Product Manual

ABB i-bus® EIB / KNX

Security Module
SCM/S 1.1

Intelligent Installation Systems

Contents

Page

This manual describes the function of the Security Module SCM/S 1.1 with the application program "Security Slave/2".
Subject to changes and errors excepted.

Exclusion of liability:
Despite checking that the contents of this document match the hardware and software, deviations cannot be completely excluded. We therefore cannot accept any liability for this. Any necessary corrections will be inserted in new versions of the manual.
Please inform us of any suggested improvements.

1 General

The Security Module SCM/S 1.1 is an EIB/KNX device for DIN rail mounting with a width of 2 modules. It is used to control security functions as a central logic device.

The Security Module evaluates detectors of any type (e.g. motion detector, window and door contacts) and links them to a security and monitoring system. It further controls the alarm and setting/unsetting logic.

The area of application covers small to medium-sized installations without VdS requirements e.g. private homes, administration buildings and industrial premises.

The device has three LEDs to display the operating state as well as a freely controllable relay output to which e.g. a signalling device can be connected. Moreover, the device has a freely controllable internal buzzer.

1.1 System overview

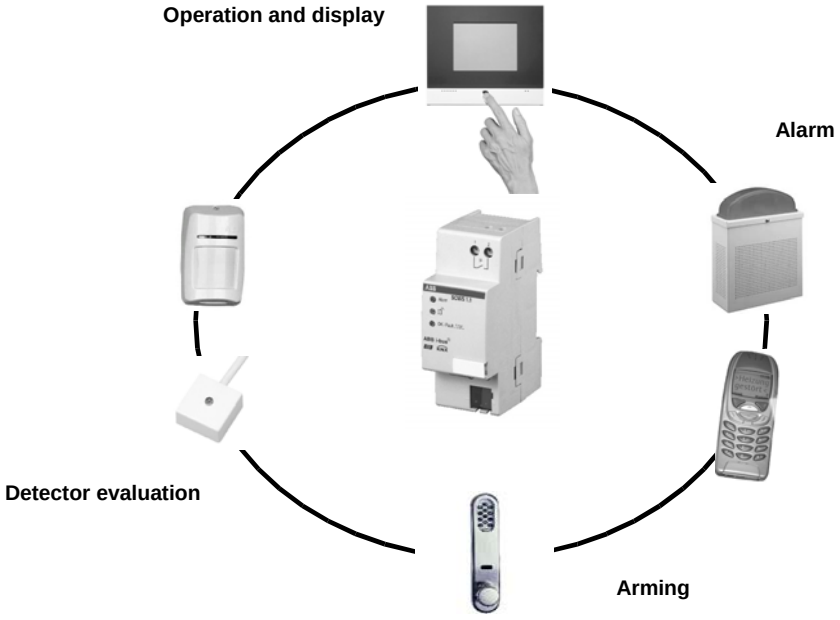


Fig. 1: System overview

The diagram above provides an overview of an alarm system based on the Security Module.

The main tasks of the device is the evaluation of the detectors which are connected to the bus via Zone Terminals.

A setting/unsetting device sets and unsets the alarm system. An LCD display with bus capability (e.g. room panel) can be used as an operating and display unit.

The alarm is carried out e.g. via signalling devices or telephone, which are controlled via a switch actuator or a Telephone Gateway.

1.2 Product and functional overview

The Security Module evaluates up to 64 detectors. There are 64 objects available for this purpose. It controls the setting/unsetting of the system, the issue of alarms and provides information at all times about the system state via status reports – if required also as a clear text display (14-byte objects).

The most important functions are described briefly in the following section.

Detector evaluation

Each of the 64 objects can be assigned to a **detector type**. It is therefore defined whether and in which way an alarm is triggered in the event of a signal.

Detector types are e.g. intruder detectors (interior/exterior), sabotage detector, technical detectors or lock monitoring detectors.

Detectors can also be **disabled** so that e.g. a window can be opened for ventilation without an alarm being triggered. This option must be enabled in the parameters.

Through the **cyclical monitoring** of detectors, it can be ensured that the wilful or inadvertent removal of a detector can be detected by the bus.

Setting/unsetting

The setting/unsetting function is an essential feature of a security system in terms of safety and convenience. The Security Module distinguishes between **internal and external setting/unsetting**. Moreover, **delayed setting/unsetting** is also possible which is started inside the building.

If a building has several entrances, it is possible to operate several setting/unsetting devices in parallel.

Alarm

The alarm notifies the user depending on the type of signal (detector type) and the setting/unsetting status. The signalling is carried out via an external or internal strobe light or siren.

The Security Module is specially designed for intelligent **remote signalling** via an EIB Telephone Gateway. There are separate communication objects available for this purpose.

A floating **relay output** is available directly on the device for signalling. Signals can also be indicated by an **internal buzzer**.

Status reports

The Security Module provides detailed information about its state at any time. The important status reports are also sent as **clear report texts**.

Three **status LEDs** directly on the device provide direct information about the status of the device. They report the correct operation, setting/unsetting state and alarm.

With the help of the **event list memory** (250 entries), the history can also be understood.

2 Device technology

Provides logic functions to built up a security system in small and medium-sized EIB/KNX installations in combination with other EIB/KNX devices, e.g. zone terminals, motion detectors. Up to 64 different zones. Internal relay can be used for alarming.

2.1 Technical data

Power supply:	– Operating voltage	21 ... 30 V DC, via the EIB
	– Max. current consumption	10 mA
Outputs:	– 1 floating relay contact	Switching voltage: 0...230 V AC/DC Switching current: 6 A, AC1 freely programmable
Operating and display elements:	– Red LED and push button	For assignment of the physical address
	– Red LED	- LED on: Alarm is triggered - LED off: No alarm
	– Yellow LED	- LED on: System is unset - LED off: System is set
	– Green LED	- LED on: Ready for operation - LED flashes: Fault - LED off: No operation
Connections:	– Floating output	2 screw terminals Wire range: finely stranded: 0.2 – 2.5 mm² single-core: 0.2 – 4 mm²
	– EIB	Bus connection terminal, included with supply
Type of protection:	– IP 20, EN 60 529	
Ambient temperature range:	– Operation	- 5 °C ... 45 °C
	– Storage	-25 °C ... 55 °C
	– Transport	-25 °C ... 70 °C
Design:	– Type of installation	on 35 mm mounting rail, DIN EN 60715
	– Mounting depth	2 modules at 18 mm
	– Housing dimensions (HxWxD)	90 x 36 x 64 mm
	– Mounting position	As required
	– Weight	0.1 kg
Certification:	– EIB- and KNX-certified	
CE mark:	– In accordance with the EMC guideline and low voltage guideline	

2.2 Device connection

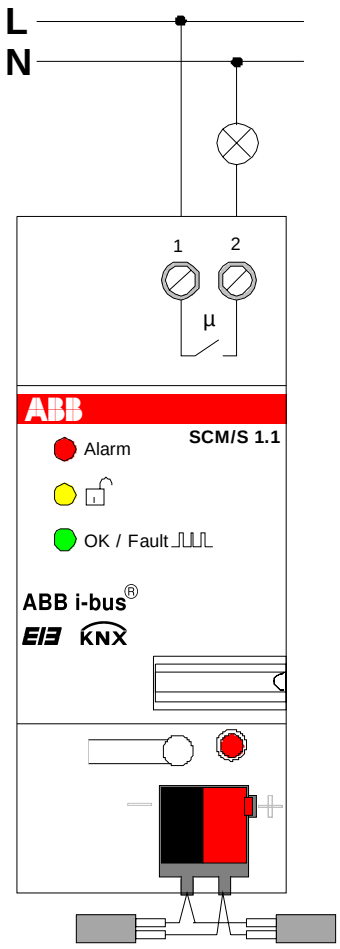


Fig. 2: Connection diagram

The device is linked with the ABB i-bus® EIB / KNX via a bus connection terminal (included with supply).

2.3 Description of the inputs and outputs

The Security Module has a floating relay output which can be freely programmed. For example fault messages like bus voltage failure can be signalled via this output.

3 Commissioning

3.1 Overview / Notes

The application program *"Security Slave/2"* controls all the functions of the Security Module. The programming requires the EIB Tool Software ETS2 **V1.2a** or higher. When using ETS3, a file of type ".VD3" must be imported.

Application program	Number of communication objects	Max. number of group addresses	Max. number of associations
Security Slave/2	142	254	255

The device is suitable for insertion in distribution boards or miniature housing for snap-on fixing on 35 mm mounting rails, in accordance with DIN EN 60715. The accessibility of the device for operation, testing, inspection, maintenance and repair must be ensured.

3.2 Parameters

3.2.1 General functions

The objects and parameters described here are visible in both operating modes ("Master" and "Slave").

3.2.1.1 Parameter window: "General"

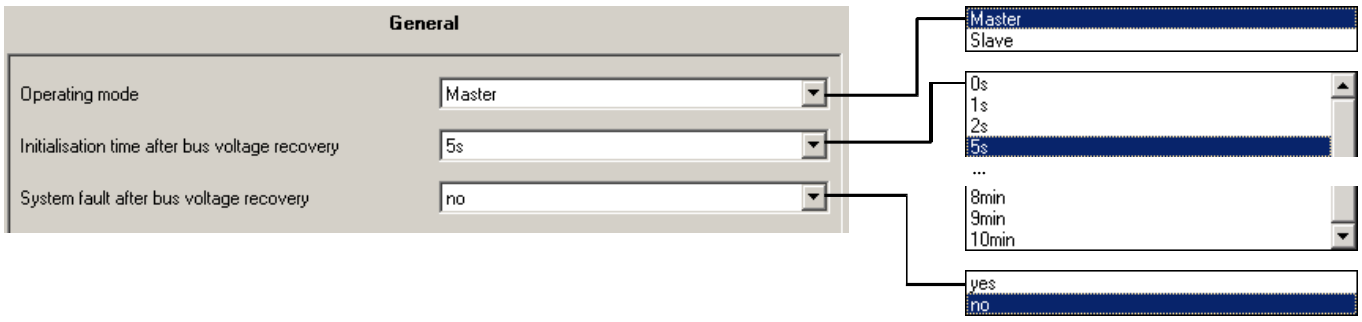


Fig. 3: Parameter window: "General"

Operation mode

The operation mode defines whether the device works alone or whether it forms a monitoring system together with other devices. Further information about the different operation modes can be found in section 4.2.

As a *"Master"*, the device works alone or it can be extended by one or several slaves. The parameters are described in section 1.1.1.

As a *"Slave"*, the device is used for the extension of an alarm system which can be a further Security Module which is set to "Master" mode or an intrusion alarm panel with EIB / KNX interface. The slave has the task of bringing together several detectors so that more than 64 detectors are possible per master. The parameters are described in section 1.1.1.

Initialisation time after bus voltage recovery

During the initialisation period, telegrams are only received and not evaluated. No telegrams are sent. The object values are only read out and processed once the initialisation period has elapsed.

The purpose of the initialisation period is to give the detectors time to update their actual status on the bus.

System fault after bus voltage recovery

It can be set here whether the device experiences a fault after bus voltage recovery. The user can thus be informed about the bus voltage failure.

The fault must be reset by the object “Reset”.

3.2.1.2 Parameter window: “Function”

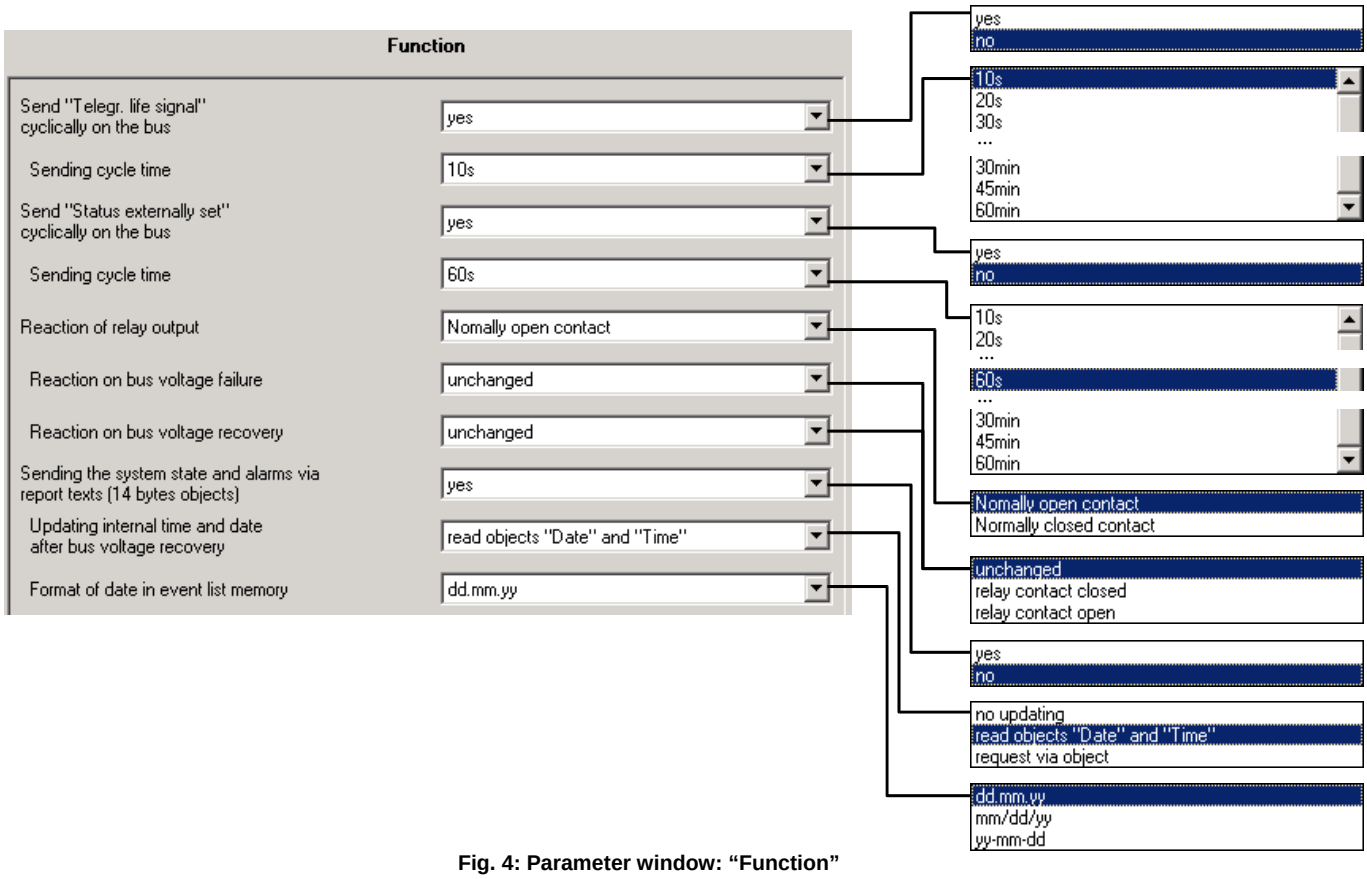


Fig. 4: Parameter window: “Function”

Send “Telegr. life signal” cyclically on the bus

This parameter enables the object “Telegr. life signal”. Using this object, the device can send a cyclical telegram to a higher priority device which monitors it for an operational fault. The interval for sending the object is defined in the subsequent parameter **“Sending cycle time”**.

Send “Status externally set” cyclically on the bus

This parameter sets whether the object “Status externally set” is sent cyclically on the bus. The interval for sending the object is defined in the subsequent parameter **“Sending cycle time”**.

The parameter is only visible in “Master” mode.

Reaction of relay output

It can be set with this parameter whether the relay output operates as a *Normally open contact* or *Normally closed contact*. It describes the function of the object *Relay output - Switch*.

In the setting *Normally open contact*, the object value “1” leads to the closing of the relay. The object value “0” opens it.

In the setting *Normally closed contact*, the object value “1” leads to the opening of the relay. The object value “0” closes it.

Reaction on bus voltage failure

The behaviour of the relay output on bus voltage failure is set here.

Reaction on bus voltage recovery

The behaviour of the relay output on bus voltage recovery is set here.

Sending the system state and alarms via report texts (14-byte objects)

This parameter the report texts via 14-byte objects. The following states and events can be displayed via report texts:

Object name / Function	Explanation
Event list memory / Text name of event Event list memory / Text name of detector Event list memory / Text date/time	For reading out the event list memory.
Detector surveillance / Text triggered detector	To display which detecor has just been triggered.
Alarming / Text name of alarm Alarming / Text alarming detector	Indicates which alarm was triggered by which detector in the event of an alarm.
Setting/Unsetting / Text setting status	Indicates the current setting/unsetting status.

The text itself is defined in the parameters.

Updating internal time and date after bus voltage recovery

After bus voltage failure, the device no longer knows the time and date. It is set via this parameter how the device is informed about the time and date.

In the setting *"no updating"*, the master clock automatically informs the Security Module about the time and date.

In the setting *"read objects 'Date' and 'Time'"*, the Security Module queries the object values itself via the bus.

In the setting *"request via object"*, the Security Module sends the object "Request date/time" on the bus directly after bus voltage recovery and requests the time and date from the master clock.

Format of date in event list memory

This parameter sets how the date is displayed in the object "Text date/time" when reading out the event list memory as a report text.

