PRODUCT MANUAL

ABB i-bus® KNX

LK/S 4.3

Line Coupler Secure

Table of contents

1 About this document

1.1 Using the product manual

This manual provides detailed technical information on the function, installation and programming of the ABB i-bus® KNX device.

1.2 Legal disclaimer

ABB AG reserves the right to make changes to the product or modify the contents of this document without prior notice.

The agreed properties are definitive for any orders placed. ABB AG does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

ABB AG reserves all rights in this document and in the subject matter and illustrations contained therein. Reproduction, transfer to third parties or processing of the content – including sections thereof – is not permitted without the prior written consent of ABB AG.

1.3 Explanation of symbols

1. 2. ⇨	Instructions in specified sequence and result
▶	Individual actions
a)	Priorities
1)	Processes run by the device in a specific sequence
•	List level 2
–	List level 2

Tab. 1: Explanation of symbols

Notes and warnings are represented as follows in this manual:

DANGER
This symbol is a warning about electrical voltage and indicates high-risk hazards that will definitely result in death or serious injury unless avoided.

DANGER
Indicates high-risk hazards that will definitely result in death or serious injury unless avoided.

WARNING
Indicates medium-risk hazards that could result in death or serious injury unless avoided.

CAUTION
Indicates low-risk hazards that could result in slight or moderate injury unless avoided.

CAUTION
Indicates a risk of malfunctions or damage to property and equipment, but with no risk to life and limb.

Example
For use in application, installation and programming examples

Note
For use in tips on use and operation

1.4 2D code

The packaging and the device are labeled with a 2D code. These codes are used for unique identification of the device and include the following information:

- Link to the product page
- Order number
- ABB device serial number

The 2D codes can be read using any mobile device with an appropriate 2D code reader.

By scanning the 2D codes with the ABB Product Scanner, you can open additional digital services.

2 Safety

2.1 General safety instructions

- Protect the device from moisture, dirt and damage during transport, storage and operation.
- Operate the device only in a closed housing (distribution board).
- Operate the device only within the specified technical data.
- Mounting, installation, commissioning and maintenance must be carried out only by qualified electricians.
- Disconnect device from the supply of electrical power before mounting.

2.2 Qualification of the specialist personnel

Programming the device requires detailed specialist knowledge – particularly about the ETS commissioning software – through KNX training courses.

2.3 Proper use

Device type LK/S 4.3 is intended to be used for data connection and galvanic isolation of two KNX lines in a KNX environment.

3 Product overview

3.1 Device description

The devices are modular installation devices (MDRC) in pro*M* design. They are designed for installation in electrical distribution boards and small housings with a 35 mm mounting rail (according to EN 60715).

The devices are KNX-certified and can be used as products in a KNX system
→ EU declaration of conformity.

The devices are powered via the KNX bus connection of the main line (1 = Main Line) and require no additional auxiliary voltage.

The connection to the bus (ABB i-bus® KNX) is made via two KNX bus connection terminals on the front of the housing.

The software application Engineering Tool Software (ETS) is used for physical address assignment and parameterization.

3.2 Product name description

The table below lists the product name descriptions of all devices in the product family.

Abbreviation	Description		
LK	Line coupler		
/S	MDRC		
x.	4	=	Hardware version
x	x	=	Version number (x = 1, 2, etc.)

Tab. 2: Product name description

3.3 Ordering details

Description	MB	Type	Order no.	Packaging unit [pcs.]	Weight (incl. packaging) [kg]
Line coupler	2	LK/S 4.3	2CDG110310R0011	1	0.10

Tab. 3: Ordering details

3.4 Connections

The devices have the following connections:

- 2 KNX bus connections

3.4.1 Inputs

Note
This section is not relevant for these devices.

3.4.2 Outputs

Note
This section is not relevant for these devices.

3.5 Product family

The product family described in this document includes the following devices:

Device type	Name	Features
LK/S 4.3	Line coupler	MDRC

Tab. 4: Product family

3.5.1 Dimension drawing

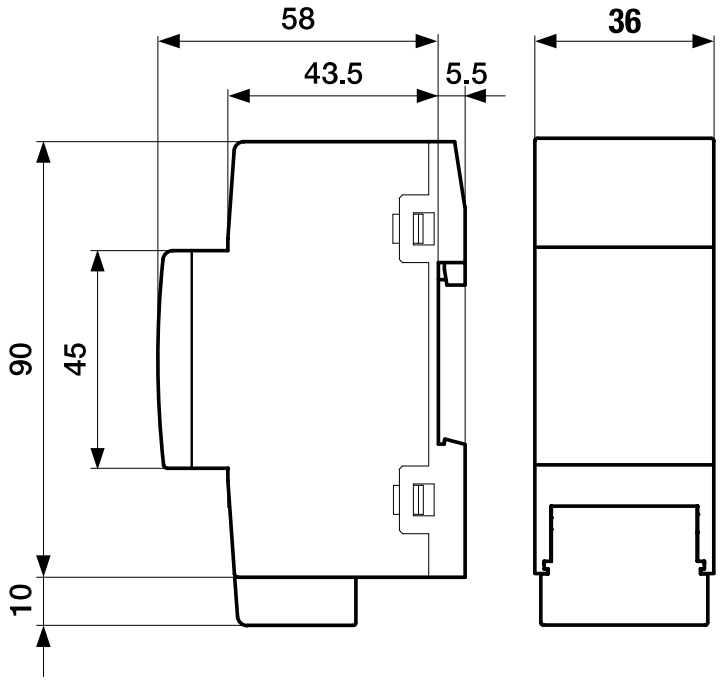


Fig. 1: Dimension drawing

2CDC072011F0015

3.5.2 Connection diagram

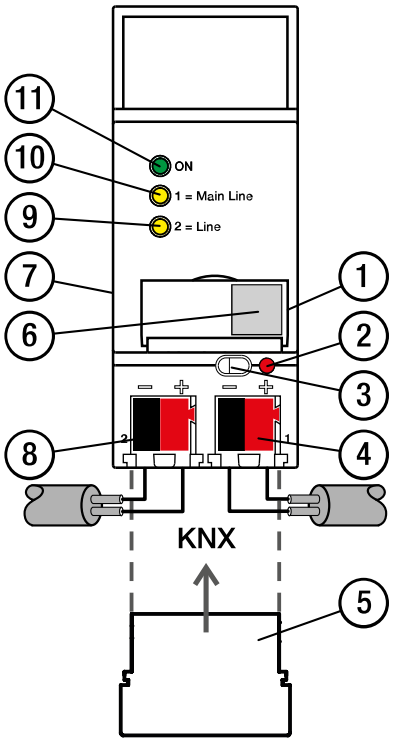


Fig. 2: LK/S 4.3 connection diagram

9AKK108464A0852

—

Legend

1 label carrier
2 *Programming* LED
3 *Programming* button
4 KNX bus connection terminal, main line
5 Cover cap
6 2D code (below label carrier)
7 Device certificate/Identification label (on the side)
8 KNX bus connection terminal, subline
9 *Line* LED (subline)
10 *Main Line* LED (main line)
11 *ON* LED

3.5.3 Operating and display elements

Note
The operating and display elements are shown with variables in the following tables for illustrative purposes only. All elements of the same type function in exactly the same way.

Operating control/LED	Description/function	Display
 *Programming* button/LED	Assignment of the physical address	LED on: Device in programming mode

Tab. 5: Operating and display elements

3.5.3.1 Manual mode

Note
This section is not relevant for these devices.

3.5.3.2 KNX operation

Operating control/LED	Description/function	Display
ON LED		LED on: Device ready for operation LED off: Device not ready for operation
Main Line LED		LED on: Main line connected LED off: Main line not connected or KNX voltage failure on main line LED flashing: Telegram traffic on main line
Line LED		LED on: Device ready for operation, main line and subline connected LED off: Main line and subline not connected LED flashing: Telegram traffic on subline

Tab. 6: Operating and display elements

3.5.4 Technical data

3.5.4.1 General technical data

		LK/S 4.3
Device	Dimensions	90 × 36 × 64.5 mm (H x W x D)
	Mounting width in space units	2 modules, 18.0 mm each
	Weight	0.074 kg
	Mounting position	Any
	Mounting variant	35 mm mounting rail
	Design	proM
	Degree of protection	IP 20
	Protection class	III
	Overvoltage category	III
	Overload protection	Yes
	Reverse voltage protection	Yes
	Short-circuit proof	Yes
	Pollution degree	2
Materials	Housing	Polycarbonate, Makrolon FR6002, halogen free
Material note	Fire classification	Flammability V-0
Electronics	Rated voltage, bus	30 V DC
	Voltage range, bus	21 … 31 V DC
	Current consumption, bus (main line)	< 5 mA
	Current consumption, bus (subline)	< 3 mA
	Power loss, device	≤ 0.25 W
	KNX safety extra low voltage	SELV
Connections	Connection type, KNX bus	Plug-in terminal
	Cable diameter, KNX bus	0.6 … 0.8 mm, solid
	Pitch	6.35 mm
	Stripping length for KNX terminal	6 mm
Certificates and declarations	CE declaration of conformity	→ 9AKK108469A3392
Ambient condition	Operation	−5 … +45 °C
	Transport	−25 … +70 °C
	Storage	−25 … +55 °C
	Humidity	≤ 95 %
	Condensation allowed	No
	Atmospheric pressure	≥ 80 kPa (corresponds to air pressure at 2,000 m above sea level)

4 Functional overview

4.1 Device functions

The LK/S 4.3 is used to provide a data connection and galvanic isolation between two KNX lines (main line and subline). The LK/S 4.3 complies with the KNX-Data-Secure-Standard → KNX Secure, Page 36.

- The LK/S 4.3 acts as a coupler with or without a filter filter table. The filter table is created automatically by ETS.
- The Secure Proxy encrypts or decrypts the telegrams with group addresses in both directions between secure and non-secure communication.
- Unauthorized access to a device via the Secure Proxy is prevented.

The device function is determined by the physical address (→ Assignment of the physical address, Page 22), the settings in the device application and how the device is used in ETS (KNX Plain/KNX Secure).

The device application for the LK/S 4.2. can be loaded onto the LK/S 4.3 so that its functionality (e.g. as a line repeater) is still guaranteed in ETS 4 or 5. The following tables provide an overview of which device functions can be implemented with the related device applications and ETS versions:

Device application LK/S 4.2	ETS 4	ETS 5	ETS 6
Line or area coupler	x	x	x
Line repeater	x	x	x
Segment coupler			
Secure Proxy			

Tab. 7: Device application LK/S 4.2 and ETS versions

Note
If an existing ETS 5 project with a line repeater is loaded into ETS 6, the function as a line repeater is retained in ETS 6.
If the device is assigned to a line in ETS 6 using the LK/S 4.2 device application, ETS automatically creates a segment. This segment has no function in this situation. If the device is parameterized as a line repeater, the device continues to operate as a line repeater.

Device application LK/S 4.3	ETS 4	ETS 5	ETS 6
Line or area coupler			x
Line repeater			
Segment coupler			x
Secure Proxy			x

Tab. 8: Device application LK/S 4.3 and ETS versions

Note
If the LK/S 4.3 is used as a line repeater in an ETS 4 or 5 project, the LK/S 4.2 device application must be used.
LK/S 4.3 supports both device applications. Before using the LK/S 4.2 device application, the device must be reset to factory settings to delete any existing secure settings and filter tables, → Unloading device or resetting to factory settings (Master-Reset), Page 23.

4.1.1 Line or area coupler

As an area coupler (address range x.0.0), the LK/S 4.3 connects the area line (terminal 1) to a main line (terminal 2). Area couplers are typically used in extensive KNX systems.

As a line coupler (address range x.x.0), the LK/S 4.3 connects the main line (terminal 1) to a subline (terminal 2).

As a line or area coupler, the LK/S 4.3 filters all telegrams on the bus (ABB i-bus® KNX) according to the settings in ETS. The filter tables are created automatically by ETS. The routing settings for different telegram types can be specified separately in the parameters.

