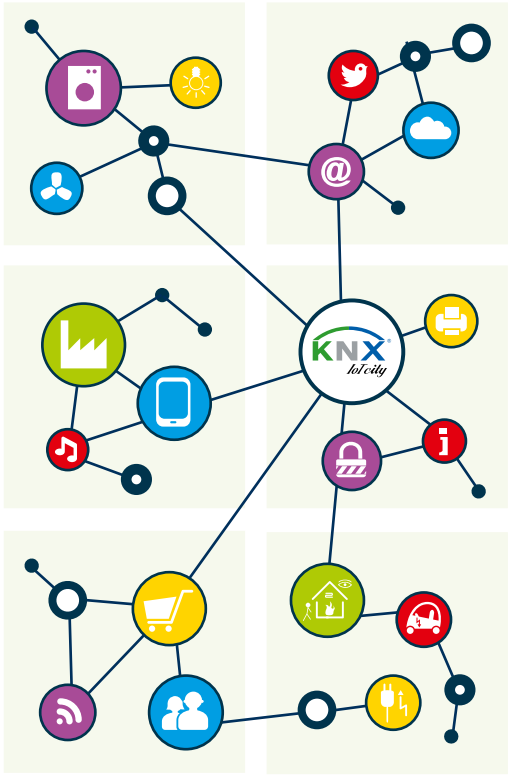


KNX News

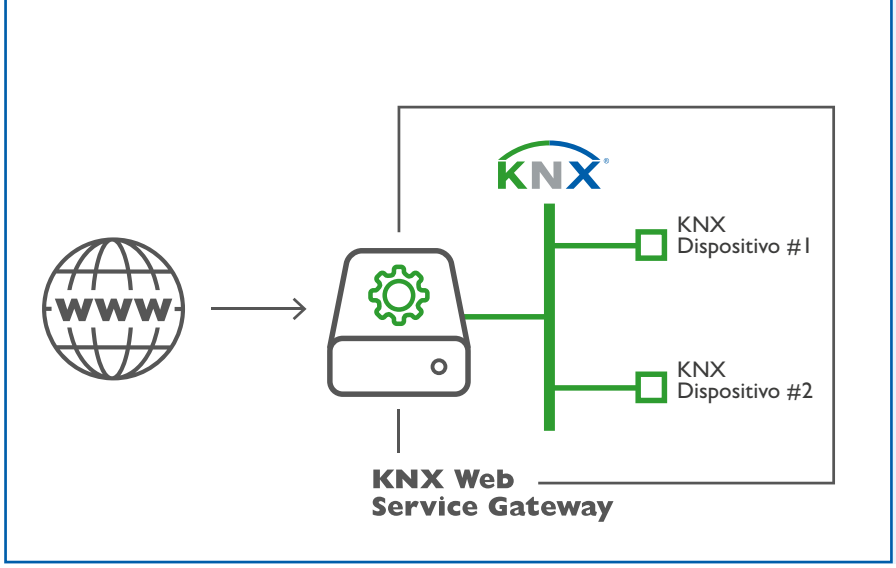
KNX Internet delle Cose,
KNX Sicuro,
ETS Inside

KNX Internet delle Cose

KNX e Internet delle Cose –
una semplice integrazione da KNX Web Services

L' "Internet delle Cose" è diventata una parola d'ordine nella tecnologia dell'informazione. Sebbene debba ancora entrare nella cultura generale è già un termine noto da tempo tra gruppi di esperti dedicati a dare un nuovo impulso allo sviluppo tecnologico. Ogni giorno gli oggetti diventano intelligenti e comunicano via internet. Secondo alcuni visionari nel 2020 ci saranno 50 miliardi di tali oggetti che comunicheranno via internet. Tuttavia, l'Internet delle Cose non è qualcosa ancora nell'aria ma è diventato una realtà già oggi. Già da lungo tempo lo Standard KNX forma parte di questo mondo globale dell'IoT. Dall'introduzione delle KNX Web Services KNX sottolinea la sua posizione di leader e apre nuove vie nell'operatività e nella visualizzazione dei sistemi KNX.