"dd.mm.yy" as "29.04.05"

"mm/dd/yy" as "04/29/05"

"yy-mm-dd" as "05-04-29" (international format)

3.2.2 “Master” mode

In the “Master” mode, the Security Module either operates alone or it evaluates further Security Modules as a central master.

3.2.2.1 Parameter window: “Setting/Unsetting”

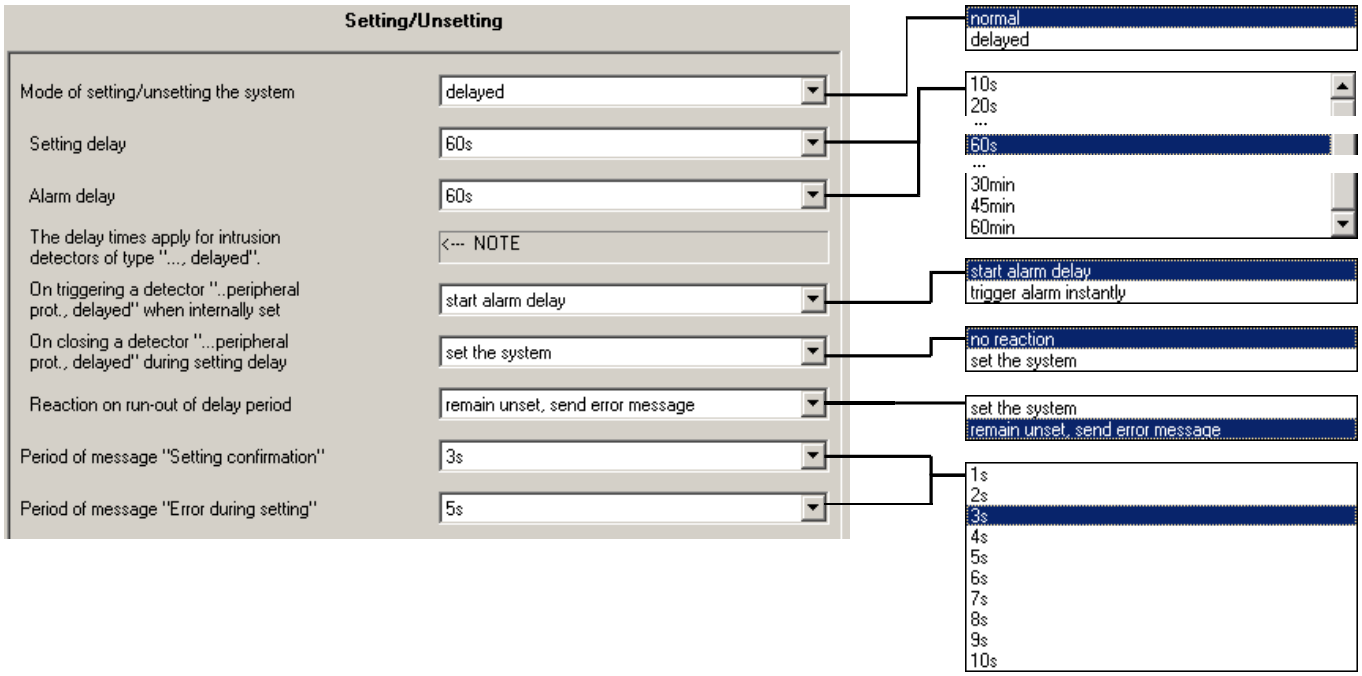


Fig. 5: Parameter window: “Setting/Unsetting” (Master mode)

Mode of setting/unsetting the system

It can be set here whether the external setting/unsetting of the system should be carried out as “normal” or “delayed”.

With *nomal setting/unsetting* the system is set instantly after a setting request is received.

With delayed setting/unsetting, the user starts the delay period from inside the security area. Within the delay period the user can leave the security area. In the meantime all detectors of the “delayed” type are inactive.

Further information about the setting/unsetting options can be found in section 4.4.

Setting delay

When delayed setting/unsetting is set, this parameter defines how much time the user has to leave the security area after an setting/unsetting request.

Alarm delay

When delayed setting/unsetting is set, this parameter defines how much time the user has to unset the alarm system on entering the security area.

On triggering a detector “..peripheral prot., delayed” when internally set

It can be set here whether a detector of type *Intrusion detector: peripheral protection, delayed* triggers an alarm immediately if the system is set internally (option *trigger alarm instantly*) or if the alarm delay is started (option *start alarm delay*). During the alarm delay the user has the possibility to unset the system.

On closing a detector “…peripheral prot., delayed” during setting delay

The system can be set immediately here if the user closes the external door during the delay (option *set the system*).

The function operates as follows: If a detector of type *Intrusion detector: peripheral protection, delayed* is closed during the delay period, the device is set immediately. This detector can be linked e.g. with the key bolt switching contact of a door.

Reaction on run-out of delay period

This parameter is visible if the value *setting the system* has been set in the parameter *Reaction on closing of a delayed detector during the delay*.

The behaviour once the delay period has elapsed is set here. It is possible to set the system or an error message may appear.

Period of setting confirmation

This parameter sets the period after which the object *Setting confirmation* is automatically reset to the value “0”.

The object *Setting confirmation* shows the user that the system has been successfully set.

Period of error message

This parameter sets the period after which the object *Error during setting* is automatically reset to the value “0”.

The object *Error during setting* reports an error during the setting/unsetting procedure.

3.2.2.2 Parameter window: “Setting Status Texts”

It is set in this parameter window which values the **object “Text setting status”** uses to display the setting state of the system. A maximum of 14 characters are possible.

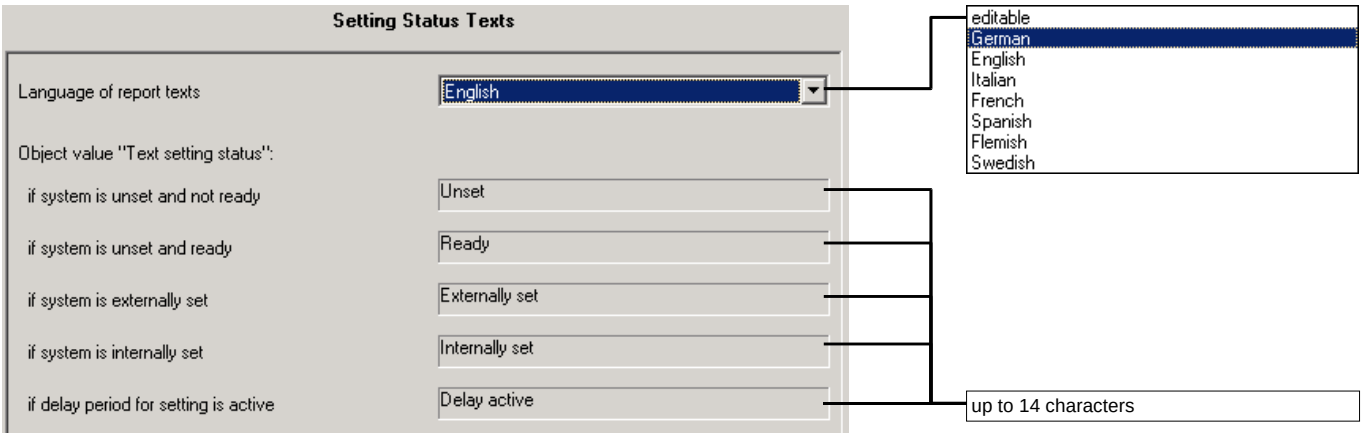


Fig. 6: Parameter window: “Setting Status Texts” (Master mode)

Language of report texts

Predefined texts for some languages can be selected here. With parameter value “editable” the texts can be edited.

Object value“Text setting status”

if system is unset and not ready

The device is unset but not ready for setting because a message is present (e.g. a detector has been triggered or a reset has not been carried out after an alarm).

if system is unset and ready

The device is unset and can be set.

if system is externally set

The device is set externally i.e. all the internal and peripheral sensors are activated.

if system is internally set

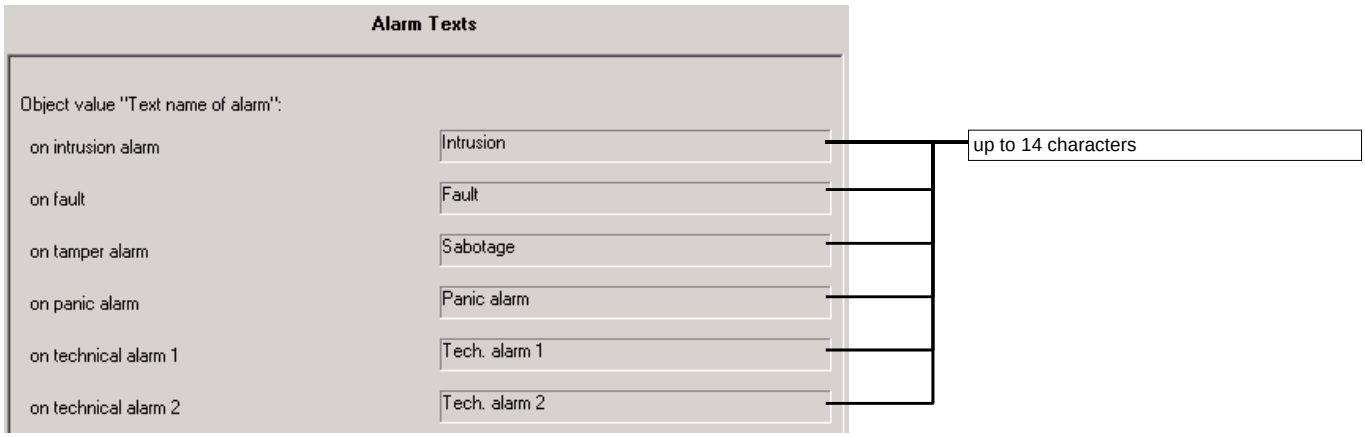
The device is set internally i.e. only the peripheral sensors are activated.

if delay period for setting is active

The delay period for setting is active. This parameter is only relevant if delayed setting has been selected (see parameter window “Setting/Unsetting”).

3.2.2.3 Parameter window: “Alarm Texts”

It is set in this parameter window which values the **object “Text name of alarm”** uses to display the kind of alarm that has occured. A maximum of 14 characters are possible.



Predefined texts for some languages can be selected in parameter window “Setting status texts”. With parameter value “editable” the texts can be edited.

Report text on intrusion alarm

...

Report text on technical alarm 2

These parameters set which report texts are sent by object “Text name of alarm” depending on the alarm type.

3.2.2.4 Parameter window: “Alarm: General”

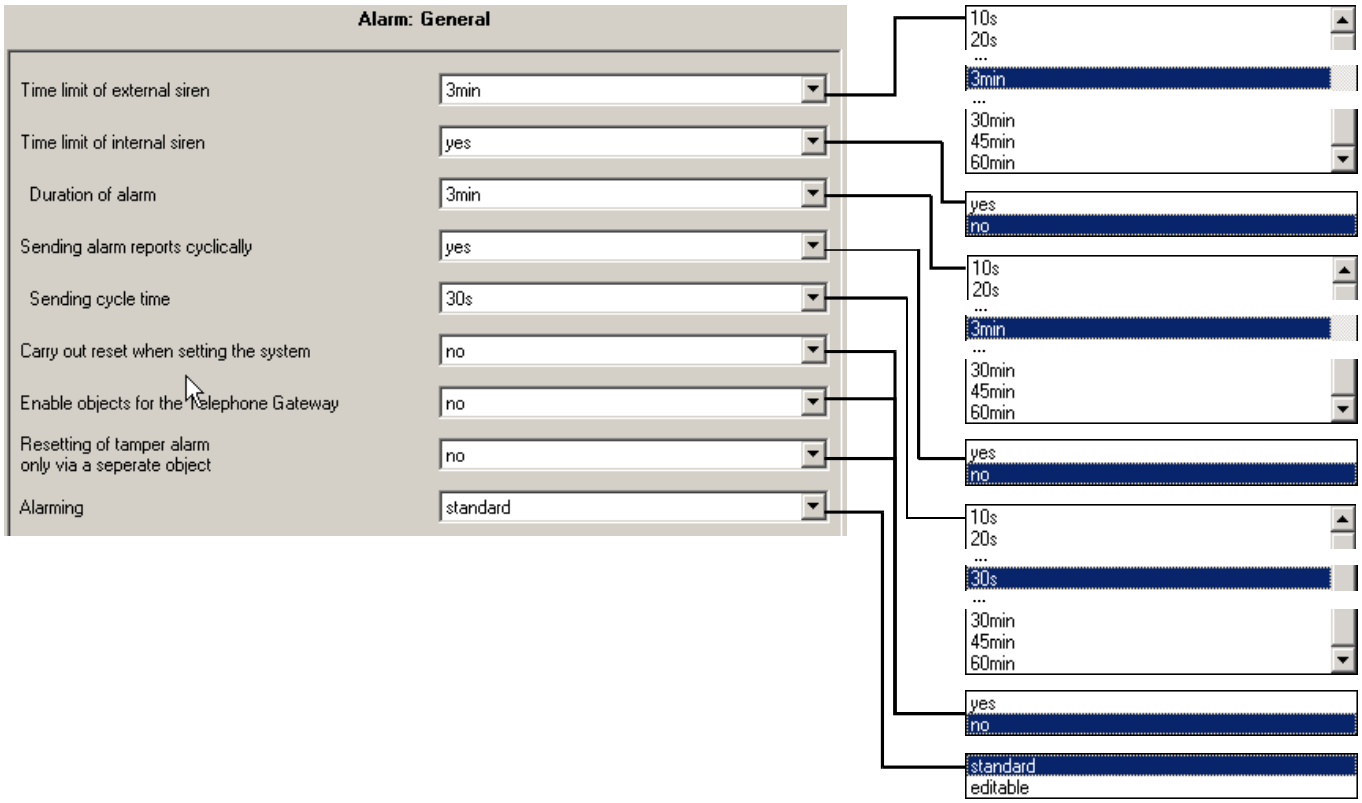


Fig. 7: Parameter window: “Alarm: General” (Master mode)

Time limit of external siren

The external siren (object *External siren*) is always controlled with a time limit. The period is set here.

Time limit of internal siren

This parameter sets whether the internal siren should be switched off again after a specific period. If yes, this period is set in the parameter **“Duration of alarm”**.

Sending alarm reports cyclically

This parameter sets how the objects “External strobe light”, “External siren” and “Internal siren” are sent cyclically if they have the object value “1”. If “yes” is selected, this period is set in the parameter **“Transmission cycle time”**.

The following additional objects are sent cyclically depending on the triggered alarm:

- Telegr. intrusion alarm
- Telegr. technical alarm 1
- Telegr. technical alarm 2
- Telegr. panic alarm
- Telegr. tamper alarm
- Telegr. fault

Carry out reset when setting the system

It is possible to carry out a reset even if a stored alarm normally prevents the system from being set.

If “yes” is selected, it is possible to check before setting the system whether the stored report texts are present. If “yes” is selected, a reset is carried out first and then the alarm system is set.

Resetting of tamper alarm only via a separate object

In this parameter, it is possible to enable the reset of the tamper alarm only by specific people e.g. the system installer.

This parameter enables the object *Tamper reset*. The object *Telegr. tamper alarm* can thus only be reset via this object. Otherwise, this object has the same function as the *Reset* object (see the object description in the section 3.3.1).

Enable objects for Telephone Gateway

This parameter enables extra objects for the remote signalling via a telephone gateway. The following objects are enabled:

Object function	Object name
Telegr. intrusion alarm	Telephone Gateway
Telegr. technical alarm 1	Telephone Gateway
Telegr. technical alarm 2	Telephone Gateway
Telegr. panic alarm	Telephone Gateway
Telegr. tamper alarm	Telephone Gateway
Telegr. fault	Telephone Gateway

Alarming

The type of alarm can be adapted here to specific needs. The parameter enables five parameter windows in which the alarm can be defined according to user requirements.

In general, the alarm is carried out depending on the type of detector which triggered the alarm. An overview of the default settings can be found in section 4.5.2.

Further information about the alarm options can be found in section 4.5.

3.2.2.5 Parameter window: ”Intrusion alarm”

It is set here which signalling device displays an intrusion alarm.

The parameter window is visible if it has been enabled in the “Alarm” parameter (parameter window “Alarm: General”).

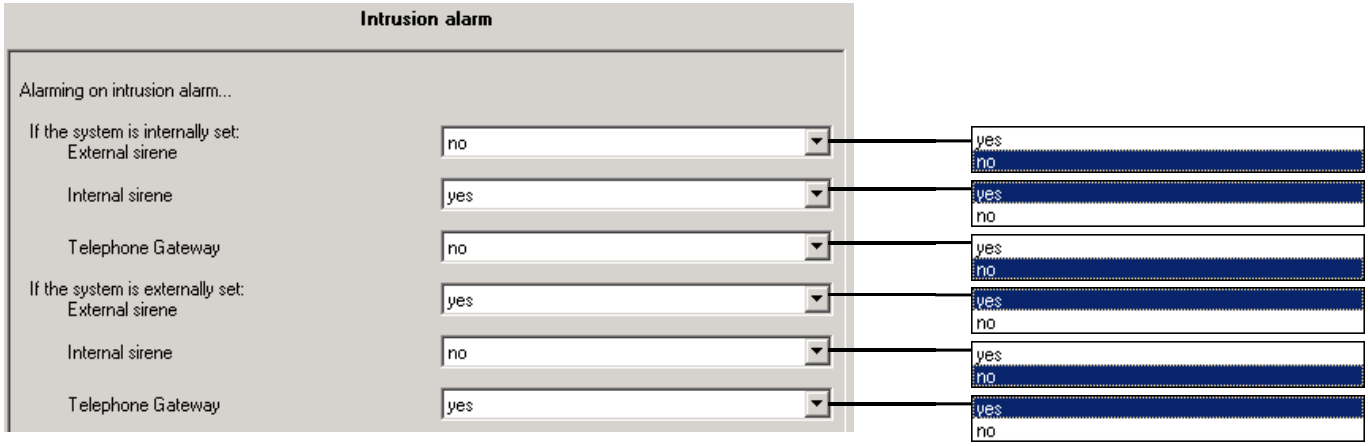


Fig. 8: Parameter window: “Intrusion alarm” (Master mode)

If the system is internally set: (3 parameters)

It is defined in these three parameters via which signalling device an intrusion alarm is indicated when the system is internally set. The alarm can be carried out as required via external signalling devices (siren/strobe light), internal signalling devices or via a Telephone Gateway.

