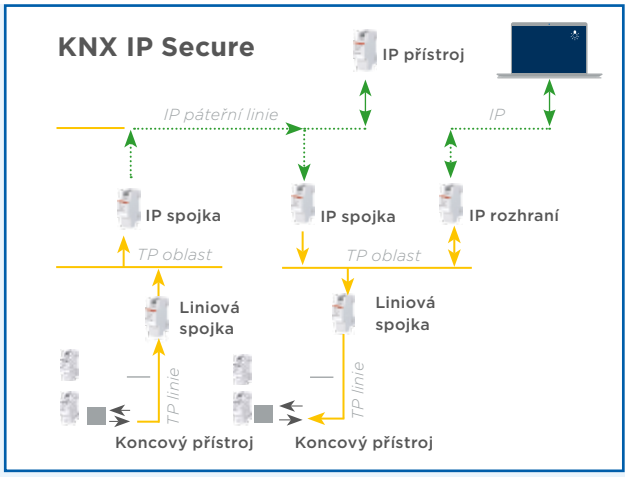
KNX Novinky

KNX Secure
KNX Internet věcí

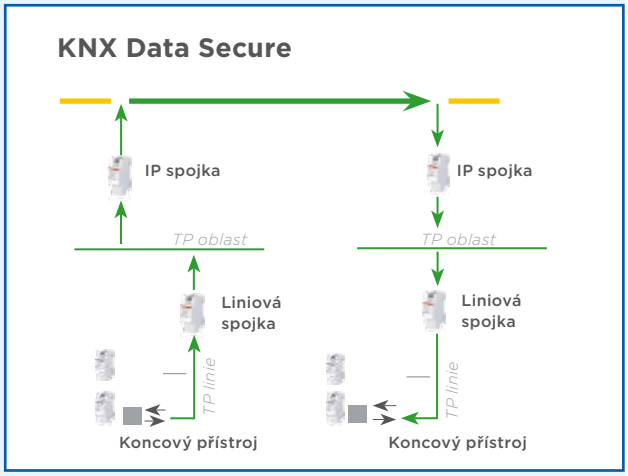
KNX Secure – maximální ochrana dat pro chytré budovy

Úvod do rozšíření bezpečnosti KNX s prvními přístroji KNX IP Secure a KNX Data Secure

Kybernetická bezpečnost je kontroverzním tématem: někteří vidí vetřelce při možnosti sledování údajů meteorologické stanice na střeše, zatímco druzí v průniku do instalace. Profesionálně zhotovené instalace KNX jsou v podstatě bezpečné. Je také skutečností, že aplikace KNX v budovách se stávají všestrannějšími, a proto mohou být citlivějšími na útoky. Potřeba zabezpečení se zvyšuje s rostoucí hrozbou. Nyní přichází na trh první přístroje KNX Secure, čímž je zajištěno zvýšení bezpečnosti KNX.



Dva typy ochrany:
KNX IP Secure chrání IP komunikaci, KNX Data Secure chrání komunikaci všemi médii při přenosu od přístroje k přístroji. Oba bezpečnostní mechanis-my lze vzájemně kombinovat a používat souběžně.



Popularita chytrých domů budí zájem hackerů. Není divu, protože inteligentní domácí technologie se často objevují na trhu rychle a levně, zatímco zajištění bezpečnosti přenosu dat se často opožďuje. Častými jsou nedostatečné kompetence s následkem nižší pečlivosti a spolehlivosti při zavádění takového systému.
KNX je jiné: KNX instalují odborníci. Ochranná opatření proti neoprávněnému přístupu do sítě budov jsou součástí předpisů pro vytváření instalace. I později jsou systémy KNX odborně udržovány v provozu. Hackeři mají proto nízké šance s průnikem do KNX.

Nebezpečné situace a rizika

Upozornění odborníků na bezpečnost informačních technologií týkajících se útoků na sítě budov by však neměly být zneužívány. Ať už je to chytrý byt nebo chytrá budova: úroveň ohrožení se změnila. Inteligentní aplikace v budovách jsou stále více univerzální. Systémy KNX také integrují bezpečnostně související funkce pro dosažení synergických efektů. Řízení přístupu, systémy řízení vstupů a poplašné systémy mohou být možnými cíli. Pokud nějaký zločinec zjistí narušení bezpečnosti, může kopírovat telegramy, vzdáleně otevřít dveře nebo dokonce deaktivovat poplašný systém. Hackeři by si mohli zobrazit nechráněné údaje ze snímačů přítom-nosti, energetických spotřebičů a administrativních programů a využívat je pro svoje úmysly. Manipulace se systémy řízení osvětlení, řízení vytápění a dalšími procesy využívanými ve stavbách je také rizikem. A nejen to: sítě v budovách jsou stále snadnějšími cíli následkem používání internetových routerů, WLAN, IP protokolu, serverů, tabletů, smartphonů a dalších komponentů IoT.