If a telegram has a transmission error or the acknowledgment is not received, the behavior can be specified separately for both lines.

As a line or area coupler, the LK/S 4.3 can act as a Secure Proxy. The Secure Proxy translates the telegrams with group addresses in both directions between secure and non-secure communication. This means that KNX Plain and KNX Data Secure devices can be combined with each other while maintaining the maximum possible security.

Note
Each line and each line segment requires a dedicated power supply.

4.1.2 Segment coupler

As a segment coupler, the LK/S 4.3 connects the primary line segment (terminal 1) in a KNX line to a secondary line segment (terminal 2) to form a logical function area and ensures galvanic isolation between the two segments.

Segment couplers can be used to split an area line, main line or subline into segments. Segmenting the system makes it easier to expand and scale the KNX system without degrading performance. For example, a segment coupler could be installed in each hotel room. The number of segment couplers in a line is specified by ETS.

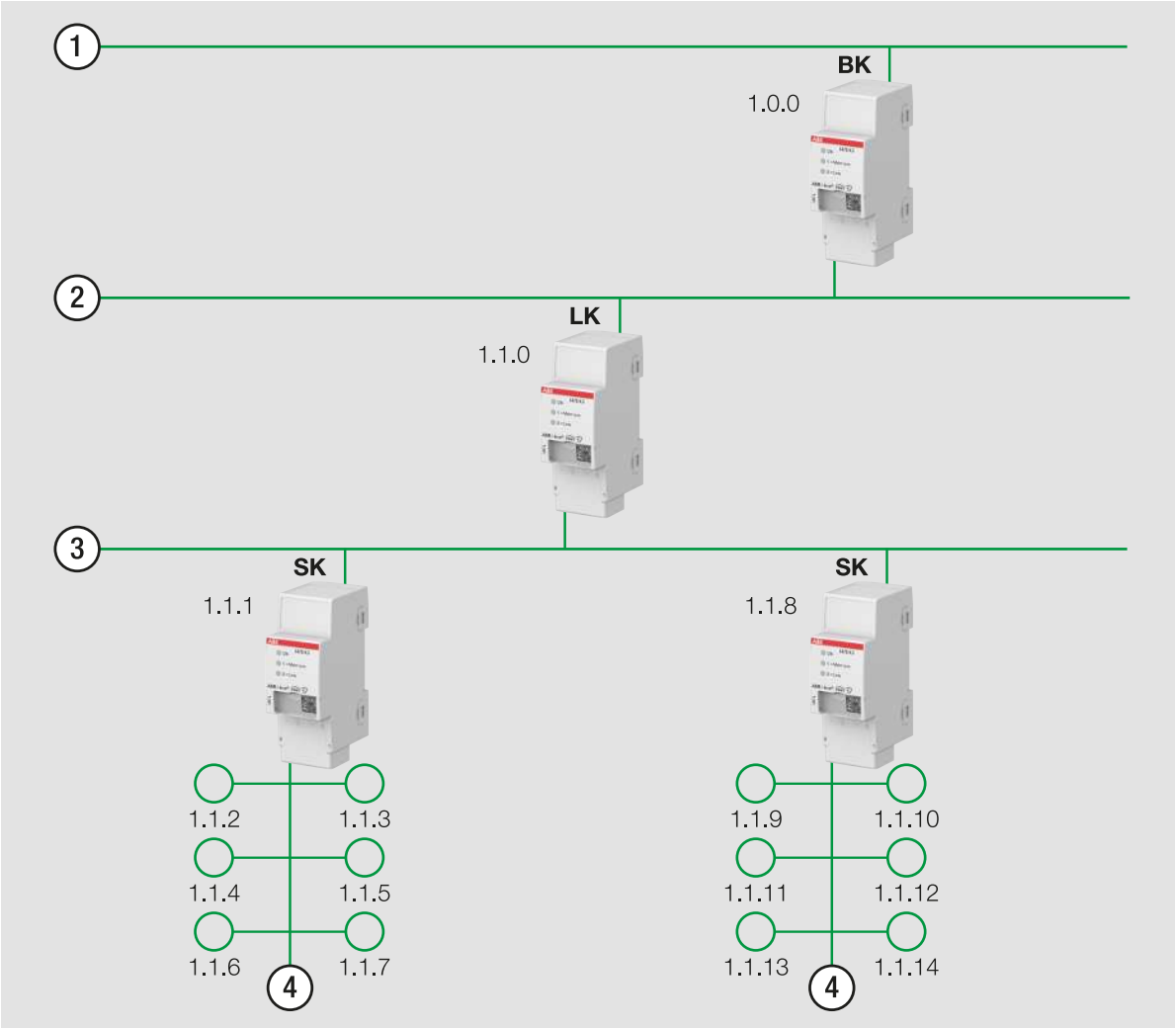


Fig. 3: Example project topology

1	KNX TP area line
2	KNX TP main line
3	KNX TP line
4	KNX TP segment
BK	Area coupler
LK	Line coupler
SK	Segment coupler

Tab. 9: Legend

For ETS to recognize a device as a segment coupler, segments must be specified in the ETS Topology view. The segment coupler must be assigned a physical address between x.x.1 and x.x.255 according to the topology in the KNX installation.

Fig. 4: Project topology in ETS

The device function is determined by the physical address (→ Assignment of the physical address, Page 22), the settings in the device application and how the device is used in ETS (KNX Plain/KNX Secure).

Segment couplers use filter tables to control telegrams between different segments. The filter table is displayed in ETS after clicking the device using the right mouse button and selecting "Preview Filter Table" on the context menu. The filter tables are created automatically by ETS.

As a segment coupler, the LK/S 4.3 can act as a Secure Proxy. The Secure Proxy translates the telegrams with group addresses in both directions between secure and non-secure communication. This means that KNX Plain and KNX Secure devices can be combined with each other while maintaining the maximum possible security.

Note
Each line and each line segment requires a dedicated power supply.

