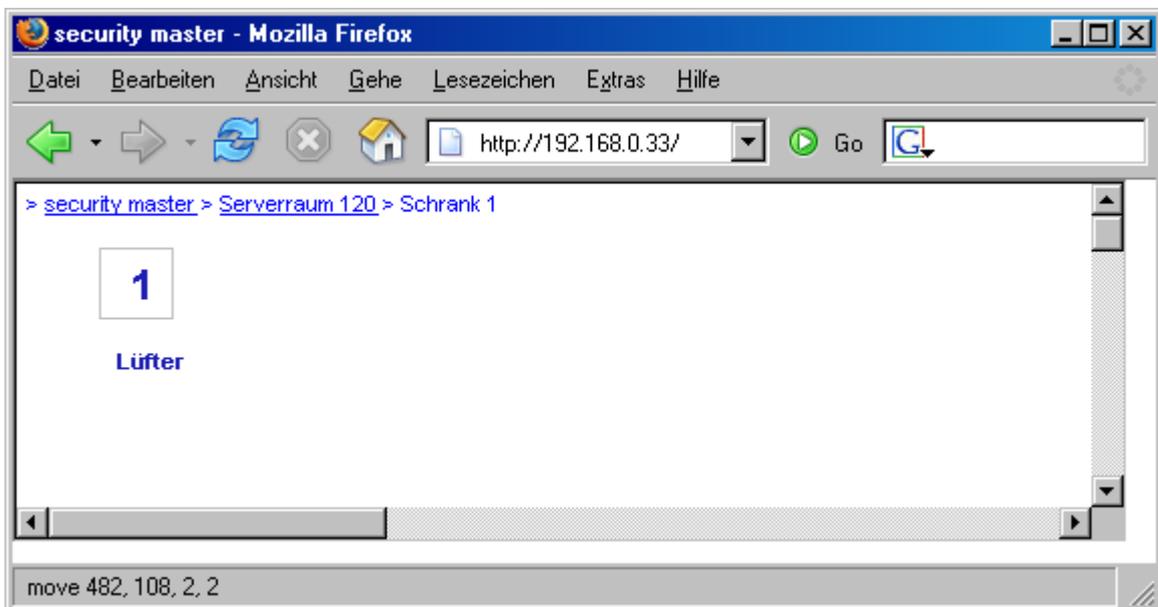
6.4.1 Test digital output

The basic setting is indicated by “0“. When the output module is switched on by a program, “1” appears. Refer to the data sheet of the module in question to see whether it is an opening or locking function.

Correspondingly, as depicted here, other digital outputs are also connected



Test of an actuator

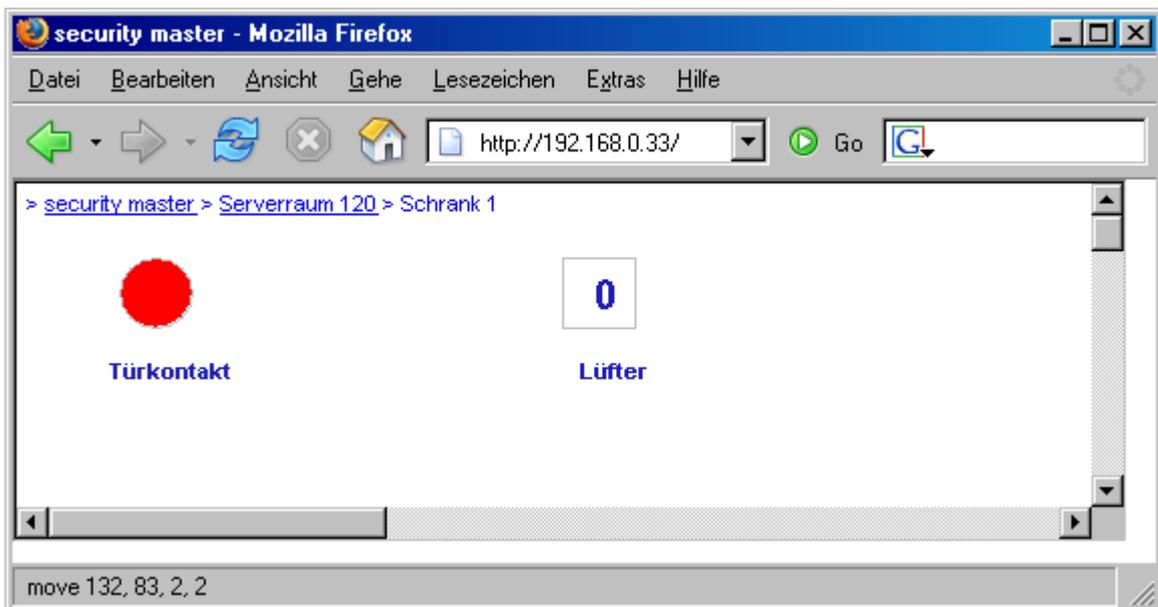


The output changes its condition with each test.

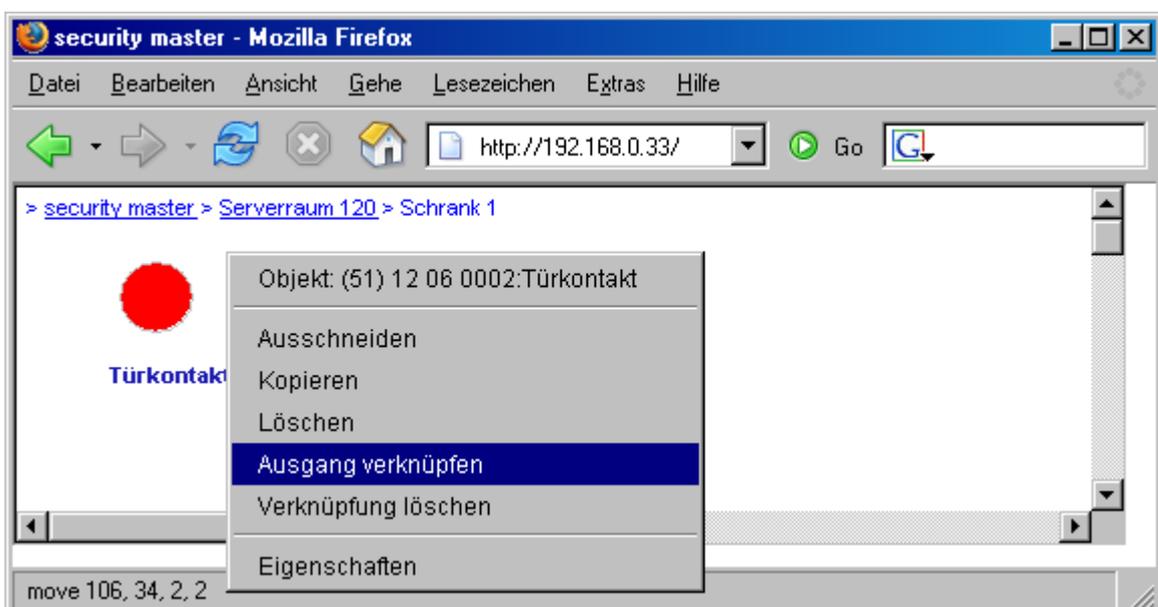
6.5 Shortcuts

6.5.1 Create output shortcut

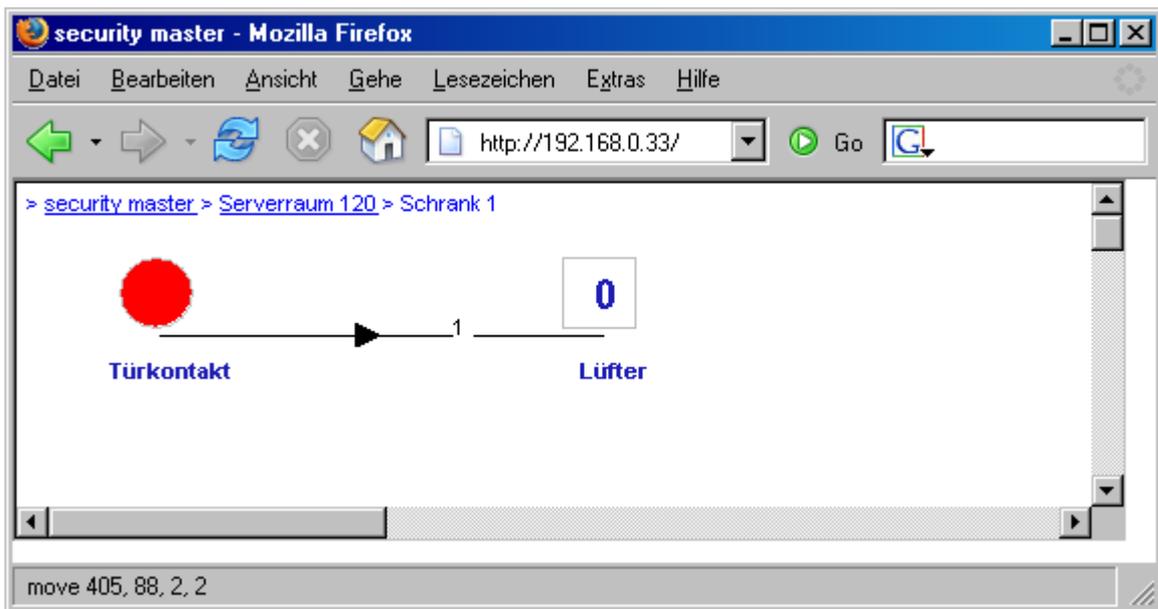
The AC relay adapter (with attached fan) should be connected with the foremost door contact of the data cupboard. The warning lamp should light up when the door is open.