KNX je bezpečné

Automatizace budov s KNX je v zásadě bezpečná. V profesionálně realizované instalaci jsou dodrženy bezpečnostní předpisy. Zde může pomoci bezpečnostní kontrolní seznam zveřejněný asociací KNX. Fyzická média by měla být například uzavřena proti přímému přístupu jak zevnitř, tak zvenku. Spojky zabraňují nechtěným přenosům telegramů mimo linie a nastavují meze přímého přístupu. Parametry jsou chráněny před neoprávněnými změnami zadaným heslem. Pokud se jako komunikační médium používá IP, měly by být pro sítě IP použity obvyklé bezpečnostní mechanismy. Například připojení VPN zabraňuje neoprávněnému čtení telegramů během konfigurace pomocí ETS.

KNX Secure může být nejen ochranným mechanismem, ale může mít i stylový design: nový skleněný snímač KNX Secure a prostorový termostat KNX od společnosti CONTOLtronic.

Photo: CONTOLtronic

Začněte s rozšířenou ochranou KNX: router KNX IP Secure společnosti Enertex ověřuje a šifruje telegramy KNX a IP a nabízí další funkce pro automatizaci budov.

Photo: Enertex

Nejvyšší ochranný standard

Aby se systém KNX přizpůsobil současnému i budoucímu vývoji automatizace budov, pokud jde o bezpečnost dat, zvýšily se bezpečnostní požadavky na techniku KNX a byla vyvinuta architektura KNX Secure. Nové přístroje KNX Secure jsou přísnou implementací předchozího rozvoje přídavných ochranných opatření. KNX Secure byl již vytvořen v roce 2015 jako bezpečnostní koncepce a byl přijat v ETS5.5 v roce 2016. Uvedené ochranné mechanismy jsou založeny na mezinárodních bezpečnostních algoritmech normalizovaných podle ISO 18033-3 a používají ověřovací šifrování v souladu s AES 128 CCM. To znamená nejvyšší úroveň ochrany dat pomocí ověřování a šifrování datové komunikace. Používají se následující metody:

- Telegramy jsou ověřeny tak, aby je příjemci mohli rozpoznat jako pravdivé nebo nepravdivé.
- Možné další šifrování činí telegramy nečitelné třetí stranou.
- Sekvenční číslo zabraňuje nežádoucímu opakování telegra-mů.

Telegramy tak mohou být ověřeny tak, aby jejich obsah byl viditelný např. pro vizualizační software. Nicméně, nelze s nimi manipulovat ani je opětovně odesílat. Komunikace s přístroji je zajištěna během projektování a uvádění do provozu s ETS. KNX Secure sestává ze dvou typů zabezpečení:

- KNX IP Secure pro ochranu komunikace KNX IP
- KNX Data Secure pro ochranu běžné komunikace, např. sku-pinovými telegramy

Oba bezpečnostní mechanismy lze kombinovat a používat souběžně. S KNX Secure mohou být instalace KNX zajištěny podle aplikací nebo jako celky.

KNX IP Secure je přizpůsobivý

Vedle nových instalací bude trh automatizace budov v budoucnu vyžadovat vylepšení stávajících systémů. Zákazníci požadují dodržování předpisů a norem. KNX Secure splňuje tento požadavek, protože je normalizován jako EN 50090-4-3. Existují dvě možnosti, jak účinně zabránit útokům hackerů:

- S protokolem KNX IP Secure lze IP komunikaci instalace KNX zajistit jednoduchým a nákladově efektivním způsobem. Stačí nahradit obvyklé routery KNX IP novými routery KNX IP Secure. Tyto routery rozšiřují protokol KNX IP o další ověřování a šifrování. Tímto procesem je IP komunikace zajištěna na úrovni telegramu.
- KNX Data Secure šifruje a ověřuje telegramy mezi koncovými přístroji prostřednictvím všech přenosových cest. Všechny zúčastněné komponenty musí být přístroji KNX Data Secure. Vedle úplné ochrany celé oblasti KNX a linií KNX je také možné chránit jednotlivé aplikace KNX, které jsou zvláště ohroženy. Zabezpečené i nezabezpečené funkce jsou možné souběžně – také v přístroji KNX Data Secure.