If the system is externally set: (3 parameters)

It is defined in these three parameters via which signalling device an intrusion alarm is indicated when the system is externally set. The alarm can be carried out as required via external signalling devices (siren/strobe light), internal signalling devices or via a Telephone Gateway.

3.2.2.6 Parameter window: “Tamper alarm”

It is set here which signalling device displays a tamper alarm.

The parameter window is visible if it has been enabled in the “Alarm” parameter (parameter window “Alarm: General”).

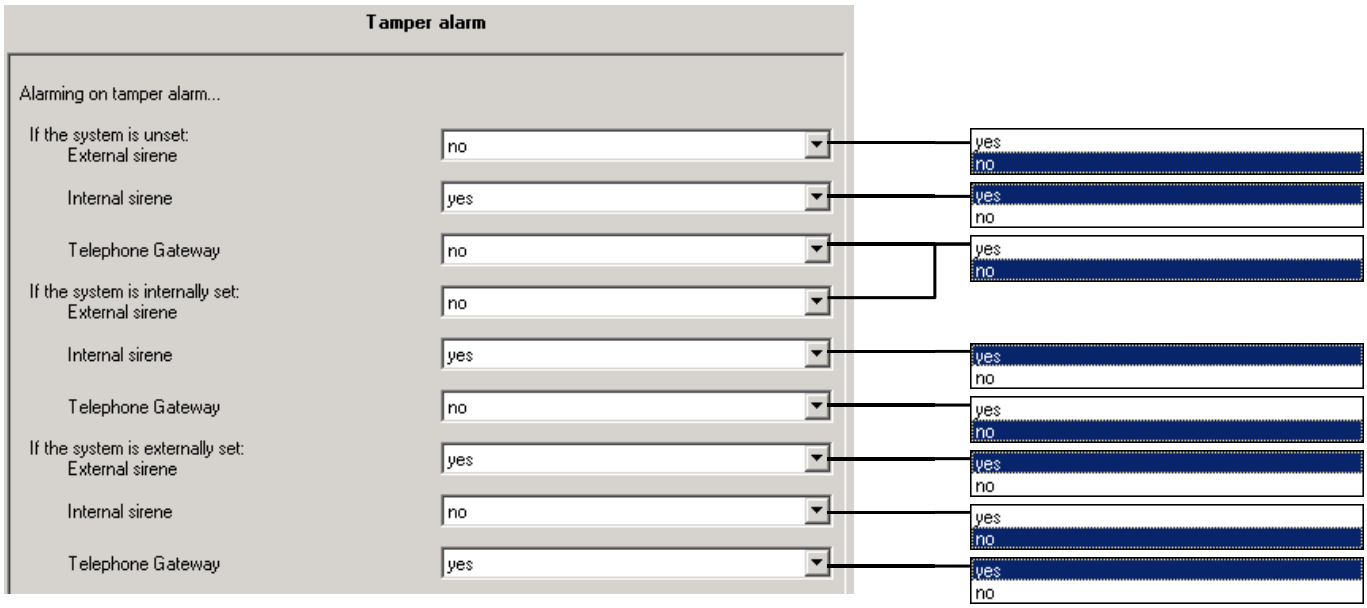


Fig. 9: Parameter window: “Tamper alarm” (Master mode)

If the system is unset: (3 parameters)

It is defined in these three parameters via which signalling device a tamper alarm is indicated when the system is unset. The alarm can be carried out as required via external signalling devices (siren/strobe light), internal signalling devices or via a Telephone Gateway.

If the system is internally set: (3 parameters)

It is defined in these three parameters via which signalling device a tamper alarm is indicated when the system is internally set. The alarm can be carried out as required via external signalling devices (siren/strobe light), internal signalling devices or via a Telephone Gateway.

If the system is externally set: (3 parameters)

It is defined in these three parameters via which signalling device a tamper alarm is indicated when the system is externally set. The alarm can be carried out as required via external signalling devices (siren/strobe light), internal signalling devices or via a Telephone Gateway.

3.2.2.7 Parameter window: “Panic/Fault”

It is set here which signalling device displays a panic alarm or fault.

The parameter window is visible if it has been enabled in the “Alarm” parameter (parameter window “Alarm: General”).

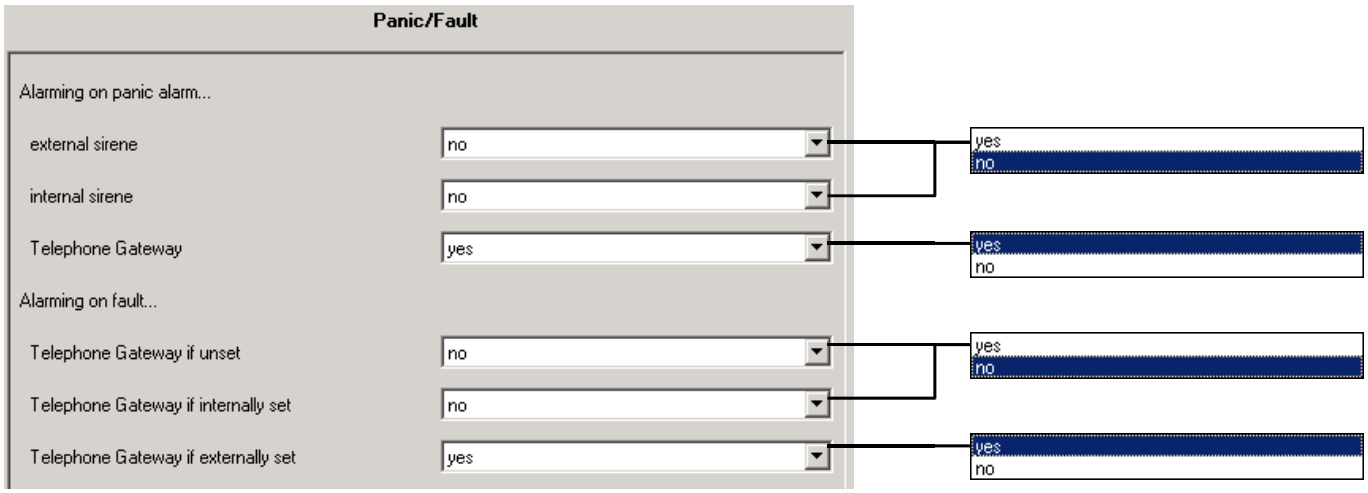


Fig. 10: Parameter window: “Panic/Fault” (Master mode)

Internal siren
External siren
Telephone Gateway

It is defined in these parameters which signalling devices report a panic alarm. The alarm is not dependent on the setting/unsetting state in principle.

Telephone Gateway if unset
Telephone Gateway if internally set
Telephone Gateway if externally set

A fault can be reported via a Telephone Gateway (object “Telephone Gateway - Telegr. fault”. It is defined in these parameters in which setting/unsetting state the Telephone Gateway reports a fault.

Tip: The object “Alarming - Telegr. fault” is suitable for displaying the fault locally.

3.2.2.8 Parameter window: “Tech. Alarm 1” and “Tech. Alarm 2”

It is set here which signalling device displays a technical alarm. Technical alarms 1 and 2 have the same functionality and are described together here.

These two parameter windows are visible if they have been enabled in the “Alarm” parameter (parameter window “Alarm: General”).

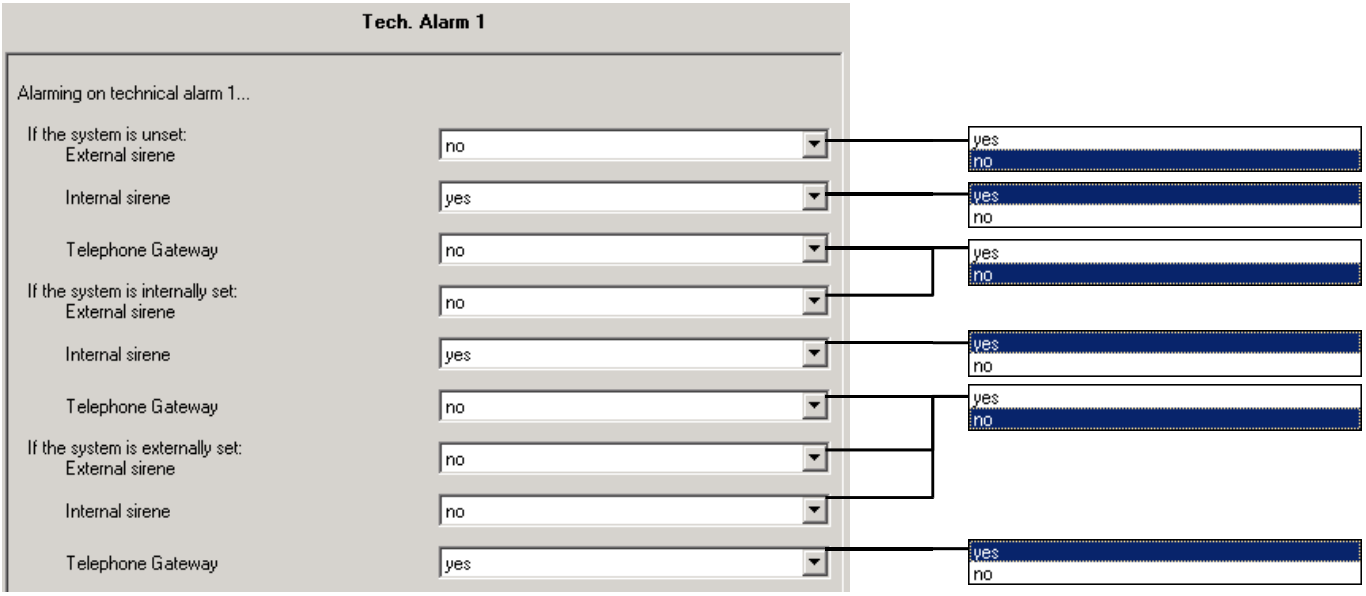


Fig. 11: Parameter window “Tech. Alarm 1” (Master mode)

If the system is unset: (3 parameters)

It is defined in these three parameters via which signalling device a technical alarm is indicated when the system is unset. The alarm can be carried out as required via external signalling devices (siren/strobe light), internal signalling devices or via a Telephone Gateway.

If the system is internally set: (3 parameters)

It is defined in these three parameters via which signalling device a technical alarm is indicated when the system is internally set. The alarm can be carried out as required via external signalling devices (siren/strobe light), internal signalling devices or via a Telephone Gateway.

If the system is externally set: (3 parameters)

It is defined in these three parameters via which signalling device a technical alarm is indicated when the system is externally set. The alarm can be carried out as required via external signalling devices (siren/strobe light), internal signalling devices or via a Telephone Gateway.

3.2.2.9 Parameter window: “Detector Inputs”

The detectors are enabled in this parameter window and the cyclical monitoring period of the detectors is set.

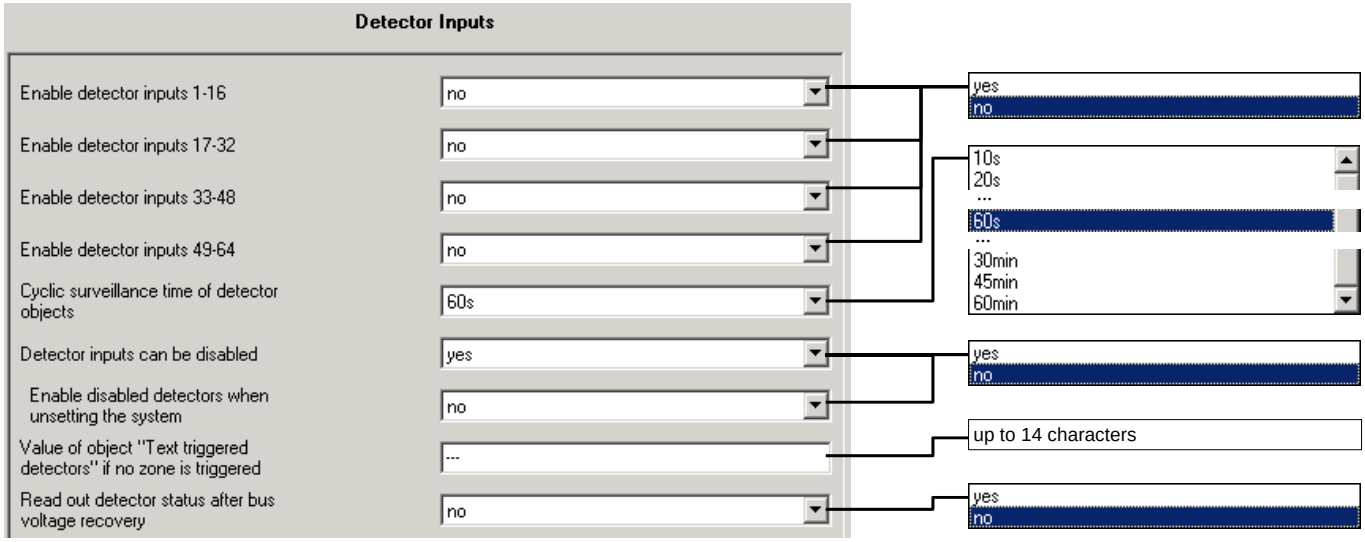


Fig. 12: Parameter window: “Detector inputs” (Master mode)

Enable detector inputs 1-16

...

Enable detector inputs 49-64

16 detector inputs can be enabled each time in these 4 parameters. When they are enabled, the corresponding parameter windows “01-02” … ”63-64” appear in which the detector settings can be carried out.

Cyclic surveillance time of detector objects

The period for the cyclical monitoring of the detector objects is set here.

It is possible to set in the parameter windows “01-02” …”63-64” whether a detector object is monitored cyclically or not.

When cyclic surveillance is active, a regular telegram is expected from a detector object within the monitoring period. If there is no telegram, it has the same effect as if the detector had been triggered.

Caution: The monitoring period should be at least twice as long as the cyclic transmission time of the detectors. Please note the bus load when the detectors are monitored cyclically.

Detector inputs can be disabled

Detectors can be disabled here. Disabled detectors behave as if they are never triggered.

15 detector disable objects are enabled with this parameter. In the parameter “Detector object is disabled by” (parameter window “01-02” ... ”63-64”), each detector can be assigned to a disable object.

Enable disabled detectors when unsetting the system

If this parameter is set to “yes”, all the disabled detectors are switched on again when the system is unset. It is thus possible to prevent a detector for example unintentionally being permanently disabled.

This parameter is visible if detectors can be disabled (parameter window *01-02 … 63-64*, parameter *Detector inputs can be disabled = yes*).

Read out detector status after bus voltage recovery

The device can read out the status of detectors automatically after bus voltage recovery. This is advisable for example if the detectors cannot send their state themselves and their current status is therefore unknown after bus voltage recovery. Further information can be found in section 4.7.

Value of object “Text triggered detectors” if no detector is triggered

This parameter defines what is shown in the text display if no detectors have been triggered.

Via the object *Text triggered detector*, the user can display the names of the detectors which have just been triggered in clear text.

This parameter is visible if the 14-byte report texts have been enabled (parameter window “Function”).

3.2.2.10 Parameter window: ”01-02” ... “63-64”

These parameter windows are visible if they have been enabled in the “Detectors” parameter window. The function of two “Detector …” objects is defined in each window. All 64 detectors have the same functional scope.

