User Manual

ABB i-bus® EIB
EIB-Interface L 208/EIB

Intelligent Installation Systems

ABB STOTZ-KONTAKT

ABB i-bus® EIB

Application Software – Alarm Panel Interface/1

Type: EIB-Interface – GH Q631 0032 R0111

Contents

This manual describes the function of the EIB-Interface in combination with the intrusion alarm panel L 208 using software version V3.00w onwards.

Technical specifications are subject to change without further notice.

1

1   Device Configuration

1.1   Introduction

The EIB-Interface enables bi-directional communication between an EIB installation and an L208 intrusion alarm panel. This allows the integration of professional security functions into intelligent installation systems and thus an increase in the total security and comfort of a building.

The EIB-Interface provides the EIB system with a multitude of security relevant signals coming from the intrusion alarm panel. This information can be used to activate various control functions or automatic procedures within the EIB installation, for example:

● when the alarm system is externally set, presence simulation can be started, lighting turned off centrally, or room temperature reduced to minimise energy wastage,

● in the event of an alarm, panic or emergency lighting can be activated or shutters opened or closed, or

● the status of the installation can be displayed or visualised centrally or de-centrally at any point within the EIB system.

In the opposite direction, selected EIB telegrams received by the EIB-Interface are transformed and passed on to the intrusion alarm panel for further evaluation. This allows the implementation of a host of comfortable applications, for example:

● operation of the intrusion alarm system via EIB from any position on the bus without additional cabling expenditure,

● central administration of important alarm and fault signals coming from the EIB installation,

● direct integration into the alarm system of EIB bus capable security sensors or conventional security sensors via the Zone Terminal MT/S 4.12.1 (up to 32 inputs), and

● tamper monitoring of the EIB and/or individual EIB devices.

1.2   Installation

The EIB-Interface is designed to be mounted in the dedicated area in the L208 intrusion alarm panel housing (see diagram below). The printed circuit board is fixed into the alarm panel using four screws (M3 x 6 mm) with washers (supplied). Instructions for the installation, commissioning and operation of the intrusion alarm panel can be found in the alarm panel user manual „Installation-Commissioning-Operation".

ESD (**E**lectro **S**tatic **D**ischarge) safety measures must be observed when installing and commissioning the EIB-Interface.

Internal Layout: L208 Intrusion Alarm Panel
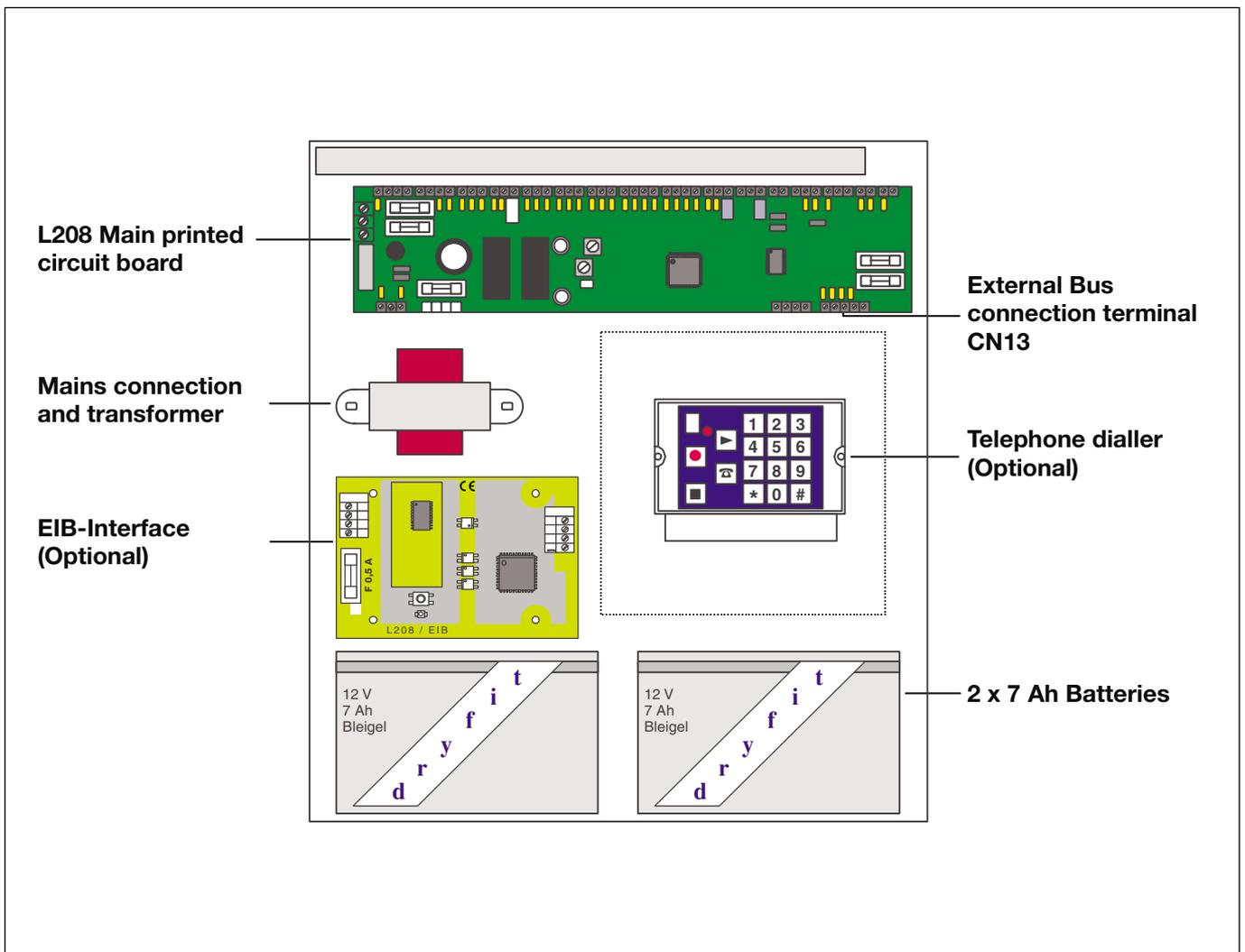
1.3 Connection

Connection of the ABB i-bus® EIB Bus and the XIB Security Bus to the EIB-Interface is made using pluggable screw terminals.

ABB i-bus® EIB   Terminal X1: + B: EIB + (red)
                                           – B: EIB – (black)

XIB Security Bus   Terminal X2: (+, –, A, B)
                            from connection terminal CN13 „Ext. Bus (XIB)"
                            on the L208 main printed circuit board.

**Auxiliary Voltage
Supply Output**   Terminal X1: (12 V, 0 V),

The auxiliary voltage supply output is an optional 12 V DC connection for supplying external security devices in the EIB installation, e.g., for supplying the Zone Terminal MT/S 4.12.1 as well as smoke detectors and/or motion detectors. The output can supply a maximum of 0.5 A and is protected against short circuit with fuse F1: 0.5 A quick blow 20mm (replacement included). The 12 V supply is buffered from the batteries of the intrusion alarm panel.

Important: When calculating the total backup time of the emergency power supply of the intrusion alarm panel, the current consumption of the auxiliary voltage supply output must also be taken into consideration.

Connection Diagram

Programming push-button and LED
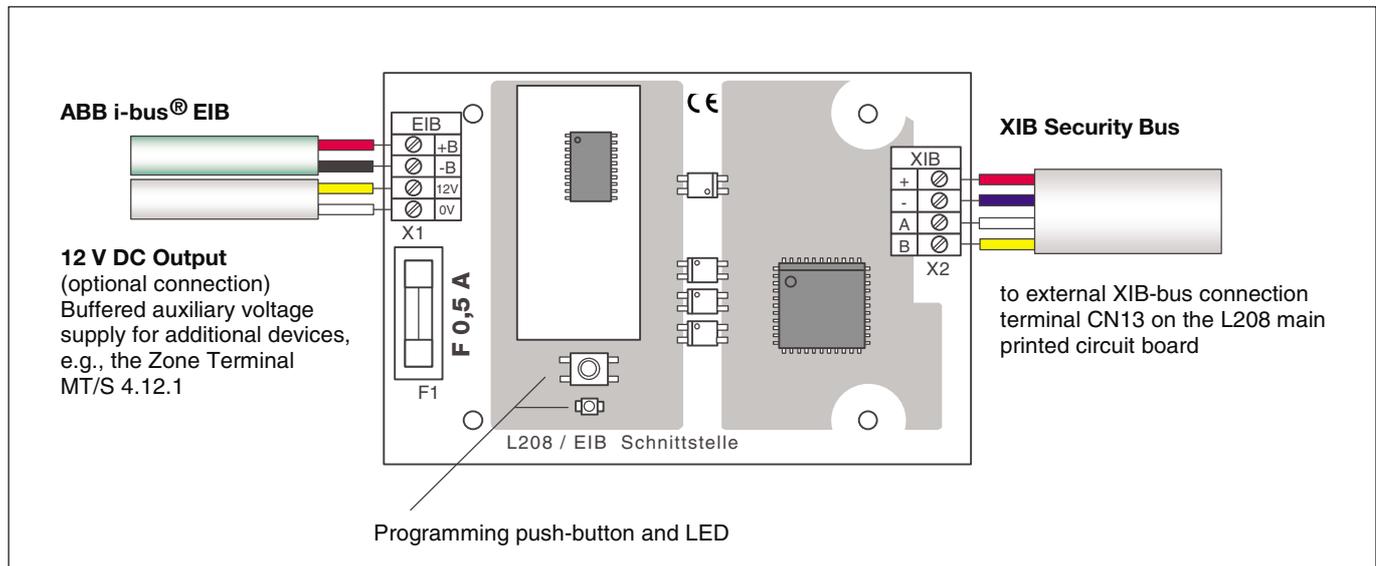
Note: Wherever the EIB-Interface is employed in couple an intrusion alarm panel to the EIB, it must be ensured that the cabling and installation of the alarm system complies with the SELV guidelines.

