EIB Alarm Central Unit, surface-mounted
75730010

Technical Documentation

Product name:	EIB Alarm Central Unit
Design:	Surface-mounted
Item no.:	75730010
ETS search path:	Berker / Alarm technology / Alarm central unit
Functional description:	

This EIB alarm central unit (ACU) is the heart of an efficient alarm system. Owing to the utilization of the Instabus EIB, expensive additional cabling work can be reduced to a minimum. Both the EIB system and individual detectors installed can, for example, also be used by other trades.

By many different parameterization options within an ETS plug-in of its own, the EIB alarm central unit facilitates its use in various kinds of buildings – from the detached family house with outer shell and interior room safeguarding up to the office building where up to four safeguarding areas (SA 1…4) can be protected individually or as groups linked up with one another. The ETS plug-in will be automatically started when the parameter setting option is called.

The EIB alarm central unit stands out for the following performance features:

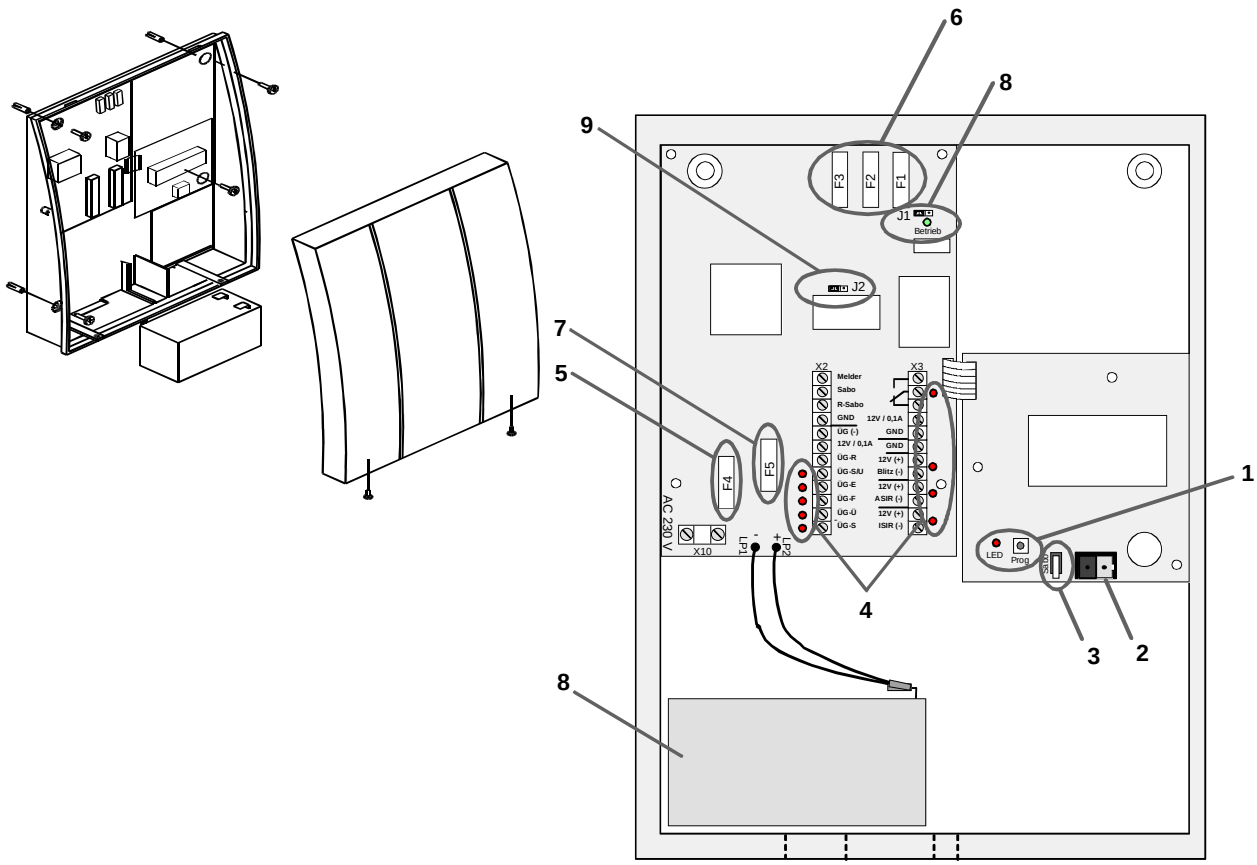
- Up to 160 detectors can be managed and integrated into up to four separate safeguarding areas.
- All sensors (detectors) are connected to the alarm central unit via the EIB. This facilitates individual identification and monitoring of all detectors.
- All events (arming, alarm, fault) will be logged together with their date and time and saved.
- The alarm indicators (siren, flashlight, alarm transmission device (ATD)) can be directly connected to the alarm central unit or triggered via the EIB.
- A rechargeable emergency battery facilitates uninterrupted operation of the alarm indicators even in the event of mains failure. An intelligent electronic charging circuit ensures that emergency power supply of at least 12 hours will always be guaranteed.
- Display and operation are exclusively decentralized and can be handled via external EIB devices (info display unit, pushbutton sensors, etc.). Sometimes, several types of arming devices (AD) can be used within an arming area (AA 1…AA 4) for arming and disarming.
- A local detector input (wired detector) can be used for safeguarding the place of installation of the alarm central unit, e. g. in a distribution cabinet. Thus, the alarm central unit will be in a position to protect 'itself'.
- An additional relay contact in the form of a potential-free output can, for example, be used for additional alarm indicator applications.

For fire and attack detectors, separate safeguarding areas are reserved. If a detector from one of such safeguarding areas responds an alarm will immediately be raised, regardless of the state of the system.
As a special variant, the alarm central unit can also be solely used for attack and fire detector applications.

A detector test mode is available, by means of which all detectors of the alarm system can be checked without raising any alarm.

Particularly large buildings (arcades, extensive factory units) can possibly not be safeguarded by one alarm central unit alone but require several alarm central units, each of them monitoring partial complexes. When several EIB alarm central units are used, such alarm central units can monitor one another by sending and receiving telegrams for mutual monitoring. After three missing telegrams from the 'partner alarm central unit', a sabotage signal will be released (armed: alarm, disarmed: fault).

Illustration:



Dimensions:

Width: 210 mm
Height: 270 mm
Depth: 73 mm

Controls:

1 Programming key and programming LED.
2 EIB connection.
3 Sabotage contact (cover contact).
4 9 red LEDs to indicate the output states: alarm transmission device (ÜG = ATD), outdoor siren (Asir), indoor siren (Isir), flashlight and potential-free relay contact (LED lit = output active).
5 Mains voltage fuse (F4 = 3.15 A, slow-blow).
6 Actuator output fuses ($F1_{BCU\ sec.\ part}$ = 100 mA, slow-blow/$F2_{add.\ +12\ V\ supply}$ = 100 mA, slow-blow/ $F3_{transm.\ unit}$ = 100 mA, slow-blow).
7 "Reverse battery protection" fuse (F5 = 3.15 A, fast-blow).
8 Jumper J1, "bus voltage failure in the armed state", "Betrieb" (device ON) LED.
The green LED indicates the status of the bus voltage. If it is blinking the bus voltage has failed or the device is being programmed. In this case, the response of the alarm central unit can be set with jumper J1 (refer to "Response to Bus Failure").
9 Although jumper J2 has no function, it must be inserted (its position is irrelevant).

Specifications	
Protective system:	IP 20
Mark of conformity:	EIB
Ambient temperature:	-5 ℃ to +45 ℃
Storage temperature:	-25 ℃ to +75 ℃ (storage above +45 ℃ will shorten the life)
Fitting position:	any
Minimum distances:	none
Type of fixing:	rigid/wall mounting
instabus EIB supply	
Voltage:	21 - 32 VDC
Power consumption:	240 mW typ.
Connection:	instabus connecting and branch terminal
External supply	
Voltage:	230 VAC +/- 10 %, 50/60 Hz
Power consumption:	24 W max.
Connection:	Screw terminals:4 mm² max. single-wire 2.5 mm² max. finely stranded without ferrule 1.5 mm² max. finely stranded with ferrule
Response to voltage failure	
Bus voltage only:	You can use jumper J1 to set the response to bus voltage failure while the system is in its armed state.

J1 1 J1 2

Position 1	The "flashlight" (Blitz) and "outdoor siren" (Asir, 180 s) wired outputs as well as the "fault signal to the ATD" (ÜG-S) and "intruder signal to the ATD" (ÜG-E) outputs will be triggered immediately.
Position 2	Only the wired "fault signal to the ATD" (ÜG-S) output will be triggered immediately.

When the system is in its disarmed state, only a fault signal (fault signal to the ATD) will be released through the wired output after 60 seconds.

Mains voltage only:

When the system is in its armed state and the mains has failed for at least 30 seconds, an alarm transmission device fault signal will be released. If the mains failure is shorter than 30 seconds such failure will only be recorded in the event log.

For a disarmed system and a mains failure of at least 30 seconds, an alarm central unit fault signal will be released, with this event being indicated by the display units. If the mains failure is shorter than 30 seconds such failure will only be recorded in the event log.

A fault signal caused by a mains failure of < 60 minutes can be temporarily reset by acknowledgement (disarming) in the individual arming areas (refer to "5.3 Fault acknowledgement operations", page 48).
A mains voltage failure of > 60 minutes, however, can only be reset after mains voltage recovery.
In the event of a mains voltage failure, the emergency battery will feed the alarm system including all alarm indicators up to 12 hours.

Bus and mains voltages:	The response to bus voltage failure can be set with jumper J1 while the system is in its armed state (refer to "Response to Bus Failure"). In any case, an alarm transmission device fault signal will be immediately released. The mains failure will be written into the event log. When the system is in its disarmed state, only a fault signal (fault signal to the ATD) will be released after 60 seconds. In addition, the mains voltage failure (> 30 seconds) will raise an alarm system fault signal if the bus voltage has reappeared at this time. The mains failure will be written into the event log. In the event of a mains voltage failure, the emergency battery will feed the alarm system including all alarm indicators up to 12 hours.
Response to recovery	
Bus voltage only:	Depending on the software (refer to "11.2 Bus voltage recovery", page 58). The "bus voltage recovery" parameter determines whether the state of the alarm central unit before the bus voltage failure ("last state") should be restored, or whether all arming areas should be disarmed ("all AAs disarmed"). After each bus voltage recovery, all detectors will be checked for their presence. Any missing detectors of armed areas will, in this case, lead to alarm raising. Missing detectors of disarmed areas will release an alarm central unit fault signal (through the "alarm central unit fault" object). Bus voltage recovery will be stored in the event log.
Mains voltage only:	The time at which the mains voltage recovers determines the response (refer to "Response to Mains Voltage Failure").
Bus and mains voltages:	Depending on the software (refer to "11.2 Bus voltage recovery", page 58). If the bus and mains voltages recover at the same time there will be no response to the mains voltage failure. If there is no mains voltage upon bus voltage recovery an alarm central unit fault signal (mains failure > 30 seconds) will be released. Bus voltage recovery will be stored in the event log.
Wired detector input:	
Number:	1
Signal voltage:	approx. +4.7 VDC (in open state/"1" signal) 0 V (when contact is closed/"0" signal)
Signal current:	500 µA typ. (when contact is closed)
Detector resistance:	max. 1 kOhm max. for "0" signal recognition
Signal period:	100 ms min.
Input line length:	200 m max. for a min. wire diameter of 0.8 mm
Connection:	Screw terminals: 1.5 mm² max., single-wire 1.0 mm² max., fiinely stranded without ferrule 0.75 mm² max., finely stranded with ferrule
Sabotage input:	
Number:	1
Signal voltage:	approx. +4.7 VDC (in open state) 0 V (for a sabotage resistance of 0 Ohms) approx. +2.8 VDC (for a sabotage resistance of 12 kOhms) approx. +3.8 VDC (for a sabotage resistance of 47 kOhms)
Signal current:	approx. 500 µA (for a sabotage resistance of 0 Ohms) approx. 200 µA (for a sabotage resistance of 12 kOhms) approx. 80 µA (for a sabotage resistance of 47 kOhms)
Signal period:	100 ms min.
Input line length:	600 m max. for a min. wire diameter of 0.8 mm
Connection:	Screw terminals: 1.5 mm² max., single-wire 1.0 mm² max., finely stranded without ferrule 0.75 mm² max., finely stranded with ferrule

ATD checkback input (ÜG-R):	
Number:	1
Signal voltage:	+5 VDC max. external SELV
Signal current:	500 µA max.
Signal recognition:	
"1" signal (no fault):	≥ +2 VDC
"0" signal (fault):	0 ... +0.8 VDC
Signal period:	100 ms min.
Input line length:	200 m max. for a min. wire diameter of 0.6 mm
Connection:	Screw terminals: 1.5 mm² max., single-wire 1.0 mm² max., finely stranded without ferrule 0.75 mm² max., finely stranded with ferrule
Alarm indicator outputs:	
Number:	3 (1 x outdoor siren/1 x indoor siren/1 x flashlight)
Switch type:	power MOS-FET, depending on output
Rated voltage:	+ 2 VDC SELV per output (+/- 1.5 V in emergency power supply mode)
Rated current:	1.6 A max. (all 3 outputs together) The outputs are electronically protected against overloading.
Output line length:	100 m max. for a min. wire diameter of 0.8 mm
Connection:	Screw terminals: 1.5 mm² max., single-wire 1.0 mm² max., finely stranded without ferrule 0.75 mm² max., finely stranded with ferrule
ATD output:	
ATD supply:	
Number:	1 x +12 VDC/1 x GND ÜG (-)
Rated voltage:	+12 VDC SELV (+/- 1.5 V in emergency power supply mode)
Rated current:	100 mA max.
Control outputs:	
Number:	5 (1 x ÜG-S/U/1 x ÜG-E/1 x ÜG-F/1 x ÜG-Ü/1 x ÜG-S)
Switch type:	transistor per control output (outputs to switch ground)
Rated voltage:	+12 VDC SELV (+/- 1.5 V in emergency power supply mode) with respect to "12 V/0.1 A" terminal
Rated current:	10 mA max. per control output
Output line length:	200 m max. for a min. wire diameter of 0.6 mm
Connection:	Screw terminals: 1.5 mm² max., single-wire 1.0 mm² max., finely stranded without ferrule 0.75 mm² max., finely stranded with ferrule
Potential-free relay output:	
Number:	1 x normally open (NO)/1 x normally closed (NC) with the same base contact
Switch type:	potential-free relay contacts
Switching voltage:	12 VAC/DC max.
Switching current:	5 A max.
Minimum load:	30 mA
Connection:	Screw terminals: 1.5 mm² max., single-wire 1.0 mm² max., finely stranded without ferrule 0.75 mm² max., finely stranded with ferrule
+12 VDC supply additional output:	
Number:	1 x +12 VDC/2 x GND
Rated voltage:	+12 VDC SELV (+/- 1.5 V in emergency power supply mode)
Rated current:	100 mA max.
Connection:	Screw terminals: 1.5 mm² max., single-wire 1.0 mm² max., finely stranded without ferrule 0.75 mm² max., finely stranded with ferrule
Storage battery:	
Type:	lead gel storage battery
Rated voltage:	+12 VDC
Capacity:	1.2 Ah
Charging voltage:	+13.4 VDC
Charging current:	150 mA max.
Internal clock	
Power reserve:	12 hours min.
Time error:	< 2 minutes per month

Wiring diagram:

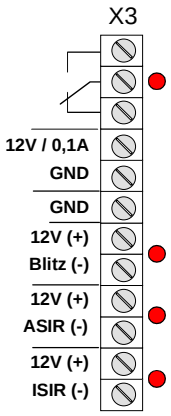
Terminal assignment:

Alarm indicators

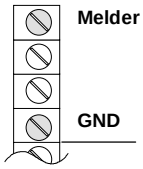
Alarm indicators can be directly connected to the EIB alarm central unit - terminal strip X3.
As an alternative, you can connect alarm indicators to the EIB via suitable actuators and trigger them by telegrams (refer to 'Object description').

Integrate the sabotage contacts of the alarm indicators into the sabotage circuit (refer to 'Sabotage security').

the red LEDs opposite to the terminals indicate when an output is being triggered (output being triggered = LED is lit).



Terminal	Function
Relay	Potential change-over contact facilitating the switching of a load. Switching capacity: 12 VAC/DC, 6 A, max.
12V/0.1A/GND	+12 V connection for the supply of external alarm components (e. g. to be switched via the relay). Max. load 100 mA (1.2 W).
12 V (+)/Blitz (-)	For the connection of a flashlight. Can be activated in the event of alarm without any time limit until disarming takes place (depending on parameter).
12 V (+)/ASIR (-)	For the connection of an outdoor siren. In the event of alarm, it may be on for a max. period of 180 s (triggering period depending on parameter).
12 V (+)/ISIR (-)	For the connection of an indoor siren. In the event of alarm, it should be on for a max. period of 180 s (triggering period depending on parameter).

Wiring diagram:	Terminal assignment:
Wired detector The alarm detectors can be connected to the instabus EIB, if necessary, via suitable binary inputs. An additional detector - or even several normally closed contacts connected in series (closed current loop) - can be directly connected to the alarm central unit. This detector contact must be connected between the "Melder" (detector) and "GND" terminal (where "GND" may be any terminal of the alarm central unit marked this way). Such detector can, for example, be used for safeguarding the area in which the alarm central unit is located. The wired detector must be assigned to one of the four safeguarding areas when the system is being configured from the ETS. Assignment to the "fire" or "attack" area will not be possible. For this reason, the wired detector input is deactivated in configuration 1. The alarm central unit comes with a wire jumper inserted between the "Melder" (detector) and "GND" terminals. If you use the detector input remove this wire jumper. The state of the contact can be transmitted to the bus: ontact closed = "0"/ contact open = "1".	X2 

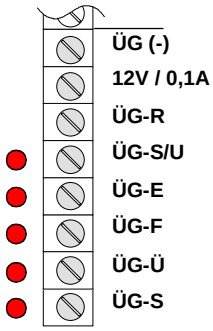
Wiring diagram:

Terminal assignment:

Alarm transmission device

Alarm transmission devices (ATDs) transmit signals of the alarm central unit through the telephone line, for example, to a property security company or a private person.
One alarm transmission device can be connected to terminal strip X2. In this connection, the individual terminals will be triggered separately.
For visual indication, the related LEDs will be lit, if their associated terminals are being triggered.
As an alternative or additionally, an EIB alarm transmission device can be triggered through the object provided for this purpose (refer to 'Object description').

X2



Terminal	Function
ÜG (-) 12V/0,1A	12 VDC supply voltage (+ and -) for alarm transmission devices without their own power supply. The maximum load to be imposed is 100 mA.
ÜG-R	Checkback input from the ATD (in the event of alarm transmission device fault/local alarm/negative acknowledgement). ("1" signal = no fault/"0" signal = fault) *
ÜG-S/U	Armed/disarmed state signal to the ATD. *
ÜG-E	Intruder signal to the ATD (the detector of anarmed area has tripped). *
ÜG-F	Fire signal to the ATD (a smoke detector has tripped). *
ÜG-Ü	Attack signal to the ATD (an attack detector has tripped). *
ÜG-S	Fault signal to the ATD (e. g. battery fault). *

*: For the direct connection of an alarm transmission device having its own power supply (the alarm transmission device is not supplied by the alarm central unit) connect the ground potential of the alarm transmission device and of the alarm central unit (terminal: "ÜG (-)") with each other to ensure proper functioning of the inputs or of the outputs, respectively. Observe the instructions given in the documentation of the alarm transmission device used.

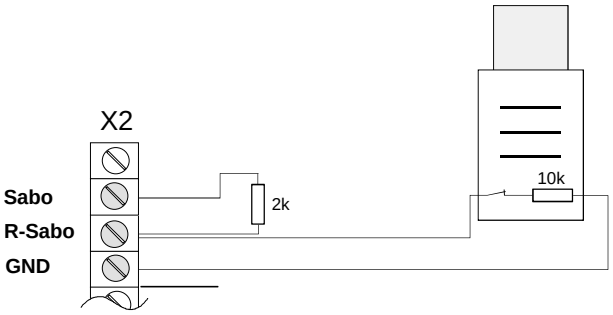
The terminal (ÜG-R) or the "ATD checkback contact fault" object (191) will be triggered by the alarm transmission device if there is a fault in the telephone network (no exchange connection) or a call could not be transmitted ("busy line"). In the event of a "silent" attack alarm (alarming only through the alarm transmission device) a (parameterizable) local alarm (siren and flashlight) can be triggered after an unsuccessful alarm signal.

Wiring diagram:

Terminal assignment:

Sabotage security ("alarm central unit wired detector sabotage")

Between the "Sabo" (sabotage) and "GND" terminals of terminal strip X2, you can connect the sabotage contacts of the wired alarm indicators (siren and flashlight) or of the wired arming devices (e. g. key-operated switches).
In this connection, and by the optional integration of a terminating resistor into the sabotage circuit (closed current loop), it will be possible not only to recognize an interruption in the circuit but, on the contrary, also to detect any short circuit or other manipulations which change the resistance of the circuit.
You can determine the resistance of the sabotage circuit when using the ETS to configure the system. You can set the following resistances: 0 Ω, 12 kΩ, 47 kΩ.
If you need a resistance which you cannot configure you can use the "R-Sabo" terminal for adaptation.



Example: You have configured 12 kΩ. The device has a firmly integrated resistor of 10 kΩ at its sabotage terminal. In this case, connect a 2 kΩ compensating resistor between "Sabo" and "R-Sabo" (potential-free contact) to obtain a total resistance of 12 kΩ.

The alarm central unit comes with a sabotage terminating resistance set to 0 Ω. If you use the sabotage input remove the wire jumper from between the "Sabo" and "GND" terminals.

Tampering with the wired sabotage circuit within armed areas will lead to sabotage alarm.
In disarmed areas, a 'global' fault signal will be released. You must separately acknowledge such signal in each arming area.

The enclosure of the alarm central unit is monitored by a microswitch. Opening the enclosure in the "disarmed" state will cause a fault signal ("alarm central unit enclosure sabotage"). If any area has been armed sabotage alarm will also be raised there.

The sabotage contacts of the devices within the safeguarded inner area and the external arming devices (e. g. key-operated switches) should be integrated into the system as sabotage detectors via the EIB (refer to "3. Detector and Sabotage Inputs", page 26). This facilitates the immediate identification of the tripped detector contact when a sabotage alarm is released.
If external ariming devices raise sabotage alarm you can no longer use it for disarming.

Remarks on the hardware

- The maximum current of all devices connected to the alarm central unit must not exceed 1.8 A.

- The alarm central unit has an overload or short-circuit detection circuit for the alarm indicator outputs. In case of overload of an output, the electronic overload detection circuit will switch off all alarm indicator outputs (terminals: Blitz (flashlight), Asir (outdoor siren), Isir (indoor siren) for about 1 second. In a subsequent test cycle, the alarm central unit will identify the overloaded or short-circuited alarm indicators by priority-related adding of the outputs (flashlight → outdoor siren → indoor siren) and will deactivate them permanently. If none of the outputs can be clearly found overloaded during the test cycle there may possibly be some sum overload. In such case, the automatic circuit will deactivate individual outputs by priority until no more overload is detected.
  Deactivated outputs will only be enabled again when the bus voltage is applied and the alarm indicator outputs are switched off by the alarm central unit in the 'usual' way, for example, after an alarm period has elapsed. If any outputs are overloaded again when the alarm indicators are switched on for the next time such outputs will be deactivated again.
  Overloaded outputs will cause an "alarm indicator overload" global alarm central unit fault.

- The alarm central unit needs 230 VAC mains voltage for permanent operation. The line fuse protection of the EIB alarm central unit should be implemented by a safety cut-out which has not been integrated in the residual current circuit breaker system of your general interior wiring.

- When programming the physical address (actuating the programming key), you should disconnect the device from the 230 V mains to ensure protection against accidental contact.

- Maximum protection against sabotage will be guaranteed if all wiring to the alarm central unit is installed in concealed fashion. Through the installation opening at the rear side of the enclosure, you can lead the wiring into the alarm central unit.

- You can use the free wires of the EIB cable (yellow and white) to supply external components of the alarm system (e. g. buzzer/LED of the key-operated switch, block connecting link, blocking element, etc.).
  For the power supply of such external components, you can use the alarm central unit (terminal strip X3, "12V/0.1A" and "GND") as source.
  Note: Follow the EIB installation rules for the second wire pair. Do not use these EIB wires for any other application. Observe the conditions for the installation of SELV.

- The battery life is approx. 5 years at an ambient temperature of 20 ℃. Exposing the battery to highe r temperatures or completely discharging it several times will extremely shorten its life.
  It is recommended to replace the emergency battery in intervals of some 4 years.
  If the battery voltage drops below 11.0 V (ageing effects or battery defect) a fault will be indicated, and you must replace the battery (refer to "12. Battery Management", page 58).

