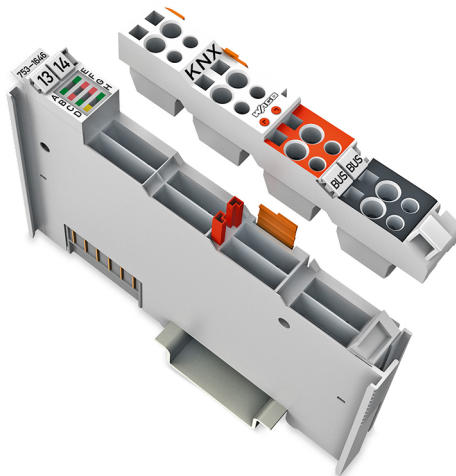


WAGO I/O System 750/753

KNX TP Secure Interface

753-1646



© 2025 WAGO GmbH & Co. KG
All rights reserved.

WAGO GmbH & Co. KG

Hansastraße 27
D - 32423 Minden

Phone: +49 571/887 – 0
Fax: +49 571/887 – 844169
E-Mail:  info@wago.com
Internet:  www.wago.com

Technical Support

Phone: +49 571/887 – 44555
Fax: +49 571/887 – 844555
E-Mail:  support@wago.com

Every conceivable measure has been taken to ensure the accuracy and completeness of this documentation. However, as errors can never be fully excluded, we always appreciate any information or suggestions for improving the documentation.

E-Mail:  documentation@wago.com

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present manual are generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1 Provisions	5
1.1 Scope of Applicability	5
2 Overview.....	6
3 Properties.....	7
3.1 View.....	7
3.2 Indicators	8
3.3 Wiring Interface	9
3.4 Control Elements	10
3.5 Circuit Diagram.....	11
4 Functions.....	12
4.1 Process Image.....	12
4.2 Operating Modes	12
4.2.1 KNX Device Mode	12
4.2.2 KNX Data Secure Mode	12
4.2.2.1 Device Certificate	12
4.2.2.2 Key Types	13
4.3 Operational Functions	14
4.3.1 Data Point Types (DPT)	14
5 Planning.....	15
5.1 Structure Guidelines	15
5.2 Security Capabilities and Hardening	15
5.2.1 Security Concept	15
5.2.1.1 Limitations of the Security Concept.....	15
5.2.1.2 KNX Data Secure Function	15
5.2.2 Hardening Measures	16
5.2.2.1 Safe Operating Environment.....	16
5.2.2.2 Secure Commissioning	17
5.2.2.3 Secure Operation	17
5.2.2.4 Secure Decommissioning	17
5.3 Compatibility	18
5.4 Requirements for Wiring and Accessories	18
5.5 Aids.....	18
5.6 Connection Example	19
6 Commissioning.....	20
6.1 Configuration	20
6.2 Secure Commissioning as a KNX Secure Device	21
7 Diagnostics	22
7.1 Diagnostics via Indicators.....	22
8 Service	24
8.1 Firmware Update/Downgrade.....	24
8.2 Factory Reset	24
8.3 Replacing the KNX Module	25
9 Appendix	26

- 9.1 Technical Data, Approvals, Guidelines and Standards 26
 - 9.1.1 Data sheet 753-1646..... 27
- 9.2 Network Structure..... 29
 - 9.2.1 KNXnet/IP Routers as Line Couplers 29
 - 9.2.2 KNXnet/IP Routers in a Mixed Topology..... 30

1 Provisions

1.1 Scope of Applicability

This document applies to the following product:

 **753-1646** KNX TP Secure Interface

Product Detail Page

 www.wago.com/753-1646

Note

Note applicable documents!

The complete operating instructions for the product consists of several, applicable documents. The product must only be installed and operated in accordance with the complete operating instructions. Knowledge of all applicable documents is required for proper use. You can find all documents and information on the product detail page.

Applicable document

System Manual I/O System 750/753

- Provisions
- Safety
- Planning
- Transport and Storage
- Assembly and Disassembly
- Conductor Termination
- Decommissioning

Additional documents

Besides this documentation/online help, the following supplementary documents are available:

-  **KNX TP Secure Interface 753-1646 Application Note**
-  **Library Description (Documentation of the library WagoAppKNX Secure)**

2 Overview

The I/O module KNX TP Secure Interface (item number 753-1646), hereinafter called the KNX module, is used to connect KNX networks.

The KNX module 753-1646 is a successor module to the KNX/EIB/TP interface 753-646 and offers the operating modes “KNX Device Mode” for unencrypted communication and “KNX Data Secure Mode” for encrypted communication.

In a KNX network, the KNX module appears as a standard KNX device and is linked via the ETS commissioning tool (Engineering Tool Software, Version 6).

The KNX module supports up to 1000 freely configurable KNX communication objects with any DPT, 2000 group addresses and 2000 associations. In the ETS, data point types (DPT) up to 14 bytes long can be assigned to each KNX communication object.

When operating as a KNX secure device, encrypted communication (KNX Data Secure) is possible for all KNX communication objects.

The head station and the KNX module are coupled via the local bus. The KNX module has four connections for the bus line for connecting the KNX bus.

The IEC application is programmed via CODESYS V3.x. A module-specific CODESYS library is available for this purpose. CODESYS function blocks are assigned to KNX communication objects via the WAGO-specific KNX app DCA (Device Configuration Application). The DCA can be loaded from the KNX product database into the ETS. Together with the DCA, the ETS is used for commissioning and configuring KNX modules, including the assignment of KNX communication objects to KNX group addresses. ETS 6 is supported.

The KNX module has two programming button connections for parameterization. Actuation of the buttons is requested by the ETS during startup of the KNX module.

Eight colored indicators on the housing of the KNX module signal active and inactive operating modes, data transfer via KNX and the local bus, the presence of a KNX bus voltage as well as internal states or error states of the KNX module.

The product can be operated on the head stations of the WAGO I/O System 750/753 indicated in section [🔗 Compatibility \[► 18\]](#).

