Komunikacijska podrška sustavima za napredno vođenje elektroenergetskih mreža

Jelić, Jure

Master's thesis / Diplomski rad

2025

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Electrical Engineering and Computing / Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:168:788950

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2025-03-23**

Repository / Repozitorij:

FER Repository - University of Zagreb Faculty of Electrical Engineering and Computing repozitory

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 724

KOMUNIKACIJSKA PODRŠKA SUSTAVIMA ZA NAPREDNO VOĐENJE ELEKTROENERGETSKIH MREŽA

Jure Jelić

Zagreb, veljača 2025.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

DIPLOMSKI RAD br. 724

KOMUNIKACIJSKA PODRŠKA SUSTAVIMA ZA NAPREDNO VOĐENJE ELEKTROENERGETSKIH MREŽA

Jure Jelić

Zagreb, veljača 2025.

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 30. rujna 2024.

DIPLOMSKI ZADATAK br. 724

Pristupnik:	**Jure Jelić (0035208846)**
Studij:	Računarstvo
Profil:	Znanost o mrežama
Mentor:	prof. dr. sc. Ivica Pavić

Zadatak: **Komunikacijska podrška sustavima za napredno vođenje elektroenergetskih mreža**

Opis zadatka:

Promjene u elektroenergetskom sektoru do kojih je došlo uvođenjem tržišnih principa značajno su utjecale i na njihove sustave vođenja pogona. Za sigurno, ali istovremeno i ekonomično vođenje pogona elektroenergetskih sustava, pred njih se postavljaju sve veći zahtjevi za čije je zadovoljenje neophodna njihova modifikacija i unaprjeđenje. Postojeći sustavi za vođenje u pravilu su zasnovani na centraliziranom, hijerarhijskom principu i starim tehnološkim rješenjima i vrlo teško se mogu prilagoditi novim zahtjevima koji se stavljaju pred njih. Razvoj informatičkih i komunikacijskih tehnologija poput optičkih mreža i WAM (Wide Area Monitoring) sustava omogućuje znatno brži i pouzdaniji prijenos podataka od mjesta njihova nastanka do dispečerskih centara u kojima se obavljaju funkcije nadzora i upravljanja elektroenergetskim sustavom. U predmetnom radu potrebno je napraviti pregled novih tehnoloških rješenja zasnovanih na distribuiranoj, mrežnoj arhitekturi i primjeni inteligentnih rješenja (Smart Grid Technology), koja se za potrebe sustava za vođenje trenutno razvijaju u svijetu. Osim toga, u radu je potrebno dati i prijedlog koncepcijskog rješenja vođenja manjih prijenosnih elektroenergetskih sustava, kakav je i prijenosni sustav Hrvatske, utemeljen na primjeni novih komunikacijskih tehnologija.

Rok za predaju rada: 14. veljače 2025.

Sadržaj

1. UVOD[18] **1**

2. ELEKTROENERGETSKI SUSTAVI I POTREBA ZA NAPREDNIM VOĐENJEM[1][2][3][4][5] **7**

2.1. OSNOVE VOĐENJA ELEKTROENERGETSKIH SUSTAVA[1][2][3] 7

2.2. UTJECAJ TRŽIŠNIH PROMJENA NA VOĐENJE ELEKTROENERGETSKIH SUSTAVA[4] 10

3. RAZVOJ KOMUNIKACIJSKIH TEHNOLOGIJA U ELEKTROENERGETSKIM MREŽAMA[6][7][8][9][10] **12**

3.1. ULOGA KOMUNIKACIJSKIH TEHNOLOGIJA U SUSTAVIMA ZA VOĐENJE[6] 12

3.2. KLJUČNE KOMUNIKACIJSKE TEHNOLOGIJE ZA ELEKTROENERGETSKE MREŽE[7][8][9] 14

3.3. EVOLUCIJA KOMUNIKACIJSKIH PROTOKOLA[10] 20

4. KOMUNIKACIJSKI PROTOKOLI U MODERNIM ELEKTROENERGETSKIM SUSTAVIMA[10][11][12][13][14][19] **22**

4.1. PREGLED KLJUČNIH KOMUNIKACIJSKIH PROTOKOLA[10][11][12][13] 22

4.2. SIGURNOSNI IZAZOVI I RJEŠENJA U KOMUNIKACIJSKIM PROTOKOLIMA[19] 36

5. PRIMJENA SMART GRID TEHNOLOGIJE U VOĐENJU ELEKTROENERGETSKIH SUSTAVA[15][16][17] **52**

5.1. DISTRIBUIRANA, MREŽNA ARHITEKTURA U ELEKTROENERGETICI[15] 52

5.2. NAPREDNA ANALITIKA I KOMUNIKACIJA U SMART GRID RJEŠENJIMA[16] 54

5.3. INTEGRACIJA DISTRIBUIRANIH IZVORA ENERGIJE I IOT UREĐAJA[17] 58

ZAKLJUČAK **72**

LITERATURA **73**

SAŽETAK **75**

SUMMARY **76**

1. Uvod[18]

Tijekom posljednjih nekoliko desetljeća, konvencionalni elektroenergetski sustavi (CPSs) prošli su kroz velike promjene s ciljem njihove transformacije u pametne mreže (Smart Grids). Faktori koji su doveli do ove transformacije uključuju starenje CPS-ova, uvođenje obnovljivih izvora energije (RESs) te značajan napredak u digitalnim tehnologijama.

Tijekom posljednjih nekoliko desetljeća, postignut je velik napredak u tehnologijama, uključujući automatizaciju, zaštitu, upravljanje, prijenos električne energije i komunikacijske sustave, osobito u mrežama prijenosa. Ovaj tehnološki napredak utro je put razvoju pametnih mreža.

Neke od ovih tehnologija primjenjuju se od samih početaka elektroenergetskog sektora, dok su se druge postupno integrirale u elektroenergetske mreže tijekom nekoliko generacija.

Uređaji tada poznati kao supervizorska kontrolna oprema omogućavali su operaterima na udaljenim lokacijama da nadziru i upravljaju lokalnim trafostanicama. Kasnih 1960-ih uveden je SCADA (Supervisory Control and Data Acquisition) sustav kako bi zamijenio supervizorsku kontrolnu opremu.

Tijekom 1970-ih i 1980-ih, SCADA sustav se proširio na većinu prijenosnih mreža s naponima od 220 kV i više, kao i na neke distribucijske trafostanice. SCADA je također koristila daljinske terminalne jedinice (RTUs) za prikupljanje podataka i upravljanje u trafostanicama.

Kasnije su RTU jedinice povezane s programabilnim logičkim kontrolerima (PLCs) putem ožičenja. Važno je napomenuti da su PLC uređaji izvorno razvijeni za potrebe industrijske proizvodnje.

Napredak tehnologije zamijenio je ožičene veze komunikacijskim sustavima, a sredinom 1990-ih, konfiguracija RTU/PLC sustava zamijenjena je novim mrežnim arhitekturama koje se sastoje od:

- zaštitnih releja/inteligentnih elektroničkih uređaja (IEDs),

- programabilnih logičkih kontrolera (PLCs),
- i drugih uređaja povezanih mrežom za koordinaciju operacija.

Mnoge elektroprivrede već su prešle na drugu generaciju ovih sustava.

Povijesno gledano, distribucijske mreže su se uglavnom upravljale ručno. Međutim, ručno upravljani prekidači i osigurači ne odgovaraju konceptu pametnih mreža.

Iz tog razloga, mnoge elektroprivrede pokrenule su programe za transformaciju distribucijskih mreža u pametne mreže. Osim toga, razvijene su i vizije pametnih mreža, s ciljem:

- povećanja pouzdanosti,
- povećanja učinkovitosti,
- poboljšanja sigurnosti svih aspekata elektroenergetskog sustava, uključujući proizvodnju, prijenos, distribuciju i krajnju potrošnju električne energije.

Konvencionalni elektroenergetski sustav (CPS) obično se sastoji od proizvodnje, prijenosa, distribucije i potrošača (opterećenja).

Sustav proizvodnje obično uključuje velike centralizirane proizvodne elektrane. Tipična moderna proizvodna jedinica ima nazivnu snagu veću od tisuću MW.

Sustav prijenosa dizajniran je za prijenos velikih količina električne energije s proizvodnih elektrana na distribucijske sustave, koristeći visokonaponske i vrlo visokonaponske vodove na velikim udaljenostima.

S druge strane, distribucijski sustavi su posebno dizajnirani da primaju električnu energiju iz prijenosnog sustava i distribuiraju je do krajnjih korisnika.

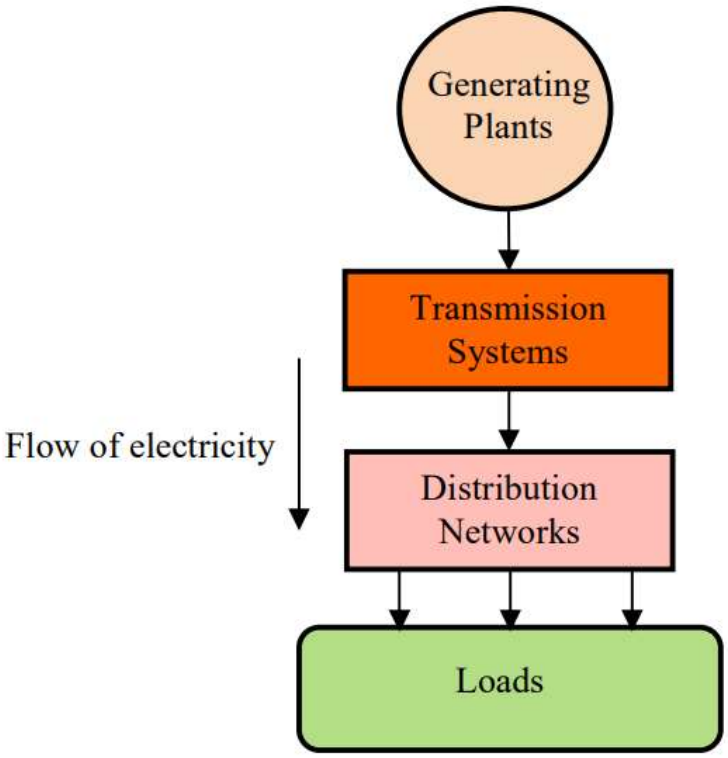
Važno je naglasiti da je uloga distribucijske mreže u CPS-ovima pasivna, tj. njezina funkcija ograničena je na prijenos električne energije primljene iz sustava proizvodnje i prijenosa do potrošača.

Konvencionalni elektroenergetski sustav ima vertikalnu strukturu, kako je prikazano na slici 1.1, koja ilustrira načela vertikalne organizacije konvencionalnog elektroenergetskog sustava.

Tijek električne energije je jednosmjeran, što je posebno izraženo u distribucijskim mrežama.

Cijenu električne energije određuje isključivo elektroprivreda kojoj je potrošač priključen. Drugim riječima, potrošači nemaju mogućnost izbora dobavljača električne energije i smatraju se pasivnim sudionicima u sustavu.

Pametne mreže se u nekoliko ključnih aspekata razlikuju od konvencionalnih elektroenergetskih sustava. Tablica 1.1 sažima osnovne razlike između ova dva sustava, s posebnim naglaskom na distribucijske mreže .



Slika 1.1

Feature/Component	Conventional Power System	Smart Grid
Communications	None or one-way; typically not real-time	Two-way, real-time
Customer interaction	Limited	Extensive
Metering	Dominated by Electromechanical type	Digital (enabling real-time pricing and net metering)
Operation and maintenance	Manual equipment checks,	Remote monitoring, predictive, time-based maintenance
Generation	Centralized	Centralized and distributed
Power flow control	Limited	Comprehensive, automated
Reliability	Prone to failures and cascading outages; essentially reactive	Automated, pro-active protection; prevents outages before they start
Restoration following disturbance	Manual	Self-healing
Topology of distribution networks	Radial; generally one-way power flow	Mesh; multiple power flow pathways

Tablica 1.1

Pametna mreža može se smatrati konceptom u kojem elektroenergetski sustav postaje pametniji zahvaljujući integraciji različitih tehnologija i znanja. Kako se pametne mreže i dalje razvijaju, neprestano će se razvijati i usvajati novi hardverski i softverski sustavi te novi standardi.

Osim što su zastarjeli, konvencionalni elektroenergetski sustavi (CPS) suočeni su s mnogim izazovima i promjenama koje se pokazalo teško integrirati u postojeće sustave:

Integracija distribuiranih izvora energije (DER) – uključujući generatore temeljene na obnovljivim izvorima energije (OIE) i sustave skladištenja energije, posebno unutar distribucijskih mreža.

Razvoj električnih vozila (EV) – koji predstavljaju novu vrstu opterećenja u elektroenergetskom sustavu i mogu uzrokovati dodatni stres na distribucijske mreže.

Liberalizacija tržišta električne energije – zbog čega dolazi do dinamičnih promjena među sudionicima tržišta i elektroprivredama, što zahtijeva uvođenje novih alata i naprednih tehnologija.

Ove promjene negativno utječu na upravljanje, rad i zaštitu konvencionalnih elektroenergetskih sustava. S druge strane, napredak u digitalnim i pametnim uređajima, komunikacijama, automatizaciji i drugim tehnologijama stvorio je nove prilike za rješavanje problema CPS-a, što je potaknulo razvoj koncepta pametne mreže.

Razvoj Napredne infrastrukture mjerenja (AMI – Advanced Metering Infrastructure) smatra se prvim korakom u modernizaciji konvencionalnih elektroenergetskih sustava i njihovoj evoluciji prema pametnim mrežama.

AMI sustav se sastoji od raznih tehnologija i aplikacija koje su integrirane u jedan sustav. Tri glavne komponente AMI sustava prikazane su na slici 1.2:

Pametna brojila - Digitalni programabilni uređaji koji mjere potrošnju električne energije u satnim intervalima (ili kraćim). Mogu bežično slati podatke elektroprivredi za praćenje i obračun potrošnje. Često nazivana "zelena brojila", jer omogućuju optimizaciju potrošnje energije i smanjenje emisije CO_2.

Komunikacijska mreža omogućava stalnu dvosmjernu komunikaciju između elektroprivrede, potrošača i upravljivih uređaja.

Mora biti otvorena, standardizirana i visoko zaštićena kako bi osigurala siguran prijenos podataka.

Sustav prijema i upravljanja podacima - Mjerne podatke koje brojila šalju putem komunikacijske mreže prima centralni sustav AMI-a.

Podaci se zatim šalju u Sustav za upravljanje podacima brojila (MDMS – Meter Data Management System).

Funkcije MDMS sustava:

Automatsko prikupljanje podataka iz različitih uređaja.

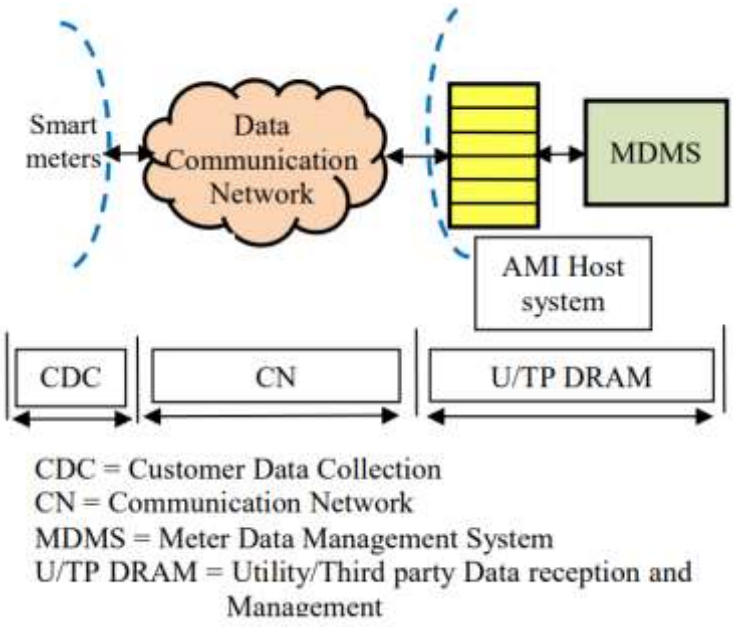
Procjena kvalitete podataka i generiranje procjena u slučaju pogrešaka ili gubitaka podataka.

Dostavljanje podataka u formatu prilagođenom sustavu naplate elektroprivrede.

Pametne mreže omogućuju integraciju distribuiranih izvora energije, naprednih mjernih infrastruktura i digitalnih tehnologija.

AMI sustav je ključan za modernizaciju elektroenergetskih sustava jer omogućava pametno upravljanje potrošnjom i distribucijom električne energije.

Uvođenjem pametnih brojila, naprednih komunikacijskih mreža i sustava upravljanja podacima, elektroprivrede i korisnici dobivaju bolje alate za optimizaciju potrošnje energije i povećanje energetske učinkovitosti.



Slika 1.2

2. Elektroenergetski sustavi i potreba za naprednim vođenjem[1][2][3][4][5]

2.1. Osnove vođenja elektroenergetskih sustava[1][2][3]

Automatizacija se širom svijeta koristi u raznim primjenama, od industrije plina i nafte, automatizacije elektroenergetskog sustava, automatizacije zgrada do malih proizvodnih pogona. Termin SCADA (Supervisory Control and Data Acquisition) obično se koristi kada se nadzire proces raspoređen na širokom geografskom području, poput elektroenergetskih sustava. Iako su SCADA sustavi široko primjenjivani u različitim industrijama, prolaze kroz značajne promjene. Uvođenje novih tehnologija i uređaja predstavlja ozbiljan izazov za obrazovne institucije, istraživače i inženjere koji moraju pratiti najnovije razvojne trendove.

SCADA sustavi definiraju se kao skup opreme koja operatoru na udaljenoj lokaciji omogućuje dobivanje dovoljno informacija za određivanje statusa određene opreme ili procesa te poduzimanje potrebnih radnji bez fizičke prisutnosti. Implementacija SCADA sustava uključuje dvije ključne aktivnosti: prikupljanje podataka (nadzor) i nadzorni nadzor procesa, čime se postiže potpuna automatizacija. Potpuna automatizacija procesa ostvaruje se automatiziranjem nadzora i upravljačkih radnji.

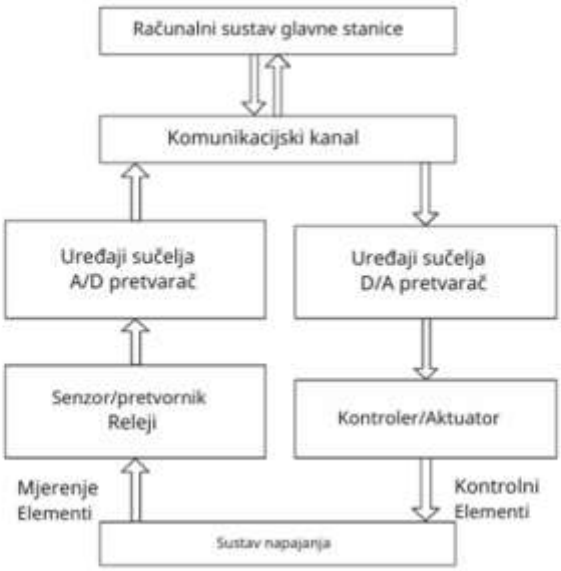
Automatizacija nadzora omogućuje operatoru u kontrolnoj sobi da „vidi" udaljeni proces na konzoli, gdje su sve potrebne informacije prikazane i ažurirane u odgovarajućim vremenskim intervalima. To uključuje sljedeće korake:

- prikupljanje podataka s terena,
- pretvaranje podataka u oblik pogodan za prijenos,
- pakiranje podataka u pakete,
- prijenos paketa podataka komunikacijskim medijima,

- primanje i dekodiranje podataka u kontrolnom centru,
- prikaz podataka na ekranima operatora.

Automatizacija upravljačkog procesa osigurava da se upravljačka naredba, koju inicira operator, prevede u odgovarajuću radnju na terenu. To uključuje:

- iniciranje naredbe od strane operatora,
- pakiranje naredbe u podatkovni paket,
- prijenos paketa komunikacijskim medijima,
- primanje i dekodiranje naredbe na terenskom uređaju te
- aktiviranje odgovarajućeg uređaja za izvršenje radnje.



Slika 2.1

Oprema za mjerenje omogućuje prikupljanje podataka s terena, dok oprema za upravljanje provodi upravljačke naredbe na terenu – slika 2.1.

SCADA je integrirana tehnologija koja se sastoji od četiri glavne komponente:

1. **RTU (Remote Terminal Unit):** RTU je osnovni element SCADA sustava koji prikuplja podatke s terena, obrađuje ih i prosljeđuje master stanici, kao i

distribuira upravljačke signale iz master stanice prema terenskim uređajima. Inteligentni elektronički uređaji (IED) danas sve više zamjenjuju RTU-ove.

2. **Komunikacijski sustav:** Ovaj sustav uključuje kanale komunikacije između terenske opreme i master stanice. Brzina komunikacije ograničena je širinom pojasa kanala.
3. **Master stanica:** Sastoji se od računala, periferne opreme i odgovarajućih ulazno-izlaznih sustava koji omogućuju operatorima nadzor i upravljanje procesima.
4. **HMI (Human-Machine Interface):** HMI predstavlja sučelje koje omogućuje interakciju između master stanice i operatora ili korisnika SCADA sustava.

Slika 2.2 Prikaz komponenti SCADA sustava

SCADA sustavi se široko primjenjuju u brojnim industrijama za potrebe nadzora i upravljanja. U industriji nafte i plina koriste se za nadzor naftnih polja, rafinerija i pumpnih stanica te za upravljanje velikim naftovodima i plinovodima. Sustavi za obradu vode, distribuciju vode i upravljanje otpadnim vodama koriste SCADA za nadzor razine spremnika, pumpnih stanica i kemijskih procesa. SCADA sustavi kontroliraju sustave grijanja, ventilacije i klimatizacije u zgradama poput zračnih luka i velikih komunikacijskih objekata. Industrije poput čelika, plastike, papira i drugih proizvodnih sektora koriste SCADA za standardizaciju i poboljšanje kvalitete proizvoda. U rudarskoj industriji integrirani SCADA sustavi omogućuju optimizaciju protoka proizvoda, logistiku materijala, praćenje radnika i sigurnosne značajke.