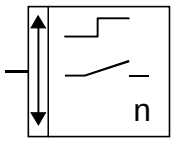
- The bus voltage and all detectors connected to the EIB will not be supplied by the emergency battery. Also to guarantee uninterrupted operation in that case you should use an EIB emergency power supply system.

Software Description

ETS search path:

Berker / Alarm technology / Alarm central unit

ETS symbol:



PEI type	11 Hex	17 Dec	Programmable I/O

Applications:

No.	Brief description:	Name:	Version:
1	Alarm central unit	Alarm central unit C00402	0.2

Application:	1. Alarm central unit C00402		
Runable from screen form version:	7.1		
Number of addresses (max.):	254	**Dynamic table management**	Yes ☐ No ☒
Number of assignments (max.):	254	**Maximum table length**	508
Communication objects:	231		

Detector objects: [2)]

Object	Function	Name	Type	Flag
0 – 159	Safeguarding area 1	Inputs 1 – 160	1-bit	C, W, T, A, (R) [1)]
0 – 159	Safeguarding area 2	Inputs 1 – 160	1-bit	C, W, T, A, (R) [1)]
0 – 159	Safeguarding area 3	Inputs 1 – 160	1-bit	C, W, T, A, (R) [1)]
0 – 159	Safeguarding area 4	Inputs 1 – 160	1-bit	C, W, T, A, (R) [1)]
0 – 159	Fire	Inputs 1 – 160	1-bit	C, W, T, A, (R) [1)]
0 – 159	Attack	Inputs 1 – 160	1-bit	C, W, T, A, (R) [1)]

Sabotage object:

Object	Function	Name	Type	Flag
160	Sabotage	Wired sabotage input	1-bit	C, T, (R) [1)]

Wired detector contact: [3)]

Object	Function	Name	Type	Flag
161	Safeguarding areas 1 – 4	Wired detector input	1-bit	C, T, (R) [1)]

Arming objects: [4)]

Object	Function	Name	Type	Flag
162	Arming area 1	Arming input	1-bit	C, W, (R) [1)]
163	Arming area 2	Arming input	1-bit	C, W, (R) [1)]
164	Arming area 3	Arming input	1-bit	C, W, (R) [1)]
165	Arming area 4	Arming input	1-bit	C, W, (R) [1)]
166	Arming area 1	Arming input	1-bit	C, W, (R) [1)]
167	Arming area 2	Arming input	1-bit	C, W, (R) [1)]
168	Arming area 3	Ready for arming	1-bit	C, W, (R) [1)]
169	Arming area 4	Ready for arming	1-bit	C, W, (R) [1)]
213	All safeguarding areas	Alarm reset	1-bit	C, W, (R) [1)]
214	All safeguarding areas	Detector test	1-bit	C, W, (R) [1)]

Armed/disarmed state signalization objects: [4)]

Object	Function	Name	Type	Flag
170	Arming area 1	Static armed state signal	1-bit	C, T, (R) [1)]
171	Arming area 2	Static armed state signal	1-bit	C, T, (R) [1)]
172	Arming area 3	Static armed state signal	1-bit	C, T, (R) [1)]
173	Arming area 4	Static armed state signal	1-bit	C, T, (R) [1)]

Armed/disarmed state signalization objects (continued): [4]

Object	Function	Name	Type	Flag
174	Arming area 1	Static disarmed state signal	1-bit	C, T, (R) [1]
175	Arming area 2	Static disarmed state signal	1-bit	C, T, (R) [1]
176	Arming area 3	Static disarmed state signal	1-bit	C, T, (R) [1]
177	Arming area 4	Static disarmed state signal	1-bit	C, T, (R) [1]
178	Arming area 1	Armed state signal pulse	1-bit	C, T, (R) [1]
179	Arming area 2	Armed state signal pulse	1-bit	C, T, (R) [1]
180	Arming area 3	Armed state signal pulse	1-bit	C, T, (R) [1]
181	Arming area 4	Armed state signal pulse	1-bit	C, T, (R) [1]
182	Arming area 1	Disarmed state signal pulse	1-bit	C, T, (R) [1]
183	Arming area 2	Disarmed state signal pulse	1-bit	C, T, (R) [1]
184	Arming area 3	Disarmed state signal pulse	1-bit	C, T, (R) [1]
185	Arming area 4	Disarmed state signal pulse	1-bit	C, T, (R) [1]
186	Arming area 1	Pre-alarm	1-bit	C, T, (R) [1]
187	Arming area 2	Pre-alarm	1-bit	C, T, (R) [1]
188	Arming area 3	Pre-alarm	1-bit	C, T, (R) [1]
189	Arming area 4	Pre-alarm	1-bit	C, T, (R) [1]
194	Arming area 1	Disarmed after alarm	1-bit	C, T, (R) [1]
195	Arming area 2	Disarmed after alarm	1-bit	C, T, (R) [1]
196	Arming area 3	Disarmed after alarm	1-bit	C, T, (R) [1]
197	Arming area 4	Disarmed after alarm	1-bit	C, T, (R) [1]

Alarming objects - safeguarding areas: [4]

Object	Function	Name	Type	Flag
190	Alarming	Safeguarding area 1 alarm	1-bit	C, T, (R) [1]
191	Alarming	Safeguarding area 2 alarm	1-bit	C, T, (R) [1]
192	Alarming	Safeguarding area 3 alarm	1-bit	C, T, (R) [1]
193	Alarming	Safeguarding area 4 alarm	1-bit	C, T, (R) [1]
201	Alarming	Fire alarm	1-bit	C, T, (R) [1]
230	Alarming	Fire fault	1-bit	C, T, (R) [1]
202	Alarming	Attack alarm	1-bit	C, T, (R) [1]
225	All safeguarding areas	Alarm reset	1-bit	C, T, (R) [1]

Alarming objects - alarm transmission device:

Object	Function	Name	Type	Flag
198	Alarming	Intruder signal to the ATD	1-bit	C, T, (R) [1]
199	Alarming	Armed/disarmed state signal to the ATD	1-bit	C, T, (R) [1]
200	Alarming	Fault signal to the ATD	1-bit	C, T, (R) [1]

Alarming objects - alarm indicators:

Object	Function	Name	Type	Flag
204	Alarming	Flashlight	1-bit	C, W, T, (R) [1]
205	Alarming	Outdoor siren	1-bit	C, W, T, (R) [1]
206	Alarming	Indoor siren	1-bit	C, W, T, (R) [1]

System monitoring objects:

Object	Function	Name	Type	Flag
203	System monitoring	ATD checkback input fault	1-bit	C, W, (R) [1]
226	All safeguarding areas	Detector test	1-bit	C, W, (R) [1]
227	Heartbeat check [5]	Heartbeat check input	1-bit	C, W, (R) [1]
228	Heartbeat check [5]	Heartbeat check output	1-bit	C, T, (R) [1]
229	System monitoring	Alarm central unit fault	1-bit	C, T, (R) [1]

Display control objects: [6]

Object	Function	Name	Type	Flag
207	Info display unit 1	Line 1	14-byte	C, T, (R) [1]
208	Info display unit 1	Line 2	14-byte	C, T, (R) [1]
209	Info display unit 1	Line 3	14-byte	C, T, (R) [1]
210	Info display unit 2	Line 1	14-byte	C, T, (R) [1]
211	Info display unit 2	Line 2	14-byte	C, T, (R) [1]
212	Info display unit 2	Line 3	14-byte	C, T, (R) [1]
213	Info display unit 3	Line 1	14-byte	C, T, (R) [1]
214	Info display unit 3	Line 2	14-byte	C, T, (R) [1]
215	Info display unit 3	Line 3	14-byte	C, T, (R) [1]
216	Info display unit 4	Line 1	14-byte	C, T, (R) [1]
217	Info display unit 4	Line 2	14-byte	C, T, (R) [1]
218	Info display unit 4	Line 3	14-byte	C, T, (R) [1]
219	Info display unit 1	Selection	1-bit	C, W, (R) [1]
220	Info display unit 2	Selection	1-bit	C, W, (R) [1]
221	Info display unit 3	Selection	1-bit	C, W, (R) [1]
222	Info display unit 4	Selection	1-bit	C, W, (R) [1]

Date/time control objects:

Object	Function	Name	Type	Flag
223	System clock	Time	3-byte	C, W, (R) [1]
224	System clock	Date	3-byte	C, W, (R) [1]

1) For the objects selected (L) the current object status can be read out (setting L flag).
2) The detector objects will be created dynamically in dependence on the parameterized detectors of the individual safeguarding areas (fire, attack, SA 1 - 4). The names of the communication objects and the object table will change correspondingly.
3) The assignment of the "wired detector input" object to one of the four safeguarding areas can be freely parameterized in dependence on the configuration.
4) These objects will be created dynamically in dependence on the parameterized arming areas.
5) The "heartbeat check" objects can be disabled or enabled through a parameter.
6) The info display objects are visible in dependence on the parameterized info display units.

Object description

☐ |	0 - 159	Inputs 1 -160	1-bit object for coupling the EIB detectors to the alarm central unit. (The polarity of the objects can be parameterized.)
☐ |	160	Wired sabotage input:	1-bit object for transmitting the state of the wired sabotage input. (Sabotage = 1/no sabotage = 0.)
☐ |	161	Wired detector input:	1-bit object for transmitting the state of the wired detector input. (NC contact: contact closed = 0/contact open = 1.)
☐→|	162 - 165	Arming input:	1-bit object for arming/disarming the corresponding arming area. (Arming = 1/disarming = 0.)
☐ |	166 - 169	Ready for arming:	1-bit object for the static signalization of the readiness for arming. (Ready for arming = 1/not ready for arming = 0.)
☐ |	170 - 173	Static armed state signal:	1-bit object for the static signalization of the armed state. (Armed = 1/disarmed = 0.)
☐ |	174 - 177	Static disarmed state signal	1-bit object for the static signalization of the disarmed state. (Disarmed = 1/armed = 0.)
☐ |	178 - 181	Armed state signal pulse:	1-bit object for the dynamic signalization of the armed state. (The period for the armed state signal pulse can, in generally, be parameterized. /pulse when armed = 1.)
☐ |	182 - 185	Disarmed state signal pulse:	1-bit object for the dynamic signalization of the disarmed state. (The period for the disarmed state signal pulse can, in generally, be parameterized. /pulse when disarmed = 1.)
☐ |	186 - 189	Pre-alarm:	1-bit object for the signalization of a pre-alarm, i. e. a delayed detector has tripped, and the alarm delay of the corresponding arming area is running down.
☐ |	190 - 193	Safeguarding area 1 – 4 alarm:	1-bit object for the transmission of an alarm in the corresponding safeguarding area. (Alarm = 1/no alarm = 0.)
☐ |	194 - 197	Disarmed after alarm:	1-bit object for the signalization of an alarm activated before in the "disarmed after alarm" state.
☐ |	198	Intruder signal to the ATD:	1-bit object for the transmission of an intruder alarm to an alarm transmission device. (Intrusion = 1/no intrusion = 0.)
☐ |	199	Armed/disarmed state signal to the ATD:	1-bit object for the transmission of an intruder alarm to an alarm transmission device. (Armed = 1/disarmed = 0.)
☐ |	200	Fault signal to the ATD:	1-bit object for the transmission of a fault signal of the alarm central unit an alarm transmission device. (Fault = 1/no fault = 0.)
☐ |	201	Fire alarm:	1-bit object for the transmission of a fire alarm. (Alarm = 1/no alarm = 0.)
☐ |	202	Attack alarm:	1-bit object for the transmission of an attack alarm. (Alarm = 1/no alarm = 0.)
☐→|	203	ATD checkback input fault:	1-bit object for receiving a fault signal from an EIB alarm transmission device. (Fault = 1/no fault = 0.)
☐→|	204	Flashlight:	1-bit object for switching a flashlight. (Flashlight ON = 1/ flashlight OFF = 0.)
☐→|	205	Outdoor siren:	1-bit object for switching an outdoor siren. (Outdoor siren ON = 1/ outdoor siren OFF = 0.)

☐→	206	Indoor siren:	1-bit object for switching an indoor siren. (Indoor siren ON = 1/indoor siren OFF = 0.)
☐ |	207 - 218	Line 1 – line 3:	14-byte object for the transmission of the display texts to the up to four info display units.
☐→	219 - 222	Selection:	1-bit object for the line control of the up to four info display units. This will enable you to select the active lines in the info display unit or to call the display messages, respectively. For the polarity of these objects, refer to the "Display texts" description.
☐→	223	Time:	3-byte object for receiving the time, for example, from a DCF-77 receiver.
☐→	224	Date:	3-byte object for receiving the date, for example, from a DCF-77 receiver.
☐→	225	Alarm reset:	1-bit object for resetting an alarm or for acknowledging various signals, respectively. (Reset/acknowledgement = 1/0 telegram will have no effect.)
☐→	226	Detector test:	1-bit object for activating a detector test. (Activate detector test = 1/deactivate detector test = 0.)
☐→	227	Heartbeat check input :	1-bit object for receiving a signal for monitoring the function of a different alarm central unit.
☐ |	228	Heartbeat check output:	1-bit object for transmitting a heartbeat check signal to a different alarm central unit.
☐ |	229	Alarm central unit fault:	1-bit object for transmitting a fault signal of the alarm central unit.
☐ |	230	Fire detector fault:	1-bit object for transmitting a group fault signal of the fire detectors by the alarm central unit. (Fault = 1/no fault = 0.)

Function scope

- You can establish up to four different safeguarding areas (circuits, signal groups) dependent on one another (nested) or independent (separate) of one another (configuration).
- The "fire" and "attack" safeguarding always exist.
- A maximum of 160 EIB detector inputs which you can assign to the different safeguarding areas independent of one another. You can assign an own text to each detector. For this purpose, you can select a detector text from 20 suggested texts or enter any text with a maximum length of 14 characters.
- You can parameterize six different detector types: "immediate detector", "delayed detector", "sabotage", "arming device (AD) sabotage", "locking mechanism" or "fault" ("fault" only for fire detector).
- In addition to the EIB detector inputs, a wired detector input and a wired sabotage input with loop resistance monitoring can be used in the alarm central unit. In this connection, you can assign the wired detector input to any of the safeguarding areas. This detector input can be used for safeguarding the place of installation of the alarm central unit, e. g. in a distribution cabinet. Thus, the alarm central unit can monitor "itself".
- The response to bus voltage recovery is parameterizable. By means of a hardware jumper, you can set the response of the alarm central unit to bus voltage failure for armed areas.
- Depending on the up to four safeguarding areas, up to four arming areas will be automatically set up. Depending on the configuration, these arming areas can act on one or several safeguarding areas, i. e. arm or disarm them, or acknowledge certain events. For better identification, you can assign a text to each of the arming areas.
- You can parameterize a maximum of four arming devices (AD1…AD4) (e. g. key-operated switches or pushbutton sensors) per arming area. These arming devices are identified by the physical addresses of the EIB components (binary inputs/pushbutton interfaces) through which the arming devices are coupled. By such unambiguous identification, sabotage of the arming devices or manipulation attempts can be recognized. In case of sabotage, it is not always possible to arm or disarm the system through the arming device concerned.
- You can parameterize an arming delay time per arming area.
- One armed/disarmed state acknowledgement can be made per arming area. For this purpose, static and dynamic acknowledgement signals (EIB objects) are available. Thus, you can also trigger door blocking elements by such signals. When using blocking elements, you can parameterize that, in the event of a fire or an attack alarm, such blocking elements will be opened by a premature disarming signal (to open the way out). In addition, acknowledgement by the flashlight, the indoor or outdoor siren, or through the potential-free relay contact is possible. The "armed" or "disarmed" state acknowledging times and the time for the dynamic pulse armed/disarmed state signal are generally parameterizable.
- The alarm delay time (for delayed detectors) per arming area is also parameterizable.
- You can raise a pre-alarm per arming area through an EIB object, for example, if a delayed detector has tripped.
- By one "disarmed after alarm" EIB object per arming area, an alarm signalled in the armed state before can be displayed after disarming independently of the actual alarming operation.
- Via the wired terminals of the alarm central unit or through EIB objects, you can couple an alarm transmission device (ATD) (e. g. telephone dialling device).
- Separate alarming for "fire", "attack" and the various arming areas is possible. In this connection, an alarm will always be raised through the "fire signal to the alarm transmission unit" or "intruder signal to the ATD" EIB objects in the event of a fire or an attack alarm. For the arming areas, alarming is possible through separate alarm objects or through the "intruder signal to the ATD" object. In addition, alarming through the flashlight, the indoor or outdoor siren or through the potential-free relay contact is possible for all areas. For these alarm indicators, you can parameterize the alarm period.

Function scope (continued)

- A fire fault signal (collective signal from all fire detectors) can be transmitted through an EIB object.
- An armed/disarmed state signal can be transmitted through the "armed/disarmed state signal to the ATD" EIB object and a fault signal through the "fault signal to the ATD" EIB object.
- You can parameterize up to four independent display units (e. g. info display unit). Such display units can be assigned to different arming areas (arming areas 1 to 4/fire/attack).
  You may also use more than four display units, the latter then having to be connected in parallel. In such case, the areas to be viewed on the display units connected in parallel, however, will be the same since the group addresses of a display group will be assigned several times.
- You can interconnect several alarm central units to keep under surveillance any possibly larger areas (manufacturing halls, shopping centres). For this purpose, two objects for mutual heartbeat checking of the alarm central units are available. It will be checked whether the life sign of the sending partner alarm central unit comes in at some monitoring interval. If such telegram does not arrive a parameterizable fault or alarm signal will be raised by the other alarm central unit.
- All detectors assigned can be monitored for presence within a monitoring period. If one of the detectors does not respond within the sampling interval a fault or sabotage signal will be raised, depending on the state of the system.
- In the event of an attack or an intrusion, you can transmit a silent alarm only through the alarm transmission device. To recognize the alarm could be transmitted without any problems it is possible for the alarm transmission devices to pass forward to the alarm central unit any transmission error which might have occurred. For this purpose, the "ÜG-R" wired (checkback) input or the "ATD checkback input" EIB object is available. For sabotage and attack, you can parameterize the response of the alarm central unit to a transmission error signalled. Thus, the flashlight, the indoor and the outdoor siren can be additionally activated should any error occur.
- Through EIB objects (e. g. by a DCF-77 receiver), you can synchronize the system clock integrated into the alarm central unit. As an alternative, the PC time can be transmitted to the alarm central unit through the ETS plug-in. The changeover from summer to winter time and vice versa will be done automatically by the alarm central unit.
- Various events (arming, alarm, fault) will be logged together with their date and time and saved. You can read out this event log via the ETS plug-in. In this connection, you can either save the read-out data into a file or print it out.
- In the detector test mode, you can check all detectors of the alarm system without raising any alarm or the like. During the test of the detectors (magnetic contacts. motion detectors, fire detectors, attack pushbuttons, etc.), the latter will be kept in the display units until you deactivate the detector test mode.

Functional Description

Contents

Functional Description

1. Configuring the Safeguarding/Arming Areas

1.1 Safeguarding areas (SA)

A safeguarding area is an area which safeguards certain building parts and individual rooms or façade areas, i. e. keeps them under surveillance to detect intrusion or vandalism. Within such safeguarding areas, detectors which can be connected together into groups, form the components which facilitate surveillance. Such detectors may be both magnetic contacts on windows or doors, motion detectors on walls or indoor ceilings a smoke detectors or attack pushbuttons. In this connection, the detectors can be connected to the EIB through suitable components or directly linked to the EIB (refer to "3.2 Connecting detectors", page 28).
Safeguarding areas signalling, for example, intrusion contain magnetic contacts or motion detectors in most cases. Such safeguarding areas can be activated or deactivated, i. e. armed or disarmed. Arming/disarming will be done by the assigned arming areas. On the other hand, an "attack detector" safeguarding area is an area which will always raise an alarm if an integrated attack detector has tripped, regardless of what the state of the system is.
A "fire detector" safeguarding area will also raise an alarm once an assigned fire detector has tripped. Thus, the "fire detector" and "attack detector" areas are always ready for operation and need not be separately activated.
How an alarm will be raised, i. e. through what alarm indicators signalization will take place can be fixed by means of the ETS while the alarm central unit is being configured.

1.2 Arming areas (AA)

Arming areas will arm or disarm the safeguarding areas assigned to them.
As a rule, one safeguarding area should be assigned to each arming area. It is, however, possible that several safeguarding areas act on one arming area. When configuring the safeguarding areas with the ETS plug-in prior to the start-up, you can define the way how the up to four safeguarding areas and the up to four arming areas should correspond with one another (separate or nested arrangement).

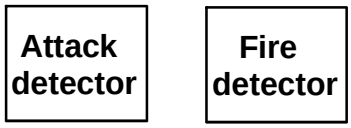
1.3 Configurations

In the following, the 15 possible configurations will be shown.

- **Configuration 1 (always released):**

1 x fire, 1 x attack,
e. g. smoke detector, attack pushbutton, etc.

In this configuration, the alarm central unit can be used for fire and attack alarms. This configuration is always released, i. e. it always exists in parallel with any other released configurations.



Please note the following if you have solely set configuration 1:

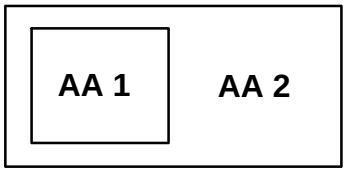
- Resetting an alarm in this configuration will only be possible by the alarm reset option. For this reason, the alarm reset option must have been included into this configuration. If you want to use an arming device for resetting you will have to set configuration 2.X, with the "fire" and "attack" areas only being used (refer to "4.1 Arming devices" and "4.2 Alarm reset").

- Global fault signals (mains voltage failure, battery failure, ATD checkback contact fault, an abortive heartbeat check between two alarm central units (if a missing telegram is to be evaluated in the same way as a fault), opening of the sabotage contact or an interruption in the wired sabotage circuit) will cause alarm central unit faults in this configuration. Such events will only be indicated by the display units (if parameterized) until they have been eliminated. Therefore, they need not be acknowledged. In such case, no active alarm central unit fault signal will be transmitted through the EIB object or the alarm transmission device.

- The wired detector input ("Melder" (wired detector) terminal) is deactivated in this configuration.

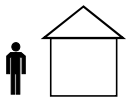
• **Configuration 2.1 (default configuration):**

1 x outer shell (SA 1), 1 x indoors (SA 2), nested,
e. g. detached family house, flat, workshop, etc.



AA 1:
SA 1 (outer shell) can be separately armed by AA 1, i. e. by an arming device located within the building.
In such case, persons are in the building. Only the outer shell will be kept under surveillance (e. g. by means of magnetic contacts on the windows, glass breakage sensors). In the event of an alarm, only the internal alarm indicators will be activated. This condition is also called "internally armed" state.

AA 2:
SA 1 (outer shell) will be automatically armed together with SA 2 (indoors) by AA 2, i. e. by an external arming device next to the entrance door.
In such case, no persons will be in the building. The outer shell and interior rooms will be kept under surveillance (additionally, for example, by PIR detectors). An alarm will activate all external alarm indicators. This condition is also called "externally armed" state.

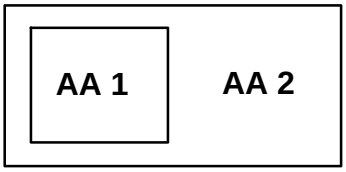


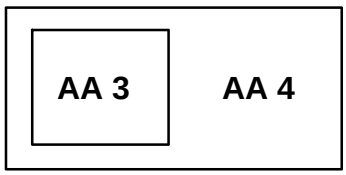
If the system is in the "internally armed" state (AA 1 is armed) AA 1 can also be disarmed by arming or disarming on an arming device of AA 2. After this, both AAs will be in the disarmed state. So it will be possible that persons who are not inside the building and are authorized to enter it can enter the building "internally armed" before without raising an alarm.

• **Configuration 2.2:**

1 x outer shell (SA 1), 1 x indoors (SA 2), nested.
1 x outer shell (SA 3), 1 x indoors (SA 4), nested,
e. g. two-family house, house with granny flat, two independent building parts (workshop and a flat).

Same as configuration 2.1, however, existing twice and independently of each other.



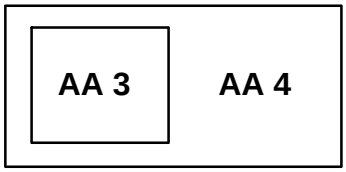


• **Configuration 3.1:**

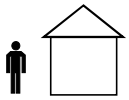
1 x separate safeguarding area (SA 1).
1 x outer shell (SA 3), 1 x indoors (SA 4), nested,
e. g. dwelling house with separate summer house, etc.