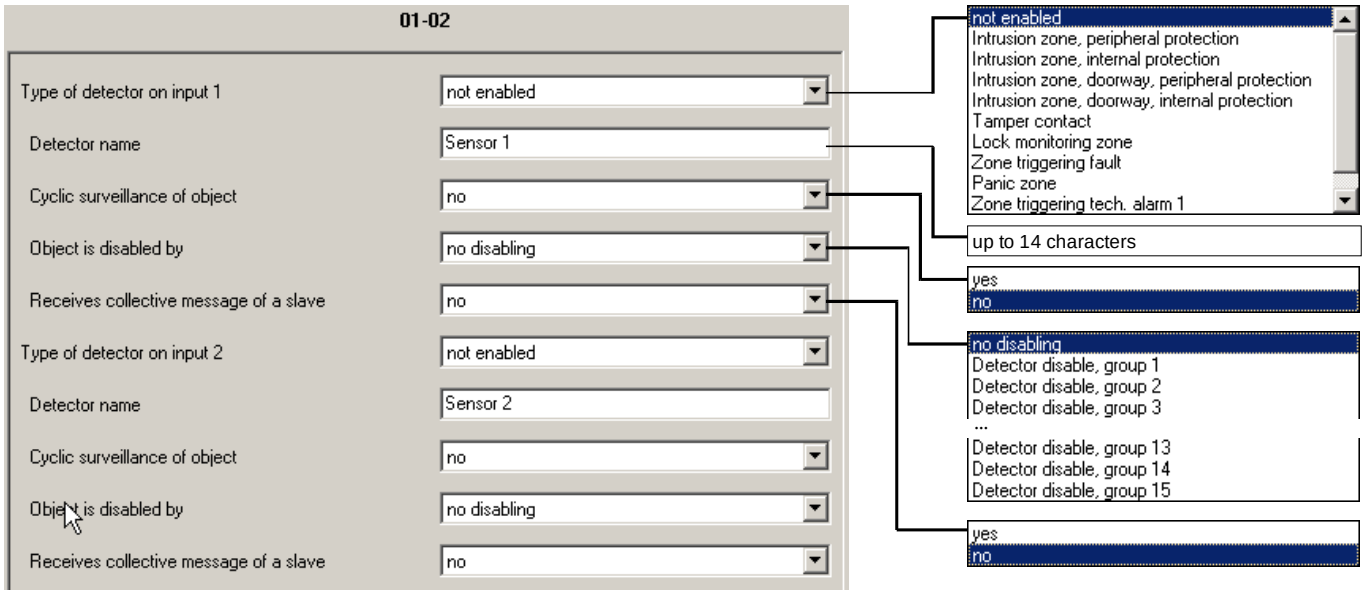


Fig. 13: Parameter window: “Detector 01-02” (Master mode)

Type of detector on input...

This parameter defines the type of detector which is assigned to the object “Detector …”. If the object receives the telegram value “1”, it is evaluated depending on the detector type and the setting/unsetting state and if necessary an alarm is triggered. Further information about the detector types can be found in section 4.3.

Detector name

The name of the detector is defined here. This name is sent e.g. via the object “Text name of detector” if this detector triggers an alarm. If the report text is empty (only spaces), nothing is sent.

Cyclic surveillance of object

The cyclical monitoring of the “Detector …” object can be enabled here.

During cyclical monitoring, the object expects a telegram at regular intervals. If no telegram is received during the monitoring period, it has the same effect as if the detector had been triggered. The monitoring period is defined in the “Detectors” parameter window.

The parameter is visible if the value “no” is set in the parameter “Detector object monitors slave report”.

Object is disabled by

It can be set here which disable object can disable the detector. A disabled detector does not trigger any alarms. If *no disabling* is set here, the detector cannot be disabled in principle.

The parameter is visible if the value “no” has been set in the parameter *Detector object monitors slave report*.

Receives collective message of a slave

It can be set here, whether the object receives a telegram as a collective message from a Security Module in operating mode “Slave” (option *yes*).

The parameter is necessary because of the following reason:
A collective message from a slave device is handled differently regarding the storing in the event list memory. A slave’s message is stored in the slave-device itself.

Further information about the function of master/slave mode can be found in section 4.2.2.

3.2.3 “Slave” mode

In slave mode, the Security Module is always subject to a central alarm device which is denoted as “master”. The slaves in this type of system only pre-evaluate the detectors.

The parameter windows “General” and “Function” are explained in section 3.2.1. Further explanations about master/slave mode can be found in section 4.2.2.

3.2.3.1 Parameter window: “Setting Status Texts”

The setting/unsetting is stored in the event list memory. In this parameter window, the texts can be defined. The setting state is communicated from the master to the slave via the communication objects “Status master”.

A maximum of 14 characters are possible.

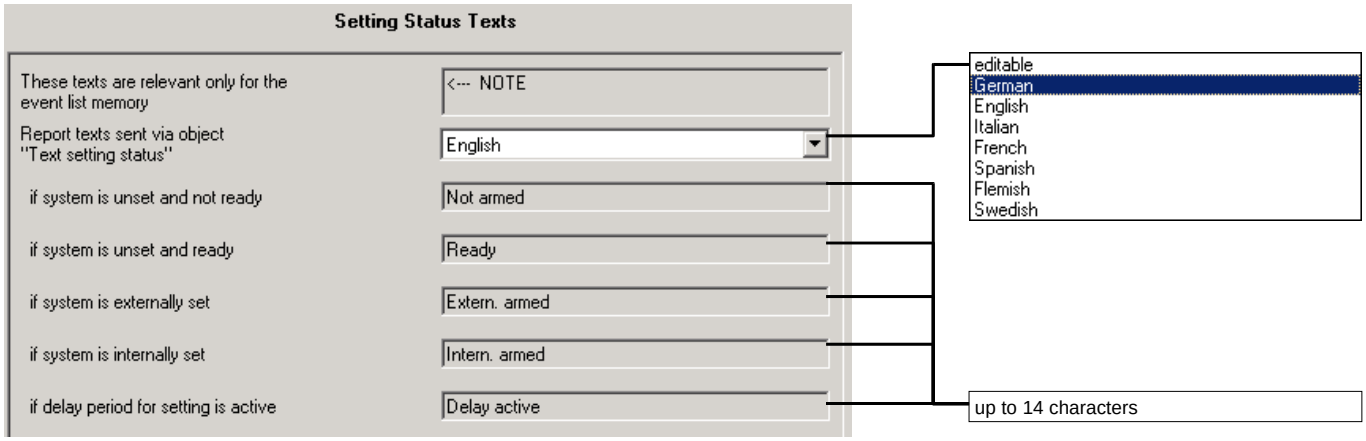


Fig. 14: Parameter window: “Setting Status Texts” (Slave mode)

Report texts sent via object “Text setting status”

Predefined texts for some languages can be selected here. With parameter value “editable” the texts can be edited.

if system is unset and not ready

The device is unset but not ready for setting because a message is present (e.g. a detector has been triggered or a reset has not been carried out after an alarm).

if system is unset and ready

The device is unset and can be set.

if system is externally set

The device is set externally i.e. all the internal and peripheral sensors are activated.

if system is internally set

The device is set internally i.e. only the peripheral sensors are activated.

if delay period for setting is active

The delay period for setting is active. This parameter is only relevant if delayed setting has been selected.

3.2.3.2 Parameter window: “Alarm Texts”

This parameter window is visible if the clear text display has been enabled (see parameter window “Function”).

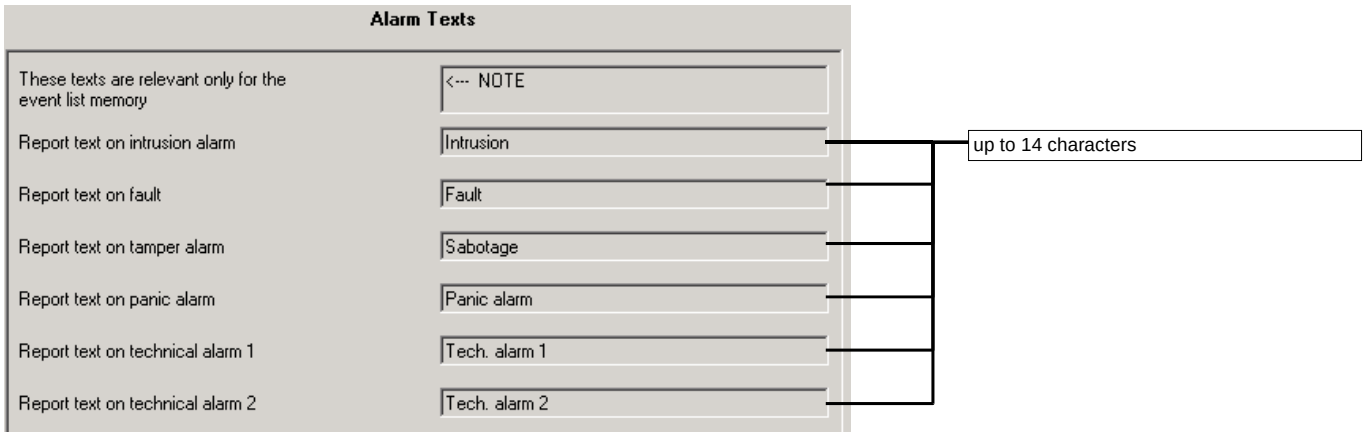


Fig. 15: Parameter window: “Alarm Texts” (Slave mode)

Predefined texts for some languages can be selected in parameter window “Setting status texts”. With parameter value “editable” the texts can be edited.

Report text on intrusion alarm

...

Report text on technical alarm 2

This parameter sets which report texts are stored for different alarms in the event list memory of this device.

3.2.3.3 Parameter window: “Detector Inputs”

The detectors are enabled and the cyclical monitoring period is set in this parameter window.

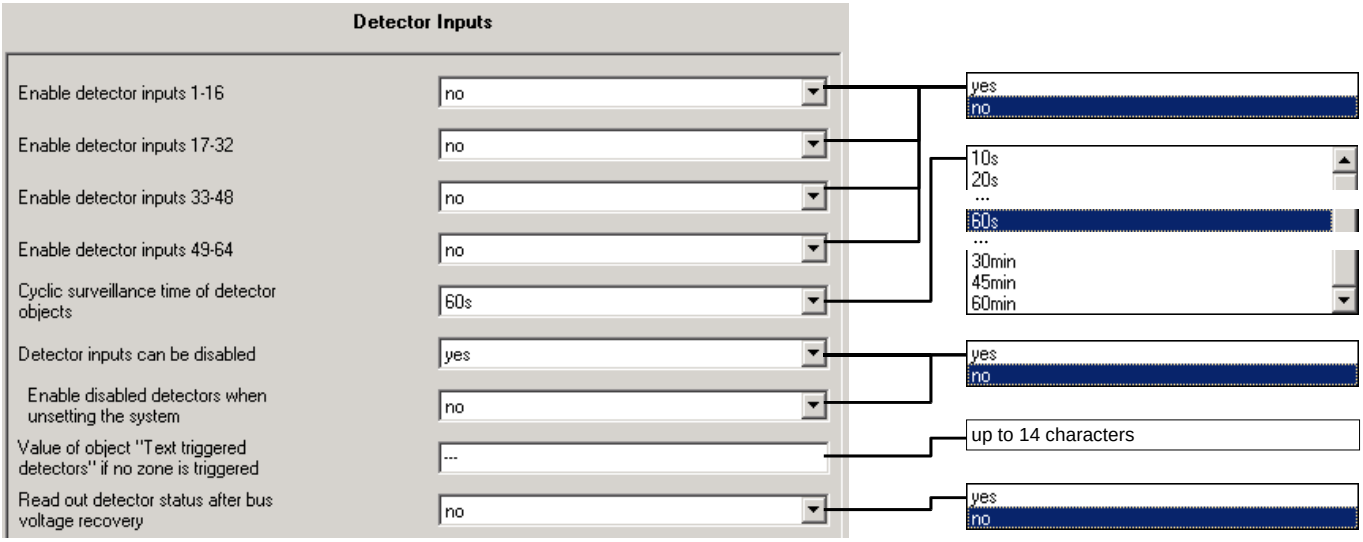


Fig. 16: Parameter window: “Detectors” (Slave mode)

Enable detectors 1-16

...

Enable detectors 49-64

16 detectors can be enabled each time in these 4 parameters. When they are enabled, the corresponding parameter windows “Detector…” appear in which the detector settings can be carried out.

Cyclic surveillance time of detector objects

The period for the cyclical monitoring of the detectors is set here.

When cyclic surveillance is active, a regular telegram is expected from a detector object within the monitoring period. If there is no telegram, it has the same effect as if the detector had been triggered.

Caution: The monitoring period should be at least twice as long as the cyclic transmission time of the detectors. Please note the bus load when the detectors are monitored cyclically.

It is possible to set in the parameter windows “Detector 01-02” …”Detector 63-64” whether a detector is monitored cyclically or not.

Detectors can be disabled

Detectors can be disabled here. Disabled detectors behave as if they are never triggered.

15 detector disable objects are enabled with this parameter. In the parameter “Detector object is disabled by” (parameter window “Detector 01-02” ... ”Detector 63-64”), each detector can be assigned to a disable object.

Enable disabled detectors on unsetting the system

If this parameter is set to “yes”, all the disabled detectors are switched on again when the system is unset. It is thus possible to prevent a detector for example unintentionally being permanently disabled.

Value of object “Text triggered detectors” if no detector is triggered

This parameter defines what is shown in the text display if no detectors have been triggered.

Via the objects “Read list of triggered detectors” and “Text triggered detector”, the user can display the names of the detectors which have just been triggered in clear text.

This parameter is visible if the 14-byte report texts have been enabled (parameter window “Function”).

Read out detector status after bus voltage recovery

The device can read out the status of detectors automatically after bus voltage recovery. This is advisable for example if the detectors cannot send their state themselves and their current status is therefore unknown after bus voltage recovery. Further information can be found in section 4.7.

3.2.3.4 Parameter window: ”01-02” ... “63-64”

These parameter windows are visible if they have been enabled in the “Detectors” parameter window. The function of two “Detector …” objects is defined in each window. All 64 detectors have the same functional scope.

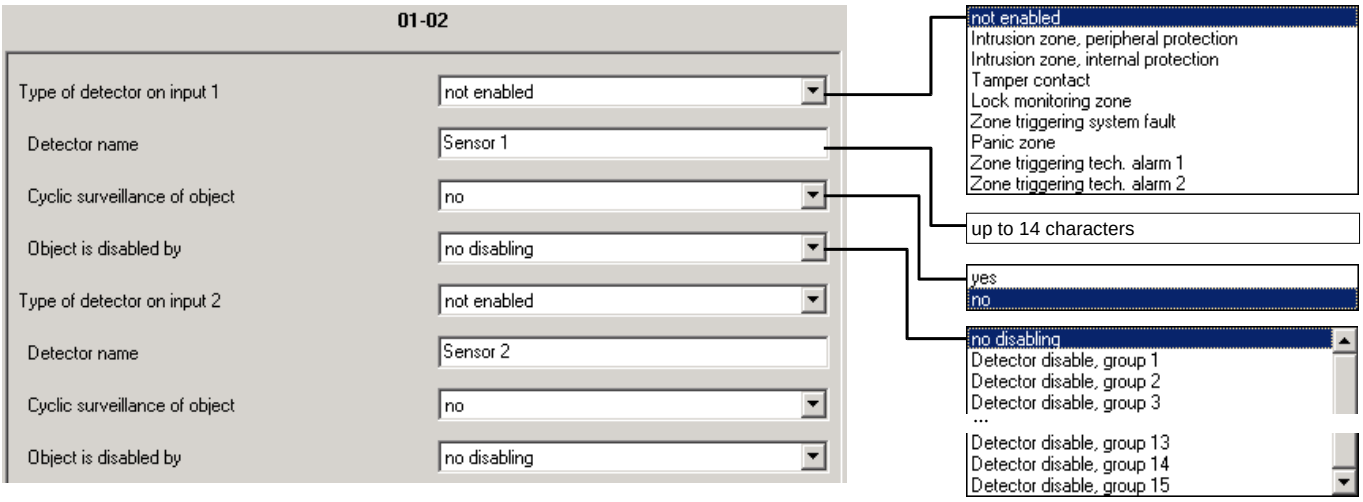


Fig. 17: Parameter window: “01-02” (Slave mode)

Type of detector on input ...

This parameter defines the type of detector which is assigned to the object “Detector input …”.

According to this setting, the detector input is assigned to one of the collective messages.

Detector name

The name of the detector is defined here. This name is written e.g. into the event list memory if this detector triggers an alarm. If the detector name is empty (only spaces), nothing is sent.

Cyclic surveillance of detector object

The cyclical monitoring of the “Detector …” object can be enabled here.

During cyclical monitoring, the object expects a telegram at regular intervals. If no telegram is received during the monitoring period, it has the same effect as if the detector had been triggered. The monitoring period is defined in the “Detectors” parameter window.

The parameter is visible if the value “no” is set in the parameter “Detector object monitors slave report”.

Detector object is disabled by

It can be set here which disable object can disable the detector. A disabled detector does not trigger any alarms. If “no disabling” is set here, the detector cannot be disabled in principle.

