Primjena KNX Secure tehnologije u radu pametnog brojila

Application of KNX Secure technology in the operation of a smart meter

Slobodanka Jelena Cvjetković[a,*], Siniša Zorica[a], Zvonimir Tomić[a], Želimir Jonić[b]

[a] University of Split, University department of professional studies, Kopilica 5, 21000 Split, Croatia
[b] Global Offshore Engineering, Singapore

*Corresponding author: sjcvjet@oss.unist.hr

INFORMACIJE O ČLANKU

Kategorija:
Stručni rad

Ključne riječi:
niskonaponska mreža
energetski kabel
energija
održavanje

Licenca: CC BY-NC-SA 4.0.

SAŽETAK

Živimo u eri enormne razmjene podataka te je cilj svake zemlje projektirati elektroenergetski sustav sa zadovoljnim krajnjim korisnikom. Za nesmetan razvoj i rad tržišta električne energije postavljaju se zahtjevi informatizacije i automatizacije elektroenergetskog sustava. Budući da je svaka ušteda energije dragocjena, cilj je racionalnije raspolagati energijom, adekvatno bilježiti potrošnju i analizirati je. Ugradnjom pametnog brojila postiže se jedna od bitnih prednosti, elastičnost tarifnog sustava i naplate. Komunikacija sustava pametnih brojila funkcionira na principu prikupljanja podataka i može se ostvariti različitim komunikacijskim tehnologijama. Međutim, tajnost podataka predstavlja kompleksnu zadaću, jer svako neovlašteno korištenje utječe na isporuku električne energije i stabilnost sustava. U svakom trenutku prenose se i obrađuju milijarde megabajta podataka. Zabrinuti smo jesu li naši najosjetljiviji podaci ugroženi. Primjenom KNX Secure tehnologije, koja je standardizirana prema EN 50090-3-4, uspješno se blokiraju hakerski napadi na digitalnu infrastrukturu umreženih zgrada. U radu će se prikazati implementacija KNX Secure sustava u skladu sa standardom ISO/IEC 18033-3. Razvojem inteligentnih elektronskih brojila i komunikacijskih uređaja omogućit će se unaprjeđenje distribucijskog sustava u smislu veće transparentnosti i poboljšane učinkovitosti svim sudionicima na tržištu električne energije.

ARTICLE INFORMATION

Category:
Professional paper

Keywords:
low voltage network
power cable
energy
maintenance

License: CC BY-NC-SA 4.0.

ABSTRACT

We live in an era of enormous data exchange, and the goal of every country is to design an electric power system with a satisfied end user. For the smooth development and operation of the electricity market, there are requirements for computerization and automation of the electric power system. Since every energy saving is precious, the goal is to use energy more rationally, adequately record consumption and analyse it. By installing a smart meter, one of the essential advantages is achieved, the flexibility of the tariff system and billing. The communication of the smart meter system works on the principle of data collection and can be achieved with different communication technologies. However, data secrecy is a complex task, because any unauthorized use affects the delivery of electricity and the stability of the system. Billions of megabytes of data are being transferred and processed at any given moment. We are concerned if our most sensitive data is compromised. By applying KNX Secure technology, which is standardized according to EN 50090-3-4, hacker attacks on the digital infrastructure of networked buildings are successfully blocked. The paper will present the implementation of the KNX Secure system in accordance with the ISO/IEC 18033-3 standard. The development of intelligent electronic meters and communication devices will enable the improvement of the distribution system in terms of greater transparency and improved efficiency for all participants in the electricity market.

1. Uvod

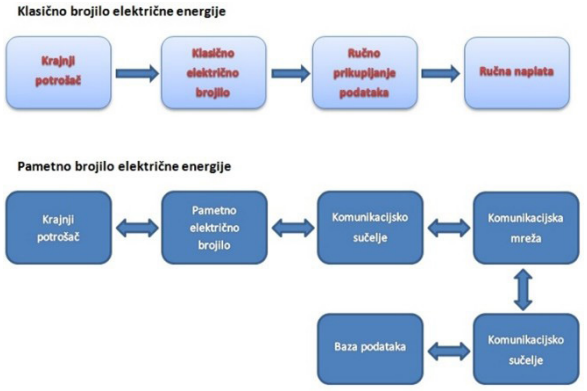
Električnim brojilima registrira se potrošnja električne energije prema tarifnim sustavima, koja su u Republici Hrvatskoj (RH) definirana kao jednotarifna ili dvotarifna. Ovisno o potrebama korisnika mjeri se djelatna [kWh] i/ili jalova energija [kVArh]. Razvojem tehnologije u sustav se implementiraju pametna brojila za pouzdaniji uvid u stanje potrošnje električne energije. U svrhu kontrole vršnog opterećenja potrebno je imati točne podatke o potrošnji energije u svakom trenutku. Brojilo se priključuje na napone između 80 % i 110 % vrijednosti nazivnog napona. Ne smije primjetno šumiti u slučaju opterećenja maksimalnom strujom i/ili pri bilo kojem opterećenju do maksimalne struje te pri ispitivanju promjena utjecajnih veličina propisanim uvjetima.

2. Izvedba pametnih brojila

Prema izvedbi i principu rada pametno brojilo je opremljeno dodatnim komunikacijskim i upravljačkim sustavima koji uvelike povećavaju njegove mogućnosti.
Pametna brojila objedinjuju hardverski, softverski i kalibracijski sustav [1]. Osnovni dijelovi digitalnog brojila su:

- analogni dio,
- analogno – digitalni pretvarač (AD pretvarač),
- digitalni dio.

