KNX Novinky

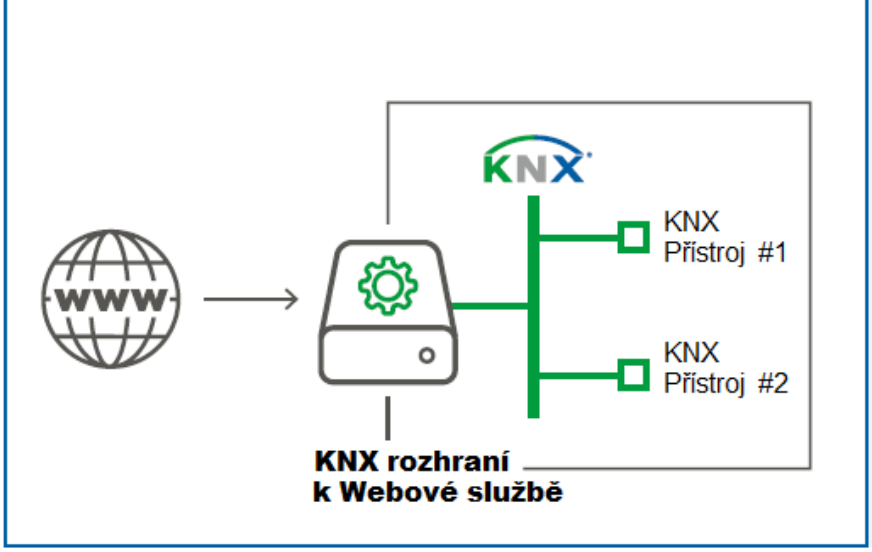
KNX Internet Věcí,
KNX Secure,
ETS Inside

KNX Internet Věcí

KNX a Internet Věcí –
Jednoduchá integrace do KNX Webových služeb

"Internet věcí" je módním slovem ve světě informačních technologií. Co se ještě musí stát součástí všeobecných znalostí, je již dlouho známý termín v expertních skupinách pro nové impulsy vývoje. Předměty každodenní potřeby se stávají inteligentními a komunikují přes internet. Podle vizionářů bude do roku 2020 komunikovat přes internet 50 miliard takových objektů. Nicméně, internet věcí není přeludem, ale je realitou již nyní. Také KNX už dlouhou dobu tvoří součást globálního světa IoT. Zavedením KNX Webových služeb KNX zdůrazňuje svoji vedoucí pozici a otevírá nové možnosti v provozu a vizualizaci KNX systémů.

Již před relativně dlouhou dobou si internet věcí (IoT) našel svou cestu k téměř všem oblastem života - a tedy i k automatizaci budov. Globální hráči jako Google či Apple pronikají do tohoto trhu budoucnosti a pokouší se zdůraznit jejich filozofii inteligentních budov s produkty schopnými pracovat v sítích, jakými jsou snímače kouře, termostatické ventily, snímače pohybu nebo spínané zásuvky. Když se uživatel snaží najít v obrovském počtu systémů vhodné řešení, dostane se více k problémům než k odpovědím. Například pevně připojený okenní kontakt systému A není schopen komunikovat s bezdrátovým pohonem ventilu výrobce B.
Kromě těchto nekompatibilit, vyplývajících z různých protokolů a přenosových médií, další skutečnosti vykazují jejich hlavní nevýhodu: řešení automatizace zařízeními vždy jednoho výrobce se obvykle neobejdou bez centrální jednotky pro výměnu dat mezi instalovanými komponenty, které nemohou komunikovat přímo mezi sebou, jako je to možné v případě KNX. Tou jednotkou může být malý počítač,



chytrý telefon nebo dokonce vzdálený internetový server. Výhodou tohoto přístupu je dostupnost dat prostřednictvím webových stránek v libovolném místě, avšak na druhé straně je to Achillovou patou sítě. V případě, že server selže, řízení budovy selže také.