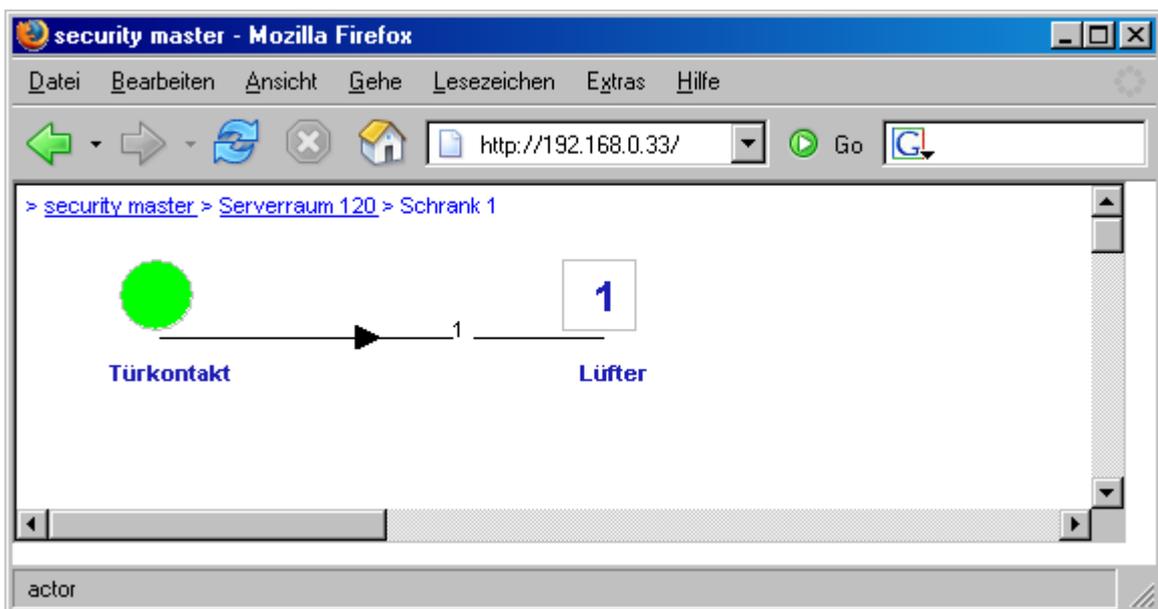
Paste in door contact (door is open)
Position door contact and AC relay adapter



Highlight source object, door contact (door front) with mouse-> Right mouse button ->create output shortcut



Target object: highlight AC relay adapter (fan) with mouse-> left mouse button-> shortcut created.



Door is closed, fan is switched on

6.5.2 Delete shortcut

Source object: ->cursor on door contact-> Right mouse button->"delete shortcut"

Target object: ->cursor on AC relay adapter (fan) ->left mouse button->shortcut is deleted.

6.6 IP camera

Firstly the IP camera is entered in the configuration:

IP Kamera: [] [neu] [löschen]

new

Neuer Eintrag

User@IPAdresse: peter@192.168.0.120

Kennwort: *****

OK

Java Applet Window

IP Kamera: [peter@192.168.0.120] [neu] [löschen]

A maximum of 2 cameras can be entered.

Once the camera has been connected a notification will appear in the “inputs” directory: the picture can be copied on to any desired page.

The camera sends 1 picture per second.

Between the **security master** and the web browser there is a time delay, which means that the pictures in the **security master** are more up to date than those in the browser window.

Once the browser window with picture display is closed, the picture transmission from **security master** to the browser will be interrupted after around 100 seconds.

When the browser window with picture display is reopened, picture transmission will resume after a delay of around 20 seconds.

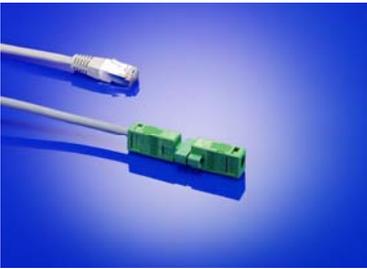
The cameras have the following factory settings:

Video Resolution	320x240
Compression Rate	Medium
Frame Rate	1

These settings may not be changed!

7 Peripherals

7.1 Analogue input module 0...10VDC [002-0109]



The analogue input module can be used to measure potential-free voltages in the range 0...10VDC.

7.2 Movement detector [002-0117]



The movement detector can control the storage of pictures in conjunction with the IP camera.

7.3 Movement detector 360° [002-0192]



The movement detector can control the storage of pictures in conjunction with the IP camera.

7.4 Digital output module 4 way [002-0107]



The 4 way digital output module has 4 potential-free relay outputs. The power rating is 24V DC, 100mA per contact.

7.5 Digital output module 8 way [002-0260]



The 8 way digital output module has 8 potential-free relay outputs. The power rating is 24V DC, 100mA per contact.

7.6 Digital input module 4 way [002-0108]



The digital input module has 4 digital inputs. Only potential-free contacts may be connected.

7.7 Digital input module 8 way [002-0250]



The digital input module has 8 digital inputs. Only potential-free contacts may be connected

7.8 Pressure sensor 0...10 bar [002-0195]



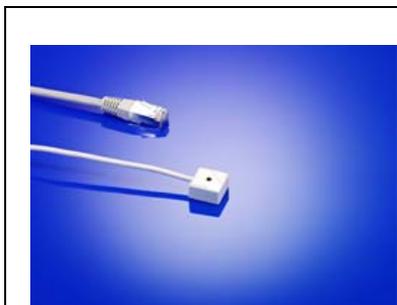
Analogue pressure display.
Pressure connector via 1/4" external thread

7.9 Shock sensor [002-0116]



The shock sensor serves to monitor shock effects caused by vandalism.

7.10 Glass breakage sensor [002-0118]



The glass breakage sensor is glued on to the glass surface to be monitored and notifies of glass breakage.

7.11 IP camera [002-0140]



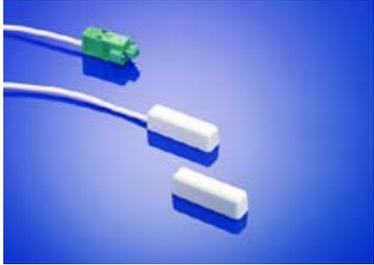
As soon as an IP address is given the cameras are interrogated.
The sample rate is approx. 1 picture per second.
The last 6 photos of each camera are buffered.

7.12 Combined sensor [002-0103]



- 1 Pc. Temperature sensor
- 1 Pc. Humidity sensor
- 1 Pc. Shock sensor
- 1 Pc. Smoke detector
- 2 Pcs. Digital inputs for door contacts [002-0119]
- 2 Pcs. Digital inputs for the connection of potential-free contacts

7.13 Door contact for combined sensor [002-0119]

	<p>These door contacts are designed for connection to the combined sensor [002-0103]</p>
---	--

7.14 Combined distributor [002-0127]

	<p>The combined distributor 002-0127 contains:</p> <ul style="list-style-type: none"> Input for a digital temperature/humidity sensor (002-0128) 2 inputs for door contacts 2 inputs for further potential-free contacts 4 way peripherals bus
--	--

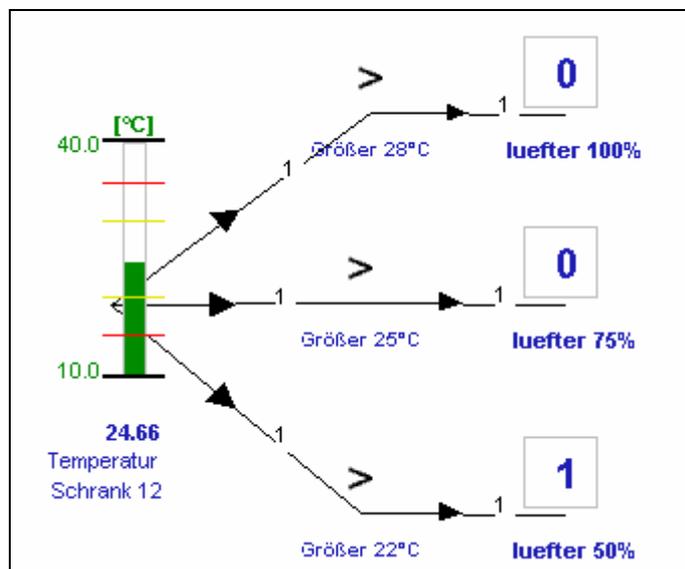
7.15 Leakage sensor [002-0180]

	<p>Leakage sensor for use with air, water, and cooling devices. To be fitted with the optics facing down at the lowest point, the collection point for escaped coolant fluid.</p>
---	---

7.16 Fan with control system [002-0150]



DC fans with a power consumption of 7.2 watts are designated.
 The maximum air throughput is approx. 200m³/h per fan.
 The fans operate at 4 switching levels:
 OFF, approx. 50% capacity, approx. 75% capacity, 100% capacity.



In this example, the fan switches up to the next capacity level when temperatures of 22°C, 25°C, and 28°C respectively are exceeded. The temperatures can be freely set.

7.17 Fan with revolution logging [002-0151]



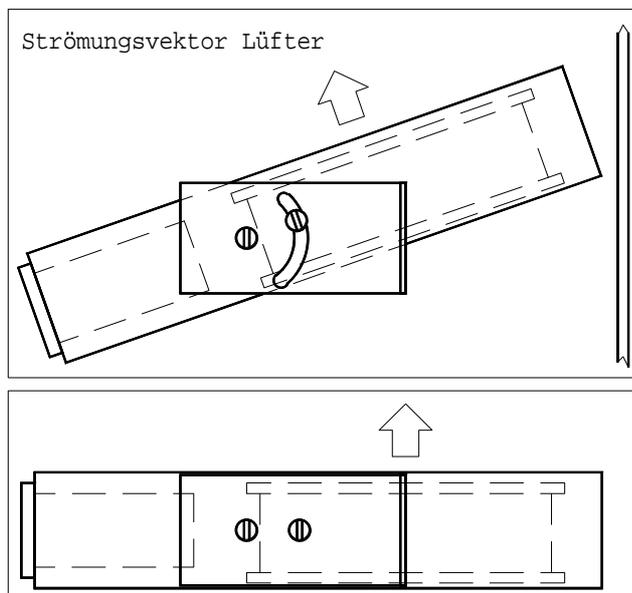
Plug-in fan module (1HE, 84TE), variable mounting angle and depth grid for optimal positioning of the fan.
 The revolution warning and alarm limits can be set separately for each fan.

7.18 High-performance fan [002-0152]

	<p>The high-performance fan has an on/off switching function and can be activated or deactivated using any desired logic operation. It can be switched using the AC relay adapter (002-0106)</p>
---	--

7.18.1 Fitting the fan module

The fan fixings are so designed as to allow for optimal positioning of the fans.



