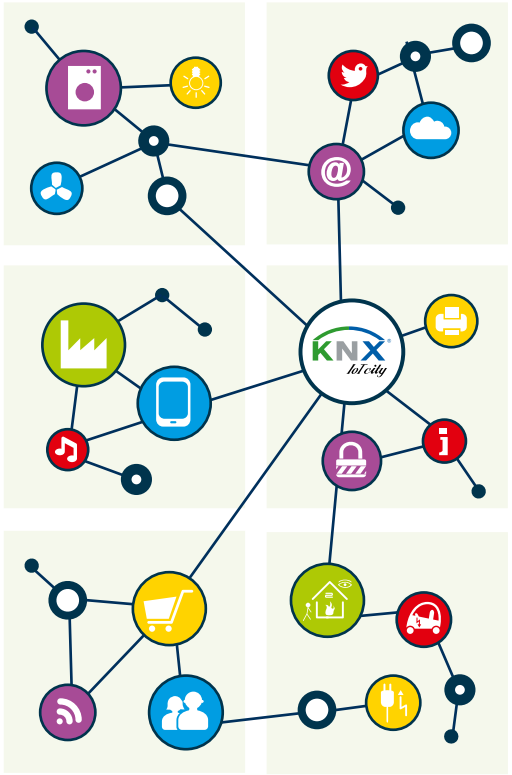
domobrain
domótica y control energético
www.domobrain.com



KNX News

KNX Internet of Things,
KNX Secure,
ETS Inside

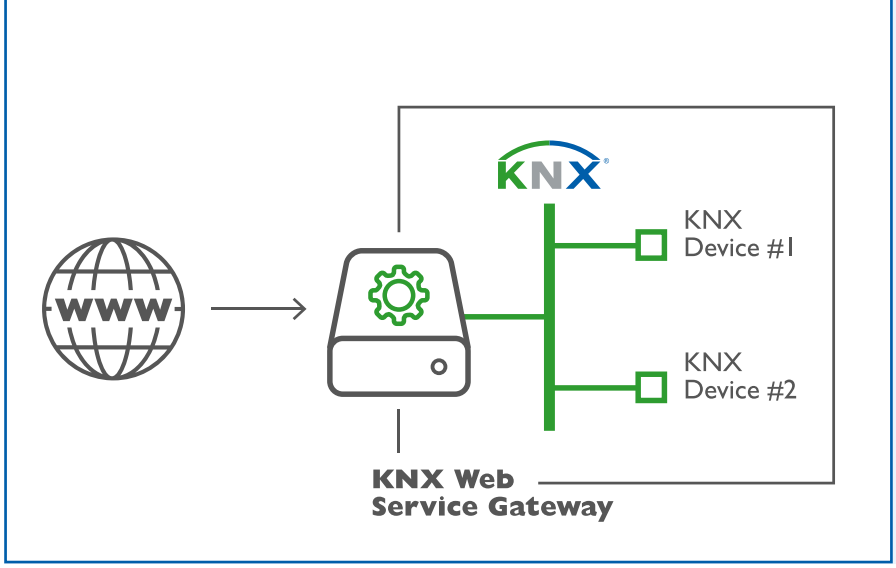
KNX Internet of Things

KNX and the Internet of Things – simple Integration by KNX Web Services

The "Internet of Things" is a buzzword in the world of information technology. What still has to become part of the general knowledge is already a long known term in expert groups for a new development boost. Everyday objects become intelligent and communicate via the internet. According to visionaries until 2020 50 Billions of such objects will communicate via the internet. However, the Internet of Things is not still up in the air but has become reality already today. Already for a long time the KNX Standard forms part of this global IoT world. By the introduction of the KNX Web Services KNX underlines its leading position and opens new ways in the operation and visualization of KNX systems.

Since a long time the Internet of Things (IoT) has found its way into nearly all areas of life – even in building automation. Global players like Google or Apple penetrate into this market of the future and try to emphasize their philosophy of intelligent buildings by networkable products like smoke detectors, radiator thermostats, movement detectors and switchable socket outlets. When trying to find in the vast number of systems a solution suited for him the user gets more problems than answers. For instance the hardwired window contact of system A is not capable to communicate with the wireless valve drive of manufacturer B.