3 Properties

3.1 View

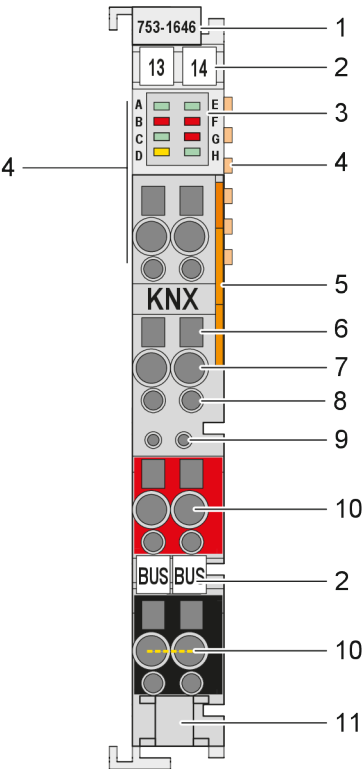
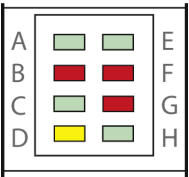


Figure 1: View

1	Item number	🔗 Scope of Applicability [► 5]
2	Slot for Mini-WSB (optional)	📖 System Manual I/O System 750/753
3	Indicators	🔗 Indicators [► 8] and 🔗 Diagnostics via Indicators [► 22]
4	Data contacts	📖 System Manual I/O System 750/753
5	Release tab	📖 System Manual I/O System 750/753
6	Access to open the associated CAGE CLAMP® connection	📖 System Manual I/O System 750/753
7	CAGE CLAMP®-Anschlüsse	🔗 Wiring Interface [► 9] , 🔗 Control Elements [► 10] und 📖 System Manual I/O System 750/753
8	Test slot for associated CAGE CLAMP® connection	📖 System Manual I/O System 750/753
9	Coding option via coding keys	📖 System Manual I/O System 750/753
10	Internal bridge in plug	🔗 Wiring Interface [► 9]
11	Fastening tab for cable ties	📖 System Manual I/O System 750/753

3.2 Indicators

Eight colored indicators on the housing of the KNX module signal active and inactive operating modes, data transfer via KNX and the local bus, the presence of a KNX bus voltage as well as internal states or error states of the KNX module.



LED	Designation	Function
A	Router Mode	Status indicator for "Router" operating mode (mode not supported by KNX module 750-1646)
B	KNX programming mode	"Programming mode" status indicator
C	Data transfer local bus	Status indicator for data transfer via local bus
D	Data transfer KNX	Status indicator for data transfer via KNX bus
E	Device mode	Status indicator for "Device" operating mode
F	Buffer overflow	Status indicator for buffer
G	Internal error	Error indicator
H	KNX bus voltage	Status indicator for KNX bus voltage

The meaning of the status indications is described section [🔗 Diagnostics via Indicators](#) [▶ 22](#).

3.3 Wiring Interface

The included KNX connector is intended exclusively for the KNX/EIB/TP interface (item number [753-646](#)) and for the KNX TP Secure Interface (item number [753-1646](#)) because the connector is internally commoned between the two KNX bus lines “+” and between the two KNX bus lines “-.”

The connector is designed with protection type IP20. Accordingly, condensation is not permitted.

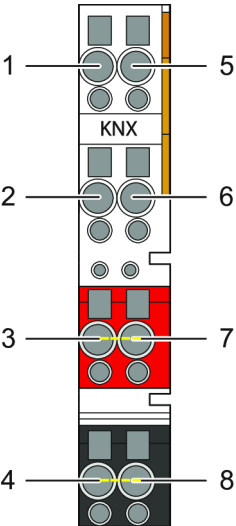


Figure 2: CAGE CLAMP® Connections

Connection	Designation	Function
1	--	<i>not assigned</i>
2	Programming button connection	Connection option for programming button (see Section Control Elements [► 10]).
3	+KNX bus	Connection of the KNX cable “+” ^{*)}
4	-KNX bus	Connection of the KNX cable “-” ^{*)}
5	--	<i>not assigned</i>
6	Programming button connection	Connection option for programming button (see Section Control Elements [► 10]).
7	+KNX bus	Connection of the KNX cable “+” ^{*)}
8	-KNX bus	Connection of the KNX cable “-” ^{*)}

^{*)}The connector has an internal bridge between pins 3 and 7 and between pins 4 and 8, so that the KNX bus is not interrupted when the connector is disconnected.

3.4 Control Elements

The KNX module has two programming button connections for parameterization:

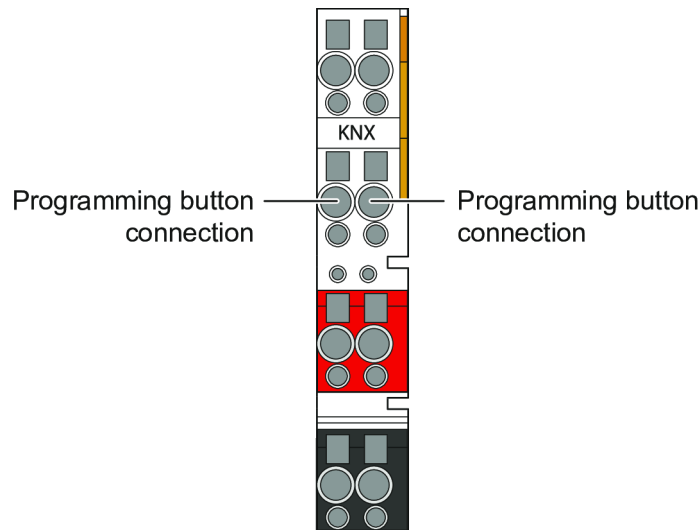


Figure 3: Programming Button Connections

The programming button connections are supplied from the KNX bus voltage. The KNX module can therefore only detect the connection of the programming button connections if the KNX bus voltage is present.

Programming mode is switched on or off by briefly establishing an electrical connection (e.g., via a wire jumper) between the two programming button connections.

Actuation of the programming buttons is requested by the Engineering Tools Software (ETS) during startup of the KNX module.

The status of the programming mode is indicated by LED B (see [🔗 Diagnostics via Indicators \[► 22\]](#)).

The programming button can also be used to perform a factory reset (see [🔗 Factory Reset \[► 24\]](#)).