Da lungo tempo l'Internet delle Cose (IoT) ha trovato la sua strada in quasi tutti ambiti della vita – anche nell'automazione degli edifici. Attori globali come Google o Apple vogliono penetrare questo mercato del futuro cercando di enfatizzare la loro filosofia di edificio intelligente tramite prodotti connessi in rete come sensori fumo, termostati, rilevatori di movimento o prese comandate. Ma quando l'utente cerca di trovare una soluzione nel vasto numero di sistemi presenti sul mercato spesso trova più problemi che risposte. Per esempio il contatto finestra cablato di un sistema A non è in grado di comunicare con l'attuatore per valvole wireless del costruttore B. Oltre a queste incompatibilità, risultante dalle differenze che ci sono tra i protocolli e i mezzi trasmissivi, un ulteriore aspetto dimostra essere un notevole svantaggio: le soluzioni di automazione proprietarie normalmente richiedono un server centrale per lo scambio dei dati tra i componenti installati, i quali non possono comunicare direttamente tra di loro come è invece possibile con KNX. Questo può essere costituito da un piccolo computer, uno smartphone o anche una soluzione basata su cloud. E' un van-



taggio di questo approccio che i dati siano disponibili in ogni luogo tramite siti web, d'altro lato però è anche il tallone d'Achille della rete. Se il server dovesse cadere, il controllo dell'edificio di conseguenza anch'esso subirebbe una interruzione.

KNX è una Rete di „Cose"

Cosa significa il termine realmente "Internet delle Cose"? Wikipedia lo definisce circa nel modo seguente: Esso descrive la connessione di oggetti fisici chiaramente identificabili con il mondo virtuale di internet. A tale scopo i "dispositivi" contengono elettronica, software, sensori e la relativa connettività di rete. Ciascun oggetto ha un indirizzo chiaramente identificabile ed è in grado di ricevere, raccogliere, analizzare e spedire dati.
Sin dall'inizio la tecnologia, KNX già dispone di tutte queste caratteristiche richieste da IoT. I dispositivi KNX possono essere visti come oggetti fisici, chiaramente identificabili e in grado di scambiare dati tra di loro. I mezzi trasmissivi TP, RF, PL e IP si prendono cura della connettività di rete. KNX stesso è un "Internet delle Cose". Tra le altre le principali caratteristiche relative alla organizzazione decentralizzata del sistema bus sono la compatibilità dei dispositivi e la possibilità che comunichino tra di loro. Questo da maggiore garanzia agli impianti, ad esempio per l'elevato livello di disponibilità.

KNX è una „Cosa" in Internet da molto tempo

Una installazione KNX è essa stessa una "Cosa" in internet? Da più di dieci anni KNX IP garantisce la comunicazione di applicazioni KNX tramite reti IP. Per questo un router KNX IP assicura due importanti funzionalità richieste. Da un lato permette la interconnessione di ogni installazione KNX remota o loro parti tramite una rete IP (routing), dall'altro abilita l'accesso basato su IP di un dispositivo terminale a una installazione KNX (tunneling).
Di conseguenza, KNX tunneling è la tecnica utilizzata dai client web, computer di visualizzazione e smartphone per comunicare con dispositivi KNX al fine di realizzare una applicazione attraente per l'utente finale.
La comunicazione tra KNX e internet sono da lungo tempo lo stato dell'arte. Tuttavia: essa richiede degli installatori esperti di KNX per la parametrizzazione. Ovvero, come regola generale, nessun problema per gli installatori KNX ma se sono già esperti di IT. La standardizzazione non esiste. Se qualcuno cerca di accedere dal mondo di internet alle "Cose" KNX, es. l'automazione degli edifici, in un modo più semplice, devono essere aperte nuove strade.

Web Services e Building Automation

La situazione è differente dal punto di vista di internet. Molto sottosistemi diversi devono essere integrati e KNX è uno di loro. La Building Automation è un terreno sconosciuto per gli esperti di IT. La soluzione ideale per questo settore potrebbe essere un traduttore che colleghi i due mondi senza la necessità di ciascuna delle parti di apprendere le regole dell'altra parte.
KNX Association ha riconosciuto questo trend da tempo e ha sviluppato la corrispondente soluzione "KNX Web Services" (KNX WS). Essa orienta se stessa verso i servizi web esistenti come oBIX, OPC UA e BACnet-WS. I web services sono componenti software modulari autonomi che possono essere descritti, pubblicati e attivati via web. Solitamente essi sono impiegati dalle applicazioni e non da persone. Dunque, una comunicazione semplice e multiforme tra i servizi web e i sistemi di building automation è oggi possibile.