Elektroničko brojilo je opremljeno protuprovalnim sustavom, koji proradi kada kupac pokuša otvoriti poklopac, ukloniti brojilo iz ormarića ili reprogramirati brojilo. Na slici 1. je prikazana mjerna struktura klasičnog i pametnog brojila.



Slika 1. Mjerna struktura klasičnog i pametnog brojila [2]
Figure 1 Measurement structure of classic and smart meter [2]

3. KNX - Secure

Živimo u eri digitalnog, povezanog, automatiziranog, pametnog tehnološkog napretka, tj. eri enormne razmjene podataka. U ovom trenutku prenosi se i obrađuje milijarde megabajta podataka. Zato smo zabrinuti jesu li naši najosjetljiviji podaci ugroženi, hoće li biti hakirani i zloupotrijebljeni. Suvremeni svijet razvojem modernih tehnologija ima beskrajne mogućnosti i isto toliko opasnosti. Zahvaljujući etičkim hakerima, prije nekoliko godina pokrenuto je pitanje sigurnosti sustava automatizacije doma i zgrade. KNX korištenjem sigurnih KNX medija upredene parice (Twisted Pair, TP) i energetskog kabela (Powerline, PL) uz mogućnost bežičnog pristupa putem radio frekvencijskih kanala (KNX Radio Frequency, KNX RF) i Internet protokola (KNXnet/IP) 2016. je predstavio novo proširenje standarda-KNX Secure. Slijedom toga KNX Association kontinuirano radi na finalizaciji KNX Secure protokola.

Komunikacijski sustavi podložni su zlouporabi i neovlaštenom korištenju te je nužno osigurati mjere kako bi se spriječila zloupotreba podataka i zaštita osobnih podataka korisnika. Tajnost podataka predstavlja kompleksnu zadaću, jer svako neovlašteno korištenje utječe na isporuku električne energije i stabilnost sustava. Tajnim podacima treba zaštiti:

- informacije o cijenama,
- upravljačke kontrole,
- tajnost podataka o korisniku i brojilu.

Osim navedenih sigurnosnih aspekata, mjerni i komunikacijski kanali ne smiju negativno utjecati na kvalitetu i isporuku električne energije. Kod priključaka sa snagom iznad 30kW, potrebno je realizirati minimalne zahtjeve i redovito provjeravati brojila. Točno mjerenje djelatne i jalove električne energije, mjerenje električne energije u više smjerova, mjerenje krivulja tereta, itd. osnova su zadovoljnog korisnika i isporučitelja električne energije. Neposredno očitavanje navedenih parametara u zadanom obračunskom razdoblju ponekad nije izvedivo i velika je vjerojatnost:

- ljudske pogreške pri očitavanju,
- gubitka očitanih podataka uzrokovanih kvarom opreme,
- nepotpunosti očitanih podataka,
- velike geografske udaljenosti i nedostupnosti mjernih mjesta,
- velikih troškova izlaska djelatnika na teren.

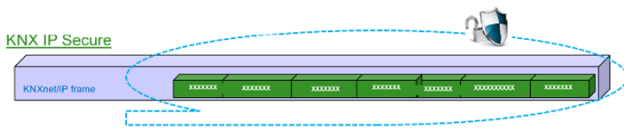
Korištenjem pametnih brojila i sustava za daljinski nadzor i očitavanje brojila izbjegnuta je zlouporaba, te je sustav isplativiji, efikasniji i pouzdaniji.

3.1. Sigurnosni aspekti i pouzdanost sustava

U nekoliko jednostavnih koraka opisati će se KNX Secure. Koristi se provjereni mehanizam šifriranja, američki državni standard za šifriranje, (Advanced Encryption Standard, AES) u skladu sa standardom ISO/IEC 18033-3. Standard AES-128 CTR Secure enkripcije progresivno koristi više rundi enkripcije za poboljšanu sigurnost u načinu rada i AES-CBC-MAC potpisom (CCM) s veličinom bloka 128 bita. Algoritam AES enkripcije koristi šifru za definiranje šifriranog teksta iz otvorenog teksta i obrnuto. Enkripcija pruža funkciju privatnosti podataka. Kada je u pitanju KNX Secure, razlikujemo KNX Data Secure (slika 2.) i KNX IP Secure (slika 3.). KNX Data Secure odnosi se na sve KNX uređaje, dok se KNX IP Secure odnosi samo na IP uređaje. Temeljna razlika temelji se na slijedećim činjenicama. KNX Data Secure šifrira samo Application Protocol Data Unit (APDU), a IP Secure šifrira cijeli KNX okvir. U kontekstu pametnih kartica APDU je komunikacijska jedinica između čitača pametnih kartica i pametne kartice. Struktura APDU definirana je ISO/IEC 7816-4. KNX DATA Secure Payload je šifriran unutar S-A Data Service.



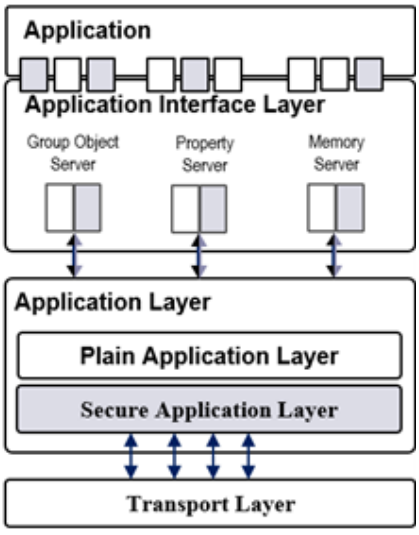
Slika 2. KNX Data Secure [3]
Figure 2 KNX Data Secure [3]



Slika 3. KNX IP Secure [3]
Figure 3 KNX IP Secure [3]

Međutim, u KNX Data Secure niža polja KNX stoga kao što su adresa izvora, TPCI i NPCI prenose se kao običan tekst, ali koriste se kao unos tijekom procesa enkripcije. Telegram Protocol Control Information, TPCI koristi prilagođenu shemu simetrične enkripcije koja se zove MTProto., a temelji se na 256-bitnoj simetričnoj AES enkripciji, 2048-bitnoj RSA enkripciji i Diffie-Hellman razmjeni ključeva. Network Protocol Control Information, NPCI prati upite i odgovore između komunikacijske opreme za određivanje odgovarajućih mogućnosti svakog kraja komunikacijske veze. Time je omogućen normalan rad postojećim usmjerivačima i spojnicama linija unutar instalacije.