In addition to these incompatibilities, resulting from different protocols and transmission media, a further fact proves to be a major disadvantage: proprietary automation solutions usually require a central server for the exchange of data between the installed components, which cannot communicate directly with each other like it is possible in case of KNX. This can be a small



computer, a smartphone or even a cloud based solution. It is an advantage of this approach, that the data are available at any place by means of websites, yet on the other hand it is the Achilles heel of the network. If the server fails, the building control fails, too.

KNX is a Network of „Things“

What does the term „Internet of Things“ really mean? Wikipedia defines it roughly as follows: It describes the connection of clearly identifiable physical objects with the virtual world of the internet. For that purpose the “devices” contain electronics, software, sensors and the related network connectivity. Each thing has a clearly identifiable address and is able to receive, collect, evaluate and send data.

Since the beginnings of the technology KNX disposes over all IoT features. KNX devices can be seen as physical objects, which are clearly identifiable and able to exchange data. The media TP, RF, PL and IP take care of the network connectivity. KNX itself is an “Internet of Things”. Amongst others the main features of this decentrally organized bus system are the compatibility of the devices and the possibility to communicate with each other. This ensures for the installations e.g. a high degree of availability.

KNX is a „Thing“ in the Internet since long time

Is a KNX installation itself also a „Thing“ in the internet? For more than ten years KNX IP enables the communication of KNX applications via IP-based networks. For this a KNX IP router ensuring two important functionalities is required. On one hand it allows the interconnection of any remote KNX installations or parts thereof via an IP network (routing), on the other hand it enables the IP based access of a terminal device to a KNX installation (tunneling). Thus, KNX tunneling is the technique used by web clients, visualization computers and smartphones to communicate with KNX devices and finally to realize an attractive operation possibility for the end user.

KNX communication and internet since long have been the state of the art. However: It requires the technical expertise of KNX installers combined with the effort for the parameterization. That is, as a general rule, no problem for KNX installers but in fact already for IT experts. Standardization does not exist. If one tries to access from the world of internet to the “Thing” KNX, i.e. the building automation, in a simpler way, new ways have to be opened.

Web Services and Building Automation

The situation is different from the point of view of the internet: Many different subsystems have to be integrated and KNX is one of them. Building automation is an unknown terrain for IT experts. The ideal solution for this sector would be a translator connecting both worlds without the need for each party to learn the strings of the other side.

KNX Association has recognized this trend of the times and developed the corresponding solution “KNX Web Services” (KNX WS). It orientates itself towards the existing realized web services like oBIX, OPC UA and BACnet-WS. Web services are self-contained modular software components that can be described, published and activated via the web. Usually they are employed by applications and not by persons. Thus, a simple and multi-faceted communication between web services and systems of building automation is possible.

A Gateway maps the KNX Project

The solution KNX IoT is realized via gateways between the KNX network and the world of internet. On one side operation panels, building management, smartphone and others communicate via web services with the gateway. Thus, the app of a web client is able to search data in the web service gateway with unified text telegrams and to transfer them. On the other side the accustomed KNX protocol has to be found. However, in order to recognize from the side of the IP infrastructure the parameters of the KNX system the ETS project has to be exported into the KNX WS-Gateway. For this purpose the new ETS Exporter App is available. The KNX installer has got the possibility to export all project data or only parts of it. When doing so the parameters have to be clearly marked. Also supplementary data can be transferred.

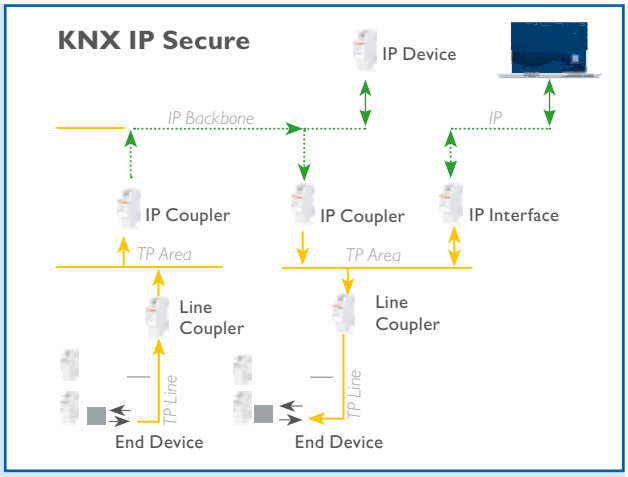
More Benefits by open Data Exchange

By KNX IoT the building automation resp. the smart home comes closer to the virtual world of the internet. It becomes simpler to use data thereof for automated functions, to present values and states of a KNX installation via the internet and to evaluate them. Just think of sensor values and consumption data of energy usage, which can help to optimize the energy management. The open data exchange between IT systems and building automation systems enables improved applications with high multiple benefits.