Un Gateway mappa il Progetto KNX

La soluzione KNX IoT è realizzata tramite gateways tra la rete KNX e il mondo di internet. Da un lato pannelli operativi, la gestione dell'edificio, gli smartphone o altri comunicano via sevizi web con il gateway. Di conseguenza, la app di un client web è in grado di trovare i dati nel gateway web service con telegrammi di testo unificati e trasferirli. Dall'altro lato deve essere trovato il protocollo abituale KNX. Tuttavia, per riconoscere dal lato dell'infrastruttura IP i parametri del sistema KNX deve essere esportato il progetto ETS nel KNX WS-Gateway. A questo proposito c'è la nuova App ETS Exporter a disposizione. L'installatore KNX ha la possibilità di esportare tutti i dati di progetto o solo una parte. Nel fare questo, i parametri devono essere chiaramente identificati. Possono essere trasferiti anche altri dati supplementari.

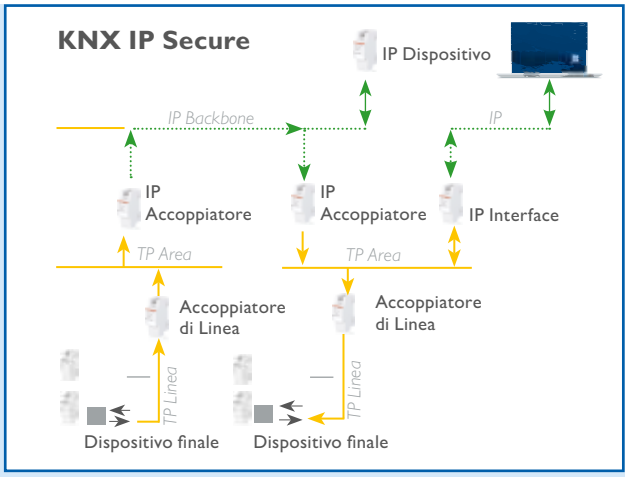
Maggiori benefici da uno Scambio Dati aperto

Con KNX IoT la building automation rispetto alla smart home diventa più vicino al mondo virtuale di internet. Diventa più semplice utilizzare i dati per le funzioni di automazione, presentare i valori e gli stati a un impianto KNX tramite internet e valutarli. Pensando ad esempio ai valori trasmessi da sensori relativi a dati di consumo energetico, possiamo ottimizzare al meglio la gestione dell'energia. Uno scambio dati aperto tra i sistemi IT e i sistemi di building automation permette di migliorare le applicazioni con molteplici benefici.

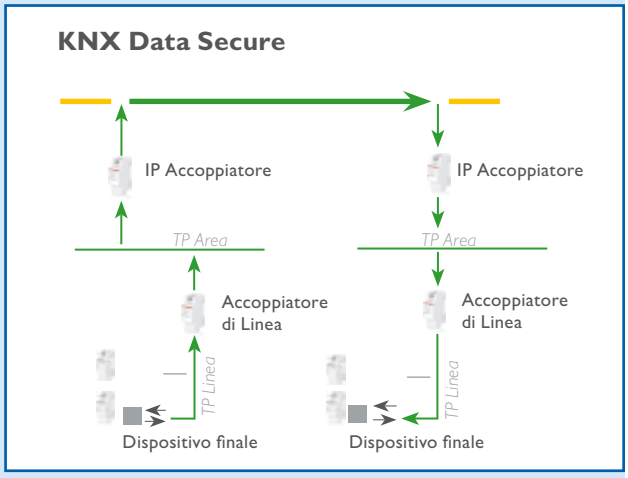
KNX Secure – La Comunicazione Sicura di KNX