AA 1:
SA 1 (separate safeguarding area) can be armed by AA 1. In the event of an alarm, the alarm indicators assigned to AA 1 will be activated.

AA 3:
SA 3 (outer shell) can be separately armed by AA 3, i. e. by an arming device located within the building.
In such case, persons are in the building. Only the outer shell is kept under surveillance (e. g. by means of magnetic contacts on the windows, glass breakage sensors). In the event of an alarm, only the internal alarm indicators will be activated. This condition is also called "internally armed" state.



AA 4:
SA 3 (outer shell) will be automatically armed together with SA 4 (indoors) by AA 4, i. e. by an external arming device next to the entrance door.
In such case, no persons will be in the building. The outer shell and interior rooms will be kept under surveillance (additionally, for example, by PIR detectors). An alarm will activate all external alarm indicators. This condition is also called "externally armed" state.

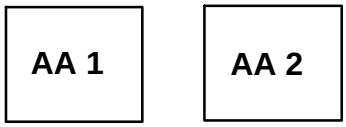


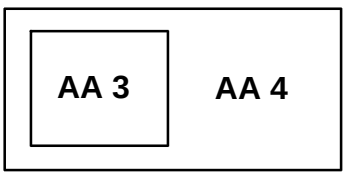
If the system is in the "internally armed" state (AA 3 is armed) AA 3 can also be disarmed by arming or disarming on an arming device of AA 4. After this, both AAs will be in the disarmed state. So it will be possible that persons who are not inside the building and are authorized to enter it can enter the building "internally armed" before without raising an alarm.

• **Configuration 3.2:**

2 x separate safeguarding areas (SA 1 and SA 2).
1 x outer shell (SA 3), 1 x indoors (SA 4), nested,
e. g. dwelling house with separate summer house and store shed, etc.

Same as configuration 3.1, however, additionally with a separate second safeguarding area (SA 2).

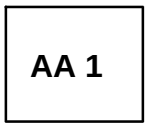




- **Configuration 4.1:**

1 x separate safeguarding area (SA 1),
e. g. arcade, holiday house, hotel, pension, trade fair/exhibition hall, etc.

AA 1:
SA 1 (separate safeguarding area) can be armed by AA 1. In the event of an alarm, the alarm indicators assigned to AA 1 will be activated.

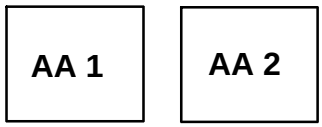


- **Configuration 4.2:**

2 x separate safeguarding areas (SA 1 and SA 2),
e. g. extended, separate areas in arcades, holiday houses, hotels, pensions, trade fair/exhibition halls, etc.

Same as configuration 4.1, however, in addition:

AA 2:
SA 2 (separate safeguarding area) can be armed by AA 2. In the event of an alarm, the alarm indicators assigned to AA 2 will be activated.

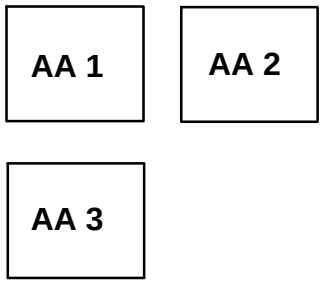


- **Configuration 4.3:**

3 x separate safeguarding areas (SA 1, SA 2 and SA 3),
e. g. extended, separate areas in arcades, holiday houses, hotels, pensions, trade fair/exhibition halls, etc.

Same as configuration 4.2, however, in addition:

AA 3:
SA 3 (separate safeguarding area) can be armed by AA 3. In the event of an alarm, the alarm indicators assigned to AA 3 will be activated.

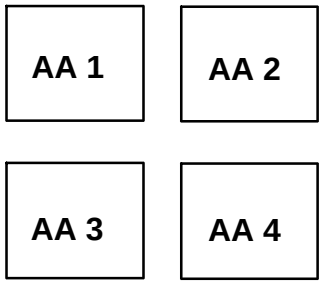


- **Configuration 4.4:**

4 x separate safeguarding areas (SA 1, SA 2, SA 3 and SA 4)
e. g. extended, separate areas in arcades, holiday houses, hotels, pensions, trade fair/exhibition halls, etc.

Same as configuration 4.3, however, in addition:

AA 4:
SA 4 (separate safeguarding area) can be armed by AA 4. In the event of an alarm, the alarm indicators assigned to AA 4 will be activated.



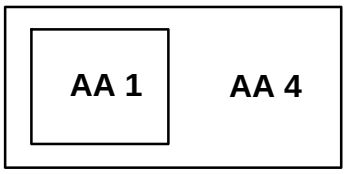
Note on configuration 4.X:

Once an alarm is raised in one of the arming areas, the other areas - as is also the case for all the other configurations - must not be armed until the alarm has been reset.

- **Configuration 5.1:**

1 x safeguarding area (SA 1), separate.
1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one, e. g. office complexes, industrial buildings, sports halls, etc.

AA 1:
SA 1 (separate safeguarding area) can be armed by AA 1. In the event of an alarm, the alarm indicators assigned to AA 1 will be activated. However, if AA 4 is in the armed state alarms will be raised by AA 4.



AA 4:
SA 4 (cascaded safeguarding area) must only be armed by AA 4 after AA 1 has already been armed. When AA 4 is in the armed state, and in the event of an alarm, no matter in which safeguarding areas, the alarm indicators assigned to AA 4 will be activated.

When AA 4 is being disarmed subordinate AA 1 will still remain armed and must be disarmed separately, if desired.

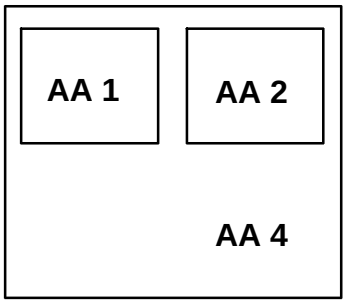
- **Configuration 5.2:**

2 x safeguarding area (SA 1 and SA 2), separate.
1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one, e. g. office complexes, industrial buildings, sports halls, etc.

Same as configuration 5.1, however, in addition:

AA 2:
SA 2 (separate safeguarding area) can be armed by AA 2. In the event of an alarm, the alarm indicators assigned to AA 2 will be activated. However, if AA 4 is in the armed state alarms will be raised by AA 4.
AA 4 must only be armed after AA 1 and AA 2 have already been armed.

When AA 4 is being disarmed the subordinate arming areas (AA 1 and AA 2) will still remain armed and must be disarmed separately, if desired.



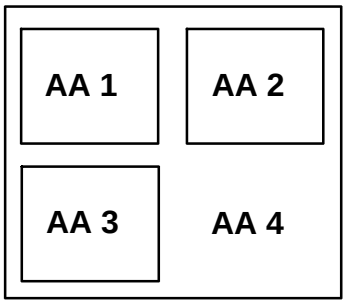
- **Configuration 5.3:**

3 x safeguarding area (SA 1, SA 2 and SA 3), separate.
1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one, e. g. office complexes, industrial buildings, sports halls, etc.

Same as configuration 5.2, however, in addition:

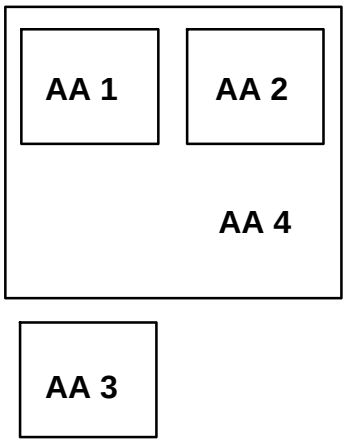
AA 3:
SA 3 (separate safeguarding area) can be armed by AA 3. In the event of an alarm, the alarm indicators assigned to AA 3 will be activated. However, if AA 4 is in the armed state alarms will be raised by AA 4.
AA 4 may only be armed after AA 1, AA 2 and AA 3 have already been armed.

When AA 4 is being disarmed the subordinate arming areas (AA 1, AA 2 and AA 3) will still remain armed and must be disarmed separately, if desired.



- **Configuration 6:**

2 x safeguarding area (SA 1 and SA 2), separate.
1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one,
1 x safeguarding area (SA 3), separate and not integrated into the cascading,
e. g. office complex with two separately safeguarded office rooms and a remote warehouse, etc.



AA 1:
SA 1 (separate safeguarding area) can be armed by AA 1. In the event of an alarm, the alarm indicators assigned to AA 1 will be activated. However, if AA 4 is in the armed state alarms will be raised by AA 4.

AA 2:
SA 2 (separate safeguarding area) can be armed by AA 2. In the event of an alarm, the alarm indicators assigned to AA 2 will be activated. However, if AA 4 is in the armed state alarms will be raised by AA 4.

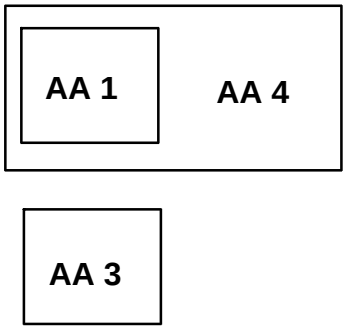
AA 4:
SA 4 (cascaded safeguarding area) must only be armed by AA 4 after AA 1 and AA 2 have already been armed. When AA 4 is in the armed state, and in the event of an alarm, no matter in which safeguarding areas, the alarm indicators assigned to AA 4 will be activated.

When AA 4 is being disarmed the subordinate arming areas (AA 1 and AA 2) will still remain armed and must be disarmed separately, if desired.

AA 3:
SA 3 (separate safeguarding area not integrated into the cascading) can be armed by AA 3. In the event of an alarm, the alarm indicators assigned to AA 3 will be activated.

- **Configuration 7.1:**

1 x safeguarding area (SA 1), separate.
1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one.
1 x safeguarding area (SA 3), separate and not integrated into the cascading,
e. g. the head's office within an office complex with a separate warehouse and, if necessary, additionally with a workshop hall, etc.



AA 1:
SA 1 (separate safeguarding area) can be armed by AA 1. In the event of an alarm, the alarm indicators assigned to AA 1 will be activated. However, if AA 4 is in the armed state alarms will be raised by AA 4.

AA 4:
SA 4 (cascaded safeguarding area) must only be armed by AA 4 after AA 1 has already been armed. When AA 4 is in the armed state, and in the event of an alarm, no matter in which safeguarding areas, the alarm indicators assigned to AA 4 will be activated.

When AA 4 is being disarmed subordinate AA 1 will still remain armed and must be disarmed separately, if desired.

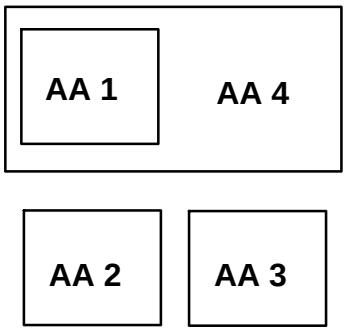
AA 3:
SA 3 (separate safeguarding area not integrated into the cascading) can be armed by AA 3. In the event of an alarm, the alarm indicators assigned to AA 3 will be activated.

- **Configuration 7.2:**

1 x safeguarding area (SA 1), separate.
1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one.
2 x safeguarding area (SA 2 and SA 3), separate and not integrated into the cascading,
e. g. the head's office within an office complex with a separate warehouse and, if necessary, additionally with a workshop hall, etc.

Same as configuration 7.1, however, in addition:

AA 2:
SA 2 (separate safeguarding area not integrated into the cascading) can be armed by AA 2. In the event of an alarm, the alarm indicators assigned to AA 2 will be activated.



1.4 Multi-area configurations

If you select a configuration where armed and disarmed areas can exist "side by side" you should keep the following rules.

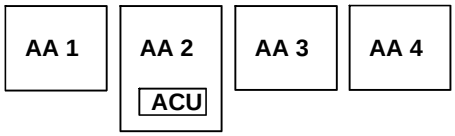
- The alarm central unit must be managed by a user who is authorized to arm and disarm all areas for servicing and in the event of alarm.
- Once an area has been armed, the alarm central unit should also be within a safeguarded area.
- To avert erroneous alarm take corresponding precautions for the place where the alarm central unit is located (e. g. in the switch cabinet). Ensure that

– the system can only be armed after the cabinet door has been locked (e. g. monitored by an interlock switch contact).
– the switch cabinet door cannot be opened as long as an area is in the armed state (e. g. guaranteed by a motor-driven blocking element).

Examples of how to integrate the place of installation into the system for multi-area configurations:

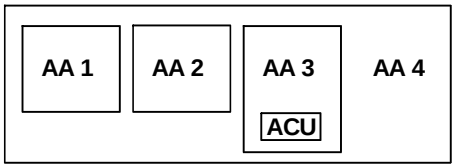
For independent areas, the alarm central unit can, in principle, not be assumed to be within a safeguarded area.

Remedy: Integrate into the sabotage loop of the alarm central unit ("Sabo" (sabotage) terminal) detectors which safeguard the alarm central unit.



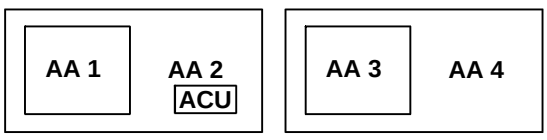
Also for cascaded areas, the alarm central unit will only be within a safeguarded area if the corresponding arming area (refer to AA 3) has been armed.

Remedy: Integrate into the sabotage loop of the alarm central unit ("Sabo" (sabotage) terminal) detectors which safeguard the alarm central unit.



For nested areas, the alarm central unit should be have been installed within an area safeguarded by the indoor detectors (detectors in SA 2, i. e. to be armed by AA 2). However, it may happen that other areas (e. g. AA 3) have been armed.

Remedy: Monitor the alarm central unit by a wired detector ("Melder" (wired detector) terminal) assigned to safeguarding area SA 3. You can also integrate detectors which safeguard the alarm central unit into the sabotage loop ("Sabo" (sabotage) terminal) of the alarm central unit.



2. Editable Texts

From the ETS plug-in, you can assign an identification text to each of the four arming areas, the four safeguarding areas, and to each integrated detector.

In this connection, a maximum of 160 independent texts is available for the identification of the detectors of the up to four safeguarding areas as well as of the "fire detector" and "attack detector" areas so that you can give each of the detectors integrated into the project a clear name. You can also identify the wired detector input. You can edit the detector texts in the parameter branch of each detector, and such texts may have a maximum length of 14 characters. The texts will already be taken over in the ETS plug-in in the parameter tree so that you can find individual detectors easier and more quickly. Typical detector identifications can be *'liv.roomwindow'* (living room window), *'kitchen motion'* (kitchen motion detector) or *'fr.doorgls.brk.'* (front door glass breakage sensor), etc. For simplification, the ETS module always suggests 20 different prepared detector texts which you can take over and extend up to a maximum of 14 characters. As an alternative, you can directly enter any text per detector.
In addition to the detector texts, you can also give each arming area an identification. Such texts may also have a maximum length of 14 characters and can be assigned to each arming area in the "arming" parameter branch. Typical identifications of arming areas are *'outer shell'*, *'inner room', 'office'*, *'workshop'*, etc.

When the alarm central unit is running the names of the detectors and of the arming areas will be read out for clear identification of the detectors or arming areas when being sampled in the display devices such as info display units. These identifications will also be saved in the event log.
You can also assign an unambiguous identification text to each safeguarding area in the "detector/sabotage" parameter branch or to each display item in the "display" parameter branch. Such text has no limited number of characters and is solely displayed in the ETS plug-in.

3. Detector and Sabotage Inputs

3.1 Detector types

Detectors are components communicating via the bus or being wired up (refer to "3.2 Connecting detectors", page 28) which keep under surveillance a part of the building and signal intrusion or an intrusion attempt to the alarm central unit. Frequently used detectors include magnetic contacts, glass breakage sensors and motion detectors. Attack and fire detectors, in general, also belong to such components.

Detector inputs may also be sabotage inputs whereby sabotage or fault signal contacts can be coupled by detectors or arming devices (e. g. key-operated switches) integrated into the system. Even locking mechanism monitoring devices such as interlock switch contacts are detectors which, however, only facilitate forced arming instead of raising alarm. So, for example, an area can only be armed when the front door is locked, the interlock switch contact thus not being active.

You can assign detectors to each of the maximum of four safeguarding areas as well as to the "fire detector" and "attack detector" safeguarding areas. In this connection, the total maximum of 160 detector inputs available will be freely linked to the safeguarding areas. The bottom left status bar of the ETS plug-in will always show the number of detectors already connected and the number of inputs not connected yet.
The following table shows how you can configure the various detector inputs with the available input types.

Safeguarding Areas	Input Types					
	Immediate Detector **	Delayed Detector **	Sabotage	Arming Device Sabotage	Locking Mechanism	Fault
Fire detector	×	---	---	---	---	×
Attack detector	×	---	×	---	---	---
Safeguarding area 1	×	×	×	×	×	---
Safeguarding area 2	×	×	×	×	×	---
Safeguarding area 3	×	×	×	×	×	---
Safeguarding area 4	×	×	×	×	×	---
Wired detector input *	×	×	---	---	---	---
Wired sabotage input	---	---	×	---	---	---

*: The wired detector input cannot be assigned to the "fire" or "attack" area.
**: For these input types, you can define the detector type (contact, motion, glass breakage).

Immediate detector:

A tripping detector will be evaluated immediately and will raise an immediate alarm when it is in the armed state. This setting is recommended for detectors which are not directly located within the entrance area of a building to be safeguarded (e. g. window or glass breakage contacts). Also fire or attack detectors will trip immediately.

Delayed detector:

A tripped detector will be evaluated at some delay. In this connection, the "alarm delay time" per arming area specified in the "arming area/arming" parameter branch will be evaluated as delay time. If you have set a delay time of 0 seconds for this parameter delayed detectors will also trip immediately.
This setting is recommended if you want to disarm the system within the safeguarding area, for example, only after a safeguarded area has been entered. In this connection, a "silent" alarm may call on you to disarm the system. "Delayed detectors" which have tripped will only be saved in the event log after the delay time has elapsed, i. e. when an alarm is being raised.
You cannot select this input type in the "fire detector" and "attack detector" safeguarding areas since immediate tripping of the detectors will be indispensable in such areas.

Sabotage:

The input will be evaluated as sabotage detector. If all arming areas are in the disarmed state only an alarm central unit fault signal will be issued through the corresponding ETS object in the event of sabotage. If a sabotage detector of an armed area signals some manipulation an alarm will be immediately raised in such arming area.
The wired sabotage input will raise an "alarm central unit wired detector sabotage" signal. The sabotage contact of the alarm central unit will raise the "alarm central unit enclosure sabotage" signal.
Sabotage signals will be saved in the event log. You cannot select this input type in the "fire detector" safeguarding area.

Arming device sabotage:

The input will be used as sabotage detector of an arming device (e. g. of a key-operated switch).
If an "arming device sabotage contact" trips the alarm central unit can no longer be triggered via the arming device assigned to this input. You can assign the sabotage detector to an arming device from the "arming" parameter branch.
If all arming areas are in the disarmed state only an alarm central unit fault signal will be issued through the corresponding ETS object in the event of "arming device sabotage".
If an "arming device sabotage" detector of an armed area signals some manipulation an alarm will be immediately raised in such arming area. You cannot select this input type in the "fire detector" and "attack detector" safeguarding areas.

Locking mechanism:

This input serves for the connection of an interlock switch contact in order to monitor the locking of the entrances to a safeguarding area. A locking mechanism detector will not raise alarms but will prevent this safeguarding area from being armed if the door is not locked (forced arming).
You cannot select this input type in the "fire detector" and "attack detector" safeguarding areas.

Fault:

To be able to evaluate collective fault outputs (e. g. battery change signals, smoke box faults) you must select this input type. Any fault of this kind will be read in the info display units (if enabled) and saved in the event log. Fire fault signals, however, will not stop the arming of the arming areas.
You can select this input type only in the "fire detector" safeguarding area.

Important:

- You can parameterize each detector input to different polarities, i. e. inputs may be active in connection with a "1" telegram or with a "0" telegram (refer to "3.2 Connecting detectors", page 28).

- Any detector input not linked to a group address in the ETS plug-in will show no response. It will not be checked for presence under the detector monitoring function.

3.2 Connecting detectors

You can connect the detectors of the alarm system to the alarm central unit through the wired detector input or via suitable EIB components (e. g. binary inputs, pushbutton interfaces). In this connection, such components must correctly evaluate the switching edges, for example, of the magnetic contacts or glass breakage sensors and issue to the bus the telegram corresponding to such edge.
You can parameterize each detector input from the ETS plug-in of the alarm central unit to different polarities, i. e. inputs may be active in connection with a "1" telegram or with a "0" telegram. The polarities parameterized in the alarm central unit must coincide with the edge parameters of the other bus devices.

Example:

When "input active at 1" has been set in the alarm central unit an intruder detector contact must not trip, unless there is glass breakage and the binary input sends a "1" telegram in this case.

The following table will make clear the effects on switching edges and on the polarity of a switching telegram in dependence on the polarity parameter of the alarm central unit for EIB detectors:

Detector Type/State	Edge Response in the Binary Input *	Object Value	Parameter in the Alarm Central Unit	Detector Trips **
NC contact/not actuated	Rising = ON	1	Active at 0	No
NC contact/actuated	Falling = OFF	0	Active at 0	Yes
NC contact/not actuated	Rising = OFF	0	Active at 1	No
NC contact/actuated	Falling = ON	1	Active at 1	Yes
NO contact/not actuated	Falling = OFF	0	Active at 1	No
NO contact/actuated	Rising = ON	1	Active at 1	Yes
NO contact/not actuated	Falling = ON	1	Active at 0	No
NO contact/actuated	Rising = OFF	0	Active at 0	Yes

*: EIB component by which the detector is connected to the bus.

**: Locking mechanism detector tripped = door not locked.

The following table explains the effects on switching edges for directly wired detectors (terminal: "Melder" (detector/ NC contact):

Detector Type/State	Object Value	Detector Trips
NC contact/not actuated	0	No
NC contact/actuated	1	Yes

The value of the "wired detector input" EIB object, in any case, corresponds to the logical state of the contact (NC contact: closed = "0"/open = "1").
In configuration 1, the wired detector input will be deactivated.

Within some monitoring period, you can check all detectors assigned whether they are still present. If a detector does not respond when being sampled from the alarm central unit during the sampling period a fault or sabotage signal will be issued, depending on the state of the system (refer to "7.1 Monitoring detectors", page 53). To facilitate the monitoring of each detector it is important that the transmitting group addresses of the detectors are unambiguous, i. e. not linked to any other transmitting bus device. Each detector should be independently connected to a detector input of its own in the alarm central unit. This is the only way to ensure that solely the addressed detector will respond. **Setting the „R“ flag for the objects of the detectors (not in the alarm central unit) is mandatory.**

Note:

Any detector input not linked to a group address in the ETS plug-in will show no response. It will not be checked for presence under the detector monitoring function.

4. Arming

4.1 Arming devices

4.1.1 Configuring arming devices

You can assign a maximum of four independent arming devices to each arming area. These arming devices such as key-operated switches, transponder arming devices, code keypads or block connecting links facilitate the activation or deactivation of an arming area, i. e. to arm or disarm it. Even simple installation pushbuttons or EIB pushbutton sensors can, in principle, be used as arming devices; however, they will not offer you any protection against unauthorized access. For this reason, pushbutton sensors are often installed within a building to be safeguarded, for example to activate outer shell surveillance ("internally armed").

Safeguarding areas signalling, for example, intrusion contain magnetic contacts or motion detectors in most cases. Only for those areas arming/disarming can be effected by the assigned arming areas or by the arming devices.
On the other hand, an "attack detector" safeguarding area is an area which will always raise an alarm if an integrated attack detector has tripped, regardless of what the state of the system is. A "fire detector" safeguarding area will also raise an alarm, once an assigned fire detector has tripped.

Arming devices can be coupled to the alarm central unit exclusively through the EIB and will act on the "arming input" ETS object which separately exists in each arming area. The polarity of this object is fixed: "1" = arming/"0" = disarming.
On the basis of the project information in the ETS database, the ETS plug-in will now automatically find out which other bus devices configured within the project are connected to the "arming input" of the alarm central unit via the group address assigned to this object (you can only link one group address to the arming input from the ETS plug-in).
The bus devices or arming devices connected have different physical addresses which you must specify when configuring these devices. To be able to assign to an arming area an arming device existing in the project you must use the "arming device 1…4 physical address" parameter to specify the physical address of this arming device in the parameter branch of the arming area. For this purpose, the ETS plug-in will suggest the possible addresses in a selection table, out of which you must select one per arming device. You can assign a physical address only once per arming area.

Note:

The bus devices should have been configured before you configure the alarm central unit from the ETS plug-in. Changing any configuration data after configuring the arming devices (e. g. changing the physical addresses or the group addresses) can cause malfunctioning. The ETS plug-in will issue a message to point to a configuration error if the assignment between the group address of the arming input and the set physical address of an arming device is no longer given.
Also, the ETS plug-in will signal a configuration error if not all arming devices created in the project have been assigned to the corresponding arming area, or if more than four configured arming devices exist.