KNX je sítí „Věcí“

Co vlastně znamená pojem "internet věcí"? Orientační definice z Wikipedie: Je tím popisováno propojení jasně identifikovatelných fyzických objektů s virtuálním světem internetu. Za tímto účelem se k síti připojují související "přístroje" obsahující elektroniku, software, snímače. Každá věc má jasně identifikovatelnou adresu a je schopna přijímat, shromažďovat, vyhodnocovat a odesílat data.
Od počátku je KNX technika vybavena všemi vlastnostmi IoT. Na přístroje KNX lze nahlížet jako na fyzické objekty, které jsou jasně identifikovatelné a jsou schopny výměny dat. Média TP, RF, PL a IP zajišťují připojení k síti. KNX samo o sobě je "Internetem Věcí". Mimo jiné, hlavními rysy tohoto decentralizovaně organizovaného sběrnicového systému jsou kompatibilita přístrojů a možnost komunikovat mezi sebou navzájem. Tím je v instalaci zajištěn např. vysoký stupeň dosažitelnosti.

KNX je „Věc“ na internetu již dlouhou dobu

Je samotná KNX instalace také "Věc" na internetu? Již více než deset let KNX IP umožňuje komunikaci aplikací KNX prostřednictvím sítí založených na protokolu IP. K tomu je zapotřebí KNX IP router zajišťující dvě důležité funkce. Jednak umožňuje propojení všech vzdálených instalací KNX nebo jejich částí přes IP síť (routing), na druhé straně umožňuje IP přístup ke koncovým přístrojům v instalaci KNX (tunneling). KNX tunneling je technika využívající webové klienty, vizualizační počítače a chytré telefony ke komunikaci s KNX přístroji a tím i k realizaci atraktivních ovládacích možností koncovým uživatelem. KNX komunikace a internet již dávno je na aktuálním stavu techniky. Nicméně je podstatné odborné posouzení KNX integrátora v kombinaci se zpracováním parametrizace. To obecně neznamená žádný problém pro KNX instalatéry, ale ve skutečnosti pro odborníky z oblasti IT. Standardizace neexistuje. Jestliže se zkouší jednodušší přístup ze světa internetu k "Věci" KNX, tj. k automatizaci budov, mohou být otevřeny nové cesty.

Webové služby a automatizace budov

Tato situace se liší podle pohledu na internet: Je mnoho různých subsystémů, které mají být integrovány a KNX je jedním z nich. Automatizace budov je neznámé území pro IT odborníky. Ideálním řešením pro tento sektor je být překladatelem propojení obou světů, aniž by bylo nutné učit se tahat za nitky na druhé straně.
V uznání tohoto současného trendu, KNX asociace vyvinula odpovídající řešení "KNX Webové Služby" (KNX WS). To je orientováno směrem stávajících realizovaných webových služeb, jako je oBIX, OPC UA a BACnet-WS. Webové služby jsou samostatnými modulárními softwarovými komponenty, které mohou být popsány, publikovány a aktivovány přes web. Obvykle se zabývají aplikacemi, nikoli osobami. Takto je možná jednoduchá a mnohotvárná komunikace mezi webovými službami a systémy automatizace budov.

Rozhraní mapuje KNX projekt

Řešení KNX IoT se realizuje přes rozhraní mezi sítí KNX a světem internetu. Na jedné straně jsou ovládací panely, řídicí systémy budov, chytré telefony a další prostředky komunikující prostřednictvím webových služeb s rozhraním. To znamená, že aplikace webového klienta je schopna vyhledávat údaje v rozhraní webové služby s unifikovanými texty telegramů a přenášet je. Na druhé straně je potřebné nalézt KNX protokol. Nicméně k rozpoznání infrastruktury parametrů systému KNX ze strany IP, projekt ETS musí být exportován do KNX WS-rozhraní. K tomuto účelu je k dispozici nová ETS Exporter App. KNX instalatér má možnost exportovat všechna data z projektu nebo jen jejich část. Pokud tak učiní, parametry musí být přesně označeny. Přenést lze také doplňující údaje.