DŮLEŽITÉ JE VĚDĚT

- KNX IP Secure a KNX Data Secure lze používat v KNX instalaci souběžně.
- V KNX instalaci mohou být souběžně využívány zabezpečené i nezabezpečené aplikace. Ne všechny přístroje musí být zabezpečené.
- Nové zabezpečovací funkce lze také bezproblémově začlenit do již existujících instalací.
- KNX IP Secure a KNX Data Secure jsou k dispozici od ETS5.5, tedy i v novější verzi ETS5.6.

Přístroje KNX Secure mohou být provozovány jak zabezpečeně, tak i nezabezpečeně. Proto je možné zůstat flexibilní s možnostmi změn a rozšiřování stávajících KNX instalací, pokud např. v budoucnu nebudou k dispozici všechny přístroje KNX jako KNX Secure nebo pokud bude potřebné vyměnit staré přístroje.

Klíčová role ETS

Při implementaci rozšířeného zabezpečení KNX software ETS má klíčovou roli pro návrh projektu v pravém slova smyslu. Nástroj pro odborné instalace KNX byl již připraven pro KNX Secure ve verzi 5.5. Inteligentní funkce podporují zpracování projektu a uvedení do provozu přístrojů KNX Secure. Během konfigurace chrání ETS před nesprávnými nastaveními. ETS zajišťuje, aby v zabezpe-čeném režimu bylo aktivováno heslo projektu a vložen certifikát přístroje. V dialogovém okně se automaticky přiřadí klíče zabezpečení KNX Secure přístrojů a klíče runtime pro skupinové objekty a bezpečnostní klíče se ukládají do projektu.

Správa odpovědnosti

KNX Secure chrání instalace KNX lépe než obvyklým bezpečnostním standardem automatizace budov. Je povinností projektantů, instalatérů, systémových integrátorů a uživatelů budov, aby využili příslušná bezpečnostní opatření a případná rozšíření s KNX Secure. Měřítkem pro implementaci jsou možné hrozby a rizika, stejně jako zohlednění dodatečných nákladů ve vztahu k výhodám. Předpokladem je profesionální návrh a instalace systému KNX. Všechny zúčastněné strany nesou odpovědnost za to, že projekt KNX s aplikacemi KNX Secure bude maximálně chráněn před hackerskými útoky při předání projektu uživatelům budovy, servisním technikům a domácím technikům. Je velmi důležité, aby byla zachována další údržba projektu, ochrana bezpečnostních klíčů a odpovědnost za klíče.

UZNÁVANÉ NORMY A STANDARDY

- Využití uznávaných KNX bezpečnostních standardů s KNX Secure účinně brání útokům na KNX digitální infrastrukturu budov
- Architektury KNX a KNX Secure jsou normalizovány podle EN 50090-4-3 „Elektronické systémy pro byty a budovy“
- KNX Secure je založen na mezinárodně normalizovaných bezpečnostních algoritmech podle ISO 18033-3 a na šifrování CCM podle AES 128
- KNX je první a zatím jedinou normou pro inteligentní budovy, která splňuje nejvyšší bezpečnostní požadavky na zajištění v oblasti kybernetické bezpečnosti

Příklady možných aplikací s KNX Secure

- **Hotely** – bezpečné oddělení funkcí mezi jednotlivými pokoji
- **Údaje o spotřebě energie** – šifrování dat KNX chrání soukromí
- **Rezervační systémy** – šifrování telegramů na úrovni IP brání externímu přístupu
- **Správa přístupu** – autentizace a šifrování
- **Údaje o přítomnosti** – žádné sledování v reálném čase, které umožňuje zjištění přítomnosti lidí
- **Poplašné systémy** – prevence před úmyslnými falešnými poplachy

DALŠÍ INFORMACE

Další informace o předmětu KNX Secure lze nalézt na webových stránkách **http://KNXsecure.knx.org** a na stránkách **www.knxcz.cz**
Zde lze nalézt:

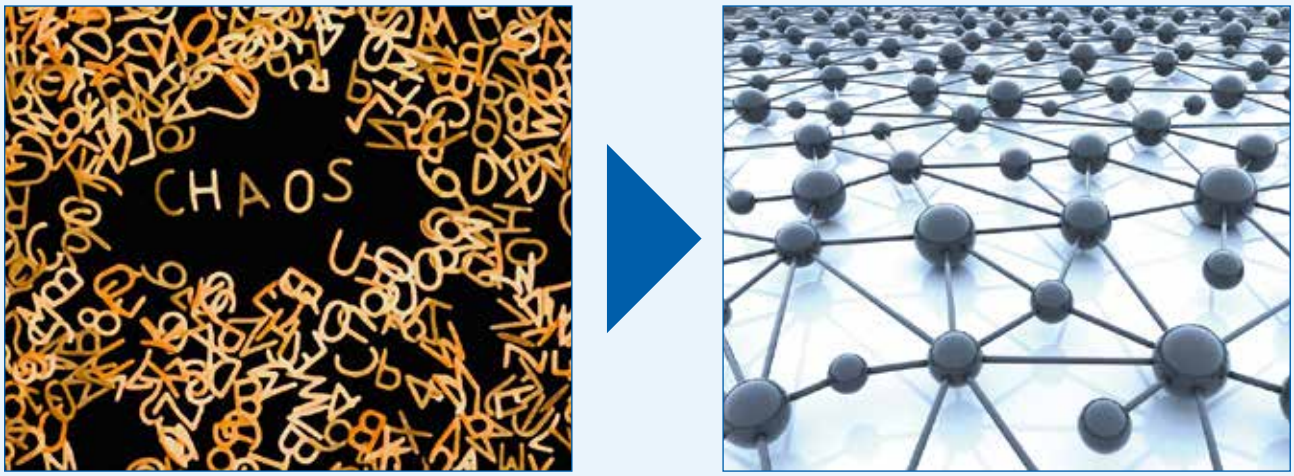
- KNX zabezpečení Kontrolní seznam
- KNX zabezpečení Přehled
- KNX zabezpečení Výrobky.

Doplňkový **webový seminář „KNX Secure“** vás aktuálně informuje o požadovaných ochranných opatřeních pro vaši instalaci KNX.
Registrace na:
www.knx.org/knx-en/training/knx-eacademy/webinars/

Kontrolní seznam pro zvýšení zabezpečení v instalacích KNX

KNX a Internet věcí (IoT)

Aktuální stav trhu IoT



Funkcionalita IoT vzrůstá

Čím hlouběji se internet věcí vytváří, tím vyšší je úroveň automatizace očekávané uživateli. K dispozici jsou další produkty a věci generující stále větší objem dat. Tyto rostoucí toky dat jsou zpracovávány velkými datovými technikami. Přístroje pracují s těmito zpracovanými informacemi a uskutečňují akce mnoha způsoby sloužící uživatelům.

Náročnost se zvýšila, spolehlivost a interoperabilita však stále není zaručena

- Nabízí se řada řešení pokrývajících vždy pouze jeden případ použití (hlasové ovládání, zvonek připojený k internetu, osvětlení a regulace prostorové teploty ovládané Aplikací, ...).
- Snaha o spolehlivé propojení různých služeb poskytovaných přístroji není triviální.
- V mnoha případech závisí správná funkce přístrojů na připojení k internetu.
- Přizpůsobená integrace softwaru může přerušit každou aktualizaci softwaru a je velmi složitá pro zabezpečení. Spolehlivost a stabilita není zaručena po delší dobu nezbytnou pro automatizaci budov.
- Integrace může záviset na cloudových službách spravovaných společnostmi třetích stran, mimo kontrolu koncového uživatele a na konkrétní obchodní situaci.

KNX = dlouhodobá podpora s certifikovanou interoperabilitou

Ve své historii, delší než 25 let, má asociace KNX bezkonkurenční zkušenosti s dlouhodobou podporou řešení automatizace v každém typu budovy. Na základě standardu KNX lze automatizaci budov vytvářet spolehlivým, interoperabilním a rozšiřitelným způsobem: přístroje od více než 400 výrobců spolupracují ve velmi stabilním distribuovaném prostředí bez jediného bodu selhání. Současný ekosystém je fyzicky snadno instalovatelný a logicky konfigurovatelný využitím jediného nástroje ETS™.