3.5 Circuit Diagram

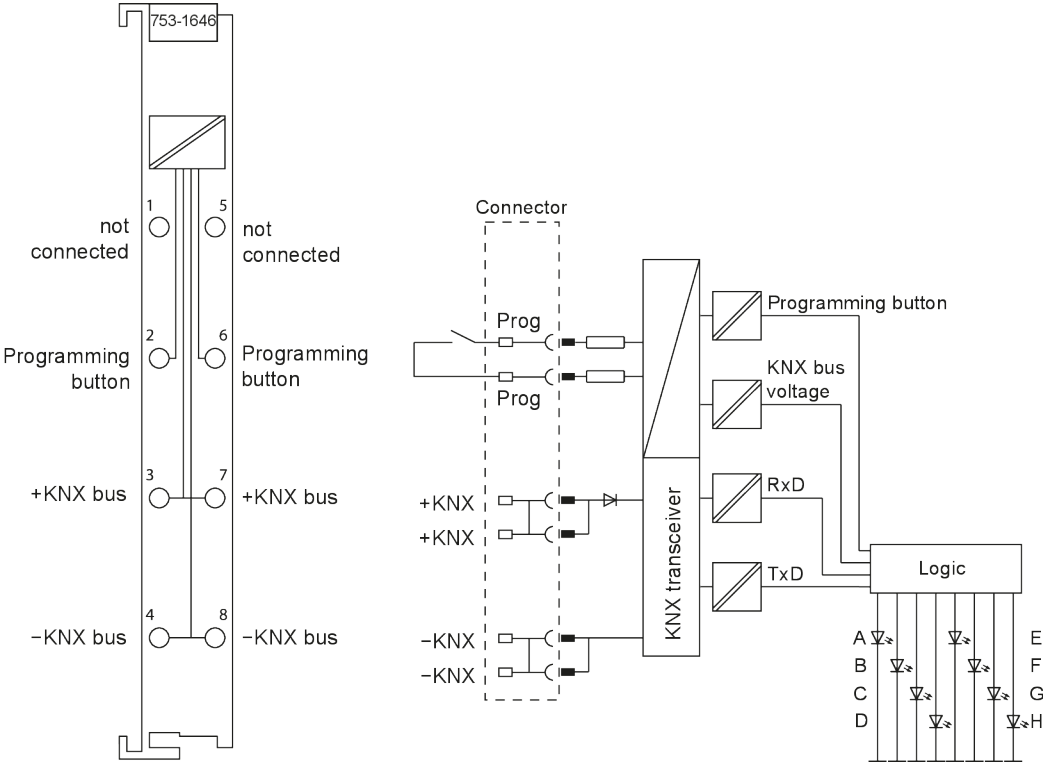


Figure 4: Circuit Diagram

For information on the system power supply, please see **System Manual I/O System 750/753**.

4 Functions

4.1 Process Image

The KNX module and the head station communicate via the “Mailbox 2.0” protocol. A corresponding CODESYS library is available for this.

4.2 Operating Modes

The KNX module 753-1646 supports the following operating modes:

- KNX Device Mode for unencrypted communication
- KNX Data Secure Mode for encrypted communication

The operating modes are described in more detail below.

The router mode and transparent mode of the KNX/EIB/TP interface 753-646 are not supported.

The data transfer via the KNX module is bidirectional via confirmed services with integrated flow control. Since KNX is a multi-master system, commands are not only passed from the head station to the KNX module, but are also actively and internally sent from the KNX module to the head station. This is the case, for example, when the event of a push-button connected to the KNX bus is sent internally via the local bus to the IEC application of the head station.

4.2.1 KNX Device Mode

The KNX module is in KNX device mode when delivered. The exchange of KNX telegrams between the KNX module and ETS is unencrypted.

WAGO provides the CODESYS 3.x library “WagoAppKNX_02” for communication between the KNX module and the IEC application (see [🔗 Aids \[► 18\]](#)). The library contains special function blocks that are required for operating the KNX module. They form the interface between the KNX objects and the application variables.

4.2.2 KNX Data Secure Mode

The KNX module supports “KNX Data Secure.” If this mode is enabled in the ETS via the “Safe Commissioning” function (see [🔗 Secure Commissioning as a KNX Secure Device \[► 21\]](#)), communication between the KNX module and the ETS is encrypted. The KNX module can then only be configured with the respective ETS project. This prevents unauthorized manipulation of the KNX installation.

If “KNX Data Secure” is enabled, communication between the KNX module and other KNX secure devices can also be encrypted. This prevents spying and manipulation of KNX telegrams.

4.2.2.1 Device Certificate

The device certificate is unique for each KNX secure device and is required for safe commissioning (KNX Data Secure).

You will find the device certificate on the side of the KNX module and on a sticker attached to the packaging.

4.2.2.2 Key Types

Three different types of keys are used to encrypt communication:

- **Factory Default Setup Key (FDSK):**
Each KNX secure device has an individual 128-bit FDSK, which is permanently stored in the KNX module and cannot be read or changed.
The FDSK is stored in the device certificate and is the default value of the tool key. The ETS uses the FDSK to establish a first encrypted point-to-point connection with the KNX secure device and then transfer the tool key to the KNX secure device and save it there. The FDSK is no longer required for further operation of the system. The FDSK is only required again when the KNX module is switched back to unencrypted mode via the ETS or when a factory reset has been performed.
- **Tool key:**
Each KNX secure device manages the 128-bit tool key for encrypted communication between the ETS and the KNX module. The tool key is set to the FDSK at the factory. For the ETS to communicate with a KNX secure device, it must know the current value of the tool key. To do this, the KNX secure device must be included in an ETS project and its device certificate added there. During this process, the tool key is set to a secret value. Communication between ETS and KNX module is then encrypted. The FDSK is now invalid, so that the encrypted communication cannot be intercepted or manipulated, even with knowledge of the device certificate or the FDSK. The tool key cannot be read or set manually. Without knowledge of the tool key stored in the ETS project, the KNX module cannot be reconfigured and is thus protected against manipulation by unauthorized persons.
When the KNX secure device is factory reset, the tool key is deleted and reset to the FDSK.
- **KNX group key:**
Group keys are used to encrypt communication between KNX secure devices via KNX group addresses.
For each KNX group address defined in an ETS project, the ETS generates a 128-bit KNX group key. All KNX secure devices that are to be given access to a specific group address receive the respective group key from the ETS via communication encrypted with the tool key.
All group keys are deleted when the KNX secure device is factory reset.

