www.knx.org

KNX zabezpečení

Přehled

Obsah

1 Úvod

Tento dokument slouží jako vodítko jak pro elektroinstalatéry, tak i pro výrobce KNX, aby se seznámili s aktuálními opatřeními, která mohou být učiněna pro zvýšení bezpečnosti instalací KNX.

2 Zabránění přístupu k síti na různých fyzických médiích KNX

2.1.1 Úvod

Vhodná koncepce zabezpečení je založena na zajištění řádné prevence před neoprávněným přístupem. V případě instalace KNX to znamená, že pouze oprávněné osoby (elektroinstalatér, správce, uživatel) mají fyzický přístup k instalaci KNX. Při navrhování a instalaci, pro každé KNX médium, musí být kritické prvky chráněny co možná nejlepším způsobem.

2.1.2 Montáž kabelů a přístrojů

- Obecně platí, že zařízení a přístroje musí být řádně připevněny, aby se zabránilo, že by mohly být snadno odstraněny a tím by byl umožněn přístup k instalaci KNX neoprávněným osobám.
- Kryty a rozvaděče obsahující KNX přístroje musí být řádně uzavřeny nebo musí být namontovány v místnostech, do nichž mají přístup pouze oprávněné osoby.
- Ve venkovních prostorách musí být přístroje namontovány v dostatečné výšce (např. meteorologická stanice, snímač větru, snímač pohybu, atd.).
- Ve všech nedostatečně hlídaných veřejných prostorách využívat klasické přístroje propojené s binárními vstupy uloženými v chráněných oblastech (např. v rozvaděčích) anebo tlačítková rozhraní skrytá v hlubokých krabicích, což je určitá prevence před nežádoucím přístupem ke sběrnici.
- Pokud možno, využít opatření proti krádežím některých aplikačních modulů (např. mechanické zabezpečení aplikačních modulů šrouby, možnost sejmutí pouze nástroji, nutnost použití nadměrné síly k sejmutí a podobná opatření).

2.1.3 Kroucený pár

- Konce kabelů by neměly být viditelné, visící vně na stěnách, ani na výstupech nebo uvnitř budovy.
- Kabel sběrnice ve venkovním prostoru představuje vyšší riziko. Fyzický přístup ke KNX kroucenému páru musí být v tomto případě ještě obtížnější než uvnitř bytu nebo domu.
- Pro dodatečnou ochranu přístrojů instalovaných v místech s omezeným dohledem (venku, v podzemních parkovištích, na WC, atd.) mohou být připojeny k samostatné linii. Aktivací filtrační tabulky v liniové spojce potom může být zabráněno přístupu hackera k celé instalaci.

2.1.4 Powerline

- Elektronické filtry by měly být použity k filtrování příchozích i odchozích signálů.

2.1.5 Radiofrekvenční

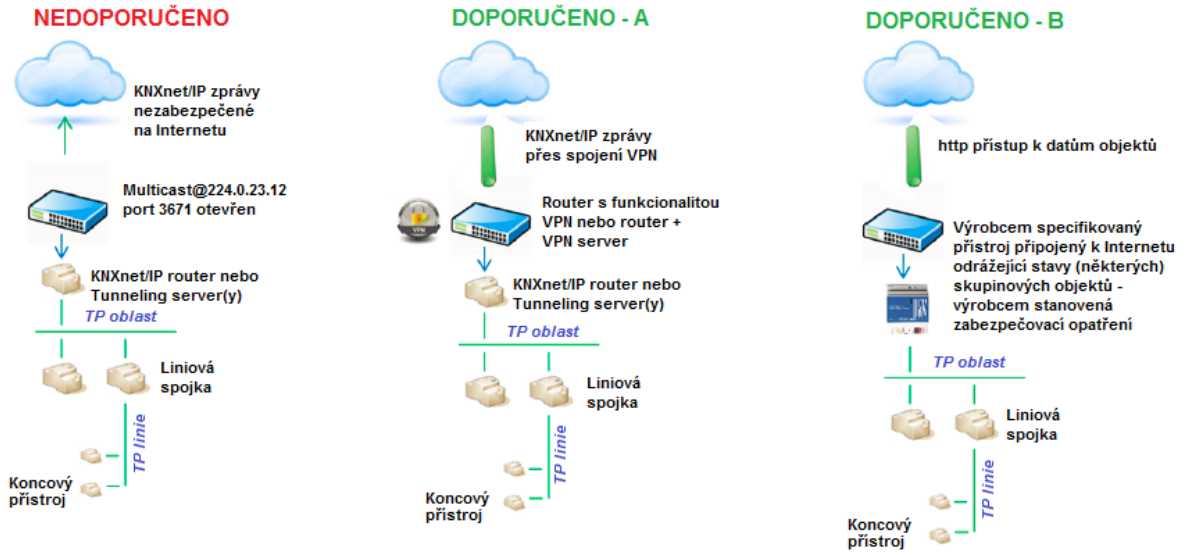
- Jelikož radiofrekvenční přenos je otevřené médium, nelze přijmout opatření ***fyzické*** ochrany pro zabránění přístupu. Proto je zapotřebí přijmout jiná opatření, která jsou uvedena v článcích 3 až 6 (a zejména ta která jsou uvedena v článku 5).