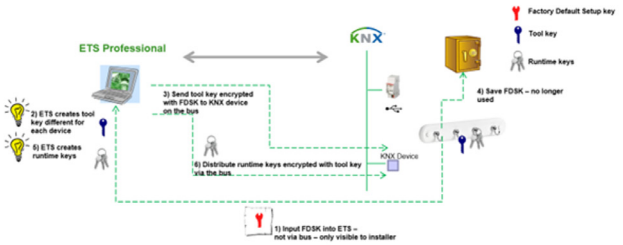
Dakle, kako se vidi na slici 4. KNX Secure format okvira odabran je u skladu s poznatim načelom standarda KNX - kompatibilnost unazad. Cjelokupna "inteligencija" Secure mehanizma unutar KNX stoga predstavljena je aplikacijskim slojem KNX stoga koji se može podijeliti na obični i sigurni aplikacijski sloj. Unutar sigurnog aplikacijskog sloja uvode se interni parametri za definiranje sigurnosti: tablica veza autentifikacije, povjerljivosti i sigurnosti. Unutar sloja aplikacijskog sučelja poslužitelja objekata, poslužitelja svojstava i poslužitelja memorije dodatno je proširena funkcionalnost za podršku sigurnosti KNX-a.



Slika 4. KNX format okvira [4]
Figure 4 KNX frame format [4]

Uvođenjem KNX Secure-a (slika 5.) definirani su novi pojmovi. Za bolje razumijevanje proširenja protokola potrebno je razumjeti značenje novih izraza: certifikat uređaja, FDSK, serijski broj, ključ alata, grupni ključ i ključ okosnice. Certifikat uređaja sastoji se od tvornički zadanog ključa (Factory Default Setup Key, FDSK) i serijskog broja te svojom dužinom ima 36 simbola.

Engineering too software, ETS je jedinstveni alat za projektiranje i puštanje u rad, koji koristi siguran preglednik i njime se onemogućuje ispitanicima pristup svemu osim sadržaju testa tijekom administracije. ETS zahtijeva certifikat uređaja za prvu konfiguraciju s KNX Secure, te skupno Data i IP Secure. Certifikati uređaja čuvaju se pohranjeni unutar ETS projekta i mogu se dobiti iz izvješća ETS projekta. Naljepnice s certifikatom uređaja (Tekst + QR kod) nalaze se na uređaju i treba ih ukloniti prije montaže istog. Certifikate uređaja (naljepnice i izvješća) treba sigurno pohraniti. Ako se izgube uređaj se više ne može koristiti u sigurnom projektu.



Slika 5. Topološki prikaz KNX Secure [4]
Figure 5 Topological view of KNX Secure [4]

FDSK je "ex-tvornička" vrijednost, što znači da je proizvođač dodjeljuje svakom uređaju tijekom proizvodnje. ETS zahtijeva FDSK za prvu konfiguraciju ili nakon svakog glavnog resetiranja. To je dio certifikata uređaja i ETS ga može očitati izravno iz QR koda. FDSK je ključ dug 128 bita i nakon prve konfiguracije postaje neaktivan, a ETS nakon toga koristi ključ alata. FDSK se ne može promijeniti te se zamijeni ključem alata za slučaj ako jedan proizvođač ima problem s privatnošću FDSK. Na mjestu instalacije ostali uređaji nisu ugroženi. Serijski broj kao dio certifikata uređaja, za sve KNX proizvođače, je jedinstveni broj od 6 bajta. KNX serijski broj ima ključnu ulogu tijekom puštanja u rad s ETS-om te omogućuje reprogramiranje uređaja bez fizičkog pristupa tipkalu za programiranje.

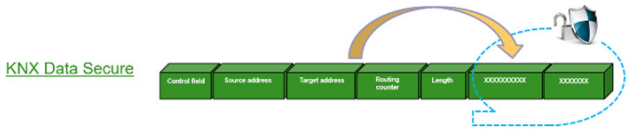
Tijekom konfiguracije može se pristupiti uređaju korištenjem ključa, komunikacijskom vezom od točke do točke. Ključ alata generira se u ETS-u i uređaju se dodjeljuje se tijekom prvog puštanja u rad. Ključ alata pohranjuje se u ETS projektu te izvješću o projektu definira sigurnost projekta. Ako se ETS projekt izgubi zajedno s tipkom Tool moguće je samo vraćanje na tvorničke postavke. U tom slučaju FDSK se ponovno aktivira jer vraćanjem na tvorničke postavke briše se alatna tipka i preuzima FDSK. Tijekom komunikacije između grupnih adresa koristi se ključ grupe.

U jednom projektu, za svaku grupnu adresu postoji pojedinačni ključ. Ključ je dugačak 128 bita, dodjeljuje se i pohranjuje unutar ETS-a. Također, nalazi se u izvješću o projektu - sigurnost projekta. Nakon vraćanja na tvorničke postavke ovi se ključevi brišu. Ključ okosnice koristi se za sigurno IP usmjeravanje. Svi IP uređaji u jednom projektu imaju isti ključ okosnice. Nakon resetiranja na tvorničke postavke briše se i glavni ključ.