4.1.3 Secure Proxy

The Secure Proxy is a coupler or IP router function specified in the KNX standard. A Secure Proxy permits the combination of KNX Plain and KNX Secure products while maintaining the maximum possible security.

The Secure Proxy can operate in the LK/S 4.3 in area, line or segment couplers. The Secure Proxy encrypts or decrypts the telegrams with group addresses in both directions between secure and non-secure communication. Depending on the topology, ETS ensures that telegrams remain encrypted for as long and as far as possible to guarantee maximum security.

The Secure Proxy is configured fully automatically via ETS. A Secure Proxy requires at least one KNX Secure device in the installation.

In ETS version 6.1.1 or later, the coupler must be commissioned using the Secure device certificate. ETS detects the suitability of the coupler as a Secure Proxy and enters the group addresses to be translated in the Secure Proxy table for the coupler. The devices in the ETS project must be placed topologically in the correct position.

The Secure Proxy table and the group address filter table are updated automatically while the coupler application is loaded. The Secure Proxy table is displayed in ETS after clicking the device using the right mouse button and selecting "Preview Filter Table" on the context menu.

More information → ABB documentation "KNX Secure"

5 Mounting and installation

5.1 Information about mounting

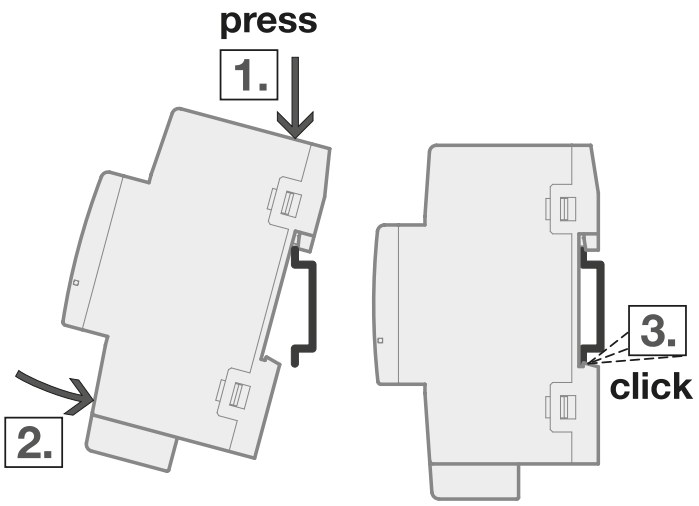
The device can be mounted in any position as required on a 35 mm mounting rail.

The connection to the bus (ABB i-bus® KNX) is made using the KNX bus connection terminals supplied.

Note
The maximum permissible current consumption on a KNX line must not be exceeded.
- During planning and installation, ensure that the KNX line is correctly dimensioned. The device has a maximum current consumption of 5 mA.

5.2 Mounting on mounting rail

Note
No additional tools are required for mounting on a mounting rail.



2CDC072013F0015

Fig. 5: Mounting on mounting rail

1. Place the mounting rail holder on the upper edge of the mounting rail and push down.
2. Push the lower part of the device toward the mounting rail until the mounting rail holder engages.
   ⇨ The device is now mounted on the mounting rail.
3. Relieve the pressure on the top of the housing.

6 Commissioning

6.1 Prerequisites for commissioning

A PC with ETS and a connection to the bus (ABB i-bus® KNX), e.g. via a KNX interface, are required to commission the device.

- Required ETS version: dependent on area of application→ Device functions, Page 15
- Product-specific device application: installed

Note
See software information on the website → www.abb.com/knx.

6.2 Secure commissioning of KNX Secure devices

Note
ETS version 6 or later is required when using KNX Secure. The use of the latest ETS version is recommended. Using older ETS versions can cause errors during project planning, problems during commissioning (e.g. while replacing devices), or while undertaking diagnostics on group addresses and devices.

Note
To program a Data Secure device in secure mode, the interface used (e.g. USB/S 1.2 or IPS/S 3.x.1) must support "Extended/Long Frames".

To commission the device securely, note the following points:

- A project password must be assigned while importing a KNX Secure device into a KNX project. By assigning the project password, the project is protected against unauthorized access.
  - If a password is not assigned, none of the devices in the project can be operated as KNX Secure devices. This means the security of the whole project will be that of a conventional KNX network (KNX Plain).
  - The project password must be kept in a safe place. Access to the project is not possible without it. Not even the KNX Association or ABB AG will be able to access it.
- A device certificate is required while commissioning a KNX Secure device. This device certificate includes the FDSK (Factory Default Setup Key) and the device's KNX serial number.
  - The device certificate is located on two detachable stickers applied to the device. The stickers should be removed from the device and kept in a safe place.
  - When adding the device from the ETS product catalog, a window opens in ETS, prompting the user to enter the device certificate. The device certificate can be entered using a webcam, a barcode scanner or manually.
  - The device certificates of all KNX Secure devices integrated in the project can be entered in advance in ETS, → Properties/Settings/"Add Device Certificate". Because the device certificate contains the FDSK and the KNX serial number of the device, ETS can automatically manage the assignment of the certificates to the correct device during commissioning.
  - If the device certificate was entered in ETS, the physical address of the device can be assigned via the KNX serial number,
    → Properties/Pending Operations/"Use Device Certificate".
  - The device certificate is only required for initial encryption and authentication of communication between KNX Secure devices and ETS. As it is read, the device certificate is resolved into the FDSK and KNX serial number.
  - During commissioning, ETS assigns a device key (Tool Key) to the device. The device certificate will be required again only if the device is reset to its factory settings (e.g. if the device is to be used as a KNX Secure device in a different system with a different ETS project).

6.2.1 Device certificate

The device certificate is located on two detachable stickers applied to the device. Each sticker contains the following information:
- Device certificate as QR code
- Device certificate as a 36-character combination of numbers and letters

The device certificate is required for securely commissioning the device in a KNX Secure project and contains the following information:
- KNX serial number of the device
- FDSK (Factory Default Setup Key)

For secure commissioning of the device, the device certificate must be entered in ETS (scan the QR code or enter the combination of numbers and letters directly, → Properties/Settings/"Add Device Certificate").