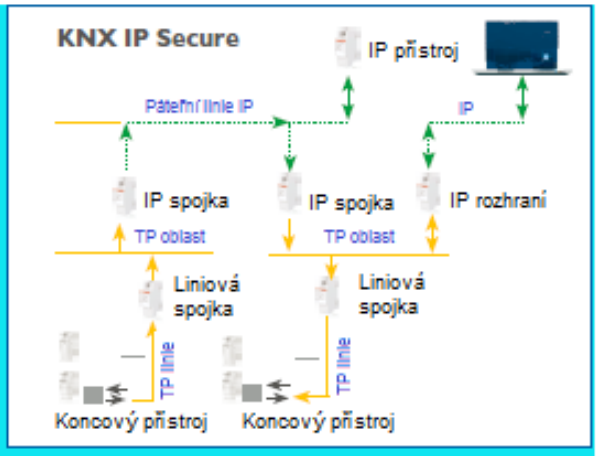
Více výhod s otevřenou výměnou dat

S KNX IoT se automatizace budov resp. chytrých domů přibližuje k virtuálnímu světu internetu. Tak se stává jednodušším použít data automatických funkcí, prezentovat hodnoty a stavy KNX instalace přes internet a vyhodnocovat je. Tím jsou zamýšleny hodnoty snímačů a údajů o spotřebě a využití energie, které mohou přispět k optimalizaci hospodaření s energií. Otevřená výměna dat mezi IT systémy a systémy automatizace budov umožňuje vylepšené aplikace s mnohonásobnými výhodami.

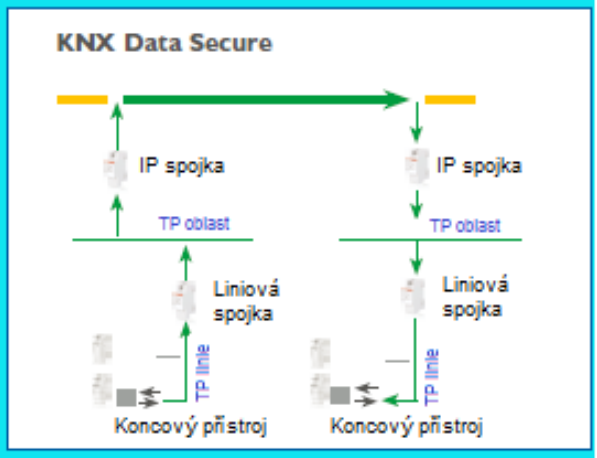
KNX Secure – zabezpečená KNX komunikace

KNX IP Secure a KNX Data Secure poskytují zabezpečený přístup ke KNX instalacím

Existují hackeři zasahující do technického vybavení budov. Chvástají se tím, že zapnuli osvětlení u souseda. Nicméně takovéto trestní jednání a s tím související know-how může způsobit obrovské škody. Proto KNX Security je žhavou otázkou. Ovšemže KNX dosud splňuje bezpečnostní požadavky, pokud montéři systému řízení funkcí v budovách se postarají o doporučená ochranná opatření proti nežádoucím manipulacím. Přesto, nová média, jako je LAN a WLAN s přístupem k internetu, koncepce bezdrátového provozu a jejich aplikace v citlivých oblastech, zvyšují riziko narušení nežádoucími vetřelci. Podle toho a také s ohledem na další požadavky má KNX developer k dispozici novou bezpečnostní koncepci: KNX Data Secure a KNX IP Secure. Obě části jsou založeny na celosvětově zavedených bezpečnostních protokolech a mohou být integrovány do stávajících systémů KNX.