4.3 Operational Functions

4.3.1 Data Point Types (DPT)

The KNX module supports the following lengths of KNX data point types:

- 1 ... 7 bits
- 1 ... 4 bytes
- 6 bytes
- 8 bytes
- 10 bytes
- 14 bytes

For more information on data point types (“Interworking Data Point Types”), please refer to the website  <https://support.knx.org>.

5 Planning

This section provides helpful information for planning the use of the product in a node.

5.1 Structure Guidelines

Up to four KNX modules (item numbers 753-646 and 753-1646) can be operated simultaneously and independently of one another at a head station of the 750/753 system. The use of additional KNX modules is basically possible, but depends on the specific framework conditions and must be checked in individual cases. The KNX module supports TP-256.

Up to 1000 KNX communication objects can be used on one KNX module. However, if more than 200 KNX communication objects are used, handling in the ETS can be significantly slowed down. Therefore, it is recommended to use one KNX module per 200 KNX communication objects.

If no external connection is established, the individual KNX TP lines of the various KNX modules are electrically and logically isolated from each other.

5.2 Security Capabilities and Hardening

5.2.1 Security Concept

5.2.1.1 Limitations of the Security Concept

Regardless of the encrypted communication, the following security risks exist when operating a KNX secure device:

- Local bus communication is not encrypted.
- Operation with other system components (e.g., DALI modules) is not encrypted.
- The ETS project is insufficiently protected without a sufficiently strong password.

5.2.1.2 KNX Data Secure Function

For effective data encryption and authentication to be possible using “KNX Data Secure,” all keys used must remain secret. To minimize the risk of possible attacks on secured KNX systems, observe the following instructions.

Factory Key (FDSK)

The FDSK can be derived from the KNX device certificate, which is shown on the KNX module page and on the label included in the scope of delivery. Therefore, keep the KNX device certificate confidential until the secure commissioning has been completed:

- Do not leave the KNX module lying around in an accessible place at the construction site.
- After mounting the KNX module, cover the corresponding device side with another I/O module or end module.
- Lock the control cabinet.
- Keep the supplied label in a safe place in your records, out of the reach of unauthorized persons.

Tool Key

If an attacker knows the FDSK and can also spy on the communication between ETS and the KNX module, they could obtain the tool key. Therefore, perform safe commissioning of the KNX module in the smallest possible network.

- If possible, temporarily disconnect all KNX lines, KNX devices and KNX infrastructure components (routers, line couplers, gateways, etc.) that are not required for communication between ETS and the KNX module.
- If possible, use a direct access to the TP line to which the KNX module is connected (without detours via routers, line couplers, gateways, etc.).
- Make sure that no one can spy on or record communication between ETS and the KNX module during secure commissioning.

Group Key

An attacker who has obtained the tool key can also spy on the transmission of the group keys or configure new group keys. This would render the encryption and authentication of KNX telegrams using “KNX Data Secure” ineffective. Therefore, please take the following additional security measures:

- Protect your ETS project with a strong password.
- Prevent unauthorized access to the ETS project file.

5.2.2 Hardening Measures

The hardening measures described are not alternatives to one another. To ensure good protection, the various hardening measures must be implemented in addition to each other.

5.2.2.1 Safe Operating Environment

The product must only be operated in a secure operating environment. A secure operating environment helps prevent various attacks. A secure operating environment meets the following requirements at a minimum:

- Physically protected access
- Recorded access and entry

Physically protected access

The product comes with a conspicuous device certificate. It must only be installed in suitable enclosures, cabinets or electrical operating rooms that meet the following requirements at a minimum:

- Access area is protected.
- Access is only granted to authorized persons.
- Only necessary connections lead physically to the outside.

Protected KNX Network Segment

The product with the secure operating mode is a device with KNX interfaces. It may only be used in a protected KNX network segment that meets the following requirements at a minimum:

- There is no unprotected connection to the Internet.
- All KNX network devices are located in a protected KNX network segment.

Recorded access and entry

The product with the secure operating mode requires a temporary reduction in security in certain situations. This may be necessary for engineering/service activities or in the event of a fault.

Logging must capture the following events at a minimum:

- Configuration in the protected KNX network segment (e.g., changing the boundary of the protected KNX network segment)
- Access to the physically protected area (e.g., service personnel)

5.2.2.2 Secure Commissioning

Secure product commissioning helps prevent various attacks. Secure commissioning meets the following requirements at a minimum:

- Protected ETS project file

5.2.2.3 Secure Operation

Secure operation of the product helps prevent various attacks. Secure operation meets the following requirements at a minimum:

- Time-limited access and entry for engineering/service activities or in the event of a fault
- Action following a security event/incident

Access and entry for engineering/service activities or in the event of a fault

- Only grant access to the ETS project file on a temporary basis.

Following a security event

- Take action following a security event.

The following actions at a minimum must be taken following a security event:

- Each product whose key is or was stored in the product to be disposed of must be securely commissioned again.

Verified and current firmware (updates)

- Use only verified and current firmware (updates).

WAGO recommends using current firmware.

The current version of a firmware corresponds to the current state of the art and security. Previous firmware versions can present vulnerabilities in technology and security.

5.2.2.4 Secure Decommissioning

Secure product decommissioning helps prevent various attacks. Secure decommissioning meets the following requirements at a minimum:

- Deleted keys in the product
- Deleted data in the product

Data in the Product

- Delete all keys saved in the product.
- Delete all data saved in the product.

The following requirements must be met at a minimum:

- Product is reset to factory settings (factory reset).
- Each product whose key is or was stored in the product to be disposed of must be securely commissioned again.
- If a factory reset is not possible: Arrange for scrapping by a disposal service provider qualified in cybersecurity.

5.3 Compatibility

The KNX module can be operated on the following head stations of the WAGO I/O System 750/753 from the specified version:

Table 1: Compatibility List

Head Station	Item Number	Firmware Version
Basic Controller 100; 2ETH; ECO	750-8000	≥ FW 3
Basic Controller 100; 2ETH	750-8001	≥ FW 3
PFC100 Generation 2	750-811x	≥ FW 27
PFC200 Generation 2	750-821x	≥ FW 27
PFC300	750-83xx	≥ FW 27

Use of the KNX module on fieldbus couplers is excluded.