3.3 Communication objects

3.3.1 Objects for “Master mode”

Objects for the event list memory and for displaying triggered detectors

No	Function	Object name	Data type	Flags
0	**Request time/date**	**Event list memory**	**1 bit (EIS1) DPT 1.002**	**C, T**
The Security Module can request the current time and date from a master clock via this object after bus voltage recovery. To do so, it sends the object value “1”. This is necessary if the master clock does not send it automatically. The object is enabled by the parameter “Updating internal time and date after bus voltage recovery” (“Function” parameter window).				
1	**Input time**	**Event list memory**	**3 byte (EIS3) DPT 10.001**	**C, W, U**
The device receives the current time from a central clock via this object. The time is required for the event list memory of the device. The object is visible if parameter “Sending the system state and alarms via report texts” is set to “yes”.				
2	**Input date**	**Event list memory:**	**3 byte (EIS4) DPT 11.001**	**C, W, U**
The device receives the current date from a central clock via this object. The time is required for the event list memory of the device. The object is visible if parameter “Sending the system state and alarms via report texts” is set to “yes”.				
3	**Open event list memory**	**Event list memory**	**1 bit (EIS1) DPT 1.010**	**C, W**
With the help of this object, the latest entry in the event list memory is displayed via the objects “Text name of event”, “Text name of detector” and “Text date/time”. 0 : Close event list memory The text display is deleted (overwritten with spaces) 1 : Open event list memory The latest event is shown in the text display. The object is visible if the clear text display function has been enabled.				
4	**Read up/down**	**Event list memory**	**1 bit (EIS1) DPT 1.008**	**C, W**
It is possible to browse through the event list memory with this object. The text display is carried out via the objects “Text name of event”, “Text name of detector” and “Text date/time”. 0 : Read previous (earlier) entry of the event list 1 : Read next (older) entry of the event list If the oldest entry is reached, the display returns to the latest entry (and vice versa). The object is visible if the clear text display function has been enabled.				
5	**Text name of event**	**Event list memory**	14 byte (EIS15) **DPT 16.000**	**C, R, T**
First part of an entry in the event list memory. It contains the type of event such as the name of the alarm (as entered in the parameters). Character format: ASCII. The object is visible if the clear text display function has been enabled.				
6	**Text name of detector**	**Event list memory**	14 byte (EIS15) **DPT 16.000**	**C, R, T**
Second part of an entry in the event list memory. It generally contains the name of the relevant detector (as entered in the parameters). If the event was not triggered by a detector, the object sends spaces. Character format: ASCII. The object is visible if the clear text display function has been enabled.				

No	Function	Object name	Data type	Flags
7	**Text date/time**	**Event list memory**	14 byte (EIS15) **DPT 16.000**	**C, R, T**
Third part of an event in the event list memory. It contains the time and date when the event occurred. The date format can be set in the parameters. Character format: ASCII. The object is visible if the clear text display function has been enabled.				
8	**Read list of triggered detectors**	**Detector surveillance**	**1 Bit (EIS1)** **DPT 1.008**	**C, W**
Requests a further text entry from the list of triggered detectors. The text is sent by the object “Text triggered detector”. The object is visible if the function “Report texts” is enabled (“Function” parameter window).				
9	**Text triggered detector**	**Detector surveillance**	14 Byte (EIS15) **DPT 16.000**	**C, R, T**
Sends the name of a detector which has just been triggered on the bus and thus prevents the system being set. The object value is requested by the object “Read list of triggered detectors”. If several detectors have been triggered, the object always sends the next entry in the list. If no detectors have been triggered, the text from the parameter “Value of object ‘Text triggered detectors’ if no detector is triggered” (“Detectors” parameter window) is displayed. Character format: ASCII. The object is visible if the function “Report texts” is enabled (“Function” parameter window).				

Objects for “Setting/unsetting”

No	Function	Object name	Data type	Flags
10	**Internal setting/unsetting**	**Setting/unsetting**	**1 bit (EIS1)** **DPT 1.001**	**C, W, T**
Used for setting/unsetting the system internally (only peripheral sensors are set). 0 : “Unset” request 1 : “Set” request If the device is not ready to set, this object will send back a “0”-value after receiving a “1”. This will happen if - a detector is triggerd - a reset was not carried out after an alarm A technical detector will not prevent the setting.				
11	**External setting/unsetting**	**Setting/unsetting**	**1 bit (EIS1)** **DPT 1.001**	**C, W, T**
Use for setting/unsetting the system externally (internal and peripheral sensors are set). 0 : “Unset” request 1 : “Set” request If the device is not ready to set, this object will send back a “0”-value after receiving a “1”. This will happen if - a detector is triggerd - a reset was not carried out after an alarm A technical detector will not prevent the setting.				
12	**External setting, delayed**	**Setting/unsetting**	**1 bit (EIS1)** **DPT 1.001**	**C, W**
Used to request a delayed setting/unsetting of the system. If system is unset: 0 : Cancel delayed setting (end delay period) 1 : Request delayed setting (start delay period) If system is set: 0: Unset immediately 1: No reaction				

No	Function	Object name	Data type	Flags
13	**Delay time is active**	**Setting/unsetting**	**1 bit (EIS1) DPT 1.002**	**C, T**
Indicates that the delay period is active (for delayed setting/unsetting) 0 : Delay period is not active 1 : Delay period is active				
14	**Enable setting/unsetting**	**Setting/unsetting**	**1 bit (EIS1) DPT 1.003**	**C, W**
Used to enable and disable the setting/unsetting function 0 : Disable setting/unsetting 1 : Enable setting/unsetting By default, this object has the value “1”. Application: e.g. for creating subordinated setting/unsetting areas: The Security Module can only be set once another Security Module has been set.				
15	**Status externally set**	**Setting/unsetting**	**1 bit (EIS1) DPT 1.002**	**C, T, R**
0 : The device is not set externally 1 : The device is set externally (internal and peripheral sensors)				
16	**Status internally set**	**Setting/unsetting**	**1 bit (EIS1) DPT 1.002**	**C, T, R**
0 : The device is not set internally 1 : The device is set internally (peripheral sensors only)				
17	**Status ext. or int. set**	**Setting/unsetting**	**1 bit (EIS1) DPT 1.002**	**C, T, R**
0 : The device is unset 1 : The device is set internally or externally				
18	**Status ready external setting**	**Setting/unsetting**	**1 bit (EIS1) DPT 1.002**	**C, T, R**
0 : The device is not ready to be set externally (e.g. external/internal set, detector triggered) 1 : The device is ready to be set externally				
19	**Status ready delayed setting**	**Setting/unsetting**	**1 bit (EIS1) DPT 1.002**	**C, T, R**
0 : The device is not ready for delayed setting 1 : The device is ready for delayed setting				
20	**Status ready internal setting**	**Setting/unsetting**	**1 bit (EIS1) DPT 1.002**	**C, T, R**
0 : The device is not ready to be set internally 1 : The device is ready to be set internally				
21	**Setting confirmation**	**Setting/unsetting**	**1 bit (EIS1) DPT 1.002**	**C, T**
Sends the telegram value “1” after external setting followed by a “0” after a parameterisable period. It is therefore possible to trigger e.g. an LED or a buzzer to signal to the user that the system has been set successfully.				
22	**Error during setting**	**Setting/unsetting**	**1 bit (EIS1) DPT 1.002**	**C, T**
To signal an error when operating the setting/unsetting device (“negative acknowledgement”). The object sends a “1” followed by a “0” after a parameterisable period. For delayed setting/unsetting, the object is sent with the value “1” if it is not possible to set the system once the delay period has elapsed (e.g. door is not locked). For normal setting/unsetting, the object is sent with the value “1” if an attempt to set the system has failed (e.g. because a window is still open).				
23	**Text setting status**	**Setting/unsetting**	14 byte (EIS15) **DPT 16.000**	**C, T, R**
Sends parameterisable clear text about the current setting/unsetting status.				

Objects for “Alarming”

No	Function	Object name	Data type	Flags
24	**External strobe light**	**Alarming**	**1 bit (EIS1)** **DPT 1.001**	**C, T, R**
Used to control an external strobe light 0 : Strobe light is switched off 1 : Strobe light is switched on				
25	**External siren**	**Alarming**	**1 bit (EIS1)** **DPT 1.001**	**C, T, R**
Used to control an external siren 0 : Siren is switched off 1 : Siren is switched on In contrast to the strobe light, the siren always has a time limit. The duration can be parameterised.				
26	**Internal siren**	**Alarming**	**1 bit (EIS1)** **DPT 1.001**	**C, T, R**
Used to control an internal signalling device (e.g. siren or horn) 0 : Internal signalling device is switched off 1 : Internal signalling device is switched on				
27	**Telegr. intrusion alarm**	**Alarming**	**1 bit (EIS1)** **DPT 1.002**	**C, T, R**
Indicates an intruder alarm. On an intrusion alarm the object value is set to “1”. After a reset the object value is reset to “0”.				
28 **29**	**Telegr. technical alarm 1** **Telegr. technical alarm 2**	**Alarming**	**1 bit (EIS1)** **DPT 1.002**	**C, T, R**
Indicate a technical alarm. On an technical alarm the object value is set to “1”. After a reset the object value is reset to “0”.				
30	**Telegr. panic alarm**	**Alarming**	**1 bit (EIS1)** **DPT 1.002**	**C, T, R**
Indicates a panic alarm. On a panic alarm the object value is set to “1”. After a reset the object value is reset to “0”.				
31	**Telegr. tamper alarm**	**Alarming**	**1 bit (EIS1)** **DPT 1.002**	**C, T, R**
Indicates a tamper alarm. On a tamper alarm the object value is set to “1”. After a reset the object value is reset to “0”.				
32	**Telegr. fault**	**Alarming**	**1 bit (EIS1)** **DPT 1.002**	**C, T, R**
Indicates a fault. On a fault, the object value is set to “1”. - If the fault was caused by a bus voltage failure: The object value can be set to “0” by object “Reset”. - If the fault was caused by a detector of the type “Detector triggering system fault”: The object value is automatically set to “0”, after the cause of the fault is fixed.				
33	**Text name of alarm**	**Alarming**	14 byte (EIS15) **DPT 16.000**	**C, T, R**
Sends parameterisable clear text about the type of alarm when an alarm is triggered (e.g. “Intrusion”). If several types of alarm are triggered at the same time, this object will send each type sequentially in a period of 3 seconds.				

No	Function	Object name	Data type	Flags
34	**Text alarming detector**	**Alarming**	14 byte (EIS15) **DPT 16.000**	**C, T, R**
Sends parameterisable clear text with the name of the detector which has triggered this alarm.				
35	**Reset**	**Alarming**	**1 bit (EIS1)** **DPT 1.001**	**C, W**
Used to reset an alarm or a fault (telegram value “1”). The reset is only possible when the system is unset.				
36	**Tamper reset**	**Alarming**	**1 bit (EIS1)** **DPT 1.001**	**C, W**
Used to reset a tamper alarm. The reset is possible only when the system is unset. If this object is not enabled, a tamper alarm is reset via the object “Reset request”.				
37	**Status reset**	**Alarming**	**1 bit (EIS1)** **DPT 1.002**	**C, W**
This object indicates that the device has just carried out a reset. During the reset, it has the value “1”, otherwise it has the value “0”. A reset lasts approx. one second.				

Objects for the Telephone Gateway

No	Function	Object name	Data type	Flags
38	**Intrusion**	**Telephone Gateway**	**1 bit (EIS1)** **DPT 1.002**	**C, T, R**
Reports an intruder alarm to the Telephone Gateway. 0 : No alarm 1 : Alarm				
39 **40**	**Telegr. technical alarm 1** **Telegr. technical alarm 2**	**Telephone Gateway**	**1 bit (EIS1)** **DPT 1.002**	**C, T, R**
Reports a technical alarm to the Telephone Gateway. 0 : No alarm 1 : Alarm				
41	**Telegr. panic alarm**	**Telephone Gateway**	**1 bit (EIS1)** **DPT 1.002**	**C, T, R**
Reports a panic alarm to the Telephone Gateway. 0 : No alarm 1 : Alarm				
42	**Telegr. tamper alarm**	**Telephone Gateway**	**1 bit (EIS1)** **DPT 1.002**	**C, T, R**
Reports a tamper alarm to the Telephone Gateway. 0 : No alarm 1 : Alarm				
43	**Telegr. fault**	**Telephone Gateway**	**1 bit (EIS1)** **DPT 1.002**	**C, T, R**
Reports a fault to the Telephone Gateway. 0 : No alarm 1 : Alarm				

Objects for “Detector surveillance”

No	Function	Object name	Data type	Flags

No	Function	Object name	Data type	Flags
44 ... 107	**Input telegram ... Input telegram**	**Detector input 1 … Detector input 64**	**1 bit (EIS1) DPT 1.001**	**C, W**
Detector inputs. 0 = Detector OK 1 = Detector has been triggered **The object may only be linked with one group address.**				
108 ... 122	**Detector disable, group 1 ... Detector disable, group 15**	**Detector surveillance**	**1 bit (EIS1) DPT 1.001**	**C, W**
Detectors can be disabled via these objects. A detector can be assigned to any disable object in the parameters. 0: Detector is not disabled (normal function) 1: Detector is disabled and behaves as if it is always OK.				
123	**Status detector disabled**	**Detector surveillance**	**1 bit (EIS1) DPT 1.002**	**C, W**
This object indicates whether a detector has been disabled (“1”) or whether all the detectors are enabled (“0”). 0: All objects “Detector disable, group …” have value “0”. 1: At least one object “Detector disable, group …” has value “1”.				
124 … 131	**Report list entry**	**Event list slave 1 … Event list slave 8**	**1 Byte DPT 5.010**	**C, T**
This object is used if a master is working together with one or more slaves. Via this object, the master receives the information, that the slave has stored a new event in the event list memory. The object value contains the address of the event in the list (0...249).				
132 … 139	**Read list entry**	**Event list slave 1 … Event list slave 8**	**1 Byte DPT 5.010**	**C, T**
This object is used if a master is working together with one or more slaves. It is used to read out an entry in the event list memory of the slave device. The object value contains the address of the event in the list (0...249).				
125	**Telegr. life signal**	**General**	**1 bit (EIS1) DPT 1.001**	**C, R, T**
This object reports a life signal by being sent cyclically on the bus. It further indicates whether the device has a fault. 0 : No fault 1 : Device is faulty				
141	**Switch on/off**	**Buzzer**	**1 bit (EIS1) DPT 1.001**	**C, W, T**
Controls the internal buzzer of the device. 0 : Buzzer is switched off 1 : Buzzer is switched on				
142	**Switch**	**Relay output**	**1 bit (EIS1) DPT 1.001**	**C, W, T**
Used to control the relay; can be inverted via parameters. Normally open contact (normal mode): 0: Contact is open 1: Contact is closed Normally closed contact (inverted mode): 0: Contact is closed 1: Contact is open				

3.3.2 Objects for “Slave mode”

Examples for the object assignments between the master and slave can be found in section 4.2.2.

Objects for the event list memory and for displaying triggered detectors

No	Function	Object name	Data type	Flags
0	**Request date/time**	**Event list memory**	**1 bit (EIS1) DPT 1.002**	**C, T**
The Security Module can request the current time and date from a master clock via this object after bus voltage recovery. To do so, it sends the object value “1”. This is necessary if the master clock does not send it automatically. The object is enabled by the parameter “Updating internal time and date after bus voltage recovery” (“Function” parameter window). **This object must be assigned the same group address as the master.**				
1	**Input time**	**Event list memory**	**3 byte (EIS3) DPT 10.001**	**C, W, U**
The device receives the current time from a central clock via this object. The object is visible if the clear text display function has been enabled. **This object must be assigned the same group address as the master.**				
2	**Input date**	**Event list memory**	**3 byte (EIS4) DPT 11.001**	**C, W, U**
The device receives the current date from a central clock via this object. The object is visible if the clear text display function has been enabled. **This object must be assigned the same group address as the master.**				
3	**Open event list memory**	**Event list memory**	**1 bit (EIS1) DPT 1.010**	**C, W**
With the help of this object, the latest entry in the event list memory is displayed via the objects “Text name of event”, “Text name of detector” and “Text date/time”. 0 : Close event list memory The text display is deleted (overwritten with spaces) 1 : Open event list memory The latest event is shown in the text display. The object is visible if the clear text display function has been enabled. Normally, this object must not be used since the reading of the event list memory is controlled by the master. When it is used, it only shows the events of the slave device.				
4	**Read up/down**	**Event list memory**	**1 bit (EIS1) DPT 1.008**	**C, W**
It is possible to browse through the event list memory with this object. The text display is carried out via the objects “Text name of event”, “Text name of detector” and “Text date/time”. 0 : Read previous (earlier) entry of the event list 1 : Read next (older) entry of the event list If the oldest entry is not reached, the display returns to the latest entry (and vice versa). The object is visible if the clear text display function has been enabled. Normally, this object must not be used since the reading of the event list memory is controlled by the master. When it is used, it only shows the events of the slave device.				
5	**Text name of event**	**Event list memory**	14 byte (EIS15) **DPT 16.000**	**C, R, T**
First part of an entry in the event list memory. It contains the type of event such as the name of the alarm (as entered in the parameters). Character format: ASCII. The object is visible if the clear text display function has been enabled. **This object must be assigned the same group address as the master.**				

No	Function	Object name	Data type	Flags
6	**Text name of detector**	**Event list memory**	14 byte (EIS15) **DPT 16.000**	**C, R, T**
Second part of an entry in the event list memory. It generally contains the name of the relevant detector (as entered in the parameters). If the event was not triggered by a detector, the object sends spaces. Character format: ASCII. The object is visible if the clear text display function has been enabled. **This object must be assigned the same group address as the master.**				
7	**Text date/time**	**Event list memory**	14 byte (EIS15) **DPT 16.000**	**C, R, T**
Third part of an event in the event list memory. It contains the time and date when the event occurred. The date format can be set in the parameters. Character format: ASCII. The object is visible if the clear text display function has been enabled. **This object must be assigned the same group address as the master.**				
8	**Read list of triggered detectors**	**Detector surveillance**	**1 bit (EIS1) DPT 1.008**	**C, W**
Requests a further text entry from the list of triggered detectors. The text is sent by the object “Text triggered detector”. The object is visible if the function “Report texts” is enabled (“Function” parameter window). **The display of triggered detectors is carried out without dependence on the master and must be assigned its own group address.**				
9	**Text triggered detector**	**Detector surveillance**	14 byte (EIS15) **DPT 16.000**	**C, R, T**
Sends the name of a detector which has just been triggered on the bus and thus prevents the system being set. The object value is requested by the object “Read list of triggered detectors”. If several detectors have been triggered, the object always sends the next entry in the list. If no detectors have been triggered, the text from the parameter “Value of object ‘Text triggered detectors’ if no detector is triggered” (“Detectors” parameter window) is displayed. Character format: ASCII. The object is visible if the function “Report texts” is enabled (“Function” parameter window). **The display of triggered detectors is carried out without dependence on the master and must be assigned its own group address.**				