By the assignment of the physical addresses, the alarm central unit can find out which arming devices or bus devices are authorized to arm or disarm the system. Only telegrams from authorized bus devices will be executed.
Telegrams from unauthorized devices which act on the "arming input" object will lead to sabotage alarm ("arming device sabotage") in the "armed" state. In the "disarmed" state, there will be no response.

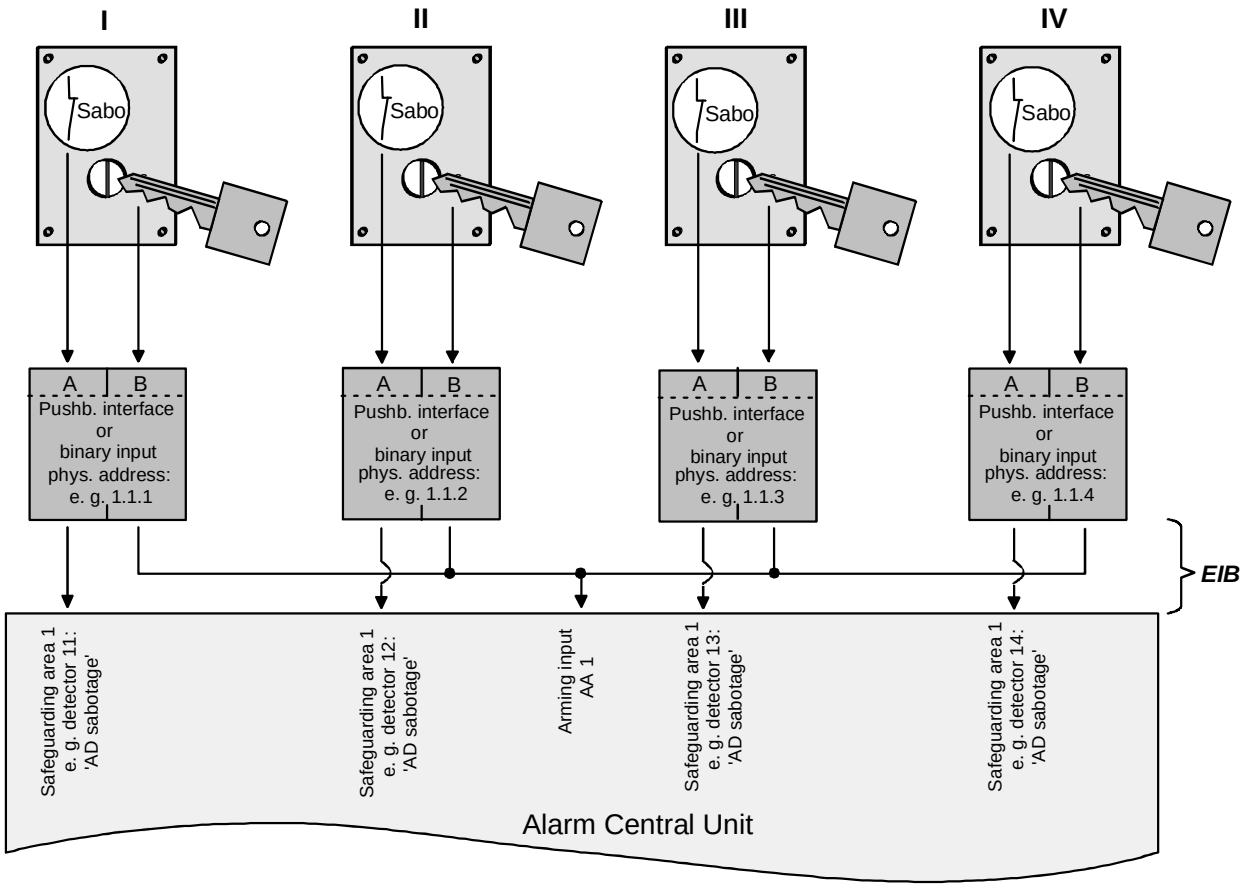
As a rule, arming devices also have sabotage contacts. Such contacts can be assigned to the safeguarding areas as detectors parameterized to "arming device sabotage".
If an arming device is tampered with such device must no longer be authorized to disarm the system. In such case, the alarm central unit will inhibit all telegrams which have been sent by the bus device 'tampered with' and will raise an alarm when in the armed state. In the disarmed state, an alarm central unit fault signal will be issued. If you have parameterized any info display units a sabotage signal from an arming device must first be called into the display before you can reset the fault signal (refer to "5. Operating the Alarm Central Unit", page 40).
The assignment of a sabotage detector of an arming device of the corresponding safeguarding area can be done by the "arming device sabotage input number" parameter in the "arming/arming area X" parameter branch. For this purpose, it is assumed that an "arming device sabotage" detector has been created in the corresponding safeguarding area (refer to "3. Detector and Sabotage Inputs", page 28). A created "arming device sabotage" detector can only be linked with an arming device. In a list, the ETS plug-in will automatically suggest which detector inputs will be possible as arming device sabotage inputs.

Important note:
In systems which only have one arming device and which has been tampered with, you can only reset the fault signal or disarm the system by an alarm reset.

4.1.2 Connecting options of arming devices

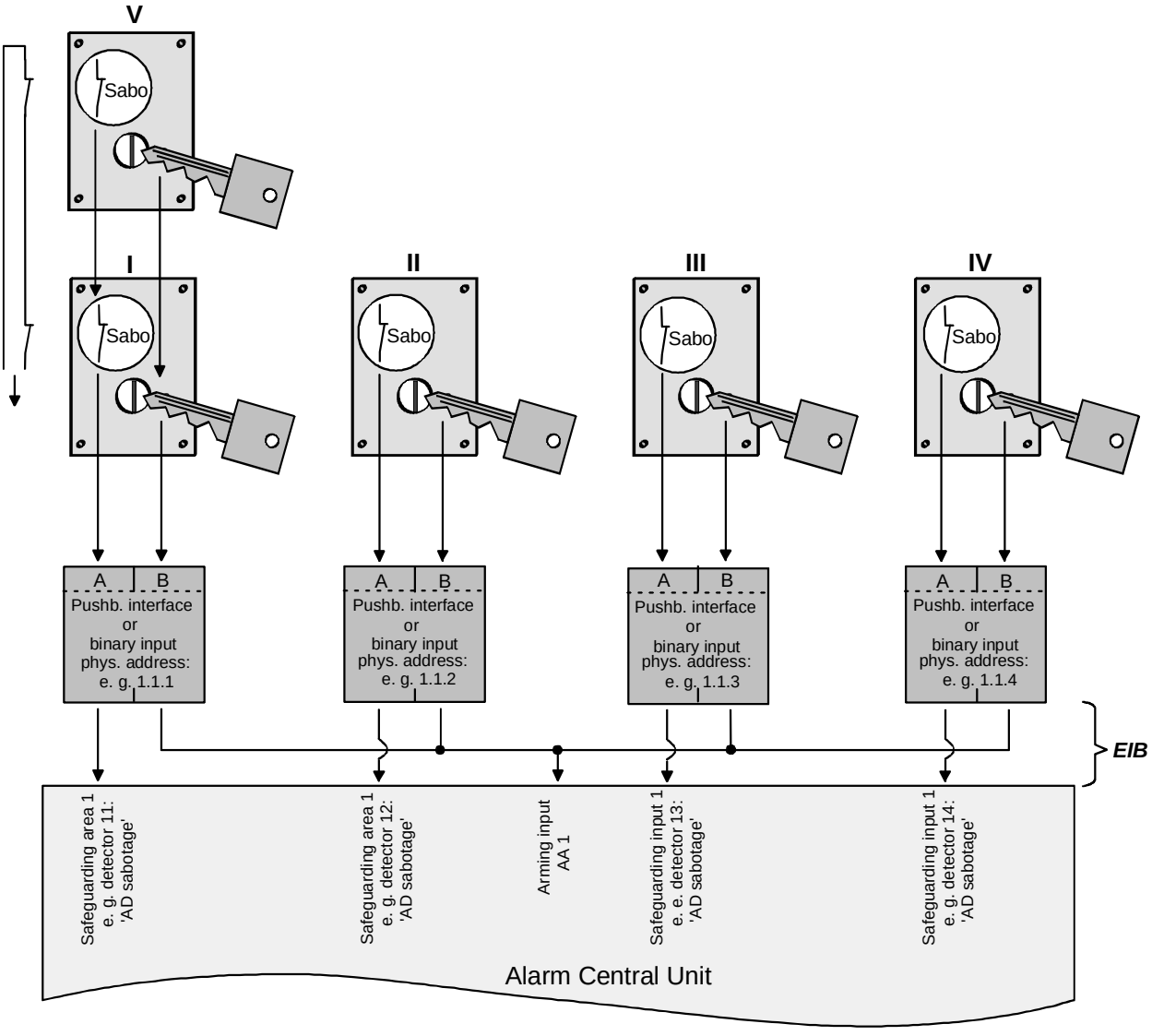
Example 1:

A maximum of four independent arming devices per arming area (I - IV).
For this purpose, it is assumed that all arming devices have been connected through bus devices, each of them having a different physical address.
Such circuitry is recommended, for this will be the only way to enable the alarm central unit to clearly distinguish among the individual arming devices. If one of the devices has been tampered with you can still use the remaining arming devices for disarming.



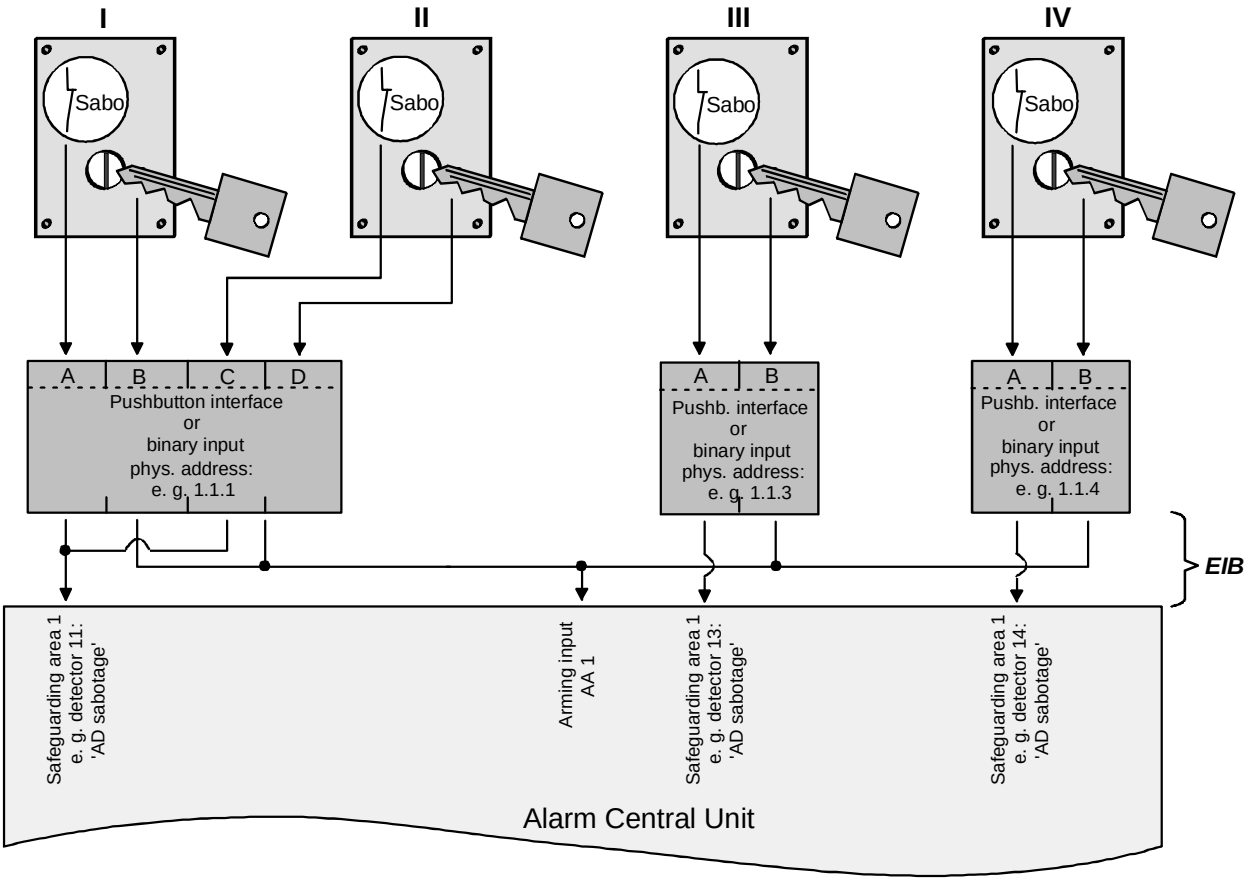
Example 2:

Five arming devices per arming area, two of them being independent of each other (I + V), i. e. they act together on the same input of the pushbutton interface/binary input.
Thus, these two arming devices have the same physical address and can no longer be clearly distinguished between by the alarm central unit. The sabotage contacts of the independent arming devices (I + V) must be connected in series and act on the same input. Once one of the interdependent arming devices has been tampered with, you can no longer use both of these devices for disarming. However, disarming through the independent arming devices (II - IV) will still be possible.



Example 3:

Four arming devices per arming area, two of them being independent of each other (I + II), i. e. they act together on the same input of the pushbutton interface/binary input.
Thus, these two arming devices have the same physical address and can no longer be clearly distinguished between by the alarm central unit. Although the sabotage contacts of the interdependent arming devices (I + II) have been connected to different inputs of the pushbutton interface/binary input, they act, however, on the same input in the alarm central unit as only one 'Sabo SE' (arming device sabotage input) can be linked to one physical address. Once one of the interdependent arming devices has been tampered with, you can no longer use both of these devices for disarming. However, disarming through the independent arming devices (III + IV) will still be possible.



4.2 Alarm reset

The alarm central unit has an "alarm reset" ETS object (polarity: "1" = alarm reset/"0" = no response) through which alarms and all fault signals can be reset and messages in the displays acknowledged. To be able to reset fault signals it is assumed that the messages have been called into the display by the user (if any display units have been activated).
If, for example, arming devices have been tampered with, or the system can no longer be disarmed for any other reasons, this alarm reset will be the only way to deactivate an alarm or to acknowledge signals. Also in configuration 1 (only "fire detector" and "attack detector"), you can only cancel an alarm by the alarm reset option. Therefore. it is absolutely necessary that you set this in configuration 1.
For these reasons, it is recommended that, for example, you should hide a pushbutton sensor in the vicinity of the place where the alarm central unit has been installed and configure it to the alarm reset object. If you do not assign a group address to this object the ETS plug-in will issue a message to point to this unassigned object when you exit the tool.

4.3 Signalization/acknowledgement

When you arm and disarm the system the alarm central unit can confirm ("acknowledge") its change of state through the alarm indicators. So it will be possible to recognize whether the system has, as desired, responded to an arming or disarming request or not. This is, above all, important when you operate the system from outside without seeing the display units.

In addition, various signals for the state indication of an arming area are available. You can pick off such signals through EIB objects.
For example, the "static armed state signal" and the "static disarmed state signal" per arming area statically indicate the armed/disarmed state of the system.

"Static armed state signal": "1" = AA is in the armed state/"0" = AA is in the disarmed state,
"Static disarmed state signal": "1" = AA is in the disarmed state/"0" = AA is in the armed state.

Furthermore, two dynamic status signals are available which trigger the "armed state signal pulse" or the "disarmed state signal pulse" ETS objects. Compared with the static signals, the pulse signals are time-limited. In this connection, the "armed/disarmed state signal pulse" time under the "alarm central unit" parameter branch defines the "1" triggering period or the pulse time, respectively. A "0" object value stands for 'not triggered'.

"Armed state signal pulse: "1" (object triggered after the pulse time) = the AA has been armed,
"Disarmed state signal pulse: "1" (object triggered after the pulse time) = the AA has been disarmed.

Acknowledgement can be made through the alarm indicators in the form of a visual or audible feedback. Thus, the flashlight, the indoor or outdoor siren or the potential-free relay contact can acknowledge arming or disarming for each arming area. Per arming area, you can use the "acknowledgement by …" parameters in the "arming" parameter branch to assign the alarm indicators to an acknowledgement.
Under the "alarm central unit" parameter branch, you can separately parameterize for the "armed" and "disarmed" states the acknowledging periods for the alarm indicators. So the "armed state acknowledging time" will be started if arming has been successful, whereas the "disarmed state acknowledging time" will start running after successful disarming.
If you are arming the system (arming request) and the areas concerned are, however, not ready for arming yet no acknowledgement will follow, i. e. the alarm indicators assigned to an acknowledgement will not be triggered (negative acknowledgement).
To clearly recognize arming or disarming you should parameterize different lengths of the "armed state" and "disarmed state" acknowledging times.

Feedback through an alarm transmission device ("ÜG-Scharf" (armed state signal to the ATD) terminal or ETS object) is also possible for arming/disarming. For this purpose, set the "signalization by 'armed state signal' to ATD = "yes"" parameter in the "arming" parameter branch separately for each arming area.
Since the "armed state signal to the ATD" signal may sometimes be used by the up to four arming areas the configuration window in the ETS plug-in will indicate the areas assigned to this signal in the "'armed state signal' to the ATD" option used by" line.

Display units will give additional information on the states of the system and of the detectors. For simpler systems in the form of indicator lamps (ON/OFF), and for more comfortable systems, info display units will inform you on the state of the system by text messages such as "kitchen window - open".

4.4 Pre-alarm

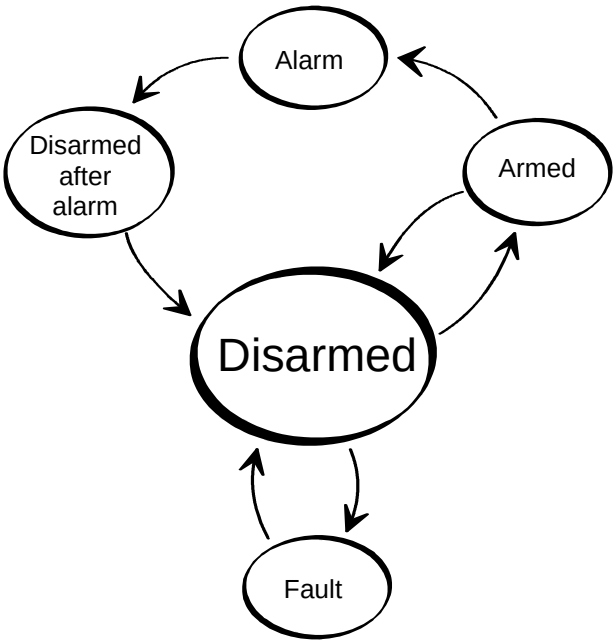
Once a delayed detector in an armed area has tripped, the alarm delay time (parameterizable per arming area from the "arming" parameter branch) will be started and a pre-alarm raised through the "pre-alarm" ETS object. Visual or audible alarm indicators will primarily be triggered by this object. So a person entering the building from outside through the front door in the 'internally armed' state will recognize that the alarm delay time is running and that disarming should take place as soon as possible.
If disarming takes place within the alarm delay period no alarm will be raised.
A pre-alarm will not be recorded in the event log.

4.5 Disarmed after alarm

After an alarm has been reset by disarming through an arming device of the arming area or through the alarm reset option (all audible alarm indicators are deactivated) the system will change to the "disarmed after alarm" state (refer to "4.6 System states", page 34). In this state, the "disarmed after alarm" EIB object which is available in each arming area will be triggered.
In this way, an alarm not detected before due to the fact that all alarm indicators had already been in the deactivated state when disarming was taking place can be detected subsequently. In such case, the "disarmed after alarm" signal should trigger visual or audible alarm indicators (if necessary, even the alarm buzzer of a display unit).

4.6 System states

Depending on the state the individual arming areas have taken, the alarm central unit will respond to incoming signals or commands in different ways. You can distinguish among the following states:



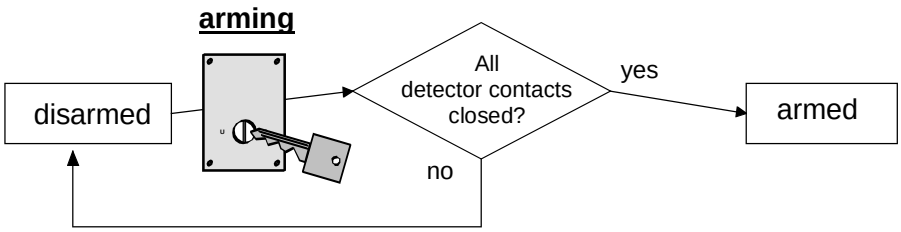
"Disarmed" state:

If some safeguarding areas (SA 1, SA 2, SA 3 or SA 4) have been disarmed intruder and sabotage signals in such areas (e. g. opening a window or opening the enclosure of the alarm central unit) will not lead to alarm. In such state, sabotage signals will result in an alarm central unit fault signal which will be transmitted through the corresponding ETS object (refer to "fault" state).
The "disarmed" state can be indicated for each arming area through the "static armed/static disarmed state signal" objects.

In this state, you can address and programme the alarm central unit via the bus.

"Armed" state:

You can only arm an area as soon as all detectors assigned to such area are not active, i. e. do not trip, and if there is no fault. The display units will indicate this by reading the "ready for arming" message. In systems without display units, this state can be indicated through the "ready for arming" object ("0" = not ready for arming/ "1" = ready for arming).



Once an arming area has been activated, its assigned safeguarding safeguarding areas will be kept under surveillance. In such case, intrusion and attack signals will raise alarm in this arming area. Depending on the application and the distribution of the safeguarding areas (configuration), you can distinguish between:

- internally armed: Only the outer shell of a building will be kept under surveillance. The user is in the inside and will not raise an alarm unless he/she interferes into the outer shell. Although motion detectors installed in the inside will recognize his/her movements, no alarm will be raised. Sabotage signals from the inside will cause an alarm central unit fault signal.
  and
- externally armed: All internal and external detectors will be monitored. If any of the detectors or even a sabotage detector responds alarm will be raised.

If an area is not ready for arming you can read "not ready" in the displays, the value of the "ready for arming" object being "0". Before you can do arming in this case, you must recognize and eliminate the cause such as an open detector. The display units will indicate open detectors.

You can parameterize an arming delay time per arming area. This time may become necessary if the arming device is located within an area to be safeguarded, and, in addition, if such area must be left before arming. The delay time specifies the time after which the system will really be armed after an arming command (plan some time reserve). Only after the delay time has elapsed, no detector (this also applies to the sabotage contact) must still be active, or arming will not take place.

In this state, you cannot address and programme the alarm central unit via the bus. Nevertheless, if you try to do so such access will raise an alarm in the armed areas. Access via the bus in this state will be recorded in the event log.

"Alarm" state:

If a detector within an armed safeguarding area responds the alarm system will change to the "alarm" state. The alarm indicators - siren, flashlight, alarm transmission device, etc. - will be activated (in accordance with how they have been programmed).
If you have parameterized detectors as "delayed" a "pre-alarm" per arming area can first be raised through the "pre-alarm" object. The transition into the "alarm" state will then only follow after the corresponding alarm delay time, which you can parameterize per arming area, has elapsed.

If another detector trips after an alarm has already been raised (alarm indicators activated for a certain period have already been switched back off) a subsequent alarm will follow. This will reactivate all alarm indicators parameterized to a certain time period. A subsequent alarm will also directly trigger inputs parameterized as "delayed".
You can only deactivate an alarm through arming devices of the arming area (disarming) which have not been tampered with or through the alarm reset option.

In this state, you cannot address and programme the alarm central unit via the bus. Nevertheless, if you try to do so such access will raise a subsequent alarm in the armed areas after the alarm indicators have already ceased after the first alarm. Bus access in this state will be saved in the event log.

Note: The following applies to all configurations: Once an alarm has been raised in an arming area, all the other areas will not be ready for arming before the alarm is reset.

"Pre-alarm" state:

After a delayed detector has tripped in the armed state because a safeguarded area was, for example, entered before disarming the "pre-alarm" will only be activated if you have parameterized an alarm delay. In this state, you can disarm the area without raising an alarm. A pre-alarm will not be stored in the event log.

In this state, you cannot address and programme the alarm central unit via the bus.