6.3 Commissioning overview

The following factory settings are configured in the state as supplied:
- Physical address of the device: 15.15.0
- Device application: preloaded
- All group addresses are routed
- Physical addresses are filtered
- Broadcast telegrams are routed
- The device functions as a line coupler

The device can be programmed only using ETS.

ⓘ Note
If access to the devices in the project is blocked by a BCU Key, this situation has no effect on this device. Data can still be read and programmed in this device.

6.4 Putting the device into operation

ⓘ Note
The device is supplied with power via the KNX bus connection of the main line (terminal 1).

1. Connect the device to the bus (ABB i-bus® KNX).
2. Switch on KNX voltage.
   ⇨ *Programming* LED lights up 1 s.

⇨ *ON* LED lights up green continuously, device is ready for operation.

6.5 Assignment of the physical address

ⓘ Note
The device function is determined by the physical address assigned to the devices in ETS. The physical address must match the logical topology of the KNX system.
- An area coupler is logically assigned to the subordinate area and is within the address range x.0.0 (x = 1 … 15).
- A line coupler is logically assigned to the subordinate line and is within the address range x.x.0. (x = 1 … 15)
- A segment coupler is within the address range x.x.1 … x.x.255. For ETS to recognize this as a segment coupler, segments must be set up in ETS.

Triggering assignment of the physical address via ETS:

1. Press the *Programming* button.
   ⇨ Programming mode active. The *Programming* LED lights up.
2. Start programming process in ETS.

⇨ Physical address is assigned. Device restarts. All states are reset.

Note
If a KNX Secure device was securely commissioned, the KNX serial number of the device can be used to assign the physical address, → Secure commissioning of KNX Secure devices, Page 21.

6.6 Software/device application

6.6.1 Device applications

The following device applications are available for the devices described in this document:

Device type	Device application
LK/S 4.3	Line/Area/Segment Coupler Secure/…
LK/S 4.2	Couple Repeat/…

Tab. 10: Device applications

Note
… = current version number of the application.
See software information on the website, → www.abb.com/knx.

6.7 Unloading device or resetting to factory settings (Master-Reset)

6.7.1 Resetting device to factory settings using the Programming button

1. Disconnect the device from the bus (ABB i-bus® KNX, terminal 1).
2. Wait 10 seconds, then press and hold the *Programming* button.
3. Connect the device to the bus (ABB i-bus® KNX, terminal 1).
   ⇨ *Programming* LED flashes at 2 Hz.
4. Keep *Programming* button pressed for at least 5 s, then release.

⇨ Device executes a Master-Reset; *Programming* LED is off.

⇨ Settings are reset to factory settings.

⇨ The last application version loaded is retained.

⇨ The firmware version is retained.

⇨ The device key (Tool Key) assigned by ETS is reset on the FDSK. The device certificate is required for recommissioning if it is not still available in the ETS project from the original commissioning.

⇨ The filter table is reset.

⇨ All Secure Proxy settings are reset.

⇨ All segment coupler settings are reset.

6.7.2 Unloading device via ETS

Note
A KNX Secure device can only be unloaded via ETS if the device certificate has been entered in the project and ETS has assigned a device key (Tool Key).

Unloading application

- The physical address is retained.
- The last application version loaded is set to FF (invalid).
- The device key assigned by ETS (Tool Key) is retained. The device certificate is not required for reprogramming.
- The Secure Proxy table is reset.
- The segment coupler filter table is reset, the function as a segment coupler is retained.

Unloading physical address and application

- Settings are reset to factory settings.
- The last application version loaded is set to FF (invalid).
- The firmware version is retained.
- The device key (Tool Key) assigned by ETS is reset. The device certificate is required for recommissioning if it is not still available in the ETS project from the original commissioning.
- The filter table is reset.
- All Secure Proxy settings are reset.
- All segment coupler settings are reset.

7 Parameters

7.1 General

Note
ETS (Engineering Tool Software) is used to parameterize the device.

The following sections describe the device parameters based on the parameter windows. The parameter windows have a dynamic design. Parameters are shown or hidden depending on parameterization and function.

The default values for the parameters are underlined, e.g.:
no (checkbox cleared)
yes (checkbox ticked)

Note
The default values in the device application can vary from the values stated in the product manual depending on the product variant.

Note
The largest and most extensive device in the product family is described below as an example.

7.1.1 Prerequisites for visibility

In the "Prerequisites for visibility" the ETS settings and product variants necessary to display a parameter window/parameter/Group Object are listed. If no "Prerequisites for visibility" are specified, parameter windows/parameters/Group Objects are always shown or the prerequisites are given by the higher-level parameter window.

The "Prerequisites for visibility" are structured as follows:
- Parameter windows: all necessary prerequisites
- Parameters: Settings in other parameter windows, higher-level parameters, product variant required
- Group Objects: all necessary prerequisites

7.2 Parameter windows

7.2.1 Parameter windows Main line > Line

The following settings can be made in this parameter window:

- Specification of telegram routing settings from the main line to the line

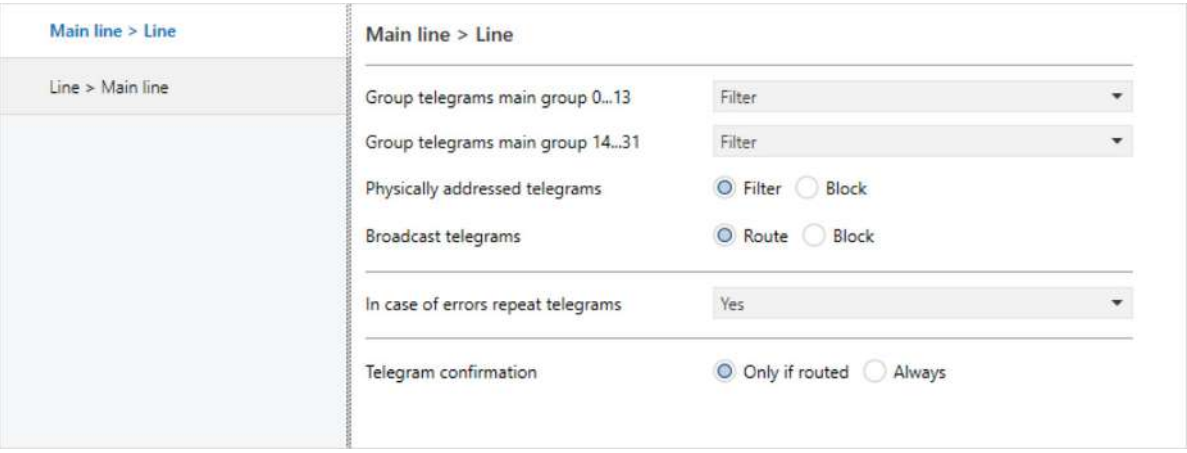


Fig. 6: Main line > Line parameter window

This parameter window includes the following parameters:

→ Group telegrams main group 0 … 13, Page 26
→ Group telegrams main group 14 … 31, Page 26
→ Physically addressed telegrams, Page 27
→ Broadcast telegrams, Page 27
→ In case of errors repeat telegrams, Page 27
  → Repeat group addressed telegrams, Page 28
  → Repeat physically addressed telegrams, Page 28
  → Repeat broadcast telegrams, Page 28
→ Telegram confirmation, Page 28

7.2.1.1 Group telegrams main group 0 … 13

This parameter is used to specify the routing settings for group-addressed telegrams.

Option	
Filter	Only telegrams with group addresses entered in the filter table are routed. The filter table is created automatically by ETS.
Route	All telegrams of this telegram type are routed.
Block	All telegrams of this telegram type are blocked.

7.2.1.2 Group telegrams main group 14 … 31

This parameter is used to specify the routing settings for group-addressed telegrams.

Option	
Filter	Only telegrams with group addresses entered in the filter table are routed. The filter table is created automatically by ETS.
Route	All telegrams of this telegram type are routed.
Block	All telegrams of this telegram type are blocked.

7.2.1.3 Physically addressed telegrams

This parameter is used to specify the routing settings for physically addressed telegrams.

Physically addressed telegrams are used to download and diagnose KNX devices. The *Block* option can be selected to block access to KNX devices via the coupler.

Note
If the routing of physically addressed telegrams is blocked, devices on the line cannot be accessed via the bus (ABB i-bus® KNX).
With this setting, devices cannot be programmed using ETS. It is not possible to establish a connection via i-bus® Tool.
If a point-to-point connection is required for special applications (e.g. monitoring via the EUB/S monitoring module), this parameter must be set to "filter".

Option	
Filter	Only telegrams with destination addresses within the range of the physical address of the device are routed.
Block	All telegrams of this telegram type are blocked.

7.2.1.4 Broadcast telegrams

This parameter is used to specify the routing settings for broadcast telegrams.

Note
If the routing of broadcast telegrams is blocked, it is not possible to assign the physical address for the devices on the line.

Option	
Route	All telegrams of this telegram type are routed.
Block	All telegrams of this telegram type are blocked.

7.2.1.5 In case of errors repeat telegrams

This parameter is used to specify whether telegrams are sent again if transmission errors occur.

Option	
No	If a transmission error occurs, all telegrams are not sent again, independent of the telegram type.
Yes	If a transmission error occurs, all telegrams are sent again up to three times, independent of the telegram type.
User-defined	The behavior if transmission errors occur can be set separately for each telegram type. The following dependent parameters are shown: • *Repeat group addressed telegrams* • *Repeat physically addressed telegrams* • *Repeat broadcast telegrams*

7.2.1.6 Repeat group addressed telegrams

This parameter is used to specify whether group-addressed telegrams are sent again if transmission errors occur.

Option	
No	If a transmission error occurs, all telegrams of this telegram type are not sent again.
Yes	If a transmission error occurs, all telegrams of this telegram type are sent again up to three times.

Prerequisites for visibility

- Parameter window *Main line > Line* \ Parameter *In case of errors repeat telegrams* \ Option *User-defined*

7.2.1.7 Repeat physically addressed telegrams

This parameter is used to specify whether physically addressed telegrams are sent again if transmission errors occur.

Option	
No	If a transmission error occurs, all telegrams of this telegram type are not sent again.
Yes	If a transmission error occurs, all telegrams of this telegram type are sent again up to three times.

Prerequisites for visibility

- Parameter window *Main line > Line* \ Parameter *In case of errors repeat telegrams* \ Option *User-defined*

7.2.1.8 Repeat broadcast telegrams

This parameter is used to specify whether broadcast telegrams are sent again if transmission errors occur.

Option	
No	If a transmission error occurs, all telegrams of this telegram type are not sent again.
Yes	If a transmission error occurs, all telegrams of this telegram type are sent again up to three times.

Prerequisites for visibility

- Parameter window *Main line > Line* \ Parameter *In case of errors repeat telegrams* \ Option *User-defined*

7.2.1.9 Telegram confirmation

This parameter is used to specify telegram confirmation. The parameter is used to prevent repetitions that would have to be sent by other devices if there is no other interested party for this telegram.

Option	
Only if routed	Only routed telegrams are confirmed.
Always	All telegrams are confirmed.