2.1.6 IP

- Automatizace budov by měla běžet přes vyhrazený LAN a WLAN s vlastním hardwarem (routery, přepínače, atd.).
- Bez ohledu na typ instalace KNX, musí se v každém případě dodržovat obvyklé ochranné mechanismy pro IP sítě. Ty mohou zahrnovat:
  - MAC filtry
  - Šifrování bezdrátových sítí ve spojení se silnými hesly (změna výchozího hesla - WPA2 nebo vyšší) a ochrana proti neoprávněným osobám.
  - Změna výchozí SSID (SSID je název, pod kterým je bezdrátový přístupový bod viditelný v síti, většinou výrobce a typ výrobku). Výchozí SSID může poukázat na s výrobkem spojené slabiny použitých přístupových bodů, čímž tak mohou být zvláště citlivé na hackery). Přístupový bod může být kromě toho nastaven tak, že je zabráněno periodickému přenosu mezi jiné SSID.
- Pro KNX IP multicast musí být použita jiná IP adresa jako výchozí (224.0.23.12). Vhodnou adresu lze dohodnout se správcem sítě.
- IT síťoví specialisté se budou podílet na větších projektech s připojením ke KNXnet / IP: takto bude možné optimalizovat konfiguraci sítě (řiditelné přepínače, VLAN, přístupové body podle IEEE802.X atd.) a mohou být využity další mechanismy na ochranu jako filtrování e-mailů a antivirus.

2.1.7 Internet

- KNXnet / IP routing a KNXnet/ IP tunneling nejsou určeny k použití prostřednictvím internetu. Proto není vhodné otevřít porty routerů k internetu a tím KNX komunikaci učinit viditelnou přes internet.
  - Instalace (W) LAN musí být chráněna firewallem.
  - Není-li nutný jakýkoli externí přístup k instalaci, výchozí rozhraní může být nastaveno na hodnotu 0 a takto zablokovat veškerou komunikaci s internetem.
- Přeje-li si někdo realizovat přístup k instalaci přes internet, pak to může být uskutečněno následujícím způsobem:
  - Zajištění přístupu k instalaci KNX prostřednictvím připojení VPN: To však vyžaduje router, který podporuje funkce serveru VPN nebo přímo server s funkcemi VPN.
  - Některé z jednoúčelových řešení specializovaného výrobce, které je na trhu k dispozici a vizualizace (např. umožnění přístupu http).
  - KNX je v současné době ve fázi zadávání, s cílem stanovit standardizované řešení KNX pro přístup k instalacím KNX přes internet prostřednictvím webových služeb.