KNX IP Secure pro zabezpečený KNX přenos mezi budovami



KNX Data Secure zabezpečený KNX přenos v budově

Bezpečnostní požadavky na instalace KNX narůstají. Kritické a důvěrné informace jsou stále více přenášeny ze stále širších oblastí použití. Jsou to například:
- informace o spotřebě, které by neměly být vnímány třetími stranami,
- signály bezpečnostních prvků (například dveřních kontaktů), které musí být chráněny proti manipulaci,
- KNX přístroje pro kritické funkce, které smí komunikovat pouze s ověřenými účastníky,
- ochrana údajů v bezpečnostních aplikacích; zde kód pro přístupový systém, nebo dokonce pro aktivaci a deaktivaci poplašného systému mohou být zasílány pouze šifrované a ne v otevřeném tvaru.

Jak chránit v budoucnu stále lepší média a přístroje v instalacích KNX, je stále větší výzvou pro projektanty, montéry a výrobce. Také proto byla v KNX vyvinuta nová rozšíření systému: KNX IP Secure a KNX Data Secure.

KNX zabezpečení

Základem každé bezpečnostní koncepce KNX je pečlivá ochrana systému proti neoprávněnému přístupu. Proto pouze instalatéři a uživatelé mohou získat fyzický přístup ke KNX instalacím. Přístroje a sběrnicové kabely TP (nebo IP) musí být uloženy takovým způsobem, aby byly chráněny proti neoprávněnému přístupu. Zejména v citlivých oblastech, jakými jsou venkovní části instalací, jsou řešením oddělené linie s aktivními filtračními tabulkami. Powerline (PL-linie) mohou být odděleny pásmovými oddělovacími filtry. Je potřebné vyhnout se nežádoucí a pro funkci zbytečné komunikaci na zabezpečné straně, pokud možno vhodnou konfigurací routerů a spojek. Potom potenciální sabotování parametrů a narušení přístrojů zvenčí může připadat do úvahy jen v rámci příslušné linie. Má-li KNX být propojeno se zabezpečovacími systémy, potom dobrým řešením je použití KNX přístrojů schválených VdS nebo striktní oddělení rozhraními. Používání internetového protokolu KNX IP v oddělených LAN nebo WLAN sítích by mělo být samozřejmostí. Musí být použity další standardní bezpečnostní mechanismy pro IP sítě. Pokud existuje přímé připojení k internetu, komunikace musí být přiměřeně chráněna. Také zde KNX nabízí odpověď s KNX bezpečnými rozhraními. V budoucnu také nově specifikované KNX rozhraní zvýší zabezpečení komunikace mezi KNX a internetem prostřednictvím webových služeb.

Koncepce dvojité ochrany

Zejména možnost dálkově ovládat instalaci KNX prostřednictvím internetu anebo bezdrátové sítě WLAN vyžaduje další ochranná opatření. Vzhledem k přístupu k přístrojům a médiím existuje nebezpečí manipulace s datovým provozem. Proto je nezbytné chránit předané informace na každém médiu (KNX TP, PL, RF, IP) proti změně nebo protokolování telegramů a jejich opakování z vnějšku, nežádoucí manipulací. Vzdálený přístup ke sběrnicovému systému KNX přes internet by měl být zajištěn takovým způsobem, aby provoz a konfigurace sběrnicových přístrojů bylo možné uskutečnit pouze ověřenými oprávněnými osobami. V takovém případě se jedná o účinný ochranný mechanismus proti manipulaci, protože sběrnicové přístroje mohou komunikovat pouze mezi sebou, jelikož jsou samy o sobě součástí sběrnicového systému. Podle těchto a dalších požadavků byly v KNX vyvinuty nové bezpečnostní koncepce: KNX Data Secure a KNX IP Secure. Oba používají mechanismy, které jsou např. použity pro bezpečný přenos dat mezi elektroměry a energetickými společnostmi.