U elektroenergetskom sektoru SCADA sustavi imaju ključnu ulogu u generaciji, prijenosu i distribuciji električne energije te će se daljnja rasprava usredotočiti na ovu specifičnu primjenu.

Upravljanje elektroenergetskim sustavom ima ključnu ulogu u osiguravanju stabilnog, pouzdanog i sigurnog rada elektroenergetske mreže, čija je glavna funkcija neprekidna opskrba električnom energijom uz zadovoljenje tehničkih i ekonomskih uvjeta. S obzirom na sve veće tehničke zahtjeve, izazove integracije obnovljivih izvora energije (OIE) te decentralizaciju sustava, upravljanje elektroenergetskim sustavom postaje sve složeniji zadatak.

Osnovni cilj upravljanja je održavanje stabilnosti sustava i vraćanje u ravnotežno stanje nakon poremećaja poput kratkih spojeva, gubitka proizvodnje ili opterećenja. Stabilnost sustava dijeli se na tri glavna područja: rotor-kutnu stabilnost, stabilnost napona i stabilnost frekvencije. Svako od ovih područja ima specifične karakteristike i zahtjeve upravljanja. Na primjer, rotor-kutna stabilnost osigurava sinkronizaciju generatora nakon poremećaja, dok stabilnost napona i frekvencije osigurava održavanje tih parametara unutar prihvatljivih granica kako bi se izbjegli prekidi u radu sustava.

SCADA (Supervisory Control and Data Acquisition) sustavi imaju ključnu ulogu u modernim elektroenergetskim mrežama. SCADA omogućuje prikupljanje podataka, praćenje i upravljanje procesima u stvarnom vremenu. Uz pomoć SCADA sustava, operateri mogu analizirati stanje sustava, donijeti potrebne odluke te provesti akcije za sprječavanje poremećaja ili vraćanje u stabilno stanje nakon poremećaja.

2.2. Utjecaj tržišnih promjena na vođenje elektroenergetskih sustava[4]

Tijekom većeg dijela dvadesetog stoljeća, potrošači električne energije nisu imali mogućnost izbora pri kupnji električne energije. Električnu energiju morali su kupovati od lokalnih komunalnih poduzeća koja su imala monopol na opskrbu u

određenim geografskim područjima. Ta poduzeća su često bila vertikalno integrirana, što znači da su sama proizvodila energiju, prenosila je do glavnih centara opterećenja te distribuirala krajnjim korisnicima. U drugim slučajevima, komunalna poduzeća bavila su se isključivo distribucijom i prodajom električne energije, dok su sami morali kupovati energiju od većih, regionalnih proizvođača i prijenosnih poduzeća.

Ovaj monopolistički model omogućio je veliki napredak u razvoju elektroenergetskih sustava i doprinio značajnom povećanju kvalitete života. U industrijaliziranim zemljama, mreža za distribuciju električne energije pokriva gotovo sve stanovništvo, a napredak u inženjerskim rješenjima omogućio je visoku pouzdanost opskrbe. U mnogim dijelovima svijeta prosječni potrošač suočava se s prekidom opskrbe od svega nekoliko minuta godišnje.

Međutim, 1980-ih godina ekonomisti su počeli preispitivati ovaj model. Smatrali su da monopolistički status komunalnih poduzeća uklanja poticaj za učinkovito poslovanje te vodi nepotrebnim ulaganjima. Privatna poduzeća s monopolom često su prenosila troškove svojih grešaka na potrošače, dok su javna poduzeća bila previše podložna političkim utjecajima. To je rezultiralo neadekvatnim investicijama ili ograničenjem cijena koje nisu pokrivale stvarne troškove.

Ekonomisti su predložili da bi cijene električne energije bile niže, a cjelokupno gospodarstvo učinkovitije ako bi se opskrba električnom energijom podvrgnula tržišnim zakonitostima umjesto regulaciji monopola ili državnoj politici. Deregulacija, koja je već bila prisutna u sektorima poput avioprijevoza i prirodnog plina, proširila se i na elektroenergetski sektor. Zagovornici tržišnih reformi tvrdili su da posebnosti električne energije kao proizvoda nisu nepremostiva prepreka za slobodnu trgovinu. Uvođenjem konkurencije, tvrtke bi bile motivirane za učinkovitije poslovanje, a potrošači bi imali koristi od nižih cijena i inovacija.

Unatoč prednostima koje tržište donosi, električna energija nije jednostavna roba poput brašna ili televizora, koja se može skladištiti i isporučiti po potrebi. Pouzdana i kontinuirana opskrba zahtijeva složene proizvodne kapacitete i stabilne mreže za

prijenos i distribuciju. Deregulacija tržišta stoga zahtijeva pažljivo planiranje i implementaciju kako bi se osigurala ravnoteža između tržišnih zakonitosti, tehničkih ograničenja i pouzdanosti sustava.

3. Razvoj komunikacijskih tehnologija u elektroenergetskim mrežama[6][7][8][9][10]

3.1. Uloga komunikacijskih tehnologija u sustavima za vođenje[6]

Napredna elektroenergetska mreža, poznata kao pametna mreža (Smart Grid), predstavlja moderniziranu električnu mrežu koja koristi informacijske i komunikacijske tehnologije za prikupljanje i analizu podataka o proizvodnji i potrošnji električne energije. Cilj pametne mreže je poboljšati učinkovitost, pouzdanost, ekonomičnost i održivost energetskog sustava.

Jedan od ključnih izazova implementacije pametnih mreža leži u integraciji velikog broja uređaja različitih tehnologija u jedinstveni telekomunikacijski sustav. Ovaj sustav mora osigurati pouzdanu komunikaciju, dostupnost informacija u stvarnom vremenu, fleksibilnost prema promjenama i sigurnost podataka.

Trenutno u elektroenergetskom sektoru dominiraju tradicionalne komunikacijske tehnologije poput PDH (Plesiochronous Digital Hierarchy), SDH (Synchronous Digital Hierarchy) i ATM (Asynchronous Transfer Mode). Ove tehnologije su zatvorenog tipa i nisu prilagođene zahtjevima integracije i fleksibilnosti koje nameće koncept pametne mreže.

PDH tehnologija se koristi za prijenos velikih količina podataka, ali ima ograničenja poput nesinkroniziranog prijenosa i niske skalabilnosti. Iako je bila ključna u ranijim sustavima, danas je zastarjela i zamjenjuje je SDH tehnologija.

SDH omogućuje sinkronizirani prijenos digitalnih podataka preko optičkih vlakana. Unatoč poboljšanjima u odnosu na PDH, SDH ima ograničenja poput fiksnih brzina

prijenosa i niske iskorištenosti kapaciteta. Iako se još uvijek koristi, sve više se zamjenjuje modernijim tehnologijama.

ATM omogućuje visokobrzinski prijenos podataka i podržava različite vrste komunikacija poput glasa, videa i podataka. Unatoč tome, njezina primjena opada zbog prelaska na novije tehnologije poput Ethernet/IP.

Komunikacijske tehnologije prilagođene pametnim mrežama, poput Ethernet/IP, Transportnog Etherneta i MPLS, omogućuju fleksibilniju i učinkovitiju integraciju sustava.

Ethernet/IP je najpopularnija tehnologija za lokalne mreže, koja koristi IP protokol za globalno adresiranje uređaja. Iako je pouzdana i fleksibilna, ne zadovoljava zahtjeve poput ograničenog kašnjenja i zajamčenog kvaliteta usluge, koji su ključni u nekim dijelovima pametne mreže.

Transportni Ethernet dodatno poboljšava pouzdanost, skalabilnost i upravljanje u mrežama. Omogućuje prijenos podataka preko različitih medija poput bakrenih kabela, optike i bežičnih mreža, uz vrijeme oporavka od kvara kraće od 50 ms.

MPLS koristi labele za usmjeravanje paketa podataka, čime omogućuje bržu i učinkovitiju obradu podataka. Ova tehnologija eliminira potrebu za više mreža i optimizira prijenos različitih vrsta podataka, uključujući IP, ATM i Ethernet okvire.

IP/MPLS kombinira prednosti IP-a i MPLS-a te omogućuje visokokvalitetne usluge poput SCADA sustava, pametnih brojila i video nadzora. Ova tehnologija predstavlja temelj za modernizaciju komunikacijskih mreža u elektroenergetskom sektoru.

Sigurnost informacija u pametnoj mreži ključna je za njezino funkcioniranje. Zbog otvorenosti sustava prema različitim vrstama komunikacije, mreža je izložena prijetnjama poput neovlaštenog pristupa, cyber-napada i industrijske špijunaže.

Mogući sigurnosni incidenti uključuju:

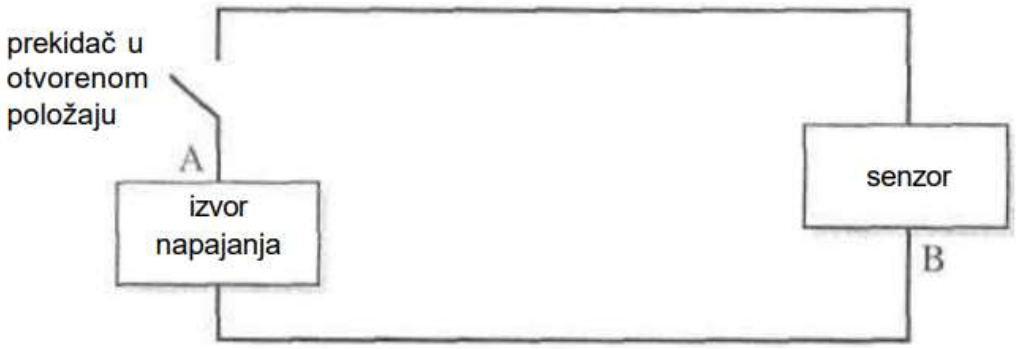
- Neovlašten pristup SCADA sustavima i baza podataka.

- Presretanje i izmjena komunikacija unutar mreže.
- Napadi putem opreme s internetskim pristupom.

3.2. Ključne komunikacijske tehnologije za elektroenergetske mreže[7][8][9]

Predstavit ćemo neke osnovne aspekte i načine komunikacija. Nakon toga će biti razmotreni razlozi za postojanje velikog broja različitih načina za prijenos podataka.

Jedna od najstarijih vrsta medija za prijenos je vodljivi metal koji se koristi za prijenos informacija od 1837., kada je Samuel Morse izumio telegraf. Uglavnom, to je strujni krug koji ima izvor napajanja, sklopku i senzor (slika 3.2.1). Prekidač na mjestu A može se otvoriti i zatvara se ručno, kontrolirajući na taj način hoće li struja teći kroz krug. Senzor na mjestu B detektira elektricitet i stvara zvuk škljocanja kakav ste čuli na TV-u. Na slici 3.2.1 prikazan je telegrafski sustav koji omogućuje prijenos samo u jednom smjeru.



Slika 3.2.1

Najčešća primjena bakra je u kabelima s upletenim paricama, u kojima su dva izolirane bakrene žice upletene. Izolacija sprječava kratke spojeve između vodiča. Za prijenos balansiranih signala najčešće se koriste kabeli s upletenim paricama. Ovo znači da svaka žica nosi struju, ali signali su fazno pomaknuti za 180°. Učinci vanjskih elektromagnetskih izvora na struju gotovo su poništeni, tako da je degradacija

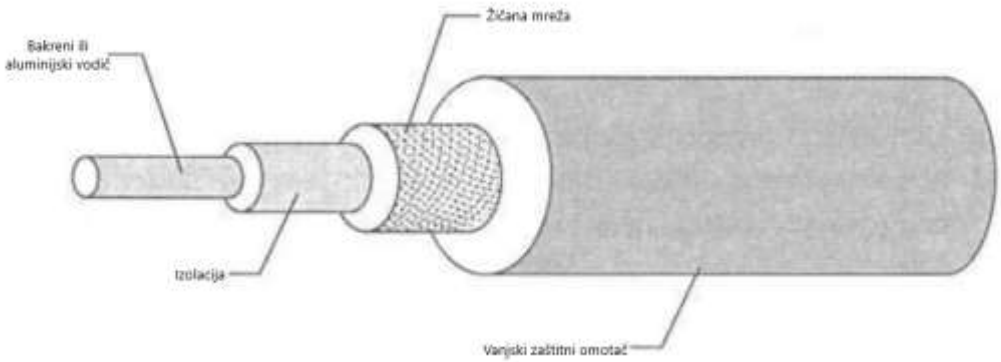
signala značajno smanjena. Uvijanje žica smanjuje smetnje iz vanjskih izvora. Ako žice nisu upletene, jedna žica može biti izložena smetnjama u većoj mjeri od druge. Uvijanjem se smetnje ravnomjerno distribuiraju preko obje žice i signal, budući da je uravnotežen, nastoji eliminirati smetnje.

Iako je bakar dobar vodič, električni otpor ipak postoji i neophodno je postaviti repetitore između dvije točke (slika 3.2.2). Repetitor je uređaj koji presreće emitirani signal prije nego što se previše izobliči, ili oslabi, a zatim ga ponovo generira i prenosi dalje ka njegovom odredištu. Ovdje se nameće logično pitanje na kom rastojanju je neophodno postaviti repetitore. Rastojanje zavisi od karakteristika, kao što su tip signala, opseg signala i kapacitet žice za prijenos struje određene jačine. Mnogi signali mogu da se prenose kilometrima prije nego što bude neophodno regeneriranje signala. Sa repetitorima nema nikakvoga ograničenja u pogledu udaljenosti na koje signal može da se prenese.

Slika 3.2.2

Sljedeći tip uobičajenog medija je koaksijalni kabel (slika 3.2.2), koji se sastoji od četiri komponente. Prva je unutarnji vodič, za koji se obično koristi bakrena žica. Kao i kod upletenih parica, jezgra prenosi signal. Izolacijski sloj okružuje jezgru i sprječava vodič da dođe u dodir s trećim slojem, obično gusto isprepletenom žičanom mrežom. Žičana mreža štiti jezgru od elektromagnetskih smetnji. Osim toga, štiti je i od gladnih glodavaca koji traže nezaštićene metalne žice.

Koaksijalni kabel obično prenosi informacije ili u osnovnom frekvencijskom opsegu ili u širokopojasnom opsegu. U modu osnovnog opsega (baseband mode) cijeli frekvencijski opseg signala rezerviran je za jedan niz podataka. Zbog toga veći frekvencijski opseg omogućava prijenos podataka većim brzinama.



Slika 3.2.2

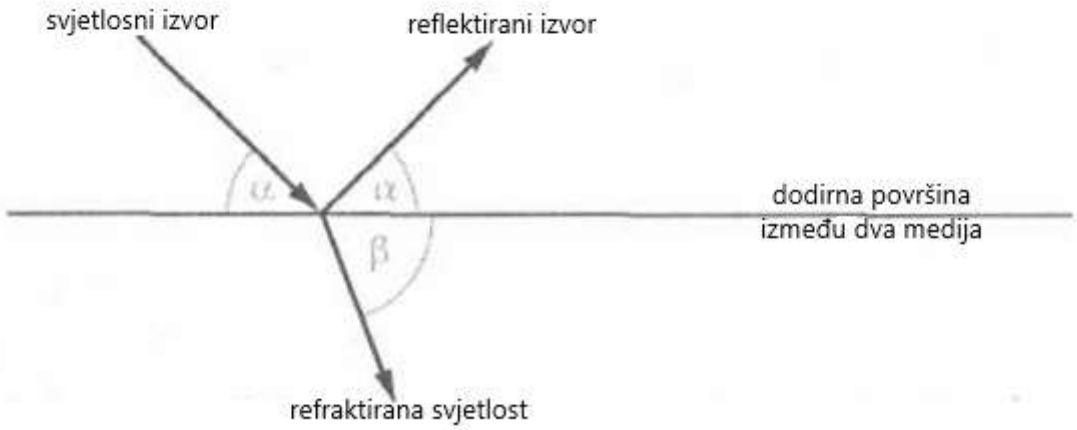
Optičko vlakno za prijenos informacija koristi svjetlost, a ne električnu struju. Telefonske tvrtke široko primjenjuju optičko vlakno, posebno za pružanje usluga na velikim udaljenostima. Uklonjene su mogućnosti za električni šum, a postoji i kapacitet za prijenos golemih količina informacija. Osim toga, optičko je vlakno vrlo tanko (u usporedbi s običnim kabelima), tako da se na manjem prostoru može postaviti veći broj kabela nego što je to moguće s tradicionalnim kabelima.

Razmotrimo svjetlosni izvor usmjeren prema nekoj površini (slika 3.2.3). Površina predstavlja granicu između dva medija, kao što su zrak i voda. Neka a bude kut pod kojim svjetlost sije na granicu. Jedan dio svjetlosti se reflektira natrag pod kutom a u odnosu na ravninu, a drugi dio prolazi kroz granicu u drugi medij. To je refrakcija (prelamanje). Međutim, na granici dolazi do promjene kuta pod kojim se svjetlost širi. Drugim riječima, ako je p kut pod kojim svjetlosni valovi putuju od granice, $\beta \neq \alpha$. Zatim, možete se zapitati je li β veći ili manji od α.

Ako je β > α (kao na slici 3.2.3), kažemo da drugi medij ima veću optičku gustoću od prvog (kao što voda ima veću gustoću od zraka). Međutim, ako prvi medij ima veću optičku gustoću, tada je β < α. Refrakcija objašnjava zašto leće u naočalama izobličuju normalni prikaz, ili zašto objekti koji se nalaze ispod vodene površine izgledaju izobličeno kada se gledaju s površine vode. Svjetlost koja se reflektira od objekata je izobličena i zato oni izgledaju drugačije. Relacija između β i α je zanimljiva. Fizičari za njezino opisivanje koriste mjeru koja je poznata kao indeks refrakcije (koeficijent brzine svjetlosti u vakuumu i brzine svjetlosti u specifičnom mediju). Osim toga, dobro poznat rezultat u fizici, Snellovo (Snell) pravilo "kaže" da je koeficijent indeksa refrakcije dva različita medija (prikazana na slici 3.2.3) jednak odnosu

cos(α)/cos(β).

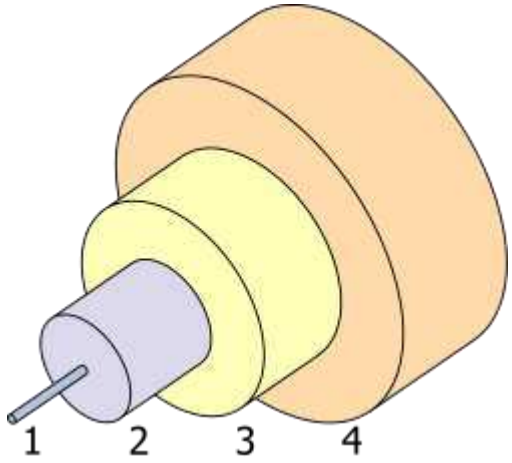
Ako je ovaj odnos manji od 1, svjetlost putuje u medij s manjom optičkom gustoćom, a ako je odnos veći od 1, to znači da svjetlost putuje u medij s većom optičkom gustoćom.



Slika 3.2.3

Sljedeći zanimljiv fenomen javlja se kada je ovaj koeficijent manji od 1 (α > β). Kada je a manji od određenog kritičnog kuta, nema refraktirane svjetlosti. Drugim

riječima, sva svjetlost se reflektira. Zahvaljujući ovom fenomenu, omogućeno je funkcioniranje optičkog vlakna.



Slika 3.2.4 - Presjek kroz tipični jednomodni kabel:

1. jezgra: 8 µm promjer

2. obloga: 125 µm promjer

3. razdjelnik: 250 µm promjer

4. omot: 400 µm promjer.

Bluetooth je bežična tehnologija kratkog dometa koja je izvorno zamišljena kao zamjena za kablove koji povezuju prijenosne i/ili fiksne elektroničke uređaje. To je standard tehnologije koji koristi radio veze kratkog dometa. Bluetooth koristi frekvencijsko skakanje šireg spektra (FHSS) kako bi izbjegao smetnje. Bluetooth radio uređaji rade u nelicenciranom ISM području na 2.4 gigaherza koristeći 79 kanala između 2.402 GHz i 2.480 GHz.

Jedan podatkovni kanal skače nasumično 1600 puta u sekundi. Profili definiraju kako koristiti Bluetooth. Bluetooth Special Interest Group (SIG) razvila je Bluetooth protokolsku stazu. Glavni cilj ove specifikacije je postizanje interoperabilnosti između različitih proizvođača uređaja. Postoji mnogo Bluetooth profila, poput A2DP, AVRCP, DUN, PAN, HFP, HSP, FTP, PBAP, SDP, MAP, HID, HDP, OPP, OBEX, BPP, BIP itd.

Svaki profil je definiran za specifičnu svrhu. Na primjer, A2DP profil se koristi za slušanje zvuka.

Svaki kanal je podijeljen u vremenske slotove duge 625 mikrosekundi. Raspon Bluetooth komunikacije je od 0 do 100 metara, ovisno o snazi uređaja. Svaki Bluetooth uređaj je klasificiran u tri klase (klasa 1, klasa 2 i klasa 3) ovisno o svom dosegu.

Postoje dva tipa prijenosa podataka između uređaja: SCO (Synchronous Connection Oriented) i ACL (Asynchronous Connectionless). Na tržištu su dostupne različite verzije Bluetootha, koje su dizajnirane za unazadnu kompatibilnost. Danas je Bluetooth uobičajena značajka u mnogim elektroničkim uređajima, uključujući mobilne telefone, tablete, prijenosna računala itd.

Bluetooth tehnologija radi pomoću dva koncepta: Bluetooth protokola i Bluetooth profila. Bluetooth protokol definira kako Bluetooth radi, a Bluetooth profili definiraju kako se koristi.

Wi-Fi je opći pojam koji se odnosi na IEEE 802.11 komunikacijski standard za bežične lokalne mreže (WLAN). Wi-Fi mreže povezuju računala međusobno, s internetom i s žičanom mrežom.

Standard 802.11 razvijen je kako bi omogućio bežično povezivanje unutar lokalne mreže u 2.4 GHz ili 5.2 GHz ISM (Industrijski, znanstveni i medicinski) područjima, koja su kvalificirana od strane Savezne komisije za komunikacije (FCC). Točno područje frekvencija koje koristi 802.11 spada u nelicencirane pojaseve, što znači da ih svatko može koristiti za radio komunikaciju (bez dozvole). Točne frekvencije koje se koriste (i način na koji se koriste) ovise o tome slijedi li sustav 802.11b, 802.11a ili 802.11g.