5.4 Requirements for Wiring and Accessories

The KNX module does not have its own KNX power supply. Hence, the connection of a separate KNX supply module is required.

According to the KNX Association, a standard MSR line (e.g., PYCYM 2×2×0.8) or a telecommunications line (e.g., J-Y(St)Y 2×2×0.8) is recommended for the KNX bus line. The red and black strands are used for this. The bus line is installed in free topology.

Ring topologies may not be created.

Because the cable length of a bus line is limited and the maximum cable lengths between bus devices must not be exceeded, general KNX guidelines must be observed.

5.5 Aids

Engineering Tool Software (ETS)

To configure and commission the system, you need the ETS with the WAGO product database and the WAGO DCA included. ETS 6 is supported.

The **WAGO DCA** as well as general application notes and the product manual can be found on the product detail page at www.wago.com.

The **ETS** is available on the KNX Association website at <https://www.ets6.org>.

CODESYS “WagoAppKNX_02” Library

To use the KNX module with CODESYS V3.x, you need the “WagoAppKNX_02” library.

The library is available at <https://downloadcenter.wago.com/wago/learning-material>.

5.6 Connection Example

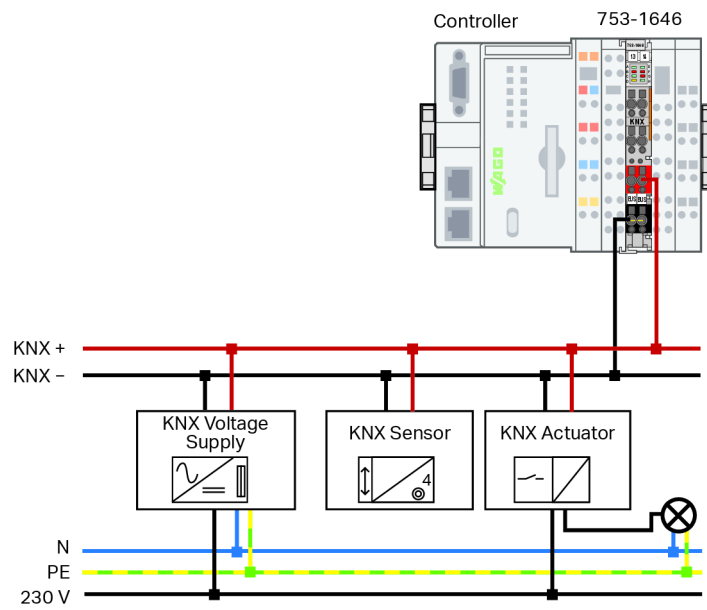


Figure 5: Connection Example

6 Commissioning

6.1 Configuration

If a corresponding request is displayed in the Engineering Tool Software (ETS), the KNX module must be set to programming mode (see [🔧 Control Elements \[► 10\]](#)). To avoid ambiguity, only one KNX module may be in programming mode at a time.

For the KNX module to communicate with other subscribers in the KNX network, CODESYS V3.x function blocks must be created from the CODESYS library “WagoApp-KNX_02.” When creating (compiling) the user-specific IEC application with the CODESYS development environment, all network variables are exported in a symbol configuration file (XML file). You can find more information on this in an application note.

The ETS and DCA import the symbol configuration file with the IEC network variables. The imported network variables can be linked to KNX group addresses and loaded into the KNX module. Telegrams are sent in the KNX net via the KNX group addresses.

A solid green LED E indicates that it has been downloaded successfully. If the LEDs A and E continue to flash synchronously, the IEC application must be checked. A possible cause of error is, for example, that an incorrect or modified symbol configuration file has been loaded into the KNX module.

This startup behavior is also evident when the bus node is already running but the IEC application has been modified.

If DPT function blocks have been renamed, deleted, moved or otherwise edited, the network variables may need to be reimported.

The KNX module is then ready for operation, so that communication can take place between the IEC application and the KNX module, and via the KNX module to connected TP networks. The figure below shows the data flow after the configuration has been completed.

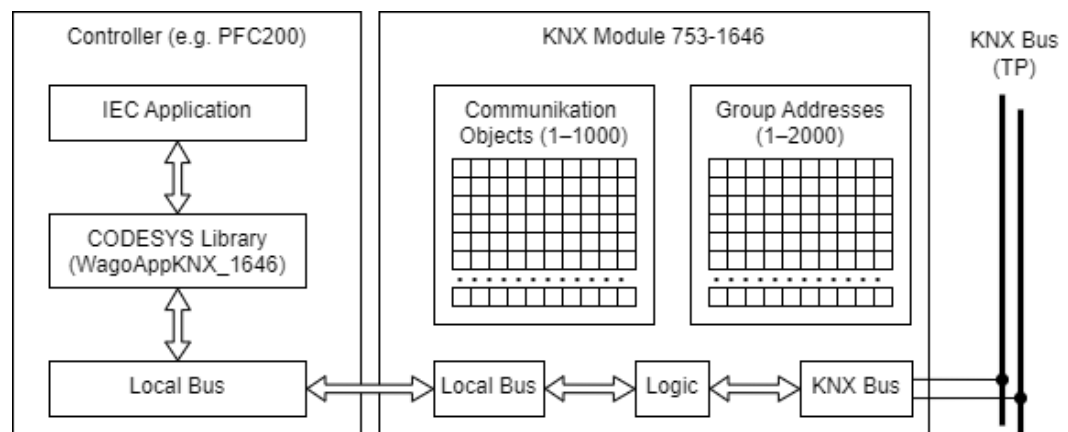
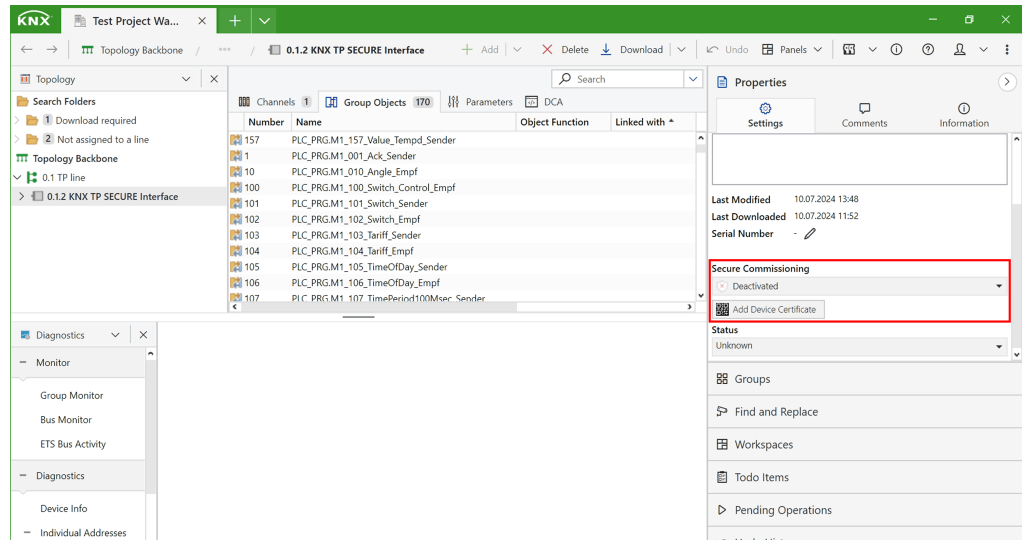


