UNIVERZA V LJUBLJANI
FAKULTETA ZA ELEKTROTEHNIKO

Edvard Košnjek

INFORMACIJSKO-KOMUNIKACIJSKI SISTEMI IN AKTIVNA OMREŽJA ZA DISTRIBUCIJO ELEKTRIČNE ENERGIJE

MAGISTRSKO DELO

Mentor: prof. dr. Stanislav Kovačič

Ljubljana, 2010

Univerza v Ljubljani
Fakulteta za elektrotehniko

Tržaška 25
p.p. 2999
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
faks: 01 426 46 30
www.fe.uni-lj.si
e-mail: dekanat@fe.uni-lj.si

Št. naloge: M-1163/2010
Datum: 25. 03. 2010

Fakulteta za elektrotehniko Univerze v Ljubljani izdaja naslednjo nalogo:

Kandidat: **Edvard Košnjek, univ. dipl. inž. el.**

Naslov: **Informacijsko komunikacijski sistemi in aktivna omrežja za distribucijo električne energije**

Naslov v angleščini: **Information communications systems and smart grids for electricity distribution**

Vrsta naloge: **Magistrsko delo**

Tematika naloge:

V zadnjih letih je EU sprejela strategijo trajnostnega razvoja in jo vključila v večino svojih politik, tudi v energetsko in okoljsko. Prevzela je vodilno vlogo v boju proti podnebnim spremembam na mednarodni ravni in se hkrati obvezala k spodbujanju na znanju temelječega in energetsko učinkovitega gospodarstva. Evropska komisija ocenjuje, da bo imela informacijsko-komunikacijska tehnologija pri zmanjšanju porabe energije in povečanju energetske učinkovitosti v EU pomembno vlogo. V tem kontekstu se veliko pričakuje od t.i. »pametnih omrežij« (Smart Grids), ki predvidevajo izgradnjo sodobnih informacijsko komunikacijskih sistemov v distribuciji električne energije.

V magistrski nalogi analizirajte stanje tehnike na področju informacijsko komunikacijskih sistemov v distribuciji električne energije. Analizirajte potreben razvoj informacijsko komunikacijskih sistemov za bodoče potrebe aktivnih omrežij. Preverite možnosti uporabe različnih telekomunikacijskih tehnologij: lastnih optičnih in radijskih zvez ter komercialnih brezžičnih sistemov. Posvetite posebno pozornost varnosti informacijsko komunikacijskih sistemov in predlagajte rešitev evolucije obstoječih sistemov na bolj prožne, standardizirane in varne informacijsko komunikacijske sisteme.

Mentor: S. Kovačič
prof. dr. Stanislav Kovačič

Fakulteta za elektrotehniko • UNIVERZA V LJUBLJANI • 2

Predstojnik katedre:
prof. dr. Borut Zupančič

Dekan:
prof. dr. Janez Nastran

Z A H V A L A

Iskreno se zahvaljujem svojemu mentorju prof. dr. Stanislavu Kovačiču, univ. dipl. inž. el., ki me je s strokovnimi nasveti vodil in usmerjal pri izdelavi magistrskega dela.

Zahvaljujem se predsedniku uprave Elektra Gorenjska, d.d., mag. Jožetu Knavsu za podporo moji želji po dodatnem strokovnem izobraževanju in za razumevanje pri nelahkem usklajevanju mojih delovnih in študijskih obveznosti.

Hvala vsem sodelavcem v Elektru Gorenjska za pomoč pri spoznavanju elektroenergetike in telekomunikacij, še posebej g. Janezu Hudobivniku, mag. Marjanu Jereletu, g. Tomažu Mavcu, g. Damjanu Prašnikarju, g. Janezu Smukavcu, g. Boštjanu Tišlerju in g. Petru Zagožnu.

Na tem mestu moram posebej poudariti, da študija ne bi tako uspešno končal brez nesebične podpore moje žene Marjane in hčerke Nives, ki jima tudi posvečam to delo.

VSEBINA

SEZNAM UPORABLJENIH SIMBOLOV IN OKRAJŠAV

AAA …… **A**uthentication, **A**uthorization, **A**ccounting – avtentikacija, avtorizacija in zapisovanje (beleženje) dogodkov

AMI …… Advanced Metering Infrastructure – napredna merilna infrastruktura, nadgradnja AMM, AMR; vključuje tudi upravljanje meritev plina, vode …

AMM …… Advanced Metering Management – napredna merilna infrastruktura, omogoča tudi upravljanje merilnega mesta, npr. daljinski odklop

AMR …… Automated Meter Reading – avtomatsko odčitavanje merilnih naprav

AN-URE …… Nacionalni akcijski načrt za energetsko učinkovitost za obdobje 2008-2016

CFP ……..…..… Customer Feedback Programes – programi DR, temelječi na povratnih informacijah

CIM ……..….. Common Information Model – poenotena podatkovna struktura

DCV ……..…… distribucijski center vodenja

DLC ……..…. Distribution Line Carrier

DoS (attack)…… Denial of Service - napad z zavrnitvijo storitve, onemogoči delovanje računalnika ali storitve

DP ……..…..… Dynamic Pricing – program DR, temelječ na spremenljivih cenah

DR ……..…..… Demand Response – sposobnost porabe za odziv

DSB …….. Demand Side Bidding - ponudba odjemalcev s področja DSM

DSM ……..…..… Demand Site Management – upravljanje porabe

DSO ……..….. Distribution system operator - sistemski operater distribucijskega omrežja (SODO)

EAP ……. Extensible Authentication Protocol - razširljiv avtentikacijski protokol

EAP-GTC …… EAP-Generic Token Card - avtentikacija z žetonskimi karticami

EAP-MSCHAPv2 EAP Microsoft Challenge Handshake Authentication Protocol v2, Microsoftov avt. protokol, temelji na metodi izmenjave gesel

EAP-OTP …… EAP-One Time Password - avtentikacija z enkratnimi gesli

EAP-TLS ……. EAP-Transport Layer Security

EAP-TTLS ……. EAP Tunneled Transport Layer Security – tuneliran TLS

EC …….. Energy Conservation - zmanjševanje porabe

ECS SCADA ..... Energy Control Systems SCADA – SCADA sistem za upravljanje elektroenergetskih sistemov

EDF …….. Electricité de France – francosko podjetje, ki združuje proizvodnjo, prenos in distribucijo EE

EE …….. električna energija

EES ……. elektroenergetski sistem

EG ……..…. Elektro Gorenjska, d.d., podjetje za distribucijo električne energije, Ul. Mirka Vadnova 3a, 4000 KRANJ

ENEL ……. Ente Nazionale per l'energia Elettrica – italianski nacionalni distributer EE

EZ ……. Energetski zakon

GPRS …….. General Packet Radio Service - storitev paketne izmenjave podatkov

IDP ……. Intrusion Detection & Prevention System - sistem za odkrivanje in preprečitev napadov na IKS

IDS ……. Intrusion Detection System – sistem za odkrivanje napadov na IKS

IEC ……..... International Electrotechnical Commission – Mednarodna komisija za elektrotehniko: mednarodna organizacija za standardizacijo s področja elektrotehnike

IKS ……..…….. informacijsko–komunikacijski sistem

IKT…….... informacijsko komunikacijska tehnologija

IP …….. Internet Protocol

IPSec …… IP security – varnostni IP protokol

IRP …… Integrated Resource Planning – proces optimizacije energetskih prihrankov

ISM ….....…. Industrial, Scientific and Medical radio bands – frekvenčni pasovi, namenjeni uporabi v industriji, raziskavah in medicini

ISO – OSI …… ISO: Internatonal Organization for Standardization, OSI: Open Systems Interconnection; ISO – OSI je sedem stopenjski osnovni arhitekturni model za komunikacijo med računalniki

KT ……. konična tarifa

LAN …….. Local Area Network – lokalno (računalniško) omrežje

LCP ……. Load Control Programes - programi temelječi na krmiljenju bremena

LEAP …….. Lightweight EAP, EAP s šibko avtentikacijo, uporaba fiksnega gesla

LM ……..…… Load Management – upravljanje obremenitve

MIB ……. Management Information Base – porazdeljeno skladišče podatkov za upravljanje omrežja

MMS …… ..…... Manufacturing Message Specification

MT ……. mala tarifa

NN …… nizka napetost (0,4 kV)

NTP ……... Network Time Protocol - protokol za sinhronizacijo sistemskega časa računalniških sistemov

PEAP ……... Protected EAP – zaščiten (tuneliran) EAP, npr. PEAP/EAP-MSCHPv2

PIN ……. Personal Identification Number – osebna identifikacijska številka

PPP ……. Point to Point Protocol – protokol za izmenjavo sporočil točka – točka

RADIUS …….. Remote Authentication Dial-In Services – storitev avtentikacije na daljavo

RP …….. razdelilna postaja

RTP ……..…. razdelilno transformatorska postaja

SCADA ……. Supervisory Control And Data Acquisition – nadzorno vodenje in zajem podatkov

SiGen-CA …… Slovenian General Certification Authority – slovenski overitelj digitalnih potrdil

SN …… srednja napetost (10 kV , 20 kV, 35 kV)

SNMP ……. Simple Network Management Protocol - protokol za upravljanje TCP/IP in drugih omrežij

SODO ……... Sistemski operater distribucijskega omrežja

TCP …….. Transmission Control Protocol

TCP/ IP…….. Transmission Control Protocol / Internet Protocol

TK …….. telekomunikacije

TOU …….. Time of use pricing – sistem tarifnih časov

TP ……..…..… transformatorska postaja

VN …….. visoka napetost (v distribucijskem omrežju 110 kV, v prenosnem 400 kV, 220 kV ali 110 kV)

VPN …… Virtual Private Network – navidezno privatno omrežje

VT ……. visoka tarifa

WEP ……... Wired Equivalent Privacy – varnostni protokol za mobilna omrežja (starejši)

WLAN …… Wireless Local Area Network – brezžično lokalno (računalniško) omrežje

WPA(2) ……... Wi Fi Protected Access - varnostni protokol za mobilna omrežja (sodobnejši)

KAZALO TABEL

KAZALO SLIK

POVZETEK

Magistrsko delo obravnava stanje tehnike in potreben razvoj na področju informacijsko-komunikacijskih sistemov v distribuciji električne energije. V boju proti podnebnim spremembam in spodbujanju, na znanju temelječega in energetsko učinkovitega gospodarstva v EU, je nujno zmanjšanje porabe energije in povečanje energetske učinkovitosti, pri čemer bo imela informacijsko-komunikacijska tehnologija pomembno vlogo. V tem kontekstu se veliko pričakuje od t.i. »pametnih omrežij« (Smart Grids), ki predvidevajo izgradnjo sodobnih informacijsko-komunikacijskih sistemov v distribuciji električne energije.

Namen dela je prikazati izzive, s katerimi se soočajo distribucijska podjetja v Sloveniji in po svetu ob postopnem prehodu k aktivnim omrežjem za distribucijo električne energije. Predstavljeno je stanje tehnike na področju obratovalnih meritev, nadzora in vodenja distribucijskega omrežja ter obračunskih meritev električne energije.

Upravljanje porabe električne energije pri odjemalcih (DSM) je ena od neizkoriščenih priložnosti za izboljšanje energetske učinkovitosti. V delu so predstavljeni izvedljivi ukrepi s področja upravljanja porabe in pogoji za njihovo implementacijo, tako pravni kot tehnični.

V nadaljevanju je predstavljen koncept sodobnega informacijsko-komunikacijskega sistema v distribuciji električne energije, ki bo temeljil na sodobnih standardiziranih rešitvah komunikacijskih sistemov, na sodobnih komunikacijskih standardih in poenotenju podatkovnih struktur. Sledi obravnava prednosti in slabosti različnih komunikacijskih tehnologij: optičnega omrežja, javnega mobilnega omrežja, digitalnega radia ter tehnologij WiMax in Wi-Fi.

V delu je posebna pozornost namenjena zagotavljanju varnosti informacijsko- komunikacijskega sistema. Varnost je obravnavana tako s teoretičnega kot tudi z vidika načrtovanja varnega telekomunikacijskega sistema za aktivna omrežja.

Sklepni del povzema ugotovitve predhodnih poglavij in potrdi hipotezo o nujnosti celovitega pristopa k izgradnji aktivnih omrežij ter podaja predvidene aktivnosti Elektra Gorenjska, d.d., na tem področju.

Ključne besede: aktivna omrežja (Smart Grids), distribucija električne energije, AMR, AMM, AMI sistemi, upravljanje porabe EE pri odjemalcu (DSM), ISO-OSI 7-plastni model, IEC 61850, poenotenje podatkovnih struktur – CIM, IEC 61970, IEC 61968, varnost TK sistema, avtentikacija, IPSec VPN, GPRS/UMTS, Ethernet, TCP/IP

ABSTRACT

Master's thesis deals with the state of the art and the necessary development in the field of information communication systems in the distribution of electricity. The fight against climate change and promote a knowledge-based economy is an important objective of EU policies. Therefore, the EU seeks to reduce power consumption and increase energy efficiency. Important role in achieving these goals will have the information and communication technology. In this context, much is expected from the so-called "Smart Grids", which require the construction of modern information and communication systems in the distribution of electricity.

The purpose of thesis is to show the challenges faced by distribution companies in Slovenia and the world at a gradual transition to an active network for the distribution of electricity. The state of the art in the areas of: operational measurement, control and management of distribution networks and power measurements account are defined.

Demand side management (DSM) is one of missed opportunities to improve energy efficiency. The study presents the legal and technical conditions for implementation of feasible measures in the area of power management.

Furthermore, the concept of the modern information and communication system in the distribution of electricity, based on advanced standardized solutions for communication systems, modern communication standards and standardization of data structures are presented. Thereafter, a discussion of strengths and weaknesses of various communication technologies: optical networks, public wireless networks, and digital radio technologies, WiMax and Wi-Fi is stated.

In concluding part, particular attention is paid to ensuring security of information and communication system. Safety is also addressed from a theoretical point of view as well as secure telecommunications system planning for active networks.

Final section summarizes the previous findings and confirms the hypothesis on the necessity of a comprehensive approach to building active networks and provides planned activities of Elektro Gorenjska, d.d., in this area.

Key words: Smart Grids, distribution of electrical energy, AMR, AMM, AMI systems, Demand Side Management (DSM), ISO-OSI 7-layer model, IEC 61850, Common Information Model – CIM, IEC 61970, IEC 61968, TK system security, avtentication, IPSec VPN, GPRS/UMTS, Ethernet, TCP/IP.

1 UVOD

V zadnjih letih je problematika vplivov človeka na okolje postala prvovrstna gospodarska in predvsem politična tema. Javnost (skoraj) ne dvomi v katastrofalen vpliv človekovega izrabljanja fosilnih goriv in izpustov CO_2. Čeprav je vedno več tudi skeptikov, ki dvomijo v človekovo moč vplivati na predvsem naravne procese, ostajata dejstvo, da človeštvo razpolaga z znanjem in tehnologijo, s katero je mogoče že danes učinkoviteje in bolj gospodarno uporabljati omejene vire energije.

Evropska politika v svetovnem merilu izstopa s paketom ambicioznih ciljev z marketinškim imenom 20–20–20 do leta 2020[1]. Ne glede na (ne)uresničljivost zadanih ciljev se njihovemu doseganju namenja veliko pozornosti, pa tudi denarja.

Proizvodnja, prenos in distribucija električne energije imajo pomembno vlogo tako pri zagotavljanju večjega deleža energije iz obnovljivih virov, posredno pa tudi pri zmanjšanju izpustov toplogrednih plinov in pri racionalizaciji porabe energije. Povečevanje izkoriščanja obnovljivih virov energije, npr. potenciala vodne energije, vetra, sončne energije, izkoriščanja biomase, bioplina, na drugi strani pa omejevanje uporabe deleža fosilnih goriv pri proizvodnji električne energije, povečuje delež energije iz obnovljivih virov in zmanjšuje izpuste toplogrednih plinov. Predvsem distribucija električne energije lahko z ukrepi usmerjene porabe (Demand Side Management – DSM) vpliva na racionalnejšo rabo energije. Tu je še pospešen razvoj in pričakovana večja uporaba električnih vozil in zmogljivejših hranilnikov električne energije.

Množično priključevanje majhnih enot za proizvodnjo električne energije na distribucijsko omrežje, električna vozila kot hranilniki energije, zahteva po merjenju porabe električne, pa tudi toplotne energije, vode, plina ... prinaša precejšnje spremembe v logiko obratovanja distribucijskega omrežja, pri katerem smo bili do sedaj vajeni (predvsem) enosmernega pretoka in razdeljevanja energije, proizvedene v velikih proizvodnih enotah. Nadzor in vodenje posledično mnogo bolj »aktivnega« distribucijskega omrežja postajata vedno večji izziv.

[1] Politični cilj EU je do leta 2020 v primerjavi z letom 1990 zmanjšati emisije toplogrednih plinov CO_2 za 20 %, povečati proizvodnjo energije iz obnovljivih virov za 20 % in zmanjšati porabo končne energije za 20 %.

V javnosti se v zadnjem času vse pogosteje izpostavlja nujnost izgradnje »pametnih omrežij« za distribucijo električne energije (Smart Grids). Povsem neupravičene so domneve, da gre pri tem za uvajanje informacijsko-komunikacijskih sistemov tam, kjer jih do sedaj ni bilo in da bodo šele »pametna omrežja« začetek informatizacije distribucijskega omrežja. V Sloveniji so že dlje časa vse razdelilno transformatorske postaje (RTP) VN/SN daljinsko vodene in nadzorovane, pomembnejši stikalni aparati (odklopniki, ločilni odklopniki ...) na SN omrežju so daljinsko vodeni, obratujejo SN zanke z avtomatskim izločanjem okvarjenega odseka zanke, telemetrični permanentni monitoring kakovosti napetosti je uveden v vseh RTP, vsi odjemalci električne energije s priključno močjo 41 kW ali več so opremljeni s telemetričnimi merilnimi sistemi, avtomatsko odčitavanje se postopoma uvaja tudi na segmentu gospodinjskih odjemalcev. Distribucijska podjetja razpolagajo z lastnimi optičnimi in radijskimi komunikacijskimi sistemi, nadzornimi centri in centri vodenja.

Kljub dolgi tradiciji uporabe informacijsko-komunikacijskih sistemov distribuciji EE pa moramo priznati, da ravno ti sistemi zaradi svoje heterogenosti, strogo namenske uporabe, nepovezanosti in drugih tehničnih omejitev postajajo ozko grlo in ovira hitrejšemu razvoju. Nujna je izgradnja sodobnih sistemov vodenja za optimalno uravnavanje pretokov električne energije med razpršeno proizvodnjo iz obnovljivih (in nezanesljivih) virov energije in zahtevnimi uporabniki električne energije. Očitno brez tehnološkega preskoka na področju uporabe informacijsko-komunikacijskih sistemov v distribuciji električne energije ne bo šlo.

1.1 Zastavljena naloga, temeljni cilji, predvidevanja in omejitve

Namen tega dela je predstaviti trenutno stanje tehničnih informacijsko-komunikacijskih sistemov v distribuciji električne energije in prikazati izzive, s katerimi se soočajo distribucijska podjetja v Sloveniji in po svetu ob postopnem prehodu k aktivnim omrežjem[2] za distribucijo električne energije.

Namen mojega dela bo dosežen s predstavitvijo trenutnega stanja na področju obratovalnih ter obračunskih meritev v omrežju za distribucijo električne energije, sistemov vodenja in informacijsko-komunikacijskih sistemov. Vloga in delovanje distribucijskega elektroenergetskega sistema bo s prehodom na aktivna omrežja mnogo bolj kompleksna,

[2] V delu je uporabljen pojem »aktivna omrežja« za EE omrežja prihodnosti (Smart Grids). Večina avtorjev v Sloveniji sicer še uporablja prevod »pametna omrežja«, ki pa v strokovni javnosti vzbuja upravičene pomisleke.

tehnološki razvoj bo še posebej temeljit na področju informacijsko-komunikacijskih sistemov in njihovega zlivanja z elektroenergetskim omrežjem in sistemi, kot jih poznamo danes.

Osnovna hipoteza dela je, da je k izgradnji aktivnih omrežij potreben celovit pristop, pri čemer mora v prihodnje razvoj informacijsko-komunikacijskih sistemov temeljiti na standardiziranih rešitvah, ki morajo biti dovolj prožne, v smislu možnosti nadgradnje obstoječih sistemov in uporabe vseh razpoložljivih telekomunikacijskih tehnologij. Ravno na področju telekomunikacij in prenosa ter obdelave množice podatkov, ki bodo na voljo za obvladovanje aktivnih omrežij, je pričakovati največ težav.

Pri obravnavanju obstoječega stanja se delo večinoma omejuje na konceptualne rešitve merilnih in informacijsko-komunikacijskih sistemov in izhaja iz stanja tehnike v obravnavanem podjetju, Elektro Gorenjska[3], d.d. Pri tem je potrebno pripomniti, da je obravnavano podjetje eno od petih podjetij za distribucijo EE v Sloveniji in da z vidika razvoja med slovenskimi distribucijami na področju tehničnih informacijsko-komunikacijskih sistemov ni velikih konceptualnih razlik.

Področje aktivnih omrežij in z njim povezan razvoj informacijsko-komunikacijskih sistemov v elektroenergetiki je v tem trenutku izredno dinamično. Še leta 2006 so bila prizadevanja avtorja za hitro uvedbo Ethernet tehnologij in informatizacijo SN omrežja v večjem delu strokovne javnosti deležna precejšnje skepse, pa tudi pozornosti[4]. Pogledi na prihodnost informacijsko-komunikacijskih sistemov v elektroenergetiki so se v tem času bistveno spremenili. Delo zato nima ambicije podajanja konkretnih tehničnih rešitev z vsemi podrobnostmi, saj bi le-te hitro postale neaktualne.

Proučevanje zahtev za bodoči razvoj aktivnih omrežij, predvsem na področju upravljanja porabe EE pri odjemalcih, v Sloveniji ni dovolj razvito in temelji predvsem na tujih izkušnjah ter na študiju tuje literature.

1.2 Metodologija in vsebina dela

[3] Elektro Gorenjska, podjetje za distribucijo električne energije, d.d., Kranj, Ulica Mirka Vadnova 3a. Avtor je zaposlen v obravnavani organizaciji od leta 2002.

[4] Avtorju je Gospodarska zbornica Slovenije – Območna zbornica za Gorenjsko leta 2007 podelila srebrno priznanje za inovacijo »Sistem obratovalnih meritev v distribuciji EE – komunikacijski del«, v kateri je avtor predlagal souporabo komunikacijskih poti za prenos obračunskih in obratovalnih podatkov ter uvedbo Etherneta v TP SN/NN.

Vsebina dela je razdeljena na poglavja. Uvodnemu poglavju sledi poglavje, v katerem je podana definicija aktivnega omrežja in ključni izzivi nadaljnjega razvoja elektroenergetskih omrežij. V tretjem poglavju je opredeljena vsebina in pomen obratovalnih meritev v omrežju za distribucijo električne energije. Rezultati obratovalnih meritev so nepogrešljivi pri načrtovanju distribucijskega omrežja, pri sprotnem spremljanju obratovanja in vzdrževanja omrežja in nenazadnje tudi pri kontroli odjema električne energije. Predstavljeni so sistemi, ki zajemajo merilne vrednosti v TP SN/NN, sistemi za nadzor in vodenje RTP VN/SN ter sistemi za nadzor kakovosti EE.

Četrto poglavje obravnava obračunske meritve električne energije; razvoj sistemov avtomatskega merjena (AMR, AMM, AMI), arhitekturo sistema AMI in evropsko prakso na tem področju. Peto poglavje poglobljeno obravnava problematiko upravljanja porabe EE pri odjemalcih (Demand Side Management – DSM). DSM je obravnavan z vidika vseh ključnih akterjev, podane so tudi ugotovitve, zakaj je DSM v Sloveniji ena od številnih neizkoriščenih priložnosti za dosego učinkovitejše rabe energije in optimalnejšega razvoja EE sistema. Posebna pozornost je namenjena potrebni informacijsko-komunikacijski infrastrukturi za izvajanje programov DSM.

Šesto poglavje govori o informacijsko-komunikacijskih sistemih v distribuciji EE danes in pojasnjuje, kakšne bodo zahteve za informacijsko-komunikacijski sistem v prihodnje. Predstavljen je koncept sodobnega informacijsko-komunikacijskega sistema, ki mora temeljiti na paketnem prenosu podatkov in uporabo sodobnih komunikacijskih standardov, kot je IEC 61850, ter na poenotenju podatkovnih struktur (CIM – Common Information Model). Sedmo poglavje predstavlja tehnologije TK omrežij, ki so glede na stanje tehnike lahko temelj bodočemu razvoju informacijsko-komunikacijski sistemov. To so optična omrežja, analogne in digitalne radijske zveze, komercialna brezžična omrežja (GPRS/UMTS), novejše brezžične tehnologije (WiMax, WiFi), opredeljene so tudi njihove prednosti in slabosti ter uporabnost z vidika potrebne kapacitete komunikacijskega kanala.

Osmo poglavje je posvečeno varnosti informacijsko-komunikacijskega sistema: kaj je varnost informacijsko-komunikacijskih sistemov, kaj jo ogroža, kakšna je ranljivost sistemov. Predstavljeni so gradniki zaščite komunikacijskih sistemov, še posebej je poudarjena vloga avtentikacije. Na osnovi zahtev za bodoči informacijsko-komunikacijski sistem, razpoložljivih komunikacijskih tehnologij in potrebe po zagotovitvi varnosti je v devetem poglavju predstavljeno načrtovanje varnega informacijsko-komunikacijskega sistema.

V desetem, sklepnem poglavju so povzete temeljne ugotovitve dela: stanje tehnike na področju informacijsko-komunikacijskih sistemov v distribuciji EE danes, bodoče potrebe

aktivnih omrežij, ki bodo temeljile na sodobnih informacijsko-komunikacijskih sistemih. in rešitve, kako zagotoviti varno evolucijo obstoječih sistemov na bolj prožne, standardizirane in varne informacijsko-komunikacijske sisteme.

1.3 Kratka predstavitev distribucijskega omrežja Elektra Gorenjska, d.d.

Elektro Gorenjska, d.d. (EG) je lastnik in pogodbeni izvajalec dejavnosti sistemskega operaterja distribucijskega omrežja (SODO), ki se nahaja v SZ delu Slovenije. EG je eno od petih podjetij, ki v Sloveniji izvajajo distribucijo električne energije. EG pokriva približno 10 % državnega ozemlja in distribuira 10% EE končnim odjemalcem.

Slika 1.1 Območje Elektra Gorenjska, d.d.

1.3.1 Osnovni podatki o distribucijskem omrežju EG

Elektro Gorenjska sestavljajo poleg sedeža družbe v Kranju še obrat v Žirovnici in osem krajevnih nadzorništev (KN Bohinj, KN Cerklje – Visoko, KN Jesenice-Kranjska Gora, KN Kranj, KN Radovljica – Bled, KN Škofja Loka – Medvode, KN Tržič ni KN Železniki.

Slika 1.2 Krajevna nadzorništva EG

Osnovni podatki o distribucijskem območju in tehnični podatki o napravah s stanjem na dan 1. 1. 2010 so v Tabeli 1.1.

Tabela 1.1: Osnovni podatki o distribucijskem območju in napravah EG

Površina preskrbovalnega območja	**2.091 km2**
Število uporabnikov	**86.128**
Daljnovodi 110 kV	115.029 m
Daljnovodi 35 kV	53.851 m
Daljnovodi 20 kV	796.412 m
Daljnovodi 10 kV	10.064 m
SN daljnovodi skupaj	**975,359 m**
Kablovodi 110 kV	1.301 m
Kablovodi 35 kV	2.780 m
Kablovodi 20 kV	721.319 m
Kablovodi 10 kV	23.624 m
SN kablovodi skupaj	**749.024 m**
NN omrežje skupaj	**3.703.167 m**
OMREŽJE SKUPAJ	**5.427.550 m**
RTP	**15**
RP	**6**
TP	**1.491**

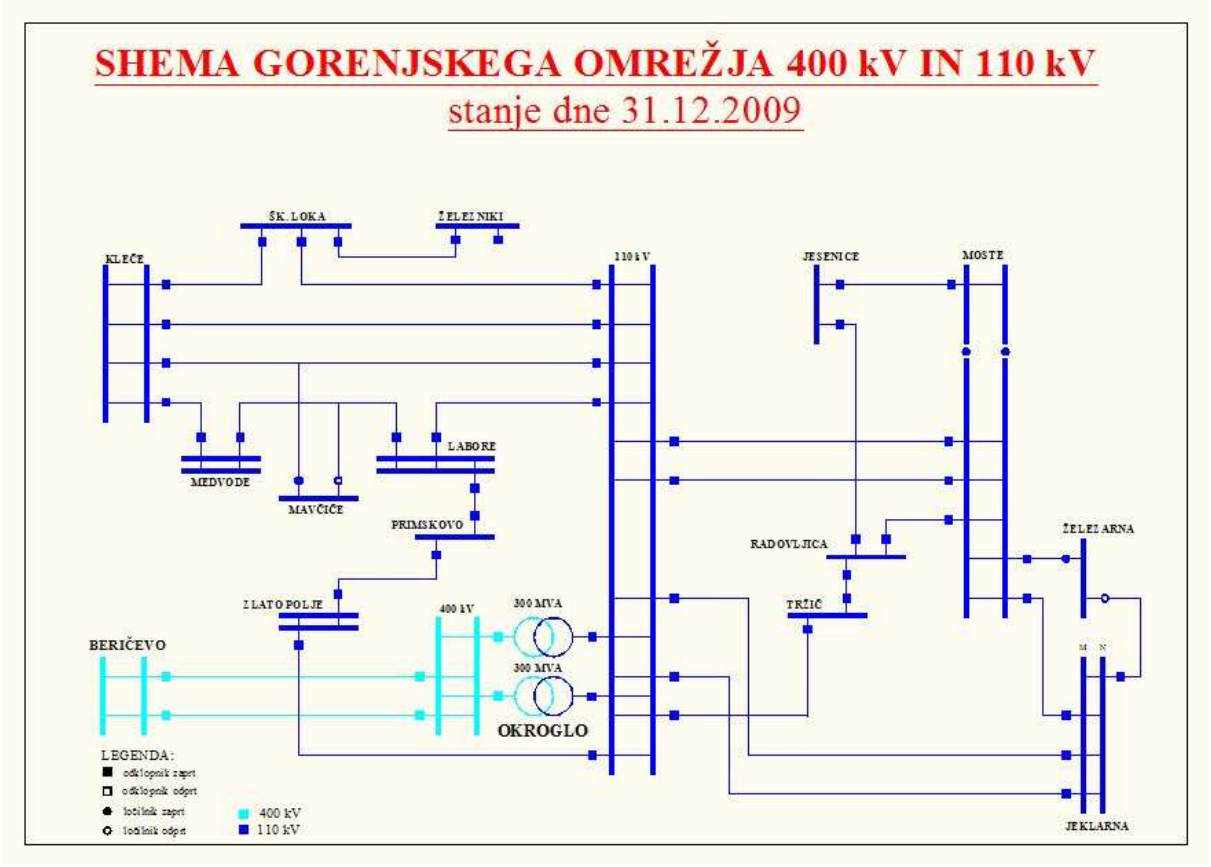
EG je konec leta 2006 s prehodom mesta Kranj zaključila prehod na 20 kV napetostni nivo. Ostanki 10 kV napetostnega nivoja so prisotni le še na manjšem številu lokacij (planinske koče, manjša smučišča). Napajanje je izvedeno s transformacijo 20kV/10kV ali 20kV/0.4kV/10kV. Ukinjanje 35 kV napetostnega nivoja bo na Gorenjskem zaključeno po izgradnji nove RTP Moste, predvidoma konec leta 2010.

EG je zaradi cenovne sprejemljivosti in nižjih obratovalnih stroškov že leta 2003 sprejela odločitev za intenzivnejšo gradnjo kabelskih NN in SN omrežij. Od leta 2003 se tako zmanjšuje obseg prostozračnega omrežja in povečuje obseg kabelskega omrežja.

Na območju EG je preko 130 kvalificiranih proizvajalcev EE. Po številu še prevladujejo HE, v zadnjem času pa se močno povečuje število fotovoltaičnih elektrarn [1].

1.3.2 Povezave distribucijskega omrežja EG s prenosnim omrežjem

Distribucijsko omrežje EG je s prenosnim omrežjem povezano preko RTP 400/110 kV Okroglo. V RTP Okroglo se nahajata dva transformatorja 400/110 kV moči 300 MVA. RTP Okroglo je povezano z daljnovodom 400 kV v RTP Beričevo, v RTP Kleče pa s 110 kV daljnovodi. Poleg EG je odjemalec na 110 kV nivoju še Železarna Jesenice. Večje proizvodne enote (HE Moste, HE Mavčiče, HE Medvode) so preko transformacije (v bližnjih RTP) priključene na 110 kV napetostni nivo.