Postoji mnogo metoda sigurnosti koje se koriste za sprječavanje neovlaštenog pristupa Wi-Fiju ili prijetnji sigurnosti. Najčešće metode sigurnosti su Wireless Equivalent Privacy (WEP) i Wi-Fi Protected Access (WPA). WEP je jedna od najmanje

sigurnih metoda, koja je zamijenjena WPA-om. WPA2 je napredna verzija WPA, koja je sigurnija od WPA.

ZigBee je specifikacija za skup visoko-nivoa komunikacijskih protokola koji koriste male, niskopotrošne digitalne radio uređaje temeljenje na IEEE 802 standardu za osobne mreže. ZigBee uređaji često se koriste u obliku mreže s više čvorova (mesh) za prijenos podataka na duže udaljenosti, prosljeđujući podatke kroz međupredajne uređaje kako bi stigli do udaljenijih odredišta. ZigBee je namijenjen aplikacijama koje zahtijevaju nisku brzinu prijenosa podataka, dugu životnost baterija i sigurnu mrežu. ZigBee ima definiranu brzinu od 250 kbit/s, što je najbolje za periodički ili povremeni prijenos podataka ili za jedinstveni prijenos signala s senzora ili ulaznog uređaja. Aplikacije uključuju bežične prekidače za svjetla, električne brojila s prikazima u kući, sustave za upravljanje prometom i druge potrošačke i industrijske uređaje koji zahtijevaju bežični prijenos podataka na kratkim udaljenostima i relativno niskim brzinama.

ZigBee je standard za nisku cijenu, nisku potrošnju energije i bežičnu mrežu s više čvorova. Niska cijena omogućuje široku primjenu tehnologije u bežičnim kontrolama i aplikacijama za nadzor. Niska potrošnja energije omogućuje dulji vijek trajanja s manjim baterijama. Mreža s više čvorova pruža visoku pouzdanost i širi domet. Proizvođači ZigBee čipova obično prodaju integrirane radijske uređaje i mikro-kontrolere s flash memorijom između 60 KB i 256 KB.

ZigBee se temelji na IEEE 802.15.4-2003 specifikacijama koje postavljaju standarde za fizički i MAC sloj. Protokolska staza se dovršava dodavanjem vlastitih mrežnih i aplikacijskih slojeva ZigBee-a. Crtanje analogija s OSI protokolskom stazom pojednostavljuje proučavanje ZigBee protokola. ZigBee uređaji postoje u tri vrste – ZigBee Koordinator (ZC), ZigBee Router (ZR) i ZigBee Krajni uređaj (ZED).

3.3. Evolucija komunikacijskih protokola[10]

IEC 60870.5 i DNP3.0

IEC 60870.5 protokol prvenstveno je definiran za telekomunikaciju električnih sustava i informacija za upravljanje, te stoga ima podatkovne strukture koje su specifično povezane s ovom primjenom. Iako uključuje opće podatkovne tipove koji bi se mogli koristiti u bilo kojoj SCADA primjeni, korištenje IEC 60870 uglavnom je ograničeno na industriju električne energije.

Tijekom istog razdoblja, kada je IEC 60870.5 postupno objavljivan, razvijen je i protokol DNP3 te je objavljen u Sjevernoj Americi. DNP3 je otvoreni protokol koji je razvila Harris Controls Division, Distributed Automation Products, početkom 1990-ih, a objavljen je industrijskoj korisničkoj grupi DNP3 Users Group u studenom 1993. godine.

Iako se protokol obično naziva DNP3 ili Distributed Network Protocol verzija 3.0, to je telekomunikacijski standard koji definira komunikaciju između glavnih stanica, daljinskih telemetrijskih jedinica (RTU) i drugih inteligentnih elektroničkih uređaja (IED). Razvijen je kako bi se postigla interoperabilnost među sustavima u industrijama električne energije, nafte i plina, vodoopskrbe/otpadnih voda i sigurnosnim industrijama.

IEC protokol je ograničen na industriju distribucije električne energije, dok je DNP3 našao širu primjenu u industrijama nafte i plina, vodoopskrbe/otpadnih voda i sigurnosnim industrijama.

Ključna značajka DNP3 protokola je ta što je to otvoreni standard protokola koji je usvojilo značajan broj proizvođača opreme. DNP3 je prepoznat po svom snažnom sustavu usklađenosti. Osim što ima sveobuhvatan specifičan skup podatkovnih objekata, DNP3 ima detaljan sustav certifikacije usklađenosti. To se temelji na definiranju implementacijskih podskupova za koje uređaji moraju biti certificirani. Ovo pruža način za proizvođače da implementiraju sustave smanjene funkcionalnosti koji ipak pružaju definirane razine funkcionalnosti.

I DNP3 i IEC 60870-5 dizajnirani su specifično za SCADA (nadzornu kontrolu i prikupljanje podataka) aplikacije. One uključuju prikupljanje informacija i slanje

naredbi za kontrolu između fizički odvojenih računalnih uređaja. Dizajnirani su za pouzdan prijenos relativno malih paketa podataka na način da poruke dolaze u deterministočkoj sekvenci. Po tom su pitanju različiti od općih protokola, poput FTP-a koji je dio TCP/IP-a, koji mogu slati vrlo velike datoteke, ali na način koji obično nije pogodan za SCADA kontrolu.

4. Komunikacijski protokoli u modernim elektroenergetskim sustavima[10][11][12][13][14][19]

4.1. Pregled ključnih komunikacijskih protokola[10][11][12][13]

IEC 60870-5-104

Komunikacija unutar standarda IEC104 temelji se na tri vrste jedinica:

APDU - Jedinica podataka aplikacijskog protokola (Application Protocol Data Unit),

APCI - Informacija o upravljanju aplikacijskim protokolom (Application Protocol Control Information),

ASDU - Jedinica podataka aplikacijske usluge (Application Service Data Unit).

Osnovna komunikacijska jedinica korištena u IEC104 je APDU, koja se sastoji od APCI-a i ASDU-a. ASDU se ne koristi uvijek; ova jedinica je dizajnirana za prijenos korisnih podataka (payload). Poruke (telegrami) mogu se razlikovati ovisno o duljini, koja može biti fiksna ili promjenjiva. Fiksni telegrami sastoje se samo od APCI-a, početnog bajta (0x68), duljine APDU-a i kontrolnih polja (CF) . Na temelju vrijednosti CF-a koriste se tri različita formata APCI okvira:

I-format - upravlja prijenosom između nadzirane i nadzorne stanice. Duljina je promjenjiva, a ASDU je dio APDU-a.

S-format - koristi se za izvođenje nadzornih funkcija. Duljina je fiksna, a ASDU se sastoji samo od APCI-a.

U-format - kontrolira status prijenosa (START, STOP) i testira komunikacijsku liniju koristeći TEST okvire.

DNP3 (Distributed Network Protocol):

DNP3 ili Distributed Network Protocol Version 3.3 je telekomunikacijski standard koji definira komunikaciju između glavnih stanica, udaljenih telemetrijskih jedinica (RTU) i drugih inteligentnih elektroničkih uređaja (IED). Razvijen je kako bi se postigla interoperabilnost među sustavima u elektroenergetskim sustavima, industriji nafte i plina, upravljanju vodom/otpadnim vodama te sigurnosnim sustavima.

DNP3 je posebno dizajniran za SCADA (Supervisory Control and Data Acquisition) aplikacije. Ove aplikacije uključuju prikupljanje informacija i slanje upravljačkih naredbi između fizički odvojenih računalnih uređaja. DNP3 je osmišljen za prijenos relativno malih paketa podataka na pouzdan način, pri čemu poruke stižu u determinističkom slijedu. U tom pogledu razlikuje se od općenitijih protokola, poput FTP-a koji je dio TCP/IP-a, a koji može slati velike datoteke, ali na način koji općenito nije pogodan za SCADA sustave upravljanja.

Ključna značajka DNP3 protokola je to što je otvoreni standardni protokol koji je usvojen od strane značajnog broja proizvođača opreme. DNP3 je jedan od otvorenih protokola za SCADA komunikacije koji su se pojavili nakon ere vlasničkih protokola.

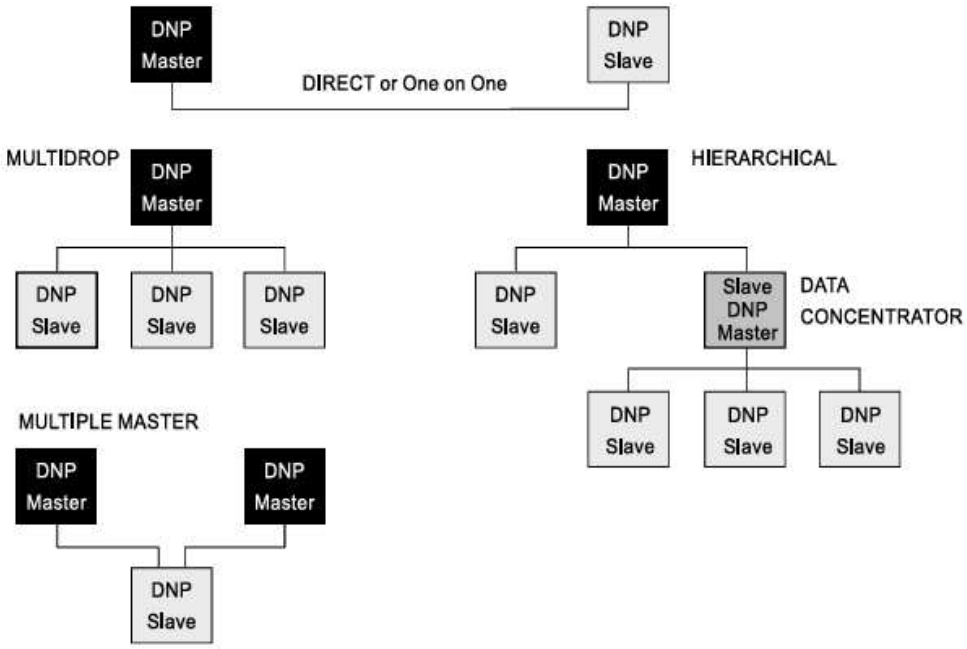
Prednost otvorenog standarda je što omogućuje interoperabilnost između opreme različitih proizvođača. To znači, na primjer, da korisnik može kupiti sustavsku opremu poput glavne stanice od jednog proizvođača, a zatim dodati RTU opremu nabavljenu od drugog proizvođača. RTU može imati niz kontrolnih releja povezanih s njim, koji su inteligentni elektronički uređaji i također koriste DNP3 protokol. Sva ova oprema može potjecati od različitih proizvođača, bilo u početnoj instalaciji ili postupno kako se sustav razvija tijekom vremena.

Topologija sustava

Topologije sustava uključuju:

- *Master-slave*
- Višestruke veze (*multidrop*) s jednim glavnim uređajem (*master*)
- Hijerarhijsku strukturu s posrednim koncentratorima podataka
- Višestruke glavne uređaje (*multiple master*)

Ove topologije prikazane su na slici 4.1.



Slika 4.1

DNP3 podržava komunikaciju s više podređenih uređaja (multiple-slave), peer-to-peer komunikaciju i komunikaciju s više glavnih uređaja (multiple-master). Također podržava načine rada koji uključuju ispitivanje (polled operation) i tihi način rada (quiescent operation). Potonji se često naziva izvještavanjem po iznimci (reporting by exception).

Tihi način rada naziva se takvim jer ispitivanje za provjeru promjena nije potrebno. To je zato što glavna stanica (master) može računati na to da će udaljena stanica (outstation) poslati "nezahtijevani odgovor" kada dođe do promjene koju treba prijaviti. U slučaju da nema promjena, sustav ostaje u tihom stanju, bez ispitivanja od strane glavne stanice ili odgovora od udaljenih stanica. Ovaj način rada omogućuje bolje iskorištavanje kapaciteta komunikacijskog sustava.

Sposobnost podrške peer-to-peer i tihog načina rada zahtijeva da stanice koje nisu glavne mogu inicirati komunikaciju. To se ponekad naziva "uravnoteženom" komunikacijom (balanced communications), što znači da svaka stanica može djelovati i kao primarna (pošiljatelj) i kao sekundarna (primatelj) stanica istovremeno.

Unatoč mogućnosti da stanice koje nisu glavne iniciraju komunikaciju u DNP3, samo glavne stanice mogu pokrenuti zahtjeve za podacima ili izdati naredbe drugim stanicama. Dakle, iako se termin "uravnotežen" primjenjuje na komunikacijski sustav, razlika između glavnih (master) i podređenih stanica (slave) ostaje nužna. Ponekad se termini "glavna" i "udaljena stanica" (outstation) koriste kako bi se točnije odrazile mogućnosti sustava.

DNP3 je otvoreni protokol koji stječe široko prihvaćanje i upotrebu u brojnim industrijama i zemljama. Optimiziran je za SCADA komunikaciju te osigurava sigurnu i učinkovitu razmjenu poruka koje prenose ti sustavi.

Razlozi zašto korisnici usvajaju DNP3 uključuju:

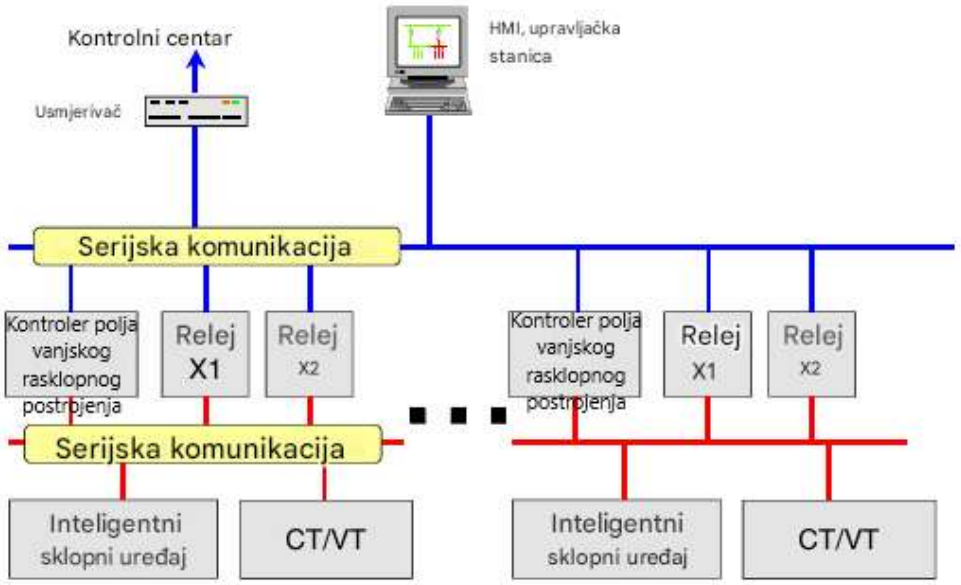
- To je otvoreni protokol
- Optimiziran je za SCADA komunikaciju
- Omogućuje interoperabilnost između opreme različitih proizvođača
- Podržava ga značajan broj proizvođača SCADA opreme
- Pruža korisnicima trenutne i dugoročne koristi

IEC 61850

U električnim postajama, inteligentni elektronički uređaji (IED) koriste se za upravljanje i zaštitu opreme postaje, uključujući vodove koji izlaze iz postaje. Da bi obavljali svoje funkcije, potrebno je razmjenjivati informacije između ovih IED-ova, lokalnih HMI-a (sučelja za čovjeka i stroj) i centra za upravljanje mrežom. Dok je u prošlosti ta razmjena informacija uglavnom bila temeljena na mnogobrojnim kabelima koji su prenosili binarne ili analogne signale, u modernim postajama koriste se komunikacijske mreže.

Kako bi se standardizirala razmjena informacija putem komunikacijskih mreža i osigurala interoperabilnost između IED-ova, razvijen je standard IEC 61850, "Komunikacijske mreže i sustavi u električnim postajama", koji je objavljen između 2003. i 2005. godine. Slika 4.1.1 prikazuje tipičnu konfiguraciju sustava automatizacije postaja temeljenog na standardu IEC 61850.

IEC 61850 definira komunikacijske usluge koje se koriste za razmjenu informacija između IED-ova, kao i prema lokalnim HMI-ima i centru za upravljanje. Definiran je opsežan skup usluga koji podržava razmjenu informacija pokrenutu događajima prema centru za upravljanje, kao i razmjenu vremenski kritičnih informacija između samih IED-ova. Ove usluge koriste standardnu Ethernet tehnologiju s MMS-om (specifikacija za proizvodne poruke) i TCP/IP protokolom.



Slika 4.1.1

IEC 61850 specificira objektno orijentirani i hijerarhijski podatkovni model koji je specifičan za područje primjene i uključuje semantiku. Logički čvorovi (Logical Nodes) predstavljaju osnovne elemente podatkovnog modela. Oni predstavljaju ili sadržaj informacija funkcije unutar sustava automatizacije postaje (npr. **PDIS**, logički čvor za funkciju zaštite udaljenosti) ili informacije iz vanjske procesne opreme (npr. **XCBR**, logički čvor za sučelje s prekidačem strujnog kruga).

Slika 4.1.2 prikazuje primjer logičkog čvora **XCBR** s glavnim informacijama. Logički čvorovi sastoje se od podataka i atributa podataka koji su standardizirani i koji predstavljaju informacije. Međutim, model informacija nije ograničen samo na procesne informacije. On također uključuje informacije o konfiguraciji, nazivnu pločicu (nameplate) i dijagnostičke informacije.

Nazivna pločica i dijagnostičke informacije dostupne su kako za softver i hardver sustava automatizacije (IED i logičke čvorove), tako i za procesnu opremu.

Dijagnostičke informacije sažimaju se u status uređaja, koji prikazuje stanje uređaja putem indikatora: zeleno (u redu), žuto (upozorenje) i crveno (alarm).

Podatkovni model podržava **samopopisivanje** (self-description). To znači da klijent može pretraživati uređaj za dostupne podatke te da se podaci mogu dohvatiti, uključujući specifikaciju formata, bez prethodnog poznavanja uređaja. Dodatno, atributi za opis mogu operatoru pružiti objašnjenje semantike podataka. Samopopisivanje također omogućuje provjeru je li sustav konfiguriran prema očekivanjima.

XCBR

	Data Name	Type	Explanation
Common LN Information	Mode	INC	enable / disable
	EEHealth	INS	ok / warning / alarm
	EEName	DPL	Name plate
	OpCnt	INS	operation counter
Controls values	Pos	DPC	Position (control / status)
	BlkOpn	SPC	Block opening
	BlkCls	SPC	Block closing
	ChaMotEna	SPC	Charger motor enabled
Status information	CBOpCap	INS	op. capability (o-c...)
	POWCap	INS	point on wave capability
	MaxOpCap	INS	maximal op. capability
Extension	TrCoilFail1	SPS	Failure of trip coil 1
	TrCoilFail2	SPS	Failure of trip coil 2
	HydrLeak	SPS	Leakage of hydraulic

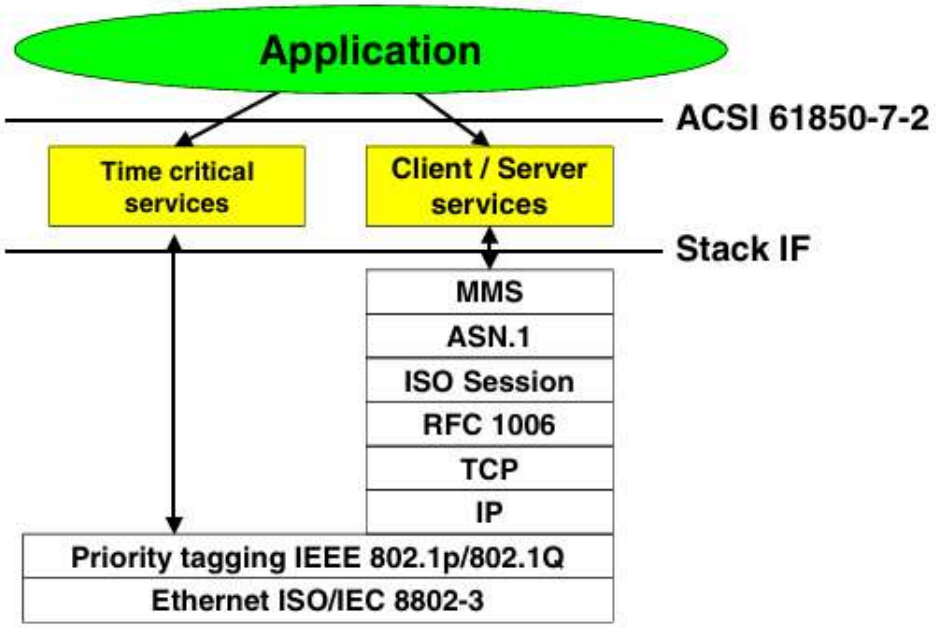
Slika 4.1.2

Jezik za konfiguraciju postaje (SCL) temelji se na XML formatu datoteka koji omogućuje razmjenu konfiguracijskih informacija između alata. Na temelju specifikacije sustava i datoteka s opisima sposobnosti uređaja, alat za konfiguraciju sustava koristi se za konfiguriranje postaje. Rezultat je datoteka s opisom konfiguracije postaje koja se zatim koristi za alate za konfiguraciju IED-ova kako bi se izradila konfiguracija za preuzimanje.

Dostupnost konfiguracijskih informacija u standardiziranom formatu datoteka omogućuje korištenje tih informacija i za aplikacije izvan same postaje.

IEC 61850 osmišljen je tako da bude otporan na buduće promjene. Komunikacijske usluge i modeli dizajnirani su u apstraktnom obliku, poznatom kao ACSI (Abstract Communication Service Interface). Te usluge zatim se preslikavaju na postojeće komunikacijske protokole poput MMS-a i TCP/IP-a putem Ethernet tehnologije.