"Disarmed after alarm" state:

After an alarm has been reset by disarming through an arming device of the arming area or through the alarm reset option (all audible alarm indicators are deactivated) the system will change to the "disarmed after alarm" state.
After an alarm, you must always recognize and eliminate the cause which has led to such alarm.
In this state, tripped detectors of an arming area will be indicated by the display units if you have parameterized such display units. In this connection, all events from the arming of the system up to its disarming will be displayed.
Before you can return to the "disarmed" state you will first have to call all messages into one of the display units.
You can initiate the change of state by disarming again through an arming device of the arming area after the messages have been processed.
If you actuate the alarm reset option you can change back to the "disarmed" state without having called the messages into the display units.

You can only re-arm the system after you have reset all previously tripped detectors of the safeguarding areas concerned. The tripped detectors will be indicated in the display units.

Only in the "disarmed" state, the event log, which stores all tripped detectors one after the other, all alarms as well as all arming/disarming commands, can be read out by the ETS plug-in (refer to "9. Event Log", page 57).

In this state, you cannot address and programme the alarm central unit via the bus.

Notes on configurations 5.X and 7.X:

Please note for the "cascaded" configurations that the subordinate areas will remain armed after you have reset the higher-ranking area (AA 4) into the "disarmed" state. If any detectors of an area subordinate to AA 4 have already raised an alarm they will no longer be evaluated in the subordinate area until you disarm the area. However, these detectors which have already tripped will not prevent the higher-ranking area (AA 4) from being re-armed. Such detectors can, once more, raise alarm in the higher-ranking area.

"Fault" state:

The system will change to the "fault" state if the functioning of individual components is adversely affected to such an extent as not to guarantee proper operation any longer.
In a disarmed area, a fault will entail that such area can no longer be armed. In such case, the fault must first be recognized and eliminated, if necessary. Also for nested or cascaded areas (refer to "1.3 Configurations", page 19), this may lead to the effect that you even cannot arm higher-ranking areas any longer.
So, for example, sabotage of an arming device in a disarmed area will result in a fault signal. In an armed area, such tampering would raise an alarm (sabotage alarm).
In the event of a 'global' fault signal such as mains voltage failure, an open sabotage contact of the alarm central unit or an interrupted or resistance-manipulated sabotage circuit, the fault signal must be acknowledged separately in each arming area until the individual arming areas are ready for arming again.

Fault messages will be transmitted through the "alarm central unit fault" ETS object or through an alarm transmission device ("ÜG-S" terminal or "fault signal to the ATD" ETS object). The latter only applies in the event of bus voltage failure, mains voltage trouble, alarm transmission device malfunctioning, or to an abortive heartbeat check among the alarm central units.

In this state, you can address and programme the alarm central unit via the bus.

4.7 Arming behaviour in dependence of the configuration

Arming areas can take different states at the same time and independently of one another. If areas are nested with one another or cascaded (refer to "1.3 Configurations", page 19) their states may possibly influence one another.
For example, individual arming areas, regardless of what their configurations are, can thus not be armed as soon as only one of them is in the "alarm" state.

Internally/externally armed:

- External arming:
  The higher-ranking arming area (e. g. AA 2) can only be activated if its subordinate area (e. g. AA 1) is ready for arming. If there is a fault in this area, or if a detector is permanently open, you cannot arm the system.

- Internal disarming:
  In the "internally armed" state (e. g. AA 1 is armed), you can disarm the system through an arming device of the higher-ranking area (e. g. AA 2) by arming or disarming on this device. This will be possible in the "internally armed" or "pre-alarm" states.
  In addition, signals can also be acknowledged in the "disarmed after alarm" or "fault" system states in the subordinate area by the arming device assigned to the higher-ranking area.

  In the "internally armed" state and in the event of an alarm, the latter can also be deactivated by an arming device assigned to the higher-ranking area, provided that this device has not been tampered with.

  Once an "external" arming device has been tampered with in the "internally armed" state and if you try to do disarming through the device tampered with a sabotage alarm will be immediately raised in the subordinate area. In addition, the higher-ranking area will change into the fault state as soon as the sabotage of the arming device has been detected. You can only view such fault in the display units (if parameterized) after you have disarmed the subordinate area.

Cascaded:

- Arming:
  You can only arm the higher-ranking area (AA 4) after you have armed all areas subordinate to it. Therefore, the higher-ranking area cannot be activated if there is a fault or if there are open detectors in the subordinate areas.
  Once the higher-ranking area (AA 4) has been armed, the arming devices assigned to the subordinate areas are deactivated, i. e. you can no longer use them for disarming. Tampering with a subordinate arming device will lead to an alarm when AA 4 is in the armed state.

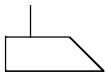
- Disarming:
  You can only disarm the subordinate areas after you have already disarmed the higher-ranking area (AA 4).
  Please note for the "cascaded" configurations that the subordinate areas will remain armed after you have reset the higher-ranking area (AA 4) into the "disarmed" state. If any detectors of an area subordinate to AA 4 have already raised an alarm they will no longer be evaluated in the subordinate area until you disarm the area. However, these detectors which have already tripped will not prevent the higher-ranking area (AA 4) from being re-armed. Such detectors can, once more, raise alarm in the higher-ranking area.

Important:

- In the event of a 'global' fault signal such as mains voltage failure or an open sabotage contact of the alarm central unit, the fault signal must be acknowledged separately in each arming area until the individual arming areas are ready for arming again.

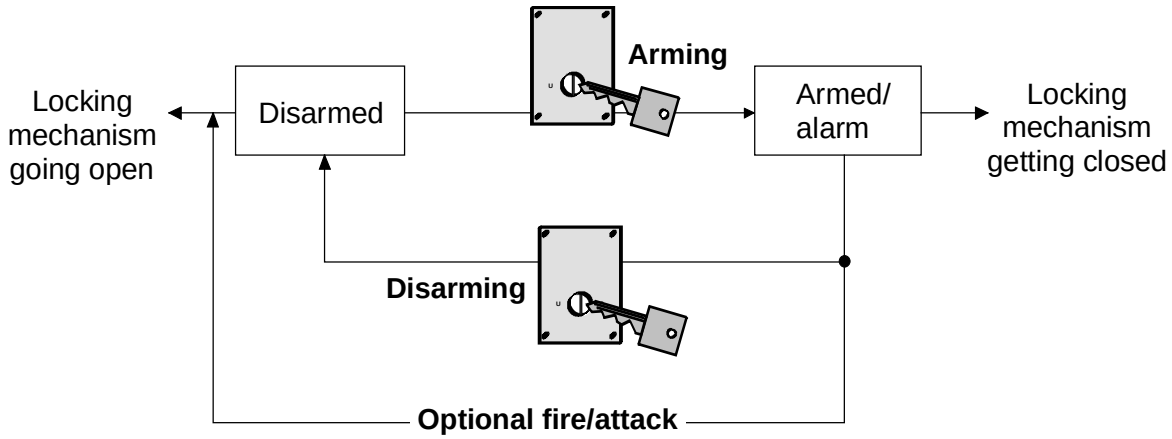
- Please note that both the alarm reset option and the actuated arming devices, for example, to reset an alarm will act on other areas where they can reset signals or possibly disarm such areas.

4.8 Connecting components to implement forced arming



- Motor-driven locking element and pulse door opener:
  An authorized person should only be allowed to enter a safeguarded building if no alarm is raised thereby, i. e. if the alarm system is in the disarmed state. For this purpose, you can install additional door locking mechanisms which will only permit the opening of the door and access to the room while the system is in its disarmed state (forced arming).
  The door locking mechanisms such as motor-driven locking elements or pulse door openers can be coupled to the bus through suitable EIB components and triggered by the static or dynamic arming/disarming signals per arming area.
  In this connection, the locking mechanisms will go open or closed when the corresponding areas are being armed or disarmed. If you have parameterized an arming delay time for such area the door locking mechanisms will be activated correspondingly later.

  From the ETS plug-in, you can parameterize whether the door locking mechanisms are expected to go open earlier by a static or dynamic disarming signal in the event of a fire or an attack alarm, i. e. already when such alarm is being raised. Thus, it will be possible to keep open the way out, for example, in case of fire.
  The "open blocking element in case of fire/attack" parameter exists per arming area in the "arming/arming area X/armed state/disarmed state acknowledgement" parameter branch.
  If you have set "static disarming signal yes" or "disarming signal pulse yes" a disarming signal will always be issued through the signal outputs immediately after a fire or an attack alarm in accordance with what you have parameterized, no matter whether the arming areas are in the armed or unarmed states.
  Setting "no" will be typical if you do not use any door locking mechanisms. If you do have locking mechanisms under this option please note that they will not go open earlier in the event of a fire or an attack alarm.



Note:

Such additional door locking mechanisms will prevent unintentional access to an armed area. They should not be equated with mechanical locks, and they are not necessarily of the same mechanical stability either.

- Block connecting link:

A block connecting link can be installed into the front door or into the door to the flat instead of a conventional bolt lock. You can operate it through a common closing cylinder.
You can use a block connecting link to open or close the door and, at the same time, to arm or disarm the alarm system. In this connection, the first shifting of the bolt normally causes the door to be mechanically locked. The second shifting of the bolt will arm the alarm central unit. For this purpose, you will need the information whether all detectors are closed, i. e. the system is in the ready-to-arm state.
If this is the case, current is applied to a coil in the block connecting link which facilitates the second shifting of the bolt. If the alarm system has not enabled arming yet, for example, because a window is still open, the second shifting of the bolt will be mechanically blocked. The "ready to arm" information can be sent to the block connecting link through a suitable switching actuator which is connected to the EIB and linked with the "ready to arm" ETS object of the corresponding arming area.
The arming contact of the block connecting link can be connected to the "arming input" ETS object of the alarm central unit through a suitable binary input.

Likewise, you can only enter the safeguarding area after you have disarmed it through the block connecting link.

- Interlock switch contact:

An interlock switch contact (also: striking plate contact) facilitates lock monitoring of a door. It can be mounted into the striking plate of the door frame so that the door lock bolt will press against a micro switch of the interlock switch contact when the door is being locked. Thus, it can be signalled whether the door is locked or not. The alarm central unit can use this information to monitor the locks of the entrances to the safeguarding areas. Instead of raising alarm, an interlock switch contact will prevent the arming of the safeguarding area concerned as long as the door is not locked.
You can only arm the alarm central unit after the lock bolt of the door has been extended.

Note:
Any arming delay will not be interrupted as long as locking mechanism detectors are active (unlocked doors). Only after the delay time has elapsed (actual arming), all doors must be locked.

You should not use an interlock switch contact to arm or disarm alarm systems as, otherwise, breaking the door open could disarm safeguarded areas.

Via suitable binary inputs and through the ETS objects, you can connect interlock switch contacts to detector inputs of the alarm central unit configured as "locking mechanisms".

5. Operating the Alarm Central Unit

5.1 Display units

The alarm central unit can trigger various display units. Thus, the system states of the alarm central unit can be visualized and signals polled through up to four independent display units. EIB objects, by means of which you can, for example, trigger suitable info display units or display panels, are available for the coupling of the display units.
In this connection, you can trigger more than four display units by multiple configuration of the group addresses. In this case, the information to be viewed will, however, be identical for the display units having the same assignments.

It is not necessarily required to use display units for the operation of the alarm central unit. Although you can operate the system without any display units, it is not recommended to do so. So, for example, you can only clearly recognize the reason why you cannot arm the system (open detectors) if you use display units.

5.1.1 Enabling the display units

Depending on the configuration, the ETS plug-in will automatically suggest the maximum number (up to four) of independent display units.
Through the "display unit X available" parameter in the "display/display unit X" parameter branch, you can optionally activate (setting = "yes") the display units created.
In this connection, you can assign an unambiguous identification text to each display unit. Such text has no limited number of characters and is solely displayed in the ETS plug-in.

Furthermore, you can use the "displayed areas" parameter for the selected display unit in this parameter branch to fix, in principle, which of the arming areas or of the "fire detector" and "attack detector" safeguarding areas can be viewed in the corresponding display unit while the alarm central unit is in operation.

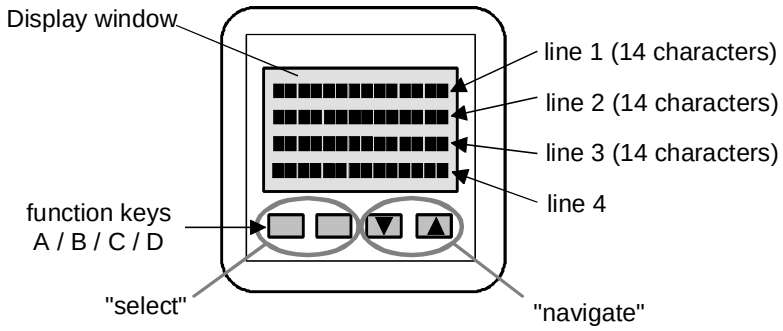
If you have activated only one display unit in your configuration please note that you will first have to view or acknowledge various signals in the display units before you can reset them (refer to "5.2 Arming/disarming and alarm acknowledgment operations", page 44).

The "fire detector" and "attack detector" areas will only be visible in the display units if they have, in principle, been enabled from the ETS plug-in (see above) and an event (tripped detector) has occurred in these areas.
Configuration 1 ("fire detector" and "attack detector" only) represents an exception. In this configuration, the "fire detector" and "attack detector" areas will always be visible in the display units.
To enable the user of the system even in this case to get informed on signals of the alarm central unit, global fault signals (mains voltage failure, battery fault, ATD checkback contact fault, abortive heartbeat check between two alarm central units (if a missing telegram is to be evaluated in the same way as a fault), opening of the sabotage contact or an interruption in the wired sabotage circuit) will also cause alarm central unit faults in this configuration. Such events will only be indicated by the display units until they have been eliminated. Therefore, they need not be acknowledged. In such case, no active alarm central unit fault signal will be transmitted through the EIB object or the alarm transmission device.

5.1.2 Triggering the display units (by the example of concealed info display unit 2.0 from version 2.x or later)

Through the info display unit, a great variety of information on the general EIB installation can be visualized. To enable info display unit 2.0 to issue information of the alarm central unit you must have parameterized a page in the ETS plug-in of the display as "page function = alarm central unit display". When doing so, you will permanently assign certain functions to the individual text lines and display keys.

Updating the display contents is event-controlled for this page function. Thus, the alarm central unit will update the display texts automatically once any change of the system state (e. g. faults or alarms) occurs in an area.
In the armed state or in the "alarm" state, the display texts of the arming areas concerned will always be hidden.



Text lines:

Line 1 will be addressed by the alarm central unit. For this purpose, a "line 1" ETS object used for the display is enabled to which the alarm central unit sends the text to be issued. Thus, the identification text for the arming areas or for the "fire detector" or "attack detector" areas parameterized from the ETS plug-in will be displayed in this line, depending on which of these areas you have selected by the two function keys on the left.

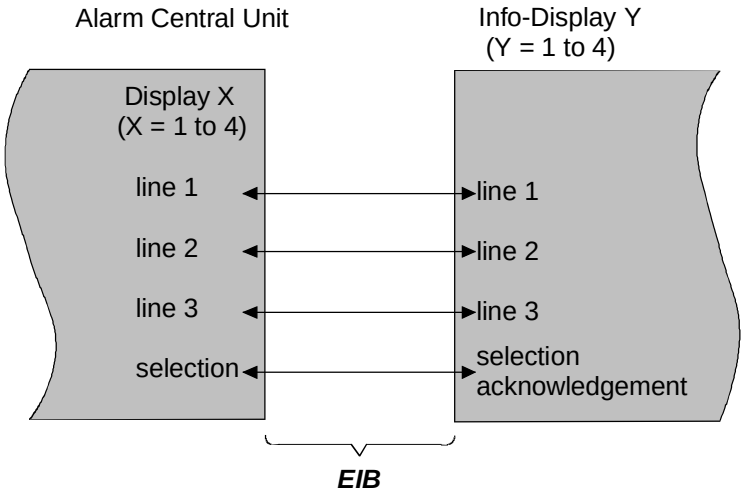
Line 2 will also be addressed by the alarm central unit through the "line 2" ETS object. At this position, the alarm central unit will issue the editable detector texts or, if no detectors are concerned, directly indicate the system state of the area selected in line 1.

Line 3 will complete line 2, i. e. the detector states will be displayed if any detectors are concerned, or further text messages will be issued. In the "disarmed after alarm" state, the exact time and date when the alarm was raised will, among other things, be visualized at this position (refer to "4.6 System states/"disarmed after alarm" state", page 34).

Line 4 can be parameterized from the ETS plug-in of the info display unit through the "line 4 text" parameter. In this line, you should 'name' the functions of the function keys below (refer to the description of the function keys given later). Line 4 will always display the entered text in inverse form.

Assignment of the ETS objects between the alarm central unit and the info display units:

Link the display objects of the alarm central unit to the ETS objects of the info display unit 1:1 per display unit.



When you use info display unit 2.x the object polarities will be fixed and cannot be changed (refer to the description of the function keys).

If you want to use more than four display units you must assign the corresponding group addresses of the EIB objects several times. In this case, the areas to be viewed will, however, be identical for the display units having the same assignments.

5.1.3 Readable information and text output control
(by the example of concealed info display unit 2.0 from version 2.x or later)

The info display unit has function keys, by means of which you can trigger the alarm central unit and thus control the text output in the display:

Key A (outer left) and key B (left middle):
"Select" function. Use the "key 1 function" and "key 2 function" parameters in the parameter branch of the page to define the function of these keys from the ETS plug-in of the info display unit. In this connection, you can distinguish between the following two functions.

- "more…"
  In this case, a "1" telegram will be sent to the alarm central unit through the "select" EIB object when you actuate this key. You can use this function to scroll one by one through the areas enabled for the display, i. e. you can call all messages of the alarm central unit in the enabled areas step by step. When you reach the last message of the last area you will automatically 'jump' back to the first message of the first area after actuating the key once more.

- "Back to previous area"
  In this case, a "0" telegram will be sent to the alarm central unit through the "select" EIB object when you actuate this key. This will induce the alarm central unit to change to the enabled areas in backward order. If any messages have been issued for an area you can 'jump' back to the beginning of the visible areas without having all other areas displayed. Successively actuating the key several times will cause the 'skipping' of several areas.

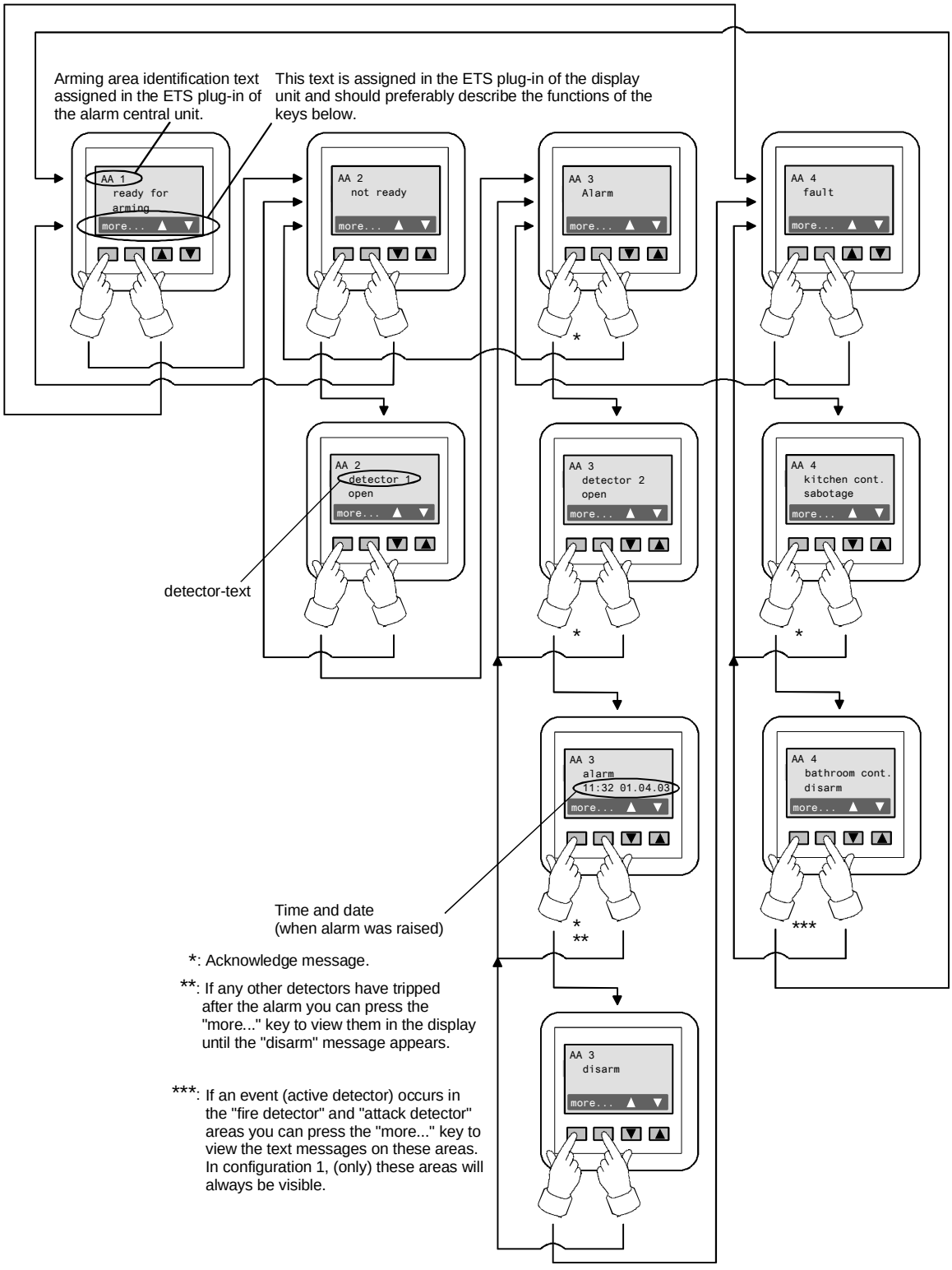
Key C (right middle) and key D (outer right):
"Navigate" function. Actuating one of these keys (C or D) will change the pages configured in the info display unit. If you use only one page in the display (alarm central unit display) actuating keys C and D will have no function.

The operational chart on the next page is to explain the selection control and navigation in the display.

The following operational chart takes into consideration a configuration with four independent arming areas.

Example: AA 1 is ready for arming; AA 2 is not ready because of an open detector; AA 3 is in the "disarmed after alarm" state; AA 4 is in the "fault" state since a sabotage detector is open and a second one was open. The "fire detector" and "attack detector" areas cannot be viewed in this configuration as no event (no active detector) has occurred in these areas.

You can actuate key A or B to change among the display texts or to acknowledge messages.



*: Acknowledge message.

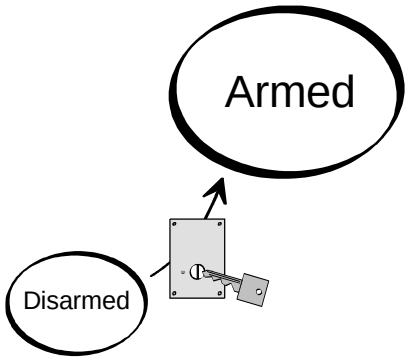
**: If any other detectors have tripped after the alarm you can press the "more..." key to view them in the display until the "disarm" message appears.

***: If an event (active detector) occurs in the "fire detector" and "attack detector" areas you can press the "more..." key to view the text messages on these areas. In configuration 1, (only) these areas will always be visible.

5.2 Arming/disarming and alarm acknowledgement operations

5.2.1 Arming

The corresponding area must be ready for arming in the "disarmed" state. The display units will signal such readiness by issuing the "ready for arming message" per arming area.
For this purpose, it is assumed that the corresponding arming area has been assigned to at least one display unit in the ETS plug-in. If there is no display unit the readiness for arming can be recognized through the "ready for arming" ETS object provided per arming area.
For arming, a "1" telegram must be received from an 'authorized' bus device as an arming request through the "arming input" ETS object. Each arming area has an object of its own for this purpose. In addition, you can issue acknowledgement through different alarm indicators.



e. g. key-operated switch

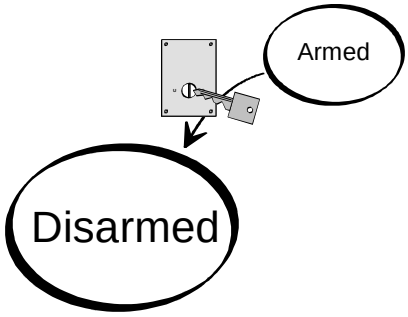
Once some areas have been armed (wait any possible arming delay periods), the display texts of all activated arming areas will no longer be visible in the displays.

5.2.2 Disarming

For disarming, a "0" telegram must be received from an 'authorized' bus device through the "arming input" ETS object. In this connection, you can issue acknowledgement through different alarm indicators. You can also effect disarming by resetting the alarm.

Important: Please note that alarm resetting will also act on other areas, resetting signals or possibly disarming such areas.

Unless any alarm has been raised before, the displays will read "ready for arming". If any locking mechanism detectors are open a "not ready" message will be caused in the displays after disarming as such are will then not be ready for arming.