Objects for “Collective message”

No	Function	Object name	Data type	Flags
14	**Intrusion (peripheral detector)**	**Collective message of slave**	**1 bit (EIS1) DPT 1.005**	**C, R, T**
This object puts together all the detectors of type “Intrusion detector (peripheral protection)” and routes the information to the master. 0: Detector OK 1: Detector has been triggered				
15	**Intrusion (internal detector)**	**Collective message of slave**	1 bit (EIS1) **DPT 1.005**	**C, R, T**
This object puts together all the detectors of type “Intrusion detector (internal protection)” and routes the information to the master. 0: Detector OK 1: Detector has been triggered				
16	**Tamper**	**Collective message of slave**	1 bit (EIS1) **DPT 1.005**	**C, R, T**
This object puts together all the detectors of type “Tamper contact” and routes the information to the master. 0: Detector OK 1: Detector has been triggered				

No	Function	Object name	Data type	Flags
17	**Lock monitoring**	**Collective message of slave**	1 bit (EIS1) **DPT 1.005**	**C, R, T**
This object puts together all the detectors of type “Lock monitoring” and routes the information to the master. 0: Detector OK 1: Detector has been triggered				
18	**System fault**	**Collective message of slave**	1 bit (EIS1) **DPT 1.005**	**C, R, T**
This object puts together all the detectors of type “System fault” and routes the information to the master. 0: Detector OK 1: Detector has been triggered				
19	**Panic**	**Collective message of slave**	1 bit (EIS1) **DPT 1.005**	**C, R, T**
This object puts together all the detectors of type “Panic alarm” and routes the information to the master. 0: Detector OK 1: Detector has been triggered				
20	**Technical alarm 1**	**Collective message of slave**	1 bit (EIS1) **DPT 1.005**	**C, R, T**
This object puts together all the detectors of type “Technical alarm 1” and routes the information to the master. 0: Detector OK 1: Detector has been triggered				
21	**Technical alarm 2**	**Collective message of slave**	1 bit (EIS1) **DPT 1.005**	**C, R, T**
This object puts together all the detectors of type “Technical alarm 2” and routes the information to the master. 0: Detector OK 1: Detector has been triggered				

Status objects to be linked with the master:

The following objects must be linked via a group address with the corresponding object of the master:

No	Function	Object name	Data type	Flags
10	**Internally set**	**Status master**	**1 bit (EIS1) DPT 1.002**	**C, W**
Via this object, the device learns from the master whether it is set internally. In this case, the storing of alarms is enabled for all peripheral sensors. **Link with the object “Status internally set” of the master.**				
11	**Externally set**	**Status master**	**1 bit (EIS1) DPT 1.002**	**C, W**
Via this object, the device learns from the master whether it is set externally. In this case, the storing of alarms is enabled for all intruder detectors. **Link with the object “Status externally set” of the master.**				
13	**Delay time is active**	**Status master**	**1 bit (EIS1) DPT 1.002**	**C, W**
Via this object, the device learns from the master whether the delay period is active. This is only relevant for delayed setting/unsetting. **Link with the object “Delay time is active” of the master.**				

No	Function	Object name	Data type	Flags
25	**Intrusion alarm**	**Status master**	**1 bit (EIS1) DPT 1.002**	**C, W**
The master informs the slave via this object that an intruder alarm has been triggered. No further intruder signals are stored in the event list memory until the alarm is reset. **Link with the object “Telegr. intrusion alarm” of the master.**				
26	**Technical alarm 1**	**Status master**	**1 bit (EIS1) DPT 1.002**	**C, W**
The master informs the slave via this object that an intruder alarm has been triggered. This prevents a further technical alarm signal 1 being stored in the event list memory until the alarm has been reset. **Link with the object “Telegr. technical alarm 1” of the master.**				
27	**Technical alarm 2**	**Status master**	**1 bit (EIS1) DPT 1.002**	**C, W**
The master informs the slave via this object that an intruder alarm has been triggered. This prevents a further technical alarm signal 2 being stored in the event list memory until the alarm has been reset. **Link with the object “Telegr. technical alarm 2” of the master.**				
28	**Panic alarm**	**Status master**	**1 bit (EIS1) DPT 1.002**	**C, W**
The master informs the slave via this object that an intruder alarm has been triggered. No further panic signals are stored in the event list memory until the alarm is reset. **Link with the object “Telegr. panic alarm” of the master.**				
29	**Tamper alarm**	**Status master**	**1 bit (EIS1) DPT 1.002**	**C, W**
The master informs the slave via this object that an intruder alarm has been triggered. No further tamper signals are stored in the event list memory until the alarm is reset. **Link with the object “Telegr. tamper alarm” of the master.**				
30	**System fault**	**Status master**	**1 bit (EIS1) DPT 1.002**	**C, W**
The master informs the slave via this object that an intruder alarm has been triggered. No further fault signals are stored in the event list memory until the alarm is reset. **Link with the object “Telegr. fault” of the master.**				

Objects for “Alarming”

33	**Text name of alarm**	**Alarming**	14 byte (EIS15) **DPT 16.000**	**C, T, R**
Sends parameterisable clear text about the type of alarm when an alarm is triggered. **This object must be assigned the same group address as the master.**				
34	**Text alarming detector**	**Alarming**	14 byte (EIS15) **DPT 16.000**	**C, T, R**
Sends parameterisable clear text with the name of the detector which has triggered this alarm. **This object must be assigned the same group address as the master.**				
35	**Reset**	**Status Master**	**1 bit (EIS1) DPT 1.002**	**C, W**
Receives the information from the master that a reset must be carried out. Used to reset an alarm (telegram value “1”) in the event of a fault. The object is visible if the parameter “System fault after bus voltage recovery” = yes. **Link with the object “Status reset” of the master.**				

Objects for “Detector surveillance”

No	Function	Object name	Data type	Flags
44 ... 107	**Detector 1 ... Detector 64**	**Detector surveillance**	**1 bit (EIS1) DPT 1.001**	**C, W**
Detector inputs: 0 = Detector OK 1 = Detector has been triggered **The object may only be linked with one group address.**				
108 ... 122	**Detector disable, group 1 ... Detector disable, group 15**	**Detector surveillance**	**1 bit (EIS1) DPT 1.001**	**C, W**
Detectors can be disabled via these objects. A detector can be assigned to any disable object in the parameters. 0 = Detector is not disabled (normal function) 1 = Detector is disabled and behaves as if it is always OK.				
123	**Status detector disabled**	**Detector surveillance**	**1 bit (EIS1) DPT 1.002**	**C, W**
This object indicates whether a detector has been disabled (“1”) or whether all the detectors are enabled (“0”).				
124	**Report list entry**	**Event list slave**	**1 byte DPT 5.010**	**C, T**
Via this object, the slave sends the information, that it has stored a new event in the event list memory. The object value contains the address of the event in the list (0...249).				
125	**Read list entry**	**Event list slave**	**1 byte DPT 5.010**	**C, W**
Via this object, the master reads out an entry in the event list memory of the slave device. The object value contains the address of the event in the list (0...249).				
140	**Telegr. life signal**	**General**	**1 bit (EIS1) DPT 1.001**	**C, R, T**
This object reports a life signal by being sent cyclically on the bus. It further indicates whether the device has a fault. 0 : No fault 1 : Device is faulty The object can be assigned to a detector of the master (e.g. of type “System fault”) via a group address. For further information, see section 4.2.2.				
141	**Switch on/off**	**Buzzer**	**1 bit (EIS1) DPT 1.001**	**C, W, T**
Controls the internal buzzer of the device. 0 : Buzzer is switched off 1 : Buzzer is switched on				
142	**Switch**	**Relay output**	**1 bit (EIS1) DPT 1.001**	**C, W, T**
Used to control the relay; can be inverted via parameters. Normally open contact (normal mode): 0: Contact is open 1: Contact is closed Normally closed contact (inverted mode): 0: Contact is closed 1: Contact is open				

4 Application and planning

4.1 Important notes

When setting up installations for issuing signals and alarms, the planning, installation and commissioning must be carried out with care. False alarms in particular must be avoided to prevent damage being caused.

Please observe the notes in section 5.2.

4.2 The operating modes

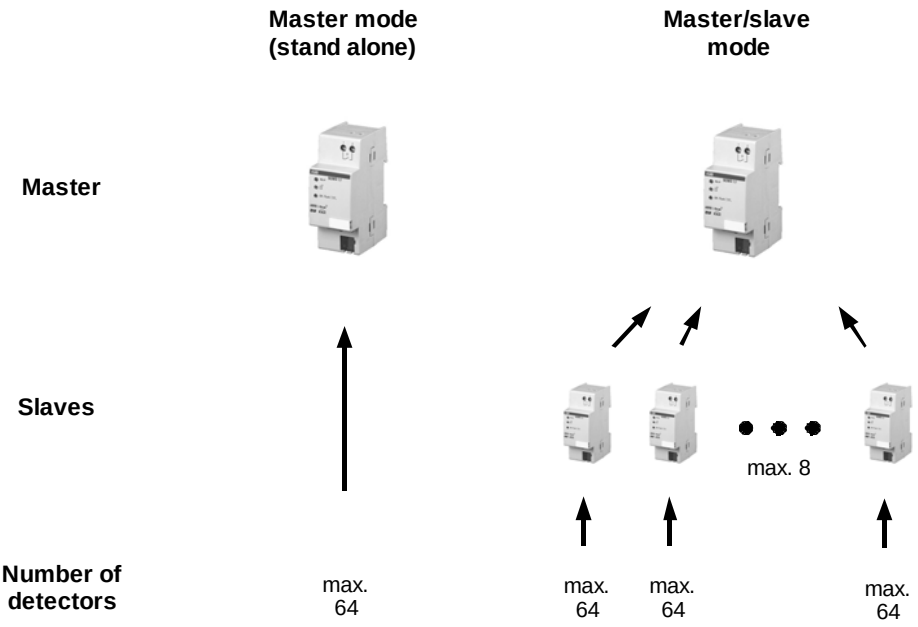


Fig. 18: “Master” and “Slave” mode

The operating modes are described in the following section.

4.2.1 Master mode (stand alone)

The “Master mode” is the standard operating mode. In this case, the Security Module operates alone (“stand alone”) and controls all the security functions. The master can monitor up to 64 detectors.

4.2.2 Master/slave mode

If the 64 detectors of the master are not sufficient, it can be supplemented by up to eight Security Modules (“slaves”). The functional principle is explained first in this section. The process for linking group addresses is then described with the aid of examples.

The slave is responsible for grouping together detectors while the master controls the setting/unsetting of the system and the issue of alarms. The following diagram provides an overview:

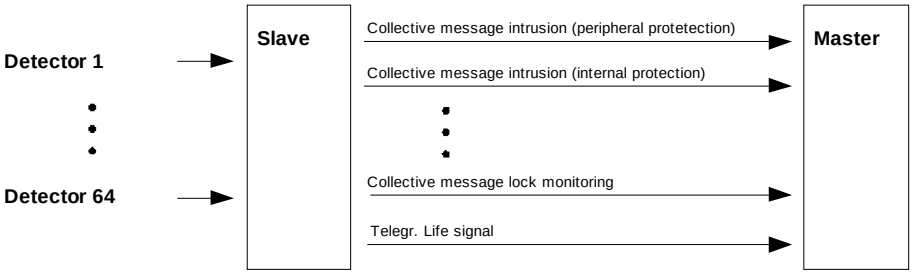


Fig. 19: Assembling together the detectors into collective messages

All the detectors of the same type are assembled together into a collective message in the slave. This corresponds to a logical OR function: If a detector has been triggered, the collective message is also triggered.

Eight different detector types can be set in the Security Module in slave mode:

- Intrusion detector: peripheral protection
- Intrusion detector: internal protection
- Tamper contact
- Lock monitoring detector
- System fault
- Panic detector
- Technical alarm 1
- Technical alarm 2

By assembling all the detectors of the same type into a collective message which is then routed to the master, one detector input is occupied in the master.

Example: All the detectors of type *Intrusion detector: peripheral protection* are grouped together in the slave and routed to the master detector input *Intrusion detector: peripheral protection*. The report text in the detector parameter window of the master should therefore be changed as follows to provide a better overview:
C-Intr.periph (for collective message *Intrusion: peripheral sensor*).

A master detector can only be occupied once e.g. only 63 out of the total of 64 detectors of the master remain freely available. The remaining detectors can be freely assigned (e.g. with local detectors), depending on the number of slave collective messages.

Example: A slave groups together all the detectors of type *Intrusion detector: peripheral protection*. If one of these detectors has the value “1”, the collective message *Intrusion: peripheral sensor* reports this to the detector of the master. The detector of the master must be parameterised as a slave message of type *Intrusion detector: peripheral protection*.

Settings of the master

When a detector input object of the master is used to receive a collective message of the slave, the parameter *Object monitors slave report* has to be set to *yes*.

Assignment of the group addresses

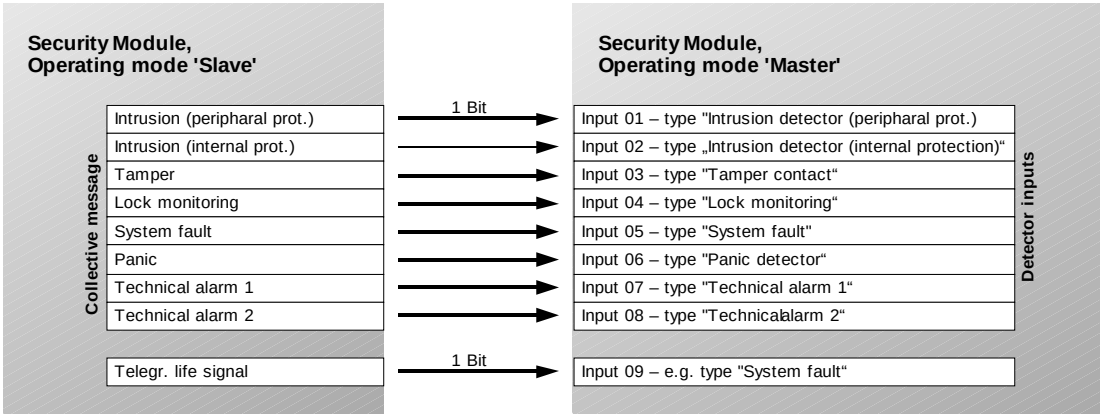


Fig. 20: Assignment of the objects from the slave to the master (example)

The diagram above shows the communication from the slave to the master. The objects are linked together via group addresses. If a slave does not use one or more detector types, the collective message does not need to be assigned.

The *“Life signal”* can be sent cyclically by the slave and monitored cyclically by the master. If a telegram is omitted (e.g. removal of the slave from the bus), a fault would then be triggered in the example above – alternatively another type of alarm is possible.

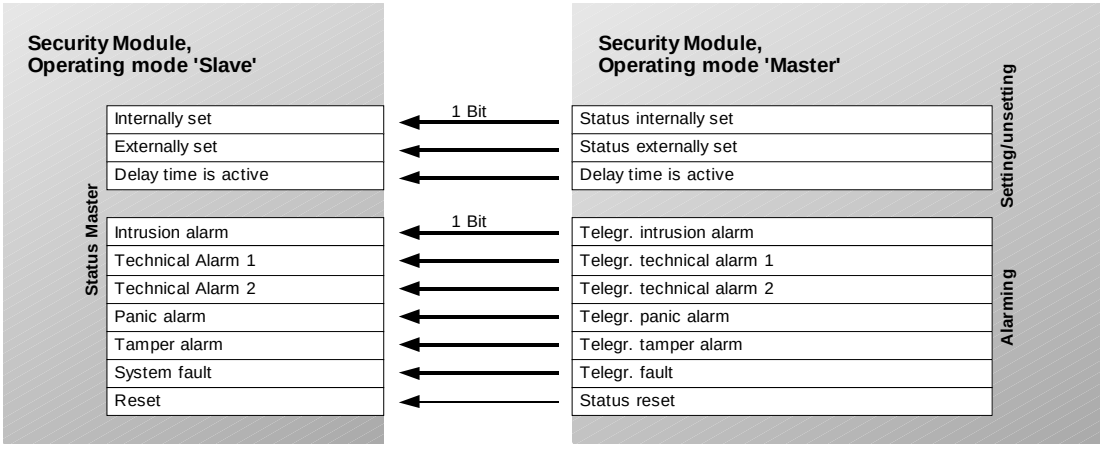


Fig. 21: Assignment of the objects from the master to the slave

The diagram above shows the communication from the master to the slave. The master the setting state and the alarm state to the slave. Thus the slave is informed, which events are to be stored in the event list memory.

The objects are linked together via group addresses. If an object is not visible, it does not need to be linked.

If several slaves are available, the master sends the objects to all the slaves at the same time – they are then linked with the same group address.