Šifrované telegramy

Mají-li být data odesílána přes internet, spojení mezi vysílající a přijímající sítí může být chráněno virtuální privátní sítí (VPN). Přesto to nezajišťuje odesílatelovo oprávnění ke konfiguraci sběrnicového systému nebo k výměně dat s ním. Zde KNX IP Secure nabízí dodatečnou jistotu rozšířením protokolu KNX IP takovým způsobem, že přenášená data jsou kompletně šifrována. Toho lze dosáhnout i ve stávajících instalacích jen s malým úsilím. Mají-li být data přenášena v KNX pouze lokálně, k ochraně dat postačí rozšíření sběrnicového protokolu. Zadaný ochranný mechanismus KNX Data Secure ověřuje věrohodnost anebo šifruje vybrané KNX telegramy nezávisle na médiu. Klíče jsou přiřazeny k přístrojům nebo k objektům z ETS. Jelikož v jednom KNX systému mohou být jak zabezpečené, tak i nezabezpečené aplikace, není nutné zabezpečit všechny přístroje. Také stávající systém komponentů nemusí být vyměňován. Takovéto úsilí je minimalizováno, čímž je zachována investice do techniky KNX sběrnice.

KNX IP Secure a KNX Data Secure jsou dostupné v ETS5.5

DŮLEŽITÉ VĚDĚT

- V KNX instalacích lze paralelně použít zabezpečené KNX IP Secure a KNX Data Secure.
- V KNX instalacích mohou být současně použity zabezpečené i nezabezpečené aplikace, tedy ne všechny přístroje musí být zabezpečené.
- Nové zabezpečovací funkce mohou být integrovány do stávajících instalací.
- KNX IP Secure a KNX Data Secure jsou dostupné v ETS5.5

Bezpečnostní protokol zaveden celosvětově

V budoucnu nově uváděné ochranné mechanismy KNX Data Secure a KNX IP Secure umožní vytváření zabezpečených komunikačních kanálů mezi účastníky KNX. Tak může být zabráněno pronikání zmanipulovaných zpráv zamýšlených k ovládání systému. Proto je každá zpráva vybavena ověřovacím kódem. Automatické přidělování číselných řad nebo identifikačních posloupností zabrání pokusům o záznam dat a jejich pozdějšího přenosu za účelem sabotáže. Konečně, šifrování datového provozu činí instalaci KNX prakticky nezranitelnou. Tento postup je založen na celosvětově existujících bezpečnostních protokolech.

Zavedení do ETS5.5

V neposlední řadě projektanti, montážníci i systémoví integrátoři musí zajistit, aby hackeři neměli šanci. Musí se seznámit s ochrannými opatřeními a aplikovat je. Při předání systému i při periodických kontrolách již pracujícího systému by měla být prověřena zamýšlená úroveň zabezpečení. Nové bezpečnostní funkce, zejména pro přístup přes internet, mohou být aplikovány do stávajících systémů využitím rozhraní s novými KNX bezpečnostními mechanismy. KNX IP Secure a KNX Data Secure zajišťuje podporu novým softwarem ETS5.5 pro projektování a uvádění do provozu.