KNX již lze kombinovat s IoT

Existuje široká škála dobrých řešení od výrobců KNX, která již nyní propojují systém KNX se systémem vyšší úrovně IoT. Internetová stránka těchto produktů však není standardizována nebo je vytvořena tak, aby odpovídala konkrétním případům použití. Jak již bylo zveřejněno v roce 2016, Asociace KNX učinila jako první krok k normalizaci na straně internetu publikováním specifikací webových služeb a rozhraní KNX IoT, která umožňují sladit brány s existujícími webovými protokoly oBIX, OPC/UA a BACnet webovými službami.

Přidání KNX výhod k IoT

Jako druhý krok v rámci projektu KNX IoT si nyní KNX přeje, aby klíčové výhody KNX interoperability, spolehlivosti a rozšiřitelnosti byly k dispozici i na úrovni IoT.

Příspěvek KNX k IoT

Kombinace více druhů věcí s promyšleným řešením

Následující prvky (níže vyznačené zeleně) jsou základními kameny systémové architektury KNX IoT:

Sémantika

Je stěžejní otázkou, aby

- přístroje si vzájemně rozuměly
- lidé mohli pochopit, co přístroj nebo služba nabízí.

Pochopení významu dat (= sémantika) je nezbytné k tomu, aby bylo možné kombinovat funkčnost a vytvářet nové funkce.

Současný systém KNX to zajišťuje vytvořením projektu v ETS, čímž se spoléhá na standardizované datové typy KNX, které kombinují řadu produktů / funkčností. Pro IoT je důležité být schopen sdílet tyto sémantické informace i mimo hranice ekosystému KNX.

Sémantiky umožňují interakci zařízení a služeb na různých úrovních. Například nástěnný spínač může přímo ovládat určité svítidlo, zatímco aplikace pro mobilní telefon může nastavit budovu do režimu „mimo domov“, čímž nepřímo ovládá stejné svítidlo.

Sémantika umožňuje odstranit technické detaily a tím vytvářet zvláštní hodnoty. Jako příklad takové zvláštní hodnoty lze vytvořit příkazy jako „vypnout topení, když je okno otevřené“. Dalším příkladem je „ztlumit osvětlení v obývacím pokoji“, přičemž součásti distribuovaného systému mohou rozhodnout, zda by to mělo vést k pohybu žaluzie nebo stmívání osvětlení.

Propojené údaje jsou již normalizovaným a dobře přijatým způsobem, jak sdílet sémantické znalosti. Propojená data jsou technologie se sémantickým webem, tzv. „Webem věcí“. KNX využívá tohoto standardu a na základě této technologie vytvořil ontologii KNX IoT. Tento zásobník zajišťuje sdílení a interpretaci informací běžným způsobem.

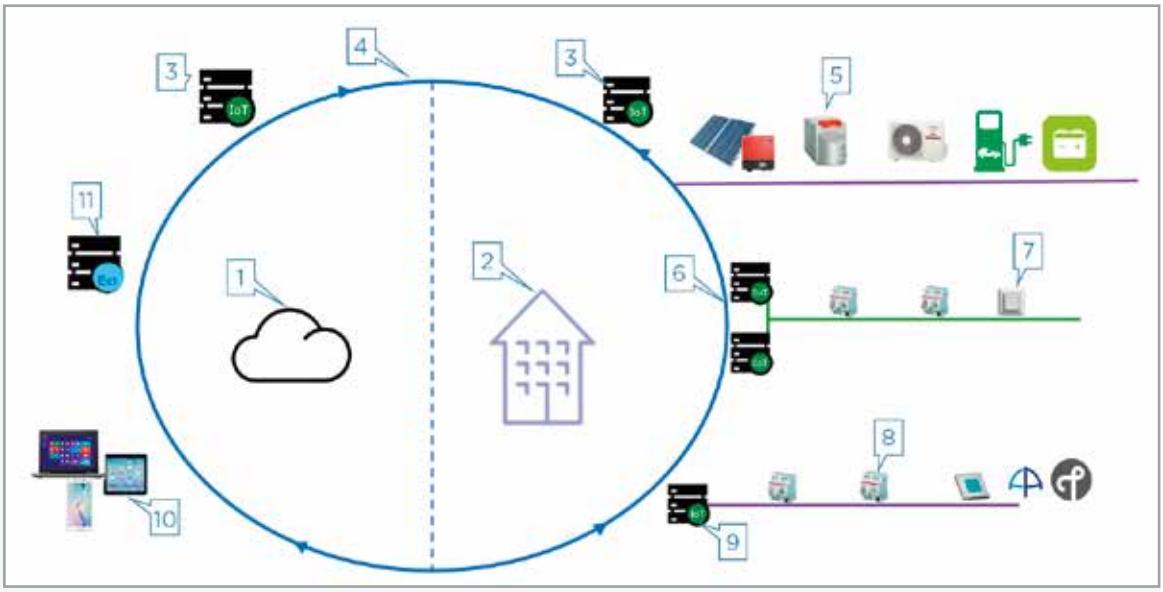
Pro vytváření těchto sémantických informací je možné použít jako výchozí bod to, co je nyní možné s ETS, ale bude se nadále rozvíjet. Tyto vylepšené informace budou zpřístupněny standardizovaným způsobem mezi povolenými zúčastněnými přístroji nebo službami a zajistí, aby lidé i stroje mohli interpretovat vytvořené funkce.