Za enkripciju se koriste različiti ključevi u slučaju kada je određeni dio KNX instalacije ugrožen. Korištenjem različitih ključeva za šifriranje sprječava se kompromitacija podataka cjelokupne KNX instalacije. Još su neke značajke uvedene za potrebe KNX sigurnosti, a to su grupna dijagnostika objekata i prošireni (dugi) okviri. Ali, nisu ekskluzivne za KNX sigurnost.

Redni broj usluge S¬¬-A Data dug je 6 bajta. Uređajima koji šalju telegrame na KNX sabirnice dodjeljuje se jedan redni broj po uređaju. Redni broj se kontinuirano povećava na poslanoj poruci. Međutim, uređajima koji primaju telegrame sa sabirnice dodjeljuje se jedan redni broj po svakom komunikacijskom partneru. Tijekom primanja telegrama s KNX sabirnice prihvaćaju se samo poruke s većim rednim brojevima. Ukratko, redni broj definira i osigurava trenutnu razmjenu podataka sprječavajući njihovo snimanje i reprodukciju.

S-A Data usluga Secure Control Field osim sekvencijskog broja, dužine jedan bajt, sadrži i prenosi informacije (slika 6.):
- pristupa li se korištenoj usluzi ključem alata
- razlikuje S-Data i S-A Sync uslugu (unutar S-A Data usluge pakiraju se sve dosad poznate usluge, a S-A Sync se koristi za potrebe ažuriranja rednih brojeva između komunikacijskih partnera u bilo kojem trenutku)
- daje informacije o autentifikaciji i povjerljivosti.



Slika 6. Prikaz S-A Data servisa [4]
Figure 6 Display of S-A Data service [4]

Poznato je da su autentifikacija i povjerljivost interni parametri Secure Application Layer. Autentikacija realizirana Message Authentication Code, MAC dužine je 4 bajta i njom se osigurava integritet podataka sprječavajući napade na podatke. Za izračun MAC-a koristi se AES. Informacije ulaze iz običnog okvira, uključujući duljinu i tajni ključ iz ETS-a. Povjerljivost onemogućava praćenje podataka. Payload je šifriran AES-om, te se za unos koriste informacije iz običnog okvira i drugi tajni ključ iz ETS-a.

S-A Data uslugom može se isključivo pristupiti šifriranim osobnim kodom ili koristiti s ovjerenim povjerljivim pristupom. Uslugom S-A Sync koristimo se uvijek s šifriranim osobnim kodom (autentifikacijom) koji je ovjeren te je pristup siguran i za povjerljivu razmjenu podataka. Uz MAC S-A Sync dolazi Challenge koji je također dug 4 bajta.

3.2 KNX IP Secure

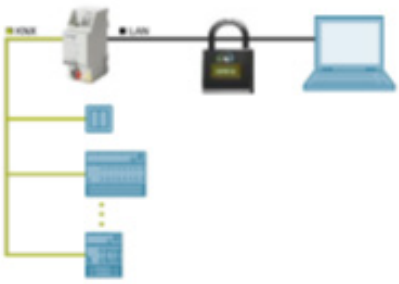
Dva su poznata protokola koja se koriste u KNXnet/IP: tuneliranje i usmjeravanje. Tuneliranje je protokol koji omogućuje siguran prijenos podataka s jedne mreže na drugu. Protokol usmjeravanja koristi se za komunikaciju između IP uređaja. Može se reći da se na razini usmjeravanja IP Secure štiti podatke na IP mreži.

U IP Secure protokolu KNX telegram je upakiran u Secure okvir i šifriran glavnim ključem. Tijekom višesmjerne komunikacije koristi se isti ključ šifriranja. Za razliku od TP uređaja, preporuka je da svi IP uređaji podržavaju KNX IP Secure. U KNX IP Secure uvedeno je više novih usluga, ali postojeće standardno KNXnet/IP zaglavlje je nepromijenjeno i podržava se verzija protokola 10h - ponovno je osigurana kompatibilnost s prethodnim verzijama. Na principu AES-a izračunava se enkripcija korisnih podataka na način kao i za Data Secure. Razmjenu trenutnih podataka omogućuje Time Stamp, dijeljeni mjerač vremena, koji se dodaje svakom okviru prilikom slanja. Okviri sa zastarjelim mjeračima vremena se odbacuju prilikom primanja novih podataka. Protokol tuneliranja u KNX komunikaciji koristi se za ETS i softver za vizualizaciju putem IP sučelja ili IP rutera. Za svaku tunelsku vezu potrebna je jedna lozinka. Na razini tuneliranja, KNX IP Secure štiti KNX mrežu od neovlaštenog pristupa.

Iako se desetljećima smatrao jednim od najsigurnijih i najpouzdanijih sustava za automatizaciju potrebno je uvesti nove mehanizme šifriranja instalaciju KNX-a. Kada se ispravno instalira, primjenom KNX sigurnosnih popisa KNX instalacija ostaje sigurna. Sigurnosni propisi kojih se trena pridržavati su slijedeći:
- ograničavanje pristupa instalaciji (kabelima i uređajima),
- pohranjivanje uređaja u zatvorenu kutiju,
- sprječavanje izravnog pristupa internetu,
- omogućavanje pristupa samo putem VPN-a itd.

Međutim, prednost KNX-a je njegova fleksibilnost. Može se proširiti u bilo kojem trenutku spojnicama za medije/segmente, dodavanjem bežičnih i IP uređaja postojećim ili novim instalacijama tako da instalaciju zaštiti u slučaju opasnosti od hakiranja i ugrožavanja podataka i zlouporabe . Kako bi zadržao status sigurnog i pouzdanog sustava automatizacije KNX je proširen na KNX Secure ponudu.