KNX IP Secure e KNX Data Secure forniscono un accesso sicuro agli impianti KNX

Esistono - gli hacker - che si intromettono nei sistemi di automazione degli edifici. Dei beffardi individui che accendono le luci al vicino di casa e si vantano per questo. Tuttavia, una intenzione criminale e un relativo know-how possono causare un danno immenso. Pertanto per KNX la sicurezza è un tema rovente. Già fino ad ora KNX è conforme ai requisiti di sicurezza, a patto che gli installatori di sistemi di automazione degli edifici si prendono cura delle misure di protezione consigliate contro le manipolazioni. Tuttavia, i nuovi media come LAN e WLAN con accesso ad internet, i concetti di funzionamento wireless e applicazioni in aree sensibili aumentano il rischio di danni da parte di intrusi indesiderati. Per questo ma anche per soddisfare altri requisiti KNX ha sviluppato nuovi concetti di sicurezza: KNX Data Secure e KNX IP Secure. Entrambi si basano su protocolli di sicurezza consolidati in tutto il mondo e possono essere integrati perfettamente nei sistemi KNX esistenti.



KNX IP Secure per una trasmissione KNX sicura tra gli edifici



KNX Data Secure per una trasmissione sicura dentro l'edificio

I requisiti di sicurezza degli impianti KNX stanno crescendo. Informazioni critiche e confidenziali sono sempre più trasmesse attraverso aree applicative estese. Esse sono ad esempio:

- informazioni su dati di consumo che possono essere viste da terze parti,
- segnali dai sistemi di controllo accesso (es. contatti porta) che devono essere protetti contro le manipolazioni,
- dispositivi KNX dedicati a funzioni critiche, che devono essere comunicate solo a persone autenticate
- la protezione dei dati nelle applicazioni di sicurezza; il codice per il sistema antintrusione o anche per impostare o disattivare un sistema di allarme deve essere trasmesso in forma criptata e non in chiaro.

Come proteggere ancor meglio in futuro le reti e i dispositivi KNX negli impianti sarà una sfida crescente per i progettisti, gli installatori e i costruttori. Per questa ragione KNX ha sviluppato le nuove estensioni del sistema denominate KNX IP Secure e KNX Data Secure.

KNX Security consolidato

La base del concetto KNX di sicurezza è l'attenzione alla protezione del sistema contro accessi non autorizzati. Di conseguenza, solo gli installatori e gli utenti sono autorizzati ad avere accesso fisico agli impianti KNX. I dispositivi e i cavi bus TP (o IP) devono essere installati in modo tale da essere protetti contro intromissioni. In particolari aree sensibili come le strutture esterne, linee separate con tabelle filtro attive offrono una soluzione. Le linee powerline (PL) possono essere separate da filtri di banda. Con lo scopo di mantenersi maggiormente protetti meglio ridurre le comunicazioni non necessarie tramite la configurazione corretta dei router e degli accoppiatori. Facendo cosi un ipotetico sabotaggio esterno di qualcuno che vuole accedere ai parametri di sistema o ai dispositivi rimarrebbe limitato alla singola linea interessata e non si estenderebbe a tutto l'impianto. Se KNX è accoppiato con sistemi di sicurezza, dispositivi KNX approvati da VdS (ndt. VdS è un'impresa dell'Associazione tedesca delle compagnie assicuratrici GDV che opera come ente di certificazione indipendente per le tecnologie dedicata alla sicurezza in Germania, per l'Italia fare riferimento agli enti

preposti) o rigide separazioni tramite interfacce sono soluzioni possibili.
Quando si usa il protocollo internet KNX IP dovrebbe essere dedicata una LAN o WLAN separata. Ulteriori meccanismi di sicurezza per le reti IP devono essere applicati. Se c'è una connessione diretta a internet, la comunicazione deve essere appropriatamente protetta. Anche qui KNX offre una risposta con le interfacce KNX Secure. In futuro anche una nuova specifica interfaccia KNX aumenterà via web services la sicurezza della comunicazione tra KNX e internet.