Páteřní síť IoT

Nová norma IoT asociace KNX poskytne svobodu při realizaci páteřní sítě KNX IoT, po níž jsou informace vyměňovány, a také nabízí výchozí cloudové služby. Jelikož řešení je standardizováno, bude možné je realizovat s různými komponenty podle vlastních potřeb.

Například využitím jiného poskytovatele cloudu, soukromého cloudu, vlastního hardwaru na veřejném internetu nebo soukromé síti, místních přístrojů nebo serverů v budově apod. Tato svoboda je důležitá pro zajištění realizace pokročilých případů použití, a tím se těší výhodě vysoké dostupnosti a odolnosti proti chybám platformy.

Páteřní síťový protokol bude podporovat případnou konzistenci dat, neboť nelze se vyhnout tomu, aby se prvky v síti staly nedostupnými, např. když budova je krátkodobě



1 Internet
2 Domácí nebo firemní síť
3 KNX Stack: kombinuje informace o KNX ontologii a projektové informace – exportované z ETS směrem na rozhraní a klienty. Mohou být v cloudu nebo v budově
4 KNX IoT páteřní síť: zajišťuje konzistenci dat
5 KNX IoT schopné přístroje: IP přístroje s vyšší kapacitou (výkon, paměť, rychlost)
6 KNX IoT rozhraní s bohatou sémantikou definovanou standardizovanou KNX ontologií
7 Klasické KNX přístroje
8 KNX IoT omezující přístroje: IP přístroje na úrovni pole, KNX aplikační vrstva, nižší vrstvy vyvinuté společně s Fairhair/Thread
9 Přenosový router
10 IP klienti (notebooky, tablety, telefony, ...): schopné k připojení k bytu nebo budově za pomoci pověření z MyKNX
11 Cloudový server: může a nemusí být

offline. Během této doby, kdy některé části sítě nejsou dostupné, bude stále možné změnit stav osvětlení jak místně v budově, tak prostřednictvím internetu. Páteřní síť KNX IoT však informuje o nedostupných částech sítě a umožní řídit, jaký stav „vyhraje“, jakmile bude síť opět plně funkční.

IP schopné přístroje

Více typů přístrojů bude přímo součástí („plných občanů“) sítě KNX IoT včetně přístrojů na fyzických vrstvách nestandar-dizovaných asociací KNX, ale jsou standardizovány, protože nabízejí IP komunikaci.
Takové přístroje mohou být krátkodobou anebo také trvalou součástí sítě.
IP schopné přístroje jsou charakterizovány tím, že nemají žádná omezení, pokud jde o rychlost přenosu, paměť nebo spotřebu energie.
Jedná se o služby cloudového vzdáleného přístupu, mobilní telefony přes mobilní připojení (2G, 3G, 4G, 5G), tablety na síti LAN, cloudovou službu o počasí, ...

Přístroje KNX pro kroucený pár a přístroje radiofrekvenční

Současný systém KNX sestávající z přístrojů připojovaných ke kroucenému páru nebo přístrojů radiofrekvenčních, může být stále součástí sítě IoT. Z pohledu IT bude funkčnost sémanticky zobrazena stejným způsobem a nezávisle na použitém komunikačním médiu. Komunikace na médiích jiných, než IP bude převedena na protokol IP prostřednictvím jednoho, případně více rozhraní.