2   Commissioning

2.1   Activation of the EIB-Interface

In order to commission the EIB-Interface, communication must first be established between the intrusion alarm panel and the EIB-Interface. There are two methods of activating the EIB-Interface: the automatic recognition procedure and the manual configuration technique.

In both cases, it is important that:

1) the EIB-Interface has been programmed with the EIB application software Alarm Panel Interface/1 (see chapter 3),
2) the intrusion alarm panel is programmed with software version V3.00 t or higher,
3) the EIB-Interface is correctly connected to the alarm panel and,
4) the EIB-Interface is supplied with EIB bus voltage during commissioning.

After carrying out steps 1 to 4, the automatic recognition procedure can be carried out by simply switching on the mains supply to the intrusion alarm panel. If the alarm panel is already in operation, the mains supply must first be briefly turned off (e.g. mains fuse removed), the battery or batteries isolated, and then the alarm panel switched on again.

The EIB-Interface is automatically recognised by the intrusion alarm panel and put into the last programmed configuration mode (see chapter 2.2). On commissioning the intrusion alarm panel together with an EIB-Interface for the first time, the default configuration mode „Standard" is pre-programmed.

2.2   Configuration of the Intrusion Alarm Panel

The manual configuration technique allows authorised installers and security personal to activate or deactivate the EIB-Interface using the LCD keypad (L840/PT). The EIB-Interface's mode of operation can also be changed.
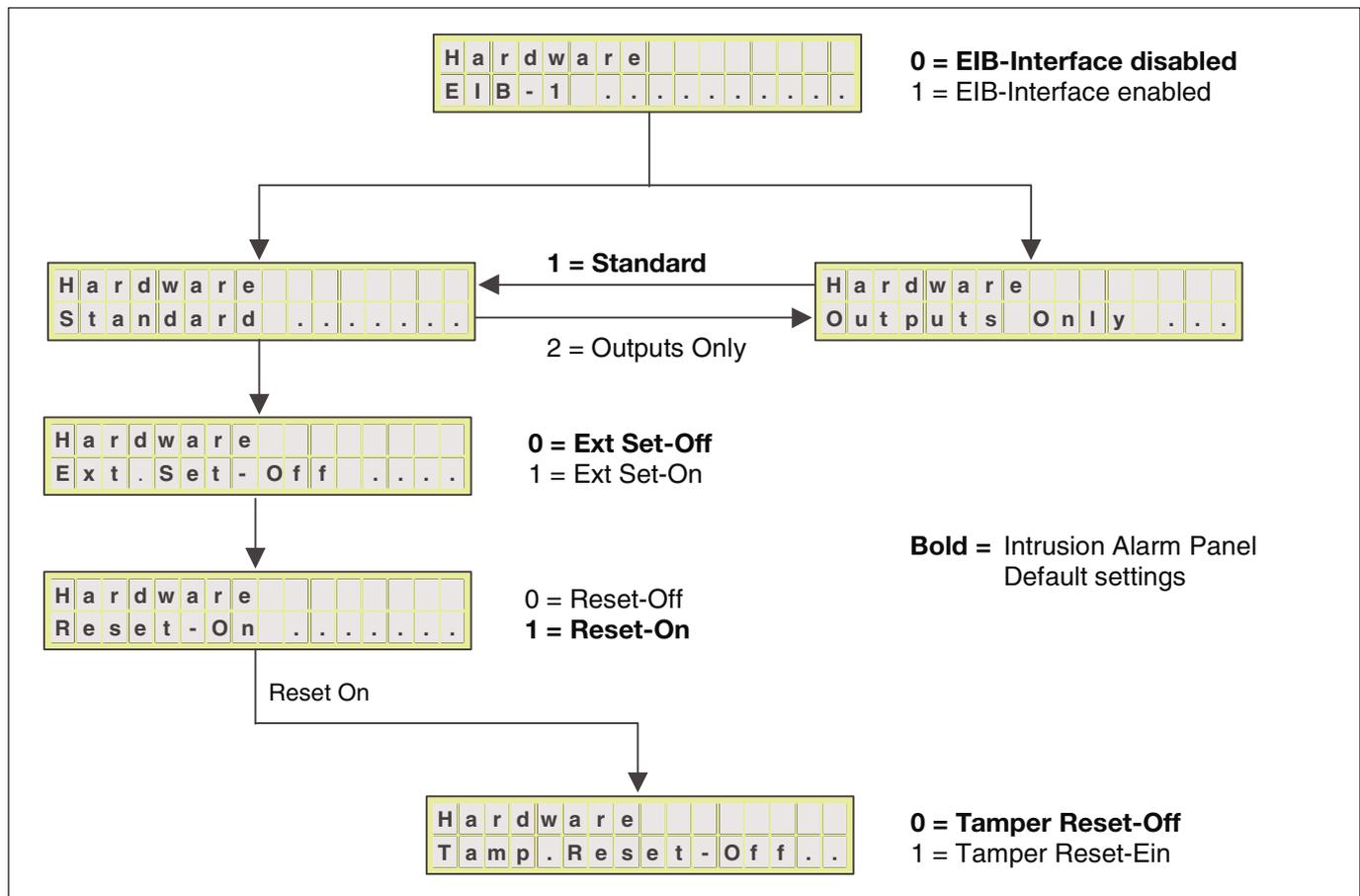
The menu structure outlined on the next page for the configuration of the EIB-Interface can be found under the ‚Engineer level' configuration menu – ‚Edit/Hardware' – in the programming menu structure of the intrusion alarm panel. Further information over the operation of the alarm panel in conjunction with the keypad L840/PT can be found in the intrusion alarm panel user manual „Installation-Commissioning-Operation".

Hardware-EIB: The option „Hardware-EIB" allows communication between the EIB-Interface and the intrusion alarm panel to be activated or deactivated.

If this option is disabled, while an EIB-Interface is connected, communication is interrupted and all EIB output communication objects and their respective values are frozen. A manual activation of the EIB-Interface communication, without an EIB-Interface being connected to the alarm panel, will result in a tamper alarm.

An active EIB-Interface can operate in two modes: „Standard" or „Outputs Only".

Intrusion Alarm Panel Configuration Menu

```
┌───────────────────────────────────────────────────────────────────────────┐
│                                                                           │
│            ┌─────────────────────────┐                                    │
│            │ H a r d w a r e         │     0 = EIB-Interface disabled     │
│            │ E I B - 1 . . . . . . . │     1 = EIB-Interface enabled      │
│            └─────────────────────────┘                                    │
│                                                                           │
│   ┌─────────────────────────┐   1 = Standard   ┌─────────────────────────┐│
│   │ H a r d w a r e         │◄───────────────  │ H a r d w a r e         ││
│   │ S t a n d a r d . . . . │ ───────────────► │ O u t p u t s  O n l y  ││
│   └─────────────────────────┘  2 = Outputs Only└─────────────────────────┘│
│                                                                           │
│   ┌─────────────────────────┐     0 = Ext Set-Off                         │
│   │ H a r d w a r e         │     1 = Ext Set-On                          │
│   │ E x t . S e t - O f f . │                                            │
│   └─────────────────────────┘        Bold =  Intrusion Alarm Panel        │
│                                               Default settings            │
│   ┌─────────────────────────┐     0 = Reset-Off                           │
│   │ H a r d w a r e         │     1 = Reset-On                            │
│   │ R e s e t - O n . . . . │                                            │
│   └─────────────────────────┘                                            │
│      Reset On                                                             │
│                                                                           │
│            ┌─────────────────────────┐                                    │
│            │ H a r d w a r e         │     0 = Tamper Reset-Off            │
│            │ T a m p . R e s e t - O f f . . │ 1 = Tamper Reset-Ein       │
│            └─────────────────────────┘                                    │
└───────────────────────────────────────────────────────────────────────────┘
```

Outputs Only: In the configuration mode „Outputs Only", information is transferred in one direction only, from the intrusion alarm panel to the EIB. Telegrams that are received by the EIB-Interface are not forwarded to the alarm panel. In this case, the intrusion alarm panel can not be influenced by events within the EIB system. The function of the alarm panel is isolated from the EIB in the sense of the VdS guidelines as the two systems are electrically isolated from one another. Although no EIB information is utilised by the intrusion alarm panel, the connection between the alarm panel and the EIB-Interface is still monitored against tamper attempts.

Standard: The configuration mode „Standard" allows a true bi-directional communication between the EIB installation and the intrusion alarm panel. In this mode, all input and output signals can be enabled.