Slika 1.3 Gorenjsko 400 kV in 110 kV omrežje

1.4 Sistemski operater distribucijskega omrežja (SODO)

Naloge sistemskega operaterja distribucijskega omrežja (DSO – Distribution system operator) v Sloveniji izvaja Družba SODO d.o.o., ki jo je ustanovila vlada RS z Aktom o

ustanovitvi družbe SODO (Ur.l. RS, št. 27/07) na podlagi 23. člena Energetskega zakona (Ur.l. RS, št. 27/07 – uradno prečiščeno besedilo, 70/08). Licenco za opravljanje energetske dejavnosti SODO je izdala Javna agencija Republike Slovenije za energijo po 6. členu Energetskega zakona, pod številko 0686-08-015/002/07, z dne 8. 6. 2007. Družbi SODO d.o.o. je Vlada RS s sklepom št. 36001-4/2007/5, z dne 14. 06. 2007 podelila koncesijo za obdobje 50 let od datuma sklenitve koncesijske pogodbe (Uredba o koncesiji gospodarske javne službe dejavnosti sistemskega operaterja distribucijskega omrežja električne energije - Ur.l. RS, št. 39/2007, z dne 4. 5. 2007). Po podpisu koncesijske pogodbe so bile podpisane pogodbe o najemu elektroenergetske infrastrukture in izvajanju storitev za sistemskega operaterja distribucijskega omrežja električne energije med družbo SODO d.o.o. in posameznimi distribucijskimi podjetji: Elektro Celje d.d., Elektro Gorenjska d.d., Elektro Ljubljana d.d., Elektro Maribor d.d., Elektro Primorska d.d. in z nekaterimi zaokroženimi gospodarskimi kompleksi [2].

Vlada Republike Slovenje je 15. marca 2007 ustanovila družbo SODO d.o.o. in ji podelila koncesijo za izvajanje dejavnosti sistemskega operaterja distribucijskega omrežja. SODO d.o.o. je s petimi distribucijskimi podjetji sklenil pogodbe o najemu infrastrukture in izvajanju storitev za SODO.

1.4.1 Temeljne naloge SODO

Po pogodbi o najemu infrastrukture in izvajanju storitev za SODO, Elektro Gorenjska kot lastnik in izvajalec storitev na svojem distribucijskem območju zagotavlja:

- varnost obratovanja,
- zanesljivost distribucije električne energije,
- zagotavljanje dostopa do distribucijskega omrežja in storitev pod splošnimi pogoji vsakomur,
- redno in trajno obratovanje,
- zagotavljanje predpisane kvalitete (neprekinjenost, kakovost napetosti, komercialna kakovost),
- varovanje okolja, kar vključuje skrb za energetsko učinkovitost in ohranjanja podnebnih razmer.

Lastnik distribucijskega omrežja je po pogodbi odgovoren za:

- izvajanje distribucije električne energije,

- vzdrževanje in razvoj omrežja za distribucijo električne energije,
- upravljanje, vodenje in obratovanje distribucijskega omrežja,
- zagotavljanje dolgoročne zmogljivosti omrežja, da omogoča razumne zahteve za priključitev in dostop do omrežja,
- upravljanje pretokov električne energije po distribucijskem omrežju, upoštevaje tudi izmenjave energije z ostalimi povezanimi omrežji ter zagotavljanje sistemskih storitev,
- varno in zanesljivo obratovanje distribucijskega omrežja,
- izvajanje optimalnega ponovnega vzpostavljanja sistema po motnjah,
- izvajanja sistemske zaščite distribucijskega omrežja,
- izvajanje števčnih in obratovalnih meritev v distribucijskem omrežju,
- izvajanje meritev in analiz na področju kakovosti oskrbe z električno energijo,
- oblikovanje obratovalne statistike,
- nediskriminatorno obravnavanje uporabnikov omrežja,
- zagotavljanje potrebnih podatkov odjemalcem, da lahko učinkovito uveljavljajo dostop do omrežja,
- napoved porabe električne energije ter potrebnih energetskih virov z uporabo metode celovitega načrtovanja in upoštevanja varčevalnih ukrepov pri porabnikih,
- izvajanje sistemskih obratovalnih navodil,
- vsaki dve leti sodelovati pri pripravi načrta razvoja distribucijskega omrežja za najmanj 10 let, pri čemer mora upoštevati načela kakovosti in zanesljivosti oskrbe ter ekonomičnosti izgradnje, vzdrževanja ter obratovanja omrežja, pri čemer mora tehnične in tehnološke rešitve izvajanja in vzdrževanja tipizirati skladno z veljavnimi predpisi,
- organizacijo stalne službe, ki mora razpolagati z ustreznim številom usposobljenih ljudi in z opremo za takojšnje posege v zvezi z odpravljanjem poškodb in okvar na distribucijskem omrežju ter na priključkih uporabnikov omrežja ali na drug način zagotoviti izvajanje te službe [1].

2 AKTIVNA OMREŽJA (SMART GRIDS) V DISTRIBUCIJI EE

V zadnjih letih se v povezavi s prihodnjim razvojem elektroenergetike vedno pogosteje omenjajo t.i. »pametna omrežja« (Smart Grids) pri čemer se zdi izraz aktivna omrežja primernejši. Informacijsko-komunikacijske tehnologije se pospešeno uveljavljajo pri vodenju in nadzoru elektroenergetskega sistema (EES). EES postaja vedno bolj kompleksen, z množičnim pojavljanjem razpršene proizvodnje pa tudi vedno težje obvladljiv. Aktivna omrežja naj bi bila pravi odgovor na izzive prihodnjega razvoja EES, poraja pa se vprašanje, kaj naj bi sploh bila aktivna omrežja. Enotnega odgovora na to vprašanje ni, pogosto se zatakne že pri sami definiciji. Žal se v strokovni, še bolj pa v laični javnosti pojavljajo poenostavitve z enačenjem »pametnih števcev« (sistemi AMR, AMM, AMI) in aktivnih (»pametnih«) omrežij. Sistemi daljinskega odčitavanja s pripadajočo informacijsko-komunikacijsko infrastrukturo so samo del mnogo bolj kompleksnega sistema.

2.1 Definicija aktivnega omrežja

Kot izhodišče za nadaljnja razmišljanja bo dobro služila definicija aktivnega omrežja, ki je nastala maja 2009 pod okriljem združenja Eurelectric[5]:

»Aktivno omrežje je elektroenergetsko omrežje, ki je zmožno aktivne povezljivosti obnašanja in odzivnosti vseh uporabnikov omrežja: proizvajalcev EE, odjemalcev EE in tistih, ki so istočasno proizvajalci in odjemalci, s ciljem, da na učinkovit način zagotovi trajnostno, ekonomsko učinkovito in zanesljivo dobavo električne energije. » [3]

Definicija dovolj dobro povzema iskanje optimalne rešitve ključnih izzivov, ki jo razvoj elektroenergetike nalaga operaterjem distribucijskih ter prenosnih omrežij v Evropi in svetu.

2.2 Vloga elektroenergetskih omrežij prihodnosti

Učinkoviti prenosni in distribucijski sistemi so predpogoj za zagotavljanje najpomembnejšega vira energije državljanom in podjetjem v EU, ki se soočajo z izzivi 21.

[5] Eurelectric – Union of the Electricity Industry je interesno združenje, ki zastopa interese evropskega elektrogospodarstva. Njeni člani so podjetja in gospodarska združenja držav širšega evropskega prostora. Ustanovljeno je bilo leta 1989 s sedežem v Bruslju. Avtor je bil leta 2008 imenovan za namestnika slovenskega predstavnika v delovni skupini za aktivna omrežja (WG SmartGrids – Network of the Future).

stoletja. Potreba po ojačitvi evropskih elektroenergetskih omrežij, povečevanje porabe električne energije, potreba po racionalizaciji porabe, odpiranje trga z električno energijo in priključevanje velikega števila novih (razpršenih) proizvodnih virov električne energije spreminjajo koncept elektroenergetskih omrežij, kot smo ga poznali do sedaj.

Ključni izziv za operaterje elektroenergetskih omrežji bo usklajevanje razpršene proizvodnje električne energije z odjemom električne energije na način, da bo ob optimalnem investiranju v omrežje in razumnih stroških vzdrževanja zagotovljena zanesljiva in kakovostna oskrba vseh odjemalcev električne energije. Neizbežna je nadaljnja informatizacija elektroenergetskih omrežij. Usklajevanje (razpršene) proizvodnje električne energije in (lokalne) porabe vse bolj zahtevnih odjemalcev in naprav zahteva napredno informacijsko-komunikacijsko infrastrukturo.

2.3 Izvajanje nalog operaterjev EE omrežij z vidika aktivnih omrežij

Spreminjajoči koncept elektroenergetskih omrežij predvideva večjo avtomatizacijo omrežja. Nadaljnja avtomatizacija je pogojena z informacijsko-komunikacijskim sistemom (IKS), ki bo zagotavljal:

- merjenje ključnih obratovalnih parametrov omrežja in daljinsko vodenje omrežja,
- merjenje obračunskih parametrov električne energije in tudi drugih energentov,
- upravljanje porabe električne energije z usklajevanjem lokalne proizvodnje in odjema,
- dodatne storitve uporabnikom in upravljavcem omrežja s katerimi bo mogoče na učinkovit način zagotavljati trajnostno, ekonomsko učinkovito in zanesljivo dobavo električne energije odjemalcem.

V naslednjih poglavjih so zato predstavljene zahteve za informacijsko-komunikacijski sistem z vidika:

- obratovalnih meritev v distribuciji EE (poglavje 3),
- obračunskih meritev EE in drugih energentov (poglavje 4) in
- upravljanja porabe EE pri odjemalcih (poglavje 5).

2.4 Evropska praksa uvajanja aktivnih omrežij

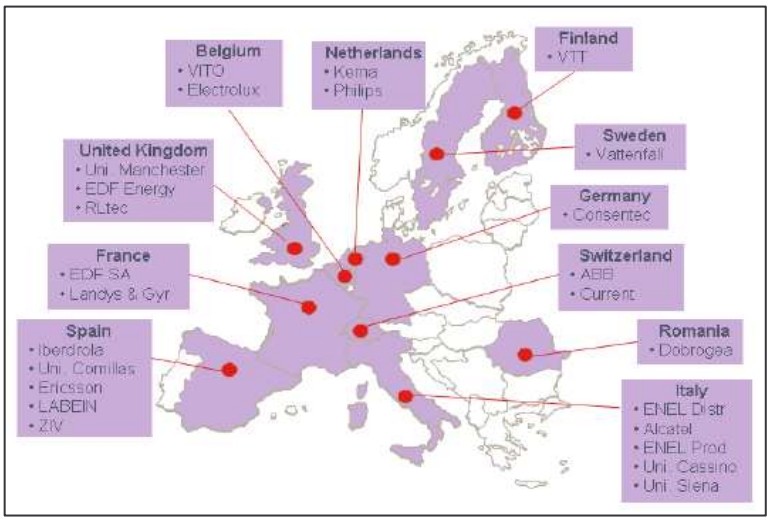
V Evropi še ni izoblikovanega enotnega koncepta aktivnega omrežja za distribucijo električne energije. V izvajanju je precej pilotnih projektov, s katerimi želijo posamezne države oz. operaterji preizkusiti tehnološke rešitve in pridobiti potrebne izkušnje za izvedbo tehnološke (r)evolucije na področju informacijsko-komunikacijskih sistemov v elektroenergetskem sektorju. V nadaljevanju je navedenih nekaj zanimivih projektov, ki so trenutno v izvajanju [4].

Italijanski sistemski operater Enel je v Evropi med uspešnejšimi pri uvajanju informacijsko-komunikacijskih rešitev. V letu 2008 je 5300 intervencijskih vozil opremil s terminali za vodenje ekip na terenu preko centra vodenja, postavil je več kot 400 testnih polnilnih točk za električna vozila. Enel naj bi:

- do leta 2011 vse odjemalce opremil z AMM števci,
- do leta 2012 naj bi bilo 32 % SN/NN postaj daljinsko vodenih,
- do leta 2012 naj bi bilo SN omrežje avtomatizirano.

Poleg tega Enel veliko pozornost namenja uvajanju novih tehnologij v VN/SN postaje (nove zaščite, novi protokoli, lokalna avtomatika), pa tudi v SN/NN postaje (detektorji okvar, zunanji napetostni in tokovni senzorji, nova zaščita za razpršene vire), uvajanju novih komunikacijskih poti in aktivni vlogi odjemalcev in malih proizvajalcev.

Enel je koordinator projekta »ADDRESS« (Active Distribution network with full integration of Demand and distributed energy RESourceS).



Slika 2.1 Sodelujoči v projektu »ADDRESS«

Leta 2008 začet projekt bo trajal 4 leta, v projekt je vključenih 25 partnerjev iz 11 EU držav, na voljo je 16 milijonov EUR sredstev, od tega EU prispeva 9 milijonov EUR. Cilji projekta so:

- razviti tehnične rešitve pri uporabnikih in na omrežju,
- preučiti morebitne ovire pri upravljanju odjema ter predlagati rešitve,
- ugotoviti koristi za vse udeležence,
- razviti primeren trg in pogodbene mehanizme,
- preveriti predlagane rešitve na treh področjih, z različnimi geografskimi, demografskimi in infrastrukturnimi značilnostmi.

Na Portugalskem izvajajo projekt »INNOVGRID«. Poudarki projekta so: pametno merjenje in DSM, problematika vključevanja mikro in razpršene proizvodnje električne energije ter aktivna omrežja. Zagotovljenih je približno 100 milijonov EUR sredstev. Ciljna skupina je 600.000 odjemalcev (10 % portugalskih odjemalcev). V okviru projekta bo zgrajenega 6.000 km optičnega omrežja. Vgrajenih bo 25.000 AMI števcev z naslednjimi lastnostmi: 4 kvadrantno merjenje, profil obremenitve, opcija več tarif, daljinski vklop/izklop, nastavitev meje obremenitve, brezžični vmesnik za komunikacijo z napravami odjemalca, mehanizem pred goljufijami, registracija kakovosti energije in dogodkov, sistemska nadgradnja in komunikacija med števcem ter posameznimi porabniki (Home Area Network). V TP SN/NN bo vgrajenih 15.000 kontrolnih naprav z naslednjimi lastnostmi: 4 kvadrantno merjenje, profil obremenitve, kontrola javne razsvetljave, nadzor nesimetrije obremenitve, nadzor transformatorja, detekcija okvar, upravljanje odklopnikov, nadzor kakovosti, alarmi, komunikacije, koncentracija podatkov in sistemska nadgradnja.

Finska načrtuje do konca leta 2013 80 % odjemnih mest opremiti z merilnimi sistemi za zajem urnih vrednosti, največ 20 % merilnih mest lahko ostane odčitanih trikrat letno. Finske zahteve za pametne števce so naslednje:

- daljinsko odčitavanje,
- registracija prekinitev daljših od treh minut,
- upravljanje porabe,
- shranjevanje podatkov (6 let za meritve, 2 leti za prekinitve),
- zaščita podatkov.

Tudi ***v Avstriji*** poteka več projektov uvajanja naprednih informacijsko-komunikacijskih rešitev v distribuciji EE. Tako so v deželi Zg. Avstrija (440.000 odjemalcev) v letu 2009 zamenjali 100.000 števcev, do leta 2014 pa načrtujejo razširitev daljinskega merjenja in upravljanja odjemalcev na vse odjemalce. Regulator energetskega trga v Avstriji zahteva izvajanje ukrepov za izboljšanje energetske učinkovitosti, mesečno odčitavanje števcev in izvajanje ukrepov DSM. Država spodbuja raziskovalno delo na področju aktivnih omrežij. Ustanovljen je bil konzorcij raziskovalnih in univerzitetnih centrov, industrije in operaterjev distribucijskega omrežja, delu konzorcija pa bo v petih letih namenjenih 150 milijonov EUR.

Švedska si je zadala ambiciozne cilje na področju izboljšanja zanesljivosti in neprekinjenosti napajanja in daljinskega odčitavanja porabe električne energije. Tako predvidevajo največ 24 ur izpadov na leto na odjemalca, 5,3 milijonov števcev z mesečnimi meritvami (14 milijonov vseh odjemalcev), 80 % števcev z dvosmerno komunikacijo, 60% s podporo DSM programom, v dveh letih bo zgrajenih 500 polnilnic za električna vozila. Nova švedska zakonodaja zahteva za najmanj 80 % vseh odjemalcev urno merjenje EE do konca leta 2013.

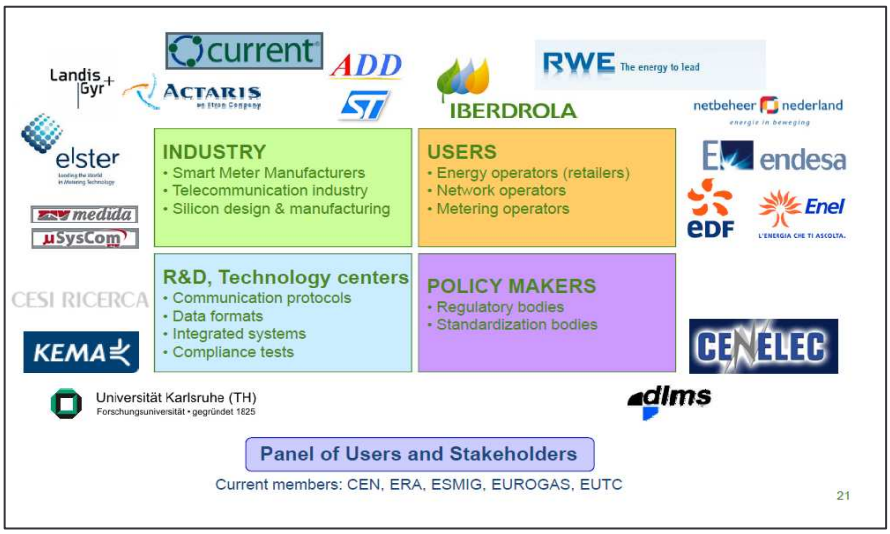
En milijon odjemalcev že ima daljinski dostop do stanja števca, odjemalec ima pravico zahtevati vmesnik za branje stanja števca oz. upravljanje porabnikov. V teku je več nacionalnih projektov s področja aktivnih omrežij: študije izvedljivosti, testni poligoni za električna vozila, baterije, fotonapetostne elektrarne …

Tudi ***v Španiji*** je v izvajanju nekaj zanimivih projektov, npr:

- PRIME - Powerline-Related Intelligent Metering Evolution,
- OPEN METER - Open and Public Extended Network metering infrastructure,
- GAD - Active Demand Management.

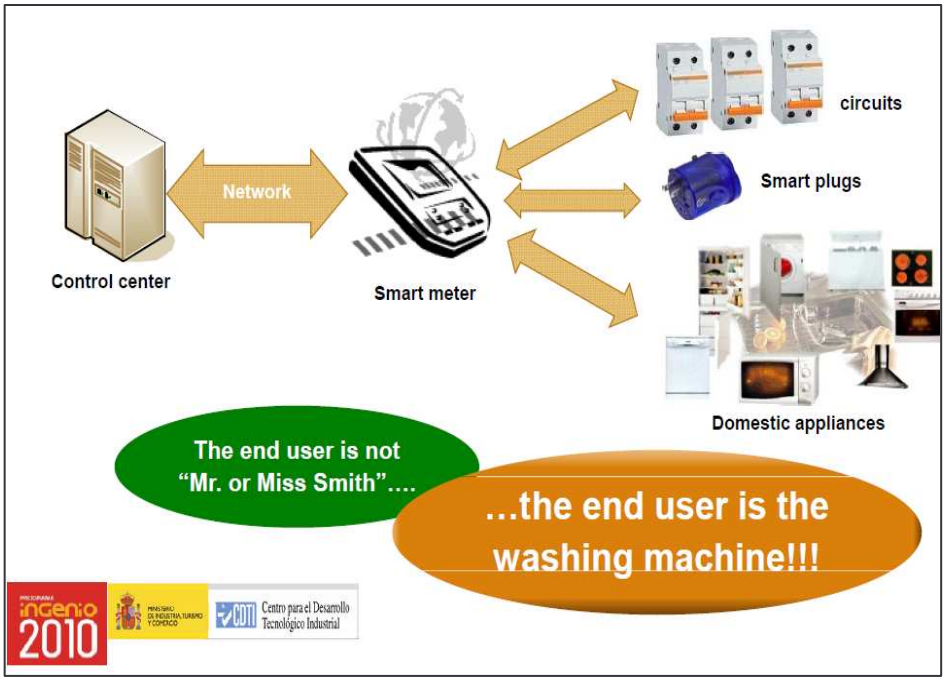
Projekt PRIME (2007–2009) predvideva vzpostavitev odprtega javnega TK standarda na osnovi PLC, ki bi bil namenjena TK infrastrukturi za AMI sisteme. V okviru projekta se poskuša poenotiti komunikacijsko opremo različnih ponudnikov.

Tudi **projekt OPEN METER** želi prispevati k vzpostavitvi IKT infrastrukture za AMI sisteme. V projekt je vključenih veliko podjetij in institucij s področja razvoja in uporabe AMI in IKT sistemov. Predstavitveni panel projekta je na Sliki 2.2.



Slika 2.2 Projektna skupina in temeljni cilji projekta OPEN METER

Projekt GAD je namenjen proučevanju aktivnega upravljanja porabe pri odjemalcih. V okviru projekta se praktično preizkuša komunikacijske povezave med posameznimi porabniki v gospodinjstvu in AMI števcem ter sistem upravljanja posameznih bremen iz nadzornega centra (Slika 2.3) [4].



Slika 2.3 Projekt GAD - aktivno upravljanje bremen v gospodinjstvih

3 OBRATOVALNE MERITVE, NADZOR IN VODENJE DISTRIBUCIJSKEGA OMREŽJA

3.1 Opredelitev in pomen obratovalnih meritev

Temeljna naloga distributerja električne energije je zagotavljanje zanesljive in kakovostne dobave električne energije vsem uporabnikom omrežja. Za izvajanje te naloge so ključnega pomena obratovalne meritve: meritve trenutnih vrednosti tokov in napetosti v vseh treh fazah, meritev trenutnih vrednosti delovne in jalove moči ter koničnih (največjih doseženih) vrednosti merjenih veličin, parametri kakovosti napetosti … Sistem za zagotavljanje teh podatkov v realnem času je zahteven in kompleksen. Distribucijska podjetja ga izgrajujejo postopoma. Obstoječi informacijski sistem obratovalnih meritev Elektra Gorenjska, d.d., omogoča zajem podatkov do nivoja SN izvoda iz razdelilno transformatorske postaje (RTP). Merilniki obratovalnih meritev v RTP so preko komunikacijskih računalnikov povezani z distribucijskim centrom vodenja (DCV). Sistem za nadzor, vodenje in zajem podatkov (SCADA) v DCV med drugim zagotavlja daljinsko vodenje in nadzor RTP ter prikaz in arhiviranje merilnih podatkov.

Za razširitev informacijskega sistema obratovalnih meritev do nivoja TP SN/NN bi bilo potrebno vgraditi merilnike obratovalnih meritev v vse TP SN/NN in zagotoviti avtomatski prenos podatkov do merilnega centra obratovalnih meritev. Na področju Elektra Gorenjska je več kot 1400 TP.

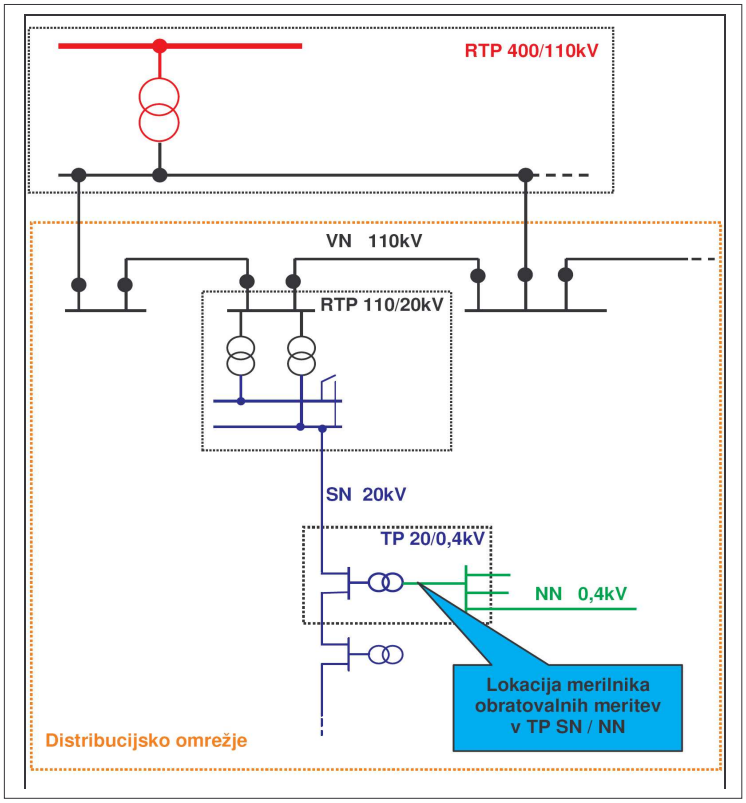
Vsekakor je najpomembnejše dejstvo, da se z razširitvijo informacijskega sistema obratovalnih meritev do nivoja TP SN/NN omogoči nadzor nad obratovanjem celotnega SN omrežja v realnem času. S tem se občutno skrajša potreben čas za ugotavljanje vzroka in mesta okvare na omrežju in možnost natančnejšega informiranja in vodenja dežurnih ekip na terenu.

Rezultati obratovalnih meritev so nepogrešljivi pri načrtovanju distribucijskega omrežja, saj so osnova za izračun pretokov moči, koničnih obremenitev, zasedenosti transformacije, tehničnih izgub itd. Na podlagi teh in drugih parametrov se odloča o potrebi in načinu ojačitve omrežja ali transformacije na določenem napajalnem območju [5].

TP so mejne točke med SN omrežjem in NN napajalnim območjem TP. Na NN omrežje so priključena gospodinjstva in drugi manjši odjemalci. Za distributerja EE je vsekakor zanimiva razlika med EE, ki jo TP oddaja v NN omrežje in vsoto porabe vseh odjemalcev na NN

omrežju. Razliko predstavljajo tehnične izgube na NN omrežju in eventualni nekontrolirani odjem (kraja).

V Elektru Gorenjska je vzpostavljen sistem permanentnega monitoringa kakovosti napetosti po standardu SIST EN 50160 na nivoju RTP [6]. Zanesljivost dobave EE se mora izračunavati za vsakega odjemalca posebej. Število in trajanje izpadov izvodov iz RTP registrira DCV in podatke za nadaljnje analize shrani v historični zbirki podatkov. Podatki o izpadu TP oziroma izvoda iz TP pa se vnašajo ročno na podlagi podatkov, ki jih DCV posredujejo dežurne ekipe na terenu. Z vzpostavitvijo informacijskega sistema obratovalnih meritev na nivoju TP ročni vnos podatkov ne bo več potreben.



Slika 3.1: Distribucijsko omrežje in lokacija merilnika obratovalnih meritev v TP SN/NN

3.2 Pomen obratovalnih meritev za izvajanje nalog operativnih služb

Prvi korak na poti do celovitega obvladovanja obratovalnih meritev je ugotoviti njihovo uporabno vrednost. Komu so obratovalne meritve potrebne? Kako morajo biti podatki pripravljeni, da jih je najenostavneje uporabiti? V naslednjih podpoglavjih je predstavljena uporaba obratovalnih meritev za potrebe razvoja distribucijskega omrežja, obratovanja in vzdrževanja, kontrole odjema EE in spremljanja kakovosti EE.

3.2.1 Razvoj distribucijskega omrežja

Pri načrtovanju razvoja distribucijskih omrežij z analizami zajamemo 110 kV napajalno omrežje, ki predstavlja primarno distribucijsko omrežje, transformacijo 110 kV/SN in SN omrežje. Zaradi močne razvejanosti SN omrežja združujemo transformatorske postaje SN/NN v vozlišča (cone) ob glavnih vodih, vendar tako, da ohranimo obratovalne značilnosti razvejanega omrežja.

V prvi fazi načrtovanja razvoja z analizami obratovalnih stanj preverjamo, ali omrežje in transformacija, ob napovedani rasti obremenitev, še izpolnjujeta kriterije načrtovanja. Ključni omejitvi v tej fazi predstavljajo dopustni padci napetosti in dopustne obremenitve elementov omrežja. Preverjanja za pričakovane letne konične obremenitve se opravijo v časovnih intervalih, ki se prilagajajo stopnji rasti obremenitev in odmaknjenosti v prihodnost. Običajno so bližnji intervali petletni, zadnji pa desetletni. V vsakem obdobju se preverja stanja normalnega obratovanja in stanja ob enojnih izpadih.

Pri dvosistemskih vodih obravnavamo izpad obeh sistemov kot enojni izpad. Preverjajo se vsa možna stanja z enojnimi izpadi, s tem da se za manjše skupine porabnikov dopušča, da nimajo možnosti rezervnega napajanja.

Ko v omrežju prekoračimo dopustne obremenitve ali padce napetosti, se odločimo za ojačitev. Časi ojačitev, dobljeni s takšno analizo, predstavljajo skrajne roke, ki ne smejo biti prekoračeni.

V drugi fazi načrtovanja s tehtanjem tehničnih, ekonomskih kriterijev in kriterijev zanesljivosti opredelimo optimalno varianto razvoja. Skrajne roke ojačitev, ki smo jih določili v prvi fazi, lahko v fazi optimizacije natančneje opredelimo. Objekt lahko zgradimo pred skrajnim rokom zaradi zmanjšanja stroškov izgub in/ali zaradi izboljšanja zanesljivosti napajanja porabnikov. V tej fazi lahko utemeljimo še kakšen dodaten objekt, ki pa mora biti v skladu s smerjo razvoja, določeno v prvi fazi.

Osnovni podatki pri načrtovanju razvoja omrežij so predvsem podatki o porabljeni električni energiji, podatki o obremenitvah po posameznih območjih, podatki o dogodkih v minulem obdobju in kakovost oskrbe odjemalcev.

Pomembno vlogo pri širitvi in oblikovanju omrežja predstavljajo investicijske dejavnosti na nivoju države, posameznih občin kakor tudi gospodarskih subjektov. Take dejavnosti se odražajo preko realizacije različnih prostorskih dokumentov (LN, ZN, PUP...), pri katerih je aktivno sodelovanje elektrodistribucije zelo pomembno [7].

3.2.2 Obratovanje in vzdrževanje distribucijskega omrežja

DCV predstavlja osrednje informacijsko vozlišče pri zagotavljanju nemotenega procesa distribucije električne energije. Osnovne funkcije vodenja obratovanja distribucijskega omrežja so realizirane s SCADA programsko opremo, ki omogoča zajemanje podatkov, izdajanje komand, kreiranje poročil in arhiviranje podatkov.

Novejši DCV, med katere sodi tudi v letu 2006 zgrajeni DCV Elektra Gorenjska, vključuje tudi dodatne, t.i. DMS[6] funkcije. Med temi so najpomembnejše dodatne funkcije za pomoč dispečerjem in ekipam na terenu pri odkrivanju in odpravljanju napak na omrežju in pri rednih vzdrževalnih delih, za avtomatsko izolacijo okvar na omrežju, za analizo pretokov moči, padcev napetosti, kratkostičnih tokov in moči, za napoved obremenitve, za izračun statistike dogodkov, izračun kazalcev kakovosti, funkcionalnosti klicnega centra, trening simulator itd.

SCADA zajema podatke, ki jih posredujejo postajni računalniki v RTP. Trenutne vrednosti analognih meritev, števčnih stanj, položajev stikalnih elementov itd. se zajemajo periodično. Periode zajemanja podatkov se nastavijo za vsak postajni računalnik posebej. Vhodni podatki so tudi dogodki (alarmi), ki so opremljeni s točnim časom nastanka.

DCV v tem trenutku ne razpolaga z informacijami o stanju in dogodkih na omrežju na nivoju TP. Ugotavljanje dejanskega stanja je tako prepuščeno dežurnemu osebju na terenu. Z razširitvijo zajema obratovalnih meritev in dogodkov (alarmov) na nivoju TP bi dosegli naslednje pomembne cilje:

- bistveno skrajšanje časa za ugotavljanje vzroka in mesta okvare na omrežju,
- možnost natančnejšega informiranja in vodenja dežurnih ekip na terenu,
- natančnejša statistika dogodkov in natančnejši izračun kazalcev kakovosti,
- boljšo podporo delovanju klicnega centra.