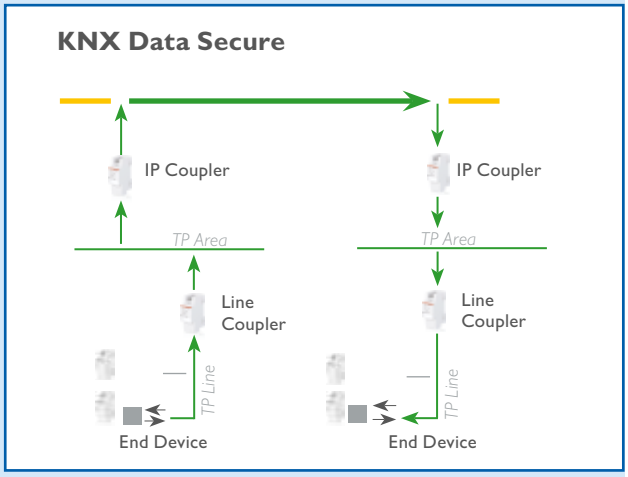
KNX Secure – Secured KNX Communication

KNX IP Secure and KNX Data Secure provide secured access to KNX Installations

They exist – the hackers – who intrude in building technology. Jesters switch on the lights at the neighbor's and boast of it. However, criminal energy and related know-how can cause immense damage. Therefore KNX Security is a red-hot subject. Already up to now KNX complies with the security requirements, as long as installers of Home and Building Control take care of the recommended protective measures against manipulations. Yet, new media like LAN and WLAN with internet access, wireless operation concepts and applications in sensible areas increase the risk of damage by unwanted intruders. According to these but also to other requirements KNX has developed new security concepts: KNX Data Secure and KNX IP Secure. Both of them are based on worldwide established security protocols and can be integrated seamlessly into existing KNX systems.



KNX IP Secure for secured KNX transmission between buildings



KNX Data Secure secured KNX transmission within the building

The safety requirements of KNX installations are growing. Critical and confidential information is increasingly transmitted due to extended application areas. These are for instance:

- information on consumption data that should not be seen by third parties,
- signals of locking systems (e.g. door contacts) which have to be protected against manipulation,
- KNX devices for critical functions, which only shall communicate with authenticated participants,
- data protection in security applications; here the code for the access system or even for setting/unsetting an alarm system may only be sent in encrypted and not in clear form.

How to protect in future even better media and devices of KNX installations will be an increasing challenge for planners, installers and manufacturers. For that reason KNX has developed the new system extensions KNX IP Secure and KNX Data Secure.

Established KNX Security

Basis of each KNX security concept is the careful protection of the system against unauthorized access. Thus, only installers and users are allowed to get physical access to KNX installations. Devices and bus cables Twisted Pair (or IP) have to be mounted in such a way that they are protected against unauthorized access. For particular in sensitive areas like outdoor facilities, separate lines with active filter tables are a solution. Powerline(PL)-lines can be separated by band elimination filters. In order to stay on the safe side unwanted resp. for a function unnecessary communication has to be reduced as far as possible by the configuration of the routers and couplers. If done so potentially sabotaged parameters and devices brought in from outside can only be active within the related line. If KNX has to be coupled with security systems, VdS approved KNX devices or a strict separation by interfaces are possible solutions. When using the internet protocol KNX IP a separate LAN or WLAN should be self-evident. Further the standard security mecha-

nisms for IP networks have to be applied. If there is a direct connection to the internet, the communication has to be appropriately protected. Also here KNX offers an answer with KNX Secure interfaces. In future also a new KNX specified interface will increase via web services the security of the communication between KNX and the internet.

Double Protection Concept

Especially the possibility to remotely control KNX installations via the internet and/or via the wireless network WLAN requires additional protective measures. Due to the access to devices and media exists the risk of manipulation of the data traffic. Thus it is necessary to protect the transmitted information on each medium (KNX TP, PL, RF, IP) against modification or logging telegrams and repeating them in a manipulating way from outside. The remote access to a KNX bus system via the internet should be secured in such a way, that the operation and the configuration of bus devices can only be done by verifiable authorized persons. It is an effective protective mechanism against manipulation if bus devices can only communicate with each other when they recognize themselves a part of the bus system. According to these and other requirements KNX has developed new security concepts: KNX Data Secure and KNX IP Secure. Both use mechanisms which are e.g. used for the secure data transmission between electricity meters and utility companies.