7.19 Supply voltage measuring adapter [002-0104]

	<p>The mains supply voltage measuring adapter is designed to be used to monitor the 230 V AC grid. It supplies readings which are to a large extent independent of temperature. The voltage to be measured is hooked up by means of a power cable with an IEC power connector.</p>
---	--

7.20 Supply voltage measuring adapter 3 Phase [002-0124]

<p>A black rectangular device with a white label on top. The label includes the 'pm+v' logo, technical specifications like 'Input 100-240VAC', and three labeled input ports (Input 1, Input 2, Input 3). A yellow warning label is also present. A blue cable is plugged into one of the ports.</p>	<p>The measuring adapter has 3 IEC power adapters for the connection of the voltage to be measured. The 3 phases are displayed individually and can be configured individually. The corresponding alarms are defined in "Alarm configuration"</p>
--	---

7.21 Supply current monitor [002-0173]

<p>A black rectangular device with a blue cylindrical component attached to its side. A blue cable is connected to the device. The device is mounted on a metal base.</p>	<p>The device has a calibrated AC current meter which may be used for consumption calculation purposes. The supply current is also measured inside the device. The measuring range is 50 A, the resolution 10 Bit. The smallest displayable change is therefore 0.05 A.</p>
---	---

7.22 Peripheral bus distributor 8+2 [002-0111]

<p>A blue rectangular device with a white label on top. The label has some text and a logo. The device has several ports on its side.</p>	<p>The peripheral bus distributor serves to connect a maximum of 9 sensors and actuators to a security master data bus.</p>
---	--

7.23 Smoke detector [002-0105]



Optical smoke detector to be connected to the **security master**.

7.24 Relay adapter AC [002-0106]



The relay adapter is used to switch fans, lamps etc. It has a switching capacity of 230 V AC, 2 A, with a semi-conductor relay, and switches in 0-point.

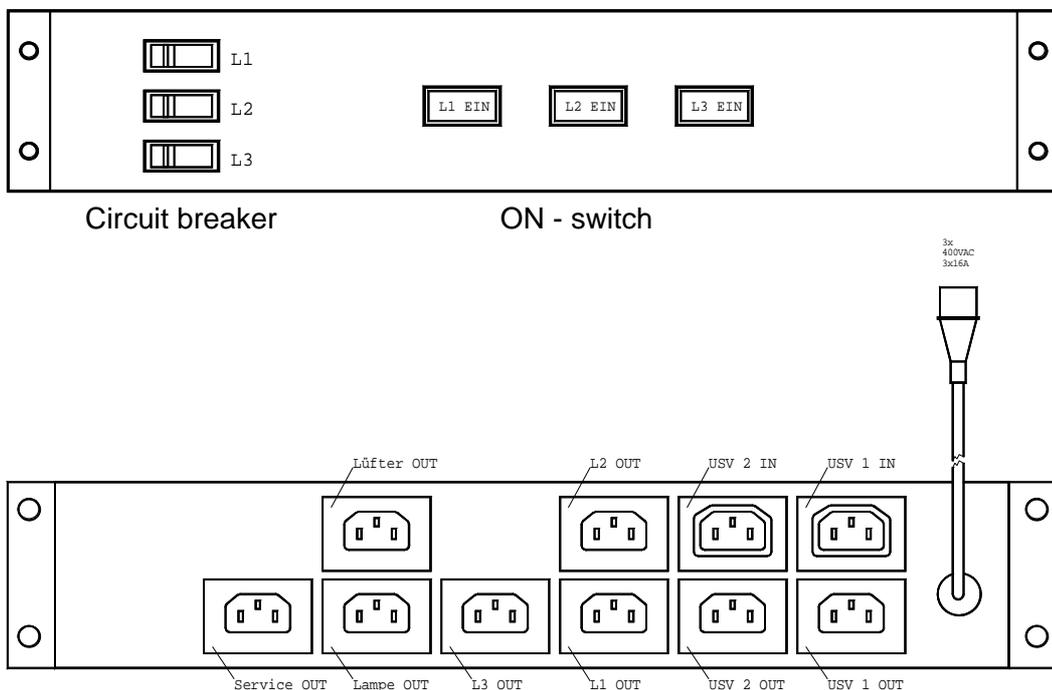
7.25 Oxygen sensor [002-0129]



The oxygen sensor's function is based on a galvanic cell. It is suitable for the qualitative monitoring of CO₂ and N₂ fire extinguishing installations.

7.26 **Switch box 16A [002-0170]**

	<p>19" current controlling and monitoring system 2HE. 3 phase 10A automatic cut-out (manually operated) Manual ON / OFF, (ON using switch, OFF via circuit breaker) Switch-off function also via security master cupboard control system. Individual phase voltage measuring. Auxiliary contact monitoring of the circuit breaker</p>
---	---



7.27 **Switch box 32A [002-0171]**

	<p>Housing 84TE, 3HE Function: 4 circuit breakers (mechanical coupling) at 10A per phase Switched on manually for each phase using manual switch at the front. Switched off manually for each phase using circuit breaker or remotely via security master. Power supply voltage measurement per phase Circuit breaker monitoring via auxiliary contacts</p>
---	--

7.28 **Swing-arm Locking system**

7.28.1 **Locking system with keypad [002-0132, 002-01132]**

	<p>The keypad is used to enter the door-opening code. Monitoring and control functions are carried out using the <i>security master</i>.</p>
---	---

7.28.2 **Locking system with transponder reader [002-0133, 002-01133]**

	<p>The transponder cards for door opening are read using the transponder reader. Monitoring and control functions are carried out using the <i>security master</i>.</p>
--	--

7.28.3 **Locking system without ID module [002-0134, 002-01134]**

	<p>This lock does not come equipped with its own data entry module. It can be operated as a slave lock or remotely, either manually or by means of a management system.</p>
---	---

7.28.4 Keypad module [002-0130]



Any desired connection e.g. cupboard opening can be implemented according to the four-eyes principle.

7.28.5 Transponder reader module [002-0131]



The transponder cards for door opening are read using the transponder reader.

7.28.6 Transponder cards [002-0858]



The transponder cards are keyed to the transponder reader module of this locking system. The cards are securely encrypted with a unique 40 Bit code.

7.28.7 General

Swing-arm locks are fitted with large condensers big enough to provide the impulse necessary to open the doors. These condensers require a starting current to perform the switching action. Therefore the number of locks which can be connected to one **security master** is limited.

7.28.8 Security

In order to ensure that access to the cupboards is still possible even should the **security master** fail, the installation should be so carried out as to allow access to the device by authorised personnel even if it fails. It may prove worthwhile to lay the cables for the peripherals bus which controls the lock of the **security master**, so that a replacement device can be connected there.

This replacement device could first quickly be configured using a backup copy of the appropriate configuration data.

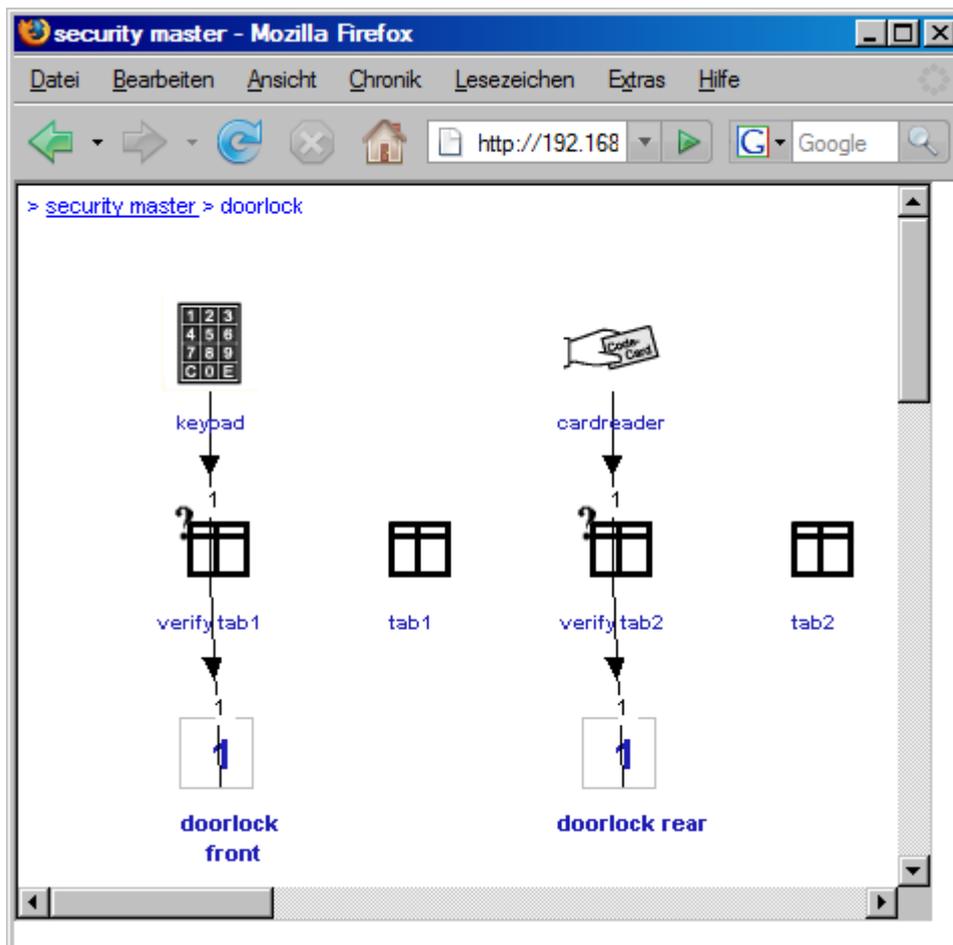
Should the door lock electronics fail due to a defect or sabotage then the cupboard will have to be forced open.

7.29 Application

The locking system using swing-arm handle is designed for use with the “Comrack“ and “Varistar“ data cupboards made by the Schroff company.

After opening the swing arm pivots upwards and the doors can then be manually unlocked. This procedure has the double advantage that it can be seen at a glance whether the door is unlocked and that ventilation continues even if the door is accidentally opened.

7.29.1 Configuration of locking system with swing-arm handle



If the code entered or the card code is stored in “tab1“ or “tab2“, the corresponding lock is opened.

7.30 Locking system with magnetic locking



Locking system with 2 permanent magnets with 420 N retention force each. These magnets can be switched off electrically.

7.31 Door locking system with magnetic clamps

Door locking systems using magnetic clamps may be used in all commonly available data cupboards, irrespective of manufacturer, as well as in rooms. The retention force of the magnets depends on their use and must be decided during the project planning phase. For data cupboards, it is standard practice to use 2 magnetic clamps with a retention force of 420 N each. However, almost any other retention force could be used instead.

There are two basic equipment models:

- 1.) Locking system with permanent magnet. If the power fails the doors are locked. To open the doors, power supply to the magnet is resumed and the retention force thus nullified. These locking systems can of course only be used in data cupboards.
- 2.) Electromagnetic locking system. If the power fails the doors are opened. The doors remain locked as long as the electromagnet is supplied with power.