3.2.3 Kontrola odjema električne energije

TP so mejne točke med SN omrežjem in NN napajalnim območjem TP. Na NN omrežje so priključena gospodinjstva in drugi manjši odjemalci (tarifni odjemalci in manjši upravičeni odjemalci). Za distributerja EE je vsekakor zanimiva razlika med EE, ki jo TP oddaja v NN omrežje in vsoto porabe vseh odjemalcev na NN omrežju. Razliko predstavljajo tehnične

[6] Distribution Management System – sistem za vodenje distribucijskega omrežja

izgube na NN omrežju in eventualni nekontrolirani odjem (kraja). Pogoji za uporabo obratovalnih meritev za kontrolo odjema EE so:

- vzpostavljen sistem avtomatskega odčitavanja števcev tarifnih odjemalcev (AMI),
- ustrezen razred točnosti merilnih naprav,
- enaki merilni metodi AMI in sistema obratovalnih meritev (15-minutna povprečja),
- časovna sinhronizacija merilnih naprav.

AMI sistemi in njihovo uvajanje v slovenski distribuciji je predstavljeno v 4. poglavju. Merilni center za zajem obratovalnih meritev (MI 7150, sodobnejši izvedbi MC 760 in MC 750 predstavljeni v poglavju 3.3.1) in sistemski števci AMI (poglavje 4.3.2.) imajo ustrezen razred točnosti. Časovno sinhronizacijo AMI sistema in informacijskega sistema obratovalnih meritev morata zagotoviti nadrejena merilna centra z enim od uveljavljenih virov točnega časa, npr. DCF-77 [7], GPS[8] ali z uporabo protokola NTP[9].

3.3 Sistemi za zajem merilnih vrednosti v TP SN/NN

V preteklosti se je na nivoju TP za potrebe obratovalnih meritev vgrajevalo večje število analognih merilnih naprav. Običajno so se TP opremljale s kazalnim V-metrom in A-metri s kazalniki maksimuma v vseh treh fazah na sekundarni strani TP. Ponekod so se vgrajevali tudi merilniki delovne in jalove moči oziroma števci delovne in jalove energije (s kazalniki maksimuma).

Ob gradnji novih ali obnovi starih TP se vgrajujejo izključno sodobni merilniki, ki so zasnovani na mikroračunalniški osnovi. S takimi merilniki je opremljenih približno 25 % TP na območju Elektra Gorenjska. Najbolj je razširjen merilnik MI 7150 proizvajalca Iskra MIS. V zadnjem času ga zamenjujeta naprednejši model MC 750 in analizator omrežja MC 760, ki sta predstavljena v nadaljevanju.

---

[7] DCF-77 je sinonim za radijski signal z informacijo o točnem času, ki temelji na cezijevi časovni normali. Oddajnik v bližini Frankfurta oddaja signal na frekvenci 77,5 kHz.

[8] Tudi sistemi satelitske navigacije (GPS – Global Positioning System) so lahko vir informacije o točnem času.

[9] NTP – Network Time Protocol je protokol za sinhronizacijo sistemskega časa računalniških sistemov, povezanih v IP omrežja npr. Internet. NTP je eden najstarejših še uporabljanih Internetnih protokolov. Podatek o točnem času zagotavlja mreža strežnikov, osnovna informacija o točnem času pa tudi temelji na cezijevi ali rubidijevi časovni normali.

3.3.1 Analizator omrežja MC 760 in zapisovalnik omrežja MC 750 (Iskra MIS)

Analizator omrežja MC 760 je namenjen permanentni analizi kakovosti električne napetosti po standardu SIST EN 50160. V internem pomnilniku se shranjujejo poročila za obdobje zadnjih 7 let. Poleg tega shranjuje tudi preko 170.000 odstopanj merjenih veličin od standardnih vrednosti, kar omogoča odkrivanje morebitnih vzrokov težav na omrežju. Za vsako opazovano značilnost je možno določiti poljubne meje in zahtevano kakovost v opazovanem obdobju.

Merilnik meri in registrira naslednje značilnosti: odklone frekvence, odklone napetosti, upade napetosti, prekinitve napetosti, neravnotežja napetosti, prenapetosti, hitre napetostne spremembe, jakost flikerja[10], THD[11], harmoniki.

Slika 3.2: Analizator omrežja MC 760 in zapisovalnik omrežja MC 750 (Iskra MIS, d.d.)

Pomembnejše lastnosti MC 760 so:

- vrednotenje kakovosti električne napetosti po SIST EN 50160,
- meritve trenutnih vrednosti preko 140 veličin (U, I, P, Q, S, PF, PA, f, φ, THD, MD, energija, cena energije po tarifah...),
- razred točnosti 0,5 ali 0,2 (na zahtevo),
- harmonska analiza faznih, medfazni napetosti in tokov do 63. harmonika,
- zapisovanje do 32 merjenih veličin in alarmov v interni pomnilnik (8 MB flash),

---

[10] Fliker je zaznavni pojav (npr. utripanje žarnic), ki je posledica nihanja amplitude napetosti v določenem frekvenčnem območju in nastopi zaradi delovanja nekaterih nelinearnih porabnikov, kot so npr. obločne peči.

11 Celostni harmonski faktor popačenja (Total Harmonic Distortion) se izračuna po enačbi $THD = \sqrt{\sum_{h=1}^{40} (u_h)^2}$

pri čemer je u_h relativna amplituda harmonske napetosti glede na osnovno napetost, h pa red harmonika.

- meritve 40 minimalnih in maksimalnih vrednosti v različnih časovnih obdobjih 32 nastavljivih alarmov,
- široko nazivno frekvenčno območje 16 Hz do 400 Hz, 128 vzorcev v periodi,
- RS 232/RS 485 komunikacija do 115.200 bit/s ali Ethernet komunikacija,
- MODBUS in DNP3 komunikacijski protokol,
- do 4 vhodi ali izhodi (analogni izhodi, pulzni izhodi, izhodi alarmov, tarifni vhodi).

Zapisovalnik omrežja MC 750 je na videz podoben analizatorju omrežja MC 760. Bistvena razlika je v manjšem pomnilniku in s tem manjšemu številu dogodkov, ki jih lahko shranjuje do prenosa v nadrejeni center ter v neizpolnjevanju nekaterih zahtev meritev po standardu SIST EN50160 (harmoniki, fliker) [8].

3.3.2 Parametri obratovalnih meritev v TP SN/NN

V predhodnem poglavju predstavljena analizator in zapisovalnik omrežja omogočata zajem oziroma izračun velikega števila merilnih podatkov. Ugotovili smo, kateri od teh podatkov so koristni oziroma katere informacije so potrebne za izvajanje nalog razvoja, obratovanja in transporta, kontrole odjema EE in spremljanja kakovosti EE. Na tej osnovi lahko opredelimo parametre, ki jih mora informacijski sistem obratovalnih meritev zajemati, zbirati v nadrejenem merilnem centru in jih shranjevati v podatkovni zbirki. Nova podatkovna zbirka mora biti zasnovana tako, da jo je mogoče povezovati z drugimi podatkovnimi zbirkami uporabnika. Merilni center obratovalnih meritev mora biti vključen v (tehnični) informacijski sistem Elektra Gorenjska.

V tabeli 3.1 so navedeni za zajem predvideni parametri obratovalnih meritev. Za vsak parameter je opredeljen namen uporabe in zahtevana perioda zajema povprečne vrednosti parametra. V šestem stolpcu (dejanska perioda – meritev) navedena perioda omogoča izračun zahtevanih vrednosti glede na namen uporabe.

V podatkovni zbirki mora biti vsak parameter opremljen z identifikacijsko številko TP, v kateri je bil izmerjen. Identifikacijska številka mora biti enaka številki sredstva (npr. TP) v bazi tehničnih podatkov (BTP). Na ta način je enoumno določeno mesto zajema parametra v distribucijskem omrežju.

Vsem parametrom mora biti pridružen tudi natančen čas in datum meritve. Analizator in zapisovalnik omrežja imata vgrajen dajalnik realnega časa. Za časovno sinhronizacijo vseh merilnikov mora skrbeti nadrejeni merilni center.

Alarmi morajo poleg podatka o točnem času in identifikacijski številki TP vsebovati tudi podatek o vrsti alarma in o vzroku nastanka, če merilnik to omogoča. Lep primer je upad napetosti ene faze, ki je lahko posledica prekinitve enega vodnika na primarni strani TP ali prekinitve varovalke. Z dodatnimi digitalnimi vhodi merilnika in indikatorji napetosti pred varovalkami je mogoče ugotoviti vzrok upada napetosti. Takšna informacija lahko bistveno skrajša potreben čas za odpravo napake na omrežju.

Tabela 3.1: Parametri obratovalnih meritev v TP SN/NN

Parameter	Perioda zajema (povprečne) vrednosti					Izračun / opomba
	potrebna perioda				*dejanska*	
	Razvoj	Obratovanje vzdrževanje	Kontrola odjema	Kakovost	Meritev	
Fazne napetosti $U_{ef1}, U_{ef2}, U_{ef3}$,	/	15 min	15 min	10 min	5 min	
Tokovi $I_{ef1}, I_{ef2}, I_{ef3}, I_n$	/	15 min	15 min	10 min	5 min	
Fazni koti	/	15 min	15 min	10 min	5 min	
Delovne moči P_1, P_2, P_3	/	15 min	15 min	10 min	5 min	
Jalove moči Q_1, Q_2, Q_3	/	15 min	15 min	10 min	5 min	
Har. popačenje THD ($I_1, I_2, I_3, U_1, U_2, U_3, U_{12}, U_{23}, U_{31}$)	/	/	/	10 min	10 min	
Konične vrednosti $P_{tmax}, Q_{tmax}, I_{tmax}$		/		/		prenos novih vrednosti ob spremembi
Frekvenca	/	/	/		/	merjeno na nivoju RTP
Padci napetosti	/		/	10ms	/	izračun časa med alarmi
Izpadi napetosti	/		/	10ms	/	izračun časa med alarmi
Harmoniki	/	/	/	10 min	*	MI7150,MC750 ne omogoča
Utripanje	/	/	/	P_{st} 10min P_{lt} 120min	*	MI7150,MC750 ne omogoča
Nesimetrija	/	/	/	/	/	izračun iz faznih kotov
Signalne napetosti	/	/	/	/	*	MI7150,MC750 ne omogoča
Alarmi (prekoračitve mejnih vrednosti)	/		/	/		ob dogodku prenos podatkov sproži MI

*** MC 760 podpira vse meritve v skladu s SIST EN 50160**

3.4 Sistemi za nadzor in vodenje SN omrežja in RTP VN/SN

Vodenje distribucijskega omrežja usklajuje distribucijski center vodenja (DCV). DCV Elektro Gorenjska se nahaja v Kranju in preko lastnih optičnih in radijskih zvez nadzoruje ter vodi delovanje 15 RTP VN/SN oziroma SN/SN, 6 RP in več kot 760 daljinsko vodenih stikal (DVS) v TP in sami SN mreži. Osnova za pravilno vodenje sistema so telemetrične meritve in obdelava merilnih podatkov. Merilni podatki se zajemajo v postajnih računalnikih posameznega dislociranega objekta (RTP, RP, DVS, TP) in se prenašajo v DCV.

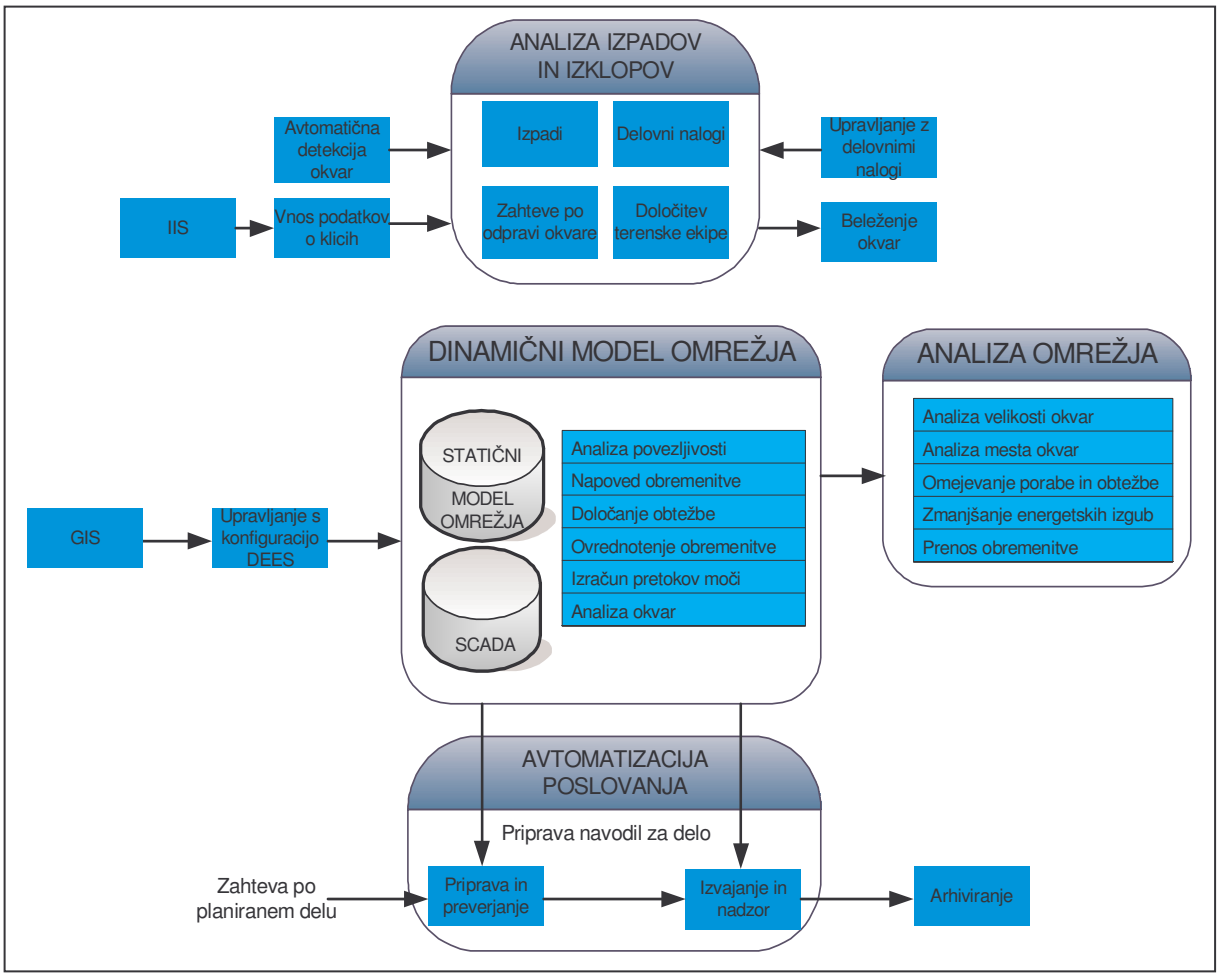
3.4.1 Sistem vodenja na nivoju DCV

Sistem vodenja na nivoju DCV obsega naslednje funkcionalnosti:

- SCADA:
    - podatkovno procesiranje,
    - grafični prikaz stanja omrežja, trendi,
    - krmiljenje stikalnih elementov, nastavitve regulacijskih parametrov,
    - alarmi in dogodki,
    - historične informacije;
- DMS funkcionalnosti:
    - stanje omrežja (analiza povezljivosti, napoved obremenitve, izračun pretoka moči),
    - analiza omrežja (zmanjšanje energetskih izgub, porazdelitev obremenitve, prenos nepredvidenih obremenitev, regulacija napetosti, analiza tokov okvare, lociranje napake in avtomatska restavracija omrežja),
    - avtomatizacija poslovanja (priprava navodil za delo, detekcija in spremljanje izpadov),
    - posebne funkcije (simulator za usposabljanje operaterjev, omejevanje porabe in obtežbe).

SCADA sistem je namenjen zbiranju podatkov o EE sistemu in njihovemu posredovanju do različnih delovnih postaj na različnih lokacijah. Osnovni sestavni deli SCADA paketa so zajemanje podatkov, procesiranje podatkov, izdajanje komand in nekateri izračuni. Operater (dispečer) dostopa direktno do sistema preko uporabniško prijaznega vmesnika človek-stroj, ki je namenjen obdelavi vseh podatkov tako v smeri sprejemanja komand od operaterja, kot

tudi prikazovanju podatkov operaterju. Prav tako pa so del enotnega vmesnika človek – stroj tudi procesiranje alarmov, procesiranje dogodkov, procesiranje historičnih podatkov in razna poročila. Programski paket ECS SCADA je zasnovan kot odprt ali distribuiran sistem vrste strežnik – odjemalec, kjer je v največji možni meri uporabljena standardna strojna in programska oprema priznanih proizvajalcev.



Slika 3.3: Blokovna shema dinamičnega modela omrežja (DNM - Dynamic Network Model)

V sklopu strežnika za SCADA funkcije se procesirajo podatki naslednjih vrst:

- **meritve:** v to skupino spadajo tako analogne kot digitalne vrednosti; meritve se lahko zajemajo iz končnih postaj ali drugih centrov vodenja, vnašajo se ročno ali izračunajo iz drugih podatkov;
- **statusi:** podajajo spremembo stanja ali prekoračitev določenega praga; tvori se dogodek, ki se nadalje obdeluje v modulu za alarmiranja; sporočila o poteku dogodkov se sproti zapisujejo v historično podatkovno bazo;

- **kronološka sporočila:** podatki opremljeni s časovno značko 1 ms in se uporabljajo za »post mortem« analizo vzrokov in posledic posameznih dogodkov na omrežju;
- **obratovalni števčni podatki:** obravnavajo se podobno kot analogne števčne meritve in se uvrščajo v skupino t.i. akumuliranih analognih vrednosti;
- **ročno vneseni podatki:** operater ima možnost ročnega vnosa kateregakoli podatka, tako vnesen podatek se na pregledih razlikuje od avtomatično zajetega podatka;
- **podatkovne značke:** ta vrsta sistemskih podatkov je namenjena lažjemu delu operaterjev in jih je možno vnašati ročno, lahko pa jih tvori sistem sam.

Podatki iz procesne podatkovne baze se beležijo v historično podatkovno bazo ciklično (meritve in podobni podatki) ali ob spremembi (dogodki, alarmi, prekoračitve, ipd.) in so v historični podatkovni bazi opremljeni s časom. Historični podatki se lahko pregledujejo v grafičnem in/ali tabelaričnem načinu.

Dinamični model omrežja (DNM - Dynamic Network Model) je osnova celotne zbirke aplikacij, ki tvorijo sistem za upravljanje distribucijskega omrežja (DMS – Distribution Management System). DNM v realnem času prikazuje trenutno poznano in predvideno stanje distribucijskega omrežja in tvori osnovo za analizo izpadov, omrežne analize, optimizacije, izvajanje zaporedja stikalnih manipulacij … DNM lahko prikazuje celotno distribucijsko omrežje, torej tako VN, SN, NN izvode iz TP in stanja transformacij, če so le na voljo obratovalni podatki o stanju omrežja na vseh napetostnih nivojih. Kot tak je praktično pripravljen za razširitev vodenja tudi na nivoju TP in izvoda iz TP TN/SN; predpogoj je seveda že omenjena razširitev obratovalnih meritev na nivo TP.

3.4.2 Komunikacijske povezave DCV

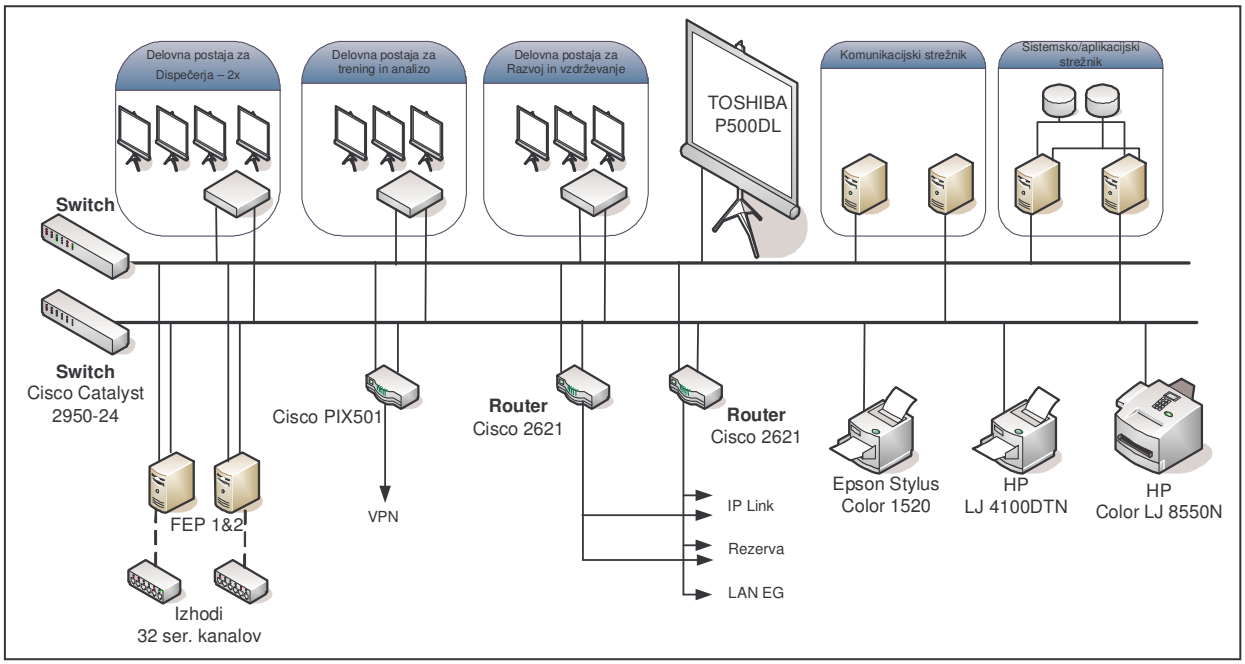
Komunikacije med posameznimi deli informacijskega sistema v sklopu DCV temeljijo na uporabi komunikacijskega protokola TCP/IP. Komunikacije s končnimi postajami in RCV pa se izvajajo preko namenskih protokolov, kot je navedeno v nadaljevanju. Vsi uporabljeni protokoli ustrezajo delitvi na plasti v skladu s 7-plastnim OSI modelom.

DVC se na telekomunikacijsko infrastrukturo navezuje preko:

- Podsistema za zajemanje podatkov iz končnih postaj DAS (Data Acquisition System), ki je sestavljen iz DAC (Data Acquisition and Control Subsystem) strežnika in FEP (Front End Processor) računalnikov; končne postaje so nameščene po posameznih objektih (DCV, RTP, RP, TP, DVS) in

- Redundančnega para usmerjevalnikov (router) do drugih centrov vodenja in do lokalnega omrežja v podjetju (IIS, intranet, razvoj omrežja ipd.).

Zajem podatkov v programskem paketu ECS SCADA[12] poteka s pomočjo priključenih končnih postaj, ki delujejo z različnimi komunikacijskimi protokoli (DNP, IEC 60870-5-101 ...). Za izmenjavo podatkov z RCV ELES je implementiran komunikacijski protokol ELCOM-90, vsi podatki pa so časovno sinhronizirani z GPS uro [9].



Slika 3.4: Topologija in konfiguracija sistema DCV EG

3.5 Sistemi za nadzor kakovosti EE

EG izvaja meritve kakovosti EE v skladu s standardom SIST EN 50160 na dva načina:

- s stalnim monitoringom kakovosti na SN zbiralkah v vseh RTP VN/SN,
- z občasnim monitoringom kakovosti na celotnem distribucijskem omrežju.

3.5.1 Stalni monitoring kakovosti EE

Stalni monitoring kakovosti napetosti je trajno beleženje merljivih parametrov kakovosti napetosti v skladu s sprejeto standardizacijo in z določili navodil, ki jih izda SODO.

[12] EG uporablja ECS SCADA sistem kanadskega proizvajalca SNC-Lavalin inc.

Ta navodila predvidevajo:

- poenotenje načina izvajanja stalnega monitoringa kakovosti napetosti,
- poenotenje poročanja o stanju kakovosti napetosti,
- evropsko primerljivost stanja kakovosti napetosti,
- načrtovanje omrežja na podlagi stanja kakovosti napetosti in
- določitev minimalnih zahtev za izvajanje stalnega monitoringa kakovosti napetosti.

Stalni monitoring kakovosti napetosti mora biti v skladu z Uredbo o splošnih pogojih za dobavo in odjem električne energije (SPDOEE) zagotovljen na zbiralkah VN/VN in VN/SN razdelilnih transformatorskih postaj in na meji med prenosnim in distribucijskim omrežjem. Na SN nivoju je stalno spremljanje kakovosti napetosti predvideno na na vseh SN zbiralnicah objektov na meji s prenosnim ali sosednjim distribucijskim omrežjem. Stalni motitoring se lahko izvaja tudi v RP, v točkah, kjer se predvideva slabša KEE ipd.

Uporabljena merilna metoda mora biti skladna s SIST EN 61000-4-30. Klasifikacija uporabljene merilne opreme mora za vse tiste značilnosti napetosti, ki se izkazujejo za dejansko problematične, ustrezati razredu A ali B.

Letno poročilo o stanju kakovosti napetosti

Izvajalec dejavnosti SODO mora vsako leto do konca aprila objaviti poročilo o kakovosti napetosti za preteklo leto. Poročilo mora vsebovati kazalce, ki omogočajo primerljivost z drugimi izvajalci dejavnosti SODO. Letno poročilo o stanju kakovosti napetosti sistema stalnega spremljanja kakovosti napetosti predstavlja splošno oceno stanja kakovosti napetosti. Poročilo je namenjeno informiranju o stanju kakovosti napetosti. Podatki se vrednotijo na podlagi standarda SIST EN 50160 ter SIST HD 472 S1, pri čemer je potrebno upoštevati standard, ki podaja strožja merila. Uporaba omenjene standardizacije se po dogovoru razširi tudi na 110 kV napetostni nivo.

Poročilo temelji na standardnih tedenskih poročilih o skladnosti. Rezultati tedenskih poročil sestavljajo tabelo podatkov o skladnosti parametrov kakovosti napetosti s standardom SIST EN 50160 po posameznih merilnih točkah v merilnem letu. Z zbranimi podatki v tabeli se izračunavajo naslednji indeksi ali pokazatelji stanja kakovosti napetosti na VN in SN nivoju:

Indeks stanja kakovosti napetosti:

$$I_{KEE} = \left(1 - \frac{\sum_{i=1}^{n} št.\ neskladnih \quad tednov}{\sum_{i=1}^{n} št.\ tednov \quad pod \quad nadzorom} \right) \cdot 100\ \%$$

i = 1… n, število merilnih točk

Indeks stanja harmonskih komponent napetosti:

$$I_{H} = \left(1 - \frac{\sum_{i=1}^{n} št.\ neskladnih \quad tednov\ harmonskih \quad napetosti}{\sum_{i=1}^{n} št.\ tednov \quad pod \quad nadzorom} \right) \cdot 100\ \%$$

i = 1… n, število merilnih točk

Indeks stanja flikerja (migotanje, utripanje, kolebanje):

$$I_{Plt} = \left(1 - \frac{\sum_{i=1}^{n} št.\ neskladnih \quad tednov\ zaradi\ Plt}{\sum_{i=1}^{n} št.\ tednov \quad pod \quad nadzorom} \right) \cdot 100\ \%$$

i = 1… n, število merilnih točk

Indeksi kakovosti napetosti so podlaga za prikaz časovnih gibanj (tendenc) nivoja kakovosti napetosti v daljšem časovnem obdobju (več let nadzora).

Načrtovani nivoji kakovosti napetosti vključujejo najbolj izpostavljene harmonske napetosti, dolgotrajni in kratkotrajni fliker, kar je v skladu s tehničnimi zmožnostmi sistema stalnega monitoringa KEE.

Tabela 3.2: Predlagane mejne vrednosti načrtovanih nivojev kakovosti napetosti

Prameter		***VN nivo***	***SN nivo***
Dolgotrajni fliker	[P_{LT}]	0,6	0,7
Kratkotrajni fliker	[P_{ST}]	0,8	0,9
3. harmonska napetost	[H3]	2%	4%
5. harmonska napetost	[H5]	2%	5%
7. harmonska napetost	[H7]	2%	4%
Skupno harmonsko popačenje	[THD]	3%	6,5%

Poročilo temelji na 10-minutnih zapisih najbolj izpostavljenih parametrov kakovosti napetosti. Statistična analiza 10-minutnih parametrov je podlaga za tabelo statistično ovrednotenih parametrov načrtovanih nivojev kakovosti napetosti po posameznih merilnih mestih.

Razširjenost in izvajanje stalnega monitoringa KEE v EG

Stalni monitoring se je v EG začel uvajati leta 2002, sistematično pa se je začel izvajati v letu 2004. Trenutno razširjenost stalnega monitoringa prikazuje tabela 3.3.

Tabela 3.3: Stalni monitoring KEE v letu 2009

1.	RTP Jesenice 110 kV	24.	RTP Primskovo 20kV TR2
2.	RTP Radovljica 110 kV	25.	RTP Zlato polje 20kV TR1
3.	RTP Tržič 110 kV	26.	RTP Zlato polje 20kV TR2
4.	RTP Primskovo 110 kV	27.	RTP Labore 20kV TR1
5.	RTP Zlato polje 110 kV	28.	RTP Labore 20kV TR2
6.	RTP Labore - DV Okroglo 110 kV	29.	RTP Labore 20kV TR3
7.	RTP Škofja loka 110 kV -Okroglo	30.	RTP Škofja loka 20kV TR1
8.	RTP Škofja Loka - DV Kleče 110 kV	31.	RTP Škofja loka 20kV TR2
9.	RTP Bled 35 kV	32.	RTP Železniki 20kV TR1
10.	RTP Bohinj 35 kV	33.	RTP Železniki 20kV TR2
11.	RTP Bled 2 0kV TR2	34.	RTP Medvode 20 kV TR4
12.	RTP Bled Kbv Radovljica20 kV	35.	RTP Medvode 20 kV TR5
13.	RTP Bohinj 20 kV	36.	TP Kranjska Gora
14.	RTP Kr Gora 20 kV TR1	37.	TP Planica
15.	RTP Kr Gora 20 kV TR2	38.	TP Zvoh
16.	RTP Jesenice 20 kV TR1	39.	TP Kabinska TR1
17.	RTP Jesenice 20 kV TR2	40.	TP Kabinska TR2,3
18.	RTP Radovljica 20 kV TR1	41.	TP Kabinska TR4
19.	RTP Radovljica 20 kV TR2	42.	TP Kržišče
20.	RTP Završnica 20 kV	43.	TP Tiha dolina
21.	RTP Tržič 20 kV TR1	44.	TP Rjava skala TR1
22.	RTP Tržič 20 kV TR2	45.	TP Rjava skala TR2
23.	RTP Primskovo 20 kV TR1		

Stalni monitoring kakovosti napetosti se je v letu 2009 izvajal na 45 merilnih mestih in sicer na napetostnih nivojih:

- VN (8 merilnih mest),
- SN (27 merilnih mest),
- NN (10 merilnih mest).

3.5.2 Občasni monitoring kakovosti EE

Občasni monitoring KEE se izvaja:

- v primeru zahteve uporabnika omrežja po izjavi o kakovosti napetosti,
- v primeru oporekanja uporabnikov omrežja ter
- po naprej opredeljenem programu meritev in analiz stanja KEE.

V postopku preverjanja skladnosti kakovosti napetosti izvajalec dejavnosti SODO ugotavlja skladnost z zahtevami standardov in določil za ocenjevanje kakovosti električne energije, objavljenimi v SPDOEE. Postopek ugotavljanja skladnosti se izvaja v smislu zahtev standarda v referenčnem tednu dni. Rezultat meritev in analiz kakovosti napetosti je izjava o kakovosti napetosti, ki se izdaja na zahtevo uporabnika le za normalno obratovalno stanje.

Postopek izdajanja izjave o skladnosti / neskladnosti kakovosti napetosti:

- na podlagi zahteve uporabnika električne energije strokovno osebje preveri skladnost kakovosti napetosti z zahtevami;
- v primeru popolne zadostitve zahtevam standardov kakovosti napetosti, izvajalec dejavnosti SODO izda izjavo o skladnosti kakovosti napetosti, v tem primeru govorimo o standardni kakovosti električne energije;
- v primeru odstopanja od postavljenih kriterijev kakovosti električne napetosti izvajalec dejavnosti SODO izda izjavo o neskladnosti kakovosti električne napetosti. V tem primeru govorimo o nestandardni kakovosti električne energije. Izjava vsebuje opozorilo odjemalcu ali dobavitelju na možnost negativnega vpliva na naprave in njihovo obratovanje, na potencialno ogroženost funkcionalne varnosti ter možnost negativnih vplivov na živo in neživo naravo. Izdela se tehnično poročilo z opredeljenimi odstopanji od postavljenih kriterijev.

V primeru izdane izjave o neskladnosti kakovosti električne napetosti sledi:

- izvajalec dejavnosti SODO ugotovi vzrok oziroma izvor neskladja,
- glede na ugotovljeni vzrok/izvor neskladja, izvajalec dejavnosti SODO sam oziroma v dogovoru z uporabnikom omrežja predloži ukrepe za odpravo neskladja;
- ukrepi za odpravo neskladja, na podlagi predhodno ugotovljenega vzroka/izvora neskladja, zavezujejo povzročitelja/izvor neskladja;
- po izvedenih ukrepih za odpravo neskladja strokovno osebje izvajalca dejavnosti SODO izvede ponovno merilno – tehnično preverjanje skladnosti z zahtevami ter posreduje izjavo uporabniku omrežja.