Hardware-Ext Set: In order to protect the intrusion alarm panel from unauthorised external set requests from the EIB installation, the option „Hardware-Ext Set" allows this function to be enabled or disabled.

Hardware-(Tamp) Reset: In the same way, it is possible using the options „Hardware-Reset" and „Hardware-Tamp.Reset" to prevent important alarm panel fault signals from being reset over the EIB. If the option „Hardware-Reset" is enabled, all fault signals, apart from tamper, can be reset over the EIB. Enabling the option „Hardware-Tamp.Reset" also permits tamper faults to be reset.

3   ETS Project Design

3.1   Communication Objects

In maximum configuration, the application software „Alarm Panel Interface/1" possesses 67 communication objects: 24 output objects and 43 input objects. All communication objects are 1-bit objects.

The communication objects are dynamic in nature and are only visible when the corresponding parameters are enabled. At the start of the project design, all EIB-Interface communication objects are disabled or inactive.

Each communication object can only be assigned a single group address.

Output Objects: Signals from the Intrusion Alarm Panel ➜ EIB

Phys.Addr.	Product	Order number	Medium Type	Program	Manufacturer
no.	Function	Object name	Type		
01.01.001	EIB-Interface L208/EIB	GH Q631 0032 R0111	Twisted Pair	Alarm Panel Interface/1	ABB
43	External Alarm (Strobe)	Output Telegram	1 Bit		
44	External Alarm (Sounder)	Output Telegram	1 Bit		
45	Internal Alarm	Output Telegram	1 Bit		
46	External Set	Output Telegram	1 Bit		
47	Internal Set	Output Telegram	1 Bit		
48	External or Internal Set	Output Telegram	1 Bit		
49	Reset	Output Telegram	1 Bit		
50	Ready to Set	Output Telegram	1 Bit		
51	Set Confirmation	output telegram	1 Bit		
52	Fault	Output Telegram	1 Bit		
53	Personal Attack	Output Telegram	1 Bit		
54	Tamper	Output Telegram	1 Bit		
55	Zone Alarm	Output Telegram	1 Bit		
56	Intrusion	Output Telegram	1 Bit		
57	Alarm Panel Zone 01 Status	Output Telegram	1 Bit		
58	Alarm Panel Zone 02 Status	Output Telegram	1 Bit		
59	Alarm Panel Zone 03 Status	Output Telegram	1 Bit		
60	Alarm Panel Zone 04 Status	Output Telegram	1 Bit		
61	Alarm Panel Zone 05 Status	Output Telegram	1 Bit		
62	Alarm Panel Zone 06 Status	Output Telegram	1 Bit		
63	Alarm Panel Zone 07 Status	Output Telegram	1 Bit		
64	Alarm Panel Zone 08 Status	Output Telegram	1 Bit		
65	Alarm Panel Zone 09 Status	Output Telegram	1 Bit		
66	Alarm Panel Zone 10 Status	Output Telegram	1 Bit		

Building View [Intrusion Alarm Panel/EIB-Interface]

Building   Building part   Room   Device   ☑ Show Objects

ABB i-bus® EIB

Application Software – Alarm Panel Interface/1

Type: EIB-Interface   – GH Q631 0032 R0111

Inputs Objects: **Signals from the EIB ➜ Intrusion Alarm Panel**

|	Phys.Addr.	Product	Order number	Medium Type	Program	Manufacturer
	no.	Function	Object name	Type		
	01.01.001	EIB-Interface L208/EIB	GH Q631 0032 R0111	Twisted Pair	Alarm Panel Interface/1	ABB
	0	Int. Set/Unset Request	Input Telegram	1 Bit		
	1	Ext. Set/Unset Request	Input Telegram	1 Bit		
	2	Reset Request	Input Telegram	1 Bit		
	3	EIB-Input Panel Zone 1 A	Input Telegram	1 Bit		
	4	EIB-Input Panel Zone 1 B	Input Telegram	1 Bit		
	5	EIB-Input Panel Zone 1 C	Input Telegram	1 Bit		
	6	EIB-Input Panel Zone 1 D	Input Telegram	1 Bit		
	7	EIB-Input Panel Zone 2 A	Input Telegram	1 Bit		
	8	EIB-Input Panel Zone 2 B	Input Telegram	1 Bit		
	9	EIB-Input Panel Zone 2 C	Input Telegram	1 Bit		
	10	EIB-Input Panel Zone 2 D	Input Telegram	1 Bit		
	11	EIB-Input Panel Zone 3 A	Input Telegram	1 Bit		
	12	EIB-Input Panel Zone 3 B	Input Telegram	1 Bit		
	13	EIB-Input Panel Zone 3 C	Input Telegram	1 Bit		
	14	EIB-Input Panel Zone 3 D	Input Telegram	1 Bit		
	15	EIB-Input Panel Zone 4 A	Input Telegram	1 Bit		
	16	EIB-Input Panel Zone 4 B	Input Telegram	1 Bit		
	17	EIB-Input Panel Zone 4 C	Input Telegram	1 Bit		
	18	EIB-Input Panel Zone 4 D	Input Telegram	1 Bit		
	19	EIB-Input Panel Zone 5 A	Input Telegram	1 Bit		
	20	EIB-Input Panel Zone 5 B	Input Telegram	1 Bit		
	21	EIB-Input Panel Zone 5 C	Input Telegram	1 Bit		
	22	EIB-Input Panel Zone 5 D	Input Telegram	1 Bit		
	23	EIB-Input Panel Zone 6 A	Input Telegram	1 Bit		
	24	EIB-Input Panel Zone 6 B	Input Telegram	1 Bit		
	25	EIB-Input Panel Zone 6 C	Input Telegram	1 Bit		
	26	EIB-Input Panel Zone 6 D	Input Telegram	1 Bit		
	27	EIB-Input Panel Zone 7 A	Input Telegram	1 Bit		
	28	EIB-Input Panel Zone 7 B	Input Telegram	1 Bit		
	29	EIB-Input Panel Zone 7 C	Input Telegram	1 Bit		
	30	EIB-Input Panel Zone 7 D	Input Telegram	1 Bit		
	31	EIB-Input Panel Zone 8 A	Input Telegram	1 Bit		
	32	EIB-Input Panel Zone 8 B	Input Telegram	1 Bit		
	33	EIB-Input Panel Zone 8 C	Input Telegram	1 Bit		
	34	EIB-Input Panel Zone 8 D	Input Telegram	1 Bit		
	35	EIB-Tamper Input 1	Input Telegram	1 Bit		
	36	EIB-Tamper Input 2	Input Telegram	1 Bit		
	37	EIB-Tamper Input 3	Input Telegram	1 Bit		
	38	EIB-Tamper Input 4	Input Telegram	1 Bit		
	39	EIB-Tamper Input 5	Input Telegram	1 Bit		
	40	EIB-Tamper Input 6	Input Telegram	1 Bit		
	41	EIB-Tamper Input 7	Input Telegram	1 Bit		
	42	EIB-Tamper Input 8	Input Telegram	1 Bit		

3.2   Parameter Options

When initially configuring the application software „Alarm Panel Interface/1" and beginning with the project design, all parameter options are disabled or inactive.

In order to minimise unnecessary telegram traffic on the bus and to ensure that the security of the installation is not compromised, only those signal and parameter options that are actually required should be enabled.

Note: Some parameter options, e.g., the external setting of the intrusion alarm panel via EIB, only function when, in addition to enabling the relevant parameter options in the EIB application software, the corresponding options in the alarm panel configuration menus have also been enabled.