Locking systems with magnetic clamps can also be opened using different functions:

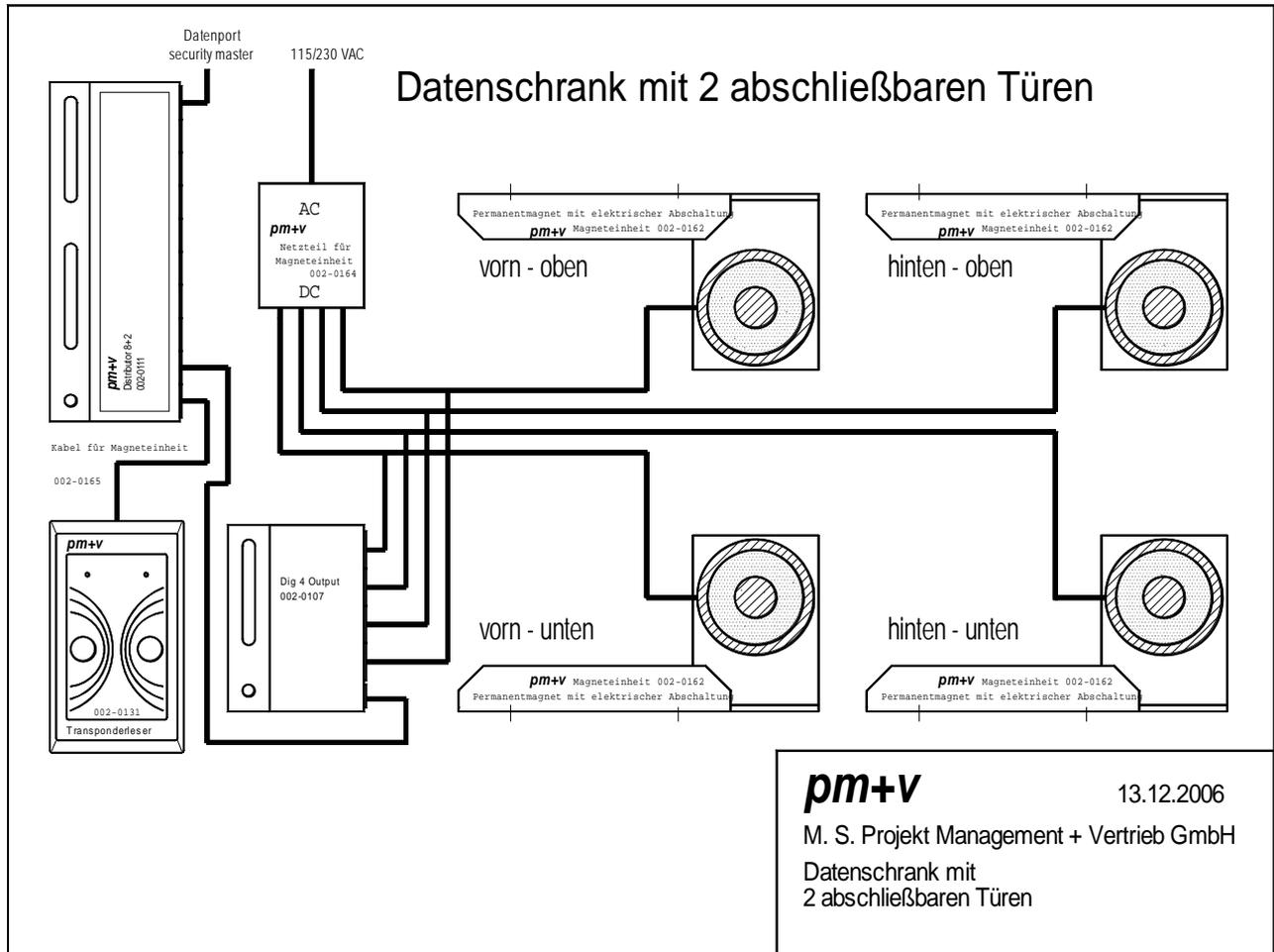
- By means of keypad code entry;
- By means of a transponder card reader;
- By means of **security master's** online function;
- By means of SNMP Set function.

7.31.1 Example

Magnetic retention systems with permanent magnets are used. 2 magnetic clamps with a retention force of 420 N (42 Kp) each are fitted to each door, one on the lower and one on the upper edge. To open the doors the magnets are supplied with power for approx. 20 seconds. For this time they lose their retention force and the doors can be opened.

Access is controlled using either transponder cards or a keypad. The front and the back of each data cupboard are fitted with either a card reader or a keypad. If an authorised transponder card is placed on the transponder reader or a correct code entered, the door is cleared to open for approx. 20 seconds. Once this period elapses the doors are automatically locked again, and the card must be replaced on the reader or the code re-entered.

7.31.1.1 Locking system with magnetic clamp and transponder reader



Two magnetic clamps per door are fitted (one at the top and one at the bottom)

7.32 Door locking system with magnetic clamps and automatic opening

Locking systems with electromagnets are used, which open the doors when the power fails. Thus there is no need for auxiliary power sources. The system is simple and reliable.

Link-ups in the security master can be used to release the door locks:

- Temperature limit exceeded
- Fan failure
- Pressure reduction in cooling ducts
- etc.

Link-ups can be created to ensure that several different alerts are necessary for this function to work.

The full range of the **security master's** alarm functions is of course also available at the same time;

- E-mails

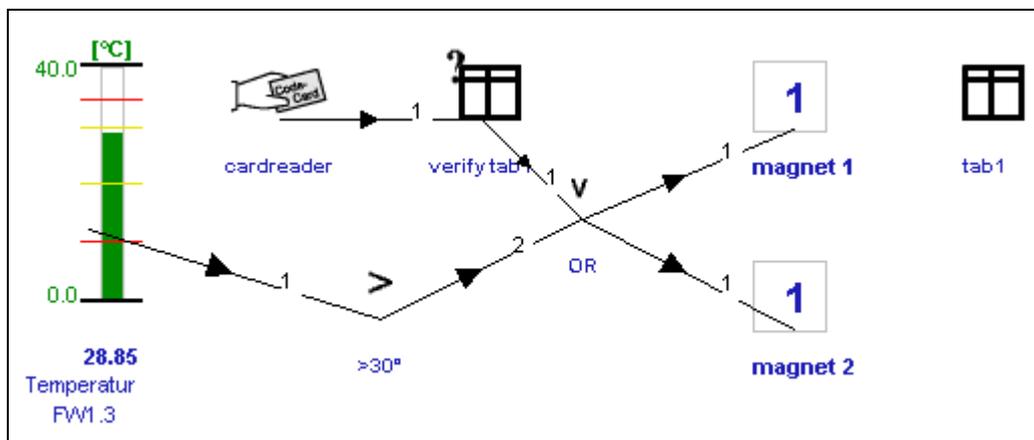
- SNMP traps
- **security master** alarm page
- Optical alarming
- Acoustic alarming

The actual opening of the doors is performed by gas-pressure struts, if necessary multiple-stage. A small, strong impetus may be necessary for the initial opening. The principal opening motion requires less pressure because the doors are very smooth-running and require very little accelerative thrust.

In case of emergency the doors can easily be pushed out of the way. They do not present a physical obstacle.

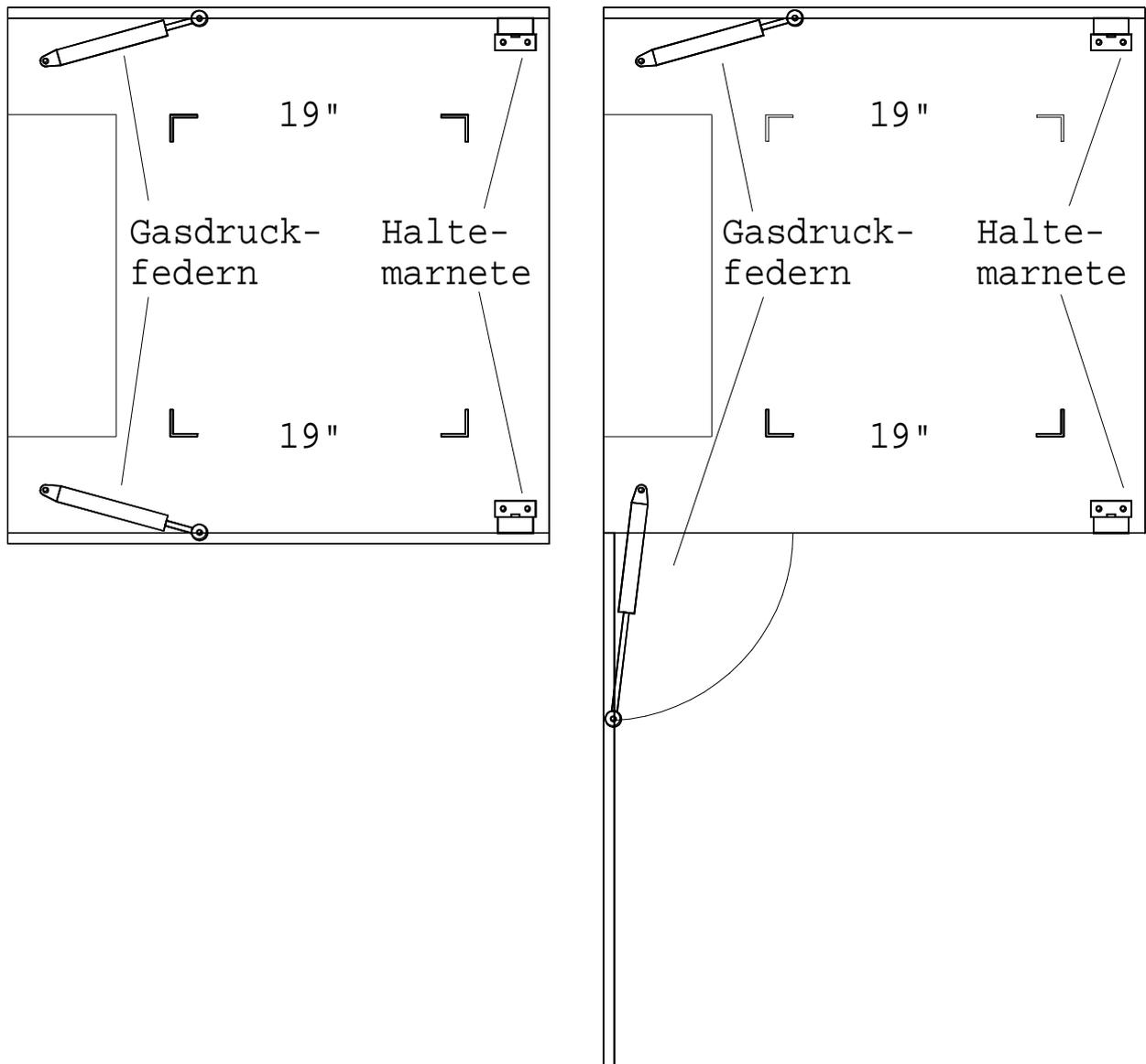
To close the doors after automatic opening the automatic functions are reactivated via the **security master** and the doors pushed on to the magnets, which are already under power. So that there is no risk of injury, the magnets' retention force only comes into play when the gap between magnet and strike plate is approx. 5 mm.