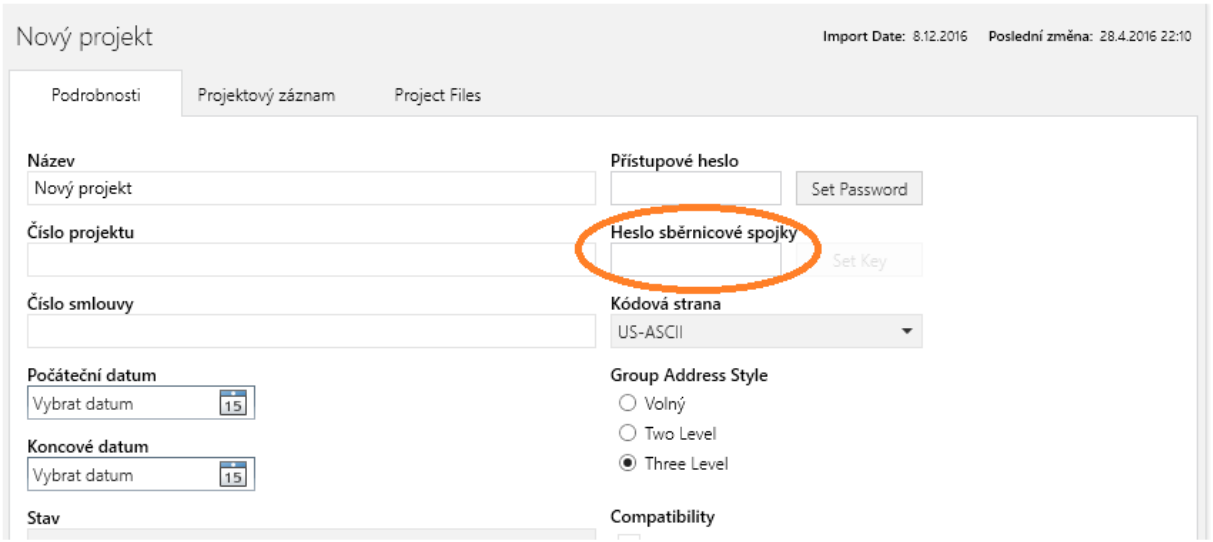
Obr. 1: Přístup k sítím KNX přes Internet

3 Omezení nežádoucí komunikace uvnitř sítě

- Individuální adresy přístrojů musí být řádně přiřazeny v souladu s topologií a routery musí být nakonfigurovány tak, aby nemohly předávat zprávy s neodpovídajícími zdrojovými adresami. Takto lze nežádoucí komunikaci omezit na jednu linii.
- Broadcastingová a nefiltrovaná komunikace přes routery musí být zablokována. Takto bude případná rekonfigurace omezena na jednu linii.
- Spojky musí být nakonfigurovány tak, aby měly nastaveny aktivní filtrační tabulky a nepřenášely skupinové adresy nepoužívané v příslušných liniích. Pokud by tomu tak nebylo, nežádoucí komunikace v jedné linii by nesla riziko nekontrolovaného šíření zpráv po celé instalaci KNX.

4 Ochrana komunikace při konfiguraci

- ETS umožňuje definovat heslo pro konkrétní projekt, jehož prostřednictvím lze uzamknout přístroje před neoprávněným přístupem. Tím se zabrání, aby konfiguraci instalace bylo možné číst nebo měnit neoprávněnými osobami.

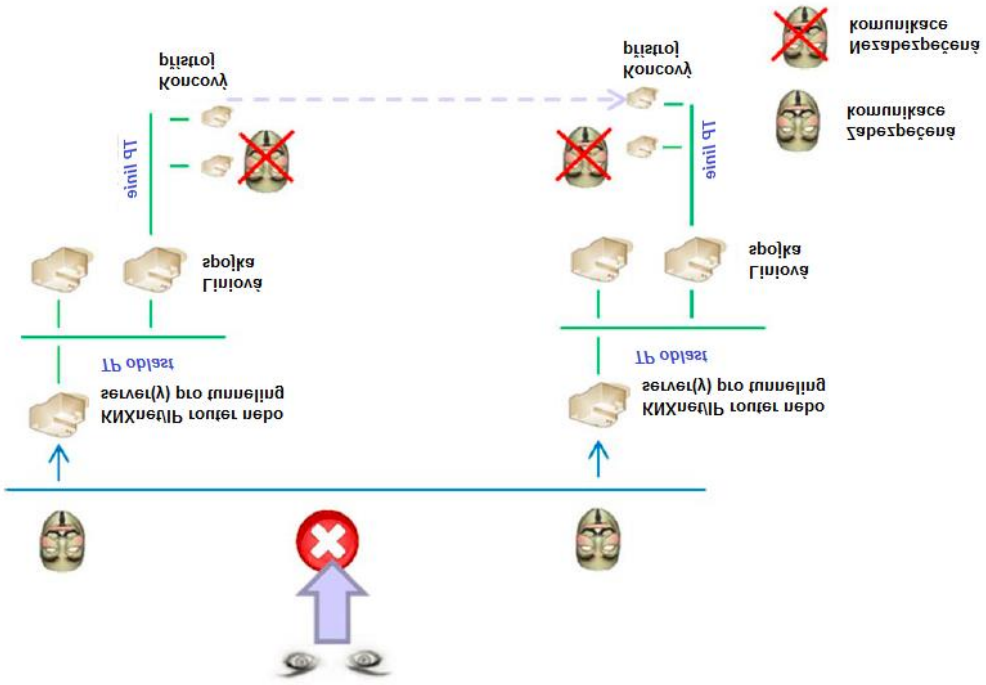


Obr. 2: Ochrana před konfigurační komunikací v ETS

5 Ochrana provozní komunikace

• KNX provozní komunikaci je možné chránit využitím:
- KNX Data Secure a
- KNX IP Secure mechanizmů