Jasno je da KNX sigurnost nije uvjet za svaki uređaj u KNX instalaciji. Moguće je kombinirati sigurne i nesigurne instalacije te proširiti postojeću instalaciju sigurnom instalacijom. Kako bi nesigurna KNX instalacija s ograničenim pristupom internetu postala sigurnija dovoljno je dodati jedno IP sučelje KNX IP sigurnom sučelju. Na slici 7. prikazan je primjer



Slika 7. Primjer KNXnet/IP sigurnog tuneliranja [4]
Figure 7 Example of KNXnet/IP secure tunneling [4]

sigurnog tuneliranja.

Kako bi postojeća KNX nesigurna instalacija s IP

linijama bila sigurna, KNXnet/IP usmjerivač treba zamijeniti KNXnet/IP sigurnim usmjerivačima.



Slika 8. Primjer KNXnet/IP sigurnog usmjeravanja [4]
Figure 8 Example of KNXnet/IP secure routing [4]

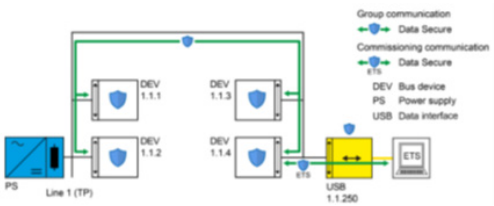


Slika 9. Topologije linija sa svim KNX Secured uređajima [4]
Figure 9 Line topologies with all KNX Secured devices [4]

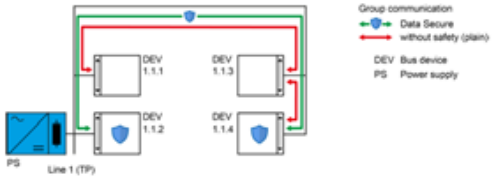
Sada će razmjena podataka između KNXnet/IP uređaja biti KNX IP Secure. Na slici 8. prikazan je primjer KNXnet/IP sigurnog usmjeravanja.

Prvi korak u povećanju zaštite nesigurnih instalacija je zamjena starih linijskih spojnica (segmentnih spojnica) KNX Secure verzijom. Zanima nas sigurna komunikacija u jednoj KNX liniji. Na slici 9. može se vidjeti primjer topologije linije sa svim KNX Secured uređajima.

KNX Data secure koristi prošireni Frame format za šifrirane podatke, ali to ne utječe na sposobnost uređaja da brzo obradi podatke i reagira. U primjeru prikazanom na slici 10. nezaštićeni uređaji koriste se



Slika 10. Nezaštićeni uređaji koriste se u istoj instalaciji s KNX Data Secure uređajima [3]
Figure 10 Unsecured devices are used in the same installation with KNX Data Secure devices [3]



Slika 11. Kombinacija sigurne i obične komunikacije [3]
Figure 11 Combination of secure and ordinary communication [3]

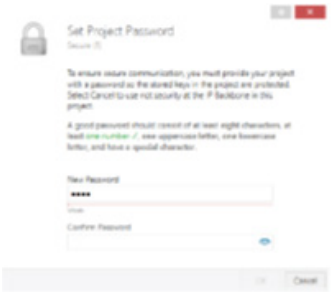
u istoj instalaciji s KNX Data secure uređajima. Nakon sigurnog puštanja u rad s ETS-om KNX Data Secure uređaji s drugim KNX Data Secure uređajima mogu razmjenjivati podatke na siguran način putem grupnih adresa. Tijekom razmjene podaci su šifrirani grupnim ključevima, ali komunicirati se može i na staromodan (nesiguran) način putem odabrane grupne adrese.

Moguća je kombinacija sigurne i obične komunikacije preko različitih komunikacijskih objekata, ali nije moguća kombinacija sigurne i obične komunikacije pomoću jednog te istog komunikacijskog objekta (slika 11.).

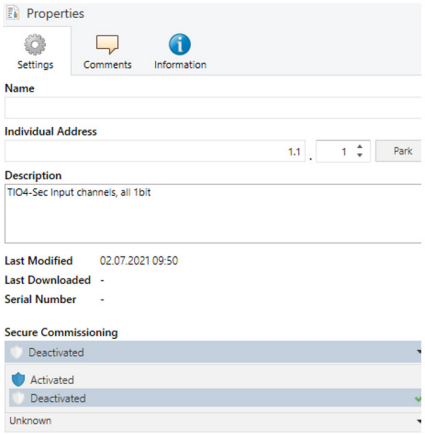
U ETS projektu je vidljivo koje grupne adrese komuniciraju na ne/siguran način. Budući da KNX Secure zahtijeva prošireni format okvira telegrama za prijenos podataka sve komponente sustava u instalacijskoj liniji, područnim i segmentnim spojnicama, te sučelja za ETS također će podržavati prošireni format okvira u mješovitoj KNX plain-secure instalaciji. Ovo je vrlo važno u komunikaciji preko linija. Međutim, u slučaju ako komponente sustava ne podržavaju KNX Data Secure niti EFF, KNX zaštićeni uređaji unutar jedne linije ili segmenta mogu i dalje komunicirati na siguran način i biti pušteni u rad na siguran način putem lokalnog sučelja.