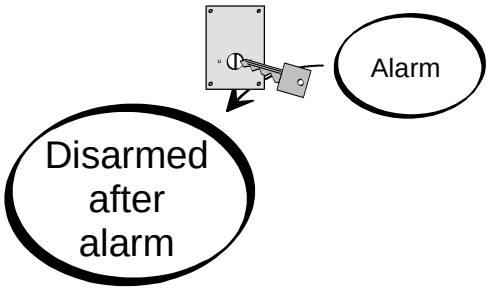
e. g. key-operated switch

5.2.3 Alarm acknowledgement after intruder or sabotage alarm

For resetting an alarm, a "0" telegram must be received from an 'authorized' bus device through the "arming input" ETS object. In this connection, the audible alarm indicators will be switched off if these are still active. The flashlight and the intruder signal alarm transmission device will remain active if they had been on at the time of resetting. The flashlight can already be deactivated when the alarm is being reset if it was activated for a certain time only when the alarm was being raised. In this case, the flashlight will be off in the "disarmed after alarm" state.
The area will change into the "disarmed after" alarm state ("disarmed after alarm" EIB object = "1"). You can also deactivate the alarm by resetting it. If arming devices have been damaged or tampered with you can no longer use such devices for disarming.

Important: Please note that alarm resetting for cancelling an alarm will also act on other areas, resetting signals there or possibly disarming such areas.

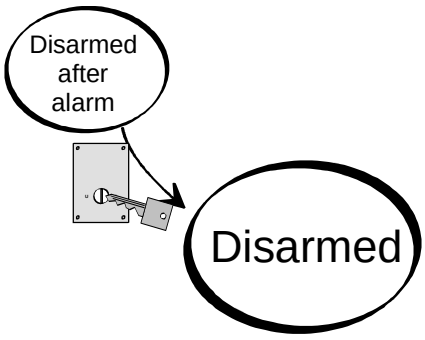
After you have reset the alarm, you can view the event log in the display units, beginning with the "alarm" message. For this purpose, it is assumed that the areas concerned will be visible in the displays (can be set from the ETS plug-in).
All events which have occurred in this area between the last arming operation and disarming (deactivation of the alarm) will be displayed.



e. g. key-operated switch

After all messages have been processed ("disarm" message visible) you can actuate the arming device once again (disarming) of the area concerned or reset the alarm to change into the "disarmed" state. If you use the alarm reset option you can change back to the "disarmed" state without having called the messages into the display units.
At this position, the visual alarm indicators (flashlight) will be switched off at the latest. The intruder or sabotage signal will be cancelled on the "safeguarding area X alarm" EIB object of the arming area concerned and in the alarm transmission device ("ÜG-E" terminal and "intruder signal to the ATD" EIB object) if you have parameterized this.

Please note for the "cascaded" configuration that the subordinate areas will remain armed after you have reset the higher-ranking area (SA 4) into the "disarmed" state. Any detectors which have already tripped and have caused the alarm will no longer be evaluated until you disarm the area concerned.



e. g. key-operated switch

Only in the "disarmed" state, the entire event log, which stores all tripped detectors one after the other, all alarms as well as all arming/disarming commands, can be read out by the ETS plug-in (refer to "9. Event Log", page 56).

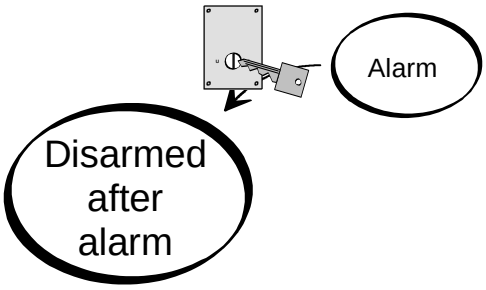
The alarm system can then change into the "fault" state if, for example, a sabotage contact was the detector which has raised the alarm and if this detector is still open, a global fault has occurred, or if detectors are missing. You will then have to separately reset the consequential fault. For this purpose, you need not call the fault message into the displays once more and acknowledge it in those areas where the fault has already raised an alarm. To be able to reset a fault message you must have eliminated the cause of the fault.
Even such faults which do not raise any alarm (e. g. mains voltage faults, battery faults or faults in the alarm transmission device) will lead to the system changing into the "fault" state.

5.2.4 Alarm acknowledgement after a fire alarm

For resetting a fire alarm, a "0" telegram must be received from an 'authorized' bus device of any arming area through the "arming input" ETS object. In this connection, the audible alarm indicators will be switched off if these are still active. The flashlight and the fire signal alarm transmission device will remain active if they had been on at the time of resetting. The flashlight can already be deactivated when the alarm is being reset if it was activated for a certain time only when the alarm was being raised. In this case, the flashlight will be off in the "disarmed after alarm" state.
The "fire detector" safeguarding area will change to the "disarmed after alarm" state. You can also deactivate the alarm by resetting it (only possible in configuration 1).

Important: Please note that both the alarm reset option and the actuated arming devices, for example, to reset a fire alarm will act on other areas where they can reset signals or possibly disarm such areas.

Already during the fire alarm and after you have reset the alarm, you can view the event log in the display units, beginning with the "alarm" message. For this purpose, it is assumed that the "fire detector" area will be visible in the displays (can be set from the ETS plug-in). If any fire detectors have already been deactivated (closed) at this time they will be displayed for a maximum period of 8 seconds when the event log is being processed.
All fire detectors which have raised the alarm will be displayed.



e. g. key-operated switch

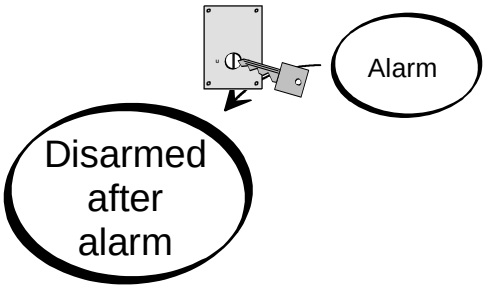
You can actuate one of the arming devices (disarm) again or reset the alarm to change back into the 'normal' ready state. This will, however, only be possible if you have reset all tripped fire detectors. In this case, you can read the tripped detectors in the fire detector areas of the display units with the addition "disarm", or "disarm" will solely be displayed when detectors have already been deactivated (closed) again and the same have already been acknowledged in the display units. It is not necessarily required to view the event log for a fire alarm on the display units, i. e. to acknowledge the fire signals which, on the other hand, will be the only way to clearly recognize the tripping detectors.
The visual alarm indicators (flashlight) will be switched off upon the return to the ready state at the latest. The fire signal will be cancelled on the "fire alarm" EIB object and in the alarm transmission device ("ÜG-F" terminal).
Only in the 'normal' ready state, the event log which stores all tripped detectors one after the other and all alarms can be read out by the ETS plug-in.

5.2.5 Alarm acknowledgement after an attack alarm

For resetting an attack alarm, a "0" telegram must be received from an 'authorized' bus device of any arming area through the "arming input" ETS object. In this connection, the audible alarm indicators will be switched off if these are still active. The flashlight and the attack signal alarm transmission device will remain active if they had been on at the time of resetting. The flashlight can already be deactivated when the alarm is being reset if it was activated for a certain time only when the alarm was being raised. In this case, the flashlight will be off in the "disarmed after alarm" state.
The "attack detector" safeguarding area will change to the "disarmed after alarm" state. You can also deactivate the alarm by resetting it (only possible in configuration 1).

Important: Please note that both the alarm reset option and the actuated arming devices, for example, to reset an attack alarm will act on other areas where they can reset signals or possibly disarm such areas.

Already during the attack alarm and after you have reset the alarm, you can view the event log in the display units, beginning with the "alarm" message. For this purpose, it is assumed that the "attack detector" area will be visible in the displays (can be set from the ETS plug-in). If attack detectors have already been deactivated (closed) at this time they will be displayed for a maximum period of 8 seconds when the event log is being processed.
All attack detectors which have raised the alarm will be displayed.



e. g. key-operated switch

You can actuate one of the arming devices (disarm) again or reset the alarm to change back into the 'normal' ready state. This will, however, only be possible if you have reset all tripped attack detectors. In this case, you can read the tripped detectors in the attack detector areas of the display units with the addition "disarm", or "disarm" will solely be displayed when detectors have already been deactivated (closed) again and the same have already been acknowledged in the display units. It is not necessarily required to view the event log for an attack alarm on the display units, i. e. to acknowledge the attack signals which, on the other hand, will be the only way to clearly recognize the tripping detectors.
The visual alarm indicators (flashlight) will be switched off upon the return to the ready state at the latest. The attack signal will be cancelled on the "attack alarm" EIB object and in the alarm transmission device ("ÜG-Ü" terminal).
Only in the 'normal' ready state, the event log which stores all tripped detectors one after the other and all alarms can be read out by the ETS plug-in.

5.3 Fault acknowledgement operations

The alarm central unit knows various causes of faults. Fault messages will be read in the display units in dependence of the areas concerned.

A fault can have one of the following causes:

Cause of Fault	Message Text in the Display Units	Remark			
Missing detector in a safeguarding area.	**"[detector text] missing detector"**	1)			
The sabotage detector of a safeguarding area has tripped.	**"[detector text] sabotage"**	1)			
The sabotage detector of an arming device has tripped.	**"[detector text] sabotage (AD)"**	1)			
The sabotage loop of the alarm central unit has been interrupted or short-circuited.	**"Alarm central unit wired detector sabotage"**	1)		3)	
The sabotage contact of the alarm central unit has been opened.	**"Alarm central unit enclosure sabotage"**	1)		3)	
Defective or weak storage battery (battery voltage < 11.0 V).	**"Battery fault"**		2)	3)	
Overload detection; e. g. short-circuit in a connected siren.	**"Alarm indicator overcurrent"**			3)	
Mains failure > 30 seconds and < 60 minutes.	**"Mains failure < 60 minutes"**		2)	3)	
Mains failure > 60 minutes.	**"Mains failure < 60 minutes"**			3)	
Alarm transmission device fault signal.	**"ATD failed"**		2)	3)	
Abortive heartbeat check between two alarm central units.	**"Subordinate alarm centr. unit missing"**	1)*		3)	
One or several fire detectors have signalled a fault.	**"Fault in the "fire detector" area"**				4)

1) Tripped sabotage detectors will lead to sabotage alarm in armed areas.
*: An abortive heartbeat check can raise sabotage alarm (parameterizable).

2) You will not have to immediately eliminate such causes of faults to keep the alarm central unit running without any interruptions. In such cases, acknowledging in the display units and resetting (disarming/alarm resetting) will be sufficient.

Only upon the next disarming of any area armed before, the alarm central unit will again signal an alarm central unit fault together with the cause of the fault in this area (in the event of a mains voltage fault in all areas). Resetting this message again (disarming/alarm resetting) will be required to enable you to continue working without any interruptions. In this case, you need not acknowledge or call such fault messages again into the display units.

The faults marked "2)" will remain in the display units until their causes have been eliminated.

In armed areas, such fault messages will not raise any alarm.
Exception: "ATD checkback input fault: You can parameterize the response to an alarm when there is a fault in the alarm transmission device (refer to "7. System Monitoring", page 53).
Any other causes of faults (not marked "2)") must be eliminated until the faults signals can be reset.

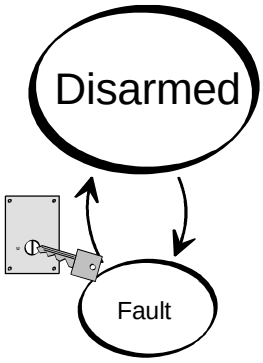
If a battery fault occurs you should replace the battery as soon as possible (refer to "12.2 Battery replacement", page 60). A battery fault message will remain active until you have replaced the storage battery.

3) Such causes of faults will lead to 'global' fault messages in all arming areas. You must separately acknowledge such messages in each arming area.
In the "fire" and "attack" areas, such fault messages will show no response.

Special case for configuration 1:
Global fault signals will cause alarm central unit faults in this configuration. Such events will only be indicated by the display units until they have been eliminated. Therefore, they need not be acknowledged. In such case, no active alarm central unit fault signal will be transmitted through the EIB object or the alarm transmission device. Global fault signals will not be recorded into in the event log for the "fire detector" and "attack detector" areas.

4) A fire detector fault will exclusively act on the "fire detector" safeguarding area. For a fire fault, the individual arming areas may be ready for arming.
A fire fault must be acknowledged on one of the display units, and its cause (open fault detectors) must have been eliminated until the signal can be reset on any arming device or by the alarm reset option. In the event of a fire fault, the "fire fault" and "alarm central unit fault" EIB objects will be triggered.

You must always acknowledge, i. e. call, each fault message on any display unit. Only after having done so, you can reset a fault message, if necessary, after eliminating the cause of the fault by disarming through an arming device of the arming areas concerned or by an alarm reset. After this, the system will change into the "disarmed" state.



e. g. key-operated switch

In the event of faults, the "alarm central unit fault" EIB object will be triggered (fault = "1") until the faults have, if necessary, been eliminated as well as acknowledged and reset in all arming areas concerned.

Important:

Any causes of faults (e. g. mains voltage failure, open sabotage detectors, fire fault, etc.) which have led to a fault signal but do no longer exist in the display units before their acknowledgement (e. g. the mains voltage has recovered, sabotage detectors or fire fault detectors have been closed) will still be read in the displays for a maximum period of 8 seconds by one of the display units after acknowledgement until they will be automatically deleted.
If sabotage detectors of safeguarding areas or fire fault detectors have been the causes of faults line 3 of the displays will, in such case, issue the "disarm" text message instead of reading the detector state.

6. Alarming

6.1 Types of alarming:

In the event of an alarm, alarming (for delayed detectors, after the delay time per arming area has elapsed) will be effected by so-called "alarm indicators".

An alarm will be raised if
- a detector within an armed area responds (intruder alarm),
- a sabotage signal is issued while an area is in the armed state (sabotage alarm),
- a detector in the "fire" safeguarding area responds (fire alarm),
- an attack detector is actuated or tampered with (attack alarm).

The following types of alarming are possible:

Local alarm:
The "local" alarm indicators such as indoor or outdoor sirens or the flashlight will be actuated. Such alarm indicators can be triggered directly, i. e. through the wired connecting terminals, or though the available EIB objects. In the latter case, you can connect the alarm indicators through suitable switching actuators. The sabotage contacts can be connected through suitable binary inputs as sabotage detectors of a safeguarding area or through the wired sabotage terminal.
The triggering period of the local alarm indicators is parameterizable.

Remote alarm:
In addition or as an alternative to the activation of the local alarm indicators (silent alarm), alarming by means of an alarm transmission device (telephone dialling device), for example, to a mobile telephone or a property security company is possible. EIB objects are available for triggering an EIB alarm transmission device. In addition, you can connect a wired alarm transmission device directly to the terminals of the alarm central unit ("ÜG" terminal).

6.1.1 Alarm indicators for local alarming:

In the event of an alarm, the following alarm indicators can be triggered (depending on the parameterization):

- Indoor siren
  Activation: - always, i. e. until the audible alarm indicators are reset.
  - time-limited (typically 3 minutes).

- Outdoor siren
  Activation: - always, i. e. until the audible alarm indicators are reset.
  - time-limited (typically 3 minutes).

- Flashlight
  Activation: - always, i. e. until acknowledgement ("disarmed after alarm" → "disarmed" state change).
  - time-limited.

- Additional alarm (relay)
  Activation: - always, i. e. until the audible alarm indicators are reset.
  - time-limited.

Important:

The EIB objects for triggering the "flashlight", "indoor siren" and "outdoor siren" alarm indicators are bi-directional. In this way, the alarm central unit can, in the event of an alarm (alarm indicator active), recognize whether the above alarm indicators have been deactivated by external manipulation via the bus ("0" telegram) in case of alarm. If so, the alarm central unit will immediately send back a "1" telegram as long as the alarm is still active, thus switching back on the alarm indicators concerned. A subsequent alarm can be raised. If such external manipulation is detected sabotage alarm will be raised in armed areas. In the "disarmed after alarm" state, the display units will issue a "programming attempt" message in such cases.

6.1.2 Alarm indicators for remote alarming:

In the event of an alarm, it is possible to trigger alarm transmission devices (depending on the parameterization). For this purpose, the following interfaces are available:

- Contacts (terminals: "ÜG") in the alarm central unit:

ÜG-E activation: Statically optional by the up to four arming areas (parameterizable) in case of an intruder alarm.

ÜG-F activation: Static, always in case of a fire alarm.

ÜG-Ü activation: Static, always in case of an attack alarm.

In addition and independent of alarming, the following signals can be generated or evaluated:

ÜG-S activation: Static, in case of a mains voltage failure of > 60 minutes, a bus voltage failure, a fault in the alarm transmission device, and in the event of an abortive heartbeat check among the alarm central units (in dependence of the parameterization), and when some overloading on the wired alarm indicator outputs is detected (the latter only being possible in the "armed" state).

ÜG-S/U activation: Static, when any arming area is being armed and disarmed; armed = activated (LED is lit)/disarmed = deactivated (LED is not lit).

ÜG-R evaluation: This terminal input will be evaluated by the alarm central unit. An alarm transmission device will signal a device or transmission fault through this input. In this case, the alarm central unit will issue an "ATD failure" 'global' fault message.

- Alarm transmission device EIB objects:

"Intruder signal to the ATD" activation:
Static, optional by the up to four arming areas (parameterizable) in case of an intruder alarm (intruder alarm = "1").

"Fire alarm" activation:
Static, always in case of a fire alarm.

"Attack alarm" activation:
Static, always in case of an attack alarm.

In addition and independent of alarming, the following EIB signals can be generated or evaluated:

"Fault signal to the ATD" activation:
Static, in case of a mains voltage failure of > 60 minutes, a fault in the alarm transmission device, and in the event of an abortive heartbeat check among the alarm central units (in dependence of the parameterization, and when some overloading on the wired alarm indicator outputs is detected (the latter only being possible in the "armed" state).

"Armed/disarmed state signal to the ATD" activation:
Static, when any arming area is being armed and disarmed; armed = activated (LED is lit)/disarmed = deactivated (LED is not lit).

"ATD checkback input fault" activation (in the "system monitoring" parameter branch):
Through this object, the alarm central unit can receive a fault signal from an EIB alarm transmission device (fault = "1"). In this case, the alarm central unit will issue an "ATD failure" 'global' fault message.

6.2 Different types of alarms

6.2.1 Fire alarm

In the event of a fire alarm, the "fire alarm" EIB object (fire alarm = "1") and the wired "ÜG-F" (fire alarm signal to the ATD) output of the alarm central unit will always be triggered. You can also link the fire alarm input of an EIB alarm transmission device to the "fire alarm" EIB object.
In addition, alarming through the local "flashlight", "indoor siren" and "outdoor siren" alarm indicators is possible. In this connection, the "flashlight", "indoor siren" and "outdoor siren" as well as the "Blitz" (flashlight), "Isir" (indoor siren) and "Asir" (outdoor siren) wired contacts will be activated. You can also trigger the potential-free relay contacts (terminal contacts in the alarm central unit). In the "alarming/fire" parameter branch, you can set the assignment to these alarm indicators. The triggering period for these alarm indicators can, in general, be specified for all areas in the "alarming/alarm indicators alarm period" parameter branch.

The "fire fault" EIB object will be triggered by the alarm central unit (fault = "1") if any detectors in the "fire detector" safeguarding area have tripped. In addition, the "alarm central unit fault" EIB object will be triggered in this case. Please note that a fire fault signal is no 'global' fault and will only act on the "fire detector" safeguarding area.

6.2.2 Attack alarm

In the event of an attack alarm, the "attack alarm" EIB object (attack alarm = "1") and the wired "ÜG-Ü" (attack alarm signal to the ATD) output of the alarm central unit will always be triggered. You can also link the attack alarm input of an EIB alarm transmission device to the "attack alarm" EIB object.
In addition, alarming through the local "flashlight", "indoor siren" and "outdoor siren" alarm indicators is possible. In this connection, the "flashlight", "indoor siren" and "outdoor siren" as well as the "Blitz" (flashlight), "Isir" (indoor siren) and "Asir" (outdoor siren) wired contacts will be activated. You can also trigger the potential-free relay contacts (terminal contacts in the alarm central unit). In the "alarming/attack" parameter branch, you can set the assignment to these alarm indicators. The triggering period for these alarm indicators can, in general, be specified for all areas in the "alarming/alarm indicators alarm period" parameter branch.

If alarming takes place exclusively (silent alarm; all visual and audible alarm indicators are not assigned by default) or additionally through an alarm transmission device a local alarm can be subsequently or again triggered for the preset alarm period if the alarm signal was unsuccessful (defect in the alarm transmission device or telephone line busy/ATD checkback input (ÜG-R) has been set). In this connection, you can parameterize (in the "ATD checkback input response to attack signal to the ATD" parameter branch) through which alarm indicators you want to raise alarms.

6.2.3 Intruder alarm/sabotage alarm

In the event of an intruder or sabotage alarm, the "safeguarding area X alarm" EIB object (alarm = "1") of the area concerned will always be triggered. In addition, you can parameterize whether the "intruder signal to the ATD" EIB object (alarm = "1") and the "ÜG-E" wired output of the alarm central units are also to be triggered. In the ETS plug-in, you can view which of the up to four arming areas act on the "intruder signal to the ATD" state.
In addition, alarming through the local "flashlight", "indoor siren" and "outdoor siren" alarm indicators is possible. In this connection, the "flashlight", "indoor siren" and "outdoor siren" as well as the "Blitz" (flashlight), "Isir" (indoor siren) and "Asir" (outdoor siren) wired contacts will be activated. You can also trigger the potential-free relay contacts (terminal contacts in the alarm central unit). In the "alarming/AA X" parameter branch, you can set the assignment to these alarm indicators per arming area. The triggering period for these alarm indicators can, in general, be specified for all areas in the "alarming/alarm indicators alarm period" parameter branch.

If alarming takes place exclusively (silent alarm) or additionally through an alarm transmission device a local alarm can be subsequently or again triggered for the preset alarm period if the alarm signal was unsuccessful (defect in the alarm transmission device or telephone line busy/ATD checkback input (ÜG-R) has been set). In this connection, you can parameterize (in the "ATD checkback input fault" parameter branch) through which alarm indicators you want to raise alarms.

7. System Monitoring

7.1 Detector monitoring

Within a parameterizable monitoring period, the alarm central unit will check the detectors created in the safeguarding areas whether they are still connected to the EIB, thus still being present. In this connection, the alarm central unit will send a value-reading telegram to the bus device to be checked, e. g. to a binary input, through the group address linked to the detector input. Such bus device must then immediately send back to the alarm central unit a value-answer telegram after receiving the reading telegram (after 1.3 seconds at the latest). This will be done automatically, once the „R“ flag (reading) has been set at the corresponding object of the addressed detector device (binary input). To facilitate the monitoring of each detector it is important that the transmitting group addresses of the detectors are unambiguous, i. e. not connected to any other transmitting bus device. Each detector should be independently connected to a detector input of its own in the alarm central unit. This is the only way to ensure that solely the addressed detector will respond.

Each detector created in the ETS plug-in will be monitored. For this purpose, you can parameterize the "detector sampling interval" (2 s to 255 s) (default: 10 s), whereby all detectors will be sampled one by one (by the object numbers).

Example:

Sampling interval: 10 s

50 detectors have been created. One detector is sampled about every 10 s. After approx. 500 s, all detectors will have been checked. After this, the cycle will proceed with the first detector.

If an addressed detector does not respond a fault signal (in the "disarmed" state) or a sabotage alarm (in the "armed" state) will be raised, depending on the state of the system. Any missing sabotage detectors will also lead to a sabotage signal or to an alarm in armed areas. If a missing detector raises an alarm other missing detectors may raise subsequent alarms.

In the event of a sabotage alarm, you must first reset the latter (deactivate the alarm indicator by disarming or by an alarm reset → "disarmed after alarm" state) before you can recognize the cause of the alarm in the display units. If you have acknowledged all messages (e. g. missing detectors) in the display units you can use one of the arming devices of the arming area concerned for disarming or reset the alarm to change into the "disarmed" state. If you use the alarm reset option you can change back to the "disarmed" state without having called the messages into the display units. Subsequently, the system may change into the "fault" state if any detectors are still missing.

In the event of a fault signal, the "alarm central unit fault" EIB object will be triggered (fault = "1") until the fault has been eliminated (missing detectors re-connected) as well as acknowledged and reset in the arming areas concerned.
You can use the arming devices of the arming area (disarming) or the alarm reset option to reset a fault signal. After this, the system will change into the "disarmed" state.

The alarm central unit will cyclically check at a shorter interval any detectors found missing to be able to quickly recognize whether such detectors have already been re-connected.
After bus voltage recovery or after programming by the ETS, the alarm central unit will check all installed detectors one by one at a short time interval.