Přístroje s omezením

Vedle současných fyzických médií KNX s nízkým úsilím pro instalaci se objevují nová fyzická média nabízející podporu protokolu IP. Taková média jsou typicky schopna vytvářet nákladově efektivnější síť IP a spotřebovávají méně energie ve srovnání s Ethernetem nebo WiFi. Jako příklady jsou prostředky založené na IEEE802.15.4, LoRA, Sigfox, ...

BEZPEČNÉ ŘEŠENÍ IoT

KNX asociace spolupracuje na definici specifikací KNX IoT se dvěma průmyslovými konsorcii: Thread Group a FairhairAlliance. Cílem této spolupráce je pracovat na společném unikátním a bezpečném systému automatizace budov, který bude sloužit potřebám pro automatizaci budov.

Technologie **Thread Group** může sloužit k rozšíření klasických instalací KNX o síť sběrnice IPv6, což umožňuje přístrojům s omezením vyměňovat standardizovaná data KNX na bezdrátové síti Thread za mezním routerem Thread, kterým se propojuje klasický svět KNX.

Fairhair Aliance usiluje o jednotnou a vhodnou sadu specifikací IEEE/IETF, která umožní všem budoucím produktům automatizaci budov založených na IP sdílení ve společné infrastruktuře odpovídající infrastruktuře IPv6.Tímto způsobem by produkty pro automatizaci budov mohly být integrovány do IP sítí pomocí mechanismů již známých administrátorům.

Souhrn

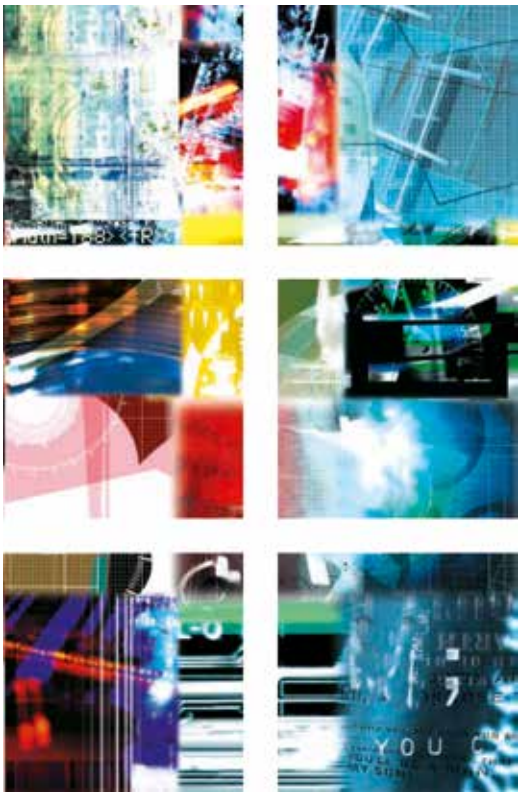
Řešení KNX IoT odstraňuje překážky přístupu KNX jako součásti internetu věcí. Cílem je snížit nároky na potřebné znalosti a otevřít současný ekosystém KNX specialistům mimo KNX prostřednictvím „out-of-the-box“ operací, a současně specialistům umožnit pokročilou konfiguraci a přizpůsobení.
Řešení KNX IoT je definováno ve spolupráci s klíčovými výrobci KNX a normalizačními orgány (jako je Fairhair a Thread group). KNX pracuje také na vyzkoušených koncepcích a schválených řešeních.
Využívání norem zaručuje vyšší hodnotu produktů KNX, takže dlouhodobou podporu lze zaručit v neustále se měnícím světě internetu. KNX má výhodu v rozsáhlé základně KNX instalací, která umožňuje čerpat z bohatých zkušeností, jež mohou úspěšně rozšiřovat integraci KNX do Internetu věcí.
Další informace o tématu KNX IoT naleznete na http://KNXIoT.knx.org

SKLADBA PŘÍSTROJŮ KNX IoT

Fairhair se zabývá:
- Definicemi bezpečnostní architektury
- Popisy a zjišťováním funkcí přístrojů
- Správou sítí
- To vše na základě norem IEEE/IETF

Thread group:
- Baterie šetrné: ideální pro přístroje s omezením
- IPv6 s 6LowPAN
- Samoopravitelné buňkové sítě 802.15.4
- Zahrnuje zabezpečení na síťové vrstvě
- Již k dostání v křemíku

KNX se soustřeďuje na to, co umí nejlépe:
nástroje pro uvádění do provozu a vzájemnou spolupráci



www.knx.org
www.knx.cz

v5-18