7.32.1 Configuration magnetic locking system



In this example the power to the magnets is cut when the temperature exceeds 30°C or when a valid transponder card is placed on the reader.

7.32.2 Universal Application



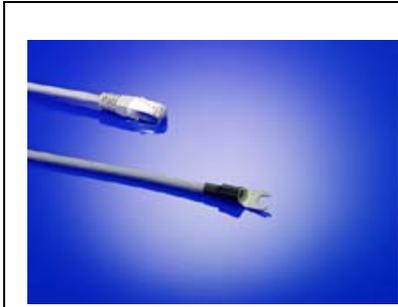
When the automatic door opening function is triggered the doors open to an angle of 90° to guarantee optimum ventilation, also for the neighbouring cupboards.

The doors can be moved by hand.

Depending on the application, one or more gas pressure struts can be fitted to each door. The struts can be so positioned as not to get in the way.

The retention force of the magnets also depends on the application in question.

7.33 Temperature sensor [002-0100]



Analogue Sensor with PT1000 Measuring element.

7.34 Temperature sensor [002-0101]



Analogue Sensor with PT1000 Measuring element.

7.35 Temperature sensor [002-0200]



The temperature sensor 002-0200 contains a digital temperature sensor. The resolution is 0.5°C. Configuration is as with sensors 002-0100 and 002-0101. The temperature sensor 002-0200 replaces the sensor 002-0101.

7.36 Temperature and humidity sensor [002-0123]



This sensor contains a temperature sensor PT1000 and a humidity sensor. Planned measurement ranges are 0...40°C for the temperature sensor and 30...90% relative humidity for the humidity sensor.

7.37 Temperature and humidity sensor [002-0203]



This sensor contains a temperature sensor and a digital humidity sensor. Planned measurement ranges are 0...40°C for the temperature sensor and 30...90% relative humidity for the humidity sensor.

7.37.1 Consumption monitor 16A uncalibrated [002-0181]



The device has an AC current meter which can be used for monitoring purposes. Mains supply voltage and current are also measured in the device. Measurement range for voltage measurement is approx. 300 V AC. The measuring range for current measurement is 25 A, the resolution 10 Bits. The smallest displayable change is therefore 0.03 A.

7.38 Consumption monitor 16A calibrated [002-0182]



The device has a calibrated AC current meter which may be used for consumption calculation purposes. Mains supply voltage and current are also measured inside the device.
 The measuring range for mains supply voltage is approx. 300 V AC.
 The measuring range for mains supply current is 25 A, the resolution 10 Bit. The smallest displayable change is therefore 0.03 A.

7.39 Consumption monitor 32A uncalibrated [002-0183]



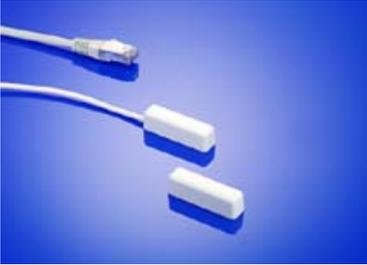
The device has an AC current meter which can be used for monitoring purposes. Mains supply voltage and current are also measured in the device.
 Measurement range for voltage measurement is approx. 300 V AC.
 The measuring range for current measurement is 50 A, the resolution 10 Bits. The smallest displayable change is therefore 0.05 A.

7.40 Consumption monitor 32A calibrated [002-0184]



The device has an AC current meter which can be used for consumption calculation purposes. Mains supply voltage and current are also measured in the device.
 Measurement range for voltage measurement is approx. 300 V AC.
 The measuring range for current measurement is 50 A, the resolution 10 Bits. The smallest displayable change is therefore 0.05 A.

7.41 Access sensor (door contact) [002-0112]

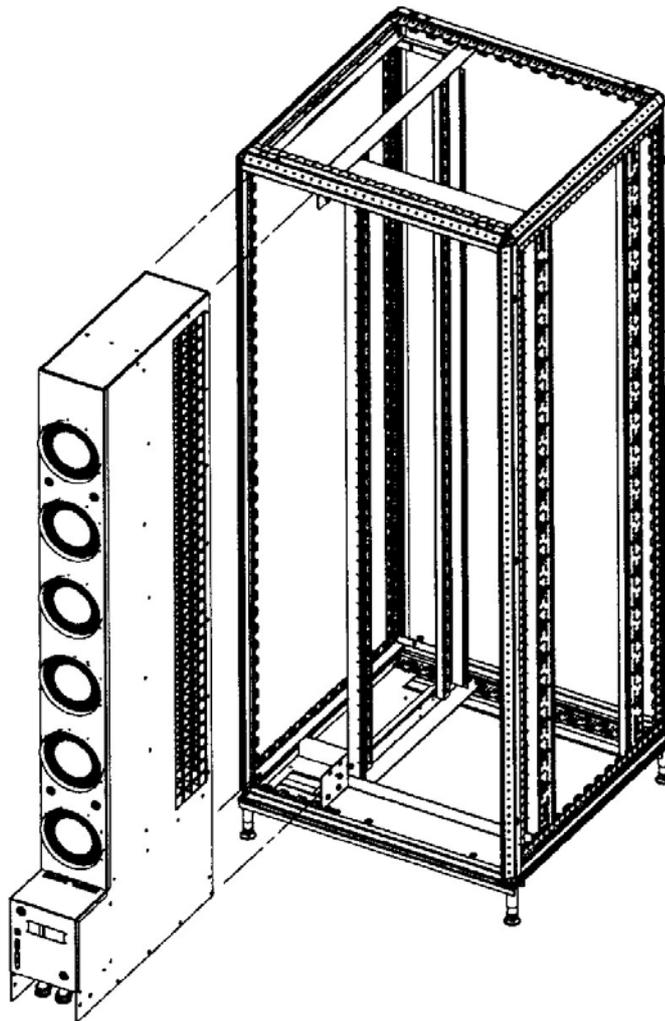


The access sensor can be fitted to data cupboards, room doors, windows etc. to monitor opening. After appropriate calibration, selected alarms will be triggered.

8 Special monitoring applications

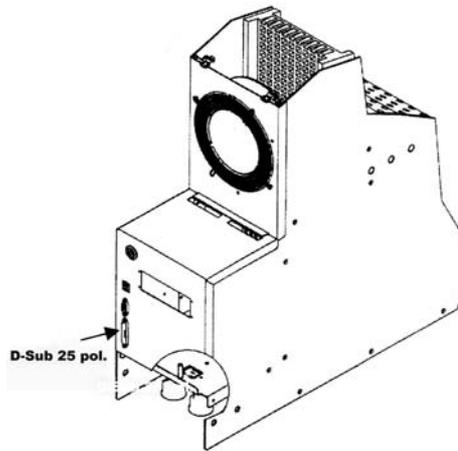
8.1 Cooling device LHX20

The LHX20's electronic control system offers different interfaces. The digital interface (D-sub 25 pin female) and the RS232 interface (D-sub 9 pin female) can both be used for communication with the *security master*



8.1.1 Digital Interface

The LHX20 offers digital inputs and outputs. Signals are routed via a 25 pin D-sub female connector, which is on the front of the controlling device below the display.



8.1.2 Signal Interfaces

The following inputs are available to the **security master**:

Input	Signal	Pin	Pin
E11	Remote control ON-OFF	10	22
E12	Emergency cooling	11	24
E13	Reserve	13	25

The following input is operated as standard by the **security master**:

Input	Signal	Pin	Pin
E12	Emergency cooling	11	24

The following outputs are available to the **security master**:

output	Signal	Pin	Pin
K4	Voltage monitoring	1	14
K5	Temperature limit value air outlet	2	15
K6	Temperature limit value water inlet	3	16
K7	Fan rotation speed	4	17
K8	Master alarm	5	18

Important

If the cupboard is equipped with automatic door opening, the following outputs can be monitored:

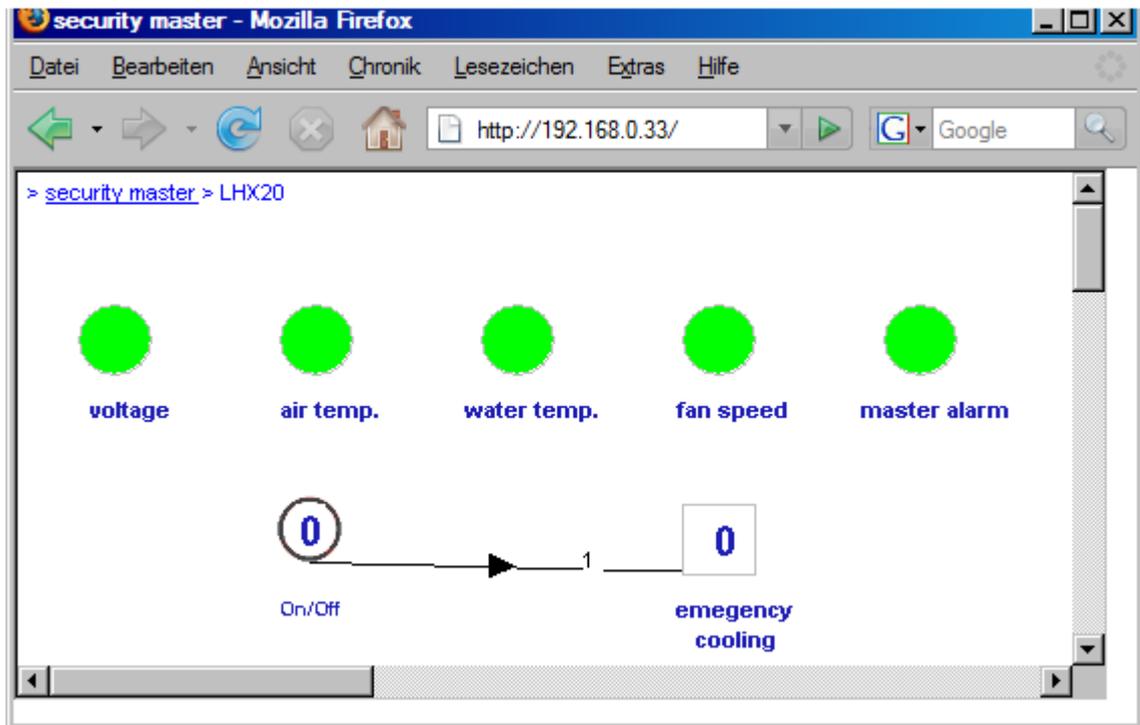
Output	Signal	Pin	Pin
K5	Temperature limit value air outlet	2	15
K7	Fan rotation speed	4	17
K8	Master alarm	5	18

8.1.3 Connection to the security master

The LHX 20 is connected by means of the LHX 20 digital interface, order number 002-0255. The associated LHX 20 digital interface cable has the order number 002-0280.