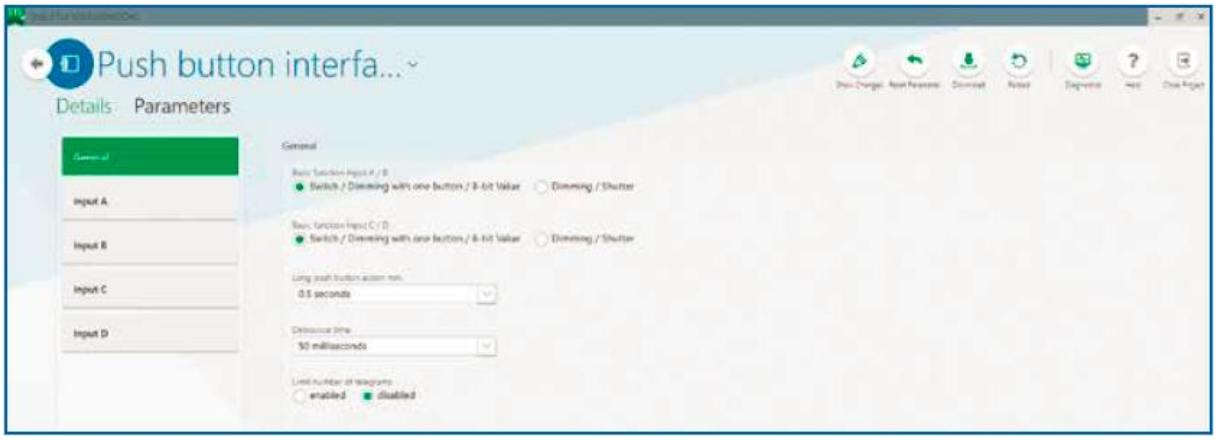
DALŠÍ INFORMACE

Další informace k předmětu zabezpečování KNX lze nalézt na našich webových stránkách pod: Download > Marketing > Flyer (www.knx.org/knx-en/downloads)
• KNX zabezpečení Kontrolní seznam
• KNX zabezpečení Přehled
Doplňující webinář „KNX Security“ informuje o aktuálně požadovaných ochranných opatřeních pro KNX instalace. Registrace na: www.knx.org/knx-en/training/knx-eacademy/webinars/

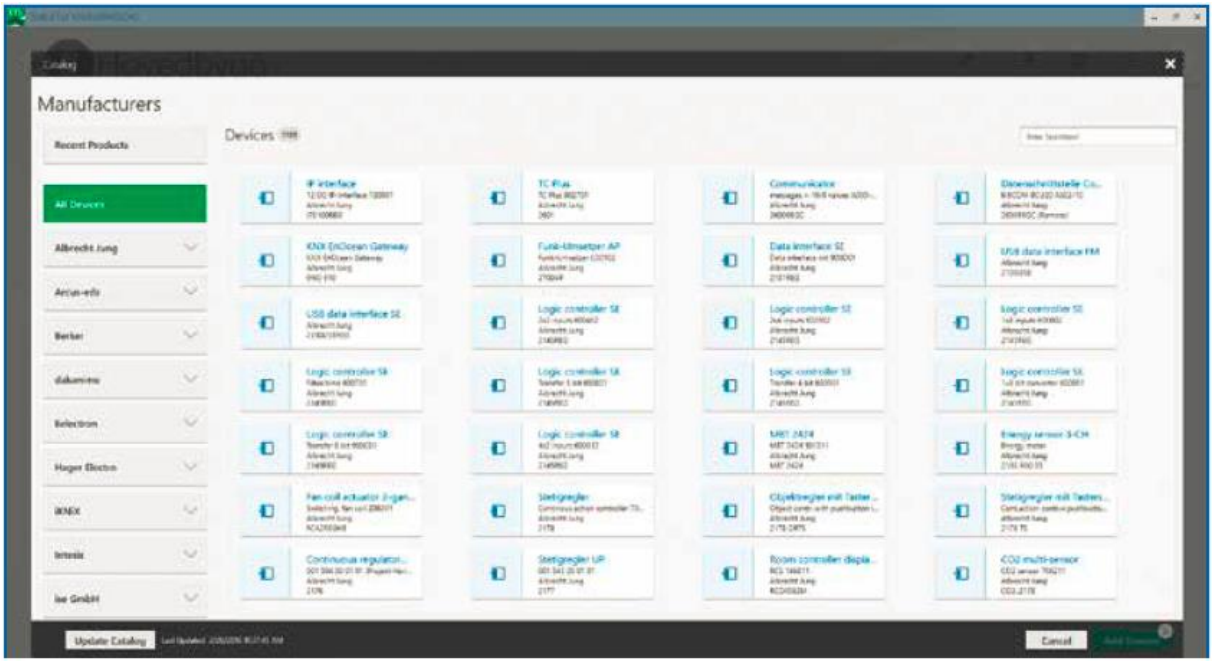
Nový ETS Inside – *chytrý*, jednoduchý, bezpečný