Important:

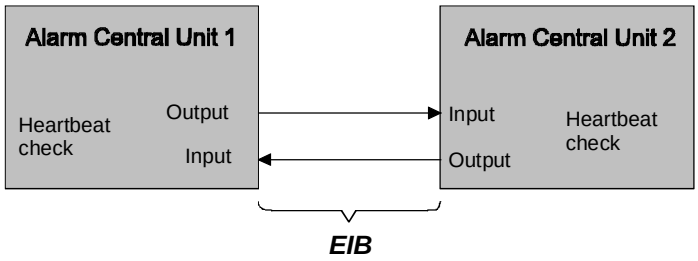
- Any detectors not linked to a group address although having been created in the ETS plug-in will not be included into detector monitoring.

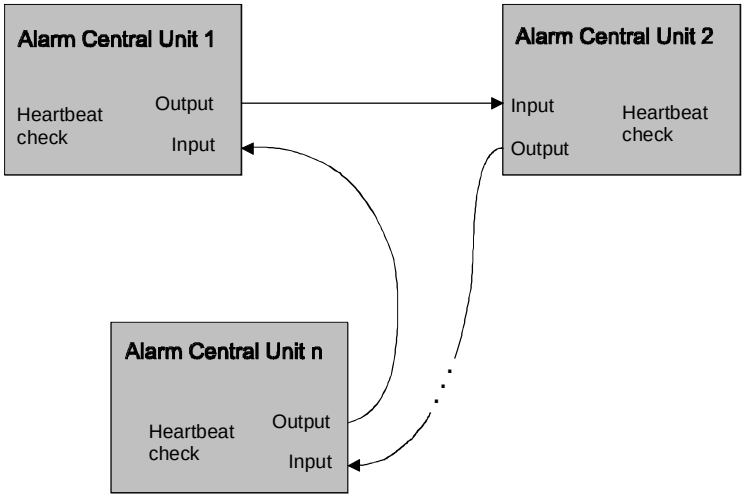
- Any missing attack detectors will always lead to an attack alarm. You can only completely reset such sabotage alarm as soon as all attack detectors are present again.

- Any missing detectors in the "fire detector" safeguarding area will only lead to a fire fault signal, thus raising no alarm.

7.2 Heartbeat check

Particularly large objects (arcades, extensive factory units) can possibly not be safeguarded by one alarm central unit alone but require several alarm central units, each of them monitoring partial complexes.
Such alarm central units can communicate with one another by sending and receiving telegrams for mutual monitoring. In this connection, you can interconnect even more than two systems.





You can enable heartbeat checking from the ETS plug-in in the "system monitoring/EIB alarm system, security" parameter branch. If you have set the "heartbeat check" parameter to "yes" you must parameterize an interval time (heartbeat check interval" 2 s to 255 s). After this time has elapsed, the alarm central unit will cyclically send the heartbeat check telegram to the bus through the "heartbeat check output" EIB object, regardless of what the state of the system is.

Within one monitoring period (fixed to three times the parameterized heartbeat check interval time), the alarm central unit is awaiting the heartbeat check telegram from the other alarm central unit through the "heartbeat check input" EIB object. If no telegram is received within the monitoring period (thus coming up to three missing telegrams) the response of the alarm central unit can be defined by the "missing heartbeat check" parameter. Thus, a sabotage signal may be caused in the event of an abortive heartbeat check ("as sabotage" setting), or the "fault signal to the ATD" and "alarm central unit fault" inputs may only be triggered (set to "fault signal to the ATD").
If you want to raise a sabotage signal a fault signal will be issued in the "disarmed" system state ("alarm central unit fault") and a sabotage alarm (for configuration 1: "attack alarm") raised in the "armed" system state.
The polarity of the heartbeat check telegrams will be toggled for each telegram transmission. The alarm central units will only check the "heartbeat check input" object for an update (regardless of what its polarity is).

If more than two alarm central units monitor one another not all systems will recognize the function failure of an alarm central unit in the event of a fault. Solely the alarm central unit connected behind the system which has failed will detect the abortive heartbeat check and will raise a fault or sabotage signal.
You should parameterize an identical heartbeat check interval for all alarm central units which communicate with one another.

7.3 ATD checkback input fault:

For remote alarming, alarming by means of an alarm transmission device (telephone dialling device), for example, to a mobile telephone or to a property security company can be raised additionally or as an alternative (for example, for a silent alarm) to activate the local alarm indicators an (refer to "6. Alarming", page 50).
However, it may happen that there is a fault or defect in the alarm transmission device, or that the telephone line is busy. In such case, the alarm transmission device cannot transmit the remote alarm. The alarm transmission device can inform the alarm central unit of such unsuccessful alarming. For this purpose, the "ÜG-R" wired (checkback) input in the alarm central unit and/or the "ATD checkback input fault" EIB object is available.

If the alarm central unit detects a signalled fault at one of these inputs it will generate a 'global' fault signal.
In the event of an intruder alarm within an area or of an attack alarm, such fault signal can be interpreted as unsuccessful alarming. In this connection, an alarm can be raised subsequently or again for the preset alarm period by the local alarm indicators (flashlight, indoor or outdoor siren). You can separately parameterize for both types of alarming (in the "ATD checkback input response to intruder signal to the ATD" or "ATD checkback input response to attack signal to the ATD" parameter branch) through which local alarm indicators you want to raise alarms.
A fault in the alarm transmission device in the event of an intruder alarm will only be evaluated if alarming through the alarm transmission device has, in principle, been enabled in the area concerned (refer to "6. Alarming", page 50).

8. Detector Test

To test the functioning of all detectors installed in the various safeguarding areas the detector test mode is available.
By activating the detector test mode ("detector test = "1"/messages in the display units: "detector test"), you can activate or deactivate the following properties of the alarm central unit for the period of the test:

- The system is passive, i. e. no alarms or faults signals can be raised.
- Arming will not be possible.
- No response to 'global' fault signals (mains failure, battery fault, "alarm central unit wired detector sabotage", "alarm central unit enclosure sabotage", "ATD checkback contact fault", abortive heartbeat check or current limitation).
- You should not programme the alarm central unit in this state, nor can you read out the event log.

In the detector test mode, you can view in the display units any tripped or missing detectors (intruder, sabotage, fire or attack detectors, wired detector input). In this connection, the detectors are sorted by the safeguarding areas (AA 1 to AA 4, fire detector, attack detector) and are only visible in the displayed areas.
Any detectors once tripped in the detector test mode will remain visible in the display units until you exit the test mode and need not be acknowledged. The detectors which have tripped in this state and the detector test itself will not be saved in the event log.

'Global' faults will not lead to system faults during the test. However, such faults will be saved in the event log and will lead to an alarm central unit fault after you have deactivated the detector test if the reason of the fault still exists when the detector test is being quitted.

In the detector test mode, you cannot check any arming devices (arming input). Using the alarm reset option will lead to the deactivation of the detector test.

You can only activate the detector test mode from the "disarmed" state. If the system is in a different state the request for changeover to the test mode will be ignored and not saved.
If the alarm central unit is in the detector test mode while a bus voltage failure occurs the system will always change into the "disarmed" state after bus voltage recovery.

After the deactivation of the detector test mode ("detector test = "0" EIB object or using the alarm reset option) all areas will be in the "disarmed" state. If any fire or attack detectors are active in this state a fire or an attack alarm will be raised immediately after you have deactivated the detector test. The alarm central unit may also change into the "fault" state.

9. Event Log

The alarm central unit has an event log memory which is non-volatile in the case of mains or bus voltage failure, and in which certain fault messages, events in the "fire detector" and "attack detector" safeguarding areas as well as all events in armed areas will be saved.

The event log can take up a total of 400 entries. Each event represents an entry and will be logged in the areas concerned. A fixed number of 40 entries each is always assigned to the "fire detector" and "attack detector" safeguarding areas. The remaining 320 entries will be dynamically distributed in dependence of the configurations of the safeguarding areas. Therefore, each area will be entitled to 80 entries if all four safeguarding areas have been enabled. If there are only two safeguarding areas each area will have a capacity of 160 entries. One area can take up a maximum of 255 entries (if only one area has been configured).
The memory has been designed as a "shift register". After the memory limit of an area has been reached the earliest entries will be overwritten by new events.

The following events will always be saved in the event log in dependence of the areas concerned:

- "Disarmed" → "armed"/"armed" → "disarmed" state change.
- Missing detectors in the safeguarding areas.
- Alarm central unit sabotage contact open ("internal sabotage").
- Tampering with the wired sabotage input ("external sabotage").
- Mains failure (will be logged immediately after the failure).
- Overloading of external alarm indicators.
- Alarm transmission device fault (ATD checkback input)
- Aborting heartbeat checking among alarm central units ("missing heartbeat check").
- Battery fault.
- Bus voltage recovery.

In addition, the following events will be logged for each armed area:

- Alarms, i. e. all open detectors (immediate, delayed (not in the "pre-alarm" state), sabotage, wired) and programming attempts.

Events in the "fire detector" and attack detector" areas will always be saved in the event log, regardless of what the state is (with the exception of the detector test mode). Fault signals will not be logged for such areas.

From the ETS plug-in, you can read out and then print the event log under "configuration/read out event log…".
Each event will be identified by the exact time and date. In addition, the detector or the arming device which has caused the event will be indicated.
In this connection, all entries will be output, sorted by the area, the date and the time.

Important:

- You can only read out the event log in the "disarmed" and "fault" system states.
- Detectors which have tripped in the detector test mode will not be saved in the event log.
- Although 'global' faults will not result in any fault signals in the detector test mode, they will be saved in the event log.
- After the complete programming (application download) of the alarm central unit, the event log will be deleted.

10. Date/Time

The alarm central unit needs the current time and the current date to mark all events with a "time stamp" and to save them in the event log.

It has two EIB objects, "time" and "date", through which, for example, an EIB-DCF77 receiver can transfer time signals (EIS 3) and date signals (EIS 4), thus setting the internal clock of the alarm central unit.
As an alternative to the use of an external time transmitter, you can download the current PC time and the current PC date into the internal clock of the alarm central unit from the ETS plug-in under "configuration/PC date and time".

The internal clock of the alarm central unit runs independently with a time error of better than 2 minutes per month and a power reserve of at least 12 hours should the bus voltage fail. The internal clock is not powered by the storage battery. Changing from summer to winter time and vice versa will be done automatically.

11. Bus Voltage Failure/Bus Voltage Recovery

11.1 Bus voltage failure

You can parameterize the response of the alarm central unit to bus voltage failure. If a bus voltage failure occurs or while the device is being programmed, the green "Betrieb" (device ON) LED will be blinking.

You can use jumper J1 to set the response to bus voltage failure while the system is in its armed state.

Position 1	The "flashlight" (Blitz), "outdoor siren" (180 s), "fault signal to the ATD and "intruder signal to the ATD" wired outputs will be triggered immediately.
Position 2	Only the "fault signal to the ATD" wired output will be triggered immediately.

It is possible that an alarm in one of the arming areas has been raised in the armed state before the bus voltage failure occurred, and that the alarm central unit has activated some wired alarm indicators. In such case, the "outdoor siren", "indoor siren" alarm indicators and the "relay contact" will, in the event of a bus voltage failure, be automatically deactivated 180 s after the occurrence of the bus voltage failure.

The wired detector input and the wired resistor sabotage loop will also be evaluated if a bus voltage failure occurs and if only one arming area was in the armed state before such failure. Thus, if a detector input is open (regardless of which area you have assigned the same to from the ETS plug-in) or in the event of sabotage, the "flashlight" alarm indicator and the "ÜG-E" terminal contact will be triggered and the "outdoor siren" switched on or re-triggered, respectively.
The wired detector input cannot be assigned to the "fire detector" or "attack detector" areas and will consequently not raise any alarm in configuration 1.

Important:

All alarms raised during a bus voltage failure will only remain active until the bus voltage has recovered (exception: alarming before a bus voltage failure).

When the system is in the disarmed state, a fault signal will be exclusively issued through the alarm transmission device ("ÜG-S" terminal) after a fixed time of 60 seconds for the period of the bus voltage failure.
Such fault will not be saved and passed forward by the alarm central unit after bus voltage recovery.

Detector states and fault signals will not be saved in the event of bus voltage failure.

11.2 Bus voltage recovery

The alarm central unit will initialize itself after bus voltage recovery. In this connection, the alarm central unit will create a defined object state by setting all EIB output objects (alarm indicators, alarm outputs, objects for triggering the alarm transmission device, etc.) to values which correspond to the system state as set after a bus voltage failure. The "bus voltage recovery" event will be entered into the event log.
What system state will be set depends on the "bus voltage recovery" parameter in the "alarm central unit" parameter branch.

- The "all AAs disarmed" setting will disarm all arming areas after initialization. In this connection, it may be possible that the system will change into the "fault" state after bus voltage recovery if, for example, sabotage contacts are open, detectors are missing or 'global' faults are signalled in individual safeguarding areas (refer to "5.3 Fault acknowledgement operations", page 48).

- After initialization, the "last state" setting will bring the system into the state which was active before the bus voltage failure or will activate the subsequent state logically following the state before the bus voltage failure. The following states can be set:

State before bus voltage failure	becoming	State after bus voltage recovery
"disarmed"	→	"disarmed" *, **
"armed"	→	"armed" ****
"pre-alarm"	→	"armed" ***, ***
"alarm"	→	"alarm" ***
"disarmed after alarm"	→	"disarmed" *, **
"fault"	→	"disarmed" *, **
"detector test"	→	"disarmed" *, **

*: The system will change into the "fault" state, if necessary, if 'global' faults (e. g. opened sabotage contact, mains failure > 30 seconds, etc.) or area-referred faults (e. g. open sabotage detector) have occurred after bus voltage recovery. Thus, a battery fault which had occurred before bus voltage failure will reappear after bus voltage recovery, unless such battery fault has not been reset yet (no battery change made).

**: Blocking elements triggered by the pulse signals of the alarm central unit will not go open automatically after bus voltage recovery as no pulse disarming signals will be produced in such case.

***: If detectors have raised an alarm prior to bus voltage failure such detectors can again raise subsequent alarm after initialization. Even detectors which are open during the initialization phase will raise alarm.

****: The system will not immediately change into the "disarmed" state after disarming. The display units of the areas concerned will read the "alarm" message which points out that there was a bus voltage failure in the "armed" state (the "disarmed after alarm" object and the alarm indicators will not be triggered in this connection). You can actuate the "more…" key to call these messages into the display units and acknowledge them. In this connection, the "bus voltage recovery" event will be displayed. Then you can only go to the "disarmed" state if you actuate an arming device of the area concerned. As an alternative, you can use the alarm reset option to go to the "disarmed" state without acknowledging the message in the display units.
The area will then be ready for arming.
Detectors which are open or active during the initialization phase (depending on their parameterization) will raise an alarm in the "armed" state after bus voltage recovery.

Important:

The system will always be in the "disarmed" state after having been programmed from the ETS.

During the initialization phase, you can read the version number of the system software in line 1 of the display units, while the text message "initializing" will be displayed in line 2. In addition, the green "Betrieb" (device ON) LED will be blinking for the length of the initialization.
Within this time, the alarm central unit will send defined telegrams to the bus to store in the EIB objects of all outputs values which correspond to the system state. In this connection, the alarm central unit will proceed by the following rhythm:

1. All parameterized display units will be triggered: line 1 indicating the version number, line 2 reading "initializing".
2. All dynamic signals of the arming areas will be reset ("0").
3. The static armed/disarmed state signals will be set in accordance with the system state.
4. Pre-alarms and fire faults signals will be reset ("0").
5. All detectors of the individual safeguarding areas created in the ETS plug-in will be checked for their presence and states one after the other by the EIB object numbers. In this connection, missing or open detectors in armed areas will raise alarm. Missing detectors will raise a fault in disarmed areas (refer to "7.1 Detector monitoring", page 53).
6. The "detector" and "sabotage" wired contacts will be evaluated and telegrams issued according to the states.
7. Subsequently, the "alarm", "ready for arming", "flashlight", "outdoor siren", "indoor siren", "fault" outputs and the outputs of the alarm transmission device will be set in accordance with the system state.
8. This will complete the initialization. The green "Betrieb" (device ON) LED will be permanently lit.

Important:

Heartbeat check telegrams will already be transmitted during the initialization phase.

12. Storage Battery Management

An emergency battery facilitates uninterrupted operation of the load part of the alarm central unit, thus feeding the directly connected external alarm indicators, if necessary, even in the event of mains voltage failure. An intelligent electronic charging circuit ensures that emergency power supply of at least 12 hours will always be guaranteed.

Important:

The bus voltage and all detectors connected to the EIB will not be supplied by the emergency battery. Also to guarantee uninterrupted operation in that case you should use an EIB emergency power supply system.

12.1 Battery check

The storage battery (lead gel) will be permanently kept charged. In this connection, the quality or the serviceability of the battery will be checked at regular intervals by cyclic cell monitoring and end-of-life detection done by the electronic charging circuit:

Cell monitoring:
Once a day, the open-circuit voltage of the battery will be measured for a short time. If the voltage measured falls below 11 V the alarm central unit will generate a permanent battery fault signal. In this case, the battery is defective and should be replaced as soon as possible.
If an open-circuit voltage of > 11 V is found by the measurement the battery is serviceable and will be kept charging.

End-of-life detection:
In addition to cell monitoring, the battery will be put under load for some period once a month, a voltage difference being determined in this connection. If this difference is < 0.5 V the battery does not show any ageing effect yet and will be kept charging. However, if a voltage difference of > 0.5 V is found the alarm central unit will generate a permanent battery fault signal. In this case, the battery is old and does no longer have its full capacity to guarantee uninterrupted operation.

There is no difference between the two types of battery fault signals (cell monitoring/end-of-life detection). Therefore, you should replace the battery as soon as this fault message appears.

During a mains voltage failure, the battery will neither be charged nor checked.

12.2 Battery replacement

If the alarm central unit signals a battery fault it will be absolutely necessary that you replace the battery. The battery replacement should be performed in the "disarmed" system state in order to avoid an alarm being raised by the opening of the sabotage contact of the alarm central unit.
Keep the following steps when replacing the battery:

1. Switch off the mains voltage. *
2. Open the alarm central unit. **
3. Disconnect and remove the defective/old battery.
4. Insert and connect a fresh battery.
5. Close the cover of the alarm central unit.
6. Switch on the mains voltage.

*: If the mains voltage failure lasts longer than 30 seconds the alarm central unit will signal a > 30 second mains voltage failure which you must separately acknowledge in each area and then reset. Mains voltage failures of < 30 seconds will be saved in the event log.

**: An "alarm central unit enclosure sabotage" fault will be signalled which you must acknowledge separately, and which you can reset after closing the cover.

After this, the automatic charging circuit will check the battery by measuring its open-circuit voltage. If this voltage falls below 10.2 V the automatic circuit will assume that the battery is defective. The alarm central unit will issue a battery fault signal, and the battery will not be charged. In such case, you should replace the battery.
If the voltage measured is > 10.2 V the battery will be charged. One hour later, the electronic charging circuit will check the open-circuit voltage again (cell monitoring). If, in this connection, a voltage of > 11 V is found the battery is O. K. and will be kept charging. If the electronic circuit finds a voltage of < 11 V individual cells of the battery will be assumed to be defective. The alarm central unit will signal a battery fault, and you should replace the battery.

13. Notes on the Integration of Various Bus Components

- komfort detectors/komfort presence detectors

  Such detectors can be integrated into the alarm central unit. For the "komfort detector" and the "komfort presence detector", you can change the mode through an EIB object while the alarm central unit is in operation. Thus, you can change the above-mentioned detectors into the alarm mode when arming individual areas so that you can made a more insensitive and adjustable motion evaluation, independent of any light control. You should link the changeover objects of the detectors (komfort detector: "mode"/komfort presence detector: "mode change") to the "armed/disarmed state signal" of the arming area of the alarm central unit.

  If you use the 'komfort detector' or the 'komfort presence detector' in configurations 2.X/3.X (nested) in the outer shell you should note the following (configuration 2.1 example):

  The mode changing EIB object must be linked to the group addresses of the "armed/disarmed state signal" EIB objects of AA 1 and AA 2 of the alarm central unit.

  This is necessary to change the detector/presence detector installed in the outer shell to the alarm mode when arming area 2 ("externally armed") is being armed as, in this case, no arming/disarming signal will be generated in arming area 1.

- Additional info display parameterization

  In addition to the display of the "standard information" of the alarm central unit in the info display units (page function: "alarm central unit display"), you can create additional pages in the display (page function: "display"). This will enable you to visualize information such as "armed/disarmed", "fault/no fault", "alarm/no alarm", etc., on such additional pages. For this purpose, you must additionally link the corresponding EIB objects of the alarm central unit to the objects of the info display unit through the group addresses created.
  You can also use the alarm function of the display units, for example, by linking to the alarm page the groups additionally created in the displays. In this case, the buzzer and/or the display background lighting will be activated when an alarm value parameterizable in the ETS plug-in of the display units is being received. So, for example, additional alarming can be effected by the info display units in the event of an alarm in the "disarmed after alarm" state (refer to the documentation of the info display units).

Parameters		
Description:	**Values:**	**Comment:**
Alarm central unit		
Configurations of the safeguarding areas		Defines the configuration of the arming areas.
	Configuration 1	Exclusively 1 x fire, 1 x attack. (The "fire detector" and "attack detector" areas always exist in parallel with another possibly enabled configuration.)
	Configuration 2.1	1 x outer shell (SA 1), 1 x interior room (SA 2), nested.
	Configuration 2.2	1 x outer shell (SA 1), 1 x interior room (SA 2), nested; 1 x outer shell (SA 3), 1 x interior room (SA 4), nested.
	Configuration 3.1	1 x separate safeguarding area (SA 1); 1 x outer shell (SA 3), 1 x interior room (SA 4), nested.
	Configuration 3.2	2 x separate safeguarding areas (SA 1 and SA 2); 1 x outer shell (SA 3), 1 x interior room (SA 4), nested.
	Configuration 4.1	1 x separate safeguarding area (SA 1).
	Configuration 4.2	2 x separate safeguarding areas (SA 1 and SA 2).
	Configuration 4.3	3 x separate safeguarding areas (SA 1, SA 2 and SA 3).
	Configuration 4.4	4 x separate safeguarding areas (SA 1, SA 2, SA 3 and SA 4).
	Configuration 5.1	1 x safeguarding area (SA 1), separate; 1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one.
	Configuration 5.2	2 x safeguarding area (SA 1 and SA 2), separate; 1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one,
	Configuration 5.3	3 x safeguarding area (SA 1, SA 2 and SA 3), separate; 1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one,
	Configuration 6	2 x safeguarding area (SA 1 and SA 2), separate; 1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one; 1 x safeguarding area (SA 3), separate and not integrated into the cascading.

Configurations of the safeguarding areas (continued)	Configuration 7.1	1 x safeguarding area (SA 1), separate; 1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one; 1 x safeguarding area (SA 3), separate and not integrated into the cascading.
	Configuration 7.2	1 x safeguarding area (SA 1), separate; 1 x safeguarding area (SA 4), cascaded, i. e. the arming areas must be armed one by one; 2 x safeguarding area (SA 2 and SA 3), separate and not integrated into the cascading.
Armed/disarmed state signal pulse	2 to 255 s, **5 s**	For arming or disarming, you can issue a time limited "1" signal through the "armed state signal pulse" and "disarmed state signal pulse" objects which are available per arming area. This parameter will define the ON period for all pulse signals.
Armed state acknowledging time	2 to 255 s, **5 s**	Specifies, in general, the ON period of the acknowledging signal for all arming areas after successful and completed arming. All alarm indicators assigned to the acknowledgement will be triggered for the period parameterized in this connection.
Disarmed state acknowledging time	2 to 255 s, **10 s**	Specifies, in general, the ON period of the acknowledging signal for all arming areas after successful and completed disarming. All alarm indicators assigned to the acknowledgement will be triggered for the period parameterized in this connection.
Bus voltage recovery		Defines the response of the alarm central unit to bus voltage recovery.
	Last state	After initialization, the system state will be set which was active before the bus voltage failure, or the subsequent state logically following the state before the bus voltage failure will be set (refer to "11.2 Bus voltage recovery", page 58).
	All AAs disarmed	All arming areas will be disarmed after initialization.