Figure 6: Data Flow after Configuration

6.2 Secure Commissioning as a KNX Secure Device

- ✓ The KNX module is ready for operation and connected to the ETS.
- ✓ The device certificate is available (see [📄 Device Certificate \[▶ 12\]](#)).

1. Select the KNX module in the ETS.
2. Select the “Settings” tab in the “Properties” container in the sidebar.



3. In the “Safe Commissioning” drop-down menu, click “Add Device Certificate.”
4. Use a webcam to read the QR code into the ETS or enter the 36-digit number into the ETS.
 - ⇒ The KNX device certificate is transmitted to the ETS. The ETS then establishes communication with the KNX module encrypted with the FDSK, generates a secret tool key and transmits it to the KNX module.
 - ➔ The ETS and the KNX module now communicate via communication encrypted with the tool key.

7 Diagnostics

7.1 Diagnostics via Indicators

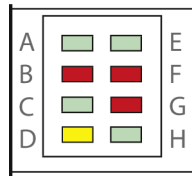


Table 2: LED A (Router mode)

Status	Possible Explanation
Off	"Router" operating mode is disabled.
Synchronous with LED E, flashing (green)	Data between the KNX module and CODESYS has not yet been compared. KNX module is not ready for operation.

Table 3: LED B (KNX Programming mode)

Status	Possible Explanation
Off	KNX programming mode is disabled.
Red	KNX Programming mode is enabled.
Flashing (red)	Factory reset is performed.

Table 4: LED C (data transfer local bus)

Status	Possible Explanation
Off	Local bus data transfer is disable.
Flashing (green)	Local bus data transfer is enabled.

Table 5: LED D (Data transfer KNX)

Status	Possible Explanation
Off	KNX data transfer is disabled.
Flashing (yellow)	KNX data transfer is enabled.

Table 6: LED E (Device mode)

Status	Possible Explanation
Off	KNX module is not ready for operation.
Green	KNX module is ready for operation.
Synchronous with LED A, flashing (green)	Data between the KNX module and CODESYS has not yet been compared. KNX module is not ready for operation.

Table 7: LED F (buffer overflow)

Status	Possible Explanation
Off	No buffer overflow.
Red	Buffer overflow (data loss due to non-functional KNX bus or unprocessed data)

Table 8: LED G (internal error)

Status	Possible Explanation
Off	No error
Red	No KNX bus voltage available (see LED H) or device fault.

Table 9: LED H (KNX bus voltage)

Status	Possible Explanation
Off	No KNX bus voltage available
Green	KNX bus voltage available

8 Service

8.1 Firmware Update/Downgrade

You can update the firmware on the Series 750, 753 and 750 XTR I/O modules with the “WAGO IO-Update 750” software. The I/O module is updated via the service interface. For ETHERNET-based fieldbuses, the I/O module can also be updated via the fieldbus connection on the head station.

Observe the following information:

- Ensure that communication with the head station is not interrupted during the update process.
- The application running on the controller must be stopped before the update process.
- Before an update via the service interface, disconnect the fieldbus cable from the head station.
- Do not close the software during the update.
- Only run the software from a local hard disk.

NOTICE

Property damage due to interruption!

Interrupting the update process can damage the product.

- Complete the update/downgrade process!

Technical Support

- Additional information about the **WAGO IO-Update 750** software is available from  **WAGO Support**.
- Contact  **WAGO Support** to discuss whether a **firmware downgrade** is possible in your situation:
Tel.: +49 (0) 571/8 87 – 4 45 55
Fax: +49 (0) 571/8 87 – 84 45 55

8.2 Factory Reset

The KNX module can be restored to its factory settings by performing a factory reset. All stored module settings including the group keys are deleted and the tool key is reset to the FDSK. The physical address is reset to 15.15.255.

When operating as a KNX Secure Device, the KNX module can no longer be configured if the ETS project or access to it is lost. Accordingly, no new keys can be programmed. To continue using the device hardware, a factory reset is required.

To reset the KNX module to the factory settings, proceed as follows:

- ✓ KNX power supply is available.
 - ✓ The KNX module is physically accessible.
1. Connect a KNX power supply to KNX modules 3/7 and 4/8.
 2. Switch off the power supply of the KNX module by switching off the power supply of the entire node.

3. Bridge the programming button connections 2 and 6 with a button or a wire jumper.
 4. Switch off the node.
 5. Switch on the node and leave the programming button connections 2 and 6 bridged.
 - ⇒ LED B (programming mode) flashes slowly.
 6. Disconnect the connection between programming button terminals 2 and 6 for less than 2 s and then reconnect it permanently until the LED B flashes quickly.
 - ⇒ The KNX module performs the factory reset.
Note: If the connection between the buttons is interrupted for more than 2 seconds, the factory reset is canceled without changes to the KNX module.
 7. When the factory reset is complete, remove the jumper between programming button connections 2 and 6.
- ➔ The KNX module has been reset to the factory settings and can be reconfigured using the ETS.

8.3 Replacing the KNX Module

When replacing a KNX module 753-646 with a KNX module 753-1646, observe the following module-related compatibility restrictions:

- Operating mode:
Router mode and transparent mode are no longer supported.
- Compatibility:
Some head stations are no longer supported (see [🔗 Compatibility \[p. 18\]](#)).
- Process data:
A new CODESYS library is required. Use the KNX TP Secure Interface 753-1646 Application Note.