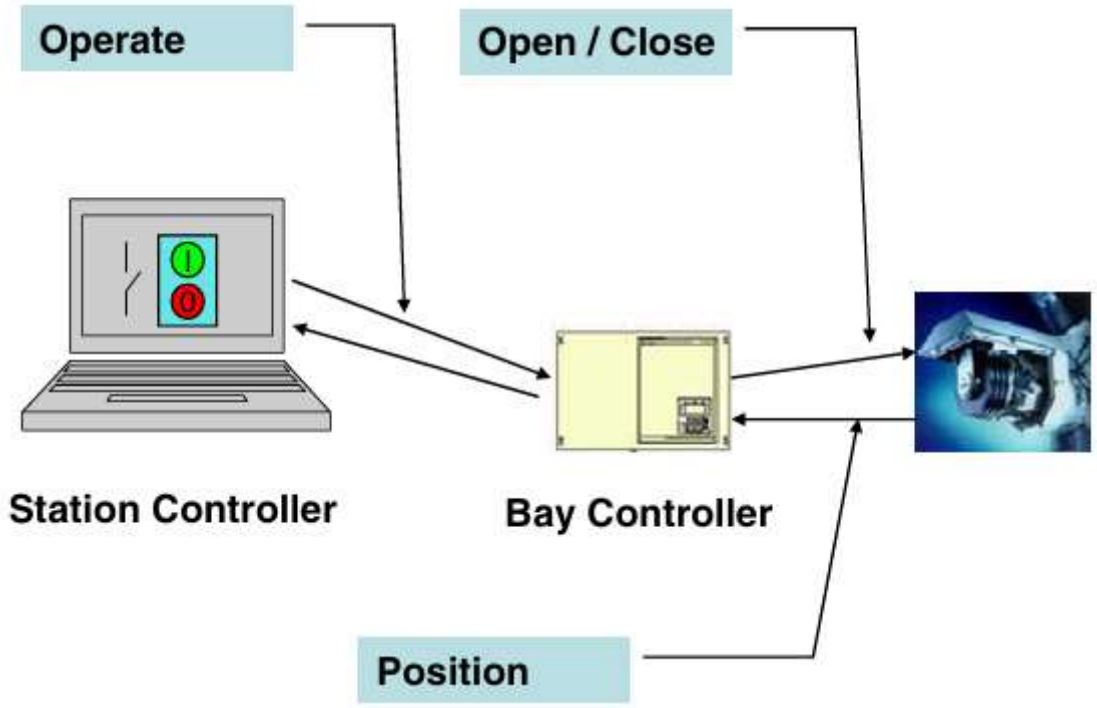
Trenutno preslikavanje koje se koristi u IEC 61850 prikazano je na slici 4.1.3. Većina komunikacija prema IEC 61850 temelji se na komunikaciji klijent/poslužitelj.



Slika 4.1.3

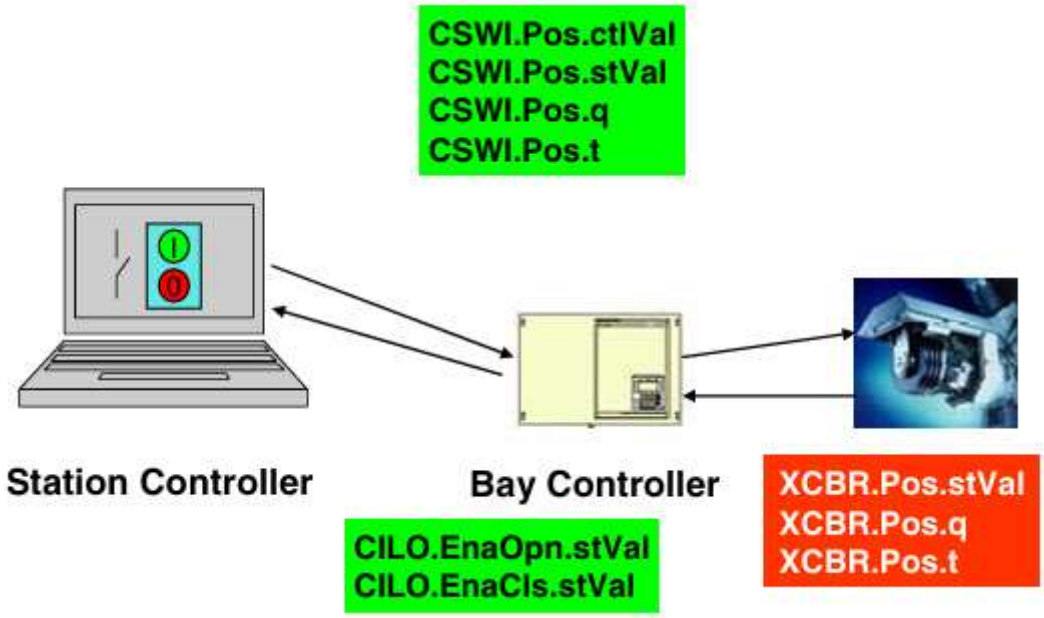
61850 U TRAFOSTANICI

Na temelju tipičnih funkcija sustava za automatizaciju trafostanice, objasnit ćemo kako se primjenjuju komunikacijske usluge i kako će uključene funkcije biti modelirane koristeći IEC 61850 logičke čvorove i podatke. Prvi primjer bavi se upravljanjem sklopnim prekidačem. Elementi funkcije prikazani su na slici 4.1.4.



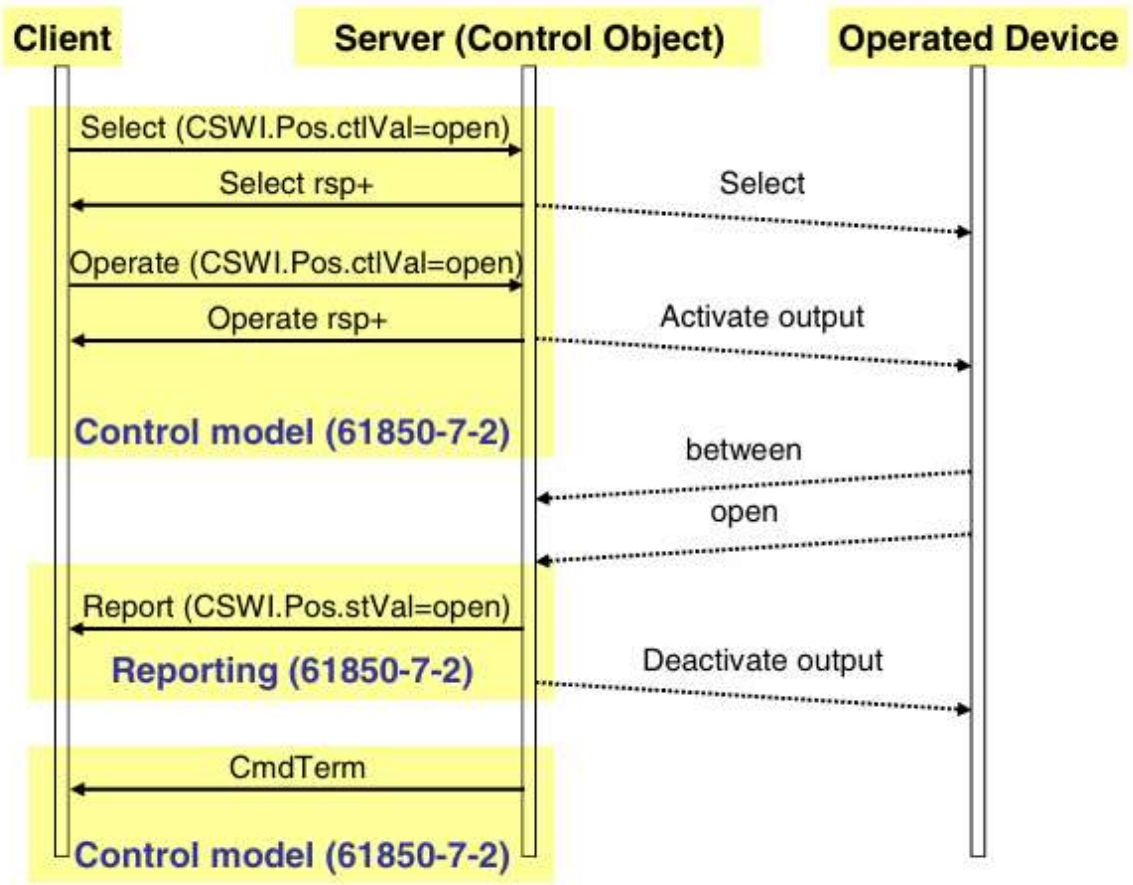
Slika 4.1.4

U našem primjeru, IED kontroler odaje pristupa sklopnom prekidaču putem binarnih izlaza koji se povezuju na zavojnice za otvaranje i zatvaranje te putem binarnih ulaza koji se povezuju na indikaciju položaja. Naredba za operaciju šalje se s lokalnog HMI-a kontrolera stanice na kontroler odaje koristeći IEC 61850 sabirnicu stanice. Nakon zahtjeva za operaciju, kontroler odaje provjerava uvjete međusprječavanja prije nego što se operacija izvrši aktiviranjem zavojnice za otvaranje ili zatvaranje.



Slika 4.1.5

Podatkovni model prema IEC 61850 za tu primjenu prikazan je na slici 4.1.5. Logički čvor **CSWI** koristi se za pokretanje operacije; kontroler stanice šalje operacijske naredbe kontroleru odaje. Redoslijed naredbi i odgovora standardiziran je u IEC 61850-7-2 i prikazan je na slici 4.1.6. Korištenje opcije *select* prije *operate* je jedna od mogućnosti.



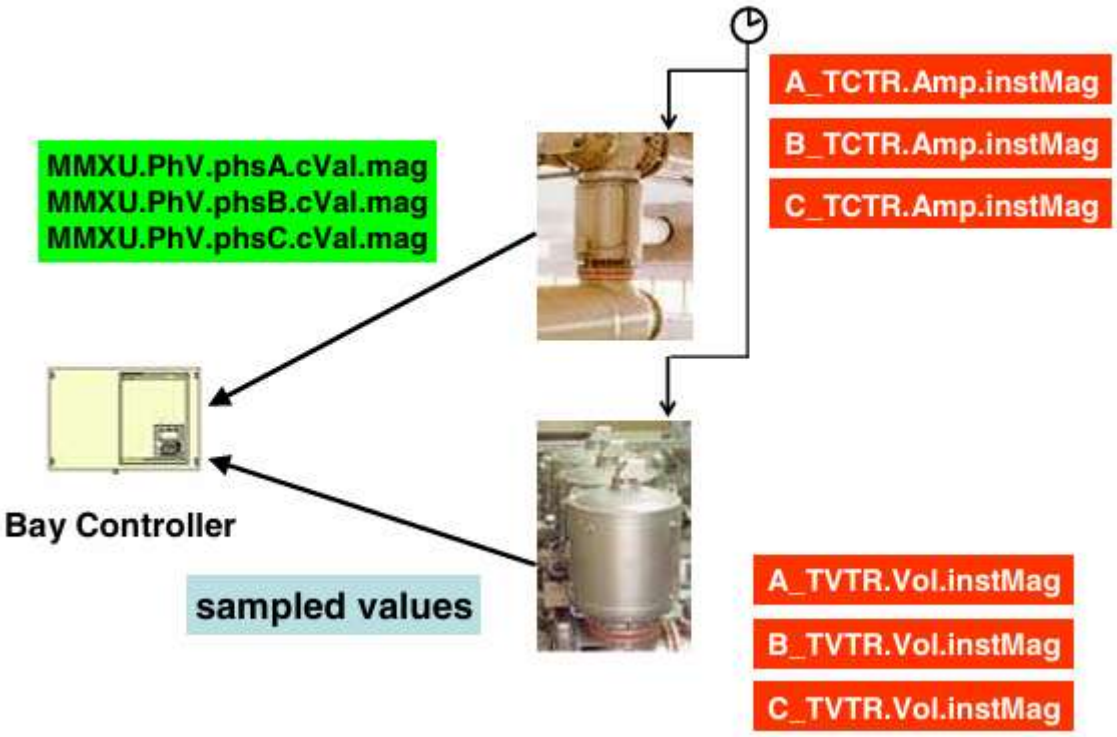
Slika 4.1.6

Nakon zahtjeva za operaciju na podatkovnom objektu **CSWI.Pos.stVal**, kontroler odaje provjerava uvjete međusprječavanja (npr. je li **CILO.EnaOpn.stVal=TRUE**) i ako je operacija dozvoljena, aktivira izlaz na zavojnicu za otvaranje sklopnog prekidača. Kontroler odaje zatim nadzire povratne informacije od sklopnog prekidača. Ako operacija završi uspješno, poruka o završetku naredbe (**CmdTerm**) će biti poslana kontroleru stanice. Ako se položaj sklopnog prekidača promijeni, ta informacija može se prenijeti spontano kontroleru stanice. Za to se koristi model izvješćivanja definiran u IEC 61850-7-2.

Mjerenje struje i napona

U drugom primjeru, struje i naponi mjere se u **CT-ovima** (transformatori struje) i **VT-ovima** (transformatori napona), a valni oblik prenosi se kao digitalni uzorci preko

komunikacijske veze na **IED** koji izračunava vrijednosti poput RMS struje ili aktivne i reaktivne snage. Slika 4.1.7 ilustrira primjer uključujući podatkovni model. Logički čvorovi **TCTR** i **TVTR** koriste se za modeliranje jednofaznih transformatora struje i napona. Logički čvor **MMXU** koristi se za predstavljanje izračunatih vrijednosti – u primjeru su prikazani fazni naponi.



Slika 4.1.7

Iako je izvorno definiran za komunikaciju unutar trafostanice, osnovni koncepti IEC 61850 čine ga prikladnim za druge primjene u industriji automatizacije komunalnih usluga. To je prepoznalo industriju, te su unutar IEC-a stvorene nekoliko novih radnih skupina koje pripremaju standarde temeljene na IEC 61850 za nove domenske aplikacije.

Korištenje IEC 61850 u proizvodnji električne energije

U tri područja proizvodnje električne energije koriste se koncepti IEC 61850 definirajući nove domenski specifične objektne modele (logičke čvorove).

Standard **IEC 61850-7-410 – Hidroelektrane – Komunikacija za nadzor i kontrolu** koristi se za kontrolu i nadzor hidroelektrane. Standard definira logičke čvorove za električne funkcije; različite kontrolne funkcije, prvenstveno povezane s ekscitacijom generatora. Novi logički čvorovi definirani unutar ove skupine nisu specifični za hidroelektrane; oni su više-manje opći za sve vrste većih elektrana. Nadalje, definira logičke čvorove za mehaničke funkcije povezane s turbinskim i pratećom opremom te logičke čvorove za hidrološke funkcije.

Drugi standard, **IEC 61850-7-420 – Komunikacijski sustavi za distribuirane energetske resurse (DER)**, namijenjen je za razmjenu informacija između DER uređaja i bilo kojih sustava koji nadziru, kontroliraju, održavaju i općenito upravljaju DER uređajima. Taj standard definira logičke čvorove za DER sustav općenito, kao i za modele DER opreme poput reciprocirajućih motora ("piston enginea"), gorivnih ćelija, fotonaponskih sustava ili uređaja za kombiniranu proizvodnju toplinske i električne energije.

Treći standard, serija **IEC 61400-25**, definira logičke čvorove za komunikaciju između komponenti vjetroelektrana poput vjetroturbina i povezanih SCADA sustava.

B. IEC 61850 za širokopojasnu komunikaciju

Kao što se detaljno raspravljalo u radnim skupinama, korištenje IEC 61850 za širokopojasnu komunikaciju, poput komunikacije između trafostanica ili komunikacije između trafostanice i kontrolnih centara, također je u fokusu.

Izvješće **IEC 61850-90-1** raspravljat će različite aspekte korištenja IEC 61850 za komunikaciju između trafostanica. U tom izvješću razmatraju se sljedeće aplikacije:

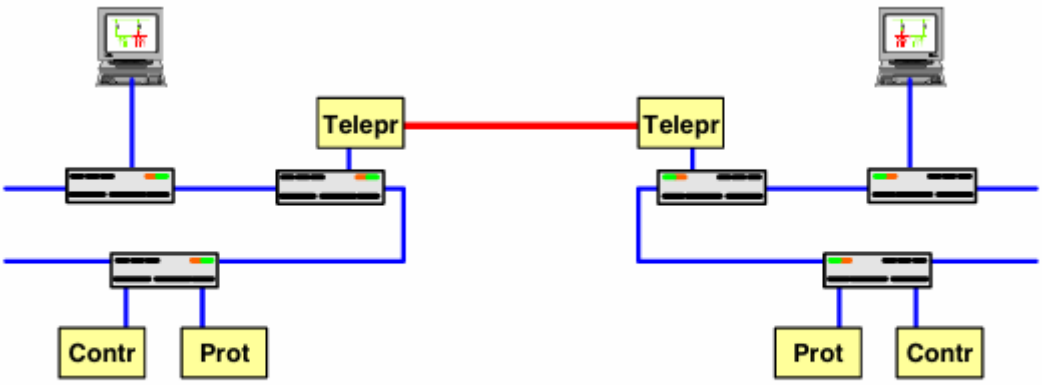
1. **Zaštitne funkcije** poput diferencijalne zaštite linije s strujom, zaštite na udaljenost s permisivnim i blokirajućim shemama, zaštite usporedbe smjera i

faze, prijenosa isključenja, prediktivne širokopojasne zaštite i shema zaštite integriteta trafostanice.

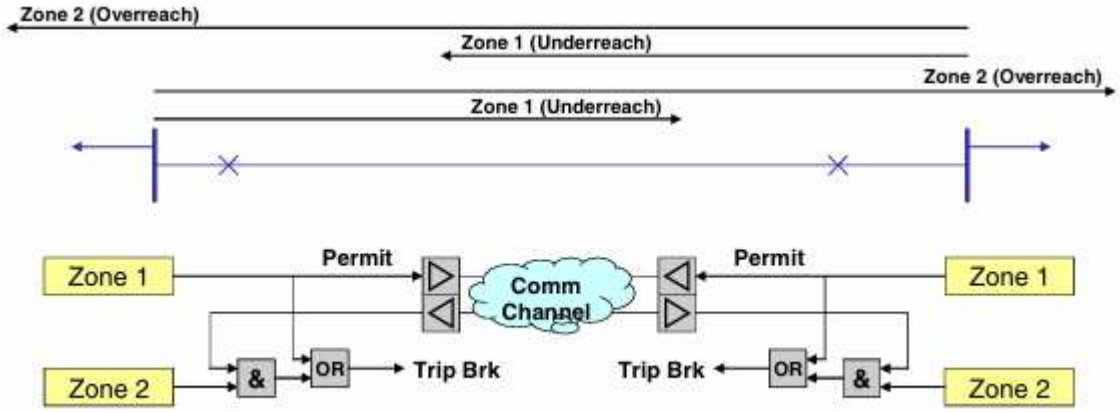
2. **Kontrolne funkcije** poput automatskog ponovnog zatvaranja, međusprječavanja, križnog okidanja, isključivanja generatora ili opterećenja, detekcije izvan koraka i određivanja topologije visokonaponskih mreža.

S komunikacijskog gledišta, moguća su dva različita arhitektonska pristupa. Prvi pristup naziva se **pristup preko gateway-a** i koristi relativno spor komunikacijski kanal sa specifičnom teleprotection opremom. Ovo je pristup koji se danas koristi; jedina specifičnost je korištenje IEC 61850 sučelja za teleprotection opremu.

Drugi pristup je **pristup tuneliranjem** prikazan na slici 4.1.11. Ovo je korištenje visokobrzinskog komunikacijskog linka s izravnim prijenosom IEC 61850 poruka s jedne trafostanice na drugu. Kao primjer, raspravlja se shema permisivnog underreach teleprotection-a. Aplikacija je objašnjena na slici 4.1.12.



Slika 4.1.11



Slika 4.1.12

4.2. Sigurnosni izazovi i rješenja u komunikacijskim protokolima[19]

Neprestani napredak informacijsko-komunikacijskih tehnologija (ICT) doprinosi razvoju tradicionalne elektroenergetske mreže u pametnu mrežu. Međutim, jedan od značajnih nedostataka razvoja pametnih mreža su problemi s kibernetičkom sigurnošću. Sigurnosni izazovi usporavaju napredak primjene pametnih mreža, no stalna poboljšanja unaprijedit će iskustva korištenja pametnih mreža u nadolazećim godinama.

Sigurnosni problemi pametne mreže uključuju osiguranje CIA trojstva (povjerljivost, integritet i dostupnost) u kontrolnim sustavima i ICT infrastrukturi. CIA trojstvo je ključno kako za komunikacijsku infrastrukturu, tako i za zaštitu, rad i upravljanje energetskim sustavima.

Ciljevi kibernetičke sigurnosti pametnih mreža moraju uključivati mjere predostrožnosti za osiguravanje informacija u skladu s načelima CIA trojstva . Ovi ključni sigurnosni principi moraju biti ispunjeni u sustavima pametnih mreža.

Povjerljivost (Confidentiality)

Povjerljivost podrazumijeva zaštitu podataka od neovlaštenog pristupa ili otkrivanja. To znači da je pristup informacijama omogućen samo ovlaštenim osobama, dok neovlašteni korisnici ne mogu pristupiti podacima.

Pametna mreža može uključivati kućanske uređaje povezane s elektroenergetskom mrežom, omogućujući dvosmjernu i realno-vremensku komunikaciju podataka. Ako napadači dobiju pristup informacijama potrošača, mogu ih zloupotrijebiti, pratiti njihov životni stil, saznati koje uređaje koriste i utvrditi jesu li kod kuće ili ne. Povjerljivost uključuje i zaštitu privatnosti, što je jedno od najvažnijih pitanja za korisnike.

Integritet (Integrity)

Podaci u sustavu nikada ne smiju biti izmijenjeni od strane bilo koga ili bilo čega. Ključno je osigurati da svi podaci budu točni i neizmijenjeni. Dakle, podaci se ne smiju mijenjati na neovlašten ili neprimijećen način.

Integritet se definira kao zaštita podataka od neovlaštene izmjene i uništenja. Također, integritet znači očuvanje točnosti i vjerodostojnosti podataka. Održavanje integriteta omogućuje siguran sustav praćenja u stvarnom vremenu u pametnoj mreži.

Dostupnost (Availability)

Elektroenergetski sustav mora biti dostupan u svakom trenutku. Također, važno je osigurati pravovremeni i pouzdan pristup informacijskom sustavu. Pouzdanost i dostupnost imaju izravan utjecaj na kontrolne uređaje u kritičnoj infrastrukturi.