As it can be seen above, the master sends its setting and alarm status to the slave. The slave is therefore informed which signals should be stored in its event list memory.

The *"Reset"* object is used if the Security Module experiences a fault after bus voltage recovery. In this case, it can be reset by the master.

Reading out the event list memory

This section describes how the event list memory is read out in master/slave mode. The objects are assigned as follows between the master and slave:

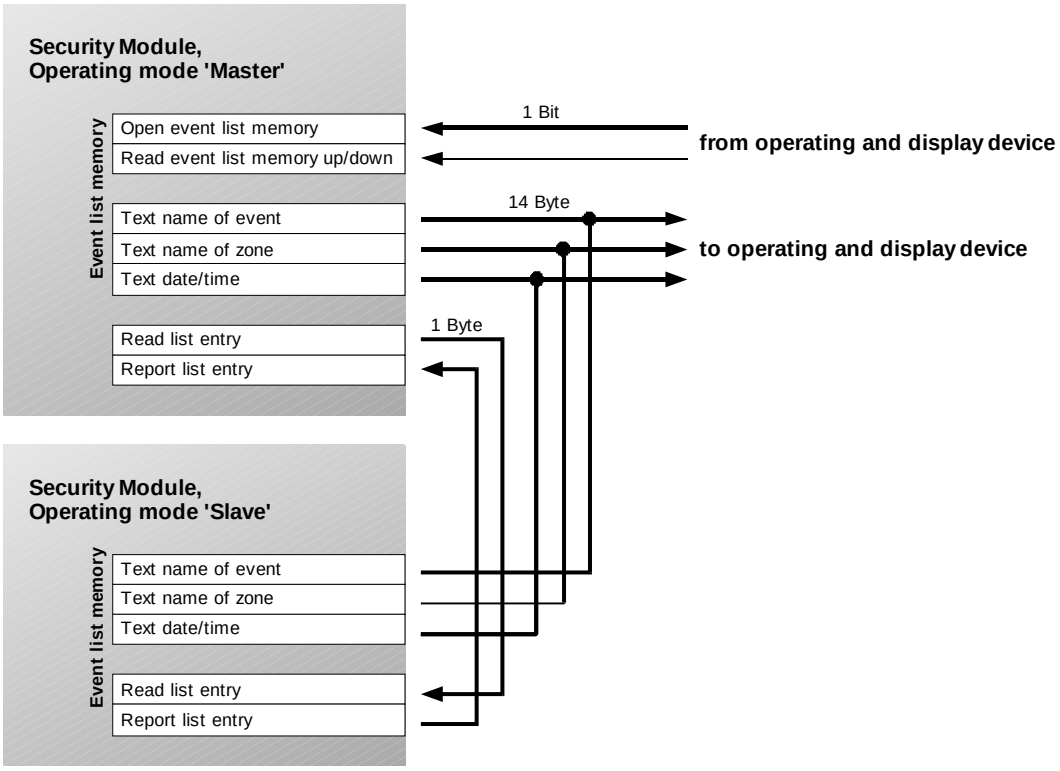


Fig. 22: Assignment of the objects for reading out the event list memory

The user can read out the event list memory via the objects *"Open event list memory"* and *"Read event list memory up/down"*.

The three *"Text..."* objects send to the same group address for the master and slave.

The object *"Coupling of slave devices"* is linked via a group address.

Time and date for the event list memory

To enter the time stamp in the event list memory, the Security Module requires the time and date at regular intervals (e.g. 1x daily).

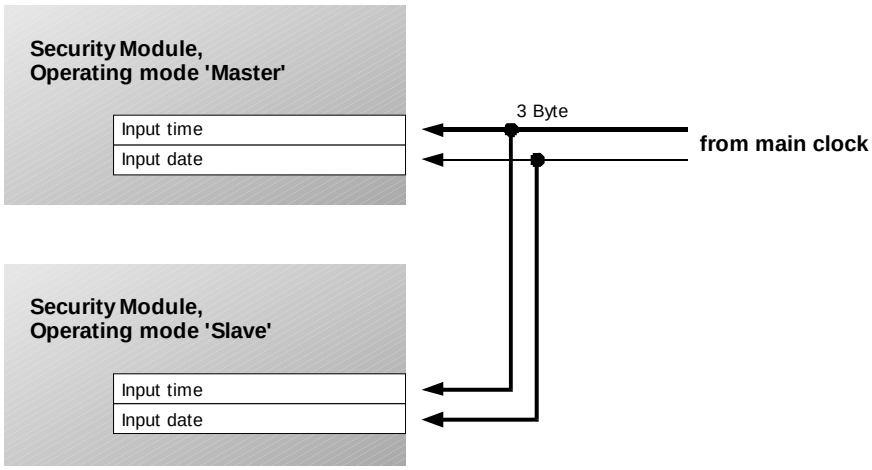


Fig. 23: Assignment of the objects “Date” and “Time”

Link *Input time* and *Input date* of all Security Modules tothe same group address.

Function of the event list memory in master/slave mode

Every incoming event is stored in the device, where it arrives first. In the master/slave mode it is normally the slave, because it receives the messages from the detectors.

Via the object *Report list entry* the slave informs the master, that a new event list entry is stored. For reading out the event list the master will recall the entry via the object *Read list entry.*

The following example explains the sequence:

1. The alarm system is set. Slave no. 2 receives a message at a detector of type *Intrusion detector: peripheral protection, delayed*.
2. The slave stores the event in its event list memory in list entry no. 20. Content:
   “Intruder alarm” – “Lounge” – “31.05.04 14:30”
3. The slave sends the value 1 via the object *Collective message – intrusion (peripheral detector)* to the master. The master triggers an alarm. After that, the slave sends the value “20” via the object *Report list entry* to the master.
4. The following event is stored in the event list memory of the master:
   “Slave #2” – “Address 20”

The sequence for reading out the event list memory is as follows:

1. The master receives the request from the display to send out an event list entry (via object *Event list memeory - Read up/down*).
2. The event list memory contains the above event which informs the master that the event of “Slave #2” has been stored in “Address 20”. The master then sends the object *Read list entry* on the bus with the value 20.

3. Slave no. 2 receives the object *Read list entry* and sends the following objects on the bus:
   - Object “Text name of event” = “Intruder alarm”
   - Object “Text name of detector” = “Lounge”
   - Object “Text date/time” = “31.05.04” “14:30”

List of triggered detectors

An important and convenient function is offered by the list of detectors which are currently preventing the system from being set. The user can e.g. browse through this list if the setting/unsetting device refuses to set the system.

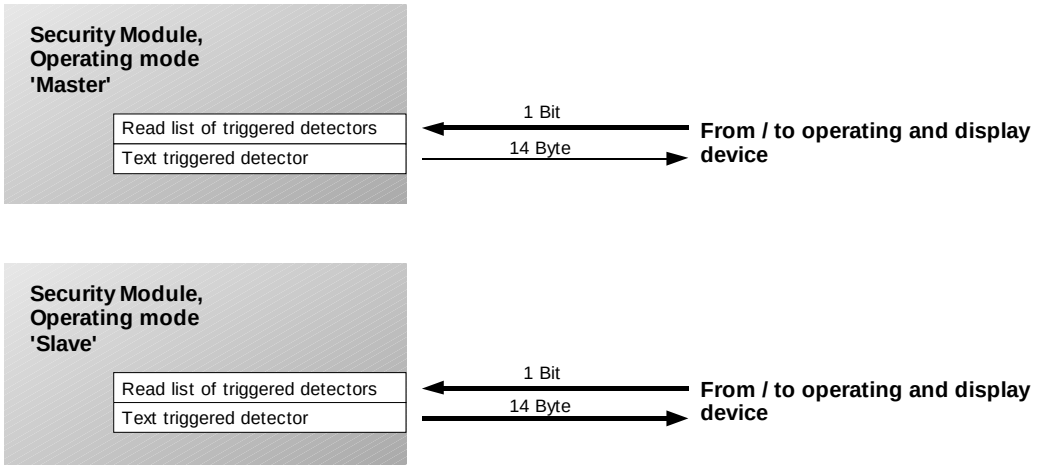


Fig. 24: Assignment of the objects for displaying the triggered detectors

The master and the slave are read out separately. There is no coupling via group addresses.

Alarm text

The alarm text “Text name of alarm” and “Text alarming detector” informs the user which alarm (e.g. intruder alarm) has been generated by which detector.

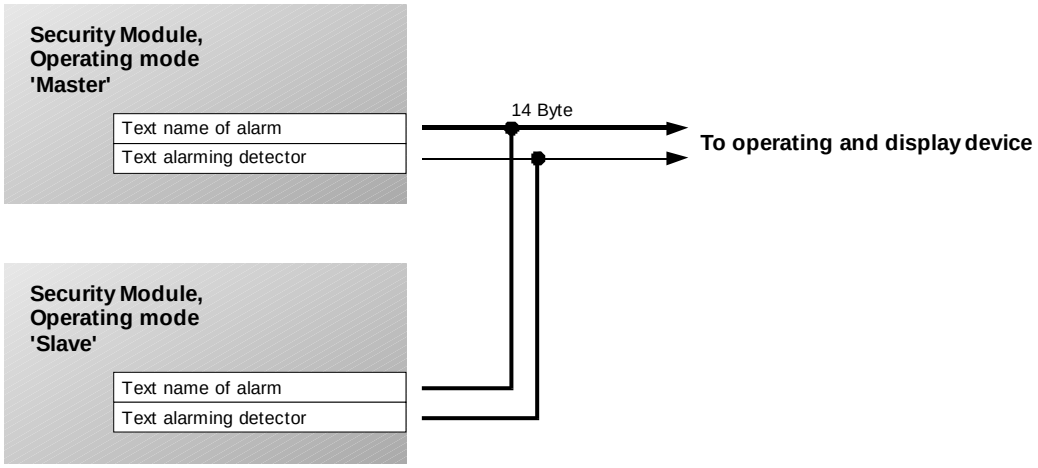


Fig. 25: Assignment of the objects for displaying the alarm text

In master/slave mode, the objects in the master and slave are assigned the same group address.

4.3 Detector evaluation

The Security Module has 64 detector objects which it uses to monitor the status of the detectors. Each of the objects is assigned a detector type which determines whether and how an alarm is triggered.

The following detector types are possible.

Detector type	Alarm
Intrusion detector: peripheral protection	Triggers an intruder alarm when the system is set internally or externally.
Intrusion detector: internal protection	Only triggers an intruder alarm when the system is set externally (e.g. motion detector)
IIntrusion detector: peripheral protection, delayed	Detector, which is disabled during the delay period when delayed setting/unsetting is selected, for example a door contact. Triggers an intruder alarm when the system is set internally or externally after run out of the delay time.
IIntrusion detector:internal protection, delayed	Detector, which is disabled during the delay period when delayed setting/unsetting is selected, for example a motion detector in the doorway. Triggers an intruder alarm when the system is set externally after run out of the delay time.
Tamper contact	Triggers a tamper alarm regardless of the setting/unsetting status. Used for example to signal a sabotage attempt on the alarm system.
System fault	Triggers a fault signal regardless of the setting status. A fault prevents the system from being set and is indicated via the flashing green LED on the device.
Panic detector	Triggers a panic alarm regardless of the setting status.
Technical alarm	Triggers a technical alarm (e.g. water, gas), regardless of the setting status.
Lock monitoring	Does not generally trigger an alarm but prevents the system from being set e.g. if the door has not been locked.

Table 1: Detector types

4.3.1 Integration of Zone Terminals

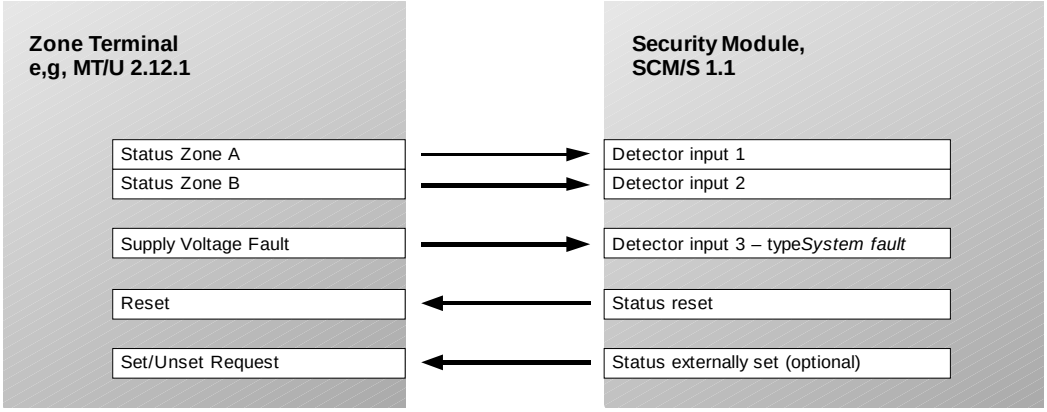


Fig. 26: Assignment of the objects to a Zone Terminal (example)

The diagram above shows the communication between a Security Module and a Zone Terminal. The objects are linked together via group addresses.

A signal is sent to a detector input object of type *System fault* via the object *Supply Voltage Fault*. The Zone Terminal can send a cyclical life signal to the Security Module via this object. In this case, the object *Supply Voltage Fault* must be sent cyclically and the detector must be monitored cyclically in the Security Module. The user is thus shown a fault signal which he must confirm by carrying out a reset.

The object *Status reset* of the Security Module **must** be assigned to the "Reset" object of the Zone Terminal. The Zone Terminal can be reset in this way (e.g. after a failure of the 12 V power supply).

The object *Status externally set* must then only be assigned to the object *Set/Unset Request* if the Zone Terminal should carry out the alarm memory function. A signal is not reset to "0" in the event of an alarm. It is therefore possible to determine at a later date which detectors were triggered during a break-in. In the example above, only peripheral sensors are connected to the Zone Terminal.

Note: A prerequisite for this function is that either only internal or only peripheral sensors are connected to the Zone Terminal.

4.3.2 Disabling detectors

For convenience purposes, detectors can be removed from the alarm system. For example, windows can be opened for ventilation while the alarm system is set internally. A disabled detector cannot trigger an alarm and also does not prevent the system from being set.

It is only possible to disable those detectors for which this function has been enabled in the parameterisation.

If any detector is disabled, this is indicated by the object "Status detector disabled".

15 disable objects

To be able to disable a detector, it is assigned to one of 15 disable objects in the parameters. If the disable object has the value "1", the detector object is deactivated.

Automatic restart

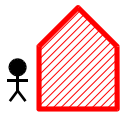
It can also be set in the parameters that all the disabled detectors are enabled again the next time the system is unset (see parameter window “Setting/Unsetting”). This prevents a detector from remaining inadvertently permanently disabled.

4.4 Setting/unsetting

The setting/unsetting device has a significant influence on the function and security of the alarm system. It should be protected against unauthorised operation.

4.4.1 External and internal setting

Internal setting



External setting

The Security Module distinguishes between internal and external setting. With *internal setting*, the user is located inside the building and only the peripheral sensors trigger an intruder alarm.

External setting is used when the user leaves the building. Both the internal and peripheral sensors are set.

With external setting, a distinction is made between “undelayed” and “delayed” setting.

Assignment of the objects

In the following example, the system is set/unset using a (primitive) setting/unsetting device in the form of a push button:

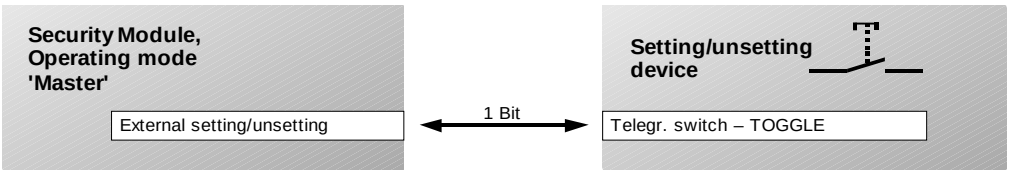


Fig. 27: Assignment of the objects for setting/unsetting (example)

After each operation of the push button, the object *Telegr. switch* inverts its value (TOGGLE).

If the Security Module is not ready for setting, it sends back the value “0” on the same group address. The switching object of the setting device is reset to “0” and is synchronous again with the setting status of the Security Module.

4.4.2 Normal setting/unsetting (no delay)

For “normal” setting/unsetting, the setting/unsetting device is mounted outside the security area (e.g. next to the entrance door).

If the building has several entrances, several setting/unsetting devices are possible.

Sequence diagram for setting

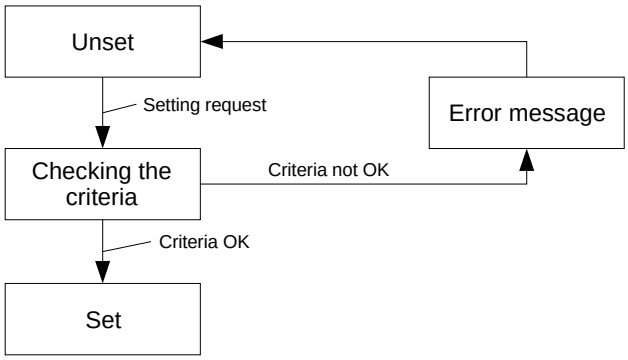


Fig. 28: Sequence for “normal” (undelayed) setting

1. The user sends an setting request via the object “External setting/unsetting”.
2. The setting/unsetting device checks the setting criteria. If one of the following criteria arises, the setting is aborted with an error signal:
   - a detector has been triggered (e.g. window open) *or*
   - the installation has a fault *or*
   - the installation has not yet been reset after an alarm

   In the event of an error signal, the object “Error during setting” is set to “1” for a parameterisable period. It is therefore possible to e.g. control a buzzer.
   NOTE: A detector triggering technical alarm will not prevent the setting!
3. If the criteria are met, the system is set.