7.2.2 Parameter windows Line > Main line

The following settings can be made in this parameter window:

- Specification of telegram routing settings from the line to the main line

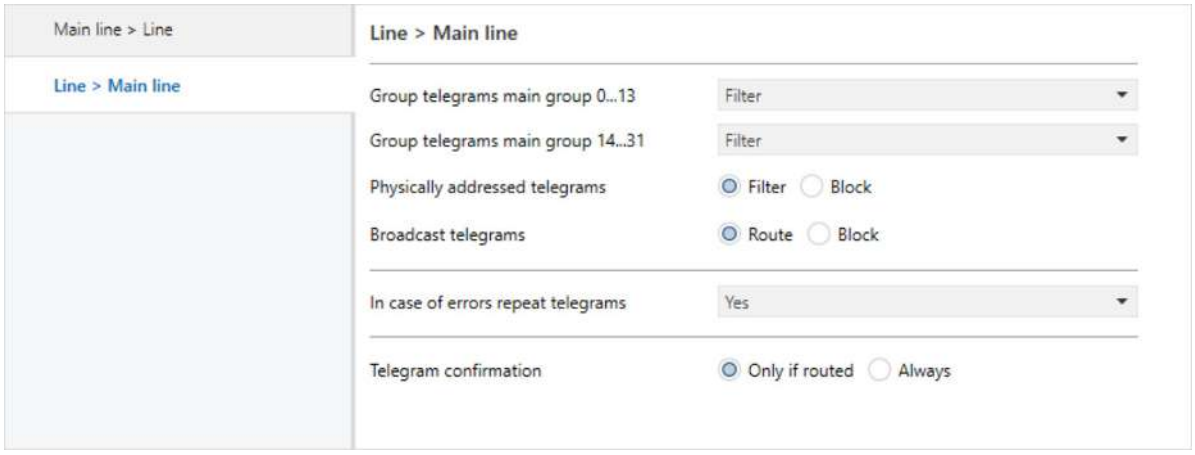


Fig. 7: Line > Main line parameter window

This parameter window includes the following parameters:

→ Group telegrams main group 0 … 13, Page 29
→ Group telegrams main group 14 … 31, Page 29
→ Physically addressed telegrams, Page 30
→ Broadcast telegrams, Page 30
→ In case of errors repeat telegrams, Page 30
  → Repeat group addressed telegrams, Page 31
  → Repeat physically addressed telegrams, Page 31
  → Repeat broadcast telegrams, Page 31
→ Telegram confirmation, Page 31

7.2.2.1 Group telegrams main group 0 … 13

This parameter is used to specify the routing settings for group-addressed telegrams.

Option	
Filter	Only telegrams with group addresses entered in the filter table are routed. The filter table is created automatically by ETS.
Route	All telegrams of this telegram type are routed.
Block	All telegrams of this telegram type are blocked.

7.2.2.2 Group telegrams main group 14 … 31

This parameter is used to specify the routing settings for group-addressed telegrams.

Option	
Filter	Only telegrams with group addresses entered in the filter table are routed. The filter table is created automatically by ETS.
Route	All telegrams of this telegram type are routed.
Block	All telegrams of this telegram type are blocked.

7.2.2.3 Physically addressed telegrams

This parameter is used to specify the routing settings for physically addressed telegrams.

Physically addressed telegrams are used to download and diagnose KNX devices. The *Block* option can be selected to block access to KNX devices via the coupler.

Note
If the routing of physically addressed telegrams is blocked, devices on the line cannot be accessed via the bus (ABB i-bus® KNX).
With this setting, devices cannot be programmed using ETS. It is not possible to establish a connection via i-bus® Tool.
If a point-to-point connection is required for special applications (e.g. monitoring via the EUB/S monitoring module), this parameter must be set to "filter".

Option	
Filter	Only telegrams with destination addresses within the range of the physical address of the device are routed.
Block	All telegrams of this telegram type are blocked.

7.2.2.4 Broadcast telegrams

This parameter is used to specify the routing settings for broadcast telegrams.

Note
If the routing of broadcast telegrams is blocked, it is not possible to assign the physical address for the devices on the line.

Option	
Route	All telegrams of this telegram type are routed.
Block	All telegrams of this telegram type are blocked.

7.2.2.5 In case of errors repeat telegrams

This parameter is used to specify whether telegrams are sent again if transmission errors occur.

Option	
No	If a transmission error occurs, all telegrams are not sent again, independent of the telegram type.
Yes	If a transmission error occurs, all telegrams are sent again up to three times, independent of the telegram type.
User-defined	The behavior if transmission errors occur can be set separately for each telegram type. The following dependent parameters are shown: • *Repeat group addressed telegrams* • *Repeat physically addressed telegrams* • *Repeat broadcast telegrams*

7.2.2.6 Repeat group addressed telegrams

This parameter is used to specify whether group-addressed telegrams are sent again if transmission errors occur.

Option	
No	If a transmission error occurs, all telegrams of this telegram type are not sent again.
Yes	If a transmission error occurs, all telegrams of this telegram type are sent again up to three times.

Prerequisites for visibility

- Parameter window *Line > Main line* \ Parameter *In case of errors repeat telegrams* \ Option *User-defined*

7.2.2.7 Repeat physically addressed telegrams

This parameter is used to specify whether physically addressed telegrams are sent again if transmission errors occur.

Option	
No	If a transmission error occurs, all telegrams of this telegram type are not sent again.
Yes	If a transmission error occurs, all telegrams of this telegram type are sent again up to three times.

Prerequisites for visibility

- Parameter window *Line > Main line* \ Parameter *In case of errors repeat telegrams* \ Option *User-defined*

7.2.2.8 Repeat broadcast telegrams

This parameter is used to specify whether broadcast telegrams are sent again if transmission errors occur.

Option	
No	If a transmission error occurs, all telegrams of this telegram type are not sent again.
Yes	If a transmission error occurs, all telegrams of this telegram type are sent again up to three times.

Prerequisites for visibility

- Parameter window *Line > Main line* \ Parameter *In case of errors repeat telegrams* \ Option *User-defined*

7.2.2.9 Telegram confirmation

This parameter is used to specify telegram confirmation. The parameter is used to prevent repetitions that would have to be sent by other devices if there is no other interested party for this telegram.

Option	
Only if routed	Only routed telegrams are confirmed.
Always	All telegrams are confirmed.

8 Group Objects

Note
This section is not relevant for these devices.

9 Operation

Note
The devices cannot be operated manually.

10 Maintenance and cleaning

10.1 Service

The devices are maintenance-free if used properly. In the event of damage, e.g. during transport and/or storage, repairs are not allowed to be carried out.

10.2 Cleaning

1. Disconnect devices from the electrical power supply before cleaning.
2. Clean dirty devices using a dry cloth or a slightly damp cloth.