Dostupnost se odnosi na zaštitu informacijskog sustava od kvarova. Napadi na dostupnost mogu oštetiti, blokirati ili usporiti prijenos informacija. Dakle, dostupnost znači da informacije moraju biti dostupne ovlaštenim stranama u pametnoj mreži kada su im potrebne, bez ugrožavanja sigurnosti.

Napadi na dostupnost uključuju sprečavanje napada uskraćivanjem usluge (DoS napadi) koji mogu uzrokovati prekide u opskrbi električnom energijom (blackout).

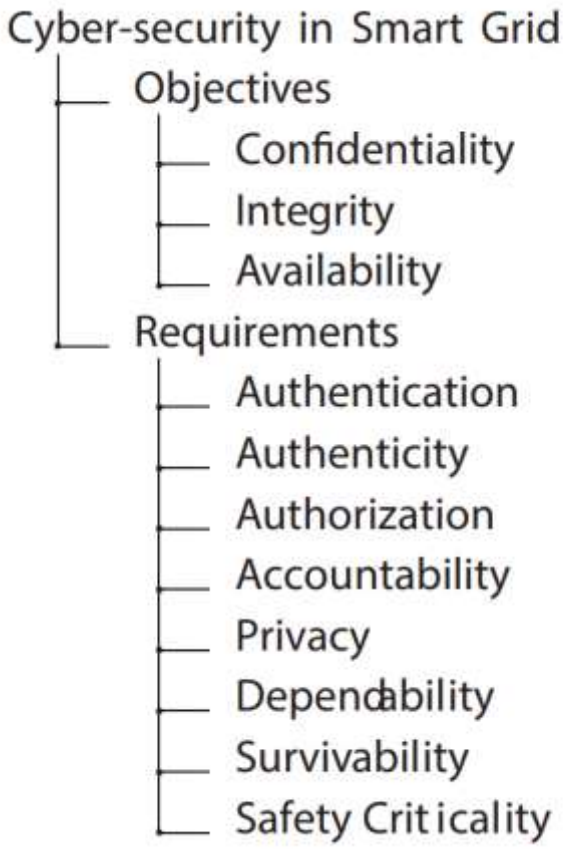
Napadi na povjerljivost imaju za cilj omogućiti neovlaštenim osobama pristup informacijama.

Napadi na integritet usmjereni su na manipulaciju izvornim podacima ili ubacivanje lažnih podataka.

Napadi na dostupnost imaju za cilj prekinuti opskrbu električnom energijom, usporiti ili prekinuti komunikaciju.

Zahtjevi za kibernetičku sigurnost

Postoje i neki sigurnosni zahtjevi osim CIA trojstva kako bi se osigurala kibernetička sigurnost u aplikacijama pametne mreže. Mnogi od ovih zahtjeva su međusobno povezani. Stoga, kako bi se postigao holistički pristup kibernetičkoj sigurnosti, pružanje ciljeva i zahtjeva treba biti osigurano zakonski. Visoko razine ciljevi kibernetičke sigurnosti i specifični zahtjevi kibernetičke sigurnosti prikazani su na slici 4.3.1.



Slika 4.3.1

Autentifikacija i identifikacija ključni su procesi potvrđivanja identiteta korisnika ili uređaja kako bi se obranio sustav pametne mreže od neovlaštenog pristupa. Omogućuje provjeru je li identitet objekta valjan. Objekti mogu biti korisnici, pametni uređaji ili bilo koje komponente povezane na mrežu. Korištenje lozinke je raširena metoda identifikacije. Postojeće protokole autentifikacije može se prilagoditi za dizajniranje autentifikacijskog procesa u pametnoj mreži. Međutim, ako sustavi za energiju ne dobiju dovoljno pažnje, proces dizajna autentifikacije je ranjiv na značajne pogreške.

Autentifikacija i enkripcija obavezni su kriptografski procesi za obranu povjerljivosti i integriteta podataka u pametnoj mreži. Također, to je važan proces identifikacije za eliminaciju napada na integritet podataka. Svi sigurnosni zahtjevi zahtijevaju verifikaciju imovine kako bi se odlučilo jesu li ovlašteni za interakciju s podacima. Integritet i autentifikacija mogu osigurati zaštitu aplikacija pametne mreže od uobičajenih kibernetičkih napada poput prerušavanja, MITM (napadi čovjek-u-sredini) i izmjene poruka.

Autentičnost prenesenih podataka može se osigurati digitalnim potpisima. Proces validacije potvrđuje strane i poruke. Upravljanje zajedničkim tajnim ključem ili infrastruktura javnih ključeva (PKI) može se primijeniti za pružanje autentičnosti za prijenos podataka preko mreže. Certifikat potvrđuje identifikaciju strana. Ovaj certifikat pruža certifikacijska vlast. PKI infrastruktura se provodi prije nego što se uspostavi bilo kakva veza između strana.

Kontrola pristupa, također poznata kao autorizacija, odnosi se na blokiranje pristupa sustavu od strane neovlaštenih osoba ili sustava bez dozvole. Autorizacija znači utvrđivanje koje razlikuje između legitimnih i ilegitimnih strana na temelju autentifikacije za sve ostale zahtjeve kibernetičke sigurnosti. Autorizacija može dovesti do sigurnosnih problema ako se prekrši. Kontrola pristupa osigurava da

resursi budu pristupani samo relevantnom osoblju i stranama u pametnoj mreži koje su točno identificirane.

Metode kontrole pristupa poput Kontrole pristupa temeljene na ulogama (RBAC), Diskrecionog kontrole pristupa (DAC) i Obavezne kontrole pristupa (MAC) mogu povećati pouzdanost sustava i smanjiti moguće sigurnosne prijetnje. Dakle, kontrola pristupa je nezamjenjiva za ograničavanje pristupa korisnika ili uređaja mreži.

Mnogi kibernetički napadi na pametnu mrežu mogu dovesti do opsežnih energetskih prekida i katastrofalnih oštećenja energetskih resursa. Također, oni mogu podrivati ciljeve i zahtjeve kibernetičke sigurnosti. Međutim, nabrajanje svih mogućih napada nije praktično zbog složenosti i velike razmjerljivosti pametne mreže. Stoga smo kibernetičke napade klasificirali na temelju sigurnosnih ciljeva pametne mreže u tri vrste. Navedene rasprave o sigurnosti za pametnu mrežu pokazuju da rješenja protiv prijetnji moraju uzeti u obzir različita ograničenja, situacije i probleme. Stoga samo jedno sigurnosno rješenje, poput enkripcije, ne može blokirati sve kibernetičke prijetnje.

Kriptografija nije jedino rješenje, ali igra vrlo značajnu ulogu u povećanju povjerljivosti i integriteta u pametnoj mreži. Enkripcija je primarna kriptografska tehnika za osiguranje sigurne komunikacije. Implementacija enkripcijskih shema nužna je za održavanje integriteta i povjerljivosti podataka u pametnoj mreži. Enkripcija značajno smanjuje napade ponovnog slanja (replay) i prisluškivanja. Mnogi postojeći autentifikacijski sheme i enkripcijski algoritmi se koriste u pametnoj mreži. Simetrična kriptografija, poput simetričnih šifri, DES, AES i 3DES ili kriptografija javnog ključa poznata kao asimetrična kriptografija široko se koristi za blokiranje mogućih kibernetičkih prijetnji u pametnoj mreži. Također, očekuje se da većina elektroničkih uređaja u pametnoj mreži ima lagane kriptografske mogućnosti.

Kibernetičke prijetnje i rješenja

Proizvodnja, prijenos, distribucija i potrošnja glavne su domene pametne mreže. Komunikacija mora biti učinkovita i sigurna u svim domenama. Povjerljivost, tajnost i autentifikacija podataka ključni su za pouzdanost, a također se mora jamčiti i učinkovitost kako bi se spriječile neovlaštene izmjene kroz cijelu infrastrukturu te stoga treba stvoriti distribuirane sustave kibernetičke sigurnosti za održavanje integriteta podataka i nadzor arhitekture. Sustavi pametne mreže imaju različite ranjivosti, a svaki od njih posjeduje različite karakteristike. Ranjivosti mogu izložiti aplikacije pametne mreže mnogim različitim kibernetičkim prijetnjama koje mogu nanijeti štetu od niskog do visokog stupnja. Ispravna identifikacija vrste sigurnosnih prijetnji i ranjivosti omogućuje određivanje odgovarajućih suzbijajućih mjera.

Napadač može izvesti samo napad ometanjem (jamming) spajanjem na komunikacijski kanal. Zero-day napadi poput Stuxneta opisuju se kao prijetnja nepoznatim sigurnosnim ranjivostima u aplikacijama sustava i mogu se otkriti nakon završetka napada. Napad prisluškivanja je oblik pasivnog napada u kojem napadač prisluškuje poruke između čvorova na komunikacijskom kanalu. Analiza prometa, krađa lozinki, prisluškivanje, napadi čovjek-u-sredini (MITM) i napadi prerušavanja (spoofing) narušavaju povjerljivost. Injekcija podataka, manipulacija podacima, wormhole, sinkronizacija vremena i napadi prerušavanja (spoofing) narušavaju integritet. DoS, puppet, buffer overflow, wormhole, jamming i flooding napadi narušavaju dostupnost u aplikacijama pametne mreže.

Malware je skraćenica za zlonamjerni softver. Malware napadi kompromitiraju CIA trojstvo kibernetičke infrastrukture indirektno ili direktno. Ovi napadi mogu dovesti do mnogih ozbiljnih posljedica u pametnoj mreži, kao što su curenje informacija o korisnicima, uništenje infrastrukture ili široko rasprostranjeni prekidi struje.

Točnost podataka ključna je za pouzdano i učinkovito funkcioniranje pametne mreže. Podaci o frekvenciji, struji, naponu ili GPS vremenskim oznakama mogu se manipulirati. Napadi prerušavanja, poput identitetskog ili podatkovnog prerušavanja, mogu uzrokovati gubitak integriteta i dostupnosti.

Također, oni ozbiljno degradiraju pouzdanost, stabilnost, sigurnost i operacije pametne mreže. Napadi prerušavanja sastoje se od MITM (napadi čovjek-u-sredini), ponavljanja poruka i napada iskorištavanja softvera. Korištenje više uređaja za nadzor komunikacijske linije za napajanje, suradnja među GPS uslugama, korištenje jednog izvora podataka i sinkronizacija mjerenja pomoću mrežnog protokola za vremensko usklađivanje (NTP) na različitim lokacijama u stvarnom vremenu neke su značajne mjere protiv napada prerušavanja. Tablica 4.3.1 prikazuje kibernetičke napade na pametnu mrežu prema CIA trojstvu.

Cyber-Security Objective	Attack Type
Confidentiality	Social Engineering, Eavesdropping, Traffic Analysis, Unauthorized Access, Password Pilfering, MITM, Sniffing, Replay, Masquerading, Data Injection Attacks
Integrity	Tampering, Replay, Wormhole, False Data Injection, Spoofing, Data Modification, MITM, Time Synchronization, Masquerading, Load-Drop Attacks
Availability	Jamming, Wormhole, Denial of Service, LDos(Low-rate Dos), Buffer Overflow, Teardrop, Smurf, Puppet, Time Synchronization, Masquerading, MITM, Spoofing Attacks

Tablica 4.3.1

Povjerljivost omogućuje sprječavanje neovlaštenog pristupa informacijama. Napadi na povjerljivost pokušavaju ukrasti informacije koje bi trebale biti dijeljene ili zadržane u tajnosti samo među sigurnim stranama. Nezakonito čitanje memorije uređaja, prerušavanje korisnog tereta (payload), napadi ponavljanja (replay) i mijenjanje kontrolnog programa pametnih brojila su neki primjeri takvih napada u pametnoj mreži. Mrežno kodiranje (network coding) koristi se za održavanje privatnosti podataka. Ovo osigurava povjerljivost u pametnoj mreži. Privatnost podataka uključuje anonimnost, nevezivost (unlinkability), neopažljivost (unobservability) i neotkrivljivost (undetectability).

U usporedbi s napadima na integritet, napadi na povjerljivost ne namjeravaju mijenjati prenesene informacije. Oni mogu presretati komunikacijske kanale u pametnoj mreži kako bi dobili željene informacije, poput potrošnje energije korisnika ili broja računa. Analiza prometa i napadi prisluškivanja (wiretapping) tipični su primjeri.

Napad na povjerljivost može se smatrati da ima trivijalan utjecaj na funkcionalnosti komunikacijskog kanala u aplikacijama pametne mreže. Međutim, važnost privatnosti korisnika i svijest o privatnosti dobile su više pažnje u posljednjim godinama, posebno moguće curenje mnogih informacija o korisnicima.

Napadi na lozinke krše povjerljivost. Pogađanje lozinki, presretanje lozinki (password sniffing), napadi rječnikom (dictionary attacks) i socijalni inženjering uobičajene su metode korištene za napade na lozinke. Posebno je socijalni inženjering metoda za provaljivanje u sustav korištenjem društvenih vještina, umjesto tehničkih napada.

Napad prisluškivanja je tip pasivnog napada i također narušava povjerljivost podataka. Napadi prisluškivanja presreću IP pakete ili presreću bežične prijenose na lokalnim mrežama (LAN) u mrežama pametne mreže. Uključuje napadača koji prisluškuje poruke koje se dijele između čvorova na komunikacijskoj mreži. Napadi prisluškivanja također narušavaju odgovornost i integritet sustava. Enkripcija podataka čuva osjetljive podatke od napada prisluškivanja.

Napadi analize prometa su pasivni napadi na povjerljivost. Napadači mogu presretati i analizirati poruke kako bi dobili vrijedne informacije o obrascima komunikacije između čvorova.

Napadi prerušavanja, također nazvani napadi impersonacije ili identitetskog prerušavanja, događaju se kada napadači se pretvaraju da su legitimna imovina kako bi dobili privilegije. Napadi prerušavanja štete CIA trojstvu i odgovornosti. Napadi prerušavanja poput MAC prerušavanja, ARP prerušavanja, IP prerušavanja su nezakonite izmjene parametara i dio su napada prerušavanja. Napadi identitetskog prerušavanja poput ponavljanja poruka (message replay), MITM i

mrežnog prerušavanja (network spoofing), omogućuju imitiranje ovlaštene imovine bez korištenja korisničke lozinke. Procesi autentifikacije su bitni za svaki uređaj u pametnoj mreži kako bi se izbjegli ovi napadi.

Napad putem bočne kanale (side-channel attack) usmjeren je na dobivanje kriptografskih ključeva. Napadi analize snage (power analysis attack), napadi na vrijeme (timing attack) i elektromagnetski napadi analize (electromagnetic analysis attack) dobro su poznate vrste ovih napada. Oni dovode do kršenja lozinki, informacija o korištenju, administrativnog pristupa i privatnosti korisnika. Kućanski aparati i pametna brojila ranjivi su na ove napade. Detekcija zasićenih kanala, zasićenje širine pojasa komunikacijskog kanala i konstrukcija diskretne infrastrukture za komunikaciju uređaja pametne mreže su pionirska rješenja.

Napadač može dobiti pristup sadržaju PMU-a ili TCP/IP paketima pametnih brojila poslanim preko mreže koristeći alate poput Wiresharka koji se koristi za presretanje i analizu paketa. PMU, TCP/IP paketi i pametna brojila glavni su ciljevi napada presretanja. Bez enkripcije, napadači mogu promatrati i prikupljati kritične informacije. Enkripcija štiti informacije od kibernetičkih napada, čini mrežu virtualnom i privatnom. Napad presretanja paketa može se ublažiti korištenjem sigurnosnog prolaza (security gateway) koji prenosi IP pakete zahvaljujući VPN tunelu, koji je dizajniran ugrađivanjem enkriptiranog IP tunela u uobičajeni IP mrežni korisni teret. Komunikacije između VPN tunela osigurane su korištenjem TLS protokola, a odnosi između različitih strana u pametnoj mreži ostvaruju se korištenjem X.509 certifikata, koji autentificiraju korisnike i razmjenjuju simetrične ključeve .

Integritet znači blokiranje neovlaštene modifikacije ili krađe informacija. Kašnjenje poruka, ponavljanje i injekcija narušavaju integritet kroz mrežu. Napadi na integritet imaju za cilj modificirati sadržaj originalnih podataka kao što su podaci o korisničkim računima, podaci o naplati, vrijednosti napona i senzora, kontrolne naredbe, operativni status uređaja, te također imaju za cilj nelegalno odgađanje i

preuređivanje toka poruka . Napadi na integritet ne uključuju samo nelegitimnu modifikaciju podataka poput injekcije lažnih podataka. Osim toga, prerušavanje uređaja, rijetki napadi i napadi ponavljanja smatraju se važnim napadima na integritet. Kriptografski algoritmi i metode koriste se za sprječavanje napada na integritet podataka. Neki pristupi su predloženi za obranu protiv kibernetičkih napada na integritet, kao što su tehnika otiska snage (power fingerprinting), shema temeljena na kontroli volt-var i pristup temeljen na povezivanju pouzdane mreže (trusted network connect). Autentičnost i nenegiranje također su važni zahtjevi za integritet podataka. Kršenje integriteta može dovesti do sigurnosnih problema gdje ljudi ili oprema mogu biti oštećeni.

Napadi na integritet podataka kao što su SQL injekcije i MITM (napadi čovjek-u-sredini) iskorištavaju ranjivosti kako bi modificirali, oteli ili korumpirali legitimne procese u pametnoj mreži. Jedinica za koncentraciju podataka (data concentrator unit) povezana je s pametnim brojilom HAN-a (Home Area Network) u aplikacijama pametne mreže. Međutim, napadač može oštetiti prijenos podataka između pametnog brojila i jedinice za koncentraciju podataka koristeći MITM ili nelegalnu modifikaciju podataka. Napadi opterećenja (loaddrop attacks) mogu se klasificirati kao napadi na integritet.

MITM napadi štete CIA trojstvu i odgovornosti sustava. Modificirani izvori i odredišta paketa, trovanje tablica ruta i kompromitirani certifikati su neke MITM tehnike. Mrežni promet treba biti enkriptiran korištenjem sigurnosnih prolaza (security gateways) kako bi se suprotstavili MITM napadima. Sigurnosni prolazi stvaraju VPN tunele za povezivanje mreža. Također, enkripcija podataka na izvoru i dekripcija na odredištu je nužna. Učinkoviti enkripcijski procesi obično se provode hardverskim rješenjima. Interoperabilnost i sigurna komunikacija podržavaju sigurnosni prolazi s IPsec protokolom u pametnoj mreži. IPsec osigurava povjerljivost i nepromijenjene podatke tijekom cijelog komunikacijskog procesa kako bi zaštitio komunikacijsku liniju. Dodatno, i izvor i odredište trebaju biti autentificirani kako bi se blokirali MITM napadi. Drugim riječima, autentifikacija i izvornih i odredišnih čvorova te enkripcija mrežnog prometa sigurnosnim prolazima

predstavljaju značajna rješenja. Također, TLS protokoli imaju unutarnje asimetrične kriptografske karakteristike koje mogu odmah otkriti i popraviti greške kako bi se izbjegli MITM napadi.

SQL injekcijski napadi imaju za cilj mijenjanje baza podataka ubrizgavanjem skriptnog koda. SQL injekcijski napadi ubrizgavaju zlonamjerne upite u bazu podataka kako bi preuzeli kontrolu nad sustavom, izbrisali ili modificirali postojeće podatke te dodali manipulirane podatke. To može ometati operacije pametne mreže i na kraju rezultirati prekidom struje. Pametna brojila kontinuirano šalju podatke o potrošnji energije za pohranu u bazu podataka za korisnike i komunalne službe. Ako upiti koje formiraju korisnici nisu precizno provjereni prije umetanja, može doći do SQL injekcije. U mrežama pametne mreže, SQL injekcijski napadi mogu se smanjiti primjenom mjera poput pozitivnog podudaranja uzoraka (positive pattern matching), statičke provjere koda (static code checking), provjere vrste unosa (input type checking), ograničavanja pristupa bazi podataka za udaljene korisnike, izbjegavanja dinamičkog SQL-a i provedbe penetracijskih testova. Znakovi poput točke-zareza (semicolon) mogu biti zloupotrebljeni od strane napadača i moraju se filtrirati tijekom provjere tipa .

Napad injekcije podataka znači manipulaciju podacima. Povratni signali, očitanja senzora i signali potrošnje energije su neki primjeri podataka. Učinci takvih napada ovise o ciljevima poput financijske koristi ili oštećenja sustava . Koristi informacije sustavnog modela za injekciju podataka što dovodi do nestabilnosti. Napadi injekcije podataka uglavnom ciljaju procjenjivač stanja (state estimator), pametna brojila i sustave za široko područje zaštite, nadzora i kontrole (WAPMC) . Procjenjivač stanja elektroenergetskog sustava sastoji se od faznih kutova i veličina napona na svakom čvorištu. Procjena stanja pruža sveobuhvatan nadzor struje i protoka energije kroz cijelu pametnu mrežu. Stoga, manipulacija mjerenjima nadzora dovodi do pogrešne procjene operativnog stanja sustava. Takvi slučajevi dovode do netočnih operativnih radnji kao što su uzrokovanje netočnog određivanja cijena ili destabilizacija pametne mreže. Kao rezultat toga, uspješan napad injekcije podataka sprječava otkrivanje nestabilnosti koja može uzrokovati pad sustava.

Napad injekcije lažnih podataka događa se kada se loši podaci ubrizgavaju u pametna brojila ili mjerenja susjednih mreža (neighborhood area network). Napad cilja infrastrukturu pametne mreže . Posebno, cilja integritet pod-sustava za mjerenje i nadzor kako bi manipulirao mjerenjima brojila i fazora. Utječe na procjenu stanja SCADA sustava. Ako napadači kompromitiraju jedno ili više pametnih brojila, mogu uspješno ubrizgavati izmijenjene podatke u SCADA centar i zaobići provjere integriteta podataka primijenjene u procesu procjene stanja .