3.3   Parameter Window: General

The basic security and monitoring functions of the EIB-Interface are configured via the parameter window "General".
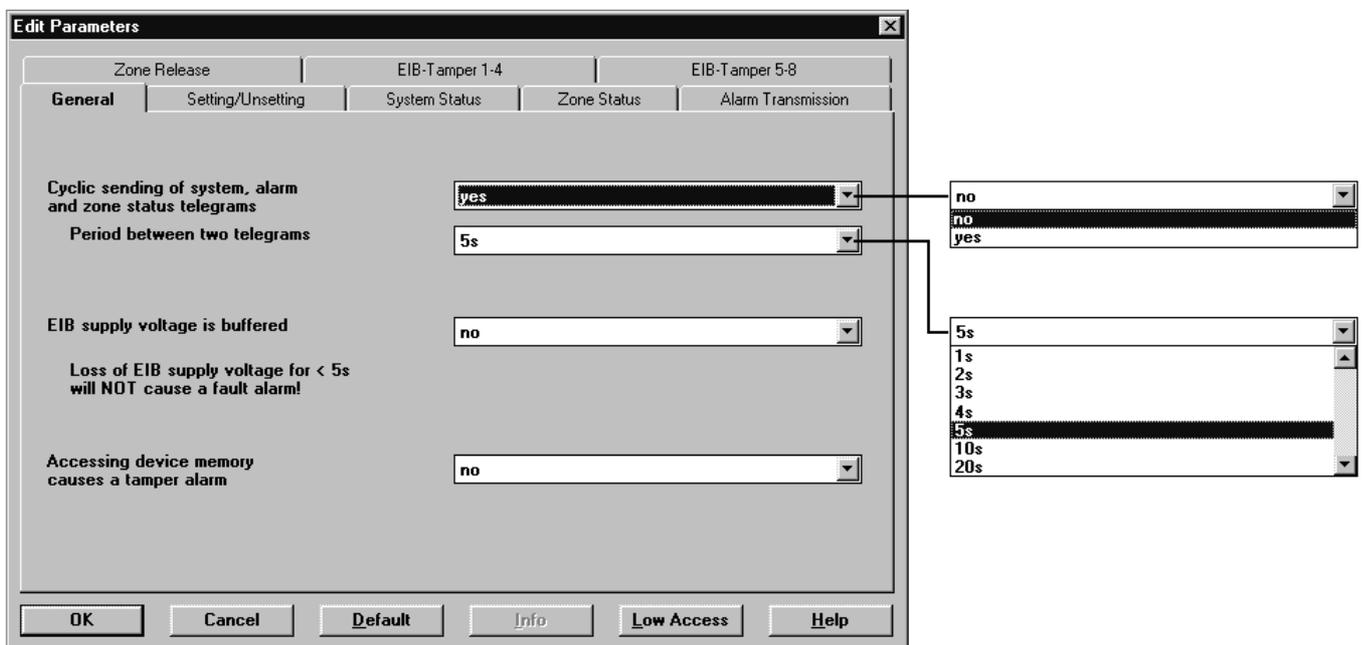
Cyclic sending of system, alarm and zone status telegrams: In order to ensure that all bus devices in the EIB security installation are always ‚up to date', information from the intrusion alarm panel can be cyclically sent onto the EIB using the parameter „Cyclic sending of system, alarm and zone status telegrams". In this way the status, e.g., of devices that have been temporarily isolated for the bus, can be updated within the shortest possible time. Telegrams are only sent cyclically from enabled communication objects.

The dynamic parameter „Period between two telegrams" allows the time between the transmission of these telegrams to be set. The time required to completely update the entire EIB security installation corresponds roughly to the period between two telegrams multiplied by the number of enabled or active output communication objects.

Important: On restoration of the EIB supply after a bus voltage failure, an automatic ‚quick update' procedure is started independently of the cyclic sending parameter settings. This procedure updates the EIB installation within approximately 5s of the bus voltage being restored.

EIB supply voltage is buffered: The intrusion alarm panel continually monitors the correct operation of the EIB-Interface. Should the EIB supply voltage fail or a fault develop in the EIB-Interface itself, a system fault is reported by the intrusion alarm panel.

If the EIB power supply is not buffered, short duration interruptions of the EIB supply voltage can intermittently occur, e.g., due to regular switching processes in the mains supply network. In order to avoid unnecessary fault information being reported by the intrusion alarm panel during this events, the parameter „EIB supply voltage is buffered" (setting „no"), can be used to make the alarm
panel insensitive to EIB supply voltage interruptions of up to approx. 5s. Supply interruptions that last for longer than 5s,will however, cause a fault to be reported.

Note: If the EIB supply voltage is not buffered or the backup time of the supply buffer is inadequate, i.e., a shorter backup time than that dimensioned in the intrusion alarm panel, the alarm panel will continue to function normally in the event of a mains failure, however, no information can be received or transmitted over the EIB. If important security or fault information from the EIB installation is being evaluated by the intrusion alarm panel, e.g., as is the case where the security system incorporates EIB components such as the Zone Terminal, the EIB power supply must be buffered for at least the same length of time as the intrusion alarm panel in order to ensure that this information is also correctly transmitted and evaluated during a mains failure.

If the EIB power supply voltage is buffered, a loss of EIB bus voltage would imply either a defective power supply or a possible tamper attempt. If the parameter „EIB supply voltage is buffered" is set to „yes", all EIB bus voltage failures result in the alarm panel reporting a fault.

Important: An intrusion alarm panel with a defective EIB communication path, i.e., EIB bus voltage failure or defective EIB-Interface, can not be set. In order to set the alarm panel alone in this condition, the EIB-Interface must first be deactivated via the configuration menus of the alarm panel.

Accessing device memory causes a tamper alarm: In order to prevent unauthorised persons from reprogramming the EIB-Interface undetected, the parameter „Accessing device memory causes a tamper alarm" can de enabled. If the setting „yes" is selected, any attempt to reprogram the application software contained in the EIB-Interface results in a tamper alarm being generated by the intrusion alarm panel.

Important: Should the EIB-Interface need to be reprogrammed while the installation is in operation and the „Accessing device memory causes a tamper alarm" option is enabled, the EIB-Interface must first be deactivated via the configuration menus of the intrusion alarm panel in order to prevent unwanted tamper alarms being generated.

3.4   Parameter Window: Setting/Unsetting

Via the parameter window „Setting/Unsetting", it is possible to define whether the intrusion alarm panel can be set and/or reset via the EIB.

Enable Setting/Unsetting over the EIB: The parameters „External Set/Unset" and „Internal Set/Unset" enable the alarm panel to be set and unset via telegrams from the EIB.

Telegram value   „1": Alarm panel set request or installation set
                    „0": Alarm panel unset request or installation unset.

If a set or unset request is successful, the set or unset state of the alarm panel is confirmed via the system status signals. If a set attempt is unsuccessful, i.e., the alarm panel was not ready to set, the set request from the EIB is automatically removed after approx. 1.5 seconds and a telegram from the corresponding „Set request" communication object is sent back to the EIB installation cancelling the request.
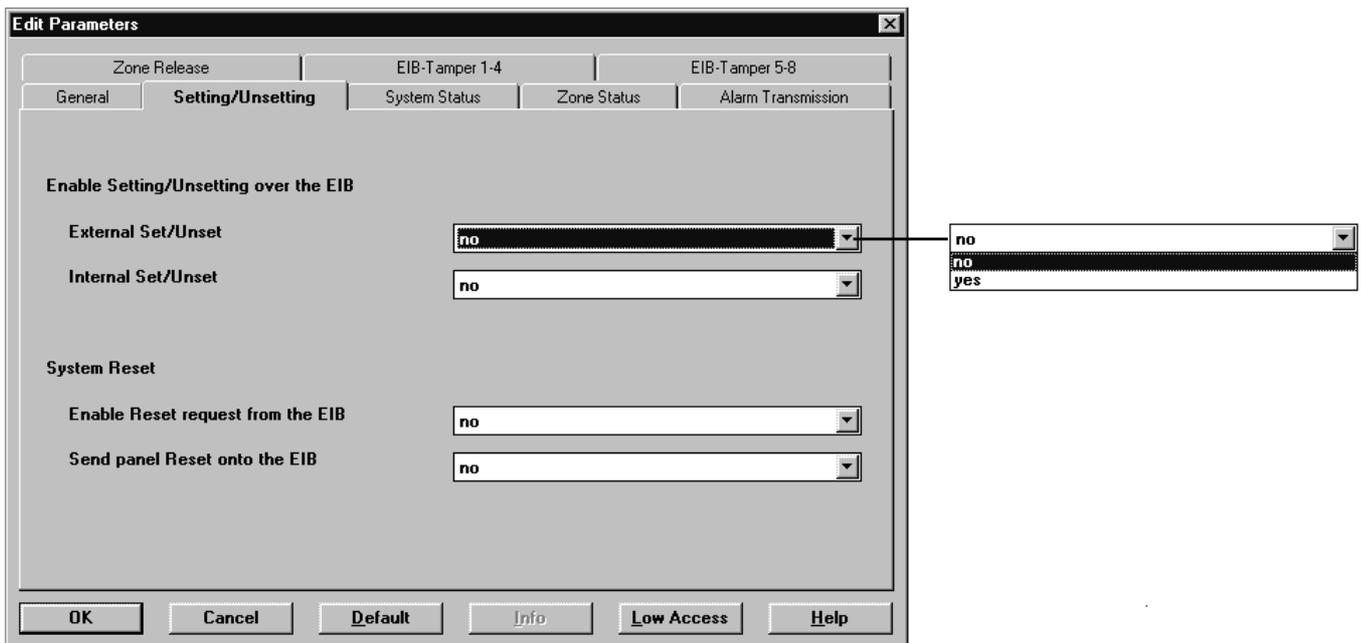
System Reset: The parameter „Enable Reset request from the EIB" permits the alarm panel to be reset via the EIB.

Telegram value   „1": Reset request (only when alarm panel is unset)
                    „0": no function

If the parameter "Send panel Reset onto the EIB" is enabled, the reset signals generated by the intrusion alarm panel are sent onto the EIB. These signals can be used to reset devices in the EIB installation, e.g., the Zone Terminal MT/S 4.12.1. Approximately 2 seconds after sending the reset signal „1", the EIB interface automatically sends a „0" via the „Reset" communication object.