8.1.4 Configuration

Once the LHX20 is connected to the **security master** the following screens can be called up:

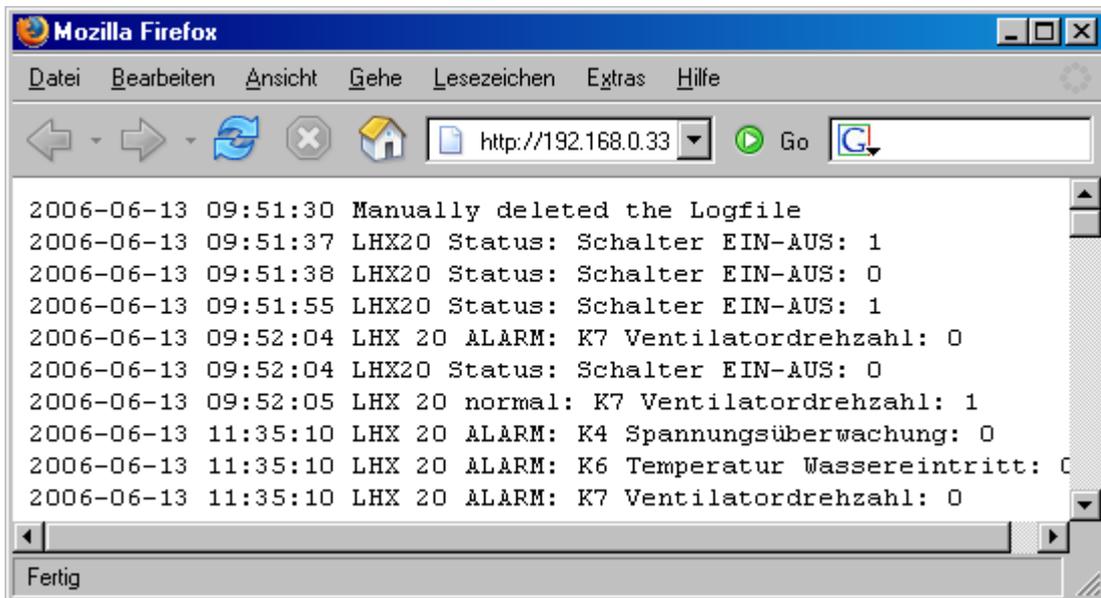


The LHX20 is connected.

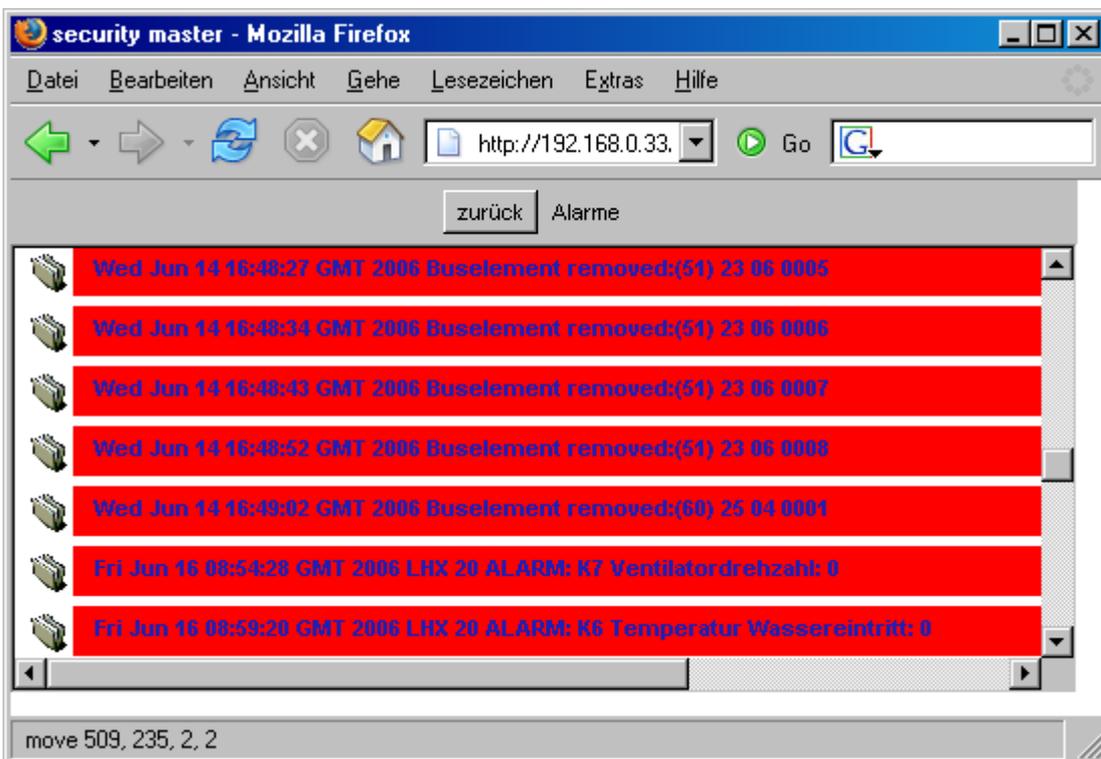
The “emergency cooling” input can be activated by switch or mouse click.

8.1.5 Log Files

The accumulated protocol data can be stored in a log file:



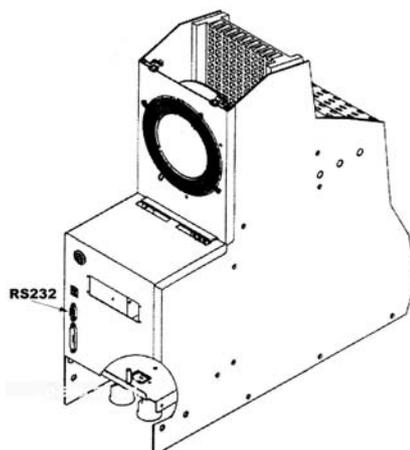
In addition, alarm records can be stored on the *security master's* alarm page:



8.1.6 RS232 Interface

Data are transferred between the security master and the LHX 20 using the RS232 interface. The signals are routed via a 9 pin D-sub female connector, which is on the front of the device below the display.

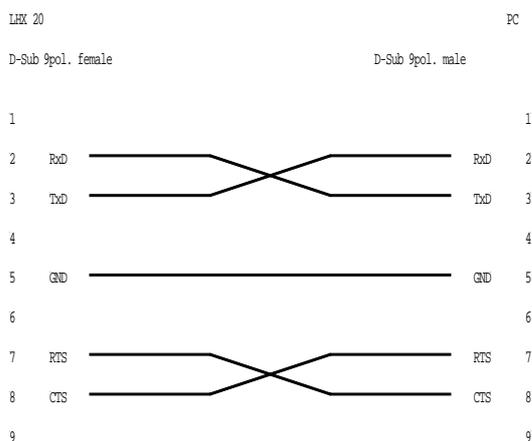
This interface makes available various data which can be read out.



8.1.6.1 Interface Parameters

57,600	Baud
8	Data bits
No	Parity
1	Stop bit

8.1.6.2 Data cable



8.1.7 RS232 Communication

Communication via RS232 can take place both with the „**security master**“ (001-0100) and with the „**security master** small size – LHX20“ (001-0102).

For data traffic between the LHX20 controller and the security master to be possible the following conditions must be fulfilled:

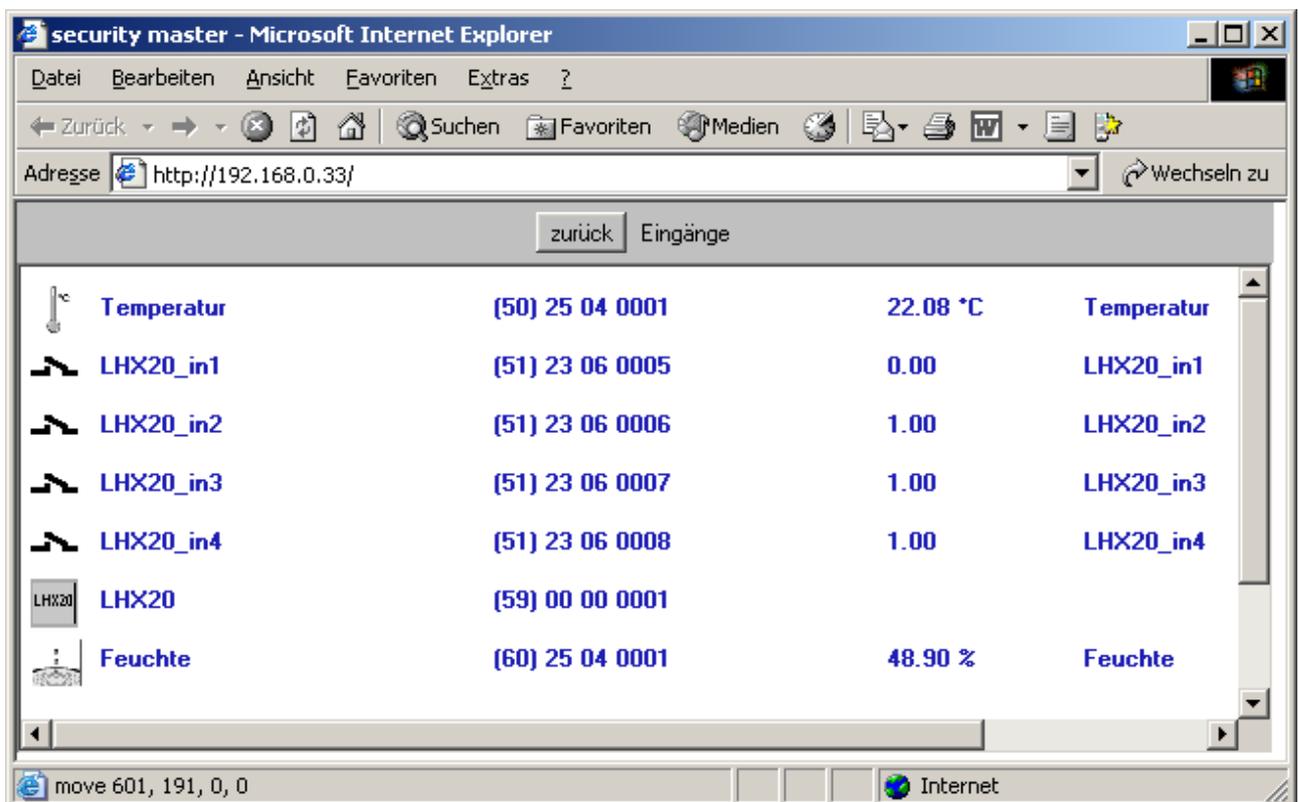
A physical connection is established between the RS232 port of the security master and the corresponding port on the LHX20. The RS232 cable supplied with the device is to be used for this purpose.