Encrypted Telegrams

If data have to be sent via the internet the connection between the sending and receiving network can be protected by a virtual private network (VPN). Yet, this does not ensure, that the sender is authorized to configure the bus system or to exchange data with it. Here KNX IP Secure offers additional security by extending the KNX IP protocol in such a way that the transmitted data are completely encrypted. This can be realized even in existing installations with little effort. If data have to be transmitted via KNX only locally, it is sufficient to protect the data by an extension of the bus protocol. The specified protection mechanism KNX Data Secure authentifies and/or encrypts selected KNX telegrams independent of the medium. The keys are allocated to the devices resp. to the objects via ETS. As in one KNX system secured and unsecured applications are possible, it is not necessary to secure all devices. Also existing system components have not to be replaced. Such the effort is kept low and the investment in the KNX bus technology is ensured.

KNX IP Secure and KNX Data Secure are available with the ETS5.5.

IMPORTANT TO KNOW

- In a KNX installation KNX IP secure and KNX KNX Data Secure can be used in parallel.
- In a KNX installation secured and unsecured applications can be used in parallel, i.e. not all devices have to be secured.
- The new security functions can be integrated seamlessly in existing installations.
- KNX IP Secure and KNX Data Secure will be available with the ETS5.5

Security Protocol worldwide established

In future the newly specified protection mechanisms KNX Data Secure and KNX IP Secure will allow the creation of secured communication channels between KNX participants. Thus the infiltration of manipulated messages in order get control of the system can be inhibited. For this purpose each message is equipped with an authentification code. The automatic allocation of sequence numbers resp. the sequence identification prevents from the attempt to log data and to re-transmit it later on for sabotage purposes. Finally the encryption of the data traffic makes the KNX installation almost invulnerable. The procedure is based on worldwide established security protocols.

Introduction with ETS5.5

Last but not least planners, installers and system integrators have to pay attention, that hackers do not have any chances. They have to become familiar with the protection measures and to apply them. While handing over the system as well as by periodic verification of the running system the envisaged security level can be ensured. The new security functions, especially for the access via the internet, can be applied to existing systems by using interfaces with the new KNX security mechanisms. KNX IP Secure and KNX Data Secure will be supported by the new ETS5.5 planning and commissioning software.

Checklist for increased security within KNX installations

FUTHER INFORMATION

Further information on the subject KNX security can be found on our website under Download > Marketing > Flyer (http://www.knx.org/knx-en/downloads/index.php)