Telegram value   „1": Reset
                    „0": no function

3.5	**Parameter Window: System Status**

Via the parameter window „System Status", it is possible to define which status signals are to be sent by the intrusion alarm panel onto the EIB. If the setting „yes" is selected, the current status of the alarm panel is transferred onto the EIB. If the option „no" is selected, no status signal is transmitted.
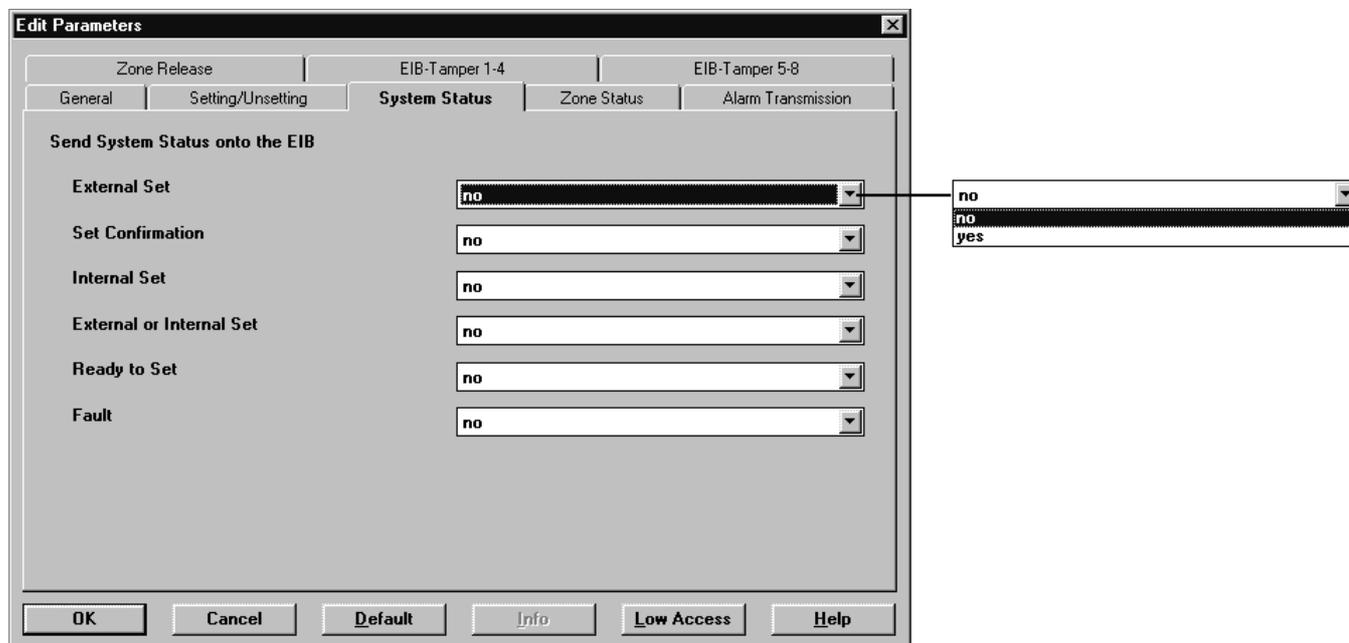
External Set: Signals whether the alarm panel has been externally set or unset.

Telegram value	„1": Alarm panel is externally set.
	„0": Alarm panel is not externally set.

Set Confirmation: Momentary signal indicating that the alarm panel has been successfully externally set. The duration of the set confirmation signal is configured in the intrusion alarm panel (Default 3s).

Internal Set: Signals whether the alarm panel has been internally set or unset.

Telegram value	„1": Alarm panel is internally set.
	„0": Alarm panel is not internally set.

External or Internal Set: Signals whether the alarm panel has been internally or externally set or unset.

Telegram value	„1": Alarm panel is externally or internally set.
	„0": Alarm panel is unset.

Ready to Set: Indicates that no zone faults or other fault signals are present that will prevent the intrusion alarm panel from being set and that the alarm panel is ready to set.

Telegram value	„1": Alarm panel is ready to set.
	„0": Alarm panel is not ready to set, faults are present

Fault: Telegrams are sent when the intrusion alarm panel reports a system fault, e.g., a mains or battery failure or a telephone dialler or EIB fault.

Telegram value	„1": Fault
	„0": no fault

**3.6   Parameter Window:
          Zone Status**

Via the parameter window „Zone Status", it is possible to define which zone status signals are to be sent from the intrusion alarm panel onto the EIB. Using the setting „Send status onto the EIB", the respective, current alarm panel zone status is transferred onto the EIB. If the option „Do not send status onto the EIB" is selected, this zone information is not transmitted.

The behaviour of these zone communication objects depends on the zone type, e.g., intrusion, tamper, etc., and the events that have taken place up to that point in time. The zone type is programmed in the intrusion alarm panel.

Alarm panel zones that are programmed as „Tamper", „Fire" or „Technical" zone types have the highest priority and their status signals are sent onto the EIB regardless of whether the system is set or unset. These status signals are stored until the alarm system is reset.

The „Personal Attack" zone type causes a momentary signal to be sent onto the EIB. The duration of the panic signal is set in the alarm panel (Default 120s).

Faults reported by „Intruder" zone types are only stored when the intrusion alarm panel is set. If one or more zone faults have been stored during the set condition, faults that are detected in previously undisrupted „Intruder" zones after the alarm system has been unset are not transmitted onto the EIB. This avoids the corruption of the stored zone fault information in the EIB. The current zone fault signals are only transmitted again onto the EIB once the alarm panel has been reset.

Faults reported by „Lock monitoring" zone types are not stored, have no alarm function and only prevent the system from being set.
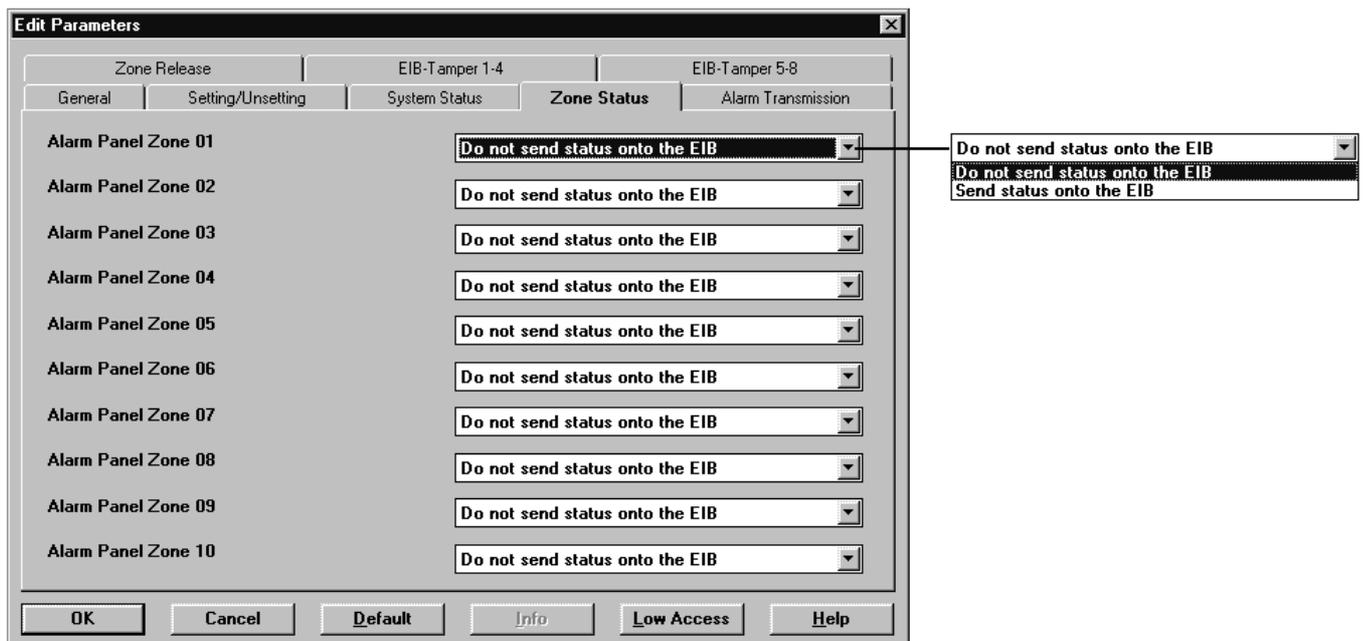
3.7	**Parameter Window:**	Via the parameter window „Alarm Transmission", it is possible to define,
	Alarm Transmission	