Napadi ponavljanja, također poznati kao napadi reproduciranja (playback attacks), imaju za cilj usmjeravanje energije na drugu lokaciju i fizičko oštećenje sustava. Napadi ponavljanja se događaju kada napadač dobije mrežni promet i zatim ga proslijedi odredištu, postupajući kao glavni izvor. Dakle, napadi ponavljanja mogu imati ozbiljne učinke na stabilnost sustava. Napadi ponavljanja imaju za cilj odgađanje ili ponovno slanje poruka, nakon što ih dobiju zahvaljujući napadima prerušavanja (masquerading attacks). Napadači ubrizgavaju podatke u sustav bez izazivanja izmjena u mjerljivim izlazima. Napadači ciljaju neenkriptirane senzore kako bi inicirali napad ponavljanja. Oni nadziru izlaze senzora i ponavljaju ih dok ubrizgavaju napadni signal. Osim ubrizgavanja lažnih kontrolnih signala u mrežu, napadači trebaju dobiti i analizirati prenesene podatke između pametnih brojila i uređaja kako bi dobili karakteristike korisničke potrošnje energije i generacije. Implementacija vremenskih oznaka (time-stamps) i brojeva slijeda (sequence numbers) su učinkovita rješenja protiv napada ponavljanja u aplikacijama pametne mreže. Također, skriveni napad (covert attack) je verzija napada ponavljanja s zatvorenom petljom.

Napad sinkronizacije vremena (Time Synchronization Attack - TSA) cilja podatke o vremenu u aplikacijama pametne mreže. Važni procesi kao što su procjena lokacije događaja i detekcija kvarova uvelike ovise o točnim vremenskim podacima u pametnoj mreži. PMU (Phasor Measurement Unit) i WAPMC (Wide-Area Protection, Monitoring, and Control) su glavni ciljevi TSA. Neke primjene PMU-a kao što su lokalizacija događaja, nadzor stabilnosti napona, detekcija kvarova u prijenosnoj liniji mogu biti pogođene TSA-om. TSA i prerušavanje GPS signala imaju za cilj da

GPS signal imitira napadač . Stoga, uzorkovanje PMU-a se izvodi u pogrešno vrijeme i generiraju se mjerenja s netočnim vremenskim oznakama. Ishodi u su dokazali da TSA može generirati pogrešne lokacijske greške i izazvati lažni alarm u vezi s postojanjem problema. Lažni alarm može uzrokovati prekid komunikacijske linije. Ova situacija može pokrenuti kaskadne kvarove u pametnoj mreži. Mora se povećati korištenje PMU-a kako bi se pametna mreža sigurnije nadzirala.

Autentifikacijske sheme i enkripcija od kraja do kraja (end-to-end encryption) su potrebni za eliminaciju gore navedenih napada na integritet u mrežama pametne mreže. Također, napadači moraju imati autentificirani pristup komunikacijskim mrežama i osjetljivim informacijama kako bi inicirali napad na povjerljivost ili integritet. Stoga su kontrola pristupa i autentifikacija ključni za sprječavanje napada na integritet pametne mreže.

Dostupnost znači da informacije budu dostupne ovlaštenim korisnicima. Napadi na dostupnost sprječavaju i mogu destabilizirati ovlašteni pristup u pametnoj mreži. Napadi na dostupnost također su poznati kao DoS napadi. DoS napadi imaju za cilj blokirati, oštetiti i odgoditi prijenos podataka. To uzrokuje nedostupnost mrežnih resursa. Napadi na dostupnost nastoje preopteretiti mreže korištenjem različitih tehnika, tako da sustav ne može ispravno funkcionirati [56].

Napadači šalju velike količine prometa kako bi preplavili prijenosne linije u mreži. To uzrokuje gubitak legitimnih IP paketa u mrežnom prometu i njihovu neobradu. IP-protokoli poput TCP/IP, IEC 61850 ranjivi su na napade na dostupnost . Budući da je dostupnost najvažniji sigurnosni zahtjev u pametnoj mreži, napredne i učinkovite suzbijajuće mjere trebaju se poduzeti protiv napada na dostupnost. Filtriranje prometa, velike cijevi (big pipes), pristupi detekciji anomalija i primjena zračno izolirane mreže (air-gapped network) neke su učinkovite mjere. Budući da su DoS napadi najveća prijetnja za IoT-temeljene sustave pametne mreže, softversko rješenje na mrežnom sloju može biti učinkovit način za ublažavanje DoS napada. IP brzo skakanje (IP fast hopping) omogućuje siguran način za klijenta da sakrije sadržaj i odredišni poslužitelj njihove komunikacijske sesije. IP brzo skakanje skriva stvarnu IP adresu odredišnog poslužitelja kako bi se spriječila identifikacija mrežnog

prometa. IP adresa poslužitelja mijenja se istovremeno u stvarnom vremenu na strani ovlaštenih klijenata i poslužitelja.

Jamming napadi imaju za cilj ispuniti bežične komunikacijske linije šumom tako da pametna brojila ne mogu povezati se s komunalnom službom. Ova situacija negativno utječe na pametna brojila na dva načina. Prvo, komunikacijski kanal se kontinuirano vidi kao zauzet od strane usmjerivača. Drugo, paketi podataka se blokiraju od primanja. Slanje nasumičnih neautentificiranih paketa svakoj bežičnoj stanici u mreži učinkovit je pristup za rješenje jamming napada.

Kibernetički napadi na pametnu mrežu općenito su koordinirani kako bi iskoristili različite komponente za pokretanje istovremenih napada. Koordinirani napad je najizazovniji tip napada. Budući da koordinirani napadi mogu nadmašiti uobičajenu obranu, oni zahtijevaju višeslojno sigurnosno rješenje s robusnim pristupima. Također, koordinirani napadi ciljaju sve sigurnosne ciljeve, zahtjeve i komponente pametne mreže. Stoga, sigurnosni pristupi postignuti analizom zahtjeva za kibernetičkom sigurnošću prema mrežnim slojevima pružit će učinkovita sigurnosna rješenja za aplikacije pametne mreže.

MITM napadi imaju za cilj presretanje i manipulaciju porukama između kontrolnog centra i terenskih uređaja. Napadač se čini kao pravi odredište kako za izvor tako i za cilj tijekom sesije protokola. MITM napadi mogu se izvoditi u svakom sloju, posebno u slojevima 2 i 3, te utječu na cijelo CIA trojstvo i odgovornost sustava. Kibernetička sigurnosna rješenja trebaju uključivati softver za detaljnu analizu paketa, a također robusni mehanizmi autentifikacije mogu zaštititi od MITM napada.

Napadi na aplikacijskom sloju mogu lako preopteretiti sustav koji ima ograničene računalne resurse. Napadi na povjerljivost i integritet općenito se iniciraju u aplikacijskom sloju jer pokušavaju dobiti ili manipulirati podacima u pametnoj mreži. DoS napadi mogu se izvoditi na različitim slojevima u aplikacijama pametne mreže . DoS napadi na aplikacijskom sloju imaju za cilj iscrpljivanje resursa sustava, poput memorije, CPU-a ili širine pojasa, preplavljivanjem intenzivnim razdobljima

zahtjeva. Budući da su komunikacijski uređaji u pametnoj mreži opremljeni ograničenim računalnim mogućnostima, oni mogu biti potencijalni ciljevi DoS napada na aplikacijskom sloju. Napad na nižem sloju općenito cilja širinu pojasa komunikacijskih kanala.

Napadi na transportnom sloju koji ciljaju dostupnost imaju za cilj ometanje konekcija od kraja do kraja konzumiranjem resursa, čime se ciljani uređaj ne može naknadno povezati s legitimnim prometom. Napadi preplavljivanja TCP i UDP su neki od uobičajenih primjera. Oni su vrsta DoS napada. Također, IP prerušavanje (spoofing) je napad na transportnom sloju. MITM napadi mogu se dogoditi tijekom IP prerušavanja kako bi se spriječila komunikacija. MITM napad omogućuje napadaču da presretne LAN pomoću ARP prerušavanja. Najistaknutija obrana protiv MITM napada upravljanog putem IP prerušavanja je korištenje enkriptirane komunikacije. Osim aplikacijskog sloja, korištenje IDS-a (Intrusion Detection System) je vrlo učinkovito kibernetičko sigurnosno rješenje i za transportni sloj, prema Radoglou-Grammatikisu i Sarigiannidisu . Anomali-based, signature-based i specification-based su tri načina detekcije za IDS/IPS sustave.

Prerušavanje (spoofing) napadi su štetne prijetnje u MAC sloju jer ciljaju i integritet i dostupnost. Prerušavanje napadi, iskorištavajući polja adresa u MAC okviru, mogu se prerušavati kako bi prosljeđivali lažne podatke drugim uređajima. PMU-ovi su glavni ciljevi prerušavanja napada u pametnoj mreži. U mrežama elektroenergetskih trafostanica, zlonamjerni čvorovi mogu emitirati lažne ARP pakete kako bi isključili konekcije svih IED-ova (Intelligent Electronic Devices) na gateway čvor trafostanice. To može oštetiti dostupnost komunikacijske mreže i legitimni čvor ne može primiti poruke.

Najčešći tip napada na fizičkom sloju koji se odnosi na dostupnost je jamming. Jamming napadi se uglavnom događaju u bežičnim mrežama na fizičkom sloju. Napadači samo trebaju spojiti se na komunikacijski kanal kako bi izveli jamming napad.

Tablica 4.3.2 prikazuje napade prema mrežnim slojevima.

Također, tablica 4.3.3 prikazuje kibernetičke napade prema mrežnim slojevima i CIA trojstvu u pametnoj mreži. Neki napadi aktivni su na više od jednog sloja.

Network Layer	Attack Type
Application Layer	CPU Exhausting, LDoS, HTTP Flooding, Protocol, Stack Buffer Overflow, Data Injection Attacks
Transport Layer	IP Spoofing, Packet Sniffing, Wormhole, Data Injection, Traffic Flooding, Buffer Flooding, Buffer Overflow, DoS/DDoS, MITM, Covert Attack, Replay Attack
MAC Layer	Traffic Analysis, Masquerading, ARP Spoofing, MITM, TSA, MAC DoS Attack, Flooding Attacks, Jamming Attack
Physical Layer	Eavesdropping, Smart Meter Tampering Attacks, TSA, Jamming Attacks

Tablica 4.3.2

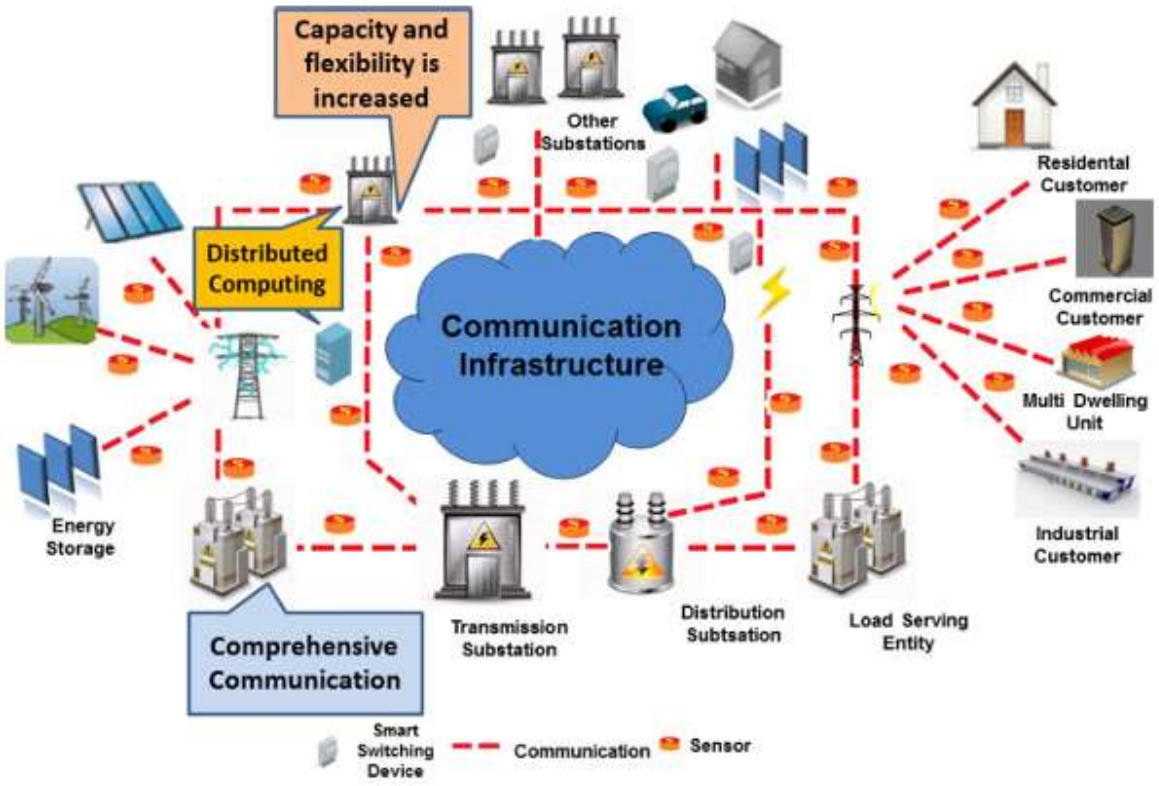
Network Layer	Confidentiality	Integrity	Availability
Application Layer	Data-Injection Attack	-	LDoS, HTTP Flooding, Buffer Overflow
Transport Layer	IP-Spoofing, Data-Injection, Sniffing, MITM, Password Pilfering Attacks	Replay, Covert, Wormhole, Data-Injection, MITM, Spoofing Attacks	Wormhole, MITM, Buffer Overflow, Buffer Flooding, DDoS Attacks
MAC Layer	ARP-Spoofing, Traffic Analysis, MITM Attacks	ARP-Spoofing, TSA, MITM Attacks	Spoofing, TSA, Jamming, DDoS, Flooding, MITM Attacks
Physical Layer	Eavesdropping	Smart Meter Tampering Attacks, TSA	Jamming Attacks, TSA

Tablica 4.3.3

5. Primjena Smart Grid tehnologije u vođenju elektroenergetskih sustava[15][16][17]

5.1. Distribuirana, mrežna arhitektura u elektroenergetici[15]

Pametna mreža je moderna infrastruktura elektroenergetske mreže za poboljšanu učinkovitost, pouzdanost i sigurnost, s glatkom integracijom obnovljivih i alternativnih izvora energije, putem automatizirane kontrole i modernih komunikacijskih tehnologija. Obnovljivi generatori energije čine obećavajuću tehnologiju za smanjenje potrošnje goriva i emisija stakleničkih plinova. Važno je da pametne mreže omogućuju nove strategije upravljanja mrežom koje osiguravaju njihovu učinkovitu integraciju u distribuiranu proizvodnju (DG) za upravljanje potražnjom i pohranu energije za balansiranje opterećenja DG itd. Obnovljivi izvori energije (RES) široko su proučavani od strane mnogih istraživača, a integracija RES-a, smanjenje gubitaka sustava i povećanje pouzdanosti, učinkovitosti i sigurnosti opskrbe električnom energijom korisnicima su neki od napredaka koje pametna mreža sustav će povećati . Postojeća mreža nema komunikacijske sposobnosti, dok je infrastruktura pametne elektroenergetske mreže puna poboljšanih senzora i naprednih komunikacijskih i računalnih mogućnosti, kako je prikazano na slici 5.1.1. Različite komponente sustava povezane su komunikacijskim putevima i čvorištima senzora kako bi se osigurala interoperabilnost između njih, npr. distribucija, prijenos i druge trafostanice, kao što su stambene, komercijalne i industrijske lokacije.



Slika 5.1.1

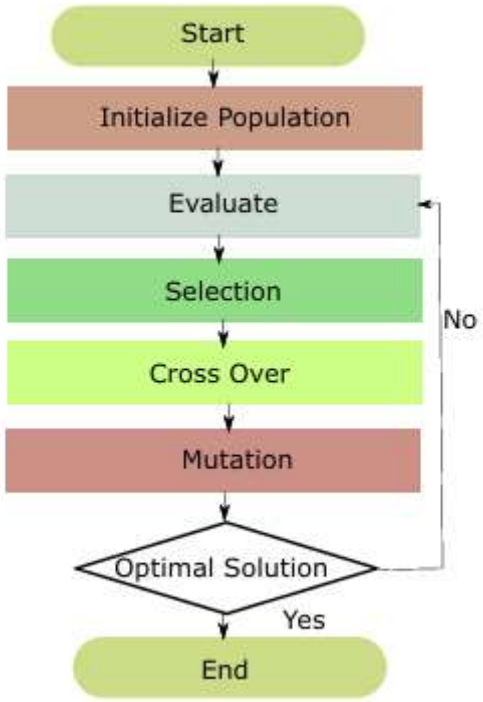
U pametnoj mreži, pouzdane i informacije u stvarnom vremenu postaju ključni faktor za pouzdanu isporuku energije od jedinica za proizvodnju do krajnjih korisnika. Utjecaj kvarova opreme, ograničenja kapaciteta i prirodnih nesreća i katastrofa, koje uzrokuju smetnje u opskrbi električnom energijom i prekide, može se uvelike izbjeći online praćenjem stanja elektroenergetskog sustava, dijagnostikom i zaštitom. U tu svrhu, inteligentno praćenje i kontrola omogućeni modernim informacijskim i komunikacijskim tehnologijama postali su ključni za ostvarivanje zamišljene pametne mreže.

5.2. Napredna analitika i komunikacija u Smart Grid rješenjima[16]

Mikro Mreže (MG) omogućuju korisnicima slobodu korištenja kada su spojene ili nisu spojene na mreže. Upravljanje Potražnjom (DR) poznato je kao promjena potražnje za korištenjem električne energije od strane krajnjih korisnika (ovisno o cijeni električne energije tijekom vršnih/niskih sati, rutinskim/dnevnim obrascima korištenja električne energije). DR pomaže u praćenju korištenja električne energije i pruža mogućnost krajnjim korisnicima za upravljanje energijom tijekom vršnih sati. Distribuirana Proizvodnja (DG) koristi se za napredne tehnologije koje pomažu u generiranju električne energije (u ili blizu objekta krajnjeg korisnika/kupca). DG uključuje solarne panele, vjetroturbine, hidroelektrane itd.. Optimizacija je tehnika koja se koristi za pronalaženje najboljeg rješenja za zadani problem, bilo maksimiziranjem ili minimiziranjem određene funkcije cilja. Postoji nekoliko optimizacijskih algoritama koji se koriste za optimizaciju u Smart Grid-ovima (SG). U ovom sistematskom preglednom članku fokusiramo se na Genetski Algoritam (GA), Optimizaciju Rojeva Čestica (PSO) i Optimizaciju Sivi Vuk (GWO) algoritam.

Genetski Algoritam (GA) bio-inspirirani je optimizacijski algoritam temeljen na konceptu biološke genetike. U osnovi, prirodni fenomen razdvajanja gena (od roditelja), vjerojatnost primanja gena (u potomcima) kombinira se u ovom pretraživačkom algoritmu kako bi pronašao najbolje/optimalno rješenje. Algoritam koristi skupinu pojedinaca (populaciju) i njihove karakteristike (kromosome) kako bi pronašao najprikladnijeg pojedinca. Proces uključuje križanje i mutaciju gena (jedan atribut/vrijednost iz kromosoma) za miješanje karakteristika između roditelja. Svaka populacija roditelja se reproducira i formira drugu populaciju potomaka s većim vrijednostima prilagodbe i mutacijama nego njihovi roditelji. Ovaj evolucijski algoritam poboljšava vrijednosti parametara u svakoj iteraciji, a proces se ponavlja sve dok se ne zadovolje željeni uvjeti završetka (optimalne vrijednosti). Slika 5.2.1 prikazuje tijek rada Genetskog algoritma. Algoritam se inicijalizira populacijom kromosoma ili skupom mogućih rješenja nazvanih generacija. Generacija se sastoji

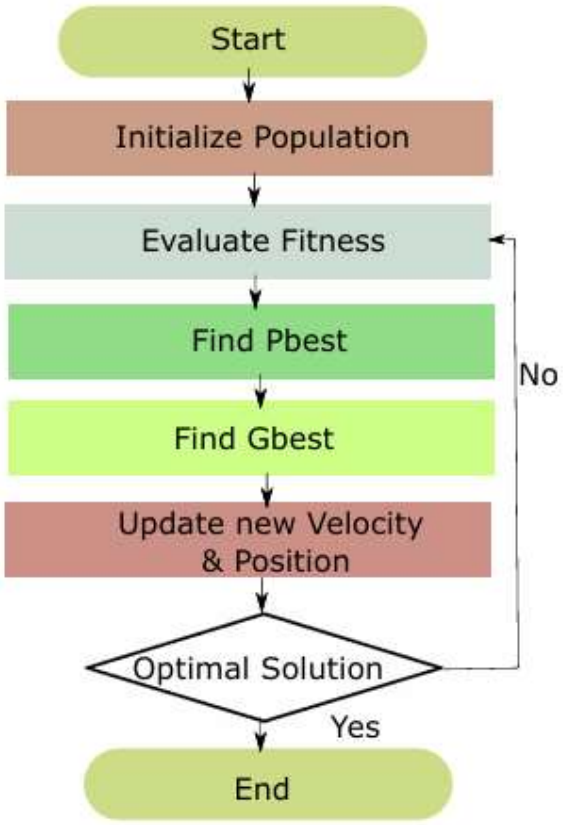
od kromosoma svakog pojedinca i ocjenjuje se njihova kvaliteta. Iz nasumičnog odabira pojedinaca iz populacije, karakteristike (kromosomi) se mijenjaju korištenjem križanja i mutacije kako bi se pronašla optimalna rješenja. Proces se ponavlja sve dok se ne postignu željeni rezultati bez slabih karakteristika u kromosomu.