3.3 Postavljanje projekta KNX Data Secure u ETS-u

Za ETS projekt koji koristi KNX Data Secure potrebna je lozinka (isto se primjenjuje na KNX IP Secure). Ova lozinka koristi se za zaštitu ključeva alata i grupe (kao i ključa okosnice u slučaju KNX IP Secure) u projektnim i sigurnosnim postavkama uređaja. Lozinka se može unijeti (slika 12.) prilikom otvaranja ili uvoza ETS projekta. Ako lozinka projekta nije postavljena, uređaji koji se koriste u ETS projektu komuniciraju isključivo u običnom načinu rada te se uređaji automatski postavlja na "nesigurne". U slučaju da se lozinka izgubi, ETS projekt se više ne može koristiti i svi podaci unutar njega su izgubljeni.
Ako su KNX Data Secure uređaji planirani za sigurnu komunikaciju tijekom rada, ETS ih također mora pustiti u rad na siguran način. Za uređaje koji se puštaju u rad na jednostavan način, tijekom rada je moguća samo komunikacija na jednostavan način.
Za svaki uređaj u ETS projektu koji podržava KNX Data Secure sigurno puštanje u rad može se uključiti ili isključiti kako je prikazano na slici 13. Pri čemu je "Sigurno puštanje u rad - aktivirano" zadana postavka za uređaje koji podržavaju sigurnost.



Slika 12. Dodjeljivanje lozinke unutar korisničkog sučelja ETS-a [4]
Figure 12 Assigning a password within the ETS user interface [4]



Slika 13. Upravljački sustav ETS-a [4]
Figure 13 Management system of ETS [4]

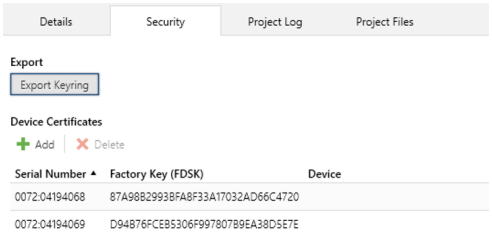
ETS će tražiti certifikat uređaja tijekom programiranja ovog uređaja i zatim će dodijeliti ključ alata kao što je objašnjeno ranije u ovom tekstu. S druge strane, "Sigurno puštanje u rad - deaktivirano" znači da će se puštanje u pogon izvršiti na poznat jednostavan način. Uređajima koji se puste u rad na ovaj način nije moguće dodijeliti grupne ključeve za KNX Data Secure runtime komunikaciju.

Treba svakako znati da se stanje može promijeniti u bilo kojem trenutku i uređaj se može ponovno pustiti u rad iako će svi sigurni podaci će biti izgubljeni kada se prebaci sigurno puštanja u rad s aktiviranog na deaktivirani.

Prije puštanja uređaja u rad postavlja se certifikat uređaja na zahtjev ETS-a (slika 14.). Iz njega i serijskog broja odredi se FDSK. Očitati se može na različitim lokacijama ETS-a, ali je intuitivno pogodnije očitati ga na nadzornoj ploči projekta.

Nakon što je projekt otvoren i postavljena lozinka popis je prazan. Klikom na ikonu plus višestruki certifikati uređaja mogu se dodati upisivanjem na tipkovnici ili skeniranjem kamerom.

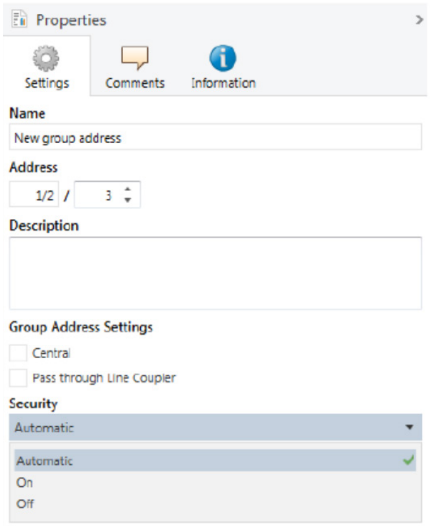
Na nadzornoj ploči projekta, kartici Sigurnost, vidi se odaslani kod za ključeve. Kod za ključeve sadrži sve certifikate uređaja, a nakon puštanja u rad pohranjuje nazive uređaja i fizičke adrese.



Slika 14. Dodjeljivanje certifikata unutar ETS-a [28]
Figure 14 Awarding of certificates within ETS [28]

3.4 Dizajniranje ETS projekta za sigurnu komunikaciju u vremenu izvođenja

Glavni cilj KNX Data Secure je osigurati end-to-end zaštitu, tj. osigurati komunikaciju od pošiljatelja do primatelja (slika 15.). Tijekom izvođenja za komunikaciju u KNX-u koristimo grupne adrese, koje se koriste u multicast komunikacijskom načinu. Grupne adrese dodjeljuju se komunikacijskim objektima u ETS-u te im se pridružuju dodatne sigurnosne postavke. Komunikacija se ostvaruje ovisno o dodijeljenom komunikacijskom objektu: uvijek na jednostavan način, uvijek na siguran način ili automatski jednostavno ili sigurno.



Slika 15. Povratna informacija sustava ETS-a [4]
Figure 15 Feedback of the ETS system [4]

3.5 "Automatska" postavka KNX Data Secure

Ako u instalaciji imamo jedan KNX Data Secure preklopni senzor TAI-X i 2 preklopna aktuatora, od kojih je jedan KNX Data Secure pušten u rad MIO-X, a drugi je pušten u rad na jednostavan način MIO. Komunikacijskom objektu izlazne komutacije TAI-X dodijeljena je ista grupna adresa kao i komunikacijskom objektu ulazne komutacije MIO-X. ETS će zbog ove postavke “sigurnosno-automatski” dodijeliti grupni ključ ovoj grupnoj adresi, na primjer 1/2/3. Ako je ovaj GA 1/2/3 također dodijeljen komunikacijskom objektu ulaznog preklapanja aktuatora MIO, ETS će prepoznati da nova veza ne može komunicirati na siguran način i ukloniti grupni ključ.