ETS Inside otevírá zajímavé perspektivy na rostoucím trhu chytrých domů

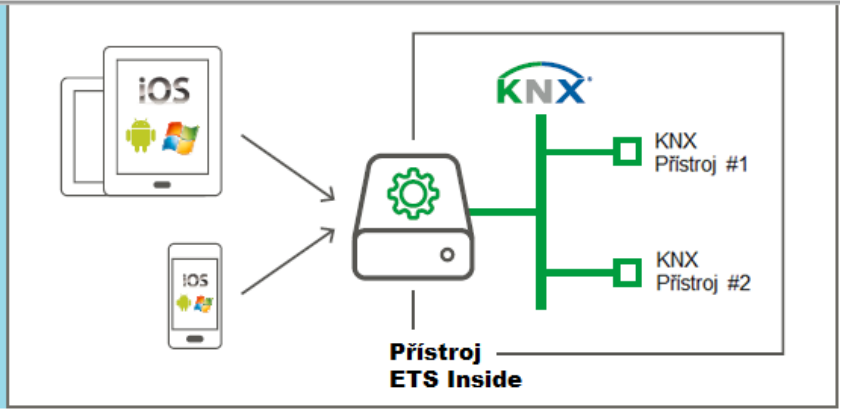
Výhody inteligentních funkcí v domácnostech si našly cestu do myslí většiny lidí. Všichni mají plná ústa Smart domů a trh tedy stojí před průlomem. Proto také KNX vydává nový ETS Inside. Dokonce i montéři s nepatrnou zkušeností z oblasti automatizace budov tak budou schopni vytvářet KNX projekty rychle a snadno s tímto nástrojem určeným pro malé a středně velké projekty. Obyvatelé velmi rádi přivítají při využívání svého inteligentního domu tím, že sami mohou aktivně přizpůsobit funkce vlastním potřebám. To proto, že ETS Inside je pevnou částí instalace KNX a vždy je aktuálně na místě. Snadno pochopitelné uživatelské rozhraní ve skutečnosti běží na tabletech a v chytrých telefonech. Dokonce - pouhým dotykem - je možné dálkové ovládání čehokoli doma. Přesto je projekt chráněn proti neoprávněnému přístupu.



Inteligentní design, minimalistický projekt, srozumitelné symboly - lze nastavit pouhým dotykem prostřednictvím nových parametrů uživatelského rozhraní.



Základní princip samostatného uživatelského rozhraní: Jednoduchá inteligentní parametrizace prostřednictvím tabletu nebo chytrého telefonu. Potřebné nástroje a projektový software jsou umístěny v přístroji ETS Inside



KNX prokazuje bezpečnost investic v nesčetných projektech již mnoho let. Otevřenost, kompatibilita, flexibilita a v neposlední řadě společný nástroj ETS, v současné době ve verzi 5, patří k tajemství jeho úspěchu. Dobře osvědčený ETS Professional umožňuje realizovat všechny instalace KNX ve všech velikostech projektů. Znalosti i praxi lze získat v certifikovaných KNX školicích centrech. Ale na trhu inteligentních domů existují i menší projekty, které vyžadují méně komplikované konfigurační práce. ETS Inside je sympatický pro všechny montéry, kteří nemají automatizaci budov ve svém portfoliu služeb, nebo tak činí pouze příležitostně. ETS Inside umožňuje realizaci projektů KNX jednoduchým způsobem a nevyžaduje rozsáhlé školení.