Merilna oprema in izvajanje občasnega monitoringa KEE v EG

Občasni monitring kakovosti v celoti obvladuje oddelek za kakovost EE (Služba za podporo obratovanju), izvajajo pa ga tako strokovnjaki oddelka za kakovost kot tudi krajevna nadzorništva. Ne glede na izvajalca meritev pa se rezultati meritev kakovosti posredujejo oddelku za kakovost, ki tudi izdaja poročila o skladnosti / neskladnosti kakovosti.

Občasni monitoring kakovosti trenutno izvajamo z naslednjo merilno opremo: Memobox 300, Memobox 300 Smart in Memobox 800.

3.5.3 Uporaba pridobljenih podatkov o stanju kakovosti EE

Pridobljene podatke o stanju KEE uporablja izvajalec dejavnosti SODO v interne namene v smislu celotnega obvladovanja kakovosti električne energije distribucijskega omrežja. Podatki o stanju kakovosti EE se upoštevajo v procesu energetskega načrtovanja, posledičnega razvoja distribucijskega omrežja, sanacije omrežja ter v procesu izdaje tehničnih pogojev za soglasja in priključitev novih odjemalcev.

4 OBRAČUNSKE MERITVE V OMREŽJU ZA DISTRIBUCIJO EE

Vpliv liberalizacije in deregulacije na področju trga z električno energijo (in plina) zahteva od distributerjev prilagajanje novim tržnim razmeram. Distribucije se soočajo s problemi primerne organiziranosti in tehnične opremljenosti ter z zagotavljanjem kakovostnejših storitev za dosego večje konkurenčnosti in pripravljenosti na poslovanje v tržnih razmerah. Ti vplivi narekujejo uporabo zmogljivejših merilnih naprav na vseh nivojih odjema, pa tudi nove naprave – registratorje, podatkovne koncentratorje in komunikacijske naprave ter namensko programsko opremo za obdelavo podatkov. Tako se je pojavila potreba po izgradnji informacijskega sistema, ki bo:

- povezal merilna mesta z ostalimi napravami v celovit sistem, sposoben zajemanja in procesiranja merilnih podatkov v kvazi-realnem času ter
- omogočal povezavo z obstoječo komunikacijsko in programsko infrastrukturo distribucij.

4.1 Razvoj sistemov za daljinsko odčitavanje porabe EE in drugih energentov

V zadnjem času smo priča izredno hitremu razvoju t.i. sistemov AMR (Automated Meter Reading) in naprednejših AMM (Advanced Metering Management – napredna merilna infrastruktura, omogoča tudi upravljanje merilnega mesta, npr. daljinski odklop) ter AMI (Advanced Metering Infrastructure – napredna merilna infrastruktura, nadgradnja AMM, AMR; vključuje tudi upravljanje meritev plina, vode …). V slovenskem distribucijskem omrežju še vedno prevladujejo indukcijski števci električne energije. Sodobni elektronski števci z možnostjo avtomatskega odčitavanja se nekaj let uporabljajo za merjenje porabe električne energije večjih odjemalcev (odjemalci s priključno močjo nad 41 kW).

Večinoma se uporabljajo elektronski števci z vgrajenim GSM – GPRS modemom, s katerimi komunicira center za obdelavo podatkov neposredno. Pri tem je pomembno dejstvo, da predstavljajo večji odjemalci po številu le 1% vseh odjemalcev. Predvsem zaradi zelo velikega števila gospodinjskih odjemalcev se je pojavila potreba po razvoju sistemov, ki bi optimirali komunikacijske poti. Kot primeren se je izkazal sistem komuniciranja po energetskih NN vodih (Distribution Line Carrier - DLC) z vgradnjo podatkovnih koncentratorjev v SN/NN transformatorske postaje. Na ta način se zmanjša število točk, s katerimi merilni center komunicira neposredno.

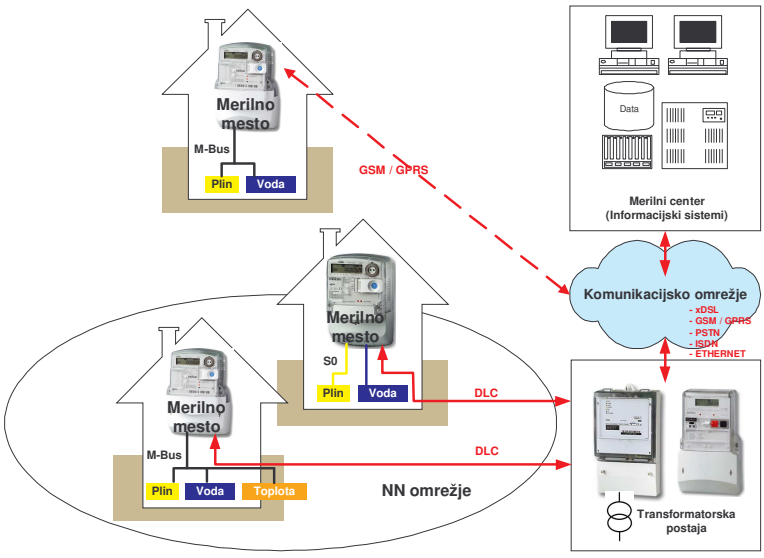
V Sloveniji je bilo v začetku leta 2010 registriranih več kot 900.000 odjemalcev električne energije. Zavedati se moramo, da predstavlja posodobitev tako velikega sistema meritev porabe električne energije zelo velik finančni zalogaj. Tudi fizične zamenjave vseh merilnih naprav ter izgradnje komunikacijskih sistemov ni mogoče realizirati v kratkem času. V času izredno hitrega razvoja AMR sistemov in borbe za trg med proizvajalci merilne opreme je potrebna velika previdnost pri izbiri sistema, ki bo po eni strani zadovoljil potrebam po avtomatskem odčitavanju porabe električne energije in bo tudi ekonomsko sprejemljiv [10].

4.2 Sistem za avtomatsko odčitavanje števcev EE

V svetu obstaja več velikih proizvajalcev sistemov za avtomatsko odčitavanje števcev EE. Večina ponuja poleg osnovnih AMR sistemov tudi naprednejše izvedbe AMM in v zadnjem času AMI. V Sloveniji sta najpogosteje uporabljana sistema proizvajalcev Iskraemeco in Landis+Gyr. Arhitektura sistema je na kratko predstavljena v nadaljevanju.

4.3 Arhitektura AMI sistema

Arhitekturo AMI sistemov lahko v grobem razdelimo na tri nivoje. To so merilna mesta, komunikacijsko omrežje in merilni center - sistemi za obdelavo podatkov.



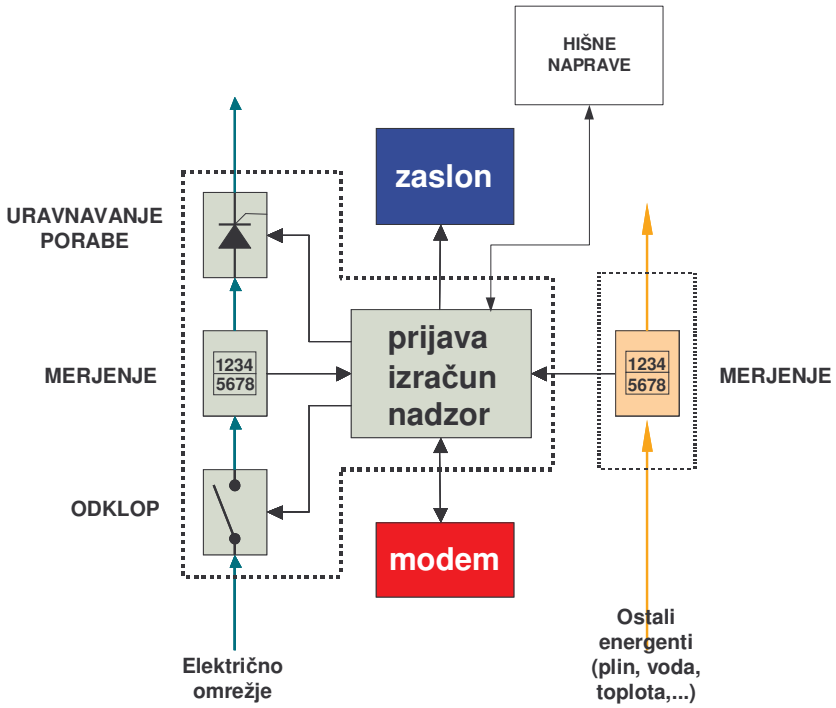
Slika 4.1 Zasnova AMI sistema [10]

4.3.1 Merilna mesta AMI sistema

Dandanes števec električne energije v večini AMI sistemov ni le merilna naprava, ampak vedno bolj postaja energetska informacijska vstopna točka za gospodinjstva, torej nek prehod (gateway) med hišnimi napravami in operaterjem distribucijskega omrežja ter drugimi udeleženci na energetskem trgu.

4.3.2 Sistemski AMI števci (Smart Meters)

Osnovni element merilnega mesta je sistemski števec (Smart Meter). Shematsko je prikazan na Sliki 4.2.



Slika 4.2 Shema AMI števca z nekaterimi bistvenimi funkcijami [10]

V AMI sistemih se poleg merjenja zahtevajo še sledeče lastnosti sistemskega števca:

- zmožnost varne dvosmerne izmenjave podatkov s sistemi za obdelavo in upravljanje s podatki,
- možnost zajema podatkov ostalih hišnih merilnih naprav (plinomer, vodomer …);
- možnost komunikacije s hišnimi napravami, npr. posameznimi porabniki in sistemi hišne avtomatike,
- nastavljivost intervala shranjevanja merilnih vrednosti in daljinskega odčitavanja ostalih merilnih naprav,

- možnost daljinskega in lokalnega odklopa in (ponovnega) vklopa ter omejevanja (upravljanja) porabe,
- možnost dinamičnih tarif oziroma daljinskega nastavljanja tarif,
- avtomatska sinhronizacija ure (točen čas),
- možnost prikaza določenih informacij (poraba, cene ipd.) na ločenem prikazovalniku – zaslonu,
- merjenje nekaterih parametrov kvalitete napetosti – možnost shranjevanja dogodkov (npr. upadov, izpadov),
- možnost daljinskega nadzora in upravljanja s števcem ter možnost avtodiagnostike,
- zmožnost sledljivosti posegov v števec in ustrezne zaščita dostopa.

4.3.3 Priključitev števcev ostalih energentov in povezava s hišnimi napravami

V gospodinjstvu se poleg električne energije običajno meri še poraba zemeljskega plina, toplote (daljinsko centralno ogrevanje) in pitne vode.

Z opremo merilnega mesta s sistemskim števcem se tako ponuja tudi možnost daljinskega odčitavanja porab zgoraj navedenih energentov in vode. Večina števcev drugih energentov ni opremljena s komunikacijskim vmesnikov. Največ kar lahko trenutno od teh števcev pričakujemo je, da imajo na voljo impulzni izhod (S0), ki je bodisi realiziran že v samem števcu kot breznapetostni kontakt ali pa ga dobimo z namestitvijo ustrezne optične glave. Sistemski števci največkrat podpirajo dve možnosti priključitve drugih števcev: impulzni vhodi (S0) in M-bus (Metering bus).

Težava pri priključitvi drugih števcev na sistemski števec je tudi v tem, da so števci običajno v različnih prostorih. Žične povezave - če so sploh mogoče -so običajno časovno zamudne in posledično drage, zato se vse bolj posega po brezžičnih (RF) možnostih povezave.

Slika 4.3 prikazuje primer rešitve RF odčitavanja, ki jo ponuja podjetje Coronis, na svetovnem spletu pa je mogoče zaslediti tudi drugačne rešitve[13]. Podatki se do koncentratorja

[13] Nekaj primerov uporabe ZigBee (vir: svetovni splet):
http://www.digi.com/learningcenter/stories/monitor-energy-consumption-in-real-time
http://www.zigbee.org/Industry_Presentation_2008_10_19/tabid/298/Default.aspx
http://www.itron.com/asset.asp?path=solutions/solutions/images/itr_016422-2.jpg

prenašajo brezžično na ISM frekvenčnih območjih (433/868/915). Enota ima lastno napajanje in lahko deluje do 15 let. Žal veliko brezžičnih rešitev ne temelji na odprtih standardih, zato interoperabilnost med napravami različnih proizvajalcev ni zagotovljena. V zadnjem času se uveljavlja ZigBee omrežje, ki obeta standardizacijo komuniciranja med merilniki različnih proizvajalcev.

Slika 4.3: Primer zajemanja podatkov iz vodnega števca preko RF povezave [10]

4.3.4 Komunikacijski koncentratorji AMI sistema

Nekatere vrste komunikacije (npr. DLC) imajo omejen domet in/ali omejeno pasovno širino, zato se uporabljajo koncentratorji, ki na lokalnem območju komunicirajo s števci, ter prenašajo informacije na višji nivo ter obratno.

Najpogostejša vrsta komunikacije na strani števcev je DLC ali pa RS485, na strani komunikacije z višjim nivojem pa imajo koncentratorji veliko več možnosti (PSTN, ISDN, GSM/GPRS, Ethernet …) in se lahko prilagodijo danemu komunikacijskemu omrežju.

4.3.5 Merilni center AMI sistema

Merilni center sestavlja najvišji nivo v arhitekturi AMI sistema. Center sestavljajo:

- strojna oprema (komunikacijska oprema, strežniki, delovne postaje, naprave za varno shranjevanje podatkov, naprave za rezervno napajanje, ipd.);
- programska oprema (programska oprema za zajem in obdelavo podatkov, upravljanje z merilnimi mesti, programska oprema za nadzor sistema, ipd.); podatki se shranjujejo v relacijskem podatkovnem strežniku MS SQL ali Oracle.

4.3.6 Komunikacijsko omrežje AMI sistema

Komunikacijsko omrežje mora zagotoviti varen prenos podatkov v obe smeri med koncentratorji, števci ter višjimi nivoji – običajno je to merilni center. Pogosto se v AMI sistemih uporabljata vsaj dve različni omrežji:

- geografsko lokalno: omrežje skrbi za komunikacijo med sistemskimi števci in koncentratorji (npr. DLC preko energetskih vodov ali pa RS485 vodilo);
- geografsko široko: omrežje pa za komunikacijo med koncentratorji in merilnim centrom.(npr. GSM/GPRS, telefonsko omrežje ipd.).

Za komunikacijo med števci in koncentratorji ali direktno med merilnim centrom in števci se najpogosteje uporablja DLMS/COSEM[14] protokol, za komunikacijo med koncentratorji in števci pa internetni protokoli temelječi na družini protokolov TCP/IP.

DLC / PLC – komunikacija po energetskih napajalnih vodih

Prenos podatkov poteka preko energetskih napajalnih vodov. Le-ti niso najbolj primerni za prenos visokofrekvenčnih signalov (veliko slabljenje, motnje …), zato je domet omejen. Ta vrsta komunikacije za potrebe AMI se največ uporablja znotraj območja transformatorske postaje (transformator predstavlja za DLC signale blokado) na NN strani in omogoča uporabne domete do 500m. Domet se da povečati z uporabo ojačevalnikov (repeator-jev) in lahko doseže največ nekaj kilometrov. Hitrost prenosa informacij je običajno 1200 ali 2400 bps. Modulacija signala je S-FSK (spread frequency shift keying).

Velika prednost DLC je v tem, da je infrastruktura že zgrajena. Števec, ki ima vgrajen DLC modem, je priključen v omrežje takoj, ko ga zmontiramo. Zanj ni potrebno nobeno dodatno ožičenje.

Mobilno omrežje (GSM/GPRS/UMTS)

Mobilno omrežje deluje na frekvencah 900MHz in 1800MHz in omogoča tudi podatkovni prenos, kar s pridom uporabimo za potrebe AMI sistemov. Priključitev na omrežje z napravo, ki vsebuje GSM/GPRS modem, je zelo enostavna. Podatkovni načini prenosa podatkov so

[14]**DLMS** (Device Language Message Specification) je družina protokolov, ki so namenjeni za izmenjavo sporočil pri merjenju električne energije, nastavitvah tarifnih časov in upravljanju z bremeni. Razvijajo in vzdržujejo se pod okriljem skupine standardov **IEC 62056. COSEM** (Companion Specification for Energy Metering) vključuje specifikacije transportne in aplikacijske plasti DLMS protokolov.

lahko različni: klasični prenos podatkov CSD, hitri prenos HSCSD in 3G CSD ter paketni prenos (GPRS in HSDPA/UMTS).

Hitrosti prenosa za paketni prenos so teoretično do 82,4 kb/s, le v omrežju UMTS, kjer je zagotovljen signal HSPA, pa z ustrezno terminalsko opremo dosegajo do 384 kb/s oziroma do 3,6 Mb/s. Komunikacija za namene AMI, ki uporablja mobilna omrežja, običajno poteka preko navideznega privatnega omrežja.

V primeru osamljenih števcev se splača vgraditi števce, ki že vsebujejo GSM/GPRS modem in so sposobni direktno komunicirati z merilnim centrom. V nasprotnem primeru pa se bolj splača vgraditi koncentrator v TP SN/NN in povezati števce preko DLC do koncentratorja in nato naprej do merilnega centra preko GSM/GPRS/UMTS. Pri velikih AMI sistemih in zahtevi za pogostejše zajemanje podatkov lahko hitro pridemo do omejitev zaradi končne zmogljivosti omrežja.

ZigBee je brezžično omrežje, prilagojeno specifičnim potrebam senzorjev in drugih merilnih in kontrolnih naprav. Te specifične potrebe se izražajo predvsem ob zahtevi po zelo majhni porabi električne energije, kar omogoča baterijsko napajanje modulov in dolgo avtonomnost napajanja (običajno od več mesecev do več let) ter ob potrebi po majhnih zakasnitvah pri prenosu podatkov.

Za ZigBee omrežja je značilno, da se s pomočjo ZigBee Alliance vzpostavlja standardizirana platforma za brezžično povezavo omenjenih naprav. Do sedaj je bilo namreč na trgu kar nekaj rešitev, ki pa so bile vezane na posamezne proizvajalce in zato povezovanje naprav različnih proizvajalcev praktično ni bilo mogoče. ZigBee torej vse bolj postaja globalni standard za omrežje senzorskih, merilnih in kontrolnih naprav.

Glavne značilnosti ZigBee so:

- mala poraba energije;
- dva načina stanja: aktivno (oddaja/sprejem) in pripravljenost (sleep);
- nizka cena, enostavna namestitev in vzdrževanje;
- velika gostota ZigBee vozlišč (naprav) v omrežju, naslovni prostor do 18.450.000.000.000.000.000 naprav;
- robusten protokol (protokol je podoben Bluetooth ali 802.11, vendar okrnjen na najbolj nujno funkcionalnost);
- frekvenčno območje 868MHz (EU) oziroma 915MHz (USA, Avstralija), ter 2.4 GHz, ki postaja glavno področje za ta omrežja v vseh deželah;

- hitrost podatkov: 250kbps pri 2.4 GHz, 40kbps pri 915 MHz, 20kbps pri 868 MHz;
- CSMA/CD dostop do komunikacijskega kanala;
- različne topologije omrežja: »peer-to-peer«, zvezda, mešano;
- doseg odvisen od okolja – od 5 do 500 m, tipično 50 m;
- možnost zagotovljenega časa prenosa podatka za aplikacije, ki zahtevajo hiter odziv v predvidenem času;
- tipičen promet: periodični podatki (npr. odčitki senzorjev), ukazi (npr. vklop/izklop stikala).

Varnost podatkov je zagotovljena na več nivojih. Že na prvem nivoju OSI modela (MAC - nivo) se uporablja AES (Advanced Encription Standard), pri posredovanju podatkov preko omrežja (multi-hop messaging) pa na omrežnem – tretjem nivoju. Varnostni mehanizmi zagotavljajo zaupnost podatkov, njihovo integriteto, kot tudi avtentičnost glede na izvor oziroma cilj.

Druga omrežja

Če distribucijsko podjetje že razpolaga s svojim hrbteničnim omrežjem, na primer optičnim omrežjem, je seveda najbolje uporabiti le-tega. Za komunikacijo koncentratorjev z merilnim centrom se lahko uporabi tudi javno telefonsko omrežje (PSTN in ISDN).

CATV omrežja, ki nudijo tudi internet storitve, so lahko tudi uporabna, vendar je v tem primeru treba zagotoviti navidezno privatno povezavo in vse potrebne varnostne mehanizme ter razmisliti o kvaliteti storitve, ki jo CATV operater ponuja.

4.4 Uvajanje AMR, AMM, AMI sistemov v Evropi

AMR in AMM sistemi so se najprej uveljavili na področju sistemskih, industrijskih in obrtniških števcev. Najprej je bila razvita merilna tehnologija (Smart Meters), kasneje se je pojavila tudi ustrezna telekomunikacijska tehnologija.

V Evropi je približno 2 milijona industrijskih in obrtniških odjemalcev, od katerih je 75 % že opremljenih z AMR ali AMM tehnologijo [10]. Z uvedbo trga električne energije v Sloveniji so AMR sistemi postali obvezni na segmentu t.i. upravičenih odjemalcev (odjemalci nad 41 kW priključne moči oz. poslovni odjemalci). Merilna mesta teh odjemalcev so že

opremljena z AMR sistemi. Po številu predstavljajo le 1% vseh odjemalcev, po odjemu pa več kot 50% odjema iz distribucijskega omrežja.

V Evropi ponekod že poteka tehnološki prehod na sodobno merilno tehnologijo tudi na področju merjenja odjema gospodinjskih odjemalcev. Uporabljene tehnične rešitve AMR in AMM sistemov ter dinamike njihovega uvajanja so od države do države različne. Pogojene so z nacionalno zakonodajo, značilnostmi ekonomskega okolja, stanjem obstoječih merilnih sistemov pa tudi s kulturno tradicijo okolja.

V članicah Evropske unije poteka več projektov celovite uvedbe AMR oz. AMM sistemov na področju gospodinjskega odjema:

- ***v Italiji*** se je ENEL odločil, da bo zamenjal vseh 30 milijonov gospodinjskih števcev z novimi ter vse gospodinjske odjemalce vključil v AMM sistem. Projekt naj bi bil zaključen leta 2011,
- ***Švedska*** je do sedaj kot edina evropska država z zakonom predpisala mesečno odčitavanje vseh 5 milijonov gospodinjskih odjemalcev do leta 2009, kar je pospešilo uvedbo AMR sistemov,
- ***na Nizozemskem*** je leta 2006 stekel Nacionalni program uvedbe AMR sistemov, po 3-letni pripravi pa je leta 2009 stekel intenzivni projekt menjave števcev, ki naj bi bil končan do leta 2015;
- ***Španija se*** je odločila, da je mogoče od 1. 7. 2007 naprej vgrajevati samo še sistemske števce;
- ***Irska*** je potrdila začetek uvajanja sistemskih števcev v letu 2008;
- ***podjetje EDF (Francija)*** je v letu 2007 najavilo začetek obsežnega pilotnega projekta kot pripravo za množično vgradnjo sistemskih števcev;
- projekti uvajanja AMR in AMM sistemov so v ***Angliji, Nemčiji, Avstriji, na Danskem in v delu držav JV Evrope*** v fazi pilotnih projektov, tehničnih specifikacij in idejnih projektov [10].

Od 250 milijonov evropskih gospodinjstev je približno 15% že opremljenih z AMR ali AMM tehnologijo. V Sloveniji na področju gospodinjskega odjema prevladuje ročno odbiranje indukcijskih števcev. Obsežnega uvajanja AMR (AMI) sistemov še ni, vsa distribucijska podjetja pa že izvajajo manjše pilotne projekte, s katerimi preizkušajo razpoložljivo tehnologijo in njeno funkcionalnost.

5 UPRAVLJANJE PORABE V DISTRIBUCIJI EE

Ker se električne energije ne da shraniti v dovolj velikih količinah in za sprejemljive stroške ter jo uporabiti, ko to želimo, mora elektroenergetski sistem (EES) s proizvodnjo stalno slediti trenutni porabi. To zahteva izgradnjo večjih proizvodnih in prenosnih kapacitet, kar pa spet vpliva na ceno energije. Zato je potrebno obratovanje EES optimizirati, da se še posebej v času energetske krize bolje izkoristi obstoječa sredstva, ki so na razpolago. V optimizaciji obratovanja EES mora za uspeh sodelovati tudi stran porabe. Področje optimizacije obratovanja EES na strani porabe je bilo v času uvajanja deregulacije v glavnem zapostavljeno in tako ostaja na tem področju eden večjih potencialov v optimizaciji delovanja EES. V preteklosti smo ugotovili interes za optimizacijo na strani porabe skozi razvoj storitev in ukrepov s področja upravljanja porabe (Demand Side Management - DSM) v EES.

Podjetje Elektro Gorenjska je sprejelo odločitev, da na področju uvajanja daljinskega odčitavanja števcev prevzame vodilno vlogo v slovenskem EES, za kar gradi obsežno informacijsko infrastrukturo. Slednja za svoje kupce in poslovne partnerje odpira popolnoma nove možnosti na področju razvoja dodatnih storitev, kar si želi podjetje izkoristiti za doseganje vodilnega položaja med distribucijskimi podjetji v Sloveniji in tudi v regiji. Za izvajanje storitev in programov s področja DSM lahko s pridom izkorišča komunikacijsko infrastrukturo, ki jo gradi. Zato je vsaj ovrednotenje potencialov uvedbe DSM v podjetju na tem področju logična aktivnost.

Na koncu ne smemo pozabiti na potencialne učinke na nacionalno gospodarstvo, ki jih ukrepi DSM prinesejo z boljšim izkoriščanjem obstoječih sredstev EES in s tem znižanjem potrebe po investicijah ter posledično znižanje rasti cen energije.

5.1 Definicije posameznih področij DSM

DSM združuje vse vidike vplivanja na porabo, tu gre predvsem za vpliv zunanjih dejavnikov (na primer direktno krmiljenje upravljavca omrežja), pa tudi samoprilagajanja porabe zaradi vpliva zunanjih dejavnikov (na primer prilaganje tarifam). Področje DSM pokriva zelo široko področje vplivanja na porabo, kamor sodijo aktivnosti na področju vpliva na energetsko učinkovitost (Energy Efficiency - EE), zmanjševanje porabe (Energy Conservation - EC) in upravljanje obremenitve (Load Management - LM). Področja niso

popolnoma neodvisna, vendar dovolj, da jih lahko obravnavamo ločeno. V nalogi so poudarjeni predvsem ukrepi LM, pa tudi ostala področja, ki so v kontekstu s tem.

Temeljni pogoj za izvajanje LM programov je sposobnost porabe za odziv (Demand Response – DR) na iniciative ukrepov in programov LM. Tudi DR je razdeljen na več skupin, ki jih v grobem delimo na:

- programe, temelječe na spremenljivih cenah (Dynamic Pricing - DP),
- programe, temelječe na krmiljenju bremena (Load Control Programes – LCP),
- programe, temelječe na povratnih informacijah (Customer Feedback Programes – CFP).

V vsaki skupini je več programskih podskupin, različni viri pa v podrobnostih navajajo različne nazive tudi za glavne komponente. Da se izognemo nejasnostim, pa je pri proučevanju in navajanju posameznih ukrepov DSM potrebna previdnost.

5.2 Interes za izvajanje ukrepov DSM

Pomembno vlogo pri uveljavljanju ukrepov DSM ima država oz. zakonodajna veja oblasti, ki s sprejemanjem zakonodaje določa usmeritve na tem in drugih področjih. Zakonodajalec, ki želi uspešno izvajanje ukrepov DSM, mora odgovornost za njegovo izvajanje podeliti pravemu partnerju, to pa je tisti, ki pri izvajanju programov DSM ne trpi finančne izgube, oz. je zanj uspešno izvajanje programov »zgodba o uspehu«.

Ugotovili smo, da so ukrepi DSM usmerjeni v varčevanje z energijo, racionalno rabo energije in uporabo energije takrat, ko jo je dovolj. Naravni zmagovalci procesa varčevanja so odjemalci, proizvajalci in trgovci z energetsko varčnimi aparati in napravami. Naravni poraženci so proizvajalci električne energije, trgovci z električno energijo (manjše prodane količine), proizvajalci konvencionalnih naprav in distribucija, če je njen prihodek v največji meri odvisen od količine distribuirane energije.

Naravni DSM sistem dobimo, če izvajanje ukrepov DSM zaupamo stranki v procesu, ki je naravni zmagovalec. V Veliki Britaniji in tudi v svetu je znan Energy Saving Trust (EST), nepridobitna organizacija, katere poslanstvo je nepristransko informirati in osveščati odjemalce električne energije o varčevanju z energijo [11].

Umetni DSM sistem dobimo, kadar je izvajanje ukrepov DSM zaupano naravnemu poražencu. V tem primeru so potrebne dodatne finančne spodbude, zaradi katerih bo »naravni

poraženec« postal »zmagovalec«. Najbolj poznan umetni DSM sistem je IRP (Integrated Resource Planning) [12].

5.2.1 IRP - proces optimizacije energetskih prihrankov

IRP je proces optimizacije energetskih prihrankov celotnega energetskega sektorja od proizvodnje do porabe in je v bistvu celovito načrtovanje energetike. Začetki tega sistema segajo v ZDA, kjer je se je IRP v osemdesetih letih začel uporabljati za načrtovanje porabe električne energije. Osnovna ideja je zagotavljanje energetskih storitev pri najnižjih skupnih stroških, ki so definirani kot skupni stroški proizvodnje, prenosa, distribucije in porabnikov električne energije. Distribucijska podjetja morajo za izvajanje IRP upoštevati tako stran proizvodnje kot stran porabe.

Cena električne energije, ki jo plača končni odjemalec, ne vpliva na optimizacijo procesa IRP, saj gre za interni denarni tok: višji stroški odjemalca so hkrati višji prihodki distributerja in obratno. Glede na ceno električne energije, ki jo plačujejo končni odjemalci, pa dobimo več variant IRP:

- cena EE po uvedbi IRP lahko ostane enaka, v tem primeru distributer nosi vse stroške, nastale na strani porabe, kot tudi izgubo dobička zaradi manjših količin distribuirane energije (t.i. »goli IRP«);
- dobavitelj dvigne cene EE, da pokrije stroške DSM ukrepov, kar mora odobriti regulator trga (t.i. »zaračunavanje voda«);
- dobavitelj dvigne cene EE, da pokrije stroške DSM ukrepov in tudi izgubo zaradi manjših distribuiranih količin (t.i. zakonsko obvezen DSM);
- dobavitelj dvigne cene EE tako, da pokrije stroške, izgubo in še dodatno zasluži (t.i. spodbujeni DSM).

V evropski praksi se je IRP uvajal v začetku devetdesetih let prejšnjega stoletja, predvsem kot »goli IRP« ali »zaračunavanje voda«. V splošnem ni bilo finančnih spodbud distributerjem za izvajanje IRP. Distributerji so IRP in DSM izvajali le zardi zakonskih obveznosti, stroške pa so v celoti prevalili na odjemalce. Ker pa so si distributerji zaračunavali prevelike stroške izpada dobička, na drugi strani pa so k učinkoviti rabi električne energije, npr. s cenejšimi varčnimi aparati, veliko prispevali proizvajalci opreme, sta DSM in IRP postala sporna.

Z intenzivnim odpiranjem trga z električno energijo pa so v Evropi nastopile nove okoliščine tudi za IRP in DSM. S pojavom trgovca z EE ni več naravne povezave med proizvodnjo, prenosom, distribucijo in odjemalcem na nekem zaključenem področju. Trgovec z EE sestavlja svojo bilančno skupino po netehničnih kriterijih in kupuje EE pri različnih dobaviteljih/proizvajalcih, zato ni več mogoče ustvariti pogojev za optimiranje celotnega energetskega sistema v skladu z IRP.

5.3 Pravni in institucionalni okviri ukrepov DSM v Sloveniji

Eden od razlogov za zelo skromen razvoj na tem področju v Evropi v zadnjih letih je tudi v relativno močni pravni regulaciji sistema trga energije ter ekspanzije multinacionalk na nova in nova podjetja, kjer se sledi predvsem korporativnemu in ne toliko tehniškemu razvoju. Zato je treba pregledati zakonodajo, ki ureja to področje pri nas in ustrezno umestiti posamezne ukrepe na trg in med igralce na trgu. Definicija posameznih ukrepov je namreč neločljivo povezana z zakonodajo in tem, kaj slednja omogoča.