Sva tri uređaja moći će komunicirati samo s grupnom adresom 1/2/3 na jednostavan način. Ukratko, svi multicast komunikacijski partneri iste grupne adrese bit će pušteni u rad na siguran način, inače će "automatska" postavka pripisati ovoj grupnoj adresi - nesigurno.

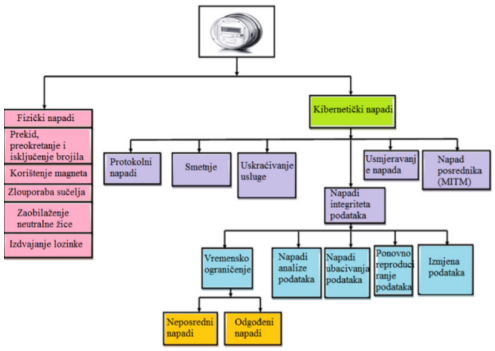
Naglasimo, KNX uređaji koji podržavaju KNX Data Secure i pušteni su u rad na siguran način, razmjenjuju podatke s drugim KNX sigurnim uređajima putem sigurnih grupnih adresa, ali također, mogu komunicirati na jednostavan način putem drugih grupnih adresa. Kombinacija rada zaštićene i obične komunikacije je moguća, ali ne preko jedne te iste grupne adrese.

Također, sigurne postavke grupnih adresa u bilo kojem trenutku mogu se razmijeniti u ETS-u. Kako bi promjena funkcionirala uređaj je potrebno reprogramirati od strane ETS-a. To utječe na više uređaja i zahtijeva se veći oprez pri razmjeni sigurnih postavki adresa središnje grupe.

3.6 Zakonski propisi za zaštitu i sigurnost podataka

Zakonski propisi Europske unije, Europske komisije i Vijeća rigorozni su po pitanju zaštite i sigurnosti podataka. Narušavanje privatnosti te zaštite podataka smatra se jednim od problema koji je neminovan implementacijom pametnih brojila. Navedena problematika je osjetljiva tema te države članice EU trebaju uskladiti svoje prijedloge zakona za implementaciju pametnih brojila prema zakonima koje su europske institucije stavile na snagu. Prvi propis kaže da sustavi pametnog mjerenja trebaju biti u skladu s važećim Pravilima Unije o zaštiti podataka (Union data protection rules).

Članak 8. Europske konvencije o ljudskim pravima (Article 8 of the European Convention on Human Rights) smatra se jednom od najotvorenijih odredbi Konvencije. Temelji se na pravu poštivanja privatnog i obiteljskog života, uz određena ograničenja koja su zakonski usklađena i neophodna u demokratskom društvu. Komisija je 2012. predložila smjernice u skladu s Preporukom 2012/148/EU koje su uključile razmatranja o sigurnosti i zaštiti podataka. Time se olakšalo državama članicama pripremu za razvoj sustava pametnog mjerenja s ciljem osiguranja temeljnih prava na zaštitu osobnih podataka i privatnosti u razvoju aplikacija i sustava pametnih mreža i implementaciji pametnog brojila. Opća uredba o zaštiti podataka, Uredba (EU) 2016/679 najstroži je propis o privatnosti, a u njemu se, između ostalog, navodi da podatkovni subjekt „ima pravo primati osobne podatke koji se tiču njega i koje je on ili ona dostavio regulatoru, u strukturiranom, često korištenom i strojno čitljivom formatu te ima pravo proslijediti te podatke drugom regulatoru". To znači da podaci dobiveni s pametnog brojila moraju biti dostupni potrošaču s vlastitom proizvodnjom, koji zauzvrat ima pravo dijeljenja istih s trećom stranom. Nadalje, potrošači imaju pravo dobiti sve relevantne podatke o vlastitoj potrošnji. Krajnji potrošač ima pravo dobiti sve relevantne podatke o odgovoru na potražnju ili podatke o isporučenoj i prodanoj energiji, besplatno, najmanje jednom u svakom obračunskom razdoblju. Potrošač može povjeriti trećoj strani upravljanje sustavom potrebnim za njegove aktivnosti, uključujući instalaciju, rad, rukovanje podacima i održavanje sustava, a da se treća strana ne smatra aktivnim potrošačem. Slika 16. prikazuje različite vrste ugrožavanja pametnog brojila, koje



Slika 15. Povratna informacija sustava ETS-a [4]
Figure 15 Feedback of the ETS system [4]

narušavaju njegovo normalno funkcioniranje. Tu se navode mogući problemi zaštite i sigurnosti podataka koji mogu narušiti osobna ljudska prava.

Pametna brojila zahtijevaju potpunu sigurnost i zaštitu u životnom ciklusu te trebaju ispuniti četiri sigurnosna zahtijeva:
- ispravnost uređaja (Device authenticity),
- povjerljivost podataka (Data confidentiality),
- ispravnost i cjelokupnost podataka (Data authenticity and integrity),
- privatnost i sigurnost potrošača (Consumer privacy and security).

Opasnost koja prijeti fizičkim i kibernetičkim napadima koji dovode do krađe podataka ili plina te oštećenje infrastrukture, problem je kojima se ODS-ovi trebaju baviti. Tehnološkim napretkom omogućio se prijenos energije na šire područje, u različite vremenske zone. Međutim, krađe su se pokazale kao velik problem. Senzorima pametnih brojila ODS-ovima se omogućava točno određivanje gubitaka i neovlaštene potrošnje, istovremeno dopuštajući potrošačima praćenje nepravilnosti i krađa s iznimnom točnošću. Međutim, za pametnu mrežu potrebno je prilagoditi infrastrukturu za milijune razmještenih i integriranih uređaja. Pametnom mrežom se pouzdano prati veliki broj uređaja te je neophodno imati savršenu svijest o cijelom sustavu kako bi se održao sigurnim i pouzdanim.