Concetto di Doppia Protezione

La possibilità di controllare da remoto gli impianti KNX tramite internet e/o reti wireless WLAN richiede in particolar modo misure di protezione addizionali. Data la possibilità di accesso agli impianti KNX o alle reti esiste il rischio di manipolazioni del traffico dati. Di conseguenza è necessario proteggere le informazioni trasmesse su ciascun mezzo trasmissivo (KNX TP, PL, RF, IP) contro le modifiche o la registrazione di telegrammi o la loro manipolazione dall'esterno. L'accesso remoto al sistema bus KNX tramite internet dovrebbe essere assicurato in modo tale da consentire le operazioni di configurazione e modifica dei dati di impianto solo alle persone autorizzate. E' un meccanismo di protezione efficace contro le manipolazioni se i dispositivi bus possono comunicare tra di loro quando essi si riconoscono parte dello stesso sistema. Secondo questi e altri requisiti, KNX ha sviluppato nuovi concetti di sicurezza: KNX Data Secure e KNX IP Secure. Entrambi usano meccanismi che sono usati, ad esempio, nella trasmissione di dati in sicurezza dei contatori delle le compagnie fornitrici di energia e le utilities.

Telegrammi Criptati

Se occorre spedire dei dati tramite internet la connessione tra trasmettitore e ricevitore connessi in rete può essere protetta da una rete privata virtuale (VPN). Tuttavia, questo non assicura che il trasmettitore sia autorizzato a configurare il sistema bus o a modificarne i dati. Qui KNX IP Secure offre una sicurezza addizionale estendendo il protocollo KNX IP in modo tale che i dati trasmessi sono completamente criptati. Questo può essere realizzato anche negli impianti esistenti con un piccolo sforzo. Se i dati devono essere trasmessi tramite KNX solo localmente, è sufficiente proteggere i dati tramite una estensione del protocollo bus. Il meccanismo specifico di protezione KNX Data Secure autentica e/o cripta telegrammi KNX selezionati a prescindere dal tipo di rete usata. Le chiavi sono allocate ai dispositivi in riferimento agli oggetti tramite ETS. Dal momento che nel medesimo sistema KNX sono ammesse applicazioni sicure e non sicure, non è necessario mettere in sicurezza tutti i dispositivi. I dispositivi esistenti inoltre non devono essere sostituiti. Tale sforzo è mantenuto basso e l'investimento nella tecnologia bus KNX è assicurata.

KNX IP Secure e KNX Data Secure sono implementati in ETS5.5.

E' IMPORTANTE SAPERE

- In una installazione KNX, KNX IP secure e KNX KNX Data Secure possono essere usati in parallelo.
- In una installazione KNX applicazioni sicure e insicure possono essere usate in parallelo, ovvero non tutti i dispositivi debbono per forza essere messi in sicurezza.
- Le nuove funzioni di sicurezza possono essere integrate senza problemi negli impianti esistenti.
- KNX IP Secure e KNX Data Secure saranno disponibili dalla versione ETS5.5

Protocollo di Sicurezza consolidato a livello mondiale

In futuro i nuovi meccanismi di protezione specificati da KNX Data Secure e KNX IP Secure permetteranno la creazione di canali di comunicazione sicuri tra i dispositivi partecipanti al sistema KNX. Allora l'infiltrazione di messaggi manipolati con lo scopo di prendere il controllo del sistema possono essere inibiti. Per questo scopo ciascun messaggio è equipaggiato con un codice di autenticazione. L'allocazione automatica di sequenze di numeri soggetti ad una identificazione previene il tentativo di registrare o ritrasmettere i telegrammi successivamente a scopo di sabotaggio. Alla fine la criptazione dei dati rende gli impianti KNX pressoché invulnerabili. La procedura è basta su protocolli di sicurezza consolidati a livello mondiale.

L'introduzione in ETS5.5

Infine, progettisti, installatori e integratori di sistema devono prestare attenzione affinché gli hackers non abbiano alcuna chance. Devono diventare familiari con le nuove misure di protezione e applicarle. All'atto del collaudo di un sistema cosi come durante la manutenzione periodica deve essere assicurato il livello di sicurezza previsto. Le nuove funzioni di sicurezza, specialmente per quanto riguarda l'accesso tramite internet, possono essere applicate ai sistemi esistenti usando delle interfacce con i nuovi meccanismi di sicurezza KNX a bordo. KNX IP Secure e KNX Data Secure saranno supportati dalla nuova versione del software di progettazione e messa in servizio ETS5.5.