4.4.3 Delayed setting

For delayed setting/unsetting, the setting/unsetting device is mounted *inside* the security area. The user triggers the setting there and a delay time is started, during which he can leave the building. The system is finally set once the period has elapsed or when locking the door. During the delay period, all the access detectors which lie on the route between the setting/unsetting device and the door are unset.

Sequence diagram for setting

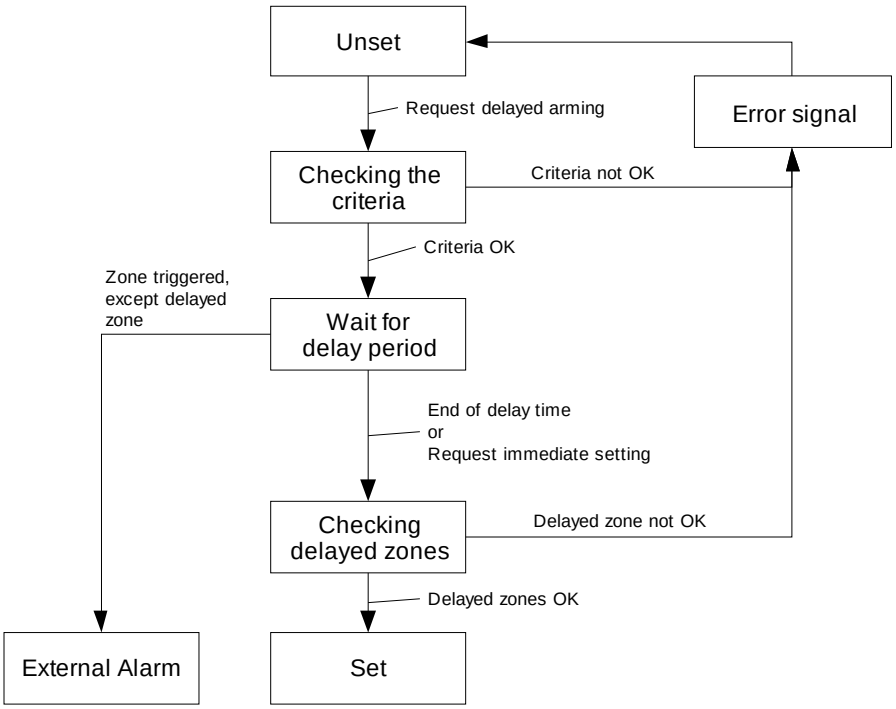


Fig. 29: Sequence for delayed setting

1. The user sends an setting request. The following setting criteria are checked. If
   - a detector has been triggered (e.g. open window)
   - the system has a fault or
   - the system has not been reset after an alarm

   the setting is interrupted with an error signal. An error signal can be displayed to the user (object “Error during setting” set to “1” for an adjustable period).
   NOTE: A detector triggering technical alarm will not prevent the setting!
2. The delay period is activated. All the detectors are set with the exception of the access detectors, which monitor the route from the setting/unsetting device to the door.
   The user can be warned via the object “Delay time is active”.
3. If a normal intrusion detector is triggered during the delay period, an external alarm is triggered.
4. The final setting is either carried out once the delay time has elapsed or if it has been parameterised, when closing the last open detector of type *Intrusion detector: peripheral protection, delayed*. The access detectors are checked beforehand. If one of them has been triggered, this is signalled by an error signal once the delay time has elapsed and no setting takes place.

Sequence diagram for unsetting

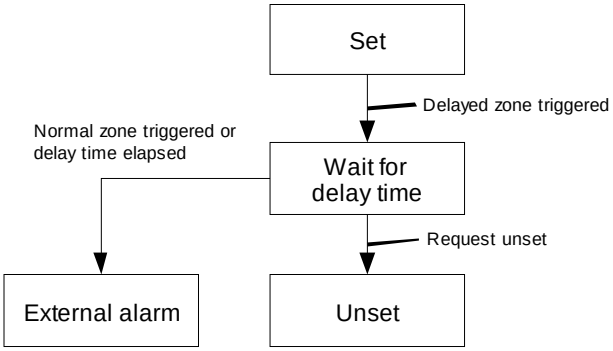


Fig. 30: Sequence for delayed unsetting

1. The user opens the door and thereby triggers an access detector of type *Intrusion detector: peripheral protection, delayed*. The delay time is thereby started.
2. All the access detectors are disabled during the delay period. If another set detector is disrupted, an alarm is triggered.
3. The user has the opportunity to unset the alarm system until the delay time has elapsed. Otherwise an intruder alarm is triggered.

4.4.4 Structure of security areas

One security area can be managed per Security Module.

The creation of sub areas is also possible by the logical connection of several Security Modules. A sub area must be set before the main area can be set.

This function can be implemented by linking the object “Status externally set” of the Security Module in the sub area with the object “Enable setting/unsetting” of the main area.

4.4.5 Further functions

If the alarm system is set internally, the user can unset the system via the external setting/unsetting device (when returning home late).

The user can see that the system has been set successfully via the object “Setting confirmation”. The object value is set to “1” for a parameterisable period and can e.g. control a buzzer.

4.5 Alarming

The alarming function informs the user depending on the type of message (detector type) and the setting status.

4.5.1 Signalling devices

The following signalling devices are provided:

Signalling device	Explanation
External siren and strobe light	A combination of signalling devices generally indicates a break-in or attempted sabotage if the system is set externally.
Internal siren	Indicates an alarm if the user is in the building i.e. the system is internally set or unset.
Telephone Gateway (dialling device)	Used for a silent alarm (e.g. in the event of a panic alarm) or for targeted remote signalling.
LCD display	The LCD display can signal an alarm or a fault via a buzzer if the user is in the building. The device indicates the type of alarm and detector in clear text.

Table 2: Possible signalling devices

Alarm via a signalling device

A signalling device is used for the visual or acoustic signalling of an alarm. It can e.g. be controlled via a switch actuator.

The signalling device is mounted indoors as an internal signalling device or outdoors as an external signalling device. The external signalling device consists of a strobe light and a siren. The latter is always controlled with a time limit by the Security Module.

Control of a Telephone Gateway (telephone dialling device)

An alarm can also be routed to a telephone with the help of a Telephone Gateway. The person who is called is informed about the type of alarm and can initiate the appropriate measures.

To make the issue of alarms via the Telephone Gateway as convenient and reliable as possible, the Security Module has its own object for each type of alarm.

4.5.2 Default settings

The type of alarming depends on the setting status and the type of detector which has triggered the alarm. The following table provides an overview of the default settings which can be modified in the parameters.

Type of signal	Setting status	Internal signalling device	External signalling device	Telephone Gateway
Intruder alarm	Int. set	yes	no	no
	Ext. set	no	yes	yes
Tamper alarm	Unset	yes	no	no
	Int. set	yes	no	no
	Ext. set	no	yes	yes
Fault	Irrelevant	no	no	yes
Panic alarm	Irrelevant	no	no	yes
Technical alarm 1	Unset	yes	no	no
	Int. set	yes	no	no
	Ext. set	no	no	yes
Technical alarm 2	Unset	yes	no	no
	Int. set	yes	no	no
	Ext. set	no	no	yes

Table 3: Default settings for alarms

“External signalling device” denotes the objects “External strobe light” and “External siren”.

4.5.3 Resetting alarms

The cancelling of an alarm by the user is denoted as a “reset”. The reset is carried out via the object “Reset”.

Note: To reset an alarm, the alarm system must be unset. This prevents a reset being carried out by an unauthorised person.

4.5.4 Faults

With a fault signal, the Security Module indicates that there is a problem with the function of the alarm system. In the event of a fault, the green LED on the device flashes and the object “Telegr. fault” is set to “1”.

A fault can either be triggered by a detector of type “System fault” or by a bus voltage failure.

A fault which has been triggered by a system fault detector is deleted again as soon as the detector has received the value “0” again.

If the fault signal was caused by a bus voltage failure, the signal must be cancelled via a reset.

4.5.5 Subsequent alarms

If a further alarm is triggered by another type of detector during an alarm (e.g. technical alarm), both alarms are displayed in parallel.

If an alarm is generated by another type of detector, the triggering of a further detector of the same type will lead to the alarm being repeated.

4.6 Storing events

The Security Module has an event list memory with 250 entries. When the number of 250 events is exceeded, the oldest event is overwritten by the newest event. The event list memory can be enabled via the parameter “Report texts” (parameter window “Function”).

The following objects are used to display an entry in the event list memory. Normally the objects indicate the latest event:

Object	Explanation
Text name of event	Contains the type of signal
Text name of detector	Contains the name of the detector which triggered the signal
Text date/time	Contains the time and date of the signal. The format can be parameterised.

Table 4: Contents of the event list memory

It is possible to browse through the contents of the event list memory via the object “Read event list memory up/down”. If a new event is stored afterwards or the object “Open event list memory” contains the value “1”, the event list memory objects again show the latest event.

In the event of an alarm, only the signal that triggered the alarm is stored. If further intrusion detectors are triggered e.g. in the event of a break-in, these events are no longer stored.

The following events are stored in the event list memory:

Event	Object “Text name of event”	Object “Text name of detector”
Alarm or fault	Name of alarm (can be parameterised)	Name of detector (can be parameterised)
Fault after bus voltage recovery	Name of the fault alarm	“Power On”
Bus voltage failure	“Power Off”	(Spaces)
Reset via ETS	“Reset”	(Spaces)
Reset via object	“Alarm Reset”	(Spaces)
Setting	Signal in state “Externally set” (can be parameterised)	(Spaces)
Unsetting	Signal in “Unset” state (can be parameterised)	(Spaces)

Table 5: Overview of the stored events

Note: A fault as a result of a bus voltage is stored in the event list memory (see above). The reset of this fault is not stored.

Deleting the event list memory

The event list memory is reset by reprogramming the device.

Updating the time and date

The Security Module has an internal clock with an accuracy of <5 seconds per day. It is only used for the time stamp in the event list memory.

The time and date must be regularly specified by a master clock. It is advisable to synchronise the time daily at 3:00 in the morning because the Security Module does not carry out a conversion between summertime and wintertime.

After bus voltage failure, the time and date are reset. The Security Module can actively query them via the bus. There are two possibilities:

1. The Security Module reads out the object values “Time” and “Date” via the bus.
2. The Security Module sends a send request to the master clock via the object “Request date/time”. This is necessary with some clocks (e.g. time switches of type SW/S or FW/S).

4.7 Behaviour on bus voltage failure and recovery

Important: On failure of the bus voltage, the EIB detectors cannot function in principle. Monitoring is therefore no longer possible!

The Security Module is designed so that it continues to operate with stability after voltage recovery and does not generate any unwanted operating faults (e.g. false alarms).

Behaviour during bus voltage failure

During bus voltage failure, the Security Module is completely without a function. The contents of the event list memory are retained.

Behaviour after bus voltage recovery

On bus voltage recovery, the device waits for the duration of the initialisation period until the system has reached a stable condition. During this period, it receives telegrams via the bus but does not evaluate them or trigger any alarms.

Once the initialisation period has ended, the device queries the status of all the detectors, if this option has been set in the parameters. The setting state before bus voltage failure is then restored and the states of the objects are evaluated.

After bus voltage recovery, the following status objects are sent on the bus in master mode:

No.	Object function	Object name
5	Text name of event	Event list memory
6	Text name of detector	Event list memory
7	Text date/time	Event list memory
9	Text triggered detector	Setting/Unsetting
15	Status externally set	Setting/Unsetting
16	Status internally set	Setting/Unsetting
17	Status ext. or int. set	Setting/Unsetting
18	Status ready for setting	Setting/Unsetting
21	Text setting status	Setting/Unsetting
22	External strobe light	Alarming
23	External siren	Alarming
24	Internal siren	Alarming
25	Telegr. intrusion alarm	Alarming
26	Telegr. technical alarm 1	Alarming
27	Telegr. technical alarm 2	Alarming
28	Telegr. panic alarm	Alarming
29	Telegr. tamper alarm	Alarming

30	Telegr. fault	Alarming
33	Text name of alarm	Alarming
34	Text alarming detector	Alarming

Table 6: Objects sent after bus voltage recovery

The voltage failure is logged in the event list memory.

5 Appendix

5.1 Terms used in security technology

The following overview is used to define some terms which are common in security and monitoring technology.

Detector

A detector is a device which detects danger by evaluating appropriate physical variables (e.g. heat radiation, vibration) and interrupts or shorts a circuit. Several detectors are combined in this type of circuit.

Zone terminal

Zone Terminal

The Zone Terminal evaluates the signals from the detectors and routes this information via the bus.

Opening surveillance, lock monitoring

The monitoring of windows, doors, skylights or similar to determine if they are open or closed is called opening surveillance.

With lock monitoring, the locked or bolted state of windows, doors or skylights is monitored. The triggering of a lock monitoring circuit does not lead to an alarm but prevents the system from being set.

Glass breakage sensor

Peripheral protection, surface surveillance

Peripheral protection involves the monitoring of all doors, windows, openings that lead outside as well as any other access points. Surfaces (panes of glass, doors, external walls) can be monitored using so-called surface surveillance which is used to detect someone breaking in (damage to the surface), climbing through (damage to the surface and penetration) or reaching in (‘smash and grab’).

Internal surveillance

Movements within closed rooms are evaluated directly by internal surveillance detectors.

Panic alarms

Panic alarms are push buttons which are operated should a person find themselves in danger. An alarm is activated immediately after a push button operation.

Combined signalling device

Alarms

Local alarm signals are carried out e.g. with acoustic signalling devices (sirens), optical signalling devices (strobe lights or flashing lights) or via a remote alarm (telephone). Indoor acoustic signalling devices can be used for an alarm within the monitored area.

Tamper monitoring

The attempt to shut down the whole or parts of a monitoring system or to interfere with its proper function leads to a tamper alarm. Cables and parts of the installation are monitored e.g. with tamper contacts.

Setting/unsetting

This term refers to intruder alarm systems. If a system is set, an alarm is triggered should an attempted break-in be detected. If the system is unset, no alarm is issued during a break-in. The setting/unsetting of the system is carried out by an setting/unsetting device such as a key lock or combination lock. The connection between the setting/unsetting device and the locking device makes it impossible to enter the building inadvertently while the system is set (forced operation).

5.2 Important application notes

This section contains important tips and hints for installing a monitoring system with a Security Module.

5.2.1 Avoiding false alarms

The top priority when installing a security system must be to avoid the triggering of false alarms. Apart from the direct costs incurred, false alarms lead to the alarm system becoming unreliable and bringing more problems than benefits.

5.2.2 Use of motion detectors

Motion detectors represent an effective opportunity for internal surveillance. Some important points must however be noted when they are used:

Selection

To avoid false alarms, detectors with reliable detection characteristics should be used. VdS-certified detectors are recommended. They offer several benefits:

- Reliable detection in adjustable areas of detection
- Protection against sabotage e.g. opening, covering or removal

Dual motion detectors which have e.g. infrared and microwave sensors offer optimum protection against false alarms. They are only triggered if both detection types sense a movement.

Positioning

Motion detectors must be positioned do that they do not ‘look’ outside. Moving objects and ventilation devices (heating/cooling) should also not be placed in the area of detection.

An external motion detector should only be used for switching the lighting.

5.2.3 ‘Priority control’ during setting

To avoid false alarms, it must be made impossible to enter a set security area unintentionally. Blocking elements are used for this purpose which move out when the alarm system is set and block the door.

Blocking elements of type ESPE can e.g. be controlled by a switch actuator.

5.2.4 Signalling

It should always be assessed whether the external alarm signal can be replaced by a signalling device inside the building. For external alarm signals, a silent alarm e.g. by a Telephone Gateway is recommended.

5.2.5 Use of Zone -Terminals

Zone Terminals are recommended for the connection of sensors. They offer considerable benefits compared to a binary input such as

- The cables from the Zone Terminal to the sensor are monitored. They therefore offer protection against intentional or wilful separation or short circuiting of the cables.
- The cables from the Zone Terminal to the sensor are electrically isolated from the bus. The bus is therefore effectively protected against external overvoltage. Considerably longer cable lengths are also possible.
- To reset specific detectors (e.g. glass breakage sensors) after a signal, the scanning voltage must be interrupted briefly. This is only carried out with a Zone Terminal.

- The Zone Terminals deliver the signals “Walk test” and “Set/Unset” to control the motion detectors.

5.3 Ordering information

Designation	Ordering information Short code	Order no.	bbn 40 16779 EAN	Unit price [EURO]	Price group	Unit weight [kg]	Pack unit [pce.]
Security Module, MDRC	SCM/S 1.1	2CDG 110 024 R0011	58391 6		26	0.1	1

ABB STOTZ-KONTAKT GmbH
P.O. Box 10 16 80, D-69006 Heidelberg
Tel (06221) 701-607
Fax (06221) 701-724
www.abb.de/stotz-kontakt

Technical Hotline:
Tel (06221) 701-434
E-mail: eib.hotline@de.abb.com

2006-12-12