9 Appendix

9.1 Technical Data, Approvals, Guidelines and Standards

Note

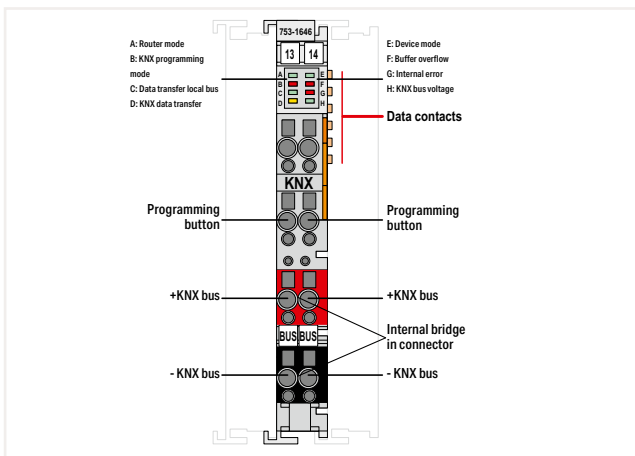
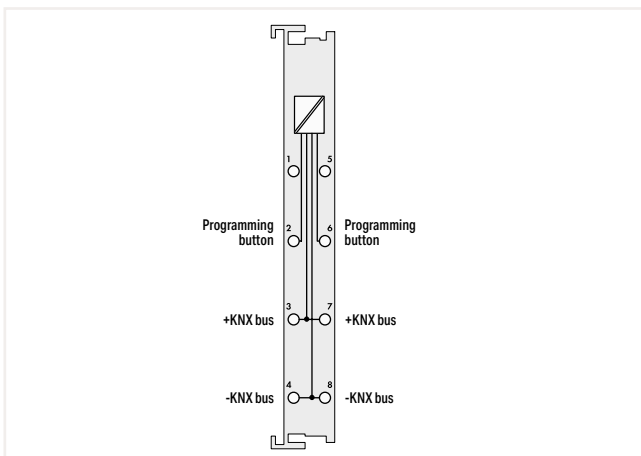
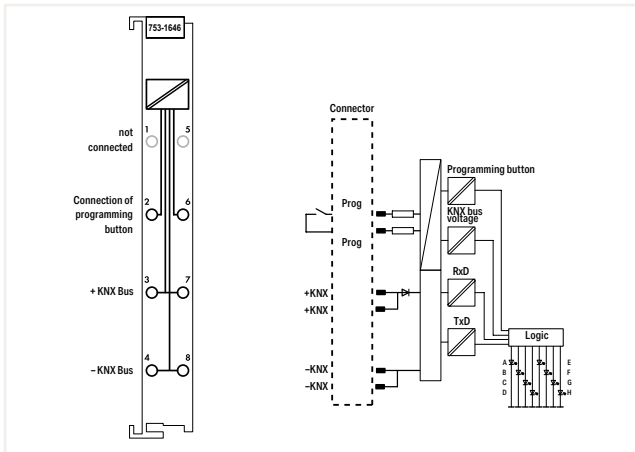
Subject to changes!

Please also observe the further product documentation! You can generate the current datasheet at any time at: www.wago.com /<item number>.

See also

 Data sheet 753-1646 [▶ 27]

KNX TP Secure Interface



The I/O module KNX TP Secure Interface (item number 753-1646) is used to connect KNX networks.

The module is compatible with the KNX/EIB/TP interface 753-646. However, router mode and transparent mode are not supported by the KNX TP Secure Interface 753-1646. In a KNX network, the module appears as a standard KNX device.

The KNX module supports up to 1000 freely configurable KNX communication objects with any DPTs, 2000 group addresses and 2000 associations. In the ETS, data point types (DPT) up to 14 bytes long can be assigned to each KNX communication object.

When operating as a KNX secure device, encrypted communication (KNX Data Secure) is possible for all KNX communication objects.

The application is programmed via CODESYS 3.x.

ETS 6 is supported.

A 753 Series plug with internally commoned contacts (3/7 and 4/8) is included.

An external KNX power supply is required to operate the KNX module.

Technical data

Communication	KNX/TP1-256 S-Mode KNX Data Secure
Device-specific	Number of communication objects: 1000; Number of group addresses: 2000; Number of associations: 2000
Current consumption, max.	7.5 mA (KNX)
Transmission rate	9.6 kBd (KNX)
Width of the process data image	24 bytes
Power supply	KNX: via KNX power supply unit
Supply voltage (system)	5 VDC; via data contacts
Current consumption (5 V system supply)	65 mA
Isolation	3.51 kV rms
Indicators	8 x LED
Supported ETS versions	ETS 6 or higher

Connection data

Connection technology: inputs/outputs	8 x CAGE CLAMP®
Connection type 1	Inputs/outputs
Solid conductor	0.08 ... 2.5 mm² / 28 ... 14 AWG
Fine-stranded conductor	0.08 ... 2.5 mm² / 28 ... 14 AWG
Strip length	9 ... 10 mm / 0.35 ... 0.39 inches
Connection point (other) designation	Programming button; bridge 2/6

KNX TP Secure Interface



Physical data

Width	12 mm / 0.472 inches
Height	100 mm / 3.937 inches
Depth	69 mm / 2.717 inches
Depth from upper-edge of DIN-rail	61.8 mm / 2.433 inches

Mechanical data

Mounting type	DIN-35 rail
Pluggable connector	pluggable

Material data

Color	light gray
Housing material	Polycarbonate; polyamide 6.6
Fire load	1.044 MJ
Weight	55.9 g
Conformity marking	CE

Environmental requirements

Ambient temperature (operation)	0 ... +55 °C
Ambient temperature (storage)	-40 ... +85 °C
Protection type	IP20
Pollution degree	2 per IEC 61131-2
Operating altitude	0 ... 2000 m / 0 ... 6562 ft
Mounting position	Horizontal left, horizontal right, horizontal top, horizontal bottom, vertical top and vertical bottom
Relative humidity (without condensation)	95 %
Vibration resistance	4g per IEC 60068-2-6
Shock resistance	15g per IEC 60068-2-27
EMC immunity to interference	per EN 61000-6-2
EMC emission of interference	per EN 61000-6-3
Exposure to pollutants	per IEC 60068-2-42 and IEC 60068-2-43
Permissible H ₂ S contaminant concentration at a relative humidity 75 %	10 ppm
Permissible SO ₂ contaminant concentration at a relative humidity 75 %	25 ppm

9.2 Network Structure

In a conventional two-wire TP1 network (see figure), a distinction is made between backbone, ranges and lines. Up to 15 ranges can be coupled at a KNX backbone using backbone couplers. Each of these ranges, in turn, is broken down into a maximum of 15 lines that are connected to the range line via line couplers. Lines can accommodate up to 64 subscribers (see KNX Standard 3/1/1).