• KNX Data Secure zajišťuje, že bez ohledu na přenosové KNX médium, vybrané zprávy odesílané KNX přístroji mohou být ověřovány anebo také šifrovány.
Aby bylo zajištěno, že i v případě, kdy taková komunikace by nebyla zabezpečena, a takovéto sítě by nebyly připojeny k IP, byly definovány výše uvedené mechanismy KNX IP Secure.
Takto je zajištěno, že KNX IP tunneling nebo routing zpráv nelze zaznamenávat ani s nimi manipulovat na IP. KNX IP Secure mechanismus zajistí přidání bezpečnostní obálky ke kompletnímu datovému provozu KNXnet / IP.

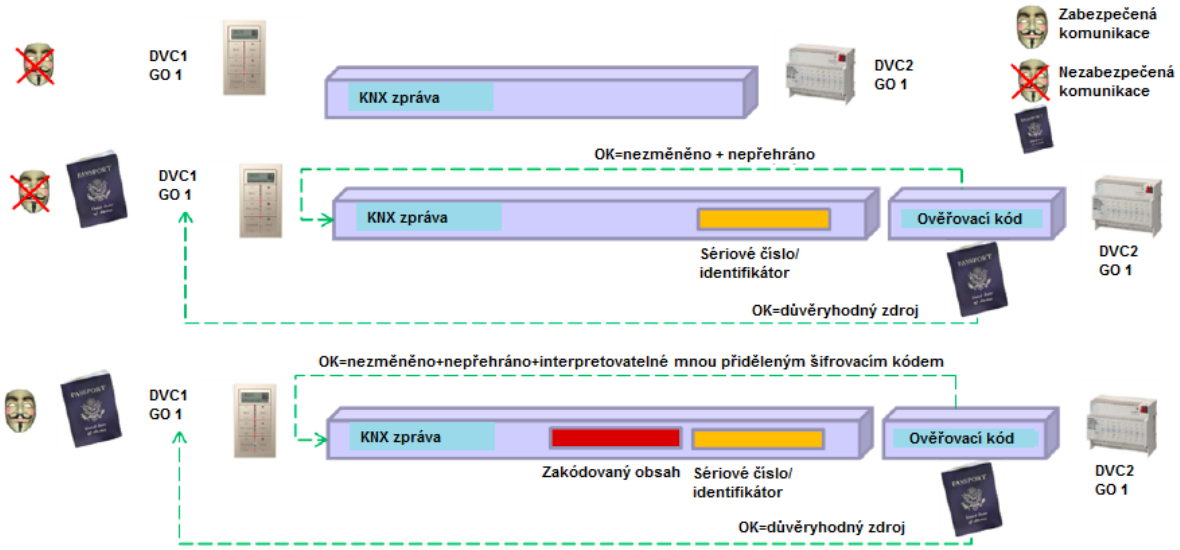


Obr. 3: Ochrana KNX provozní komunikace na síti IP s využitím KNXnet IP Secure

• V KNX Data Secure a KNX IP Secure mechanizmy zajišťují, aby:
přístroje mohly vytvořit zabezpečený komunikační kanál, čímž se zajišťuje:

- *Integrita dat*, tj. zabraňuje se útočníkovi získat kontrolu napíchnutím a manipulací s rámci. V KNX je toto zajištěno připojením **ověřovacího** kódu ke každé zprávě: tento přídavný kód umožňuje ověřit, že zpráva nebyla upravována a že skutečně pochází od důvěryhodného komunikačního partnera.
- *Aktuálnost*, to znamená, že útočníkovi zabraňuje ve využití záznamů rámců jejich pozdějším přehráváním, aniž by manipuloval s obsahem. V KNX Data Secure je to zajištěno sériovým číslem a v KNX IP Secure identifikátorem série.
- *Důvěrnosti*, tj. zašifrování provozu v síti zajišťuje minimální možnost útočníka k nahlédnutí na přenášená data. Když je umožněno **šifrování** KNX síťového provozu, přístroje KNX zajistí šifrování alespoň podle AES-128 CCM algoritmů, společně se symetrickým klíčem.