Reorganizacija in liberalizacija trga z EE je v poznih 90. letih v Evropi doživela velik razmah, podobno bo tudi v prihodnje. Do sedaj pa upravljanje z energijo na strani porabe ni bilo deležno zadostne pozornosti. Kljub temu so nove razmere postavile v ospredje nove poti in načine stimuliranja in iniciative za povečanje učinkovitosti v končni rabi in upravljanju energije na strani porabe. V preteklosti je bila energetska politika s strani državnih institucij večinoma usmerjana preko podjetij v državni lasti ali preko zakonodaje.

Danes je izboljšanje energetske učinkovitosti ena bistvenih komponent energetske politike v EU in njenih članicah. Ta politika temelji na upoštevanju sigurnosti dobave, ekonomiki in v prizadevanju za zaščito okolja (lokalno in globalno – podnebne spremembe) [12].

5.3.1 Energetski zakon

Pravno podlago ukrepom DSM daje Energetski zakon [13, 14] (EZ - EZ uradno prečiščeno besedilo EZ-UPB2, Ur.l. RS 27/2007 in Zakon o spremembah in dopolnitvah EZ-C, Ur.l. RS 70/2008). EZ-C v svojem 24. in 25. členu navaja spremembe 66.b in 67. člena EZ, ki določata obveznosti sistemskega operaterja: »Sistemski operaterji ter dobavitelji električne energije, toplote iz distribucijskega omrežja, plina in tekočih goriv končnim odjemalcem (v nadaljnjem besedilu: zavezanci) morajo zagotoviti prihranke energije pri končnih odjemalcih. Za doseganje prihrankov energije morajo zbirati prispevek iz prvega odstavka in dodatek iz četrtega odstavka 67. člena tega zakona ter pripraviti in izvajati programe za izboljšanje

energetske učinkovitosti.« Prvi odstavek 67. člena se glasi: »Finančna sredstva za izvajanje programov za povečanje energetske učinkovitosti rabe električne energije iz prvega in drugega odstavka 66.b člena tega zakona zagotavljajo vsi končni odjemalci električne energije, ki so dolžni za posamezno prevzemno prodajno mesto dobavitelju plačevati prispevek za povečanje učinkovitosti rabe električne energije.«

EZ torej nalaga sistemskemu operaterju izvajanje programov varčevanja energije pri končnih odjemalcih. Finančna sredstva za izvajanje programov pa zagotavljajo vsi odjemalci v obliki prispevka.

5.3.2 Nacionalni akcijski načrt za energetsko učinkovitost za obdobje 2008-2016

Ukrepe za izboljšanje učinkovitosti v končni rabi energije v Sloveniji opredeljuje *Nacionalni akcijski načrt za energetsko učinkovitost za obdobje 2008-2016 (AN-URE)* [15], ki je bil izdelan na osnovi 14. člena Direktive 2006/32/ES Evropskega parlamenta in Sveta z dne 5. aprila 2006. To je prvi od treh akcijskih načrtov. Ostala dva je potrebno izdelati v letu 2011 oziroma v letu 2014.

Direktiva 2006/32/ES zahteva od držav članic, da dosežejo 9 % prihranka končne energije v 9 letih, in sicer v obdobju 2008–2016, možno pa je uveljavljati tudi zgodnje aktivnosti od leta 1995 in v posebnih primerih od leta 1991. Z AN-URE naj bi Slovenija v obdobju 2008–2016 dosegla kumulativne prihranke v višini najmanj 9 % glede na izhodiščno rabo končne energije ali najmanj 4261 GWh.

AN-URE predvideva več naborov instrumentov:

- nabor **instrumentov za izboljšanje energetske učinkovitosti v gospodinjstvih:**
    - finančne spodbude za energetsko učinkovito obnovo stavb,
    - za energetsko učinkovite sisteme za ogrevanje,
    - za učinkovito rabo električne energije in
    - shemo učinkovite rabe energije za gospodinjstva z nizkimi prihodki;
- nabor **instrumentov za izboljšanje energetske učinkovitosti v storitvenem sektorju:**
    - finančne spodbude za energetsko učinkovito obnovo stavb in trajnostno gradnjo stavb, energetsko učinkovite sisteme za ogrevanje, učinkovito rabo električne energije,
    - ukrepi v javnem sektorju – »zelena« javna naročila,
    - javni sektor naj bi služil kot zgled izvajanja ukrepov za povečevanje energetske učinkovitosti;

- nabor **instrumentov za izboljšanje energetske učinkovitosti v industriji:**
    - sofinanciranje ukrepov učinkovite rabe električne energije za različne tehnologije (energetsko učinkoviti elektromotorji, frekvenčni pretvorniki za regulacijo vrtljajev motorjev, energetsko učinkovite črpalke in ventilatorji, energetsko učinkoviti sistemi za pripravo stisnjenega zraka, varčna razsvetljava);
- nabor **instrumentov za izboljšanje energetske učinkovitosti v prometu:**
    - promocija in konkurenčnost javnega potniškega prometa,
    - spodbujanje trajnostnega tovornega prometa,
    - povečanje energetske učinkovitosti osebnih vozil ter izgradnja kolesarskih poti in promocija kolesarjenja,
    - izgradnja in posodobitev obstoječe infrastrukture (predvsem železniškega in cestnega omrežja)
    - izobraževanje in osveščanje uporabnikov;
- nabor **večsektorskih in horizontalnih ukrepov za izboljšanje en. učinkovitosti**:
    - zakonodajni instrumenti (uveljavitev ali dopolnitev zakonodaje),
    - finančni instrumenti (dajatve in cene),
    - ostali instrumenti (promocijski in informativni) ter
    - prostovoljni sporazumi (oprostitev plačila dajatev).

AN-URE med večsektorskimi ukrepi predvideva zanimiv instrument št. 22 »Programi upravljanja rabe energije pri končnih porabnikih s strani podjetij za oskrbo z energijo (DSM)«. Detajli so navedeni v Tabeli 5.1.

Tabela 5.1: Programi DSM v dokumentu AN-URE za obdobje 2008-2016

Instrument	***22. Programi upravljanja rabe energije pri končnih porabnikih s strani podjetij za oskrbo z energijo (DSM)***
Vrsta instrumenta	• *obveznost izvajanja javne službe za energetska podjetja (sistemski operater distribucijskega omrežja)*
Ciljna skupina	• *podjetja za oskrbo z energijo vezano na omrežja*
Ukrepi učinkovite rabe energije	*Podjetja za oskrbo z energijo vezano na omrežja izvajajo projekte učinkovite rabe energije pri končnih porabnikih energije, zlasti v gospodinjstvih, storitvenem sektorju ter v malih in srednjih podjetjih v predelovalni industriji.* *Instrument bo zagotavljal izvedbo sledečih ukrepov učinkovite rabe energije:* • *Gospodinjstva: energetsko učinkovita raba EE: gospodinjski aparati, razsvetljava,* • *Storitveni sektor: energetsko učinkovita raba EE: razsvetljava, sistemi za prezračevanje in klimatizacije,* • *Večsektorski ukrep: učinkoviti sistemi ogrevanja in priprave sanitarne tople vode,*

	ukrepi energetske sanacije stavb.
Učinki	*Za izvedbo ukrepov bodo:* • *pripravljeni predpisi za izvajanje instrumenta DSM in spremljanje programov,* • *usposobljeni izvajalci,* • *vzporedno s tem izveden pilotni projekti.*
Pričakovani prihranki energije	*V tej fazi načrtovanja aktivnosti je predvideno, da se bo po obsegu okoli 10 % zgoraj navedenih ukrepov izvajalo na osnovi tega instrumenta, ostalih 90 % pa s pomočjo finančnih spodbud iz proračuna. Pri tej predpostavki znašajo prihranki predlaganih ukrepov za sektor gospodinjstva 183 GWh in za sektor storitvenih dejavnosti 96 GWh. Obseg ukrepov, ki bodo izvedeni s pomočjo tega instrumenta, bo natančneje določen pri prenosu Direktive 2006/32/ES (6. člen) v slovenski pravni red.*
Stanje in časovni potek izvedbe	*Instrument je nov in se še ni začel izvajati. Pravne podlage, ki omogočajo njegovo izvedbo, daje Energetski zakon. Stroški za izvedbo programa se lahko po pridobljenem soglasju Agencije za energijo deloma ali v celoti krijejo iz dodatkov k omrežnini v ceni za uporabo omrežij.* *Predvideno trajanje izvedbe instrumenta: 1/1/2008 do 31/12/2016*

Vir: AN-URE

5.3.3 Izvedljivi ukrepi DSM glede na slovensko zakonodajo

Nabor ukrepov DSM, ki jih predvideva slovenska zakonodaja, je trenutno omejen le na ukrepe, povezane z učinkovito rabo energije pri končnih odjemalcih, kot so:

- spodbujanje uporabe varčnih gospodinjskih aparatov in varčnih sijalk v gospodinjstvih,
- energetsko učinkovita raba električne energije za razsvetljavo, varčni sistemi za prezračevanje in klimatizacije v storitvenem sektorju,
- uporaba učinkovitih sistemov ogrevanja in priprave sanitarne tople vode,
- ukrepi energetske sanacije stavb.

Ukrepi s področja upravljanja porabe (Load Management) žal nimajo mesta v slovenski zakonodaji. Sistemski operater in lastniki distribucijskega omrežja tako nimajo zakonske podlage za izvajanje ukrepov DSM, s katerimi bi lahko bistveno vplivali na glajenje krivulje odjema in s tem izboljšali izkoriščenost in optimirali razvoj (ojačitve) omrežja. V uporabi je dvotarifni sistem merjenja električne energije pri gospodinjskih odjemalcih in merjenje konice odjema poslovnih odjemalcev, s čimer se odjemalce spodbuja k zmanjševanju odjema v času pričakovanih večjih obremenitev sistema. Neizkoriščen pa je velik potencial ukrepov, ki bodo predstavljeni v naslednjih poglavjih.

5.4 Identifikacija izvedljivih ukrepov s področja DSM

Za izvajanje storitev in programov s področja DSM se lahko s pridom izkorišča informacijsko-komunikacijsko infrastrukturo, ki se gradi, zato je vsaj ovrednotenje potencialov uvedbe DSM v našem podjetju v tem trenutku logična aktivnost. Analiza bo pokazala, katere storitve in programi so smiselni za uvedbo in kateri ne, nato pa bomo določili nadaljnje korake ravnanja na tem področju.

5.4.1 Nabor programov s področja upravljanja porabe (Load Management – LM)

Eden prvih pogojev za izvajanje LM programov je sposobnost porabe za odziv (Demand Response – DR) na iniciative ukrepov in programov LM. Tudi DR je razdeljen na več skupin, ki jih v grobem delimo takole:

- programi temelječi na spremenljivih cenah (Dynamic Pricing - DP),
- programi temelječi na krmiljenju bremena (Load Control Programes – LCP),
- programi temelječi na povratnih informacijah (Customer Feedback Programmes – CFP).

Programi, temelječi na spremenljivih cenah (Dynamic Pricing - DP)

Sistem časovno spremenljivih cen je primer cenovnega razlikovanja, pri katerem ponudnik blaga (storitve) ponuja isto blago (storitev) po različnih cenah, odvisno od časa dobave blaga ali izvedbe storitve. Časovno spremenljive cene so značilne za mnoge industrijske in storitvene panoge. V turizmu se na primer cene aranžmajev spreminjajo glede na sezono, cene telefonskih pogovorov so ponoči in ob dela prostih dnevih praviloma nižje. Cenovno razlikovanje je pogostejše v reguliranih panogah, to je v panogah, pri katerih je sezonski vpliv na povpraševanje zelo velik oz. povsod tam, kjer je elastičnost ponudbe in povpraševanja majhna. Popolnoma dereguliran trg in velika elastičnost ponudbe ter povpraševanja namreč onemogočata cenovno razlikovanje in s tem vpliv cene na povpraševanje.

Trg električne energije je kljub deklarirani odprtosti še vedno dokaj reguliran, predvsem pa je povpraševanje po električni energiji zelo neelastično, kar pomeni, da odjemalci v veliki meri niso pripravljeni ali zmožni prilagajati (zmanjševati) porabe električne energije trenutnim razmeram na trgu.

Trg električne energije pozna več modelov oblikovanja časovno spremenljivih cen, med njimi so največkrat uporabljeni: sistem tarifnih časov (TOU – time of use pricing), tarifiranje časa kritičnih koničnih obremenitev (critical peak pricing), dinamično tarifiranje (dynamic pricing, real-time pricing), spodbude za zmanjševanje konice odjema (peak load reduction credits).

Sistem tarifnih časov je v Slovenji dobro poznan in uveljavljen. Gospodinjski odjemalci lahko izbirajo med eno ali dvotarifnim merjenjem porabe električne energije. Pri slednjem je določena in uporabnikom v naprej znana cenovna razlika med električno energijo, porabljeno in izmerjeno v »cenejši« in »dražji« tarifi. Dvotarifni števec krmili stikalna ura ali sprejemnik krmilnega signala za preklop tarifnih časov. Odjemalce se na ta način spodbuja k prilagajanju odjema električne energije obdobjem cenejše tarife, ko je v sistemu praviloma na voljo dovolj električne energije. V Sloveniji se tarifni časi določajo z vladno uredbo. Trenutno je določena cenejša tarifa med 22.00 in 6.00 med delavniki, med vikendom in v dela prostih dnevih pa je določena nižja tarifa cel dan, torej od 00.00 do 24.00.

Tarifiranje časa kritičnih koničnih obremenitev je v osnovi podobno sistemu tarifnih časov, vendar določa posebne (višje!) cene električne energije za dneve, v katerih se predvideva nadpovprečna konica odjema. Konična tarifa (KT) se v Sloveniji določa izključno v časih visoke tarife, torej le ob delavnikih od ponedeljka do petka, in trajajo v visoki sezoni 6 ur dnevno ter v nizki sezoni 4 ure dnevno. Ure KT so opredeljene na temelju doseženih obremenitev v zadnjem 12-mesečnem obdobju. Določi jih upravljavec prenosnega omrežja Elektro Slovenija in objavi na svoji spletni strani. Da bi bil obračun konične tarife mogoč, mora biti odjemalec opremljen z merilno napravo, ki meri npr. 15-minutna povprečja odjema.

Dinamično tarifiranje predvideva spreminjanje cene električne energije tako, da se cena, ki jo plača odjemalec, kar najbolj prilagaja proizvodni oz. prodajni ceni električne energije. Predpogoj za delovanje sistema pa je sistem »pametnih števcev« (Smart Metering, AMI, AMR, AMM), preko katerega se odjemalcu v realnem času sporoča trenutno ceno električne energije.

Spodbude za zmanjševanje konice odjema so namenjene predvsem večjim odjemalcem električne energije. Cilj je spodbujati večje odjemalce, da prilagodijo svoj odjem tako, da v čim večji meri zmanjšajo konico svojega odjema, kar prispeva k zmanjševanju konice v sistemu in posledično zmanjšuje potrebo po proizvodnji vršne energije oz. ojačitvi prenosnega in distribucijskega omrežja. V Sloveniji je za večje odjemalce (nad 41 kW) uveden sistem merjenja konice odjema. Obračunska moč se ugotavlja mesečno na podlagi konične

obremenitve pri končnem odjemalcu z merilno napravo, ki evidentira 15-minutne meritve in omogoča lokalni prikaz obračunskih vrednosti, ločeno po tarifnih časih, kot povprečje treh najvišjih 15-minutnih povprečnih moči v obračunskem mesecu v urah KT oziroma v urah VT, kjer se KT ne meri. Časovne intervale KT določa sistemski operater prenosnega omrežja (Eles) na svoji spletni strani, glede na pričakovane razmere v prenosnem omrežju.

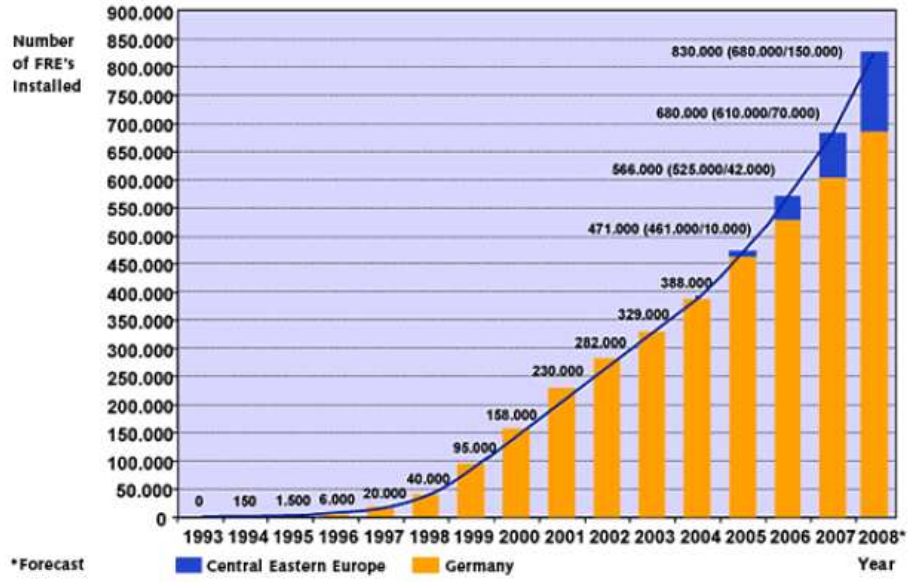
Programi, temelječi na upravljanju bremena (Load Control Programes - LCP)

Krmiljenje bremena (Load Control) je ena od možnosti, ki jo v svetu uporabljajo operaterji omrežja za zagotavljanje ravnovesja med razpoložljivo in potrebno električno energijo. Posamezni porabniki električne energije, kot so hladilni sistemi, črpalke vodnih rezervoarjev, grelniki vode … delujejo občasno in ne nujno takrat, ko je odjem v sistemu največji, to je v času konice odjema. Odjemalec in operater distribucijskega omrežja lahko vzpostavita sistem za daljinsko vodenje posameznih prej navedenih porabnikov električne energije, ki omogoča operaterju vklop in izklop posameznih bremen v omrežju, glede na trenutne razmere v sistemu. Odjemalcu, ki operaterju omogoči krmiljenje njegovih porabnikov, operater zaračuna tako porabljeno električno energijo po ugodnejši ceni.

Operater distribucijskega omrežja s pomočjo krmiljenja določenega števila bremen v omrežju po potrebi gladi krivuljo odjema in zmanjšuje konico odjema ter prioritetno razbremenjuje omrežje tam, kjer je to zaradi razmer v omrežju potrebno. Operater se na ta način lažje izogne nevarnostim razpada omrežja ali pa izravnava odstopanja napovedanega odjema.

Krmiljenje bremen ima že dolgo zgodovino in mnoge uspešne implementacije. Že v štiridesetih letih prejšnjega stoletja so se pojavili sistemi za prenos krmilnih signalov po energetskih vodih (“Ripple Control” System), danes pa se uporablja tako radijsko krmiljenje bremen kot tudi komunikacija po energetskih vodih. Sodobni AMI sistemi ravno tako omogočajo krmiljenje posameznih bremen [16].

Trenutno naj bi največji sistem krmiljenja gospodinjskih odjemalcev deloval na Floridi, kjer je nameščenih več kot 800.000 krmilnikov bremen, ki omogočajo krmiljenje 1.000 MW moči oz. 2.000 MW v izrednih razmerah. Tudi v Nemčiji naj bi bilo leta 2008 že 680.000 bremen opremljenih z radijsko vodenimi stikali za daljinski vklop/izklop bremena (Slika 5.1).



Slika 5.1: Rast števila radijsko vodenih bremen (EFR – Europaische Funk-RundSteuerung)

Programi temelječi na povratnih informacijah (Customer Feedback Prog. – CFP)

Eden od načinov spodbujanja uporabnikov k varčevanju z energijo so tudi povratne informacije odjemalcu o njegovem trenutnem odjemu, stroških električne energije, strukturi virov porabljene energije in okoljskim obremenitvam, ki jih trenutni odjem električne energije povzroča.

Rezultati pilotnih testov in opravljene raziskave v eni od držav so pokazali, da je 70 % majhnih odjemalcev (gospodinjstev) pripravljenih na spremembe, ki prinašajo prihranke električne energije, če spremembe ne bi preveč vplivale na njihove navade. Na ta način je bilo doseženo zmanjšanje odjema električne energije za približno 10 % [17].

Raziskave [18] nadalje kažejo na vprašljivost stalnega merjenja porabe električne energije in kreiranja individualnih sporočil, saj je naložba v tovrsten sistem zelo visoka. Obstaja sicer možnost izkoriščanja sodobnih AMI sistemov, vendar pa v tem primeru ne bi mogli pričakovati dodatnih prihrankov v enakem obsegu. Cenovno zelo ugoden in dokaj učinkovit pa se kaže sistem neposrednih stikov z odjemalci z intervjuji ali pa komunikacija preko spletnih strani – spletnih anket, ki imajo svetovalni značaj. Prav tako so se kot uspešna izkazala sporočila, ki spodbujajo k nakupu in uporabi energetsko učinkovitejših naprav in k učinkovitejši rabi električne energije nasploh.

5.5 Interes odjemalcev EE za sodelovanje v ukrepih DSM

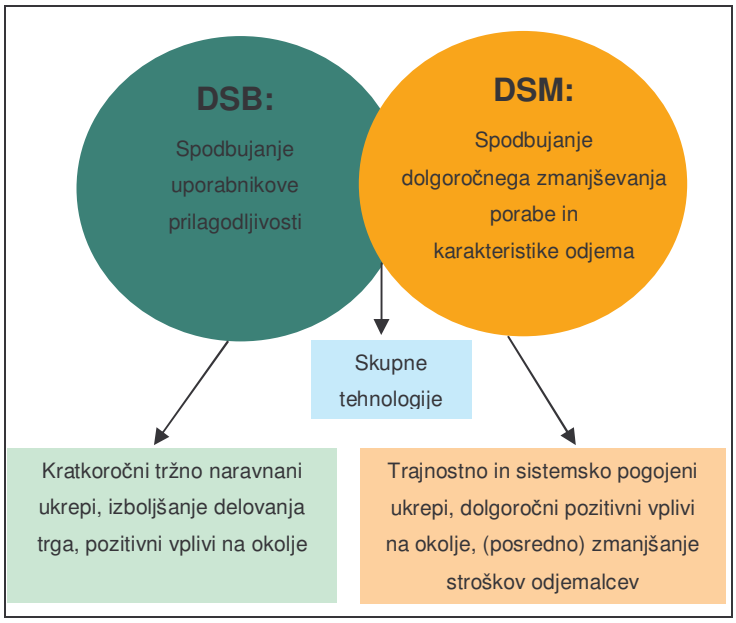
V prejšnjih poglavjih je bil večkrat poudarjen ključen pomen pripravljenosti odjemalcev za sodelovanje v programih DSM. Za uspeh ukrepov DSM je pomembno odkriti tiste mehanizme, ki bodo odjemalce spodbudili k sodelovanju v programih DSM. Seveda pa lahko na odnos med operaterjem omrežja in odjemalcem električne energije gledamo tudi drugače. Vprašajmo se, kaj lahko odjemalec s področja DSM ***ponudi*** operaterju omrežja. V tuji literaturi se za tovrstno ponudbo uporablja izraz Demand Side Bidding (DSB).

5.5.1 Ponudba odjemalcev s področja DSM – Demand Side Bidding (DSB)

Demand Side Bidding (DSB) [19] obravnava sistem vzpodbud odjemalcem električne energije, da se aktivno vključijo v (tržno) ponujanje svoje pripravljenosti za spreminjanje svojih navad povezanih z porabo električne energije. Odjemalci tako ***ponudijo*** operaterju svojo pripravljenost za sodelovanje v programih DSM, za kar so finančno ali kako drugače nagrajeni. Finančne vzpodbude se lahko nanašajo na znižanje cene električne energije (tarife), na direktna plačila za energijo, ki ni bila porabljena v času koničnih obremenitev omrežja, ali pa na znižanje plačila za odjemalčevo pripravljenost na prilagoditev odjema (daljinsko krmiljenje bremen). Marsikje v svetu se pojavlja »ponudba« pripravljenosti za prilagajanja odjema kot tržno blago, pojavljajo pa se tudi posredniki (organizatorji) trga.

Večinoma DSB razumemo kot način, kako lahko odjemalci zaslužijo oziroma privarčujejo denarna sredstva. Po drugi strani igra DSB pomembno vlogo tudi pri spodbujanju energetske učinkovitosti. DSB je lahko alternativa vključevanju sistemskih rezerv oziroma gradnji novih proizvodnih virov in ojačitvi prenosnih in distribucijskih omrežij, saj se konice v sistemu običajno pojavljajo v zelo omejenih časovnih obdobjih.

Pri obravnavanju DSB je potrebno poudariti, v čem se razlikuje od DSM. Temeljni cilj je seveda isti – uskladiti proizvodnjo, porabo in prenosne zmogljivosti sistema tako, da bo s kar najmanjšimi investicijami v sistem ter s čim manjšimi vplivi na okolje mogoče zadovoljiti potrebe odjemalcev električne energije. Razlika pa je v pristopu, saj DSB izhaja iz interesa odjemalcev, DSM pa iz interesa sistema. Temeljna naloga celovitega pristopa pa je ravno v uskladitvi interesov tako odjemalcev, kot sistema (Slika 5.2). Bistvo DSB je v spodbujanju uporabnikove prilagodljivosti sistemu in iskanje vzvodov za povečevanje odjemalčeve prilagodljivosti.



Slika 5.2: Primerjava med DSB in DSM

5.5.2 Vloga DSB kot tržnega mehanizma

Usklajevanje proizvodnje in odjema lahko razumemo kot aktivnost v realnem času in kot nalogo znotraj obdobja trgovanja:

- v realnem času je potrebno usklajevati trenutne potrebe odjemalcev in proizvodne zmogljivosti, obenem pa imeti na voljo dovolj zmogljivo in zanesljivo prenosno in distribucijsko omrežje; posledice trenutne neusklajenosti v sistemu se odrazijo kot ne*stabilnost sistema*;
- *planirano usklajevanje* znotraj obdobja trgovanja (napoved odjema); odstopanja povzročijo finančne obveznosti večjih odjemalcev do trgovca z električno energijo oziroma trgovca do proizvajalca električne energije ali dobavitelja na debelo (odstopanja bilančne skupine od voznih redov).

Zagotavljanje stabilnosti sistema je naloga sistemskih operatorjev prenosnega in distribucijskega omrežja. Planirano usklajevanje poteka po pravilih delovanja trga na relaciji med trgovci in proizvajalci električne energije. Pri usklajevanju morajo seveda upoštevati (trenutne) omejitve, ki jih narekuje stanje prenosnega in distribucijskega omrežja.

DSB in zagotavljanje stabilnosti omrežja

Odjemalci lahko ponudijo sistemskim operaterjem storitve, s katerimi operaterju pomagajo vzdrževati stabilnost sistema. Ena od nalog sistemskega operaterja je vzdrževanje frekvence izmeničnega toka v omrežju. V primeru izpada večje proizvodne enote ali zelo hitrega in nepredvidenega povečanja odjema električne energije, se elektroenergetski sistem odzove z znižanjem frekvence v sistemu. Sistemski operater mora nemudoma zagotoviti ravnotežje med proizvodnjo in odjemom, za kar ima dve možnosti: zagotovitev dodatnih (rezervnih) proizvodnih kapacitet ali pa razbremenitev omrežja. V kontekstu DSB nas torej zanima, kaj lahko odjemalci (proizvajalci) ponudijo sistemskemu operaterju za zagotavljanje stabilnosti sistema.

V Veliki Britaniji že več let uspešno deluje sistem razbremenjevanja omrežja z izklapljanjem postrojev za proizvodnjo cementa [19]. V sistem je vključenih trinajst cementarn, ki omogočajo zmanjšanje obremenitve skupne moči do 110 MW. Proces mletja v proizvodnji cementa je namreč zelo enostaven in ga je brez škode mogoče zaustaviti in ponovno zagnati.

Za sistemskega operaterja je seveda ključnega pomena zanesljivost storitve razbremenjevanja, prav tako pa potencial »negativne moči«, ki je na razpolago. Sama odzivnost odjemalcev je v veliki meri pogojena z naravo (proizvodnega) procesa, za katerega se porablja električna energija. Na splošno odjemalci čutijo prekinitve dobave električne energije kot moteč in nezaželen pojav. Vsekakor sistemski operater prenosnega omrežja v trenutku, ko potrebuje razbremenitev omrežja za nekaj deset ali sto MW težko dogovarja z množico odjemalcev, ki nastopajo kot ponudniki razbremenjevanja. Vlogo posrednika lahko prevzame trgovec z električno energijo ali pa operater distribucijskega omrežja. Ključno pri tem je poznavanje trga z električno energijo, značilnosti odjemalčevih proizvodnih procesov in obvladovanje merilno komunikacijskih tehnologij, s katerimi se zagotavlja daljinsko krmiljenje bremen.

DSB in usklajevanje voznih redov

Trgovci z električno energijo oblikujejo t.i. bilančne skupine odjemalcev. Vsota pričakovanih diagramov odjema vseh odjemalcev v bilančni skupini je osnova za napoved odjema električne energije od proizvajalcev oziroma dobaviteljev električne energije na debelo. Pripravljenost odjemalcev, da prilagajajo svoj diagram odjema tako, da trgovec uspe natančno slediti svojim napovedim, je lahko predmet pogodbenega odnosa med trgovcem in

odjemalcem. Pri tem se moramo zavedati, da bilančne skupine praviloma niso identične skupini odjemalcev na posameznem delu distribucijskega omrežja.

Cena električne energije na trgu je odvisna tudi od zasedenosti proizvodnih kapacitet. Trgovci si prizadevajo prodati čim več pasovne energije, t.j. konstantnega odjema v daljšem časovnem obdobju, saj je cena te energije na trgu najnižja. Z vidika DSB je v pomembna odjemalčeva pripravljenost, da svoj odjem prilagoditi cenejšim »oblikam« energije, to je v čim večji meri poskrbeti za stalen odjem, brez večjih konic v odjemu.

5.5.3 Priložnosti in izzivi aktivnega vključevanja odjemalcev v ukrepe DSM

Interes odjemalcev za sodelovanje je ključen za uspeh DSM. Brez pripravljenosti odjemalcev, da se odzovejo na potrebo po prilagoditvi odjema, ukrepi DSM ne morejo delovati. V okviru DSB poskušamo ugotoviti, kaj so odjemalci pripravljeni ponuditi sistemskim operaterjem in trgovcem v smislu prilagajanja svojih potreb po električni energiji in kaj za to pričakujejo. Pri tem se je potrebno zavedati, da ponujanje »storitev« prilagajanja odjema ni in ne more biti glavna dejavnost odjemalcev. Odjemalci bodo pripravljeni sodelovati le:

- če bodo finančne spodbude za sodelovanje v ukrepih DSM dovolj velike in/ali
- če ukrepi ne bodo bistveno vplivali na njihov proizvodni proces ali življenjske navade.

Večje kot bodo finančne spodbude, več sprememb v procesih oziroma navadah bodo odjemalci pripravljeni sprejeti. Vsekakor pa ima vsak odjemalec drugačno razumevanje sprejemljivosti prilagajanja odjema. Že gospodinjski odjemalci zelo različno dojemamo npr. možnost, da bi nam operater daljinsko izključil gretje sanitarne vode. Vsi odjemalci tudi nismo pripravljeni likati perila samo ob vikendih ali pozno zvečer, samo ponoči prati perilo ali pomivati posodo v pomivalnem stroju. Lahko se vprašamo, kakšna bi morala biti finančna spodbuda, da bi dopustili možnost, da ne bi imeli vsak trenutek na voljo dovolj tople vode za tuširanje oz. ali smo se pripravljeni v izrednih situacijah okopati v mrzli vodi. Ob tem ne moremo mimo dejstva, da je povprečni račun celotnega gospodinjstva za električno energijo nižji od stroškov mobilne telefonije in da bi bila finančna spodbuda za sodelovanje v ukrepih DSM lahko le nekaj (deset) odstotkov celotnega računa.

Posamezni gospodinjski odjemalec ne more samostojno nastopati kot ponudnik prilagodljivega odjema do sistemskega operaterja, zato je ključno vprašanje, kdo prevzame

vlogo združevanja potencialov, ki jih predstavljajo posamezni odjemalci. Za to so potrebni sodobni informacijsko-komunikacijski sistemi (IKS), kot je bilo prikazano v predhodnih poglavjih. Aktivno vlogo lahko prevzamejo trgovci z električno energijo, če razpolagajo z potrebnim IKS, ali pa lastniki (operaterji) distribucijskega omrežja.

Možnost in pripravljenost prilagajanja večjih odjemalcev sta odvisni predvsem od njihovega proizvodnega procesa. Odjemalec mora imeti možnost, da odjem (dela) električne energije občasno ustavi. Obstaja več možnosti:

- brez spremembe procesa (prekinitev),
- sprememba izvajanja procesa,
- sprememba samega procesa.

Proces proizvodnje lahko popolnoma prekinemo. Včasih se odjemalci odločijo, da zaradi cene vhodnih surovin in/ali energije sama proizvodnja ni rentabilna. Rezultat je lahko izgubljena proizvodnja ali pa je le-ta nadomeščena kasneje, kar pa pogosto zaradi večjega odjema ob zagonu velikih porabnikov povzroča dodatne konice v sistemu.