11 Removal and disposal

11.1 Removal

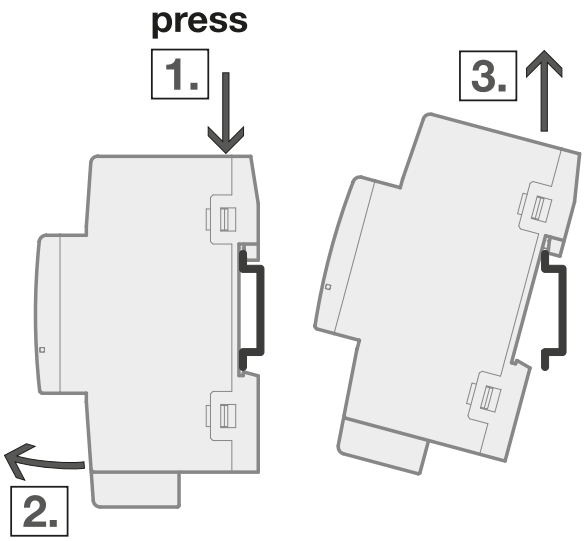


Fig. 8: Removing from the mounting rail

2CDC072012F0015

1. Press on the top of the device.
2. Release the bottom of the device from the mounting rail.
3. Lift the device up and off the mounting rail.

11.2 Environment

Consider environmental protection.

Electrical and electronic devices must not be disposed of as domestic waste.

The device contains valuable resources that can be recycled. Therefore, please take the device to a suitable recycling center. All packaging materials and devices are provided with markings and test seals for proper disposal. Always dispose of packaging material and electrical devices or their components at collection points or disposal companies authorized for this purpose. The products comply with the statutory requirements, particularly the law on electrical and electronic equipment and the REACH regulation. (EU directive 2012/19/EU WEEE and 2011/65/EU RoHS) (EU REACH regulation and the law implementing the regulation (EC) no.1907/2006)

12 Planning and application

12.1 Basic knowledge

12.1.1 KNX Secure

Note
ETS version 6 or later is required when using KNX Secure. The use of the latest ETS version is recommended. Using older ETS versions can cause errors during project planning, problems during commissioning (e.g. while replacing devices), or while undertaking diagnostics on group addresses and devices.

KNX Secure is an encryption technology that guarantees data protection in a KNX twisted pair network. KNX Secure is based on end-to-end encryption that ensures all data exchanged between KNX devices are encrypted and can only be read by authorized users.

In conventional KNX networks (colloquially termed "KNX Plain"), data are sent unencrypted on the bus. The data could be read by anyone with access to the bus and can be intercepted or falsified by unauthorized individuals.

Using KNX Secure protects transmitted data against unauthorized access, ensures data integrity and minimizes potential security risks. KNX Secure helps to increase security and privacy in KNX-based smart home or building automation systems. KNX devices that only support KNX Plain can be used in the same installation with the aid of a suitable coupler.

KNX devices that do not support KNX Secure can be connected to KNX devices that support KNX Secure. In this case, the protection provided by KNX Secure is removed. If secure communication is required in certain sections, this communication can be realized via the Secure Proxy, → Secure Proxy, Page 18.

Fig. 9: KNX Secure logo

A KNX Secure product is identifiable by the KNX Secure logo on the packaging or the product. This logo indicates that the product meets the KNX Secure security standard and supports KNX Secure encryption technology.

KNX Secure distinguishes between two types of encrypted KNX telegrams:
- KNX IP Secure can only be used on the KNX IP medium (typically the backbone line) exposed to an external IP network (e.g. the Internet). KNX IP Secure telegrams are fully encrypted.
- KNX Data Secure can be used on any KNX medium, but is only permitted to be used for the part of the KNX installation not exposed to an external IP network (e.g. the Internet). KNX Data Secure telegrams are encrypted.

For more information, see:
→ ABB documentation "KNX Secure"
→ Documentation available at knx.org

12.1.2 Network (cyber) security

The industry is increasingly faced with cyber security risks. To increase the stability, security and robustness of its solutions, ABB has introduced cyber security robustness tests as part of the product development process.

In addition, the sections below include guidelines and mechanisms that you can use to improve the security of KNX systems.

12.1.2.1 Preventing unauthorized access

The basis for any protection concept is the careful shielding of the system against unauthorized access. The following points must be taken into consideration when planning and installing a KNX system:

- Only authorized persons (installers, custodians, users) should be allowed to have physical access to the KNX system.
- Sub-distributions with KNX devices should be closed, or in rooms to which only authorized persons have access.
- If available, use the anti-theft features on the KNX devices.
- All components in a KNX system should be permanently installed and protected from unauthorized access.
- The bus cable (ABB i-bus® KNX) should not be visible inside or outside the building. Cables outdoors are an increased risk. Physical access should be made particularly difficult here.
- Devices installed in areas with limited protection (e.g. outdoor areas, underground parking lots, restrooms, etc.) should be designed using a line coupler as a separate line.
- If possible, KNX DATA Secure should be used for data transmission in KNX networks (→ KNX Secure, Page 36).
- The system should be divided into security segments that are based on the available security functions of the devices used. This is done by using segment couplers.

12.1.2.2 IP cabling inside the building

For building automation, use a separate LAN or WiFi network with its own hardware (routers, switches, etc.). Regardless of the KNX system, apply the usual security mechanisms for IP networks:

- MAC filter
- Encryption of wireless networks
- Usage of strong passwords, and password protection against access by unauthorized persons

12.1.2.3 Using filter tables

Filter tables are used to improve system security and ensure that only authorized telegrams are forwarded.

13 Appendix

13.1 Scope of delivery

The device is supplied together with the following components:

- 1 x line coupler
- 2 x KNX bus connection terminal (red/black)
- 1 x installation and operating instructions
- 1 x cover cap

ABB AG – STOTZ-KONTAKT
Eppelheimer Str. 82
DE-69123 Heidelberg
go.abb/contact
Telephone: +49 (0)6221 701 607
Email: knx.marketing@de.abb.com

Additional information and regional points of contact:
www.abb.de/knx
www.abb.com/knx

Publication number 9AKK108469A3400 Rev. A | 22.08.2025 | EN-US