Via the parameter window „Alarm Transmission", it is possible to define, which alarm signals from the intrusion alarm panel are to be sent onto the EIB. The setting „yes" allows alarm signals to be transmitted to the EIB installation. If the option "no" is selected, the corresponding signal information is not sent.
For all signals the following applies:
Telegram value   „1": Alarm
                    „0": no Alarm
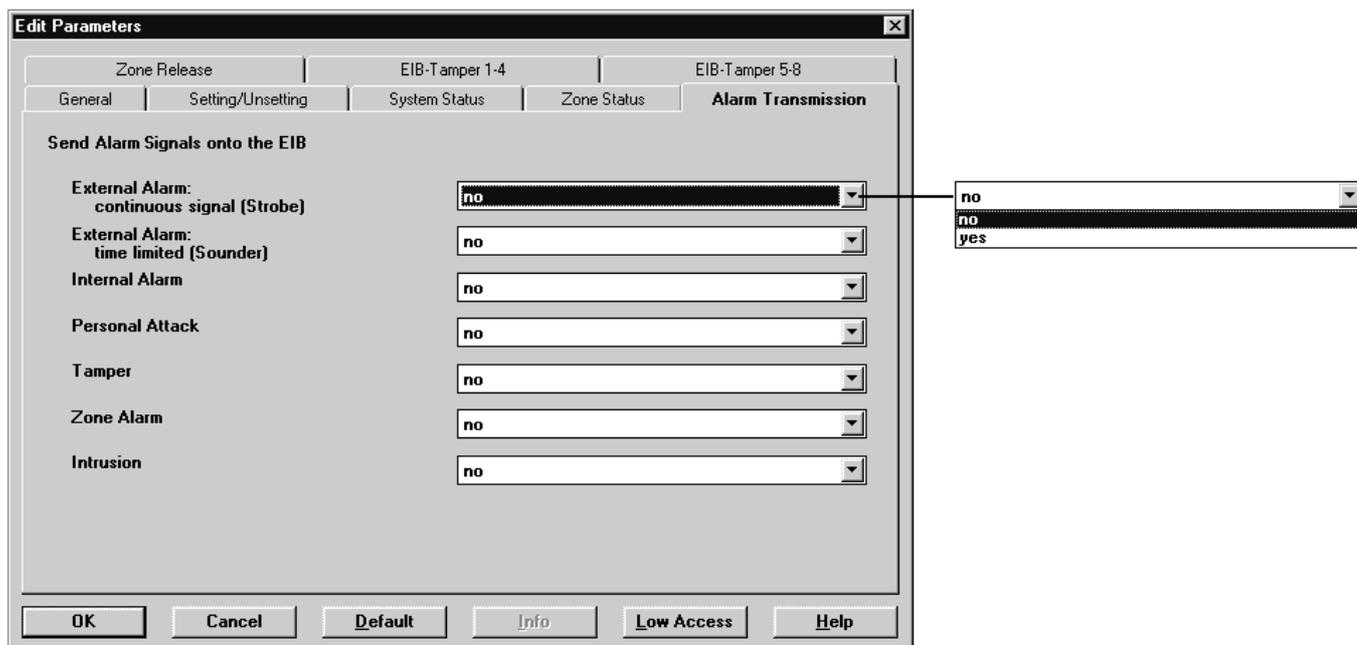
External Alarm: continuous signal (Strobe): Signals an alarm in the externally set condition. The alarm signal remains stored until a system reset is carried out.

External Alarm: time limited (Sounder): Signals an alarm in the externally set condition. The duration of the alarm signal is configured in the intrusion alarm panel (Default 120s).

Internal Alarm: Reports an alarm in the internally set condition and in the event of a tamper fault (unset condition). The duration of the alarm signal is configured in the intrusion alarm panel (Default 120s).

Personal Attack: Indicates one or more personal attack signals. The alarm signal remains stored until a system reset is carried out.

Tamper: Signals a tamper attempt on the system. The alarm signal remains stored until a system reset is carried out.

Zone Alarm: Combined alarm signal for intrusion alarms (set condition) and personal attack alarms. The alarm signal remains stored until a system reset is carried out.

Intrusion: Reports an intrusion alarm in the externally set condition.
The duration of the alarm signal is configured in the intrusion alarm panel (Default 120s).

**3.8 Parameter Window:
Zone Release**

A total of 32 communication objects for use in the EIB installation can be assigned via the EIB-Interface to the first eight zones of the intrusion alarm panel. With the parameters „Alarm Panel Zone 01 – 08", EIB communication objects can be enabled. Telegrams from the EIB installation received by these communication objects are passed on and influence the corresponding zone of the intrusion alarm panel.

This function allows important signals from the EIB installation to be centrally administrated in the intrusion alarm panel. These signals can come directly from EIB bus capable security sensors or from conventional sensors that are connected via the Zone Terminal MT/S 4.12.1.
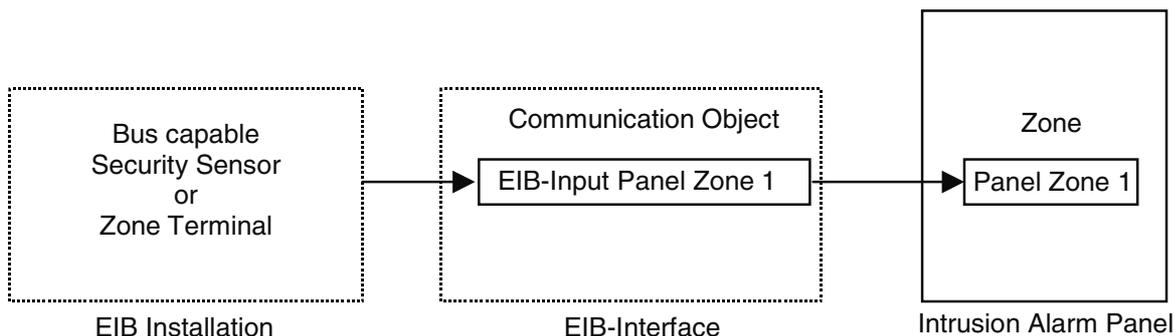
The following applies for all alarm panel zone EIB input communication objects:
Telegram value „1": Disrupt alarm panel zone
„0": Do not disrupt alarm panel zone
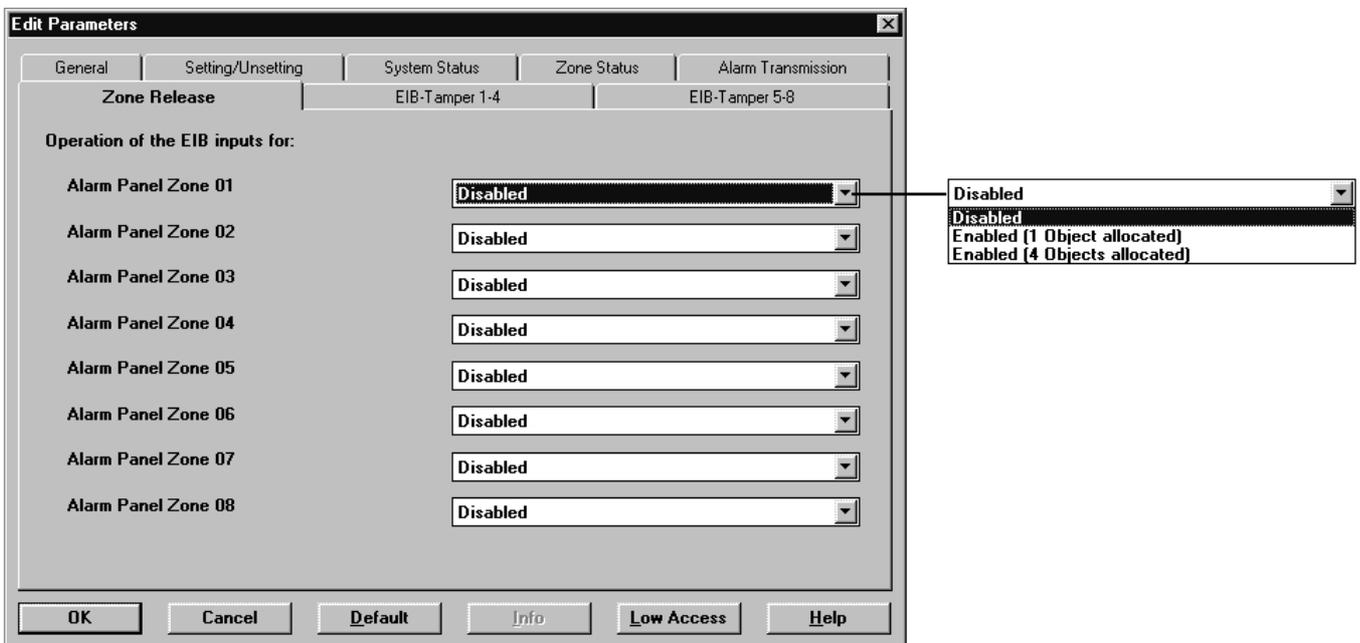
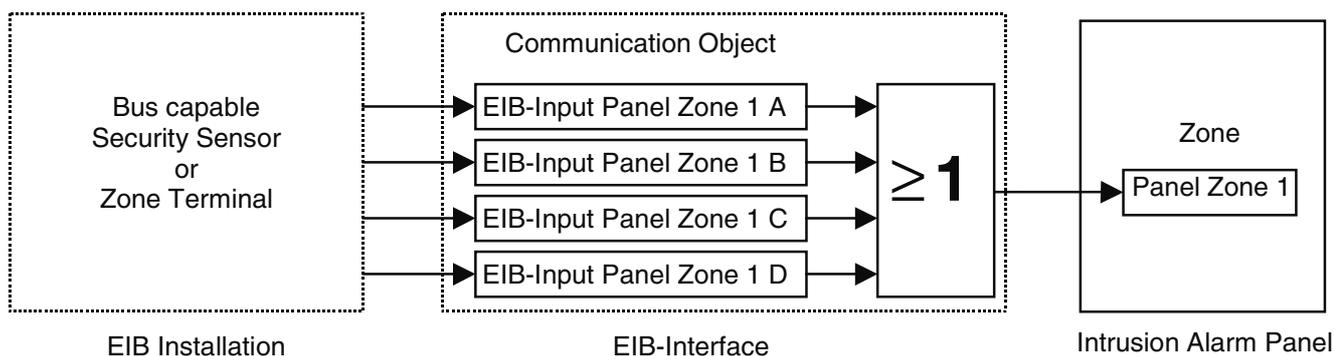**Disabled:** This setting prevents the alarm panel zone from being disrupted by signals coming from the EIB.

