The gateway

The base unit is a powerful industry grade gateway that provides LAN to WAN routing available in a number of configurations supporting 3G, LTE or fixed Ethernet WAN connectivity. The base unit can be equipped with extension cards to support a wide range of interfaces and applications.
5ABox has enriched the standard gateway to provide KNX connectivity and a number of features as described further below. The gateway can act as a standalone deployment what we call 'KNX in a box' or be seamlessly integrated in an existing KNX deployment. The former requires the KNX extension card as shown in the picture above with built-in storage, USB, bus power, real-time clock and transceiver(s), the latter requires a KNX-to-IP gateway. An overview of the supported combinations of base units and front extension cards is shown here:

BASE UNIT VERSION	EXTENSION CARD	ENVIRONMENT
WAN Ethernet	KNX board	Standalone / existing KNX deployment
	One port Ethernet board	existing KNX deployment
3G	KNX board	Standalone / existing KNX deployment
	One port Ethernet board	existing KNX deployment
LTE	KNX board	Standalone / existing KNX deployment
	One port Ethernet board	existing KNX deployment
	None	existing KNX deployment

Remark: Additionally Wifi can always be installed in the back slot of the base unit independent of the combination mentioned in the table.

The 5ABox solution has the following features:

- **USER INTERFACE**
  The web-based user interface blends seamlessly into the existing standard Option® Cloudgate interface and allows configuring in a simple and menu driven way all the functionalities described here below.

- **DATA LOGGING**
  The 5ABox gateway can log KNX datagrams configurable on a per group address basis in a sustainable way at a bus rate of up to 20 messages per second. The group addresses are discovered automatically and selected from a dropdown menu for logging. The collected data can be viewed locally in table format or graph as well as downloaded into a CSV format for further processing. The data can be transferred or based on triggers (time, internal and external events) in a secure way to external platforms or automatic upload of the data on a fixed interval basis can be enabled. Either way, this allows for bulk transfer of data in the most cost effective manner based upon the needs and requirements of your customers.

- **REMOTE ACCESS**
  The KNX bus can be accessed remotely for programming or configuration of KNX bus devices.

- **LIVE FEEDS**
  The 5ABox gateway is capable of streaming data based on group addresses to external platforms for either near real-time monitoring or anomaly detection. Multiple feeds to different platforms are supported.

- **CONFIGURATION IMPORT**
  The ETS project can be uploaded and imported onto the gateway to avoid redundant configuration.

- **SCENARIO ENGINE**
  A powerful engine based on a trigger-action mechanism can execute locally virtually every possible scenario. The triggers and actions can be combined in a limitless way; even multiple cascading scenarios are supported. The table below gives an overview.

TRIGGER	ACTION
Time based recurrent	Transfer data over (s)FTP
Time based once	Send a KNX telegram on the bus
Incoming SMS	Send an SMS
KNX bus telegram	Load another scenario
Action result	Timers with fixed and random delays
	Reboot of the gateway
	Readout Lingg-Janke meters via KNX FTP

- **SECURITY**
  Data is transferred in a secure way with server authentication. A tunnel is setup between the 5ABox and the server side over a 256-bit encrypted tunnel. Because of the server authentication no man-in-the-middle attacks are possible.
  In case the mobile network is used, through the use of private APN's, the server LAN can be extended all the way through the 5ABox and ensures the save transfer of data.

- **KNX FTP SUPPORT FOR LINGG-JANKE METERS**
  KNX devices that have implemented the KNX FTP protocol are supported to allow for the optimal way to retrieve data from the devices without overloading the bus. The data is retrieved from the different devices automatically on a daily basis. The data is cached on the gateway for quick and easy viewing access.

- **KNX ROUTING**
  The 5ABox gateway will support the routing and filtering of KNX datagrams between different lines via KNX tables similar to IP tables in the IP world. This will either be done on group address of physical address basis.

Security aspects

OVERVIEW

The security aspects from the sensors/actors up to the SCADA will be described. From an overall perspective the solution is designed with security in mind both on device level and on transmission level.

DEVICE SECURITY

Sensors/actors/meters

From a physical perspective meters can be led-sealed to detect device tampering. The devices are configured via the KNX ETS tool and this configuration information is held by the installer/user but not kept in the devices.

Gateway

From a physical perspective, special torx screws are used to prevent device tampering. The software is digitally signed and the gateway would not even startup when the image is modified. Access to the interface is done via a web browser with username/password identification that can be set by the user/installer.

As the box has the hardware capabilities for geo-location, in the future it would be possible to detect that the gateway is removed or stolen. This will allow gateway blacklisting and when a connection is made, the box can be remotely reset so that all data would be wiped.

TRANSMISSION SECURITY

Between the sensors/actors and the gateway

The transmission is done over 2-wires and the protocol used is KNX. Only via direct access to the wire, it is possible to connect to the KNX bus. Nevertheless, the communication does not contain any information about the interpretation of the data being sent. Data can come from multiple devices and can be configured differently on a per installation basis so that no 2 installations will look the same from a KNX communication perspective.

Between the gateway and the SCADA

The gateway can works in standalone mode and does not always need to be connected to the network. This can be done on-demand when data needs to be transmitted or received and thus preventing any unauthorized access from outside.

Whenever data is sent, it is done in 2 steps through:

- Identification of the SCADA via a pre-shared key to avoid man-in-the-middle attacks
- Transmission of data over a 256-bit encrypted tunnel

In case of mobile connectivity, most operators already use private IP addressing with communication only initiated by the device and thus preventing external access. However, a private APN can be used to extend the corporate LAN to the mobile network including your own private IP addressing scheme with possible AAA integration allowing secure bidirectional communication.

The ecosystem

The gateway is the central point to connect all KNX devices locally and interface with the outside world in a secure way over both fixed and wireless internet. A SCADA can collect all the data and interface with other third-party systems.