Proizvodni proces lahko izvajamo tudi s spremembo energenta. Tako lahko za ogrevanje uporabimo alternativne vire energije, velik potencial na tem področju predstavljajo kogeneracijski postroji. Poleg tega lahko sistemom hlajenja in ogrevanja določimo večje tolerančno območje, s čimer lahko podaljšamo čas izklopa teh bremen takrat, ko je to potrebno. Paziti pa moramo na povečanje izgub zaradi neoptimalnega obratovanja in se vprašati, kako to vpliva na rezultat procesa (odstopanja od želenih vrednosti morajo ostati v mejah dopustnega).

Za večje in dolgotrajnejše učinke pa je potrebno spremeniti sam proces. V procesu moramo poiskati načine za shranjevanje energije. Kot primer lahko navedeno hranilnike toplote (toplotno izolirane posode za shranjevanje tople vode) in hranilnike hladu (»banke« ledu), skladiščenje energijsko potratnih polizdelkov, zalogovnike materiala, ki jih ne polnimo času konic sistema (npr. mestni vodni stolpi) ipd.

Večji odjemalci imajo praviloma več možnosti za prilagajanje svojega odjema kot gospodinjski odjemalci, se pa med seboj tudi močno razlikujejo glede na možnosti prilagajanja odjema in stroškov prilagajanja, vplivajo pa tudi na spremembo procesov, ki bi omogočili povečati prilagodljivost odjema. V splošnem pa velja, da bo vsak odjemalec posebej presojal prednosti in slabosti vključitve v programe DSM.

5.6 Trg z EE in interes trgovcev z EE za ukrepe DSM

V Sloveniji se je trg z električno energijo odpiral postopoma. Proces se je začel leta 1999 s sprejetjem Energetskega zakona, zaključil pa 1. julija 2007, ko so tudi gospodinjski odjemalci lahko začeli prosto izbirati dobavitelja električne energije. Število ponudnikov električne energije se je ves ta čas povečevalo. V letu 2008 in 2009 se je okrepil boj med ponudniki električne energije tudi za segment gospodinjskih odjemalcev. V bližnji prihodnosti se načrtuje tudi pravna ločitev trgovskega dela petih distribucijskih podjetij, s čimer bodo prav gotovo nastopile večje spremembe na trgu z električno energijo.

5.6.1 Interes trgovcev z električno energijo za sodelovanje v ukrepih DSM

Pod pritiskom konkurenčnega boja med številnimi trgovci z električno energijo na dokaj zaprtem in omejenem slovenskem trgu se dejavnost trgovcev vedno bolj osredotoča na samo trgovanje. Glavno vodilo je dobiček, generator pa razlika med nakupno in prodajno ceno električne energije, pri čemer se mora trgovec v čim večji meri izogniti odstopanjem med napovedjo prevzema električne energije in dejansko prodajo električne energije. Vedno bolj izpopolnjeni načini za napovedovanje odjema upoštevajo čas, dnevne značilnosti (praznik, delavnik, sobota, nedelja …), meteorološke podatke itd.

Z razmahom telemetričnih meritev električne energije bodo trgovci za svoje bilančne skupine lahko z izredno natančnostjo napovedovali odjem električne energije. V bližnji prihodnosti lahko pričakujemo, da bo trgovec sposoben napovedovati odjem zelo natančno in v realnem času. Vprašamo se lahko, zakaj bi trgovca z električno energijo sploh zanimalo uvajanje ukrepov DSM, ki bi zmanjševali količino prodane električne energije, ali zakaj bi spodbujali glajenje konic odjema posameznih odjemalcev. Spodbujanje racionalne rabe električne energije je v nasprotju z interesom trgovca po prodaji čim večjih količin električne energije; spodbujanje racionalne rabe električne energije je lahko le marketinško orodje.

5.7 Ukrepi DSM in njihov vpliv na zanesljivost dobave EE

Ena od poglavitnih nalog SODO je zagotavljanje zanesljive in kakovostne oskrbe z električno energijo vsem odjemalcem po sprejemljivih cenah. Distribucijsko omrežje mora biti zgrajeno in vzdrževano tako, da zagotavlja zanesljivo obratovanje v normalnih in izrednih

razmerah ter v primeru okvar hitro odpravo le-teh in vzpostavitev normalnega obratovalnega stanja.

5.7.1 Kriteriji in metodologija načrtovanja distribucijskega omrežja

Načrtovanje razvoja distribucijskega EE omrežja mora upoštevati tehnične, zanesljivostne, ekonomske in okoljevarstvene kriterije, ki zagotavljajo dolgoročno optimalen razvoj omrežja [18]. Načrtovanje razvoja tako temelji na:

- napovedi porabe obremenitev,
- podatkih o obstoječem stanju sistema (omrežje, transformacija, obremenitve in poraba),
- kriterijih načrtovanja, ki omogočajo zagotavljanje ustrezne kakovosti oskrbe z EE,
- gospodarnosti v smislu načrtovanja, gradnje in obratovanja omrežja,
- vključevanju razpršene proizvodnje električne energije v omrežje.

Cilj ukrepov DSM z vidika načrtovanja distribucijskega omrežja je predvsem zmanjšanje konične obremenitve omrežja oziroma delov distribucijskega omrežja. Zato podrobneje poglejmo kriterije obremenljivosti omrežja z vidika načrtovanja omrežja.

Kriteriji načrtovanja omrežja

Med kriteriji načrtovanja distribucijskega omrežja so z vidika obravnave DSM še posebej zanimivi kriteriji obremenjevanja transformacije in omrežij SN, NN, dopustni padci napetosti in nenazadnje kriteriji usmerjene rabe električne energije.

Obremenjevanje energetskih transformatorjev 110 kV/SN v normalnih obratovalnih stanjih nikoli ne sme doseči nazivne moči, ker je potrebno zagotavljati rezervo ob izpadih transformatorjev. Razvoj SN omrežij je najpogosteje takšen, da so RTP povezani na SN nivoju, vendar je možnost zagotavljanja rezervnega napajanja ob izpadih transformatorjev preko SN omrežij omejena zaradi preseganja dopustnih padcev napetosti in (ali) šibkega omrežja. Rezervo za izpadli transformator zagotavljamo v samem RTP, zato so dopustne obremenitve transformatorjev v RTP z dvema transformatorjema do 60 % nazivne moči in v RTP s tremi transformatorji do 80 % nazivne moči.

Obremenjevanje SN vodov je omejeno z termično mejo, ki jo je zaradi velikih izgub dopustno doseči le v primerih rezervnega obratovanja. Dopustne obremenitve v normalnih obratovalnih stanjih so različne, odvisne od padcev napetosti in zagotavljanja rezervnega napajalnega stanja; kabelsko omrežje, grajeno po principu odprte zanke, ni mogoče

obremeniti več kot za 50 % termične moči. Pri načrtovanju obremenitve vodov v normalnih stanjih se zardi stroškov izgub omejimo na 50 % termične meje pri nadzemnih vodih in 75 % termične meje posamično radialno položenih kablov.

Dopustni padci napetosti v SN omrežjih so temeljni kriterij v načrtovanju distribucijskih omrežij. S pravilno določenimi dopustnimi padci napetosti omogočimo zagotavljanje napetosti pri porabnikih v predpisanih mejah ter posredno opredelimo nivo izgub v omrežju. Močnejše omrežje je manj občutljivo na motnje in popačenje napetosti, zato imajo dopustni padci napetosti tudi vpliv na kakovost napetosti, ki jo je omrežje sposobno zagotavljati. V načrtovanju SN omrežij upoštevamo v normalnih obratovalnih stanjih največji padec napetosti za 7,5 %. Za NN se pri odjemalcu priporoča odklon največ 5 % napetosti. V rezervnih stanjih napajanja upoštevamo, da je napetost lahko za 5 % nižja od najnižje dovoljene v normalnih stanjih.

Kriteriji usmerjene rabe električne energije skladno z Razvojnim načrtom distribucijskega omrežja v Sloveniji za obdobje 2009 do 2018 ***niso kriterij načrtovanja omrežij***. V razvojnem načrtu se sicer omenjajo programi usmerjene rabe energije pri končnih odjemalcih iz AN-URE za obdobje 2008 do 2016, po katerih naj bi pri končnih odjemalcih prihranili 279 GWh energije (vse, ne le električne). Če bi s temi ukrepi dejansko uspeli zmanjšati porabo električne energije na nekem območju ali pa bi njihovo porabo premaknili v čas, ko je obremenitev omrežja minimalna, bi dejansko dosegli znižanje konične obremenitve omrežja. Načrtovane ojačitve omrežja bi na takih področjih lahko premaknili v kasnejše obdobje, dokler se konične obremenitve ne bi približale napovedanim vrednostim. Izdelovalec razvojnega načrta 2009 do 2018, SODO d.o.o. pa dvomi v zanesljivost uspeha teh ukrepov. Ker je tveganje nepravočasne ojačitve omrežja po njegovem mnenju preveliko, prihrankov ni upošteval v izračunih potrebnih ojačitev omrežja.

5.7.2 Vpliv programov DSM na spremembe načrtovanja distribucijskega omrežja

V poglavju 5.7.1 smo ugotovili, da metodologija in kriteriji načrtovanja slovenskega distribucijskega omrežja ne upoštevajo ukrepov DSM; posledično sistemski operater oziroma lastniki omrežja DSM ne posvečajo velike pozornosti.

Tudi v tujini ugotavljajo zanemarjanje potenciala DSM pri načrtovanju omrežij. V mednarodni raziskavi [21], ki je vključevala Avstralijo, Francijo, Indijo, Novo Zelandijo, Južno Afriko, Španijo in ZDA so ugotovljene velike razlike v pristopu k načrtovanju omrežij, saj je tudi zakonodaja in organiziranost energetskega sektorja v obravnavanih državah zelo

različna, pilotni projekti DSM obstajajo, nikjer pa ukrepi DSM niso sistematično vključeni v načrtovanje omrežij. Hkrati pa raziskava podaja nekaj koristnih smernic za sistematično vključitev ukrepov DSM v kriterije načrtovanja omrežij:

- **napovedovanje bodočega odjema električne energije** mora v (večji meri) upoštevati potencial ukrepov DSM; napovedovanje bodočega odjema mora bolj ažurno upoštevati pozitivne učinke ukrepov DSM;
- **objavljanje informacij o zasedenosti (posameznih delov) omrežja** daje tudi drugim akterjem možnost, da premislijo o alternativah širitvi omrežja; prepogosto se namreč dogaja, da lastniki ali operaterji omrežij nimajo znanja ali interesa za ukrepe DSM in se raje odločajo za dražjo ojačitev omrežja;
- **razvoj ukrepov za zmanjševanje zamašitev omrežja;** operaterji ali lastniki omrežij bi morali omogočiti sodelovanje pri razvoju načinov za preprečevanje zamašitev v omrežju tretjim osebam z izkušnjami na področju;
- **vzpostavitev zakonodajnega okvira,** ki bo lastnike in operaterje omrežij spodbujal ali (in) prisilil k razvoju in upoštevanju neizkoriščenega potenciala ukrepov DSM.

5.7.3 Ukrepi DSM za kratkoročno in dolgoročno zmanjšanje obremenitev omrežja

Z ukrepi DSM lahko povečamo zanesljivost omrežja in zmanjšamo potrebo po ojačitvah omrežja. Omrežje mora biti grajeno in vzdrževano tako, da v vsakem trenutku zagotavlja kakovost distribucije električne energije vsem uporabnikom omrežja. Elektroenergetske naprave morajo biti dimenzionirane na konične obremenitve, čeprav se konica v sistemu pojavi malokrat in le za kratek čas. Temeljna cilja ukrepov DSM s stališča operaterja omrežja sta:

- preprečiti preobremenitve omrežja na ekonomsko sprejemljivejši način kot je investiranje v ojačitev omrežja in /ali
- omogočiti sistemskemu operaterju storitve, ki z različnim odzivnim časom pomagajo zmanjšati konične obremenitve omrežja.

Cilja je mogoče doseči z naslednjimi ukrepi DSM oz. njihovimi kombinacijami:

- daljinsko krmiljenje bremena,
- distribuirani viri energije, vključno s kogeneracijami in rezervnimi generatorji,
- hranilniki energije,

- odziv odjemalcev na zahtevo po zmanjšanju odjema,
- izboljšanje energetske učinkovitosti,
- zamenjava energenta,
- premik krivulje odjema,
- tarifne spodbude za glajenje krivulje odjema.

V nadaljevanju so najpomembnejši med njimi na kratko predstavljeni.

Daljinsko krmiljenje bremena

Pri daljinskem krmiljenju odjemalec v zameno za pogodbeno dogovorjene ugodnosti (npr. nižja tarifa) dovoli operaterju omrežja direktno krmiljenje (vklop/izklop) nekaterih njegovih porabnikov, npr. klimatske naprave, grelnike vode …

Daljinsko krmiljenje bremena omogoča operaterju omrežja trenutno zmanjšanje obremenitve celotnega omrežja, delov omrežja (izvodov SN) in celo posameznih elementov v omrežju (TP, NN priključek), pa tudi izvajanje mnogih drugih storitev za izboljšanje napetostnih razmer v omrežju (regulacija napetosti, zmanjšanje neravnotežja, frekvenčni odziv …). Ključna prednost daljinskega krmiljenja je v veliki hitrosti odziva, saj vklop/izklop ni odvisen od sodelovanja odjemalca in njegovega odzivnega časa.

Uspešnost uvedbe daljinskega krmiljenja je odvisna predvsem od interesa lastnika oziroma operaterja omrežja. Ta interes pa v veliki meri kroji zakonodaja in regulatorni sistem v državi, ki pa v Sloveniji žal (še) ne spodbuja uvedbe daljinskega krmiljenja bremen.

Predpogoj za izvajanje daljinskega krmiljenja bremen pa je IKT infrastruktura, predstavljena v poglavju 5.8.

Distribuirani viri energije, hranilniki energije

Distribuirani viri so manjše proizvodne enote električne energije, priključene direktno na distribucijsko omrežje. Njihova koristna lastnost je injeciranje električne energije v neposredni bližini porabnika in na ta način lahko distribuirani vir zmanjša odjem na delu omrežja, na katerega je priključen.

Velik potencial na tem področju so zagotovo hranilniki energije, ki se v zadnjem času tehnološko pospešeno izpopolnjujejo. Njihova odlična lastnost je sposobnost oddajanja energije, ko je to potrebno in odjema takrat, ko je energije dovolj (oz. preveč). Številčnost

hranilnikov energije se bo zagotovo enormno povečala s pojavom komercialno zanimivih električnih avtomobilov.

Trajno delujoči distribuirani viri zmanjšujejo celotno obremenitev dela omrežja na daljši rok. Rezervne generatorske enote, ki se vključujejo le po potrebi, pa lahko služijo za trenutno zmanjševanje konice odjema. Distribuirana proizvodnja ob tem zmanjšuje tudi izgube v omrežju, pravilno krmiljena lahko pomaga vzdrževati ustrezne napetostne razmere na koncu dolgih vodov.

Uspeh tega ukrepa je odvisen od odločitve lastnika oz. operaterja omrežja, da distribuiran vir prepozna kot alternativo ojačitvi omrežja. Kot je razloženo v poglavju 5.7.1. pa so v Sloveniji pri načrtovanju omrežja uporabljeni bolj konzervativni kriteriji, kar je sicer varneje, a dražje.

Zamenjava energenta in izboljšanje energetske učinkovitosti

Pojem energetska učinkovitost se nanaša na količino električne energije, ki jo odjemalec porabi za izdelavo enote izdelka ali storitve. Z vidika DSM in operaterja (lastnika) omrežja ima izboljšanje energetske učinkovitosti blagodejen učinek na zmanjšanje obremenitve omrežja. Podobne učinke na razmere v omrežju lahko dosežemo tudi z zamenjavo energenta, npr. ogrevanje sanitarne vode s sončnimi kolektorji namesto z električno energijo.

Zamenjava energenta in izboljšanje energetske učinkovitosti sta po drugi strani ukrepa, ki delujeta na dolgi rok. Od teh ukrepov ne moremo pričakovati trenutnega (hitrega) odziva kot pri daljinsko krmiljenih bremenih ali generatorjih, zato tudi niso primerni za zmanjševanje trenutne konice v sistemu ali za izvajanje drugih storitev na omrežju.

Spodbujanje učinkovite rabe električne energije je v Sloveniji zakonsko določena obveznost. Po drugi strani pa, dokler so prihodki lastnikov omrežja v veliki meri odvisni tudi od količine distribuirane energije, ni pričakovati pretiranega (in iskrenega) navdušenja za spodbujanje energetske učinkovitosti in zamenjave energenta.

Odziv porabe na zahtevo po zmanjšanju odjema

Odziv porabe razumemo kot reakcijo odjemalcev na zahtevo operaterja/lastnika omrežja na zahtevo po zmanjšanju obremenitve omrežja. Odziv porabe omogoča zmanjšanje obremenitve celotnega omrežja ali delov omrežja, vpliva pa tudi na izvajanje drugih storitev za izboljšanje razmer v omrežju (npr. regulacija napetosti, zmanjšanje neravnotežja …).

Uspešnost ukrepa je v veliki meri odvisna od hitrosti in zanesljivosti odziva odjemalcev. Operater/lastnik omrežja, glede na razmere v omrežju, po potrebi posreduje odjemalcem

zahtevo po zmanjšanju (povečanju) odjema. Če se odjemalec odzove v skladu z zahtevo, je deležen določenih (finančnih) ugodnosti. Uspešnost ukrepa je odvisna predvsem od interesa lastnika oziroma operaterja omrežja, ta pa je pogojen z zakonodajnim okvirom in regulatornim sistemom.

Predpogoj za izvajanje odziva porabe je IKT infrastruktura, predstavljena v poglavju 5.8.

Premik krivulje odjema in tarifne spodbude za glajenje krivulje odjema

Premik krivulje odjema (Load Shifting) zahteva spremembo navad odjemalca električne energije tako, da bo odjem električne energije v čim večji meri prenesel iz obdobij pričakovanih koničnih obremenitev omrežja v obdobje manjše obremenitve.

Konične obremenitve omrežja ne sovpadajo vedno in popolnoma s konico odjema celotnega omrežja, zato je cilj ukrepa lahko zmanjševanje konične obremenitve celotnega omrežja, posameznega geografskega območja ali celo posameznega elementa v omrežju. S premikom krivulje odjema lahko izvajamo tudi mnoge druge storitve za izboljšanje napetostnih razmer v omrežju (regulacija napetosti, zmanjšanje neravnotežja, frekvenčni odziv …). Tudi pri tem ukrepu je uspeh odvisen predvsem od hitrosti odziva odjemalcev na zahtevo po premaknitvi krivulje odjema.

Običajen način spodbujanja odjemalcev za premik krivulje odjema so tarifne spodbude. V Sloveniji je v uporabi dvotarifno merjenje, s fiksnimi tarifnimi časi. EDF (Francija) uporablja zanimiv način označevanja tarifnih obdobij z »nacionalnimi« barvami: bela – brez omejitev, najnižja cena; modra – zaželen premik odjema, srednja tarifa; rdeča - nujna razbremenitev sistema, najvišja tarifa.

Tudi tu je predpogoj za naprednejše izvajanje ukrepa dvosmerna komunikacija oziroma IKT infrastruktura, predstavljena v poglavju 5.8.

5.8 Informacijsko-komunikacijska infrastruktura v funkciji upravljanja porabe

Upravljanje porabe električne energije v osnovi zahteva IKS, ki omogoča komunikacijo med odjemalcem in operaterjem omrežja ter prenos in obdelavo vseh tistih informacij, krmilnih signalov, merilnih podatkov … med odjemalcem in operaterjem, ki so potrebni za izvajanje izbranega (izbranih) programov LM.

IKS v elektroenergetiki so raznoliki tako po tehnologiji kot tudi po kompleksnosti. IKS se še naprej razvijajo in dandanašnji poskušajo zadovoljiti kar najširši spekter zahtev. Aktivna

omrežja (Smart Grids) naj bi temeljila na vseprisotnih in hitrih komunikacijskih tehnologijah ter informacijskih sistemih, ki naj bi omogočali obvladovanje elektroenergetskega omrežja v celoti. Aktivna omrežja naj bi zagotavljala tudi podlago za izvajanje programov LM. Ker niti sami snovalci ideje aktivnih omrežij v tem trenutku še nimajo jasnega odgovora, kako naj bo zasnovan IKS za podporo aktivnih omrežij, je prav, da poskušamo določiti vsaj osnovne zahteve za izvedbo programov LM in ugotoviti, ali obstoječi IKS v elektroenergetiki že omogočajo njihovo izvedbo. Že vzpostavitev Etherneta v TP približa komunikacijsko infrastrukturo odjemalcem, s tem pa so na široko odprta vrata tudi za izvajanje DSM programov.

5.8.1 IKT za programe, temelječe na spremenljivih cenah

Med programi, temelječimi na spremenljivih cenah (Dynamic Pricing - DP), je sistem tarifnih časov (TOU – time of use pricing) daleč najbolj razširjen in uporabljan sistem. Za delovanje sistema zadošča števec električne energije z (vsaj) dvotarifnim merjenjem in stikalna ura oziroma sprejemnik krmilnega signala za preklop tarife. Odčitavanje dvotarifnih števcev gospodinjskih odjemalcev se v Sloveniji izvaja enkrat letno, odjemalci pa imajo možnost sporočanja mesečnih odbirkov po telefonu, elektronski pošti ali preko portala E-storitve. Komunikacijski sistem za daljinsko odčitavanje števcev ni potreben.

Tarifiranje časa kritičnih koničnih obremenitev (critical peak pricing) in spodbude za zmanjševanje konice odjema (peak load reduction credits) zahtevajo merilno opremo, ki omogoča merjenje 15-minutnih povprečij odjema električne energije. Odjemalce se s takšnim načinom merjenja se odčitava enkrat mesečno. Zaradi pogostejšega odčitavanja je dobrodošlo daljinsko odčitavanje podatkovnih paketov s 15-minutnimi vrednostmi odjema. V Elektru Gorenjska so že vsi tovrstni odjemalci daljinsko odčitani.

Dinamično tarifiranje (dynamic pricing, real-time pricing) zahteva implementacijo naprednih merilnih sistemov (AMR, AMM, AMI), saj naj bi se tarifa dinamično spreminjala glede na trenutne razmere v elektroenergetskem sistemu oziroma glede na trenutno tržno ceno električne energije. Poleg t.i. pametnih števcev je potreben tudi napreden informacijski sistem za obdelavo merilnih podatkov v realnem času, ki bi bil sposoben določati in sporočati števcem tarife glede na trenutne razmere v sistemu oziroma na trgu z električno energijo. Ti sistemi se v Sloveniji zaenkrat v večjem obsegu ne pojavljajo, ovira resnejši uporabi tega sistema pa je tudi zakonodaja, ki sistema dinamičnega tarifiranja zaenkrat ne predpisuje. Velika ovira široki uvedbi tega sistema so drage merilne naprave in neobstoječ

komunikacijski sistem, ki bi bil zmožen ob sprejemljivih stroških zanesljivo prenesti potrebno količino podatkov v obe smeri.

5.8.2 IKT za programe, temelječe na krmiljenju bremena

Krmiljenje bremena oziroma posameznih porabnikov, kot so grelniki vode, klimatske naprave, hladilniki … zahteva:

- vzpostavitev komunikacijskega kanala med odjemalcem in operaterjem omrežja,
- informacijski sistem pri operaterju omrežja, ki je sposoben ugotavljanja (merjenja) potrebe po razbremenjevanju/obremenjevanju delov omrežja in pošiljanja krmilnih signalov (vklop/izklop) krmilnim napravam,
- krmilne naprave, ki sprejemajo krmilne signale za vklop/izklop posameznega bremena pri odjemalcih, upoštevajoč omejitve, ki jih določa odjemalec.

Izvedbe tako komunikacijskega kot informacijskega dela sistema so zelo različne. Kot komunikacijski medij se lahko uporablja komunikacija po energetskih vodih, optiki ali preko brezžične komunikacije. Krmilniki so lahko samostojne naprave z radijskimi sprejemniki ali sprejemniki, npr. TKM signala, lahko pa se za krmiljenje posameznih bremen uporabljajo relejski izhodi sodobnih števcev.

Zanimivo rešitev na tem področju razvija podjetje za proizvodnjo gospodinjskih aparatov Gorenje. V programu gospodinjskih aparatov za t.i. pametno hišo razvija sistem avtomatizacije vseh gospodinjskih aparatov. Komunikacija med njimi in napravo za vodenje poteka po energetskih vodih hišne napeljave. Elektro Gorenjska, Gorenje in Iskraemeco načrtujejo sistem, ki bi povezal AMI števec, napravo za vodenje »pametne hiše«, in center vodenja distribucijskega omrežja tako, da bo z uporabo IKT infrastrukture AMI sistema mogoče izvajati krmiljenje posameznih bremen pri odjemalcu.

5.8.3 IKT za programe, temelječe na povratnih informacijah

Spodbujanje odjemalcev k varčevanju z energijo v programih temelječih na povratnih informacijah, zahteva stroškovno sprejemljiv in učinkovit informacijski sistem. Naloga sistema je podajati odjemalcem sporočila, ki jih bodo spodbudila k racionalni rabi energije, še posebej takrat, ko so potrebe po znižanju odjema električne energije največje.

Z implementacijo AMI sistema se ustvarijo tudi pogoji za izvajanje obravnavanih programov. V ta namen obstajajo t.i. hišni prikazovalniki, ki so komunikacijsko povezani z AMI števcem in omogočajo prikaz različnih sporočil. Mnogo cenejša, enostavnejša, a manj individualna rešitev pa je izraba interneta in drugih javnih medijev za spodbujanje odgovornejšega odnosa odjemalcev do najžlahtnejše oblike energije.

5.9 Sklepne ugotovitve v zvezi z DSM v distribuciji EE

Slovenija je s 1. 7. 2007 popolnoma liberalizirala trg z električno energijo. V prenovljeni energetski zakonodaji so našle mesto spodbude za varčevanje energije pri končnih odjemalcih, izboljšanje energetske učinkovitosti, spodbude za izrabo alternativnih virov energije in energetsko sanacijo stavb. Ukrepi s področja upravljanja obremenitve (Load Management) žal nimajo mesta v slovenski zakonodaji.

Sistemski operater in lastniki distribucijskega omrežja nimajo zakonske podlage za izvajanje ukrepov DSM, s katerimi bi lahko bistveno vplivali na glajenje krivulje odjema in s tem izboljšali izkoriščenost in optimirali razvoj (ojačitve) omrežja. Spodbud za razvoj tovrstnih omrežnih storitev s področja DSM ni, čeprav je v svetu znanih veliko uspešnih primerov, ki so z narodnogospodarskega vidika pomembni vsaj toliko kot katerikoli od prej omenjenih varčevalnih spodbud. V Sloveniji je z vidika vplivanja na krivuljo odjema v uporabi le dvotarifni sistem merjenja električne energije pri gospodinjskih odjemalcih in merjenje konice odjema poslovnih odjemalcev.

Pomanjkanje sistemskega pristopa na področju DSM z vidika sistemskega operaterja oz. lastnikov distribucijskega omrežja je tudi vzrok, da razvojni načrti ne upoštevajo usmerjene rabe energije kot kriterija načrtovanja omrežij. Neizkoriščene ostajajo številne možnosti za preprečevanje preobremenitev omrežja na ekonomsko sprejemljivejši način kot je investiranje v ojačitev omrežja in/ali zagotavljanje storitev sistemskemu operaterju, ki bi z različnim odzivnim časom pomagale zmanjšati konične obremenitve omrežja.

Pod pritiskom konkurenčnega boja med številnimi trgovci z električno energijo na zaprtem in omejenem slovenskem trgu se dejavnost trgovcev vedno bolj osredotoča na samo trgovanje. Glavno vodilo je dobiček, generator pa je razlika med nakupno in prodajno ceno električne energije, pri čemer se mora trgovec v čim večji meri izogniti odstopanjem med napovedjo prevzema električne energije in dejansko prodajo električne energije, kar v bližnji prihodnosti z razmahom telemetrije in sodobnimi sistemi za napovedovanje odjema ne bo več

velik problem. Vprašamo se lahko, zakaj bi trgovca z električno energijo sploh zanimalo uvajanje ukrepov DSM, ki bi zmanjševali količino prodane električne energije, ali zakaj bi spodbujali glajenje konic odjema posameznih odjemalcev. Spodbujanje racionalne rabe električne energije je v nasprotju z interesom trgovca po prodaji čim večjih količin električne energije; spodbujanje racionalne rabe električne energije je lahko le marketinško orodje.

Interes odjemalcev za sodelovanje je ključen za uspeh DSM. Brez pripravljenosti odjemalcev, da se odzovejo na potrebo po prilagoditvi odjema, ukrepi DSM ne morejo delovati. Odjemalci bodo pripravljeni v ukrepih DSM sodelovati le, če bodo finančne spodbude za sodelovanje dovolj velike in/ali če ukrepi ne bodo bistveno vplivali na njihov proizvodni proces ali življenjske navade. V splošnem velja, da vsak odjemalec posebej presoja prednosti in slabosti vključitve v programe DSM.

Izkušnje iz sveta kažejo na precejšnjo korelacijo med reguliranim trgom z električno energijo in uspešnostjo (ali sploh obstojem) DSM ukrepov s področja upravljanja porabe pri odjemalcih. Odprt trg in nastop močnih trgovcev, ki jim ni treba upoštevati (vseh) zakonitosti delovanja elektroenergetskega sistema od proizvodnje, prenosa do distribucije, zamegljuje odvisnost odjemalca od optimalnega delovanja sistema. Preseneča (ali pa tudi ne …) lahkotnost, s katero se zanemarja nujnost celovitega pristopa pri usklajevanju proizvodnje, porabe in prenosnih zmogljivosti sistema tako, da bo s kar najmanjšimi investicijami v sistem ter s čim manjšimi vplivi na okolje mogoče zadovoljiti potrebe odjemalcev električne energije. In v tem procesu ukrepi upravljanja porabe električne energije ne morejo in ne smejo izostati.

6 INFORMACIJSKO-KOMUNIKACIJSKI SISTEMI V DISTRIBUCIJI EE

Uporaba informacijskih in komunikacijskih tehnologij (IKT) ima v slovenski elektrodistribuciji dolgo zgodovino. Uvajanje IKT je sledilo razvoju tehnike in vedno ostrejšim zahtevam po nadzoru in vodenju distribucijskega omrežja. Dandanašnji distribucijski centri vodenja (DCV) omogočajo daljinski nadzor in vodenje RTP, RP ter posameznih daljinsko vodenih stikalnih naprav na samem SN omrežju. Izziv za bližnjo prihodnost je informatizacija celotnega distribucijskega omrežja, torej implementacija takšnih IKT, ki bodo zadostile sedanjim in tudi prihodnjim potrebam po nadzoru in vodenju celotnega distribucijskega omrežja, upravljanju porabe EE pri odjemalcih (DSM), obvladovanju razpršene proizvodnje EE, hranilnikov energije ter hkrati zagotavljale potrebno komunikacijsko infrastrukturo sodobnim AMI sistemom. Pri tem je ključno vprašanje izbire optimalne komunikacijske tehnologije, standardov in komunikacijskih protokolov.

Sistem za nadzor in vodenje distribucijskega omrežja v realnem času je zahteven in kompleksen. Distribucijska podjetja ga izgrajujejo postopoma. Obstoječi IKS omogočajo nadzor in zajem podatkov do nivoja SN izvoda iz razdelilno transformatorske postaje (RTP). Naprave za nadzor in vodenje stikalnih naprav ter drugih sistemov v RTP so preko komunikacijskih računalnikov povezane z distribucijskimi centri vodenja (DCV). Sistem za nadzor, vodenje in zajem podatkov (SCADA) v DCV med drugim zagotavlja daljinsko vodenje in nadzor RTP ter prikaz in arhiviranje merilnih podatkov. V RTP je vzpostavljen tudi permanentni monitoring kakovosti napetosti. Merilniki kakovosti so povezani s centom za nadzor kakovosti napetosti, v katerem se arhivirajo in po potrebi analizirajo podatki o izmerjenih vrednostih parametrov kakovosti po standardu SIST EN 50160.

Če izvzamemo posamezna daljinsko vodena stikala na samem SN omrežju, se avtomatiziran nadzor in vodenje distribucijskega omrežja končata na izvodu iz RTP.

6.1 Zahteve za IKS za aktivna omrežja

Za izgradnjo IKS za aktivna omrežja v distribuciji EE bi bilo (postopno) potrebno zagotoviti komunikacijski sistem, ki bi temeljil na obstoječi TK infrastrukturi in poleg vodenja SN omrežja omogočal še vsaj:

- prenos podatkov iz koncentratorja AMI števcev, ali po možnosti iz samih števcev zaradi omejitev DLC,
- upravljanje porabe pri odjemalcu (DSM) z uporabo AMI sistema,
- vgradnjo merilnih sistemov za nadzor in vodenje TP SN/NN,
- vzpostavitev permanentnega monitoringa kakovosti napetosti,
- nadzor nad NN izvodi iz TP,
- upravljanje z razpršenimi viri in kompenzacijskimi napravami.