Slika 5.2.1

Optimizacija Rojeva Čestica (PSO) inspirirana je ponašanjem i inteligencijom rojeva za donošenje optimizacijskih odluka. U PSO-u, svaki pojedinac rojeva iz populacije rojeva kreće se s određenom brzinom kako bi pronašao optimalno rješenje. Slika 5.2.2 ilustrira tijek rada PSO-a (tj. počevši od inicijalizacije populacije rojeva do pronalaženja optimalnog rješenja). Populacija rojeva sastoji se od pojedinačnih čestica/rojeva koji se kreću s nekom brzinom kako bi pretraživali najprikladnije rješenje prema zadanoj funkciji cilja. Algoritam ocjenjuje prilagodbu svake čestice i pronalazi najbolju česticu kao najbolje rješenje (Pbest), dok se globalno optimalno

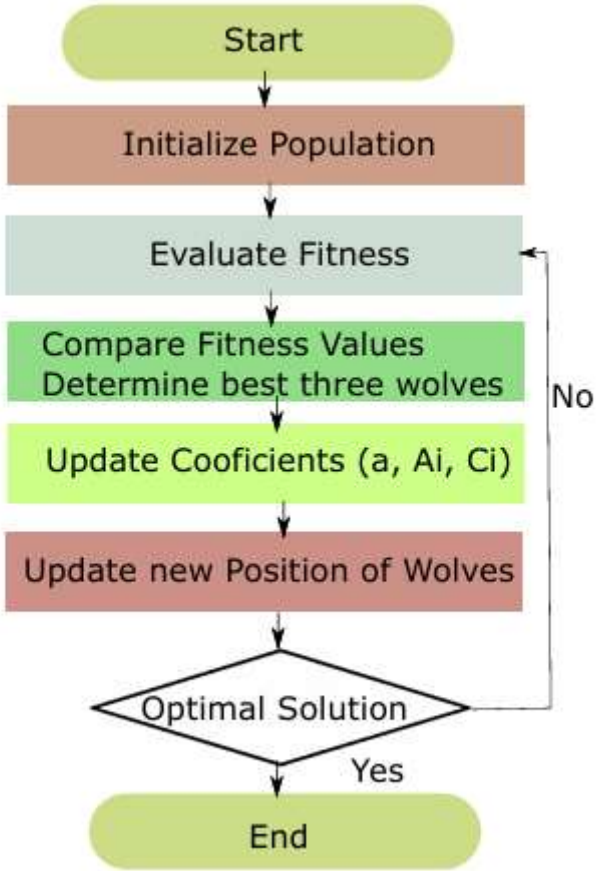
rješenje (Gbest) ažurira nakon svake iteracije kao optimalno rješenje iz populacije. Višestruka Optimizacija Rojeva Čestica (MoPSO) koristi se za rješavanje problema s više ciljeva, dok se PSO koristi samo za jednu funkciju cilja.



Slika 5.2.2

Optimizacija Sivi Vuk (GWO) još je jedna bio-inspirirana tehnika za pronalaženje optimalnog rješenja za zadanu funkciju cilja . GWO koristi prirodu lova i društvene liderske karakteristike sivih vukova. Četiri hijerarhijske grupe (Alfa, Beta, Delta i Omega) vukova koriste se za praćenje i napadanje plijena. Proces pronalaženja optimalnog rješenja definiran je prema grupnim karakteristikama vukova za kretanje, jurenje i/ili napadanje plijena. Slika 5.2.3 prikazuje tijek rada GWO-a, počevši od inicijalizacije populacije vukova za svaku grupu sivih vukova, npr., Alfa, Beta, Delta i Omega. Beta, Delta i Omega jure za optimalnim rješenjem i određuju tri

najbolje vrijednosti (vukove) za zadani optimizacijski problem. Koeficijenti vektora podešavanja, A i C, određuju najboljeg vuka u čoporu. C se može promijeniti u bilo koju nasumičnu vrijednost u svakoj iteraciji kako bi se istražila više rješenja za pronalaženje najbolje pozicije vuka. Dok je A ovisan o vrijednostima a, tako da -1 ≤ a ≤ 1. Promjenjive vrijednosti A pomažu u kretanju vukova u suprotnim smjerovima (istok/zapad, kako a mijenja od -1 do 1) od plijen centriranog na 0. Dok, i označava specifičan broj vuka iz grupe. Pomoću ovog pristupa, vukovi mogu globalno pretraživati optimalna rješenja. Jednom kada se pronađe optimalno rješenje, vukovi ažuriraju svoje koeficijente i pozicije u skladu s tim.

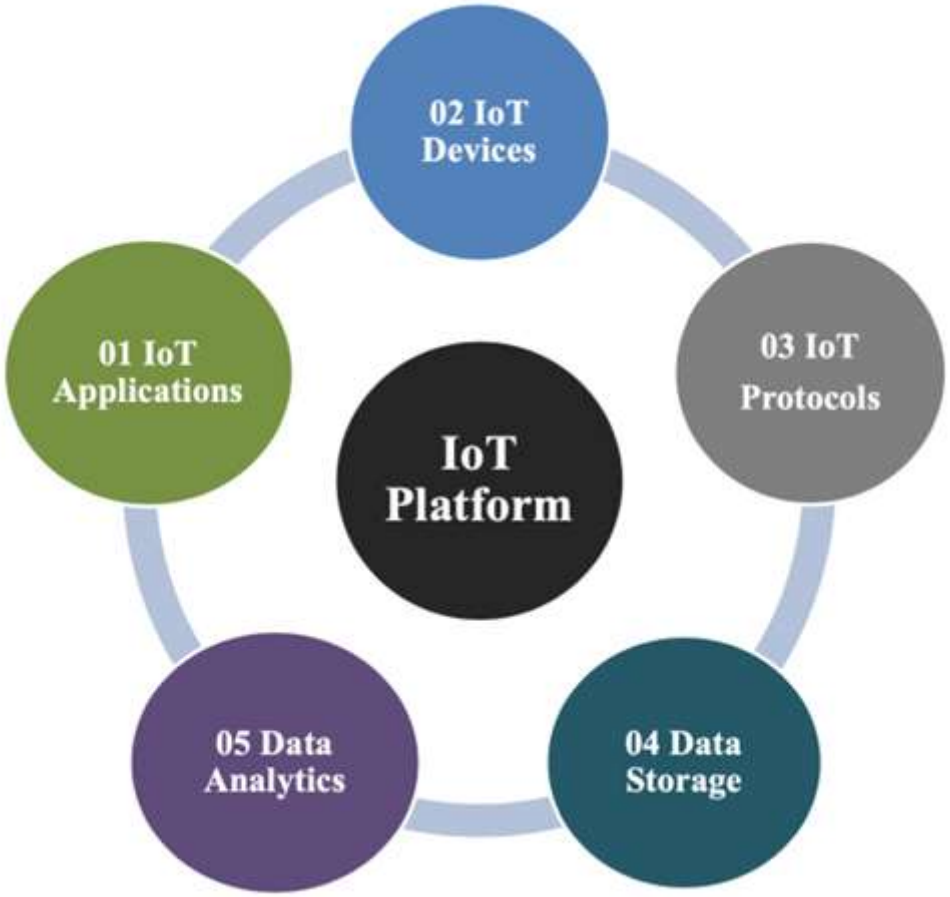


Slika 5.2.3

5.3. Integracija distribuiranih izvora energije i IoT uređaja[17]

IoT je nova tehnologija koja koristi Internet i ima za cilj pružiti povezanost između fizičkih uređaja ili "stvari". Primjeri fizičkih uređaja uključuju kućanske aparate i industrijsku opremu. Korištenjem odgovarajućih senzora i komunikacijskih mreža, ovi uređaji mogu pružiti vrijedne podatke i omogućiti pružanje raznovrsnih usluga za ljude. Na primjer, pametno upravljanje potrošnjom energije u zgradama omogućuje smanjenje troškova energije. IoT ima širok spektar primjena, poput proizvodnje, logistike i građevinske industrije. IoT se također široko primjenjuje u praćenju okoliša, zdravstvenim sustavima i uslugama, učinkovitoj upravljanju energijom u zgradama te uslugama temeljene na dronovima.

Prilikom planiranja IoT aplikacije, što je prvi korak u dizajniranju IoT sustava, odabir komponenti IoT-a poput senzorskog uređaja, komunikacijskog protokola, pohrane podataka i računalnih kapaciteta mora biti prikladan za namijenjenu aplikaciju. Na primjer, IoT platforma planirana za kontrolu grijanja, hlađenja i klimatizacije (HVAC) u zgradi zahtijeva korištenje relevantnih senzora okoliša i upotrebu odgovarajuće komunikacijske tehnologije. Slika 5.3.1 prikazuje različite komponente IoT platforme. IoT uređaji, koji su druga komponenta IoT platformi, mogu biti u obliku senzora, aktuatora, IoT gateway-a ili bilo kojeg uređaja koji se pridružuje ciklusu prikupljanja, prijenosa i obrade podataka. Na primjer, IoT gateway uređaj omogućuje usmjeravanje podataka u IoT sustav i uspostavljanje dvosmjerne komunikacije između uređaja-gateway i gateway-cloud.



Slika 5.3.1

Komunikacijski protokoli, treća komponenta IoT platforme, omogućuju različitim uređajima da komuniciraju i dijele svoje podatke s kontrolerima ili središtima za donošenje odluka. IoT platforme nude fleksibilnost u odabiru vrste komunikacijskih tehnologija (svaka s određenim značajkama), prema potrebama aplikacije. Primjeri ovih tehnologija uključuju Wi-Fi, Bluetooth, ZigBee i stanične tehnologije poput LTE-4G i 5G mreža.

Pohrana podataka je četvrta komponenta IoT platforme koja omogućuje upravljanje prikupljenim podacima sa senzora. U principu, podaci prikupljeni od uređaja su vrlo veliki. To zahtijeva planiranje učinkovite pohrane podataka koja može biti na cloud serverima ili na rubu IoT mreže. Pohranjeni podaci, koji se koriste u analitičke svrhe,

čine petu komponentu IoT platformi. Analitika podataka može se provoditi offline nakon pohrane podataka ili u obliku analitike u stvarnom vremenu. Analitika podataka provodi se za donošenje odluka o radu aplikacije. Na temelju potrebe, analitika podataka može se provoditi offline ili u stvarnom vremenu. U offline analitici, pohranjeni podaci se prvo prikupljaju i zatim vizualiziraju na lokaciji pomoću alata za vizualizaciju. U slučaju analitike u stvarnom vremenu, cloud ili edge serveri se koriste za pružanje vizualizacije, npr. stream analitike.

IoT je paradigma u kojoj objekti i elementi sustava opremljeni senzorima, aktuatorima i procesorima mogu međusobno komunicirati kako bi pružili smisleno usluge. U IoT sustavima, senzori se koriste za opažanje i prikupljanje podataka, a kroz gateway-e usmjeravaju prikupljene podatke u kontrolne centre ili u oblak za daljnju pohranu, obradu, analitiku i donošenje odluka. Nakon donošenja odluke, odgovarajuća naredba se potom šalje nazad aktuatoru instaliranom na sustavu kao odgovor na opažene podatke. Budući da postoji mnogo različitih senzorskih i aktuatorskih uređaja, komunikacijskih tehnologija i pristupa računalnoj obradi podataka, u ovom odjeljku objašnjavamo postojeće tehnologije koje omogućuju IoT. Zatim pružamo primjere iz literature kako se ove tehnologije koriste u energetskom sektoru.

Senzori su ključni pokretači IoT-a . Oni se koriste za prikupljanje i prijenos podataka u stvarnom vremenu. Korištenje senzora povećava učinkovitost, funkcionalnost i igra ključnu ulogu u uspjehu IoT-a. Postoje različite vrste senzora koje su razvijene za različite svrhe primjene. Primjeri ovih primjena uključuju poljoprivrednu industriju, praćenje okoliša, zdravstvene sustave i usluge te javnu sigurnost. U praksi, u energetskom sektoru uključujući proizvodnju, prijenos i distribuciju energije, koristi se mnogo ovih senzora. U energetskom sektoru, senzori se koriste za uštedu troškova i energije. Senzori omogućuju pametni sustav upravljanja energijom, pružaju optimizaciju energije u stvarnom vremenu i olakšavaju nove pristupe upravljanju opterećenjem energije. Istraživanja i budući trendovi senzorskih uređaja također ciljaju na razvoj senzorskih aplikacija za poboljšanje oblikovanja opterećenja i svijesti potrošača te razvoj specifičnih objekata za

unapređenje proizvodnje obnovljivih izvora energije. Ukratko, korištenje senzorskih uređaja unutar IoT-a u energetskom sektoru značajno poboljšava dijagnostiku, donošenje odluka, analitiku, optimizacijske procese i integrirane metrike performansi. Zbog velikog broja senzora koji se koriste u energetskom sektoru, u nastavku objašnjavamo nekoliko primjera uobičajenih senzorskih uređaja koji se primjenjuju u proizvodnji i potrošnji energije.

Temperaturni senzori koriste se za detekciju fluktuacija u grijanju i hlađenju sustava. Temperatura je važan i uobičajen parametar okoliša. U energetskom sektoru, osnovni princip proizvodnje energije je proces pretvorbe mehaničke energije u električnu energiju, dok se mehanička energija dobiva iz toplinske energije, npr. termoelektrane, vjetroelektrane, hidroelektrane i solarne elektrane. Ove energetske konverzije dobivaju se korištenjem toplinske energije, tj. temperature. S aspekta potrošnje energije, temperaturni senzori koriste se za maksimiziranje performansi sustava kada se temperatura mijenja tijekom normalnog rada. Na primjer, u stambenim područjima najbolje vrijeme za uključivanje ili isključivanje ventilacijskih i hlađenja sustava prepoznaje temperaturni senzor; tako se energija može pravilno upravljati kako bi se uštedjela energija.

Senzori vlage koriste se za određivanje količine vlage i relativne vlažnosti zraka. Omjer vlage u zraku u odnosu na najvišu moguću količinu vlage pri određenoj temperaturi zraka naziva se relativna vlažnost . Primjene senzora vlage u energetskom sektoru su široke. Na primjer, općenito se koriste u proizvodnji vjetroenergije. Korištenje senzora vlage na vjetroturbinama je posebno važno ako su turbine smještene na moru (zbog visokog nivoa vlage u zraku). Senzori vlage mogu se postaviti i na dnu vjetroturbina te pružiti kontinuirano praćenje vlage. To omogućuje operaterima da poduzmu mjere u slučaju promjena ili odstupanja u uvjetima rada turbine, što dovodi do konzistentnijih operacija, optimiziranih performansi i nižih troškova energije.

Senzori svjetlosti koriste se za mjerenje razine ambijentalnog svjetla ili svjetline svjetla. U potrošnji energije, senzori svjetlosti imaju nekoliko primjena u industrijskim i svakodnevnim potrošačkim aplikacijama. Budući da je glavni izvor potrošnje energije u zgradama povezan sa osvjetljenjem, koje respektivno čini gotovo 15% ukupne potrošnje električne energije. Na globalnoj razini, približno 20% električne energije koristi se za osvjetljenje. Stoga se senzori svjetlosti mogu koristiti za automatsku kontrolu razina osvjetljenja unutrašnjih i vanjskih prostora uključivanjem/isključivanjem ili prigušivanjem razina svjetla, tako da se električna razina svjetla automatski može prilagoditi u odgovoru na promjene u ambijentalnom svjetlu. Na taj način, energija potrebna za osvjetljenje unutrašnjih prostora može se smanjiti.

Pasivni infracrveni (PIR) senzori, također poznati kao senzori pokreta, koriste se za mjerenje infracrvene radijacije svjetla emitirane iz objekata u njihovoj okolini. U potrošnji energije, ovi senzori koriste se za smanjenje potrošnje energije u zgradama. Na primjer, korištenjem PIR senzora, prisustvo ljudi unutar prostora može se detektirati. Ako se ne detektira pokret u prostoru, kontrola osvjetljenja prostora isključuje svjetlo, tj. pametna kontrola osvjetljenja. Na taj način, potrošnja električne energije zgrada smanjuje se. Slično tome, ovo se može primijeniti na sustave klimatizacije koji troše gotovo 40% energije u zgradama.

Senzori blizine koriste se za detekciju prisutnosti obližnjih objekata bez ikakvog fizičkog kontakta. Primjer primjene senzora blizine je u proizvodnji vjetroenergije. Ovi senzori pružaju dugovječnost i pouzdane performanse senziranja položaja u vjetroturbinama. U vjetroturbinama, primjene senzora blizine uključuju kontrolu nagiba lopatica, položaj yaw-a, rotoru i položaj kočnice yaw-a; praćenje istrošenosti kočnica; i praćenje brzine rotora.

Aktuatori su uređaji koji pretvaraju određeni oblik energije u kretanje. Oni primaju električni ulaz iz automatizacijskih sustava, pretvaraju ulaz u akciju i djeluju na uređaje i strojeve unutar IoT sustava. Aktuatori proizvode različite obrasce kretanja poput linearnog, oscilacijskog ili rotacijskog kretanja. Na temelju izvora energije, aktuatori se kategoriziraju u sljedeće vrste.

Pneumatski aktuatori koriste stisnuti zrak za generiranje kretanja. Pneumatski aktuatori sastavljeni su od klipa ili dijafragma kako bi generirali pokretačku snagu. Ovi aktuatori koriste se za kontroliranje procesa koji zahtijevaju brzi i točni odgovor, budući da ti procesi ne zahtijevaju veliku količinu pokretačke sile.

Hidraulički aktuatori koriste tekućinu za generiranje kretanja. Hidraulički aktuatori sastavljeni su od cilindra ili tekućinskog motora koji koristi hidrauličku snagu za pružanje mehaničke operacije. Mehaničko kretanje daje izlaz u obliku linearnog, rotacijskog ili oscilacijskog kretanja. Ovi aktuatori koriste se u industrijskoj kontroli procesa gdje su potrebne visoke brzine i velike sile.

Toplinski aktuatori koriste izvor topline za generiranje fizičke akcije. Toplinski aktuatori pretvaraju toplinsku energiju u kinetičku energiju, odnosno kretanje. Općenito, termostatski aktuatori sastavljeni su od materijala za mjerenje temperature zatvorenog dijafragma koji pritiska na utičnicu za pomicanje cilindra. Materijal za mjerenje temperature može biti bilo koja vrsta tekućine, plina, voskastog spoja ili bilo kojeg materijala koji mijenja volumen ovisno o temperaturi.

Električni aktuatori primjenjuju vanjske izvore energije, npr. baterije, za generiranje kretanja. Električni aktuatori su mehanički uređaji sposobni pretvoriti električnu energiju u kinetičku energiju u obliku jednog linearnog ili rotacijskog kretanja. Dizajni ovih aktuatora temelje se na namijenjenim zadacima unutar procesa.

U energetskom sektoru, na primjer, u elektranama, pneumatski aktuatori tradicionalno se primjenjuju za kontrolu ventila. Tehnologija električnih aktuatora za kontrolu ventila omogućuje postizanje energetske učinkovitosti. Oni se također često koriste kao završni kontrolni element u radu elektrane. U literaturi postoji mnogo studija koje ilustriraju primjene aktuatora unutar IoT-a.

Bežični komunikacijski sustavi igraju glavnu ulogu u aktiviranju IoT-a. Bežični sustavi povezuju senzorske uređaje s IoT gateway-ima i omogućuju end-to-end prijenos podataka između ovih elemenata IoT-a. Bežični sustavi razvijeni su na temelju različitih bežičnih standarda, a odabir svakog od njih ovisi o zahtjevima aplikacije

poput dometa komunikacije, propusnosti i zahtjeva za potrošnjom energije. Na primjer, obnovljivi izvori energije, uključujući vjetroelektrane i solarne elektrane, često su smješteni u vrlo udaljenim područjima. Stoga je osiguravanje pouzdane IoT komunikacije u udaljenim mjestima izazov. Primjena IoT sustava na tim lokacijama zahtijeva odabir odgovarajuće komunikacijske tehnologije koja može jamčiti kontinuiranu vezu i podržati prijenos podataka u stvarnom vremenu na energetski učinkovit način. Zbog važnosti komunikacijskih tehnologija u IoT-u, u ovom pododjeljku pregledavamo neke od tih tehnologija. Također navodimo nekoliko primjera kako one funkcioniraju u energetskom sektoru. Zatim pružamo usporedbu u tablici 5.3.1 kako bismo prikazali razlike između svake od tehnologija kada se primjenjuju s IoT-om.

Bežične tehnologije kratkog dometa, npr. Wireless Fidelity (Wi-Fi) za IoT aplikacije u energetskom sektoru široko su proučavane. U energetskom sektoru, očiti slučajevi korištenja Wi-Fi-ja uključuju očitavanje energije i upravljanje energijom u zgradama . Međutim, zbog visokih zahtjeva za energijom Wi-Fi, ova tehnologija nije najbolji izbor u energetskom sektoru. Tehnologije komunikacije s niskom potrošnjom energije širokog područja (LPWAN) poput narrowband IoT (NB-IoT); ZigBee; Bluetooth low energy (BLE) tehnologija; kao i nove LPWAN tehnologije poput LoRa, Sigfox i LTE-M koje djeluju u nelicenciranom spektru, bolje su rješenja za korištenje u energetskom sektoru. To je zato što ove nove LPWAN tehnologije omogućuju uspostavljanje pouzdane, niskotarifne, niskopotrošne, dugodometne tehnologije zadnje milje za rješenja pametnog upravljanja energijom. Stoga, u ovom radu objašnjavamo tehnologije kratkog dometa i nove LPWAN tehnologije te pregledavamo nekoliko primjera njihovih primjena u energetskom sektoru. Također objašnjavamo satelitsku tehnologiju koja igra važnu ulogu u pružanju globalne IoT povezanosti za industrijske sektore smještene u udaljenim područjima. Osim toga, u tablici 5.3.1 ilustriramo različite značajke ovih tehnologija.

Technology \ Parameter	Range	Data Rate	Power Usage (Battery Life)	Security	Installation Cost	Example Application
LoRA	⩽50 km	0.3–38.4 kbps	Very low (8–10 years)	High	Low	Smart buildings (smart lighting)
NB-IoT	⩽50 km	⩽100 kbps	High (1–2 years)	High	Low	Smart grid communication
LTE-M	⩽200 km	0.2–1 Mbps	Low (7–8 years)	High	Moderate	Smart meter
Sigfox	⩽50 km	100 bps	Low (7–8 years)	High	Moderate	Smart buildings (electric plugs)
Weightless	<5 km	100 kbps	Low (Very Long)	High	Low	Smart meter
Bluetooth	⩽50 m	1 Mbps	Low (Few months)	High	Low	Smart home appliances
Zigbee	⩽100 m	250 Kbps	Very Low (5–10 years)	Low	Low	Smart metering in renewable energies
Satellite	Very Long >1500 km	100 kbps	High	High	Costly	Solar & wind power plants

Tablica 5.3.1

Bluetooth Low Energy (BLE) je bežična komunikacijska tehnologija kratkog dometa za IoT koja omogućuje razmjenu podataka korištenjem kratkih radio valova. BLE je jeftinije za implementaciju, s tipičnim dometom od 0 do 30 m, što omogućuje stvaranje trenutne osobne mreže područja. BLE je namijenjen malim IoT aplikacijama koje zahtijevaju uređaje da komuniciraju male količine podataka uz minimalnu potrošnju energije. Industrije u energetskom sektoru s dobro dizajniranim IoT strategijama mogu stvoriti nove oblike komunikacije između strojeva i između strojeva i ljudi korištenjem ove tehnologije. U energetskom sektoru, BLE se široko koristi za potrošnju energije u stambenim i komercijalnim zgradama. Na primjer, autori opisuju pametni sustav upravljanja energijom u uredu koji smanjuje potrošnju energije PC-ova, monitora i svjetala koristeći BLE. Druga studija predlaže sustav upravljanja energijom za pametne kuće koji koristi BLE za komunikaciju među kućanskim aparatima s ciljem smanjenja energije u kućama. Slično tome, korištenjem BLE tehnologije, istraživanje u uvodi fuzzy-bazirano rješenje za pametno upravljanje energijom u automatizaciji kuće, s ciljem poboljšanja sheme upravljanja energijom u kućama.