Detector/sabotage		
Fire detector safeguarding area		
[Detector text] – [fire detector safeguarding area input X], X depends on the number of all detector inputs used (will be automatically created by the ETS plug-in).		
Input type		Defines the type of the selected fire detector input.
	Immediate detector	An 'active' fire detector will be evaluated immediately and will lead to a fire alarm.
	Fault	The detector is a fault signal input of the fire detector area. An 'active' detector will raise a fire fault signal (e. g. group fault signal of various fire detectors). Important: The "input active at" parameter in this parameter branch will define when a detector input is active.
Detector text	14-character text	Defines the identification text of the selected fire detector. This text will be issued in the display units for better identification of the detectors, for example in the active state or in the event of detector sabotage (missing detector).
Input active at		Defines the polarity of the selected detector input.
	0	The detector is active at an object value of "0".
	1	The detector is active at an object value of "1".
[Detector text] – [fire detector safeguarding area input X], X depends on the number of all detector inputs used (will be automatically created by the ETS plug-in).		
Refer to the first fire detector input.		

Attack detector safeguarding area		
[Detector text] – [attack detector safeguarding area input X], X depends on the number of all detector inputs used (will be automatically created by the ETS plug-in).		
Input type		Defines the type of the selected attack detector input.
	Immediate detector	An 'active' attack detector will be evaluated immediately and will lead to a fire alarm.
	Sabotage	The detector is a sabotage signal input of the attack detector area. An 'active' detector will raise an attack sabotage signal (e. g. sabotage contact of an attack detector). Important: The "input active upon" parameter in this parameter branch will define when a detector input is active.
Detector text	14-character text	Defines the identification text of the selected attack detector. This text will be issued in the display units for better identification of the detectors, for example in the active state or in the event of detector sabotage (missing detector).
Input active at		Defines the polarity of the selected detector input.
	0	The detector is active at an object value of "0".
	1	The detector is active at an object value of "1".
[Detector text] – [attack detector safeguarding area input X], X depends on the number of all detector inputs used (will be automatically created by the ETS plug-in).		
Refer to the first attack detector input.		

[Detector text] – [alarm central unit wired detector input]		
Safeguarding area	**SA 1** SA 2 * SA 3 * SA 4 * *: The possible safeguarding areas will be automatically unhidden or hidden, depending on the configuration.	Defines the safeguarding area the wired detector input is assigned to. Important: The wired detector input cannot be assigned to the "fire detector" or "attack detector" area. Therefore, the wired detector input will be deactivated in configuration 1.
Input type		Defines the type of wired detector input.
	Immediate detector	An open wired detector input will be evaluated immediately and will lead to an alarm in the armed state.
	Delayed detector	An open wired detector input will be evaluated at some delay, taking into consideration the parameterized alarm delay time of the assigned arming area. In the armed state, an open detector will only raise an alarm after the delay time has elapsed. In the event of a bus voltage failure, the wired detector parameterized as a delayed detector will also immediately raise an alarm as soon as only one (any) arming area is in the armed state. Important: The polarity of the wired detector input is fixed (NO contact: contact closed: "0", contact open: "1").
Detector text	14-character text	Defines the identification text of the wired detector. This text will be issued in the display units for better identification of the detector, for example in the active state.
[Detector text] – [alarm central unit wired sabotage input]		
Sabotage terminating resistance	**0 Ohms** 12 kOhms 47 kOhms	Defines the loop resistance of the wired sabotage circuit.

[Safeguarding area 1 identification] – [SA 1] The visibility of this area depends on the configuration.		
Safeguarding area identification	Text (no limited number of characters)	Suggests an identification text of the safeguarding area. This text will only be used in the ETS plug-in for better identification and will not be downloaded into the device.
[Detector text] – [SA 1 input X] X depends on the number of all detector inputs used (will be automatically created by the ETS plug-in).		
Input type		Defines the type of selected detector input.
	Immediate detector	An 'active' detector will be evaluated immediately and will lead to an intruder alarm in the armed state.
	Delayed detector	An 'active' detector input will be evaluated at some delay, taking into consideration the parameterized alarm delay time of the assigned arming area. In the armed state, an open detector will only raise an alarm after the delay time has elapsed.
	Sabotage	The detector is a sabotage signal input of the safeguarding area. An 'active' detector will raise a sabotage fault signal (in the disarmed state) or a sabotage alarm (in the armed state).
	Arming device sabotage	The detector is a sabotage input of an arming device (e. g. key-operated switch) of the assigned arming area. An 'active' detector will raise an "arming device sabotage" fault signal (in the disarmed state) or a sabotage alarm (in the armed state).
	Locking mechanism	The detector is a locking mechanism detector of the safeguarding area (e. g. interlock switch contact). An 'active' detector will prevent the arming of the assigned arming area. Important: The "input active upon" parameter in this parameter branch will define when a detector input is active.
Detector text	14-character text	Defines the identification text of the selected detector. This text will be issued in the display units for better identification of the detectors, for example in the active state or in the event of detector sabotage (missing detector).

Detector type		Defines the type of the selected detector. Only the text message in the display units will be oriented towards this setting.
	Contact	The detector is of contact type, e. g. a window contact.
	Motion	The detector is a motion sensor.
	Glass breakage	The detector is a glass breakage sensor.
		Only active if "input type = "immediate detector" or "delayed detector" All other inputs are of contact type.
Input active at		Defines the polarity of the selected detector input.
	0	The detector is active at an object value of "0".
	1	The detector is active at an object value of "1".
[Detector text] – [SA 1 input X] X depends on the number of all detector inputs used (will be automatically created by the ETS plug-in).		
Refer to the first detector of the safeguarding area.		
[Safeguarding area 2 identification] – [SA 2] The visibility of this area depends on the configuration.		
Refer to safeguarding area 1.		
[Safeguarding area 3 identification] – [SA 3] The visibility of this area depends on the configuration.		
Refer to safeguarding area 1.		
[Safeguarding area 4 identification] – [SA 4] The visibility of this area depends on the configuration.		
Refer to safeguarding area 1.		

Arming		
[Arming area text] – [AA 1] The visibility of this area depends on the configuration.		
Arming area text	14-character text	Defines the identification text of the arming area. This text will be issued in the display units for better identification.
AA 1 arming		
AA 1 arming delay time	0 to 255 s, **0**	Defines the delay time of the selected arming area which must elapse before the area will actually be armed after an arming command (e. g. actuation of a key-operated switch). Only after arming is complete acknowledging signals will be generated, if necessary. An arming delay time will make sense if the arming device is located within a safeguarded area. Setting "0" will deactivate the arming delay.
AA 1 alarm delay time	0 to 255 s, **0**	Defines the delay time of the selected arming area which must elapse after the tripping of a delayed detector before an alarm is raised. An alarm delay time will make sense if the arming device is located within a safeguarded area. In this connection, you should select a time which will be necessary to reach and disarm the arming device (include a reserve for potential misoperation). Setting "0" will deactivate the alarm delay, detector inputs parameterized as delayed also being immediately evaluated.
Arming device 1 physical address	Physical address (The ETS plug-in will automatically provide the addresses of the bus devices linked in the ETS project with the group address of the arming input.)	You can install up to four independent arming devices (e. g. key-operated switches) per arming area. Here, you must define the physical address of the bus device to which the first arming device is connected (e. g. binary input, pushbutton interface, pushbutton sensor). To be able to define an address at this position the "arming input" object of the selected arming area must have been linked to a group address. Only telegrams from 'authorized' devices will be evaluated positively. If a telegram of a bus device not specified here is received in the armed state a sabotage alarm will be raised.

SA 1 arming device sabotage input number		If the selected arming device has a sabotage contact, and if such contact is connected to the alarm central unit through a detector input of the safeguarding area parameterized to "arming device sabotage" this arming device can be monitored for sabotage. You cannot disarm the system through arming devices having been tampered with.
	No arming device sabotage	The arming device has no sabotage contact, or no detector parameterized to "arming device sabotage" has been created.
	Detector number	Here, you must select the detector number of the detector input which the sabotage contact of the arming device has been connected to. The sabotage detector must have been created in the safeguarding area belonging to the arming area. Arming device in AA 1 – arming device sabotage in SA 1. Arming device in AA 2 – arming device sabotage in SA 2. Arming device in AA 3 – arming device sabotage in SA 3. Arming device in AA 4 – arming device sabotage in SA 4. You can assign a detector number only once. This parameter will only be visible if you have defined a physical address under "arming device 1 physical address".
Arming device 2 physical address	Refer to "Arming device 1 physical address".	
SA 1 arming device sabotage input number	Refer to "SA 1 arming device sabotage input number" of the first arming device.	
Arming device 3 physical address	Refer to "Arming device 1 physical address".	
SA 1 arming device sabotage input number	Refer to "SA 1 arming device sabotage input number" of the first arming device.	
Arming device 4 physical address	Refer to "Arming device 1 physical address".	
SA 1 arming device sabotage input number	Refer to "SA 1 arming device sabotage input number" of the first arming device.	

AA 1 armed/disarmed state acknowledgement		
Signalization through 'armed state signal' to the ATD	No **Yes**	Defines whether the "armed" state is to be forwarded to the alarm transmission device for arming area 1. Important: Please note that the "armed state signal to the ATD" output can be triggered by the up to four arming areas. If only one of the assigned areas in the armed state the output will be active. The "'armed state signal' to the ATD option used by" display parameter will indicate the areas assigned to output ÜG-S/U.
Acknowledgement by flashlight		You can signalize successful arming or disarming by the flashlight.
	No	No acknowledgement by the flashlight.
	Yes	The flashlight will be triggered upon an arming or disarming operation. The duration of triggering depends on the general "armed state acknowledging time" or "disarmed state acknowledging time" parameters in the "alarm central unit" parameter branch.
Acknowledgement by outdoor siren		You can signalize successful arming or disarming by the outdoor siren.
	No	No acknowledgement by the outdoor siren (recommended setting/noise protection).
	Yes	The outdoor siren will be triggered upon an arming or disarming operation. The duration of triggering depends on the general "armed state acknowledging time" or "disarmed state acknowledging time" parameters in the "alarm central unit" parameter branch.
Acknowledgement by indoor siren		You can signalize successful arming or disarming by the indoor siren.
	No	No acknowledgement by the indoor siren.
	Yes	The indoor siren will be triggered upon an arming or disarming operation. The duration of triggering depends on the general "armed state acknowledging time" or "disarmed state acknowledging time" parameters in the "alarm central unit" parameter branch.

Acknowledgement by relay		You can signalize successful arming or disarming by triggering the potential-free relay output.
	No	No acknowledgement by triggering the relay output.
	Yes	The relay output will be triggered upon an arming or disarming operation. The duration of triggering depends on the general "armed state acknowledging time" or "disarmed state acknowledging time" parameters in the "alarm central unit" parameter branch.
Opening blocking element in case of fire/attack		Blocking elements or pulse door openers are normally integrated into door frames and lock the door in armed areas. Thus, inadvertent opening of the door and unintentional access to safeguarded areas will be prevented. In the event of a fire or an attack alarm, locked blocking elements can be prematurely opened by the transmission of a disarming signal, for example, to open the way out.
	Yes, static disarmed state signal	In the event of a fire or an attack alarm, a static disarmed state signal will be prematurely transmitted in the selected arming area through the "static disarming signal" object. Please note that the arming area may, nevertheless, be in the armed state in such case.
	Yes, disarmed state signal pulse	In the event of a fire or an attack alarm, a disarmed state signal pulse will be prematurely transmitted in the selected arming area through the "disarming signal pulse" object. Please note that the arming area may, nevertheless, be in the armed state in such case.
	No	In the event of a fire or an attack alarm, no disarmed state signal will be transmitted. This setting will be typical if you do not use any door locking mechanisms. If you do have locking mechanisms under this option please note that they will not open earlier in the event of a fire or an attack alarm.

[Arming area text] – [AA 2] The visibility of this area depends on the configuration.		
Refer to arming area 1.		
[Arming area text] – [AA 3] The visibility of this area depends on the configuration.		
Refer to arming area 1.		
[Arming area text] – [AA 4] The visibility of this area depends on the configuration.		
Refer to arming area 1.		
Alarming		
Fire detector		
Alarming by flashlight	No **Yes**	Defines whether the flashlight will be activated in the event of a fire alarm. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
Alarming by outdoor siren	No **Yes**	Defines whether the outdoor siren will be activated in the event of a fire alarm. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
Alarming by indoor siren	No **Yes**	Defines whether the indoor siren will be activated in the event of a fire alarm. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
Alarming by relay	No **Yes**	Defines whether potential-free relay contact will be triggered in the event of a fire alarm. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
Attack detector		
Alarming by flashlight	**No** Yes	Defines whether the flashlight will be activated in the event of an attack alarm. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
Alarming by outdoor siren	**No** Yes	Defines whether the outdoor siren will be activated in the event of an attack alarm. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
Alarming by indoor siren	**No** Yes	Defines whether the indoor siren will be activated in the event of an attack alarm. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.

Alarming by relay	**No** Yes	Defines whether potential-free relay contact will be triggered in the event of an attack alarm. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
AA 1		
Alarming by sending an 'intruder' signal to the ATD	No **Yes**	Defines whether an intruder or sabotage signal in arming area 1 will be sent to the alarm transmission device. Important: Please note that the "intruder signal to the ATD" output can be triggered by the up to four arming areas. If there is an alarm in one of the assigned areas only the output will be active. The "'intruder signal' to the ATD option used by" display parameter will indicate the areas assigned to output ÜG-E.
Alarming by flashlight	No **Yes**	Defines whether the flashlight will be activated in the event of an intruder or an attack alarm in arming area 1. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
Alarming by outdoor siren	**No** Yes	Defines whether the outdoor siren will be activated in the event of an intruder or an attack alarm in arming area 1. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
Alarming by indoor siren	No **Yes**	Defines whether the indoor siren will be activated in the event of an intruder or an attack alarm in arming area 1. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
Alarming by relay	No **Yes**	Defines whether the potential-free relay contact will be triggered in the event of an intruder or an attack alarm in arming area 1. You can use the parameters in the "alarm indicators alarm period" parameter branch to define the triggering period.
AA 2		
Refer to arming area 1 alarming.		
AA 3		
Refer to arming area 1 alarming.		
AA 4		
Refer to arming area 1 alarming.		

Alarm indicators alarm period		
Flashlight ON period		Defines the ON period of the flashlight in the event of an alarm.
	Always ON	The flashlight will stay permanently activated until a change into the "disarmed" state takes place.
	Time-limited	The flashlight will stay activated for a certain period only. You can define the ON period in seconds. If there is a change into the "disarmed" state before this time has elapsed the flashlight will be prematurely deactivated.
Flashlight ON period	**2 to 254 s, 254**	Defines the ON period of the flashlight for time-limited activation. After this time has elapsed, the flashlight will be deactivated. If there is a change into the "disarmed" state before this time has elapsed the flashlight will be prematurely deactivated. Only for "flashlight ON period" = "time-limited".
Outdoor siren ON period		Defines the ON period of the outdoor siren in the event of an alarm.
	Always ON	The outdoor siren will stay permanently activated until the alarm is reset ("disarmed after alarm" state).
	Time-limited	The outdoor siren will stay activated for a certain period only. You can define the ON period in seconds. If the alarm is reset before this time has elapsed the outdoor siren will be prematurely deactivated. Important: If is recommended to parameterize the "time-limited" setting. In Germany, the maximum period for external audible alarm indicators is limited to 180 seconds. In hospital areas, for example, such period may even be shortened due to specific rules.
Outdoor siren ON period	**2 to 254 s, 180**	Defines the ON period of the outdoor siren for time-limited activation. After this time has elapsed, the outdoor siren will be deactivated. If the alarm is reset before this time has elapsed the outdoor siren will be prematurely deactivated. Only for "outdoor siren ON period" = "time-limited".

Indoor siren ON period		Defines the ON period of the indoor siren in the event of an alarm.
	Always ON	The indoor siren will stay permanently activated until the alarm is reset ("disarmed after alarm" state).
	Time-limited	The indoor siren will stay activated for a certain period only. You can define the ON period in seconds. If the alarm is reset before this time has elapsed the indoor siren will be prematurely deactivated.
Indoor siren ON period	**2 to 254 s, 180**	Defines the ON period of the indoor siren for time-limited activation. After this time has elapsed, the indoor siren will be deactivated. If the alarm is reset before this time has elapsed the indoor siren will be prematurely deactivated. Only for "indoor siren ON period" = "time-limited".
Relay ON period		Defines the ON period of the potential-free relay contact in the event of an alarm.
	Always ON	The relay contact will stay permanently activated until the alarm is reset ("disarmed after alarm" state).
	Time-limited	The relay contact will stay activated for a certain period only. You can define the ON period in seconds. If the alarm is reset before this time has elapsed the relay contact will be prematurely deactivated.
Relay ON period	**2 to 254 x 10 s, 254**	Defines the ON period of the potential-free relay contact for time-limited activation. After this time has elapsed, the relay contact will be deactivated. If the alarm is reset before this time has elapsed the relay contact will be prematurely deactivated. Only for "relay ON period" = "time-limited".

Display		
[Display unit 1 identification]		
Display unit 1 identification	Text **(number of characters unlimited)**	Suggests an identification text of display unit 1. This text will only be used in the ETS plug-in for better identification and will not be downloaded into the device.
Display unit 1 present	No **Yes**	Depending on the configuration, up to four independent display units can be triggered. This parameter defines whether display unit 1 will be used.
Displayed areas	AA 1 * AA 2 * AA 3 * AA 4 * **Fire detector** **Attack detector** ***:** The selectability of the arming areas depends on the configuration.	You can define which of the configured areas you can view in the display units. Important: As soon you have assigned only one display unit to an arming area, please note that you will first have to view or acknowledge various fault messages in the display units before you can reset them. Then you can, for example, actuate an arming device of the area concerned to reset the messages.
[Display unit 2 identification] Refer to display unit 1.		
[Display unit 3 identification] Refer to display unit 1.		
[Display unit 4 identification] Refer to display unit 1.		
System monitoring		
EIB alarm system, security		
Detector sampling interval	**2 to 255 s, 10**	Within a parameterizable monitoring period, the alarm central unit will check the detectors created in the safeguarding areas whether they are still connected to the EIB, thus still being present. In this connection, the alarm central unit will send a value-reading telegram to the bus device to be checked, e. g. to a binary input, through the group address connected to the detector input. Such bus device must then immediately send back to the alarm central unit a value-answer telegram after receiving the reading telegram (after 1.3 seconds at the latest). Setting the „R“ flag for all detectors is mandatory. The detector sampling interval defines the period between two sampling times. Example: Sampling interval: 10 s 50 detectors have been created. After approx. 500 s, all detectors will have been checked. After this, the cycle will proceed with the first detector.

Heartbeat check	**No** Yes	Several EIB alarm central units can communicate with one another by sending and receiving telegrams for mutual monitoring. In this connection, you can interconnect even more than two systems. This parameter will enable heartbeat checking.
Heartbeat check interval	**2 to 255 s, 30**	After this time has elapsed, the alarm central unit will cyclically send the heartbeat check telegram to the bus through the "heartbeat check output" EIB object, regardless of what the state of the system is. Within the monitoring period (fixed to three times the parameterized heartbeat check interval time), the alarm central unit is awaiting the heartbeat check telegram from the other alarm central unit through the "heartbeat check input" object. If no telegram is received within the monitoring period (thus coming up to three missing telegrams) the response of the alarm central unit can be defined by the "missing heartbeat check" parameter. Only for "heartbeat check" = "Yes".
Missing heartbeat check		If the heartbeat check telegram from the other alarm central unit fails you can define the response of the local alarm central unit.
	Same as sabotage	An abortive heartbeat check will raise a sabotage signal. Thus, a fault signal will be issued in the "disarmed" system state ("alarm central unit fault") and a sabotage alarm (for configuration 1: "attack alarm") raised in the "armed" system state.
	'Fault signal' to the ATD	In the event of an unsuccessful heartbeat check, only the "fault signal to the ATD" and "alarm central unit fault" outputs will be triggered. Only for "heartbeat check" = "Yes".

ATD checkback input response to attack signal to the ATD		
Flashlight	No **Yes**	If the alarm transmission device ("alarm" state) signals a fault in the event of an attack alarm ("ÜG-R" fault input active) subsequent alarming by the flashlight can be effected. Thus, local alarming will be guaranteed even in case the remote transmission is disturbed. This parameter will enable subsequent alarming by the flashlight.
Outdoor siren	No **Yes**	If the alarm transmission device ("alarm" state) signals a fault in the event of an attack alarm ("ÜG-R" fault input active) subsequent alarming by the outdoor siren can be effected. Thus, local alarming will be guaranteed even in case the remote transmission is disturbed. This parameter will enable subsequent alarming by the outdoor siren.
Indoor siren	**No** Yes	If the alarm transmission device ("alarm" state) signals a fault in the event of an attack alarm ("ÜG-R" fault input active) subsequent alarming by the indoor siren can be effected. Thus, local alarming will be guaranteed even in case the remote transmission is disturbed. This parameter will enable subsequent alarming by the indoor siren.
Relay	**No** Yes	If the alarm transmission device ("alarm" state) signals a fault in the event of an attack alarm ("ÜG-R" fault input active) subsequent alarming by the potential-free relay contact can be effected. Thus, local alarming will be guaranteed even in case the remote transmission is disturbed. This parameter will enable subsequent alarming by the relay output.

ATD checkback input response to intruder signal to the ATD		
Flashlight	No **Yes**	If the alarm transmission device ("alarm" state) signals a fault in the event of an intruder or sabotage alarm ("ÜG-R" fault input active) subsequent alarming by the flashlight can be effected. Thus, local alarming will be guaranteed even in case the remote transmission is disturbed. This parameter will enable subsequent alarming by the flashlight.
Outdoor siren	No **Yes**	If the alarm transmission device ("alarm" state) signals a fault in the event of an intruder or sabotage alarm ("ÜG-R" fault input active) subsequent alarming by the outdoor siren can be effected. Thus, local alarming will be guaranteed even in case the remote transmission is disturbed. This parameter will enable subsequent alarming by the outdoor siren.
Indoor siren	**No** Yes	If the alarm transmission device ("alarm" state) signals a fault in the event of an intruder or sabotage alarm ("ÜG-R" fault input active) subsequent alarming by the indoor siren can be effected. Thus, local alarming will be guaranteed even in case the remote transmission is disturbed. This parameter will enable subsequent alarming by the indoor siren.
Relay	**No** Yes	If the alarm transmission device ("alarm" state) signals a fault in the event of an intruder or sabotage alarm ("ÜG-R" fault input active) subsequent alarming by the potential-free relay contact can be effected. Thus, local alarming will be guaranteed even in case the remote transmission is disturbed. This parameter will enable subsequent alarming by the relay output.
Date/time		
System clock present	No **Yes**	This parameter has no function.

Remarks on the Software

- ETS plug-in system requirements:

  Operating system: Windows 9x, ME, NT 4.0, 2000, XP

  ETS: ETS 2 v 1.2 a or later

  PC: Pentium I processor (or similar), 166 MHz, 32 MB or better recommended.

- Programming

  The alarm central unit can only be addressed or programmed via the bus by the ETS or the ETS plug-in in the "disarmed" and "fault" system states. If only one area of the alarm central unit is in a different state the alarm central unit will discontinue the communication with the ETS and raise a sabotage alarm, if necessary. In such case, access via the bus will be recorded in the event log.

  The ETS will signal a fault during the programming process if the latter is interrupted by the alarm central unit:

  - *"Communication set-up error. Please make sure that a device having such physical address exists.",*

  or

  - *"Write operation error."*

  If one of these error messages is raised the alarm central unit is very likely to have interrupted the communication. In this case, the system will be in a state which does not respond to the bus. Disarm the alarm system completely (make an alarm reset, if necessary).

  In the "disarmed" and "fault" states, you can programme the physical address, the entire application, or perform a partial download of the parameters or group addresses. When choosing the suitable programming method, always consider the programming flags ("Adr", "Prg", "Par", "Grp") in the ETS of the device you want to programme. The green "Betrieb" (device ON) LED will be blinking during the programming process or also in the unprogrammed state.

  If the ETS issues the following error messages:

  - *"A telegram was corrupted when being sent or received. Repeat this function.",*

  there will be a communication problem with local bus coupling/the data interface. This error will not be caused by the alarm central unit. To solve this problem you should make an application download using the ETS 2 v 1.3.

  - *"Device comparison failed",*

  indicates an unsuccessful attempt to make a partial download into a device already programmed. In this connection, the ETS has figured out that the project data does not agree with the application data already programmed (e. g. partial download of a later application into a device which has already been programmed with an earlier application). In such case, you should start a complete application download.

- ETS functions

  The "Reading out the information into the device" or "Reading out the device memory" ETS functions are not possible for the alarm central unit.

  Neither can you trigger the "Betrieb" (device ON) LED of the alarm central unit by the "Test/physical address" ETS function. Such attempt will be aborted with the error message

  - *"Cannot install external physical interface."*

  Executing the "Reduce database" ETS function will lead to project data corruption for the alarm central unit and should be avoided under any circumstances.
  Renaming any group addresses already created will not be possible from the ETS plug-in of the alarm central unit either.