Lista di controllo per una maggiore sicurezza all'interno di installazioni KNX

ULTERIORI INFORMAZIONI

Ulteriori informazioni su KNX Security possono essere trovate nel nostro sito web sotto Download > Marketing > Flyer
www.knx.org/knx-it/downloads/
- *KNX Security Checklist*
- *KNX Security Position paper*

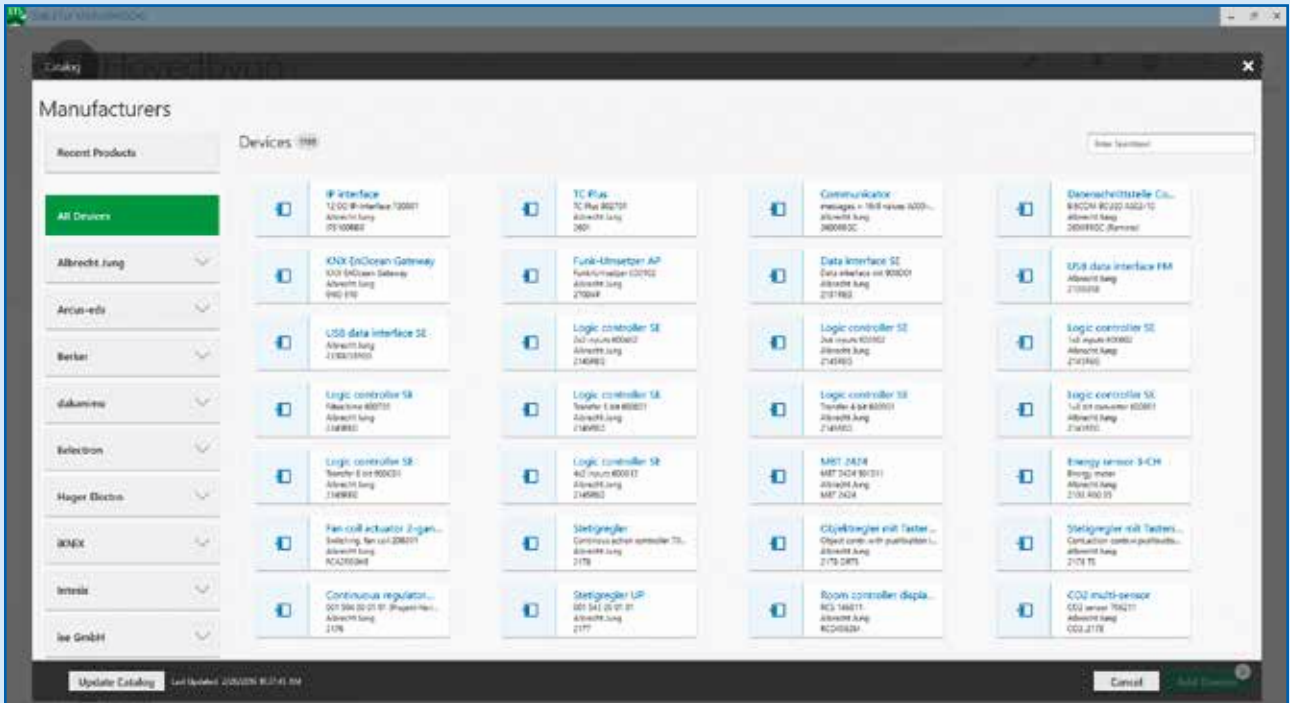
Il webinar complementare „KNX Security" vi informa sulle attuali misure richieste per proteggere i vostri impianti KNX.
Registrazione qui:
www.knx.org/knx-it/formazione/knx-eacademy/webinars/

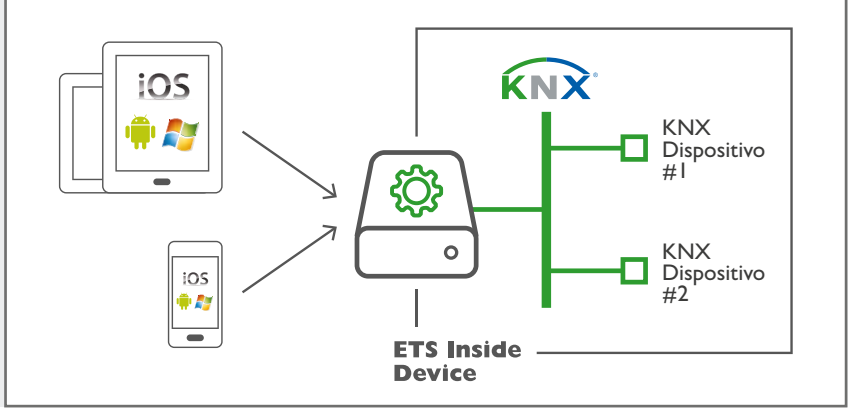
Il nuovo ETS Inside – Smart, Semplice, Sicuro