6.1.1 Sistemi daljinskega odčitavanja AMI in upravljanje porabe (DSM)

Dandanašnji smo priča izredno hitremu razvoju t.i. AMR/AMI (Automated Meter Reading / Advanced Metering Infrastructure) sistemov za avtomatsko odčitavanje porabe električne energije, plina, vode … V slovenskem distribucijskem omrežju še vedno prevladujejo indukcijski števci električne energije. Sodobni elektronski števci z možnostjo avtomatskega odčitavanja se več let uporabljajo za merjenje porabe električne energije večjih odjemalcev (odjemalci s priključno močjo nad 41 kW). Večinoma se uporabljajo elektronski števci z vgrajenim GSM/GPRS modemom, s katerimi komunicira center za obdelavo podatkov neposredno. Večji odjemalci po številu predstavljajo le 1% vseh odjemalcev. Predvsem zaradi zelo velikega števila gospodinjskih odjemalcev se razvijajo komunikacijsko optimalnejši sistemi. Kot primeren se je izkazal sistem komuniciranja po energetskih NN vodih (Distribution Line Carrier - DLC) z vgradnjo podatkovnih koncentratorjev v SN/NN TP. Na ta način se zmanjša število točk, s katerimi merilni center komunicira neposredno.

AMI sistem v povezavi s »pametnimi« gospodinjskimi aparati – porabniki EE v gospodinjstvih, so lahko osnova za upravljanje porabe EE pri odjemalcih (Demand Side Management - DSM). Potrebno je zagotoviti prenos podatkov o želeni spremembi odjema iz centra vodenja do vsakega gospodinjstva. Več o tem v poglavju 4.

6.1.2 Nadzor in vodenje celotnega SN omrežja

Najpomembnejša prednost IKS za nadzor in vodenje do nivoja TP SN/NN je zagotovitev avtomatiziranega nadzora nad obratovanjem celotnega SN omrežja v realnem času. S tem se občutno skrajša potreben čas za ugotavljanje vzroka in mesta okvare na omrežju in možnost natančnejšega informiranja in vodenja dežurnih ekip na terenu [22], [23].

6.1.3 Načrtovanje in razvoj distribucijskega omrežja

Rezultati obratovalnih meritev so nepogrešljivi pri načrtovanju distribucijskega omrežja, saj so osnova za izračun pretokov moči, koničnih obremenitev, zasedenosti transformacije, tehničnih izgub itd. Na podlagi teh in drugih parametrov se odloča o potrebi in načinu ojačitve omrežja ali transformacije na določenem napajalnem območju [5].

6.1.4 Nadzor nad porabo EE

TP so mejne točke med SN omrežjem in NN napajalnim območjem TP. Na NN omrežje so priključena gospodinjstva in drugi manjši odjemalci. Za distributerja EE je vsekakor zanimiva razlika med EE, ki jo TP oddaja v NN omrežje in vsoto porabe vseh odjemalcev na NN omrežju. Razliko predstavljajo tehnične izgube na NN omrežju in eventualni nekontrolirani odjem (kraja).

6.1.5 Nadgradnja stalnega monitoringa kakovosti napetosti

V slovenski elektrodistribuciji je vzpostavljen sistem permanentnega monitoringa kakovosti napetosti po standardu SIST EN 50160 na nivoju RTP [6]. V TP vgrajeni merilni centri, ki zagotavljajo meritve kakovosti napetosti skladno s standardom SIST EN 50160, bi predstavljali razširitev permanentnega monitoringa napetosti na celotno SN omrežje.

6.1.6 Nadzor nad NN omrežjem

Nadzor nad NNO izvaja izključno osebje na terenu (krajevna nadzorništva). Informatizacija TP SN/NN odpira vrata tudi nadzoru NNO, vsaj na nivoju posameznih izvodov iz NN razdelilca. Naprava za nadzor bi morala biti sposobna zaznati dogodke na NN izvodu (npr. prekinitev NN varovalke) in oddati sporočilo v obliki alarma v DCV [22].

6.1.7 Spremljanje parametrov zanesljivosti oskrbe pri odjemalcu

Zanesljivost dobave EE se mora izračunavati za vsakega odjemalca posebej. Število in trajanje izpadov izvodov iz RTP registrira DCV in podatke za nadaljnje analize shrani v historični zbirki podatkov. Podatki o izpadu TP oziroma izvoda iz TP pa se vnašajo ročno na podlagi podatkov, ki jih DCV posredujejo dežurne ekipe na terenu. Z vzpostavitvijo informacijskega sistema obratovalnih meritev na nivoju TP ročni vnos podatkov ne bi bil več

potreben. Distribucijska podjetja trenutno lahko spremljajo sistemske kazalce zanesljivosti oskrbe (SAIDI, SAIFI). Zakonodaja zahteva ugotavljanje zanesljivosti oskrbe pri vsakem odjemalcu, česar pa brez celovito vzpostavljenega AMI sistema ni mogoče zagotoviti.

6.1.8 Upravljanje z razpršenimi viri in kompenzacijskimi napravami

Energetska politika EU daje velik poudarek razpršenim virom energije. Z naraščanjem deleža porazdeljene proizvodnje na distribucijskem omrežju se lahko pojavijo težave v obratovanju, ki izvirajo predvsem iz širokega spektra tehnologij za proizvodnjo električne energije, slabe napovedljivosti nekaterih virov (veter, sonce, voda), odzivnosti odjemalcev in zahtevnosti vodenja kompleksnega distribucijskega omrežja.

Ena od rešitev obratovalnih težav, ki izvirajo iz povečanega deleža porazdeljene proizvodnje, je združevanje proizvodnih virov in odjemalcev v t.i. virtualno elektrarno. Ta ima v osnovi podobno funkcijo kot večja elektrarna, saj v komunikaciji z nadrejenimi centri vodenja komunicira kot ena enota. Glavni izziv virtualne elektrarne predstavlja optimalno obratovanje, ki upošteva tako proizvodne vire kot tudi bremena, ki so v splošnem odzivna.

Enote razpršene proizvodnje (npr. fotovoltaične elektrarne) večinoma uporabljajo module močnostne elektronike (razsmernike), ki jih je mogoče uporabiti tudi za regulacijo napetosti, izvajanje aktivnega filtriranja višjih harmonskih komponent omrežne napetosti, kompenzacijo nesimetričnih bremen ipd. Seveda pa morajo takšni kompenzatorji delovati nadzorovano in glede na trenutne potrebe distribucijskega sistema na mestu priključitve.

Za nadzor in upravljanje takšnega sistema je potreben zmogljiv IKS, ki zagotavlja medsebojno komunikacijo med številnimi in heterogenimi »pametnimi« enotami na omrežju.

6.2 Koncept sodobnega IKS za aktivna omrežja

Osnovna naloga IKS je povezovanje uporabnikov in tehnologije v produktivno celoto. Krajevno razpršene računalniške vire med seboj povezuje *komunikacijski del sistema*. Računalniški viri postanejo uporabno orodje le, če jih opremimo z aplikacijami. Aplikacije omogočajo manipulacijo s podatki, torej so bistveni element *informacijskega dela sistema*.

Pri obravnavanju IKS je pomembna njegova *transparentnost* in *plastnost* funkcionalnih sklopov. Razlog in osnovni cilj plastenja IKS je strukturiranje sorodnih problemov, ki so funkcionalna vsebina posamezne plasti. Uporabnika informacijskega sistema ne zanima, kako

se je skozi komunikacijski sistem prenesla, npr. elektronska pošta, ki jo je poslal prejemniku. Informacijski dialog med uporabnikoma elektronske pošte poteka po logičnem informacijskem kanalu, uporabniku prijazno storitev zagotavlja aplikacija »odjemalec e-pošte«. Komunikacijski sistem poskrbi za fizični prenos podatkov. Fizični prenos podatkov predstavlja preoblikovanje elektronskega sporočila v podatkovne pakete, njih prenos preko prenosnega medija do prejemnika in preoblikovanje prenesenih podatkovnih nazaj v elektronsko sporočilo (Slika 6.1.).

Plastnost IKS nakazuje logična izmenjava sporočila v obliki e-pisma med uporabnikoma (uporabniško poslovanje), izmenjava e-pisma med aplikacijama »odjemalec e-pošte«, logični transport podatkovnih (IP) paketov med oddaljenima računalnikoma, logični prenos podatkovnih paketov po komunikacijskem kanalu, kjer se fizično izvede prenos (električnih, optičnih, radijskih) signalov preko prenosnega medija (parica, optično vlakno, »eter«).

Transparentnost sistema pomeni izvajanje storitev na uporabniku neviden način. Z vidika posameznih plasti IKS transparentnost pomeni, da je za opazovano plast popolnoma nepomembno, na kakšen način plast pod njo izvede zahtevano storitev.

Plastnost IKS je standardizirana. V uporabi sta »de iure« 7-plastni ISO-OSI standard in »de facto« 4-plastni IP standard. Zakonitostim teh standardov se prilagajajo proizvajalci opreme oziroma njihova združenja standarde sooblikujejo. Z vidika uporabnikov sistema imamo tako možnost, da realiziramo posamezne plasti IKS z zelo različnimi tehnologijami. Paziti moramo le na celovitost in kakovost izvajanja storitev, ki jih mora posamezna plast zagotavljati.

Komunikacijski del IKS pokriva nižje plasti IKS, zato je pomembno, da pred nadaljnjo obravnavo spoznamo vsebino posameznih plasti.

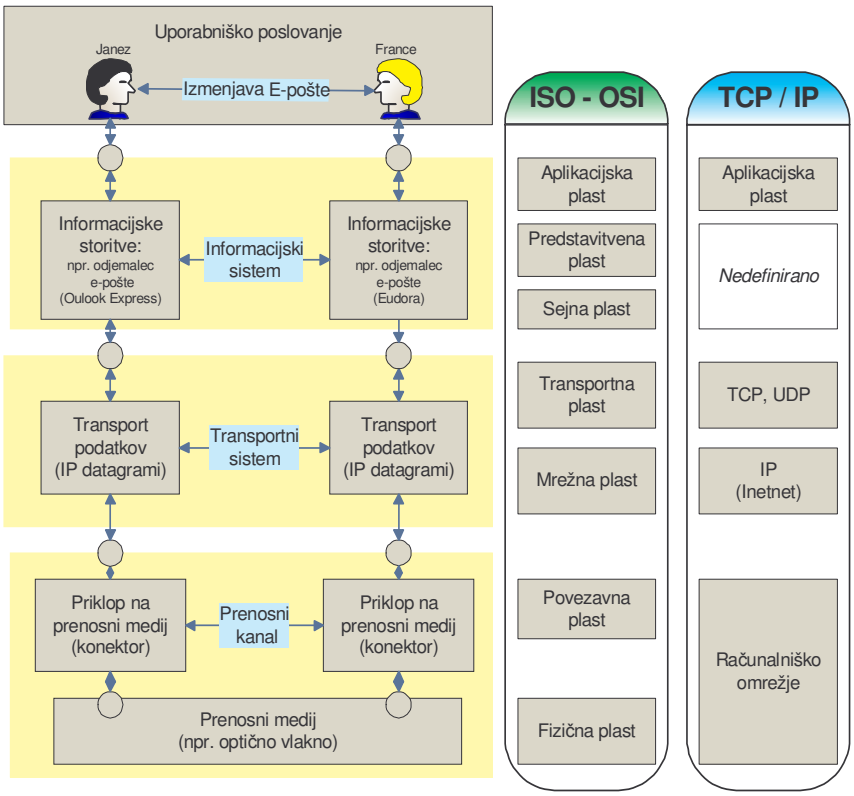
6.2.1 ISO-OSI 7- plastni in TCP/ IP 4- plastni model

Model OSI (Open System Interconnection) je referenčni model za opisovanje protokolnega sklada, ki ga je izdal ISO (International Standard Organization). Model vsebuje skupek določil in priporočil za implementacijo arhitekture IKS. Sestavlja ga 7 plasti. Model opisuje funkcije vsake plasti in določa način povezovanja med njimi. Zgornje tri plasti modela opisujejo informacijski del, spodnje štiri pa komunikacijski del IKS. V grobem so naloge posameznih plasti naslednje:

- aplikacijska plast zagotavlja, da dva aplikacijska procesa (npr. izmenjava e-pošte) lahko medsebojno delujeta ne glede na to, na kakšnih sistemih delujeta in kako sta med sabo fizično povezana;

- predstavitvena plast zavaruje aplikacijsko pred razlikami v obliki in sintaksi prenesenih podatkov ter skrbi za zaščito podatkov;
- plast seje skrbi za urejen dialog med uporabniki z vzpostavitvijo seje;
- transportna plast skrbi za krmiljenje informacijskega pretoka; zagotavlja zanesljiv pretok datagramov od oddajnika do sprejemnika;
- omrežna plast skrbi za usmerjanje podatkovnih paketov skozi omrežje;
- povezavna plast prenaša podatkovne okvirje (Frame) med dvema točkama, ki sta povezana s prenosnim medijem. Pomembna naloga te plasti je odkrivanje napak, ki se pojavijo med prenosom po fizičnem mediju;
- fizična plast prenaša bite z uporabo električnih, optičnih, elektromagnetnih ali drugih signalov in določa vmesnike ter komunikacijske nosilce fizičnega nivoja.

Štiriplastni TCP/IP model je nastal pod okriljem IETF in je starejši kot OSI model. Ime izhaja iz najpogosteje uporabljanega protokola transportne plasti (TCP) in omrežne plasti (IP). Sestava sklada je na sliki 6.1. Ko govorimo o TCP/IP modelu, moramo imeti v mislih vse protokole vseh štirih nivojev in ne samo prej omenjenih, ki se največ uporabljata.



Slika 6.1: Plastnost IKS in primerjava ISO - OSI ter TCP/IP modela

Aplikacijska plast vsebuje veliko aplikacijskih protokolov, ki omogočajo končnim uporabnikom dostop do omrežja, npr. SMTP za prenos e-pošte, HTTP za prenos besedila, slik, videa preko spleta (WWW).

Transportni nivo skrbi za zanesljiv prenos in kontrolo prenesenih podatkov. V praksi se največ uporabljajo trije protokoli: TCP (Transmission Control Protocol), ki ima vgrajeno odkrivanje napak in izvaja zahteve za ponovno pošiljanje okvarjenih paketov, UDP (User Datagram Protocol), ki je enostaven protokol za prenos podatkov brez zaznavanja napak, ter SCTP (Stream Control Transmission Protocol) za nadzor nad podatkovnim tokom;

Omrežni nivo je zadolžen za iskanje ustrezne poti do ciljnega uporabnika in za dostavo paketov na ciljni naslov. V tej plasti je implementiran protokol IP (Internet Protocol), ki je nepovezavno naravnan protokol (ne daje nikakršnih zagotovil o prenosu podatkov).

Plast nosilnih storitev ustreza povezavni in fizični plasti ISO-OSI modela. Omrežni nivo se povezuje s povezovalnim nivojem preko omrežnega vmesnika. Uporabljajo se različne tehnologije: Ethernet, PPP, ATM ipd [24].

6.2.2 Tokokrogovno komutiran in paketni način komuniciranja

Pri komunikaciji med dvema točkama se uporablja dva načina prenosa podatkov: tokokrogovno komutiran in paketni način komuniciranja.

Pri **tokokrogovno komutiranem načinu** imata točki, ki komunicirata, zagotovljeno pasovno širino ves čas trajanja zveze. Kadar so zasedene vse zmogljivosti omrežja, novih zvez ni mogoče vzpostaviti. Tak primer je telefonsko omrežje. Dobra lastnost tega načina je stalno zagotovljen komunikacijski kanal, kar omogoča prenos podatkov brez zastojev. Slabost je zasedanje kapacitet omrežja tudi takrat, ko to ni potrebno, s tem povezan je tudi slabši izkoristek omrežja.

Paketni način komuniciranja omogoča izmenjavo podatkov brez vnaprejšnjega vzpostavljanja povezav. Komunicirajoče strani si ves čas delijo njegove zmogljivosti. Blokade posameznih točk, ki želijo komunicirati, ni, se pa omrežje na večje obremenitve vse počasneje odziva. Paketni način prenosa uporablja Ethernet in omrežje IP. Podatki se razdelijo na manjše pakete, ki se nato prenašajo po omrežju. Dobra lastnost je velika izkoriščenost omrežja, slabe lastnosti pa izhajajo iz nepovezavnosti komuniciranja: pri zelo zasedenem omrežju težko govorimo o prenosu podatkov v »realnem« času.

6.2.3 Izbira načina komuniciranja in izvedbe plasti nosilnih storitev

IKS za aktivna omrežja bo sestavljalo večje število med seboj zelo različnih komunikacijskih točk. Na eni strani so to DCV, center za nadzor kakovosti napetosti, center obračunskih meritev … na drugi strani pa množica merilnih naprav, krmilnikov … različnih proizvajalcev, ki imajo sila različno dinamiko komuniciranja. Na naš komunikacijski sistem bo priključenih relativno veliko število »inteligentnih« naprav sposobnih komuniciranja. Obenem lahko ugotovimo, da je količina podatkov, ki jih mora v povprečju prejeti ali oddati katerakoli od omenjenih naprav, zelo majhna.

Ekonomsko in tehnično gledano je zahtevnost izgradnje komunikacijskega sistema odvisna predvsem od njegovih prenosnih zmogljivosti in razširjenosti sistema. Ker se bo obravnavani sistem gradil postopoma, je potrebno način komuniciranja podrediti standardiziranim in uveljavljenim rešitvam. Plast nosilnih storitev obravnavanega IKS mora imeti podobne lastnosti, kot so danes množično uporabljane v lokalnih omrežjih (LAN) V lokalnih omrežjih plast nosilnih storitev najpogosteje zagotavlja **Ethernet** (IEEE 802.x). Naprave, priključene v omrežje tipa Ethernet, uporabljajo skupen fizični medij. Signali, ki jih oddaja ena naprava, so tako dostopni vsem ostalim napravam v omrežju.

6.2.4 Izvedba omrežne in transportne plasti

V obravnavanem IKS morata omrežna in transportna plast zagotoviti prenos podatkovnih paketov. V večini primerov se lahko zadovoljimo s prenosom v kvazi realnem času. V teh primerih se zaradi dobre izkoriščenosti komunikacijskega sistema in vedno večje razširjenosti tudi v sistemih meritev, nadzornih sistemih in sistemih vodenja v elektroenergetiki kot najobetavnejši ponuja prenos podatkov po **TCP/IP** protokolu.

Nekateri kritični podatki, kot npr. alarmi, podatki pri prenosu kriterija distančne zaščite daljnovodov in drugi podatki o stanju stikalnih aparatov in zaščitnih naprav pa morajo biti dostopni v realnem času. V poglavju 6.3.2. omenjeno slabost nepovezavnosti komuniciranja je mogoče uspešno odpraviti (omiliti) z določanjem prioritet posameznim podatkovnim paketom (priority tagging), kar opredeljuje standard IEEE 802.1q [25]. Podobne rešitve uporablja tudi IP telefonija, ki zahteva neprekinjenost prenosa govora.

6.2.5 Izvedba aplikacijske plasti – standard IEC 61850

IKS za aktivna omrežja mora na aplikacijski plasti podpirati protokol, ki bo zagotavljal čim bolj enovito podporo prenosu podatkov med napravami. V predhodnih podpoglavjih je bila izpostavljena prednost paketnega prenosa podatkov, ki pa mora biti tudi dovolj hiter, da zadosti zahtevam avtomatizacije in zaščite elektroenergetskih sistemov.

V evropski in slovenski elektrodistribuciji še prevladuje uporaba komunikacijskega protokola **IEC 60870-5-101** in njegova prilagoditev na paketni prenos podatkov **IEC 60870-5-104**. Kratka predstavitev obeh protokolov je v prilogi.

V zadnjem času veliko obeta standard IEC 61850, ki je na kratko predstavljen v nadaljevanju.

IEC 61850 je standard za načrtovanje avtomatizacije elektroenergetskih sistemov, še posebej razdelilnih postaj. Področje uporabe IEC 61850 je mnogo večje kot pri protokolu IEC 60870-5-101. IEC 61850 se ne omejuje le na prenos podatkov, ampak določa tudi popoln podatkovni model. Uporabniku protokola je na voljo tudi programski jezik SCL (Substation Configuration description Language) za individualen opis naprav in njihove konfiguracije. SCL temelji na splošno razširjenem jeziku XML[15].

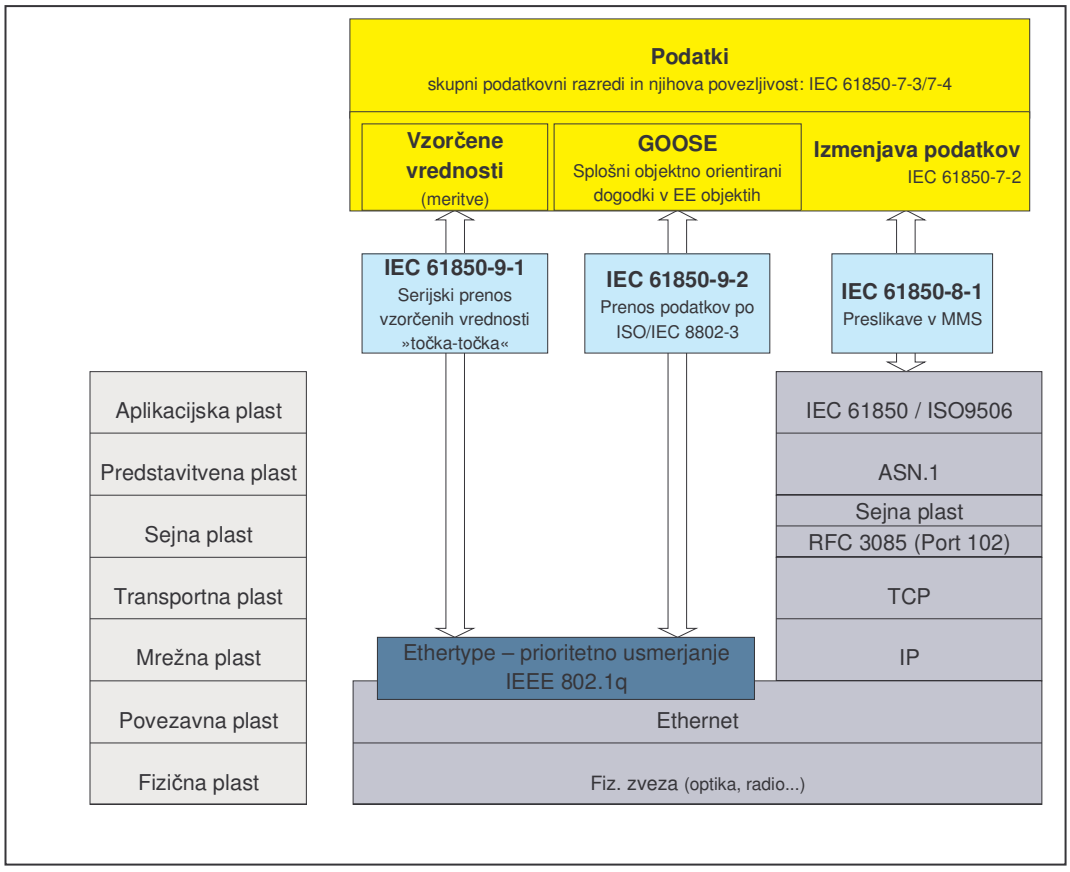
Podatkovni modeli protokola lahko podpirajo MMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Events), GSSE (Generic Substation State Events) ipd. Ti protokoli temeljijo na paketnem prenosu podatkov in zagotavljajo odzivni čas pri prenosu podatkov pod 4 ms, kar je ključno za delovanje zaščitnih sistemov v elektroenergetiki. Podrobnosti standarda IEC 61850 so predstavljeni v naslednjih dokumentih:

- IEC 61850-1: Uvod in pregled,
- IEC 61850-2: Pojmovnik,
- IEC 61850-3: Splošne zahteve,
- IEC 61850-4: Projektno vodenje in vodenje sistema,
- IEC 61850-5: Komunikacijske zahteve funkcij in podatkovnih modelov,
- IEC 61850-6: Konfiguracijski opisni jezik za komunikacijske povezave sistemov vodenja v energetskih postrojih,

---

[15] XML (Extensible Markup Language) je preprost računalniški jezik podoben HTML-ju, ki nam omogoča opisovanje strukturiranih podatkov ali arhitekture za prenos podatkov in njihovo izmenjavo med več omrežji.

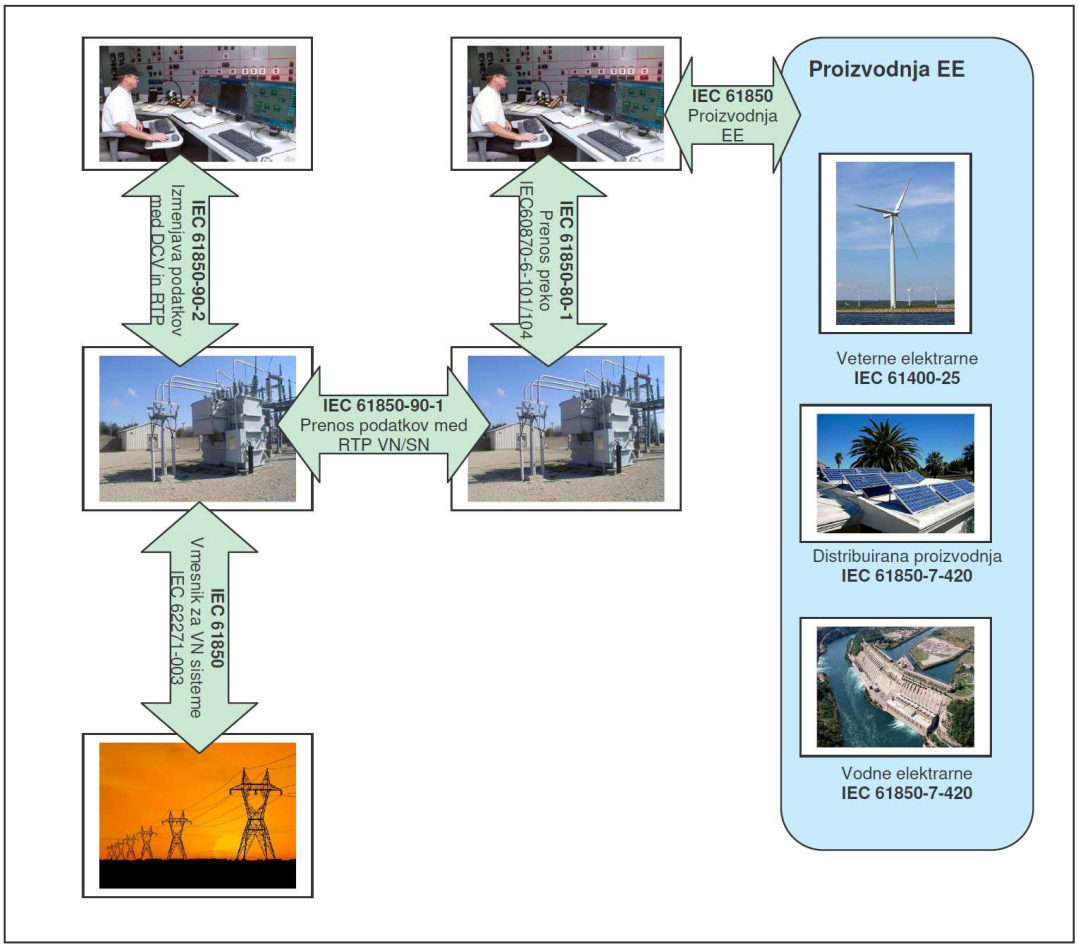
- IEC 61850-7: Osnovne komunikacijske strukture za komunikacijske povezave sistemov vodenja v energetskih postrojih:
  - IEC 61850-7-1: Načela in modeli,
  - IEC 61850-7-2: Osnovni komunikacijski vmesnik (ACSI),
  - IEC 61850-7-3: Skupni podatkovni razredi ,
  - IEC 61850-7-4: Povezljivost razredov logičnih vozlišč in podatkovnih razredov,
- IEC 61850-8: Preslikave posebnih komunikacijskih storitev (SCSM):
  - IEC 61850-8-1: Preslikave v MMS (ISO/IEC9506-1 in ISO / IEC 9506-2),
- IEC 61850-9: Preslikave posebnih komunikacijskih storitev (SCSM):
  - IEC 61850-9-1: Prenos vzorčenih vrednosti preko serijske enosmerne povezave točka-točka,
  - IEC 61850-9-2: Prenos vzorčenih vrednosti po ISO/IEC 8802-3,
- IEC 61850-10: Preizkušanje.



Slika 6.2: Plastnost standarda IEC 61850

Standard IEC 61850 je nastal iz potrebe po povezljivosti sistemov za zaščito in vodenje elektroenergetskih sistemov različnih proizvajalcev, ki so danes na voljo. Razvoj specifičnih protokolov, ki so jih prakticirali posamezni proizvajalci, je onemogočal optimalen razvoj in nadgradnjo obstoječih sistemov. Pod okriljem IEC je skupina strokovnjakov postavila standard na osnovi naslednjih izhodišč:

- enovit komunikacijski protokol za vodenje elektroenergetskega objekta, ki bo upošteval različne podatkovne modele zahteve posameznega objekta,
- opredelitev osnovnih storitev, potrebnih za prenos podatkov, tako da je komunikacijski protokol nadgradljiv z novimi zahtevami,
- zagotavljanje visoke interoperabilnosti med sistemi različnih ponudnikov,
- preprosta oblika in način shranjevanja vseh podatkov,
- določitev postopkov testiranja vse opreme, na katero se standard nanaša.



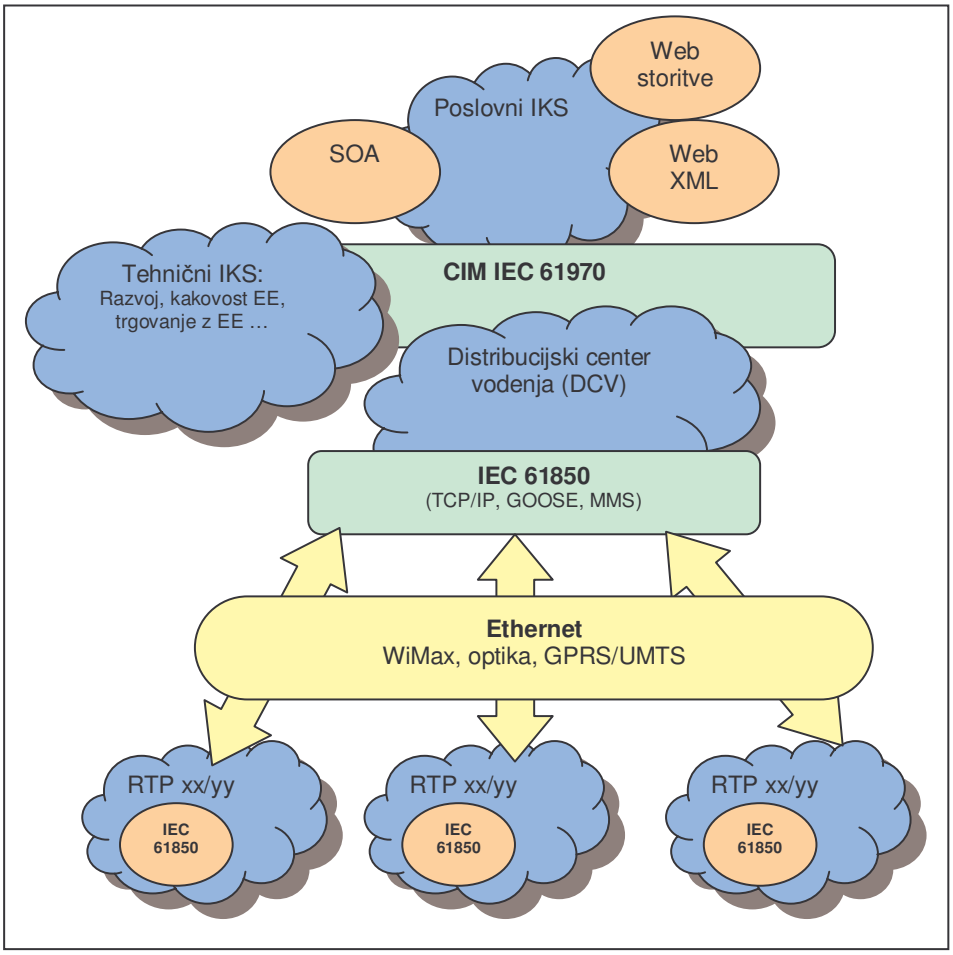
Slika 6.3: Nekatera področja uporabe standarda IEC 61850

Pomembnejša področja, ki jih IEC 61850 vključuje, so: podatkovno modeliranje, sistemi poročanja, hiter prenos podatkov, prenos vzorčenih vrednosti podatkov, prenos ukazov, shranjevanje podatkov.