Oddělené ovládání a ETS data

Základním principem ETS Inside je oddělení uživatelského rozhraní od dat z ETS. To umožňuje editaci projektů na všech běžných operačních systémech. Podkladový KNX základní software je nainstalován do ETS Inside přístroje, který je součástí instalace. Tento hardware obsahuje také KNX projekt a nabízí webový server pro nezávislé uživatelské rozhraní. Díky této nové koncepci - na rozdíl od ETS Professional založeném na Windows - projekty lze editovat na tabletech a chytrých telefonech s různými operačními systémy, jako jsou iOS, Android nebo Windows. Rozsah provozních funkcionalit ETS Inside odpovídá použitým skutečnostem. Je možné navrhovat a uvádět do provozu malé a střední projekty. To odpovídá průměrným aplikacím KNX v obytných, komerčních a veřejných budovách. Jsou podporována všechna média (TP, IP, RF a PL).
Projekty vytvořené využitím ETS Inside lze kdykoli synchronizovat s ETS Professional, např. s cílem rozšířit KNX instalaci o přístroje, upravit topologii o některé další linie nebo použít přístroje vyžadující velmi rozsáhlou parametrizaci.

Chytrý – dotyk prstu namísto kliknutí myší

Nový ETS Inside je vhodný pro dnes běžně používané a jednoduše ovládané tablety a chytré telefony. Nové uživatelské rozhraní je organizováno minimalistickou cestou a je přizpůsobeno displejům iPad, iPhone, tabletům Android, tabletům Windows apod. A nabízí inteligentní design. Plochá tlačítka se snadno srozumitelnými symboly umožňují intuitivní ovládání. Parametrizace je velmi jednoduchá dokonce i s chytrými telefony, protože ETS Inside je citlivý na dotek.

Jednoduchý – Nástroj pro instalatéry i koncové zákazníky

Montéři a koncoví uživatelé mohou těžit z ETS Inside. Projekty KNX lze realizovat jednoduše a s úsporou nákladů. Je také možné, že systémový integrátor navrhne projekt v ETS Professional a synchronizuje jej později s přístrojem Inside. Následně odpovědný elektroinstalatér udržuje projekt pro svého zákazníka. ETS Inside podporuje následující oblasti: Koncoví zákazníci mohou požádat svého elektromontéra o odblokování určitých parametrů tak, aby si je kdykoliv mohli měnit v určitém rozsahu. To mohou být hodnoty stmívání, časové programy, světelné scény apod., které si upravují sami podle potřeb, bez nutnosti volat řemeslníka.

Bezpečný – Žádný neautorizovaný přístup

ETS Inside nabízí trojitou ochranu:
• Pro editaci projektu je nutné přihlášení podle předem zadaných údajů. Neoprávněné osoby proto nemohou získat přístup k přístroji ETS Inside.
• Pro zachování záruky elektroinstalatér rozhoduje, po dohodě se svým zákazníkem, jaké parametry pro něho odblokuje. Obvykle jsou to takové, které nemají vliv na kterékoli funkce související se zabezpečením.
• V neposlední řadě ETS Inside podporuje novou KNX Secure koncepci. Takže hackeři nemají šanci ani zde.

Inside ETS

ETS INSIDE NABÍZÍ PŘESVĚDČIVÉ ARGUMENTY

1. *ETS Inside nabízí instalatérům, kteří dosud jen nepatrně pracovali s KNX, nekomplikovaný vstup do stále se rozšiřujícího trhu se Smart domy.*
2. *Využitý princip uživatelského rozhraní odděleného od ETS dovoluje používat populární tablety a chytré telefony.*
3. *ETS Inside je pevnou součástí instalace a je k dispozici vždy v nejposlednější verzi.*
4. *Elektroinstalatéři mohou odblokovat zvolené parametry pro úpravy koncovým zákazníkem.*
5. *Projekt lze kdykoliv synchronizovat s ETS Professional.*
6. *Existující KNX instalace lze za určitých okolností doplnit o ETS Inside.*

ETS Inside bude k dispozici od ledna 2017. Ke každému přístroji Inside je potřebná licence.

www.knx.org

NATIONAL KNX Czech Republic

www.knx.org/cz www.knxcz.cz