ETS Inside apre entusiasmanti prospettive nella crescita del mercato della smart home

Il vantaggio delle funzioni intelligenti in casa ha trovato la sua strada nella mente della maggior parte delle persone. Smart Home è sulla bocca di tutti e il mercato è di fronte a una svolta. Per questo KNX rilascia il nuovo ETS Inside. Anche installatori con poca esperienza nei sistemi di automazione degli edifici sono in grado di creare progetti KNX velocemente e facilmente quando utilizzano questo strumento per progetti di piccole e medie dimensioni. Gli utenti saranno anche felici: essi potranno sperimentare la loro casa intelligente, diventando attivi essi stessi e adattano le funzioni alle proprie esigenze. Questo perché ETS Inside è una parte fissa dell'installazione KNX e resta sempre aggiornata in loco. L'interfaccia utente di facile comprensione funziona su tablet e smartphone. Anche semplicemente con un tocco - il controllo remoto della propria casa è possibile. In ogni caso, il progetto rimane protetto da accessi non autorizzati.

Design intelligente, layout minimalista, simboli comprensibili – tramite la nuova interfaccia utente i parametri possono essere impostati con un semplice tocco.





Principio base dell'interfaccia utente disaccoppiata: parametrizzazione intelligente e semplice tramite tablet o smartphone. Lo strumento di progettazione è integrato nel dispositivo ETS Inside.

KNX ha testato il suo investimento in sicurezza da molti anni in un numero infinito di progetti. L'apertura, la compatibilità, la flessibilità e non ultimo, l'utilizzo di uno strumento comune di progettazione ETS, giunto alla attuale versione 5, sono alla base dei segreti di questo successo. L'ormai consolidato e collaudato ETS Professional permette di realizzare installazioni KNX e progetti di tutte le dimensioni. La conoscenza e la pratica possono essere acquisite in centri di formazione KNX certificati. Ma nel mercato della Smart Home esistono anche piccoli progetti che richiedono un lavoro di configurazione meno sofisticato. Allora, ETS Inside è congeniale per tutti quegli installatori che non devono essere necessariamente coinvolti nel mercato della building automation oppure che ne accedono solo occasionalmente. ETS Inside permette di realizzare progetti KNX in un modo semplice senza richiedere una formazione estensiva.

Disaccoppiamento tra Operatività e Dati ETS

E' un principio base di ETS Inside disaccoppiare l'interfaccia utente dai dati ETS. Questo permette la modifica di progetti su tutti i sistemi operativi. Il software di base di KNX è installato nei dispositivi ETS Inside come una parte dell'impianto. Questo hardware contiene anche il progetto KNX e offre un web server per disaccoppiare l'interfaccia utente. Grazie a questo nuovo concetto – in contrasto con ETS Professional basato su Windows – i progetti possono essere editati su tablet e smartphone con diversi sistemi operativi, come ad esempio iOS, Android o Windows.

Il range delle funzionalità di ETS Inside incontra le varie necessità d'impiego. E' possibile progettare e mettere in servizio piccoli e medi progetti. Questo soddisfa i requisiti della media delle applicazioni KNX negli edifici residenziali, commerciali e pubblici. Sono supportati tutti i tipi di rete (TP, IP, RF e PL).

In ogni momento i progetti creati con ETS Inside possono essere sincronizzati con ETS Professional, esempio per estendere una installazione KNX con nuovi dispositivi, la topologia dell'impianto con ulteriori linee o usare dispositivi richiedenti una parametrizzazione estensiva.