Enabled (1 Object allocated): With this setting, an EIB input communication object is made available. If a telegram with the value „1" is received by this communication object, this causes a fault in the corresponding zone of the intrusion alarm panel. The following schematic displays the described function.
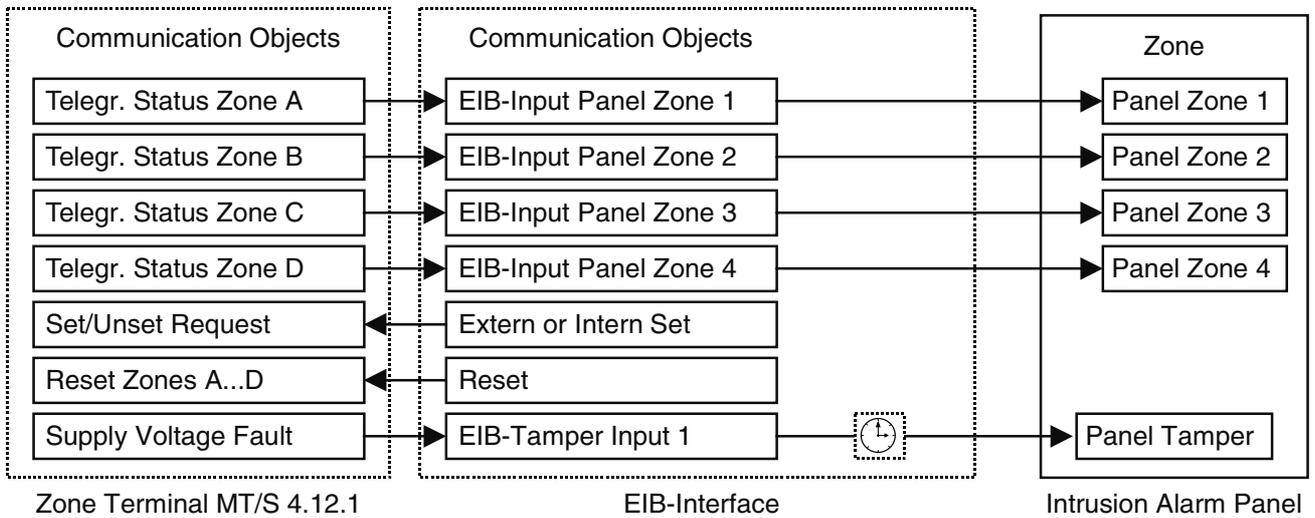
Bus capable Security Sensor or Zone Terminal	→	Communication Object [EIB-Input Panel Zone 1]	→	Zone [Panel Zone 1]
EIB Installation		EIB-Interface		Intrusion Alarm Panel

Enabled (4 Objects allocated): With this setting, four EIB input communication objects are made available. If one or more of these communication objects receives a telegram with the value „1", a fault in the corresponding zone in the alarm panel is generated (logical ‚OR' function). The following schematic displays the described function.

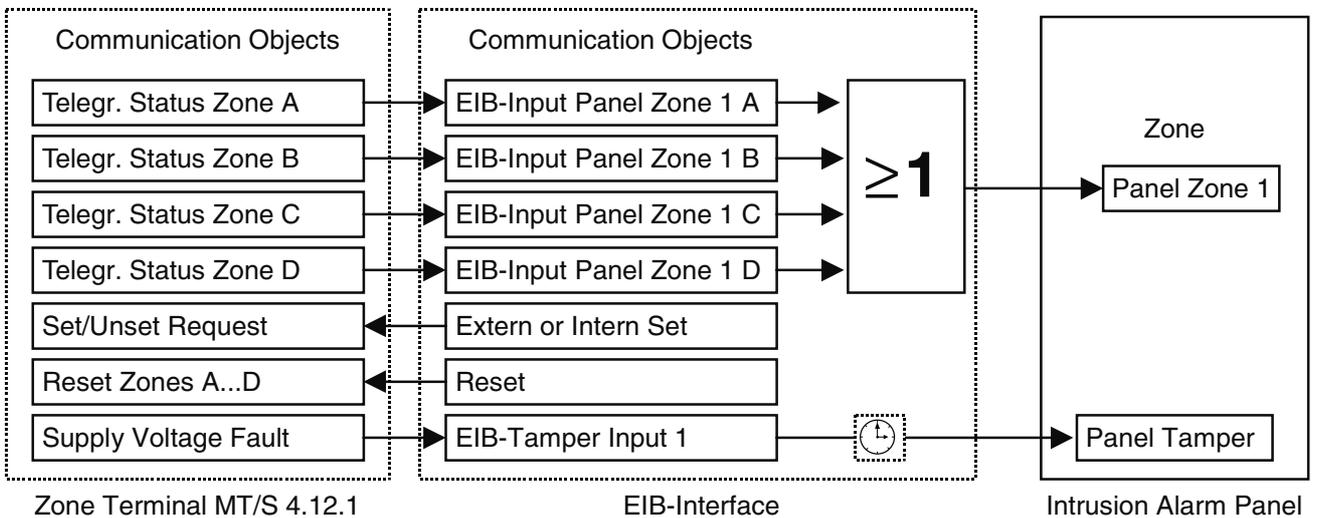| Bus capable Security Sensor or Zone Terminal	Communication Object EIB-Input Panel Zone 1 A EIB-Input Panel Zone 1 B EIB-Input Panel Zone 1 C EIB-Input Panel Zone 1 D	≥1	Zone [Panel Zone 1]
EIB Installation	EIB-Interface		Intrusion Alarm Panel

With this setting, it is possible to assign all four zones of a Zone Terminal MT/S 4.12.1 to a single intrusion alarm panel zone. This enables the number of zones on the EIB side to be extended up to a maximum of 32.

Important: If a Zone Terminal MT/S 4.12.1 is linked with the intrusion alarm panel, **all** the zones of the Zone Terminal must be assigned to communication objects in the EIB-Interface, i.e., the zones of the intrusion alarm panel, either individually or as a group. In addition, the Zone Terminal communication object „Supply Voltage Fault", must be linked with one of the EIB tamper inputs of the EIB-Interface, independently of whether the communication object is set for cyclical sending or not.

16

**Connection of a Zone Terminal with Single Object Allocation**

Communication Objects		Communication Objects			Zone	
Telegr. Status Zone A	→	EIB-Input Panel Zone 1	→		Panel Zone 1	
Telegr. Status Zone B	→	EIB-Input Panel Zone 2	→		Panel Zone 2	
Telegr. Status Zone C	→	EIB-Input Panel Zone 3	→		Panel Zone 3	
Telegr. Status Zone D	→	EIB-Input Panel Zone 4	→		Panel Zone 4	
Set/Unset Request	←	Extern or Intern Set				
Reset Zones A...D	←	Reset				
Supply Voltage Fault	→	EIB-Tamper Input 1	→ 🕐 →		Panel Tamper	

Zone Terminal MT/S 4.12.1   EIB-Interface   Intrusion Alarm Panel

Connection of a Zone Terminal with 4-fold Object Allocation

Communication Objects		Communication Objects				
Telegr. Status Zone A	→	EIB-Input Panel Zone 1 A	→			
Telegr. Status Zone B	→	EIB-Input Panel Zone 1 B	→	≥1	Zone	
Telegr. Status Zone C	→	EIB-Input Panel Zone 1 C	→		Panel Zone 1	
Telegr. Status Zone D	→	EIB-Input Panel Zone 1 D	→			
Set/Unset Request	←	Extern or Intern Set				
Reset Zones A...D	←	Reset				
Supply Voltage Fault	→	EIB-Tamper Input 1	→ 🕐 →		Panel Tamper	

Zone Terminal MT/S 4.12.1   EIB-Interface   Intrusion Alarm Panel

3.9 Parameter Window: EIB-Tamper 1 – 4 and 5 – 8

Via the parameter windows „EIB-Sabotage 1 – 4 and 5 – 8", it is possible to enable EIB-Tamper input communication objects.