The following interface parameters are set on the LHX20:

57.600	Baud
8	Data bits
No	Parity
1	Stop bit

The address of the LHX20 is set to 5.

8.1.8 Inputs



The LHX20 appears on the “Inputs“ page.

8.1.8.1 Actual value display

The following actual values should be displayed:

Index	Name	Description
0	I 0	Temperature F1 PTC
1	I 1	Temperature F2 PTC
2	I 2	Temperature F3 PTC
3	I 3	Temperature F4 PTC
4	I 4	Temperature F5 PTC
5	I 5	Temperature F6 PTC
6	I 6	Temperature F7 power input

Index	Name	Description
9	I 9	Rotation speed N1 Fan 1
10	I10	Rotation speed N2 Fan 2
11	I11	Rotation speed N3 Fan 3
12	I12	Rotation speed N4 Fan 4
13	I13	Rotation speed N5 Fan 5
14	I14	Rotation speed N6 Fan 6

8.1.8.2 Display range – limit values

The display range for the temperature sensors is:

MIN **0 °C**
MAX **60 °C**

The display range for the fan is:

MIN **0 min⁻¹**
MAX **6000 min⁻¹**

8.1.8.3 Status display

The following error messages should be displayed:

8.1.8.3.1 Status 0

Bit	Name	Cause
0		Control system on/off

8.1.8.3.2 Status 1

Bit	Name	Cause
0	F1	Sensor error sensor 1 (Break or short circuit)
1	F2	Sensor error sensor 2 (Break or short circuit)
2	F3	Sensor error sensor 3 (Break or short circuit)
3	F4	Sensor error sensor 4 (Break or short circuit)
4	F5	Sensor error sensor 5 (Break or short circuit)
5	F6	Sensor error sensor 6 (Break or short circuit)
6	F7	Sensor error sensor 7
7	F8	Motor breakdown Fan 1
8	F9	Motor breakdown Fan 2
9	F10	Motor breakdown Fan 3
10	F11	Motor breakdown Fan 4
11	F12	Motor breakdown Fan 5
12	F13	Motor breakdown Fan 6
13	F14	Version Battery voltage: power supply interruption 1
14	F15	Version Battery voltage: power supply interruption 2
15	F16	Air outlet temperature at tolerance limit
16	F17	Air inlet temperature at tolerance limit
17	F18	Water inlet temperature at tolerance limit
18	F19	(OPTIONAL) malfunction message: door open
19	F20	Malfunction message: emergency cooling (Digital input)
20	F21	Cooling at maximum
21	F22	(OPTIONAL) Malfunction message: water leak
22	F23	(OPTIONAL) Moisture at tolerance limit
23	F24	(OPTIONAL) Malfunction message: external water cooler
24	F25	(OPTIONAL) water outlet temperature at tolerance limit

8.1.8.4 Depiction of security master

The data provided by the LHX20 are shown on the screen:



The screen is divided into 5 sections:

Sensor values (Temperatures)

Temperature F1 PTC
Temperature F2 PTC
Temperature F3 PTC
Temperature F4 PTC
Temperature F5 PTC
Temperature F6 PTC
Temperature F7 power input

Fan values (rotation speeds)

Rotation speed N1 Fan 1
Rotation speed N2 Fan 2
Rotation speed N3 Fan 3
Rotation speed N4 Fan 4
Rotation speed N5 Fan 5
Rotation speed N6 Fan 6

Sensor messages (errors)

F1 Sensor error sensor 1 (Break or short circuit)
F2 Sensor error sensor 2 (Break or short circuit)
F3 Sensor error sensor 3 (Break or short circuit)
F4 Sensor error sensor 4 (Break or short circuit)
F5 Sensor error sensor 5 (Break or short circuit)
F6 Sensor error sensor 6 (Break or short circuit)
F7 Sensor error sensor 7

Fan messages (errors)

F8 Motor breakdown Fan 1
F9 Motor breakdown Fan 2
F10 Motor breakdown Fan 3
F11 Motor breakdown Fan 4
F12 Motor breakdown Fan 5
F13 Motor breakdown Fan 6

Other messages (errors)

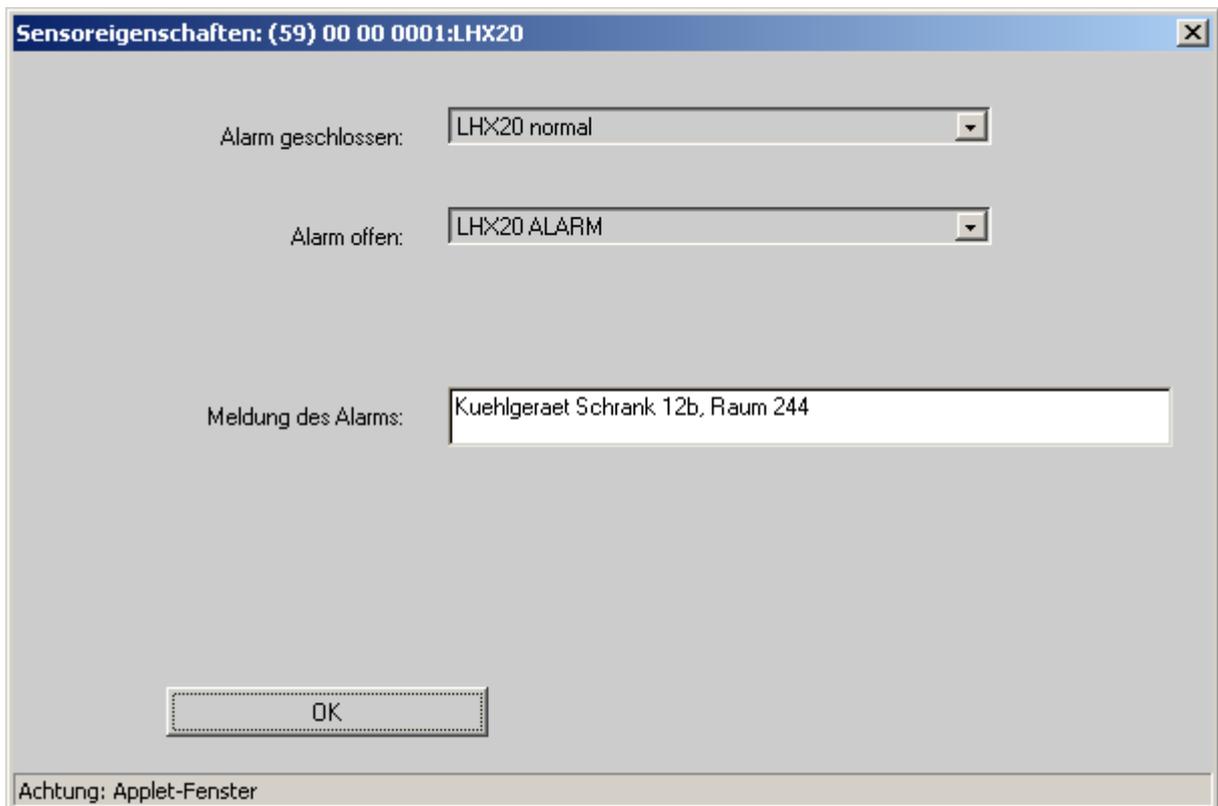
F14 Version Battery voltage: power supply interruption 1
F15 Version Battery voltage: power supply interruption 2
F16 Air outlet temperature at tolerance limit
F17 Air inlet temperature at tolerance limit
F18 Water inlet temperature at tolerance limit
F19 (OPTIONAL) malfunction message: door open
F20 Malfunction message: emergency cooling (Digital input)
F21 Cooling at maximum
F22 (OPTIONAL) Malfunction message: water leak
F23 (OPTIONAL) Moisture at tolerance limit
F24 (OPTIONAL) Malfunction message: external water cooler
F25 (OPTIONAL) Water outlet temperature at tolerance limit
ON Control system ON/OFF

Sensor Indicators F1-F25 are green if no error is detected, red if an error is detected. The ON indicator is red as long as the control system is switched off. It turns to green as soon as the control system is switched on.

8.1.8.5 Configuration



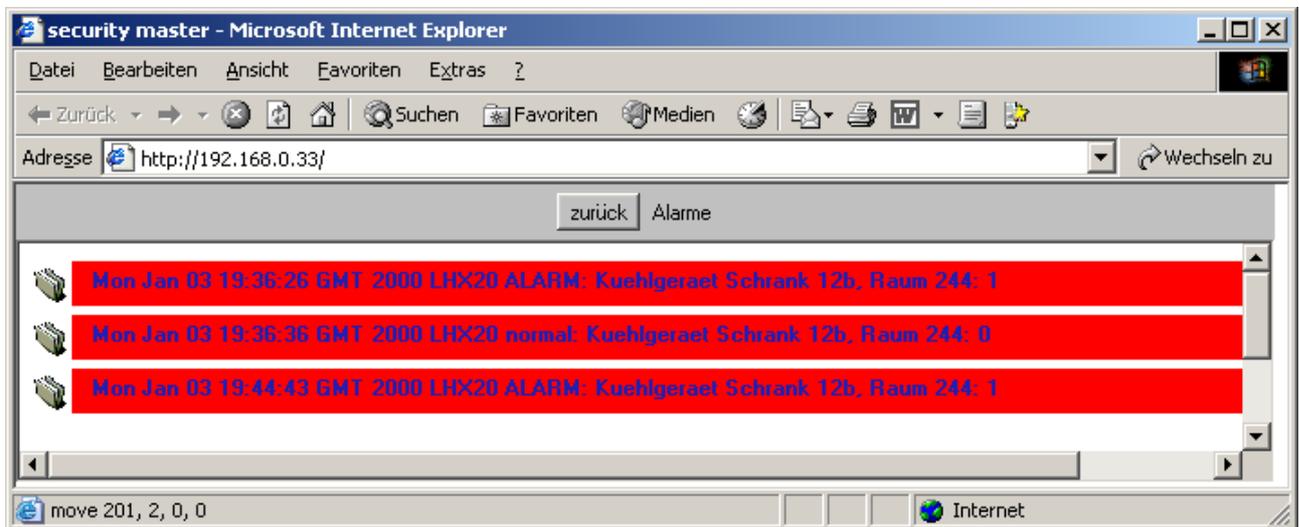
The LHX20 control system is represented by an icon
 The configuration page is opened by right clicking on the icon and left clicking on the menu option "Properties".