Zigbee je komunikacijska tehnologija dizajnirana za stvaranje osobne mreže područja i cilja na male aplikacije. Zigbee je jednostavan za implementaciju i planiran je za pružanje niskotarifnih, niskodatnih i visoko pouzdanih mreža za aplikacije s niskom potrošnjom energije. Zigbee također koristi specifikaciju mreže umreženosti (mesh network) gdje su uređaji povezani s mnogim međusobnim vezama. Korištenjem značajke mreže umreženosti Zigbee-ja, maksimalni domet komunikacije, koji je do 100 m, znatno se proširuje. U energetskom sektoru, primjeri IoT aplikacija Zigbee-ja uključuju sustave osvjetljenja (zgrade i ulična rasvjeta), pametne mreže, npr. pametna električna brojila, sustave automatizacije kuća i industrijsku automatizaciju. Ove aplikacije ciljaju pružanje pristupa za učinkovitu potrošnju energije. U literaturi, s ciljem minimizacije troškova energije potrošača, istraživanje u procjenjuje performanse aplikacije za upravljanje energijom u kući uspostavljanjem bežične senzorske mreže koristeći Zigbee.

Long Range (LoRa) je bežična komunikacijska tehnologija dizajnirana za IoT. LoRa je isplativa komunikacijska tehnologija za velike implementacije IoT-a, može dodati mnoge godine baterijskom vijeku. LoRa se također koristi za uspostavu dugoročnih prijenosa (više od 10 km u ruralnim područjima) uz vrlo nisku potrošnju energije. Značajke ove tehnologije čine je prikladnom komunikacijskom tehnologijom za korištenje u energetskom sektoru, prvenstveno u pametnim gradovima, kao što su pametne mreže i sustavi automatizacije zgrada, npr. pametno brojanje. U literaturi, rad u cilja na optimizaciju potrošnje energije implementacijom sustava upravljanja energijom u zgradama koristeći LoRa. Rad predlaže platformu integrirajući više sustava, poput klimatizacije, osvjetljenja i praćenja energije, za izvođenje optimizacije energije u zgradama.

Sigfox je tehnologija širokog područja mreže koja koristi ultra uski pojas. Sigfox omogućuje uređajima da komuniciraju s niskom potrošnjom energije kako bi omogućili IoT aplikacije. Za prikladnost ove tehnologije u energetskom sektoru, na primjer, studija u pregledava tehnološke napretke i predstavlja Sigfox kao jedno od najboljih niskopotrošnih rješenja za pametno brojanje kako bi omogućila usluge energetske u stvarnom vremenu za domaćinstva. Osim toga, studija uspoređuje

različite tehnologije komunikacijskih mreža s niskom potrošnjom energije širokog područja i zaključuje da je Sigfox prikladno rješenje za korištenje s senzorima utičnica u pametnim zgradama.

Narrowband IoT (NB-IoT) je LPWAN komunikacijska tehnologija koja podržava veliki broj IoT uređaja i usluga s visokom brzinom prijenosa podataka uz vrlo nisku latenciju. NB-IoT je niskotarifno rješenje koje ima dugi vijek trajanja baterije i pruža poboljšano pokriće. Zbog značajki latencije NB-IoT, ova tehnologija je potencijalno rješenje za pametne mreže distribucije energije pružajući niskotarifnu komunikaciju za pametna brojila.

Long Term Evolution for Machine-Type Communications (LTE-M) je standardizacija treće generacije partnerstva (3GPP) koja je dizajnirana za smanjenje složenosti uređaja za komunikaciju između strojeva (MTC). LTE-M podržava sigurnu komunikaciju, pruža sveprisutno pokriće i nudi visoku kapacitet sustava. LTE-M također nudi usluge niže latencije i veće propusnosti nego NB-IoT. Osim toga, ova tehnologija nudi energetski učinkovitu alokaciju resursa za uređaje s malom potrošnjom energije, čineći je potencijalnim rješenjem za pametna brojila i komunikacije pametne mreže.

Weightless je LPWAN otvoreni bežični standard koji je razvijen za uspostavu komunikacije među velikim brojem IoT uređaja i strojeva. Weightless je potencijalno rješenje za pametno brojanje u energetskom sektoru. Na temelju studije u [89], Weightless je prikladna bežična tehnologija koja se može koristiti u IoT aplikacijama pametnih kuća za pametno brojanje i komunikacije pametne mreže.

Satelitska je još jedna komunikacijska tehnologija koja ima vrlo široko područje pokrivenosti i može podržavati aplikacije s niskom brzinom prijenosa podataka u obliku komunikacije između strojeva (M2M). Satelitska tehnologija je prikladna za podršku IoT uređajima i strojevima u udaljenim mjestima. Studija u predstavlja IoT-baziranu satelitsku komunikaciju između strojeva koja je primjenjiva na pametnu mrežu, posebno za sektor prijenosa i distribucije (T&D).

Računarstvo i analiza podataka generiranih od strane IoT-a omogućuju stjecanje dubljeg uvida, preciznog odgovora sustavima i pomažu u donošenju prikladnih odluka o potrošnji energije sustava. Međutim, računarstvo IoT podataka predstavlja izazovan problem. Budući da IoT podaci, poznati kao Big Data, odnose se na ogromne količine strukturiranih i nestrukturiranih podataka, generiranih iz različitih elemenata IoT sustava poput senzora, softverskih aplikacija, pametnih ili inteligentnih uređaja i komunikacijskih mreža. Zbog karakteristika Big Data-a, koje su veliki volumen, visoka brzina i velika raznolikost, potrebno ih je učinkovito obraditi i analizirati. Obrada Big Data-a nadilazi kapacitete tradicionalnih metoda, tj. pohranjivanje na lokalnim tvrdom disku, računarstvo i kasniju analizu. Potrebne su napredne računalne i analitičke metode za upravljanje Big Data-om. U nastavku objašnjavamo cloud računarstvo i fog računarstvo, koje se široko koriste za obradu i računarstvo Big Data-a.

Cloud računarstvo je pristup obradi podataka koji nudi usluge, aplikacije, pohranu i računarstvo putem interneta te omogućuje računarstvo podataka koji se streamaju s IoT uređaja. U cloud računarstvu, "cloud" se odnosi na "Internet", a "računarstvo" na računalne i procesorske usluge koje nudi ovaj pristup. Cloud računarstvo se sastoji od aplikacijskih usluga koje se pristupaju putem interneta i hardverskih sustava koji se nalaze u podatkovnim centrima. Korištenjem ovih karakteristika, cloud računarstvo omogućuje obradu Big Data-a i pruža složene računalne mogućnosti. Glavne prednosti korištenja cloud sustava oslanjaju se na:

Iako je cloud računarstvo jedan od najboljih računalnih paradigmi za obradu podataka za IoT aplikacije, zbog kašnjenja i ograničenja propusnosti centraliziranih resursa koji se koriste za obradu podataka, potrebni su učinkovitiji načini. Fog računarstvo je distribuirana paradigma i proširenje clouda, koja premješta računalne i analitičke usluge bliže rubu mreže. Fog računarstvo je paradigma koja proširuje cloud na većoj mjeri i može podržati veće opterećenje. U fog računarstvu, svaki uređaj s mogućnostima računarstva, pohrane i mrežne veze djeluje kao fog čvor. Primjeri ovih uređaja uključuju, ali nisu ograničeni na, osobna računala, industrijske kontrolere, prekidače, rutere i ugrađene servere. U ovoj računalnoj

paradigmi, fog pruža lokalnu obradu i pohranu IoT podataka na IoT uređajima umjesto da ih šalje u cloud. Prednosti ovog pristupa uključuju poboljšane sigurne usluge potrebne za mnoge IoT aplikacije, kao i smanjenje mrežnog prometa i latencije. Stoga, u suprotnosti s cloud računarstvom, fog nudi usluge obrade i računarstva s bržim odgovorom i većom sigurnošću. To omogućuje brže donošenje odluka i poduzimanje odgovarajućih akcija.

Danas je energetski sektor visoko ovisan o fosilnim gorivima, koja čine gotovo 80 % konačne energije globalno. Pretjerano vađenje i sagorijevanje fosilnih goriva imaju negativne utjecaje na okoliš, zdravlje i ekonomiju zbog onečišćenja zraka i klimatskih promjena, samo da navedemo neke. Energetska učinkovitost, tj. potrošnja manje energije za pružanje iste usluge, i implementacija obnovljivih izvora energije su dvije glavne alternative za smanjenje negativnih utjecaja korištenja fosilnih goriva.

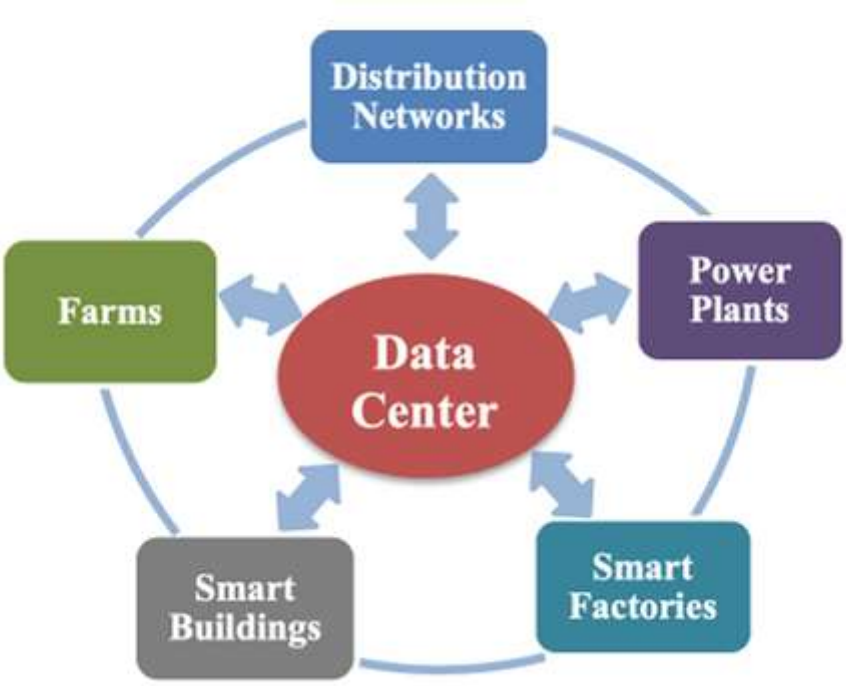
U ovom odjeljku raspravljamo o ulozi IoT-a u energetskom sektoru, od vađenja goriva, operacija i održavanja (O&M) energetskih generativnih resursa, do prijenosa i distribucije (T&D) te krajnje upotrebe energije. IoT može igrati ključnu ulogu u smanjenju gubitaka energije i smanjenju emisija CO2. Sustav upravljanja energijom temeljen na IoT-u može pratiti potrošnju energije u stvarnom vremenu i povećati razinu svijesti o energetskim performansama na bilo kojoj razini lanca opskrbe. Ovaj odjeljak prvo raspravlja o primjeni IoT-a u fazama generacije energije. Zatim nastavljamo s konceptom pametnih gradova, što je sveobuhvatan termin za mnoge IoT-bazirane pod-sustave poput pametnih mreža, pametnih zgrada, pametnih tvornica i inteligentnog transporta. Sljedeće, pojedinačno raspravljamo o svakoj od gore spomenutih komponenti.

Pametne mreže su moderni sustavi koji koriste najsigurniju i najpouzdaniju ICT tehnologiju za kontrolu i optimizaciju proizvodnje energije, prijenosa i distribucije (T&D) te krajnje potrošnje energije. Povezujući mnogo pametnih brojila, pametna mreža razvija višesmjerni tok informacija, koji se može koristiti za optimalno upravljanje sustavom i učinkovitu distribuciju energije. Primjena pametnih mreža

može se istaknuti u različitim podsektorima energetskog sustava pojedinačno, npr. proizvodnja energije, zgrade ili transport, ili ih se može razmatrati zajedno.

U tradicionalnim mrežama, baterije su se punile adapterima putem električnih kabela i AC/DC invertora. Ove baterije se mogu bežično puniti u pametnoj mreži, koristeći induktivnu tehnologiju punjenja. Osim toga, u pametnoj mreži, uzorak potražnje energije krajnjih korisnika može se analizirati prikupljanjem podataka putem IoT platforme, na primjer, vrijeme punjenja mobilnih telefona ili električnih automobila. Tada najbliža bežična stanica za punjenje baterija može dodijeliti odgovarajuće vremensko prozorsko razdoblje i to uređaj/vozilo može biti napunjeno. Još jedna prednost je da uporaba IoT-a dovodi do bolje kontrole i praćenja uređaja opremljenih baterijama, te stoga, prvo, distribucija energije može se prilagoditi, a drugo, isporuka električne energije ovim vozilima može biti zajamčena. To će znatno smanjiti nepotrebnu potrošnju energije.

Nadalje, IoT se može primijeniti u izoliranim i mikro mrežama za neka otoka ili organizacije, posebno kada je energija potrebna svakog trenutka bez izuzetka, npr. u bazama podataka. U takvim sustavima, svi resursi povezani na mrežu mogu međusobno komunicirati. Također, podaci o potražnji energije bilo kojeg resursa su dostupni. Ova interakcija može osigurati savršeno upravljanje distribucijom energije kad god i gdje god je potrebno. Što se tiče suradničkog utjecaja pametnih mreža, kao što je prikazano na slici 5.3.2, u pametnom gradu opremljenom IoT-baziranim pametnim mrežama, različiti dijelovi grada mogu biti povezani zajedno.



Slika 5.3.2

Tijekom suradničke komunikacije između različitih sektora, pametna mreža može upozoriti operatere putem pametnih uređaja prije nego što se dogodi bilo kakav akutni problem. Na primjer, kroz kontinuirano praćenje, može se detektirati ako potražnja energije premašuje kapacitet mreže. Stoga, prikupljanjem podataka u stvarnom vremenu, vlasti mogu usvojiti različite strategije i potrošnja energije može biti preusmjerena na drugo vrijeme kada je očekivana potražnja niža. U nekim regijama, pametne (ili dinamičke) cijene tarifa razmatrane su za varijabilne cijene energije u tom pogledu. Tarife s cijenama u stvarnom vremenu (RTP) kao i cijena energije bit će veće u određenom vremenu kada je potrošnja energije vjerojatno viša. Kroz podatke prikupljene iz komponenti pametne mreže, potrošnja i proizvodnja energije mogu se savršeno optimizirati i upravljati dugoročnim strategijama. Smanjenje prijenosnih gubitaka u T&D mrežama putem aktivnog upravljanja naponom ili smanjenje netehničkih gubitaka korištenjem mreže pametnih brojila su drugi primjeri primjene IoT-a.

Zaključak

Elektroenergetski sustav prolazi kroz temeljitu transformaciju, napuštajući dosadašnju jednosmjernu, centraliziranu koncepciju i prelazeći na kompleksnu, višesmjernu i digitalno povezanu mrežu. Razlog za ovu promjenu leži u potrebi da se odgovor na nove izazove – poput starenja postojeće infrastrukture, rastuće integracije obnovljivih izvora energije te sve većih zahtjeva za fleksibilnošću i sigurnošću – pronađe u tehnološkim inovacijama i automatizaciji. Pametne mreže (Smart Grids) kao koncept omogućuju uspostavu brze i pouzdane komunikacije među uređajima, operatorima te krajnjim korisnicima, što ih čini nužnima za učinkovito upravljanje složenim i dinamičnim elektroenergetskim sustavima. Uvođenje naprednih sustava upravljanja i nadzora, poput SCADA sustava, donijelo je mogućnost praćenja rada mreže u stvarnom vremenu i izdavanja upravljačkih naredbi na daljinu. Rješenja poput IEC 60870-5 i DNP3 protokola pridonijela su standardizaciji komunikacije unutar klasičnih SCADA okruženja, dok IEC 61850, s objektno orijentiranim pristupom i Ethernet/MMS protokolom, omogućuje još višu razinu integracije i interoperabilnosti, osobito u automatizaciji postrojenja poput trafostanica. Komunikacijske tehnologije također su doživjele značajan napredak: od tradicionalnih (PDH, SDH, ATM) polako se prelazi na modernije protokole (Ethernet/IP, MPLS) koji nude veću skalabilnost i prilagodljivost, dok bežične metode (Wi-Fi, ZigBee, LoRa, LTE/5G) osiguravaju pokrivenost i na teže dostupnim područjima. Kibernetička sigurnost postala je nezaobilazan čimbenik. Rastuća primjena distribuiranih izvora energije (DER), električnih vozila i sustava pohrane stavlja dodatni naglasak na uspostavu lokalnih, decentraliziranih modela upravljanja, uz korištenje IoT uređaja i naprednih analitičkih alata. Na taj se način postiže realno-vremenski uvid u stanje mreže, rano otkrivanje kvarova te optimizacija proizvodnje i potrošnje.

Literatura

[1] Thomas, M. S., & McDonald, J. D. (2017). *Power system SCADA and smart grids*. CRC press.

[2] Bevrani, H. (2014). *Robust power system frequency control* (Vol. 4, No. 2014). New York: springer.

[3] Paithankar, Y. G., & Bhide, S. R. (2022). *Fundamentals of power system protection*. PHI Learning Pvt. Ltd..

[4] Kirschen, D. S., & Strbac, G. (2018). *Fundamentals of power system economics*. John Wiley & Sons.

[5] Borlase, S. (Ed.). (2017). Smart grids: infrastructure, technology, and solutions. CRC press.

[6] Miladinovic, N. M., Polužanski, V. S., & Milosavljević, S. B. (2013). Komunikacione tehnologije u naprednoj elektroenergetskoj mreži. Zbornik radova, Elektrotehnički institut" Nikola Tesla", 23(23), 99-109.

[7] Shay, W. A., & Ivanišević, D. (2004). *Savremene komunikacione tehnologije i mreže: stvarni svet*. Kompjuter biblioteka.

[8] https://hr.wikipedia.org/wiki/Opti%C4%8Dko_vlakno

[9] Chhabra, N. (2013). Comparative analysis of different wireless technologies. International Journal of Scientific Research in Network Security and Communication, 1(5), 13-17.

[10] Clarke, G., Reynders, D., & Wright, E. (2004). Practical modern SCADA protocols: DNP3, 60870.5 and related systems. Newnes.

[11] Musil, P., & Mlynek, P. (2020, October). Overview of communication scenarios for IEC 60870-5-104 substation model. In *2020 21st International Scientific Conference on Electric Power Engineering (EPE)* (pp. 1-4). IEEE.

[12] Mackiewicz, R. E. (2006, June). Overview of IEC 61850 and Benefits. In *2006 IEEE Power Engineering Society General Meeting* (pp. 8-pp). IEEE.

[13] Brunner, C. (2008, April). IEC 61850 for power system communication. In *2008 IEEE/PES Transmission and Distribution Conference and Exposition* (pp. 1-6). IEEE.

[14] Schwarz, K. (2008). Comparison of IEC 60870-5-101/-103/-104, DNP3, and IEC 60870-6-TASE. 2 with IEC 61850.

[15] Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. IEEE transactions on Industrial informatics, 7(4), 529-539.

[16] Aslam, S., Altaweel, A., & Nassif, A. B. (2023). Optimization algorithms in smart grids: A systematic literature review. arXiv preprint arXiv:2301.07512.

[17] Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of Things (IoT) and the energy sector. *Energies*, *13*(2), 494.

[18] Salman, S. K. (2019, September). Evolution of conventional power systems to smart grids. In *2019 54th International Universities Power Engineering Conference (UPEC)* (pp. 1-6). IEEE.

[19] Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094.

Sažetak

Komunikacijska podrška sustavima za napredno vođenje elektroenergetskih mreža

Ovaj rad objašnjava ključne promjene u elektroenergetskom sektoru na putu prema konceptu pametnih mreža (Smart Grids). Polazi od konvencionalnih elektroenergetskih sustava i prikazuje njihov razvoj u smislu transformacije, ugradnje novih tehnologija te integracije distribuiranih izvora energije. Ističe se važnost SCADA sustava, protokola poput IEC 60870-5-104, DNP3 i IEC 61850, kao i uloga komunikacijskih tehnologija (Ethernet, IP/MPLS, ZigBee, LoRa itd.) u vođenju i nadzoru modernih mreža. Poseban naglasak stavljen je na sigurnosne izazove, osobito na očuvanje povjerljivosti, integriteta i dostupnosti podataka. U konačnici, opisane su mogućnosti napredne analitike, IoT-a i distribuiranih arhitektura u optimizaciji rada, proizvodnje i potrošnje električne energije.

Ključne riječi: SCADA, pametna mreža, IoT (Internet stvari)

Summary

Communication support for advanced control of power networks

This paper explains the key changes in the power sector on the path toward the concept of Smart Grids. It starts from conventional power systems and describes their development in terms of transformation, the adoption of new technologies, and the integration of distributed energy sources. The importance of SCADA systems and protocols such as IEC 60870-5-104, DNP3, and IEC 61850 is highlighted, as well as the role of communication technologies (Ethernet, IP/MPLS, ZigBee, LoRa, etc.) in managing and monitoring modern networks. Special emphasis is placed on security challenges, especially preserving the confidentiality, integrity, and availability of data. Finally, the paper outlines the possibilities of advanced analytics, IoT, and distributed architectures for optimizing the operation, generation, and consumption of electrical energy.

Keywords: SCADA, Smart grid, IoT (Internet of Things)