Smart – Un tocco del dito al posto del click del mouse

Il nuovo ETS Inside è adatto per l'uso comune odierno ed è semplice da usare con tablet e smartphones. La nuova interfaccia utente organizzata in maniera essenziale si adatta ai display di iPads, iPhones, Android tablets, Windows tablets ecc. e offre un design intelligente. I pulsanti con simboli facilmente comprensibili aiutano l'utente ad operare intuitivamente. La parametrizzazione è molto semplice anche con gli smartphone perché ETS Inside è sensibile al tocco.

Semplice – Uno strumento per installatori e utenti finali

Installatori e utenti finali beneficeranno entrambi di ETS Inside. I progetti KNX possono essere realizzati in maniera efficiente e semplice. E' anche possibile che un integratore di sistema sviluppi il progetto con ETS Professional e lo sincronizzi successivamente nel dispositivo con ETS Inside. Successivamente il responsabile dell'installazione elettrica può conservare il progetto per il suo cliente. Un ulteriore elemento a favore di ETS Inside: gli utenti finali possono chiedere al loro installatore elettrico di sbloccare certi parametri per poter effettuare piccole modifiche loro stessi all'occorrenza. Ad esempio, valori di dimmerizzazione, temporizzazioni, scenari luce, ecc..possono essere modificati autonomamente e adattati alle loro mutate circostanze o preferenze senza la necessità di chiamare un tecnico specializzato.

Sicuro – Nessun accesso non autorizzato

ETS Inside offre una tripla protezione:

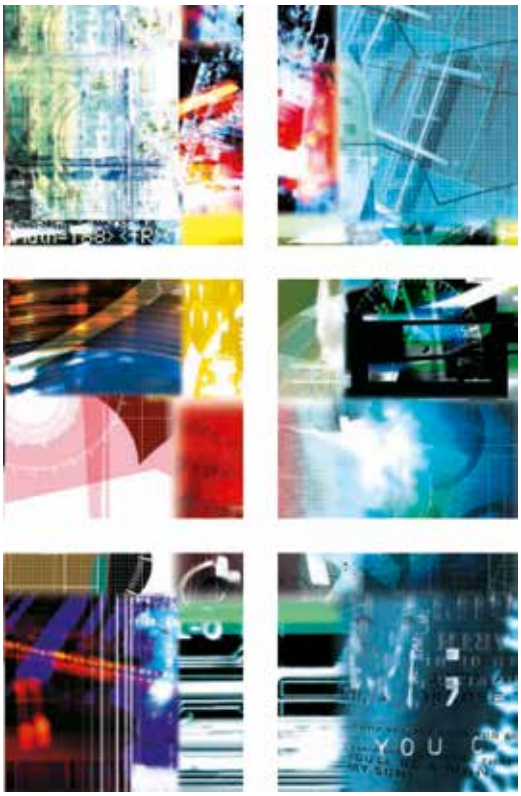
- Se si vuole modificare un progetto occorre inserire dei dati di accesso. Persone non autorizzate non possono accedere ai dispositivi ETS Inside.
- Per mantenere la garanzia sugli impianti l'installatore elettrico può decidere di sottoscrivere un accordo con il suo cliente che specifichi quali parametri vengono sbloccati e messi a sua disposizione. Solitamente questo influenza le relative funzioni di sicurezza.
- Non ultimo, ETS Inside supporta il nuovo concetto KNX Secure. Di conseguenza gli hackers non hanno grandi chance anche qui.

Inside ETS

ETS INSIDE OFFRE INTERESSANTI OPPORTUNITA'

1. ETS Inside offre agli installatori, che sino ad ora hanno lavorato solo con piccoli impianti KNX, un modo semplice per entrare nel sempre più vasto mercato della smart home.
2. Il principio dell'interfaccia utente separata da ETS permette l'utilizzo tramite gli ormai popolari tablets e smartphones.
3. ETS Inside è una parte fissa dell'impianto ed è sempre disponibile in loco con l'ultima versione.
4. Gli installatori elettrici possono sbloccare certi parametri e metterli a disposizione degli utenti finali.
5. Il progetto può essere sincronizzato con ETS Professional in ogni momento.
6. In certe circostanze gli impianti KNX esistenti possono essere equipaggiati con ETS Inside.

ETS Inside sarà disponibile da Gennaio 2017. Per ogni installazione sarà richiesta una licenza.



www.knx.org