- *KNX Security Checklist*
- *KNX Security Position paper*

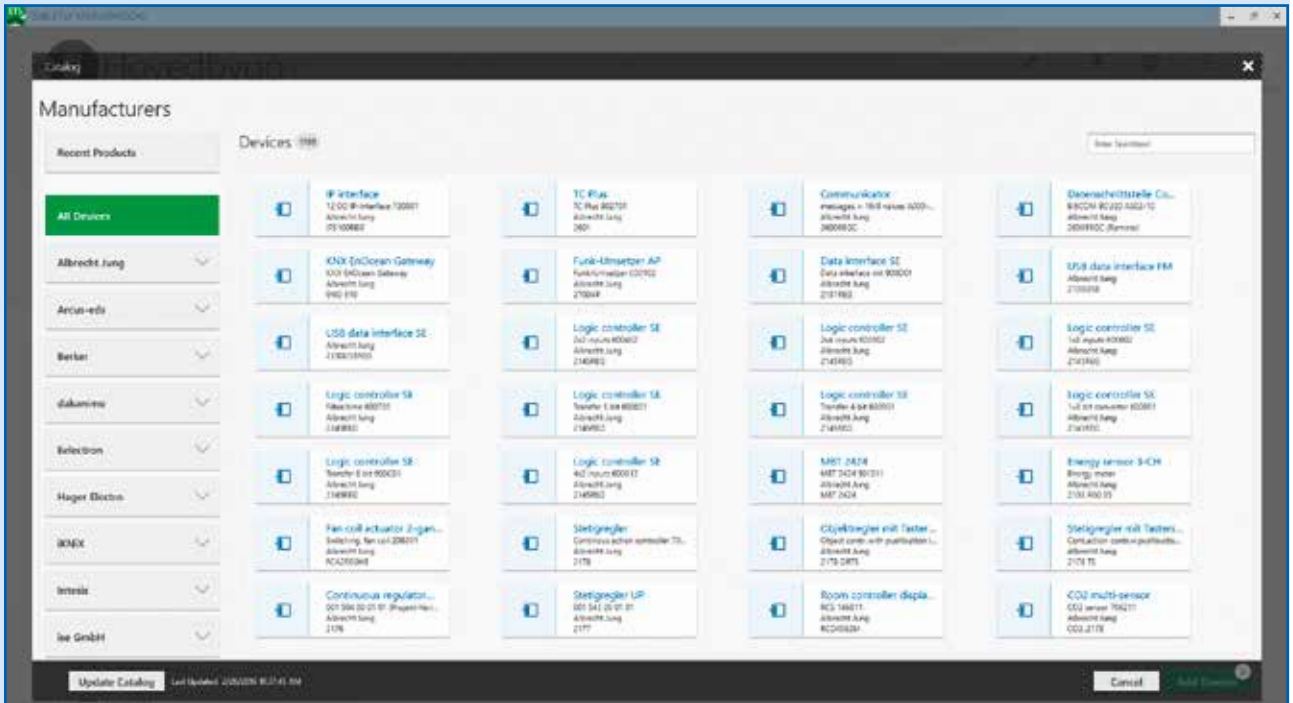
The complementary webinar „KNX Security“ informs you currently on the required protection measures for your KNX installation. Registration under: http://www.knx.org/knx-de/schulung/knx-eacademy/webinars/index.php

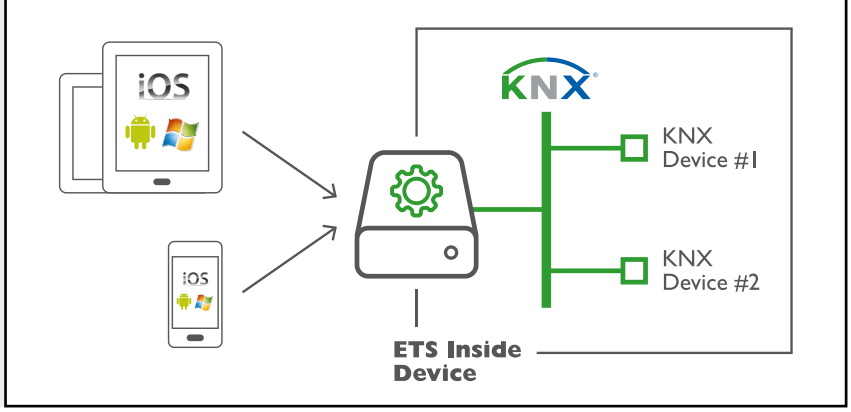
The new ETS Inside – Smart, Simple, Safe

ETS Inside opens up exciting perspectives in the growing smart home market

The advantage of intelligent functions in the home has found its way into the minds of most people. Smart Home is on everyone's lips and the market stands before breakthrough. Therefor KNX releases the new ETS Inside. Even installers with little experience in building automation are able to create KNX projects fast and easily when using this tool for small and medium sized projects. The inhabitants will be delighted, too: They experience their intelligent home by becoming active themselves and by adapting functions to their own needs. That's because ETS Inside is a fixed part of the KNX installation und always up-to-date on site. The easily understandable user interface actually runs on tablets and smart phones. Even – just by a touch – the remote control of one's home is possible. Nevertheless the project is protected against unauthorized access.

Intelligent design, minimalistic lay out, understandable symbols – via the new user interface parameters can be set by a simple touch.





Basic principle of a decoupled user interface: Intelligent and simple parameterization via tablet or smartphone. Tool- and project-software are located within the ETS Inside device.

KNX has proved its investment security since many years in a countless number of projects. Openness, compatibility, flexibility and last but not least the common tool ETS, currently version 5, belong to its secrets of success. The well proven ETS Professional allows realizing all KNX installations and all sizes of projects. Knowledge and practice can be acquired in certified KNX training centers. But, in the smart home market exist also smaller projects requiring less sophisticated configuration work. Thus, ETS Inside is congenial for all installers, who do not have building automation in their service portfolio or just do it occasionally. ETS inside allows the realization of KNX projects in a simple way and does not require extensive training.