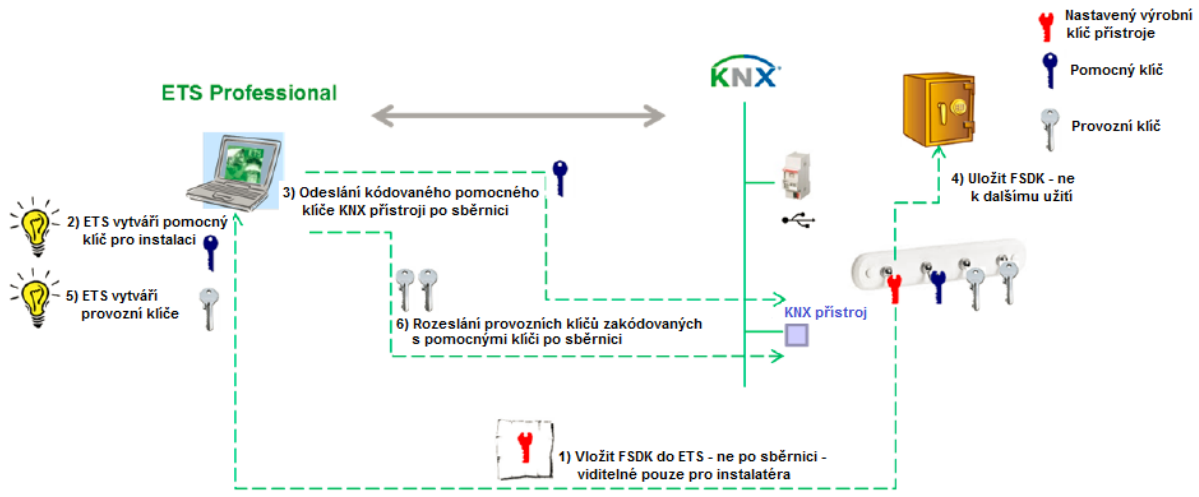
Symetrický klíč znamená, že stejný klíč používá odesílatel k ochraně odchozí zprávy (ověření + důvěrnost!), jakož i v přijímači(ích) k ověření při příjmu této zprávy.



Obr. 4: Přehled činnosti KNX Data Secure

V KNX Data Secure jsou přístroje chráněny následujícím způsobem:

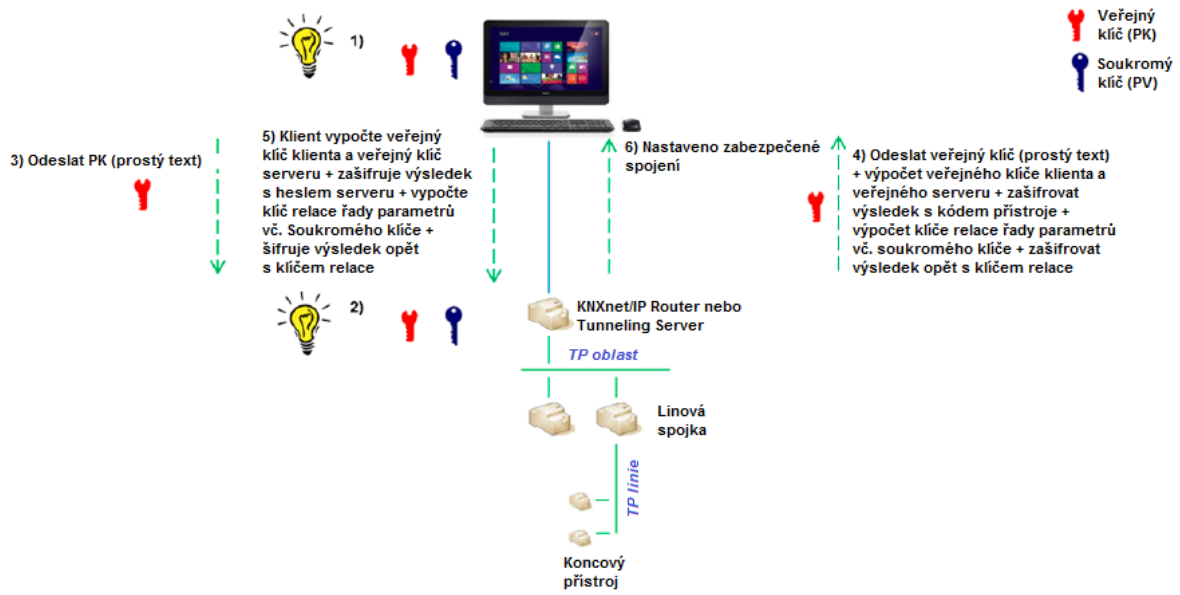
- Přístroj se dodává s jedinečným Nastaveným výrobním klíčem přístroje (FDSK).
- Instalatér vloží tento FDSK do konfiguračního nástroje ETS (tuto akci ale v žádném případě nelze uskutečnit po sběrnici).
- Konfigurační nástroj vytváří pro projekt specifický pomocný klíč.
- ETS po sběrnici odešle přístroji, který má být konfigurován pomocným klíčem, avšak pomocí šifrování a ověření zprávy s předem zadanou FDSK. Ani nástroj ani klíč FDSK nejsou nikdy obsaženy v přenášeném prostém textu na sběrnici.
- Přístroj od té doby využívá pouze pomocný klíč k dalším konfiguracím v ETS. FDSK se již při následné komunikaci nepoužívá.
- ETS vytváří pomocné klíče (kolik jich je zapotřebí) pro skupinovou komunikaci, kterou je nutné zabezpečit.
- Po sběrnici ETS odesílá přístroji, který má být konfigurován tyto provozní klíče, ovšemže využitím šifrování a ověřování zpráv pomocným klíčem. Provozní klíče nejsou nikdy přenášeny po sběrnici ve formátu prostého textu.