Alarm configuration LHX20

8.1.8.5.1 Alarm Alert

In the case of an alarm the LHX20's control system generates an alarm signal – Collective fault. Once this message has been received the security master generates in turn the alarm message defined for each individual case.

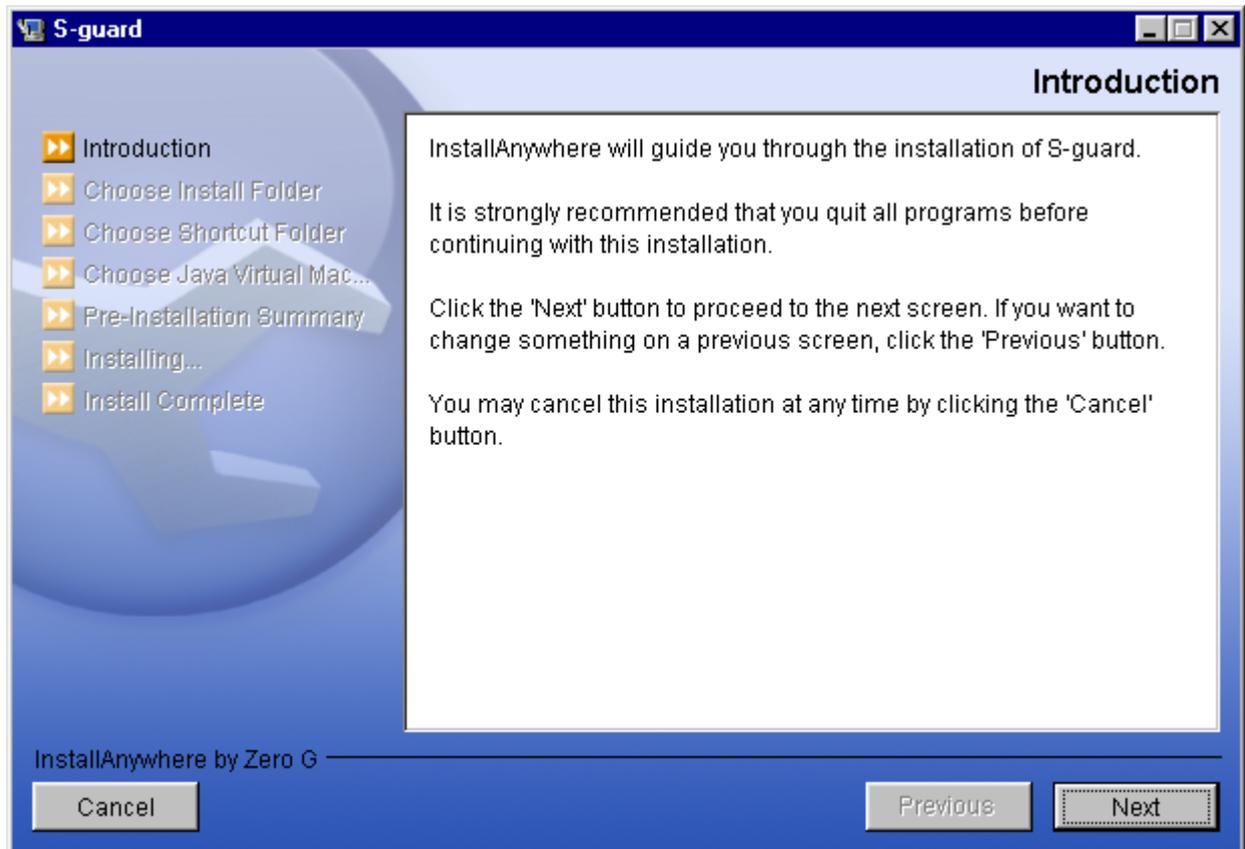


9 Service Programme

9.1 Sguard backup program installation

Service access to the **security master** is provided using the “Sguard Backup” program on the enclosed CD.

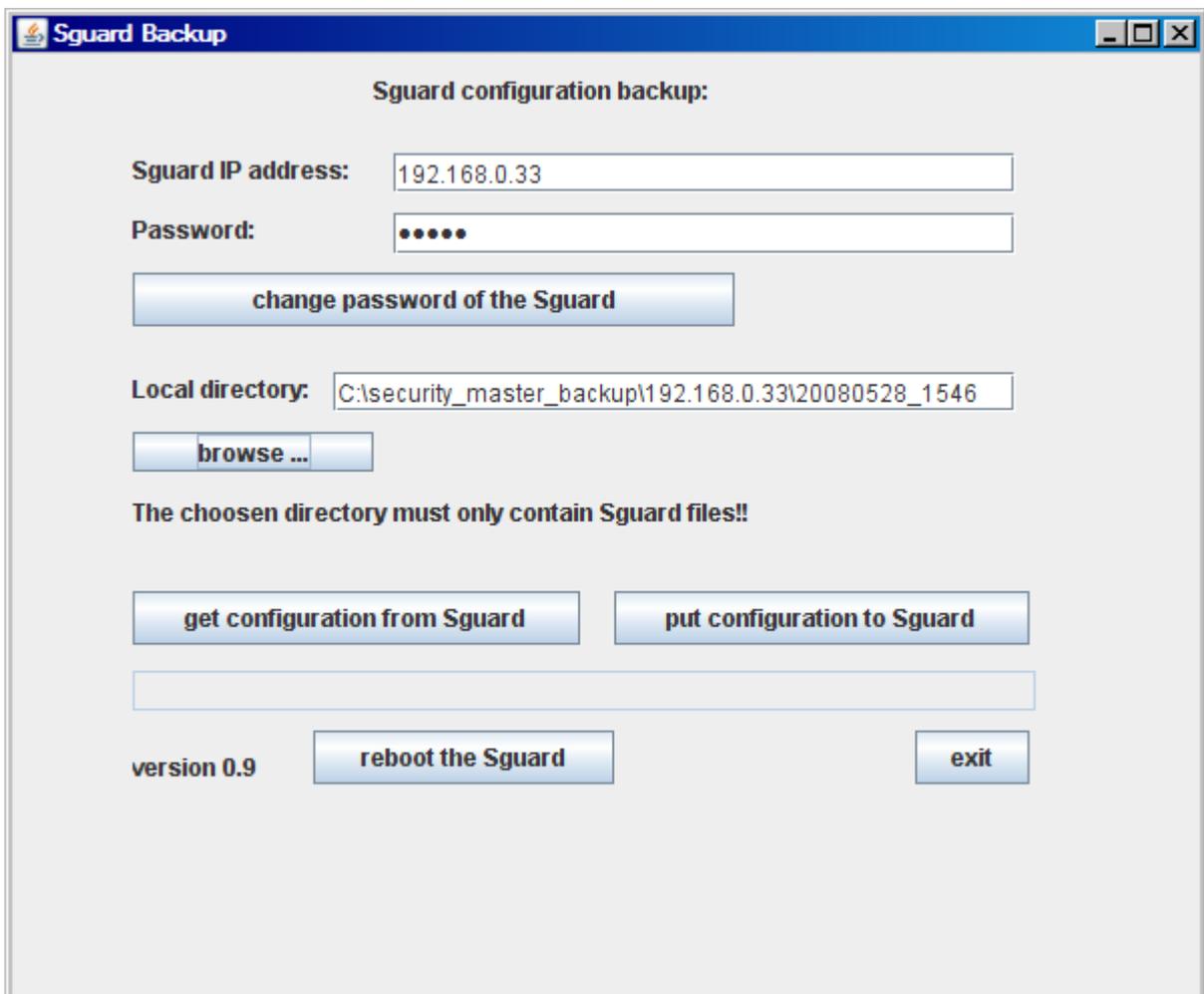
This program is to be installed on a PC:



Follow the instructions. Please note that a Java Virtual Machine needs to have been previously installed. Refer to the relevant selection page in the setup program. The “Sguard backup” program can now be found in the selected program group.

9.2 Device configuration backup

Start the program „Sguard Backup“.



Enter the IP address of the security master in question and the root password (factory setting: peter) and select the directory in which the backup files are to be saved. Now click on “get configuration from Sguard”.



The program registers on the device



and then saves the configuration in the selected directory.



9.3 Restore device configuration

Start the program „Sguard Backup“.
 Complete the mask as described above.
 Now click on “put configuration to Sguard“.



The program registers on the device and then saves the configuration in the device.



After the automatic reboot the device is ready to use.

9.4 Change service (root) Password

Start the program „Sguard Backup“.

Sguard configuration backup:

Sguard IP address:

Password:

Enter the IP address of the security master in question and the root password (factory setting: peter).
Now click on “change password of the Sguard”.

new password dialog

password:

reenter:

Click on OK to confirm.

Authorization is OK, wait ...

version 0.9

The program registers on the device and then saves the new password in the device.



The root password has been changed

Attention: if you forget the service password (root password) it cannot be restored. In this case you have to exchange the Flash drive!

9.5 Program updates

Current updates can be found at

<http://www.pmv-gmbh.de/securitymaster/updates.htm>

First the update is downloaded and copied on to the **security master**, for example, into the "Siebertz" directory under "winscp".

Then "putty" is called up and the following sequence of commands processed:

```
mount -o remount,rw /
cd /
tar xzf /Siebertz/smUpdxxxxxxxx.tgz
mount -o remount,ro /
reboot -f
```

After the reboot has been completed and the browser restarted the newly installed program starts to work.