This function allows important tamper signals from the EIB installation to be centrally administrated in the intrusion alarm panel. Among other possibilities, this allows tamper monitoring of the EIB Bus and the connected devices, e.g., the Zone Terminal MT/S 4.12.1.
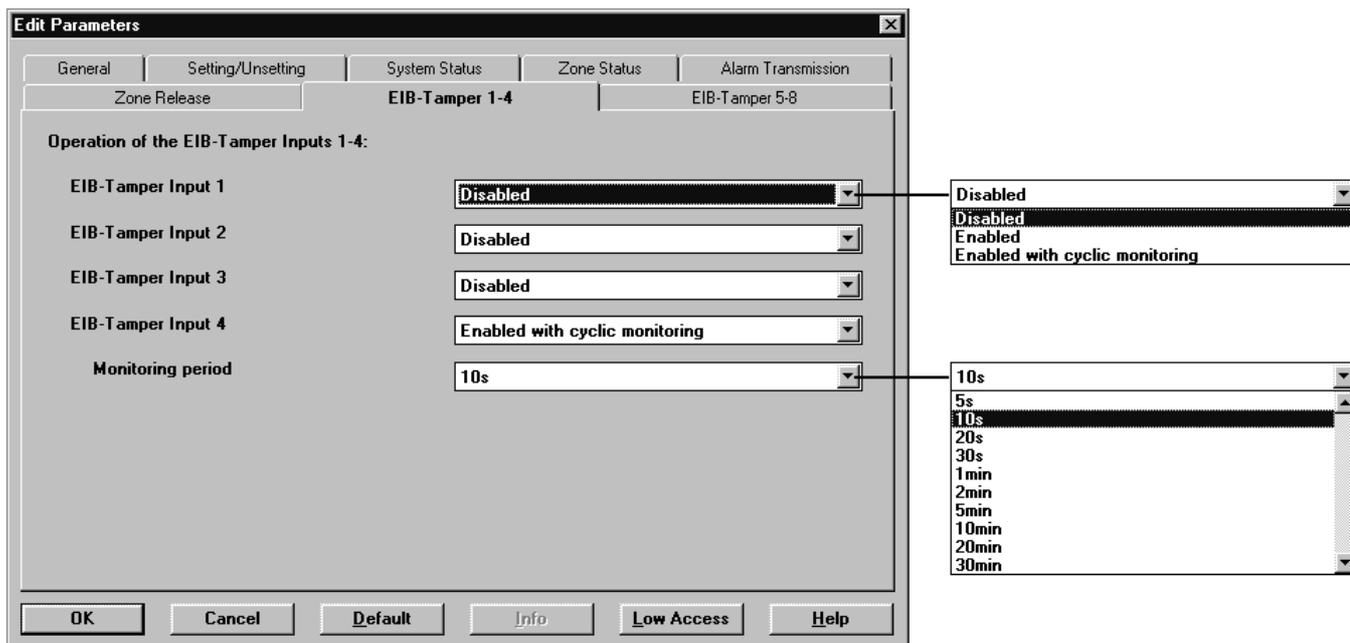
Disabled: This setting prevents tamper faults from being transmitted from the EIB to the intrusion alarm panel.
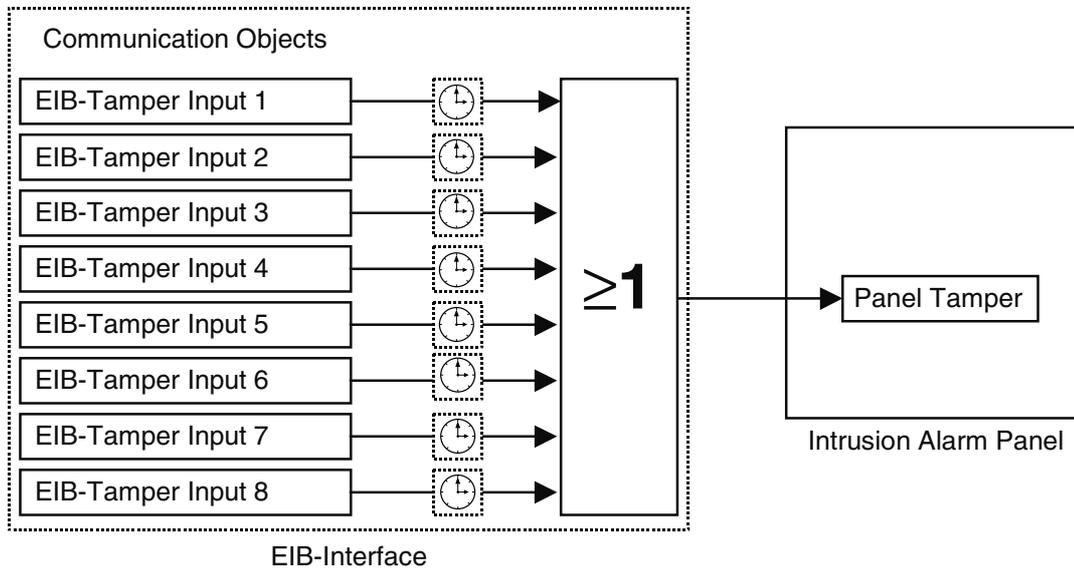
Enabled: This setting causes an EIB-Tamper input communication object to be made available. Should one or more of the eight communication objects receive a telegram with the value „1", a tamper alarm is generated in the intrusion alarm panel. The eight communication objects are linked in a logical OR function (see schematic on following page).
The following applies for all EIB-Tamper communication objects:
Telegram value „1": Tamper fault
„0": no tamper

Enabled with cyclic monitoring: This setting allows EIB input communication objects to be made available that not only react to the value of the received EIB telegrams but also monitor the interval between the received telegrams. If a cyclically sending EIB bus device is isolated from the bus cable or the bus cable is cut, the telegram interchange between this device and the EIB-Interface is interrupted and a tamper alarm is generated. With the parameter „Monitoring period", it is possible to define the maximum permitted interval between two telegrams without a tamper alarm being generated. The monitoring period can be set individually for each communication object.

Important: The cyclic sending interval of the security devices should be set to approximately half the value of the monitoring period of the EIB-Tamper input of the EIB-Interface in order to prevent unwanted tamper alarms.
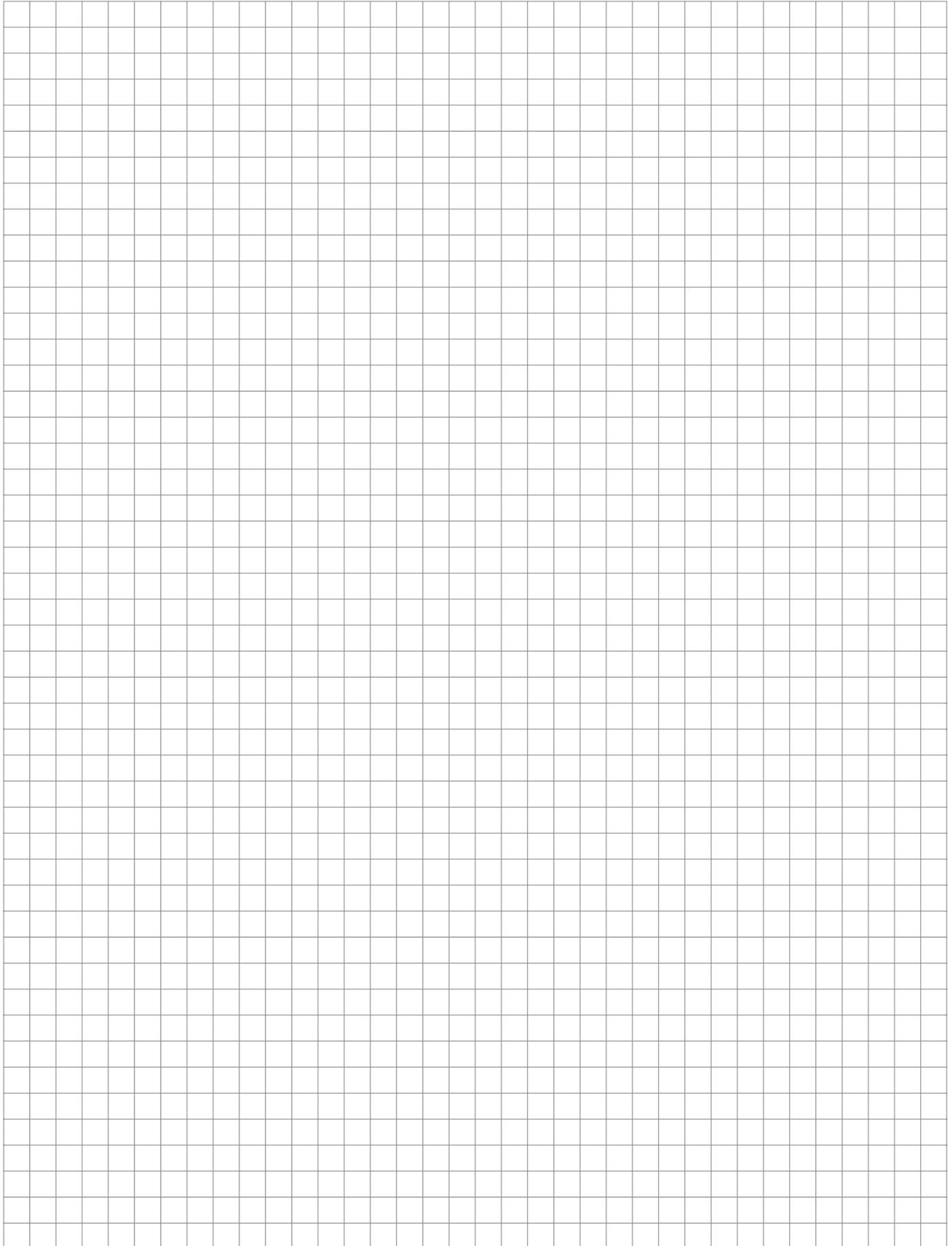

EIB-Interface

Notes

ABB