Obr. 5: Proces zabezpečení KNX přístrojů

Pro KNX IP Secure, zabezpečené připojení (Tunneling nebo Device Management) je stanovena následujícím způsobem:

- Jak klient, tak i server vytvoří individuální veřejný / soukromý pár klíčů. To se označuje jako asymetrické šifrování.
- Klient pošle svůj veřejný klíč na server jako prostý text.
- Server odpoví s veřejným klíčem v prostém textu, který je přiložen k výsledku následujícího výpočtu: vypočtená hodnota XOR serveru veřejného klíče pomocí veřejného klíče klienta, zašifruje se kódem přístroje pro ověření klienta a zašifruje se podruhé s vypočteným klíčem relace. Ověřovací kód přístroje je buď přiřazen z ETS během konfigurace, nebo je to pomocný klíč. Tento ověřovací kód přístroje musí být poskytnut provozovateli vizualizace, která má být bezpečně propojena s příslušným serverem.
- Klient uskuteční stejnou operaci XOR, ale ověřuje se sám šifrováním, a to nejprve s jedním z hesel serveru a ještě podruhé s klíčem relace.
  Je třeba poznamenat, že použitý šifrovací algoritmus (Diffie Hellmann) zajišťuje, že klíč relace klienta a serveru jsou shodné.
  Hesla serveru musí být poskytována provozovateli vizualizace, když chce navázat bezpečné spojení s příslušným serverem.



Obr. 6: Nastavení KNX IP Secure spojení

6 Propojení KNX do zabezpečených systémů

Připojení KNX k takovým aplikacím, jakými jsou zabezpečovací systémy proti vloupání / požární ochrana / vstupní dveřní systémy, lze zajistit:

- KNX přístroji nebo rozhraními s příslušnou certifikací místních pojišťoven;
- bezpotenciálovými kontakty (binárními vstupy, tlačítkovými rozhraními apod.);
- odpovídajícími rozhraními (jako RS232) nebo hradly: v tomto případě musí být zajištěno, aby komunikace KNX nevyvolala příslušné funkce zabezpečení v bezpečnostní části instalace.

7 Detekce neautorizovaných přístupů ke sběrnici

- Je samozřejmé, že sběrnici lze monitorovat a tak vysledovat neobvyklý provoz.
- Některé typy přístrojů mohou detekovat, zda jiný přístroj nevysílá telegramy s jejich individuální adresou. To není samovolně oznámeno v síti, ale lze to načíst z PID_DEVICE_CONTROL.
- Velmi aktuální implementace se může projevit již v PID_DOWNLOAD_COUNTER. Porovnáním čtení hodnoty (pravidelně) s referenční hodnotou bude signalizována změna v konfiguraci přístroje.

8 Literatura

[1] AN 158 v02 KNX Data Security DP Version
[2] AN 159 v04 KNX IP Secure DP Version
[3] Volume 3/8/x KNXnet/IP Specifications – KNX Standard Version 2.1