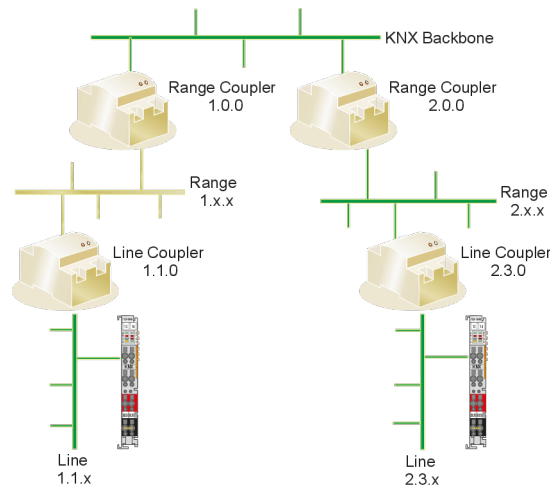


Figure 7: Traditional TP1 Network

Because there can be significant data traffic on the KNX backbone (range line) and the transmission speed for twisted pair lines is a maximum of 9,600 baud, it makes sense to flatten the network topology and replace the KNX backbone with an IP backbone. Doing so makes much higher transmission speeds possible.

9.2.1 KNXnet/IP Routers as Line Couplers

The KNXnet/IP router acts as a link between the IP backbone and the lines when it is used as a line coupler.

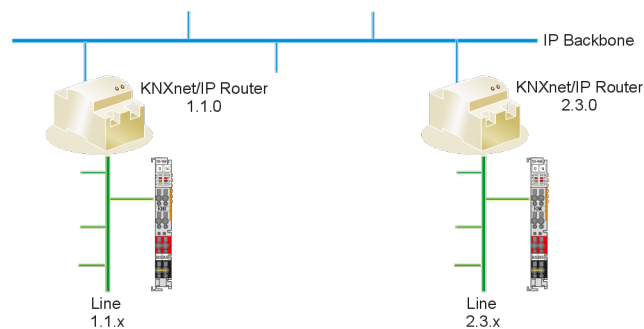


Figure 8: KNXnet/IP Routers as Line Couplers

The number of lines that can be created in the ETS is limited to 15 per range (backbone).

9.2.2 KNXnet/IP Routers in a Mixed Topology

If required, routers can also be used as range and line couplers together in a network. In this example, the KNXnet/IP router with the physical address 1.1.0 fulfills the function of a line coupler, while the KNXnet/IP router with the physical address 2.0.0 corresponds to an backbone coupler.

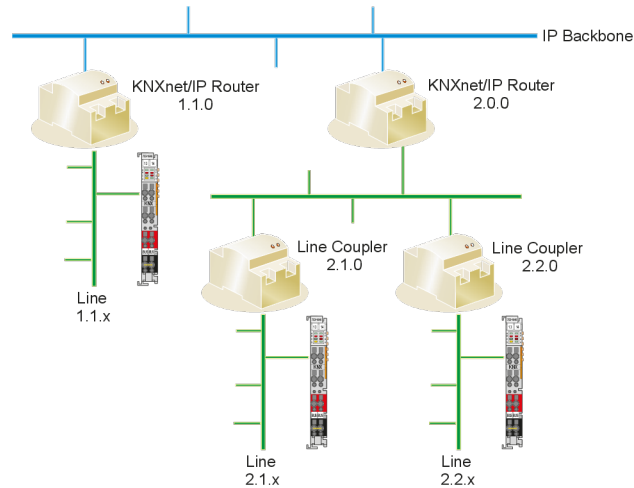


Figure 9: KNXnet/IP Routers in a Mixed Topology

A backbone coupler is not possible below a KNXnet/IP router, i.e., if a line is connected directly to the IP backbone via a KNXnet/IP router, there must be no backbone coupler for the area of this line. In the topology of the example figure, no backbone coupler with the address 1.0.0 is possible on the IP backbone.

List of Tables

Table 1	Compatibility List.....	18
Table 2	LED A (Router mode)	22
Table 3	LED B (KNX Programming mode)	22
Table 4	LED C (data transfer local bus).....	22
Table 5	LED D (Data transfer KNX).....	22
Table 6	LED E (Device mode)	22
Table 7	LED F (buffer overflow).....	22
Table 8	LED G (internal error)	23
Table 9	LED H (KNX bus voltage)	23

List of Figures

Figure 1	View	7
Figure 2	CAGE CLAMP® Connections.....	9
Figure 3	Programming Button Connections	10
Figure 4	Circuit Diagram	11
Figure 5	Connection Example.....	19
Figure 6	Data Flow after Configuration	20
Figure 7	Traditional TP1 Network	29
Figure 8	KNXnet/IP Routers as Line Couplers	29
Figure 9	KNXnet/IP Routers in a Mixed Topology	30

WAGO GmbH & Co. KG

Postfach 2880 · D - 32385 Minden
Hansastraße 27 · D - 32423 Minden

✉ info@wago.com

🌐 www.wago.com

Headquarters
Sales
Order Service
Fax

+49 571/887 – 0
+49 (0) 571/887 – 44 222
+49 (0) 571/887 – 44 333
+49 571/887 – 844169

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Copyright – WAGO GmbH & Co. KG – All rights reserved. The content and structure of the WAGO websites, catalogs, videos and other WAGO media are subject to copyright. Distribution or modification of the contents of these pages and videos is prohibited. Furthermore, the content may neither be copied nor made available to third parties for commercial purposes. Also subject to copyright are the images and videos that were made available to WAGO GmbH & Co. KG by third parties.