4. Zaključak

U današnje vrijeme svaka ušteda energije je dragocjena. U cilju racionalnijeg raspolaganja energijom potrebno je na zadovoljavajući način bilježiti potrošnju energije, analizirati je i poduzimati odgovarajuće akcije. Ugradnjom pametnog brojila postiže se značajna prednost za potrošača i operatora s aspekta elastičnosti tarifnog sustava i naplate.

Isporučitelj električne energije ostvaruje uštedu i kontrolu opterećenja na način da veće potrošače električne energije uključuje u satima manje potrošnje uz ponudu jeftinijih tarifa. Jeftinije tarife za rezidencijalne korisnike predlažu se u popodnevnim

i noćnim satima, te za vrijeme vikenda i blagdana. Time se smanjuje dnevno opterećenje i postiže se ravnomjernija potrošnja energije tijekom cijelog dana. Također, smanjuje se negativan utjecaj na proizvodnju i energetski sustav za vrijeme vršnih opterećenja.

Putem pametnog brojila vrši se provjera ispravnosti i djelovanja zaštitnih sustava i uređaja za isklop napajanja u slučaju nužde (nevrijeme, požar, potres, itd.). Ispitivanje se vrši na način da brojilo registrira ispad napona u slučaju njihovoga djelovanja, čime se isključuje potreba za izlaskom radnika na teren. Za potpuni rad pametnog brojila nužna je dobra komunikacijska veza između brojila i distributera električne energije.

Pomoću relejnih izlaza brojila i sklopnih aparata moguće je daljinski uključiti ili isključiti krajnjeg korisnika – npr. isključivanje neplatiša.
Razvojem daljinske komunikacije zadnjih godina postignut je novi zamah razvoja elektroničkih brojila. Time je dobivena mogućnost manipuliranja velikim brojem brojila s jednog centralnog mjesta te se štedi novac i vrijeme. Prednosti elektroničkih brojila su očite.
Pitanje je vremena kada će elektromehanička brojila biti u potpunosti potisnuta i zamijenjena elektroničkim. Otvaranjem tržišta električne energije povećavaju se zahtjevi prema mjeriteljstvu distribucijskog sustava, kako u potrebi novog organiziranja rada sa mjernim podacima, tako i u povećanim zahtjevima prema količini mjernih podataka. Otvoreno tržište ima nove zahtjeve prema prikupljanju mjernih podataka:

- podaci moraju biti što prije raspoloživi za korištenje,
- zahtjeva se pristup do baze mjernih podataka,
- podaci se pohranjuju u bazu i dostavljaju sudionicima prema unaprijed dogovorenim terminima.

Svi komunikacijski sustavi podložni su zlouporabi i neovlaštenom korištenju. Nužno je osigurati mjere kako bi se spriječila zloupotreba podataka i zaštita osobnih podataka korisnika. Tajnost podataka predstavlja kompleksnu zadaću, jer svako neovlašteno korištenje utječe na isporuku električne energije i stabilnost sustava.

U radu je opisan KNX Secure sustav i implementacija istog za potrebe sigurnosti prijenosa podataka. Koristi se provjereni mehanizam šifriranja u skladu sa standardom ISO/IEC 18033-3. Sustav nudi potpuno nove pristupe u pogledu skraćivanja vremenskih intervala očitavanja. Temeljem očitanih mjernih podataka mogu se koristiti napredniji tarifni modeli. Razvoj mjeriteljske tehnike, inteligentnih elektronskih brojila i komunikacijskih uređaja, naposljetku će omogućiti razvoj naprednijih, prilagođenijih tarifnih modela rezultirajući unaprjeđenjem distribucijskog sustava u smislu veće transparentnosti i poboljšane učinkovitosti prema svim korisnicima distribucijske mreže kao i prema svim sudionicima na tržištu električne energije.

Cilj je svake zemlje projektirati takav sustav u kojem krajnji korisnik ima što manje briga oko praćenja potrošnje, kvarova i straha zbog nedopuštenih radnji kao što je ilegalno priključivanje, koje može imati tragične posljedice (npr. požar zbog opterećenosti instalacija).

Literatura

[1] npower. E.ON group. Smart meters. Getting the most from your smart meter. Smart energy display help [Pristupljeno 11 lipnja 2020].

[2] Zheng, J., Wenzhong Gao, D., Lin, L. Smart Meters in Smart Grid: An Overview. IEEE Green Technologies Conference, 2013. https://smartmeterdesign.weebly.com/uploads/3/9/7/6/39767258/6_smart_meters_in_smart_grid.pdf [Pristupljeno 21 travnja 2026].

[3] TAPKO technologies. https://www.tapko.de/ [Pristupljeno 19 srpnja 2026].

[4] KNX Association cvba. KNX Cookbook. Amazon Digital Services LLC; 2017. ASIN: B01NA0CE3P. KNX Cookbook Dostupno na: https://www.amazon.com/KNX-Cookbook-Association-ebook/dp/B01NA0CE3P [Pristupljeno 21 travnja 2026].

[5] Sharma K., Saini L.M. Performance analysis of smart metering for smart grid: An overview. Renewable and Sustainable Energy Reviews. 2016, p. 720-735. https://doi.org/10.1016/j.rser.2015.09.065 [Pristupljeno 21 travnja 2026].

[6] Tomić Z. Princip rada pametnog brojila. Završni rad (stručni). Split: Sveučilište u Splitu, Sveučilišni odjel za stručne studije; 2022. Dostupno na: https://urn.nsk.hr/urn:nbn:hr:228:183031 [Pristupljeno 21 travnja 2026].