Operation and ETS Data decoupled

It is a basic principle of ETS Inside to decouple the user interface from the ETS data. This allows the editing of projects on all common operating systems. The underlying KNX basic software is installed in the ETS Inside device being a part of the installation. This hardware contains also the KNX project and offers a web server for a decoupled user interface. Due to this new concept – in contrast to the Windows based ETS Professional – projects can be edited on tablets and smartphones with diverse operating systems, like e.g. iOS, Android or Windows.
The range of operation functionalities of ETS Inside matches the use cases. It is possible to design and to commission small and medium sized projects. This complies with average KNX applications in residential, commercial and public buildings. All media (TP, IP, RF and PL) are supported.
At any time projects created with ETS Inside can be synchronized with ETS Professional, e.g. in order to extend a KNX installation with devices, the topology with some further lines or to use devices requiring very extensive parameterization.

Smart – Finger tap instead of mouse click

The new ETS Inside is suitable for the today commonly used and simply to handle tablets and smartphones. The new user interface organized in a minimalistic way is adapted to the displays of iPads, iPhones, Android tablets, Windows tablets etc. and offers an intelligent design. The flat buttons with easily understandable symbols enable an intuitive operation. Parameterization is very simple even with smartphones because ETS Inside is touch sensitive.

Simple – A Tool for Installers and End Users

Installers and end users benefit from ETS Inside. KNX projects can be realized cost-efficient and in an easy way. It is also possible that a system integrator designs the project with ETS Professional and synchronizes it later on with the Inside device. Thereafter the responsible electrical installer maintains the project for his customer. A further topic favors ETS Inside: End customers can ask their electrical installer to unblock certain parameters in order to make smaller modifications by themselves at any time. Thus e.g. dimming values, time schedules, light scenes etc. can be modified by themselves and adapted to their own preferences without the need for calling a craftsman.

Safe – No unauthorized Access

ETS Inside offers a triple protection:

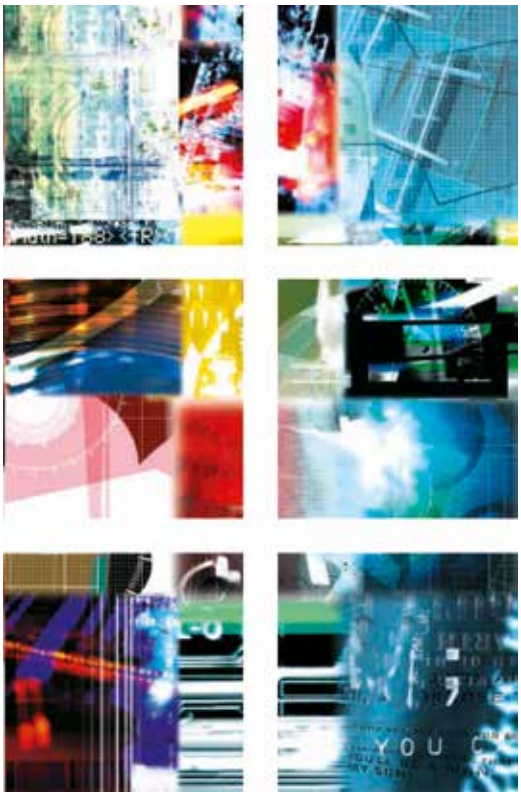
- In order to edit a project log-in data have to be entered previously. Thus unauthorized persons are not able to get access to the ETS Inside device.
- To keep the warranty the electrical installer decides in agreement with his customer which parameters he will unblock for him. Usually these will affect any security related functions.
- Last but not least ETS Inside supports the new KNX Secure concept. Thus hackers have not got a chance even here.

Inside
ETS

ETS INSIDE OFFERS CONVINCING ARGUMENTS

1. ETS Inside offers to installers, who up to now have worked only a little bit with KNX, an uncomplicated entrance to the more and more broadened smart home market.
2. The principle of a user interface decoupled from ETS allows the usage of popular tablets and smartphones.
3. ETS Inside is fixed part of the installation and is available on site always with the latest version.
4. Electrical installers can unblock certain parameters for editing by the end customer.
5. The project can be synchronized with ETS Professional at any time.
6. Under certain circumstances existing KNX Installations can be retrofitted with ETS Inside.

ETS Inside will be available from October 2016. For each installation a license is required.



www.knx.org