Standard IEC 61850 veliko obeta, njegov razvoj se nadaljuje. Danes izvedenke tega standarda srečamo v različnih elektroenergetskih sistemih (Slika 6.3) in mnogi avtorji mu pripisujejo ključno vlogo pri IKS za aktivna omrežja.

6.2.6 Poenotenje podatkovnih struktur - Common Information Model (CIM)

Vodenje distribucijskega omrežja, upravljanje porabe električne energije ipd. danes ni več proces, ki bi se informacijsko zaključil v centru vodenja distribucijskega omrežja. Vedno večje so potrebe po integraciji IKS za vodenje distribucijskega sistema z drugimi IKS v podjetju. Že v predhodnih poglavjih je bil predstavljen pomen informacij o stanju in delovanju distribucijskega sistema za različne tehnične službe v podjetju (razvoj, kakovost, priprava podatkov za trgovanje z EE …).



Slika 6.4: Poenotenje podatkovnih struktur na podlagi CIM IEC 61970

Poleg integracije tehničnih IKS je vse bolj pomembna povezava z ne tehničnim IKS v podjetju ter izmenjava informacij med različnimi operaterji omrežij. Upravljanje s sredstvi, posredovanje podatkov o stanju omrežja preko spleta, e-pošte, podatki za vodstvo podjetja … zahtevajo enostaven in učinkovit dostop do tehničnih IKS. Ključni izziv je poenotenje in standardizacija podatkovnih struktur. Potrebna je preslikava podatkov o stanju omrežja v koristne informacije za potrebe tehničnih in ne tehničnih informacijskih sistemov.

V okviru IEC TC57 se je izoblikovala vrsta standardov v družinah SIST EN 61970 (IEC 61970) in SIST EN 61968 (IEC 61968), ki postavlja temelje konceptu MDA (*Model Driven Arhitecture*) - to je koncept platformno neodvisne arhitekture informacijskih sistemov, ki izhaja iz podatkovnih modelov. Operater omrežja vzdržuje model svojega omrežja in procesov tako, da se z njim lahko povezujejo vse združljive aplikacije oziroma informacijski sistemi (npr. SCADA, EMS, DMS, tudi sistemi v merilnem centru ipd…) Glavno vlogo pri modeliranju ima CIM (*Common Information Model*), ki omogoča:

- standardizirani objektni opis omrežja - elementov EES,
- standardizirani objektni opis informacijskih tokov oziroma informacij med različnimi procesi oziroma sistemi.

Poleg načina zapisa modela so definirani tudi standardizirani vmesniki za izmenjavo podatkov - informacije o modelu, kot tudi sami podatki (vrednosti v realnem času, časovne vrste podatkov, ter alarmi in dogodki). Na voljo so preko GID (*Generic Interface Definition*) vmesnikov. CIM in GID sta osnovi za izvedbo UIB (Utility Integration Bus), ki prinaša učinkovito vodilo za integracijo aplikacij oziroma informacijskih sistemov, ki so potrebni za nadzor in vodenje omrežij ter za podporo ostalim procesom. CIM torej omogoča preslikavo podatkov v enotno podatkovno strukturo, ki je standardizirana, in jo zato lahko uporabljajo različni tehnični in netehnični IKS (Slika 6.4).

V koncept se odlično umeščajo tudi uveljavljeni standardi za avtomatizacijo omrežja, kot so SIST EN 61850 na nivoju razdelilnih postaj ter protokoli za prenosno (SIST EN 60870-6) in distribucijsko omrežje (SIST EN 60870-5). CIM prinaša v elektroenergetski sistem standardiziran opis elementov, njihovih lastnosti, relacij in povezav med njimi. CIM temelji na filozofiji objektnega programiranja. Glavne prednosti CIM-a so:

- standardiziran opis vseh elementov EES, vključno z njihovimi atributi,
- v sklopu modela je tudi topološka povezanost elementov,

- standardiziran opis procesov (npr. za obračunske meritve, upravljanje z bremeni, upravljane s sredstvi …),
- model je neodvisen od operacijskega sistema in operacijske platforme,
- omogoča učinkovito integracijo aplikacij različnih proizvajalcev v sisteme vodenja, npr. različnih aplikacij v sklopu DMS funkcij,
- omogoča interoperabilnost med aplikacijami različnih proizvajalcev,
- gre za odprt standard, ki ne zahteva plačevanja licenčnin za uporabo,
- se vključuje v vedno bolj prisoten koncept MDA (*Model Driven Architecture*) [26], [27].

Koncept in navedeni standardi bodo imeli velik vpliv na način oblikovanja in uporabe sodobne informacijske tehnologije tako tehničnih kot netehničnih informacijskih sistemov. CIM ima pomembno vlogo tudi pri poenostavitvi pretoka informacij med različnimi aplikacijami in deli sistema [27].

7 TEHNOLOGIJE TK OMREŽIJ V DISTRIBUCIJI EE

Ethernet omrežje lahko za prenosni medij uporablja žične, optične ali brezžične zveze. Ne glede na fizični medij in tehnologijo pa mora plast nosilnih storitev podpirati prenos IP paketov, torej mora biti omrežni plasti *zagotovljena transparentnost prenosa IP paketa*. V naslednjih poglavjih je predstavljenih nekaj TK tehnologij, na katerih lahko temelji paketni prenos podatkov, ki so v distribuciji EE že uporabljane ali pa se njihova širša uporaba zdi obetajoča.

7.1 Optična TK omrežja

Optična vlakna so najzanesljivejši prenosni medij. Prevajajo svetlobne signale, ki so največkrat vzbujeni z laserskimi izvori. Slabljenje optičnega medija je majhno, omogočajo 100 km dosega brez ponavljalnikov. Kapacitete optičnega kanala presegajo 100 GBit/s, pa tudi kapacitete nad 1 TBit/s niso več nedosegljive.

V elektroenergetiki predstavljajo elektromagnetne motnje zaradi vpliva energetskih naprav potencialno zelo velik problem. Optična vlakna so na tovrstne vplive neobčutljiva, kar je vsekakor dobra lastnost, ki je ne smemo spregledati.

Pokritost: EG sistematično gradi optično omrežje, vendar je za sedaj optično omrežje dostopno le 1 % TP SN/NN.

Perspektivnost: S tehnološkega vidika optična omrežja še nimajo naslednika.

Dostopnost: V EG predvidevamo uporabo optičnega omrežja samo tam, kjer je omrežje že zgrajeno oziroma bo zgrajeno v prihodnjih letih. Po pričakovanju bo na optično omrežje priključenih le nekaj odstotkov TP.

Cena je z ozirom na relativno majhne količine prenesenih podatkov zelo visoka. V primeru že zgrajenega omrežja je cena aktivne opreme grobo primerljiva s ceno aktivne opreme drugih sistemov prenosa podatkov. Razen vzdrževanja sistema pri prenosu podatkov ni drugih stroškov.

7.2 Analogne in digitalne radijske zveze

Na tem mestu obravnavamo radijske komunikacije, ki spadajo v kategorijo PMR (Private Mobile Radio), to so analogne profesionalne (zasebne) mobilne radijske komunikacije. Sistem sestavljajo bazne postaje in mobilne ter fiksne radijske postaje, skladne s standardi MPT-1327, TETRA ali APCO 25. Tipični uporabniki so policija, reševalne službe in upravljavci (elektroenergetskih) infrastrukturnih sistemov. Pomembnejše lastnosti profesionalnih radijskih sistemov so: komunikacijske zveze točka – več točk, dobro pokrivanje večjega področja z radijskim signalom, zaprte skupine uporabnikov, VHF in UHF frekvenčna področja.

Vse večje komunikacijske zahteve že marsikje presegajo zmožnosti analognih sistemov. Na tej osnovi je nastal Digitalni Mobilni Radio (DMR). DMR je nastajajoči evropski telekomunikacijski standard, ki ga je razvil Evropski inštitut za telekomunikacijske standarde (ETSI). DMR naj bi nadomestil analogne PMR sisteme. Opisi standardov so dostopni na spletni strani ETSI.

Pokritost s signalom je odvisna predvsem od uporabljenih frekvenc in delno od tehnologije.

Perspektivnost sistema je slaba. Na tržišču nam, razen že omenjenih tehnologij, še ni uspelo odkriti opreme, ki bi delovala v sistemu točka - več točk na dovolj nizkih frekvencah, z dovolj velikim podatkovnim tokom in za kolikor toliko sprejemljivo ceno. V EG PMR (standard MPT-1327) uporabljamo za komunikacijo z RTU za vodenje TP, kjer pa je podatkovna pasovna širina le 9600 b/s. Tudi naslednja generacija tovrstne opreme ne prinaša nič bistveno novega.

Dostopnost: Nekaj DMR opreme v Sloveniji že deluje (npr. Elektro Maribor), Sintal. Uporablja se enak frekvenčni pas kot za že obstoječo komunikacijo z RTU-ji za vodenje TP.

Cena je odvisna od tehnologije obstoječih sistemov in izbire nadgradnje. V EG bi bilo potrebno zamenjati radijske postaje in ponavljalnike, kar bo zagotovo naslednji korak v nadgradnji obstoječega sistema radijskih zvez EG.

7.3 Uporaba komercialnih brezžičnih omrežij

Slaba lastnost komercialnih brezžičnih omrežij je njihova nezanesljivost in pogosta prezasedenost. Vzpostavljanje povezave povzroča precejšnje zakasnitve. Tudi prenos

podatkovnih paketov ni popolnoma zanesljiv, zato je kljub obstoječi infrastrukturi in dostopnost uporaba teh omrežij v elektroenergetiki sporna, v nekaterih časovno kritičnih aplikacijah celo nemogoča.

GPRS (General Packet Radio Service) je mobilna podatkovna storitev v okviru standarda GSM. Druga generacija GSM omrežij (2G), ki vsebujejo tudi GPRS storitev, predstavljajo vmesno generacijo in jo označujemo kot »2.5G«. Ponuja osnovne možnosti podatkovne komunikacije, za kar uporablja neuporabljene TDMA kanale. GPRS temelji na paketnem prenosu podatkov. S tem se korenito zviša izkoristek omrežja, ko uporabniki le občasno prenašajo večje količine podatkov. GPRS storitev se lahko uporablja kot osnova za prenos podatkov po TCP/IP protokolu. GPRS zagotavlja hitrosti prenosa podatkov 56 do 114 kbit/s. V Sloveniji deluje na 900 in 1800 MHz.

E-GPRS ali EDGE je naslednja razvojna stopnja GPRS in temelji na sodobnejših kodirnih shemah. Omogoča praktične prenose do 180 kbit/s. EDGE so poimenovani tudi "2.75G sistemi".

UMTS (Universal Mobile Telecommunications System) je ena ključnih tehnologij in sestavni del tretje generacije (3G) mobilnih sistemov GSM. Najbolj razširjena je uporaba W-CDMA (Wideband Code Division Multiple Access), ki v teoriji omogoča prenos podatkov s hitrostmi do 14.0 Mbit/s s **HSDPA** (High-Speed Downlink Packet Access), vendar v realnih omrežjih uporabniki dosegajo hitrosti do 384 kbit/s in do 3.6 Mbit/s za HSDPA mobilne terminale pri prenosu podatkov k uporabniku. Precej pozornosti je posvečene tudi razvoju kakovosti in povečanju hitrosti prenosa od uporabnika proti omrežju s pomočjo HSUPA (High-Speed Uplink Packet Access). V daljšem časovnem obdobju se načrtuje povečevanje UMTS hitrosti na 4G, do 100 Mbit/s proti uporabniku in do 50 Mbit/s od uporabnika proti omrežju s pomočjo novih tehnologij vmesnikov OFDM. V Sloveniji UMTS zaseda frekvenčni pas 2100 MHz.

Pokritost: Simobil zagotavlja 90% pokritost z GPRS/EDGE [28] večinoma povsod tam, kjer obstaja GSM signal, podobno tudi Mobitel [29] in Tušmobil [30]. S 3G tehnologijo (UMTS, HSDPA, HSUPA, HSPA) zagotavljajo(ta) operaterji(ja) pokritost predvsem v naseljenih področjih in ob glavnih prometnicah. Operaterji ne objavljajo številk o pokritosti, ampak le zemljevide, npr. [31]. Tušmobil ima dovoljenje za uporabo UMTS frekvenc, podatkov o kakršnikoli pokritosti pa ni.

Perspektivnost: Po neuradnih informacijah naj bi eden od slovenskih mobilnih operaterjev svoje GSM omrežje ugasnil že leta 2013. Licence za to frekvenčno področje kot zadnjemu leta 2026 potečejo Tušmobilu. Za frekvence na UMTS področju potečejo Tušmobilu leta 2023, Mobitelu 2016 ter Simobilu in T-2 leta 2021. Ni pa znano, ali v koncesijskih pogodbah za te frekvence obstaja možnost podaljšanja.

Dostopnost: Omrežja obstajajo in se gradijo še naprej. Pokritost je odvisna od tehnologije 2.5G (GPSR/EDGE) ali 3G in od operaterja.

Cena: Prenos podatkov se plačuje na osnovi količine prenesenih podatkov. Običajno se plača zakupljena količina podatkov (1MB, 100MB …), nad to količino pa vsak kB posebej. Obstaja tudi »flat rate« - neomejena količina na mesec. Operaterji večjim uporabnikom zagotavljajo še dodatne ugodnosti.

7.4 Novejše brezžične tehnologije (WiMAX, WiFi)

WiMax (Worldwide Interoperability for Microwave Access) je brezžični digitalni komunikacijski sistem, ki omogoča brezžično širokopasovno prenašanje podatkov. Namenjen je gradnji »mestnih omrežij« (ang. Metropolitan Area Networks, MAN) pa tudi zagotavljanju širokopasovnih povezav na ruralnih področjih.

Tehnologijo WiMax podrobneje opisuje družina standardov IEEE 802.16x. Osnovni standard nosi oznako IEEE 802.16a; standardi s končnico b, c, d opisujejo različice s povečano funkcionalnostjo in hitrostjo prenosa podatkov v fiksnih brezžičnih omrežjih. IEEE 802.16e opredeljuje tudi pogoje za delovanje v mobilnih omrežjih z možnostjo gostovanja, pripravljajo pa se že nove nadgradnje (802.16h, 802.16m).

Sistemi in naprave WiMax delujejo v različnih frekvenčnih področjih, odvisno od države. V Sloveniji je trenutno določeno frekvenčno področje 3,5 GHz, možna pa so tudi druga. WiMax omogoča hitrost prenašanja podatkov kar do 70 Mbit/s. Pričakovan domet ene postaje WiMax je do 50 km, vendar so testi pokazali, da je lahko ta razdalja manjša. V prihodnje želijo to tehnologijo razširiti na prenosne računalnike in dlančnike.

Pokritost s signalom je odvisna od števila baznih postaj in dodeljenih frekvenc. Za potrebe IKS za aktivna omrežja so zanimiva predvsem nižja frekvenčna področja, ki zagotavljajo veliko pokrivanje tudi brez optične vidljivosti med bazno postajo in naročniško enoto (modem).

Perspektivnost je problematična, predvsem zaradi težavnega pridobivanja licenc za frekvence.

Dostopnost: Podjetji Telekom Slovenije in TOK telekomunikacije sta dobili koncesiji za opravljanje WiMax storitev v frekvenčnem pasu 3,5 GHz. Telekom Slovenije se je neuradno že odpovedal nadaljnji izgradnji omrežja. Frekvence dodeljuje APEK, postopek pridobivanja pa je dolg in povezan z negotovim izidom.

Cena je sestavljena iz cene investicije v lastno omrežje in letnih nadomestil za uporabo frekvenc.

Wi-Fi je blagovna znamka Wi-Fi Alliance (WECA – Wireless Ethernet Compatibility Alliance), nepridobitne organizacije, ki združuje preko 300 podjetij, katerih izdelki temeljijo na standardu IEEE 802.11 (WLAN). Standard zagotavlja brezžično povezljivost med različnimi napravami, npr. med PC, dlančniki, mobilnimi telefoni, tiskalniki, zabavno elektroniko. Wi-Fi se pogosto uporablja kot nadgradnja fiksnega Ethernet omrežja v stavbah, kjer omogoča enostavno brezžično povezljivost prej omenjenih naprav. Običajen doseg brezžične Wi-Fi dostopovne točke v zgradbah je nekaj deset metrov. Pogosta je uporaba Wi-Fi v hotelih, restavracijah, letališčih, … za brezplačen dostop do Interneta. Wi-Fi se uporablja tudi za povezovanje dveh naprav (točka – točka).

Wi-Fi omrežja imajo omejen doseg. Tako ima običajen usmerjevalnik za domačo uporabo doseg nekaj deset metrov v stavbi in do 100 metrov na prostem. Doseg je odvisen tudi od uporabljenega frekvenčnega pasu (večji doseg pri 2.4 GHz področju kot pri 5 GHz). Na prostem se z usmerjenimi antenami lahko doseže doseg do nekaj km. V Sloveniji se uporablja Wi-Fi na 2.4 GHz področju. Pri tem je treba upoštevati, da se prenosna zmogljivost deli s številom uporabnikov, ki istočasno uporabljajo posamezno pristopno točko.

Wi-Fi osnovno varnost zagotavlja z WEP (ang. Wireless Equivalent Privacy), ki pa je problematičen. Nadgradnjo predstavlja Wi-Fi Protected Access (WPA ali WPA2 – IEEE 802.11i), ki zagotavlja ustrezno varnost.

V svetu niso redki primeri mestnih Wi-Fi omrežij, npr. Sunnyvale (Kalifornija), City of St. Cloud (Florida), Norwitch, Leeds, Liverpool, London (V. Britanija), mesto Luksemburg, Moskva … ki omogočajo prost dostop do Interneta. Prednost Wi-Fi je zagotovo njegova preprosta uporaba, razširjenost in s tem cenovno ugodna komunikacijska oprema. Slabost Wi-Fi je nizek nivo varnosti pri neuporabi sodobnih varnostnih mehanizmov in dejstvo, da v Sloveniji niti v večjih mestih ni sistematično grajenega mestnega Wi-Fi omrežja.

Pokritost: Tehnologija Wi-Fi je načeloma primerna samo za področja z veliko gostoto uporabnikov, saj je področje pokrivanja enega hotspota (bazne postaje) približno en kilometer (frekvenčno področje 2,4 GHz!!!). Sistem deluje na javnih frekvencah, zato je izpostavljenost motnjam velika.

Perspektivnost: Frekvence so nelicencirane in se bodo za podobne namene zagotovo uporabljale še kar nekaj časa. Na tržišču je neomejeno število ponudnikov opreme.

Dostopnost: Uporabljati je mogoče javna omrežja MetroWi-Fi ali zgraditi lastno omrežje, če javno ne obstaja. Na Gorenjskem (še) ni ponudnikov komercialnih Wi-Fi storitev razen Domenca d.o.o. Gradnja lastnega Wi-Fi omrežja bi bila smiselna le na področjih z zelo veliko gostoto uporabnikov (mestna središča, poslovne cone).

Cena: Stroški izvedbe in obratovanja bi bili zelo nizki. Obstaja veliko število ponudnikov opreme, ki je dostopna skoraj v vsaki bolje založeni tehnični trgovini, stroškov z licencami pa ni.

7.5 Pregled prednosti in slabosti TK tehnologij za paketni prenos podatkov v DEE

V tabeli 7.1 so podane najpomembnejše lastnosti TK tehnologij za paketni prenos podatkov, ki so bile predstavljene v predhodnih poglavjih.

Tabela 7.1: Prednosti in slabosti TK tehnologij za paketni prenos podatkov

	Optika	Mobilna omrežja	WiMax	WiFi	Radio
+	• varana, zanesljiva • lastno omrežje • neobčutljivost na EM motnje EE naprav	• preprosta izvedba, • javna omrežja, (skoraj) povsod razširjena • najeta storitev prenosa podatkov	• lastno omrežje, • področje pokrivanja z ene bazne postaje je veliko • že obstoječa ostala infrastruktura (linki, stolp, prostor, UPS…)	• lastno, lahko tudi najeto omrežje • relativno nizka cena opreme (modemov)	• izgrajeno omrežje, pridobljene frekvence • privatni sistem (varnost!) • veliko področje pokrivanja (UHF)
-	• draga, nerazširjena	• plačuje se vsak preneseni bit podatkov • ni zagotovljenega nivoja kvalitete storitev • nezanesljivost prenosa, • velike časovne zakasnitve, • prespektivnost posamezne tehnologije je odvisna od ekon. interesa operaterja	• licencirane frekvence – cena ?! • negotovi postopki pridobivanja frekvenc	• zelo majhno področje pokrivanja ene bazne postaje (hot spot) • delovanje na javnih frekvencah • potrebno močno kriptiranje, • relativno lahek zlonamerni vdor v sistem	• razen DMR na trgu še ni sprejemljive point to multipoint rešitve • radijsko omrežje je občutljivo na motnje
PRENOS	• ekstremna kapaciteta prenosa	• hitrost prenosa podatkov: - srednja (GPRS), - srednje velika (EDGE), - velika (HSPA)	• srednje visoka hitrost prenosa podatkov	• visoka hitrost pri prostem omrežju, • z zasedenostjo omrežja hitrost strmo pada	• nizka hitrost, tudi pri digitalnem radiu (DMR)

7.6 Potrebna kapaciteta komunikacijskega kanala

Potrebno kapaciteto komunikacijskega kanala med posamezno TP in sedežem podjetja bomo določili na podlagi delovanja obstoječih sistemov vodenja (RTU z radijsko komunikacijo v TP) in pilotnega projekta AMI sistema (TP »Komunalni servis« v Stražišču pri Kranju) ter pilotnih projektov telemetričnih obratovalnih meritev z merilnimi centri IskraMIS (MI xxx, MC xxx).

7.6.1 Potrebna kapaciteta prenosa podatkov iz AMI koncentratorja (ftp, webservices)

AMI sistem TP Komunalni servis vključuje 88 gospodinjstev. Odčitavajo se urne vrednosti odjema električne energije, tople in hladne vode ter ogrevanja. Na mesec se s ftp protokolom prenese 25 MB, na leto torej 300 MB.

Z implementacijo Webservices naj bi se prenašale samo spremembe, torej meritve od zadnjega uspešnega prenosa podatkov v merilni center. Po pričakovanjih bo potrebno mesečno prenesti precej manj podatkov, vendar testiranje še ni bilo izvedeno.

7.6.2 Potrebna kapaciteta za prenos podatkov iz merilnih centrov MIxxx in MCxxx

Trenutno komunikacija z merilnimi centri deluje po metodi periodičnega pozivanja (pull) merilnega centra. Bodoči sistem bo zmožen tudi sam pošiljati (push) alarme, anomalije, poročila o kakovosti, s čimer se bo potrebna količina prenesenih podatkov zmanjšala. Izračun, ki ga je podal proizvajalec IskraMIS, je za oba tipa merilnih centrov enak. Predpostavlja se 16 merilnih veličin, čas vzorčenja 5 je minut, letno pričakovanih je 1.000 alarmov, 1.000 poročil kakovosti in 5.000 anomalij po push sistemu, podatki so v Long Binary Format-u. Rezultat izračuna kaže, da bi bilo potrebno iz posameznega merilnega centra prenesti 15,6 MB podatkov na leto.

7.6.3 Potrebna kapaciteta za delovanje RTU – dolžina sporočil

Moscad RTU ob uporabi fiksne zveze (npr. optika) na vsakih 5 min poziva center zato, da preverja delovanje povezave. Vsak poziv je dolg 50 Bytov, kar pomeni približno 15 kB na dan. Glede na statistiko je k temu potrebno dodati še približno 50 Bytov na dan za morebitne

dogodke. Ob uporabi radijskih povezav se postopek preverjanja izvaja na 8 ur, za kar je potrebno prenesti približno 300 Bytov na dan. Količina prenesenih podatkov ob izpadih je enaka kot v primeru fiksnih povezav (50 B/dan). Na leto lahko pričakujemo prenos manj kot 6 MB podatkov.

7.6.4 Potrebna skupna kapaciteta

Večino kapacitet trenutno zasede prenos številčnih podatkov, ostale količine podatkov so bolj ali manj zanemarljive. Problem pa ni samo v prepustnosti, širini kanala, ampak tudi v potrebnih časovnih intervalih, v katerih odčitavamo želene količine podatkov. Praktične izkušnje kažejo, da je za prenos datoteke po ftp protokolu iz AMI koncentratorja potreben zelo različen čas: od nekaj minut do nekaj ur. Potreben čas je odvisen od mnogih parametrov: kvalitete in zasedenosti omrežja, uporabljene opreme, omejitev, ki jih postavlja ponudnik storitev; mobilni operater nam na področju EG dovoljuje samo 60 istočasnih odčitavanj (povezav).

Povzetek: če upoštevamo le potrebno pasovno širino (vsota prenesenih podatkov/časovno enoto), je GPRS/EDGE prenos podatkov zelo verjetno zadovoljiv. Z upoštevanjem neperspektivnosti GPRS tehnologije in dejstva, da bo moral IKS za aktivna omrežja zadovoljiti tudi potrebe novih elementov v distribucijskem sistemu (hranilniki EE, sodobne kompenzacijske naprave, zahtevnejši sistemi za upravljanje razpršene proizvodnje), pa je pri gradnji lastnega omrežja primerneje razmišljati o WiMax tehnologiji, širitvi lastnega optičnega omrežja in uporabi najzmogljivejših mobilnih omrežij (UMTS 3G, 4G).

8 VARNOST INFORMACIJSKO-KOMUNIKACIJSKEGA SISTEMA

Iluzorno in neodgovorno je pričakovati, da do napada na telekomunikacijski sistem ne bo prišlo. Izgovori o »zunanjih dejavnikih, na katere nismo imeli vpliva«, po uspešnem napadu in povzročeni škodi ne pomagajo. Strategije vojaške obrambe temeljijo na natančnem analiziranju moči, taktike, strategije, sredstev, vzrokov/motivov … za napad. Tudi pri obrambi IKS velja, da je natančno poznavanje »nasprotnika« ključnega pomena za načrtovanje učinkovite obrambe.

Varnost IKS se nanaša predvsem na varnost podatkov in sporočil, pri čemer moramo imeti v mislih zagotavljanje celovitosti podatkov in sporočil. Pod pojmom celovitost razumemo:

- zasebnost (vsebina sporočil in podatkov je dostopna le upravičenemu uporabniku),
- verodostojnost (sporočilo ali podatek ni bil (ne)namerno spremenjen) in
- avtentičnost (nedvomno je znana identiteta izvora podatka ali sporočila) [32].

Cilj varovanja IKS je torej zagotavljanje celovitosti podatkov in sporočil. Varovanje IKS zato obsega:

- zaščito pred nepooblaščenim spreminjanjem, uničevanjem ali razkritjem podatkov,
- zagotavljanje pravilnega delovanja sistema,
- zagotavljanje integritete podatkov ter
- preprečevanje škodljivih vplivov na delovanje sistema in izvajanje storitev.

To poglavje obravnava vidike groženj in napadov na IKS, ki jih moramo upoštevati pri načrtovanju uspešne obrambe pred nevarnostmi, ki lahko ogrozijo naš sistem. Varovanje telekomunikacijskega sistema izvajamo s pomočjo *varnostnih naprav*. Pravilno uporabo varnostnih naprav in vse vidike udejanjanja varovanja sistema pa določa *varnostna politika*.

8.1 Pojem varnosti informacijsko-komunikacijskih sistemov

Vidiki varnosti IKS so *zaupnost*, *integriteta* in *razpoložljivost* sistema. *Zaupnost* se nanaša na preprečevanje nepooblaščenega razkritja občutljivih, t.j. zaupnih informacij. *Integriteta* IKS pomeni odpornost pred nepooblaščenim spreminjanjem samega IKS. *Razpoložljivost* je

zagotavljanje nemotenega in neprekinjenega delovanja sistema in izvajanja informacijsko-komunikacijskih storitev [24].

8.2 Grožnje varnosti informacijsko-komunikacijskega sistema

Varnost IKS ogrožajo zlonamerni programi, tuja ali naša (ne)namerna napačna dejanja ter napake na strojni opremi.

Integriteto IKS ogrožajo računalniški virusi, logične bombe, »stranska« vrata (Back Door) in (ne)namerne napake uporabnikov. V nadaljevanju je navedenih nekaj najpogostejših načinov napada na IKS.

Računalniški virus je programska koda, ki se je sposobna razmnoževati in prenašati v računalniku brez vednosti in volje uporabnika. Ko se razmnoži, lahko tudi prične s škodljivim vedenjem (na primer brisanje podatkov na trdem disku). Njegovo vedenje je zelo podobno biološkemu virusu. Gostitelj virusa je računalniški program oziroma izvršna datoteka. Med razmnoževanjem in prenašanjem se začasno naseli tudi v ostale dele pomnilnika (slikovne datoteke, sistemski del trdega diska ...).

Trojanski konj ali trojanski virus je na prvi pogled nenevaren ali koristen program, ki pa vsebuje zlonamerno kodo.

Logična bomba je zlonameren program, ki se aktivira ob izpolnitvi določenega (logičnega) pogoja, npr. pretečen čas, količina podatkov …

Stranska vrata so skrivni, nedokumentirani načini dostopa do sistema. Običajno jih za namen vzdrževanja vzpostavijo sistemski programerji.

(Ne)namerne napake uporabnikov sistema so posledica (ne)namernega kršenja varnostne politike. Lahko neposredno ogrožajo korektno delovanje strojne opreme ali sistema z neustrezno uporabo/poseganjem v programsko opremo IKS.

Zaupnost IKS ogroža opazovanje delovanja sistema, t.i. brskanje prek rame, kraja gesel in nepravilno ravnanje z gesli, prisluškovanje omrežnemu prometu.

Z opazovanjem delovanja IKS in dejanj uporabnikov sistema, t.i. brskanjem prek rame, je mogoče pridobiti pomembne podatke o uporabi in uporabnikih sistema, njihovih geslih za dostop, vsebini sporočil…

Nepravilno in neodgovorno ravnanje z gesli lahko privede do kraje in posledično zlorabe gesla za nedovoljen dostop do zaupnih podatkov, ki se prenašajo preko IKS. Kraja administratorskih gesel je še posebej kritična. Poznavalcu sistema in programske opreme dovoljuje spreminjanje delovanja sistema s ciljem sistematičnega zbiranja zaupnih podatkov.

Prisluškovanje omrežnemu prometu je mogoče realizirati z nedovoljenim fizičnim priklopom na komunikacijski vod, stikalo ali drugo komunikacijsko opremo. Prisluškovanju so še posebej izpostavljena brezžična privatna omrežja, saj je s komercialno dostopno opremo mogoče nemoteno prisluškovati radijskemu prometu v radiju oddajanja signala dostopovne točke.

Razpoložljivost IKS ogrožajo naravne katastrofe (požar, poplava, potres …), okvare komponent sistema, napadi zavrnitve storitve (DoS). Zaradi teh dejavnikov je lahko občasno ali trajno prekinjeno oz. oslabljeno delovanje IKS.

8.3 Ranljivost in napadi na informacijsko-komunikacijski sistem

Ranljivost je vsaka točka v programskem paketu in/ali strojni opremi, ki omogoča uporabniku IKS, da spremeni program ali strojno opremo oziroma pridobi dostop do sistema na način, ki ni bil predviden. Ranljivost IKS povečujejo:

- pomanjkljiva varnostna politika: podjetje nima (ustrezne) varnostne politike, varnostna politika ni celovita, ne pokriva vseh vidikov varne uporabe IKS, ni izdelanih natančnih načrtov ravnanja v primeru katastrof, varnostna politika se ne nadgrajuje sistematično, pomanjkljiv je tudi nadzor zapisov in dostopa do IKS;
- konfiguracijske slabosti: napačno konfigurirana oprema, slaba ali nezavarovana gesla, napačne nastavitve varnostnih naprav ali uporaba osnovnih nastavitev;
- in tehnološke slabosti sistema: slabosti operacijskih sistemov, slabosti protokolov in aplikacij, slabosti omrežne opreme.

Napad je nameren poizkus izkoriščanja ranljivosti IKS z metodami izogibanja varnostnim mehanizmom. Namen napada je onesposobiti omrežje, zmanjšati njegovo prepustnost, uničiti ali odtujiti zaupne podatke. Napad je lahko organiziran (strukturiran napad) in usmerjen na točno določen cilj ali pa napad ni organiziran in ni usmerjen na točno določeno podjetje, IKS ali njegov sestavni del (nestrukturiran napad). Tipi napadov na IKS so:

- poizvedovalni napad: njihov cilj je zbrati čim več podatkov o omrežju, njegovi konfiguraciji, načinu delovanja, izvajanju storitev, ugotavljanju ranljivosti, ki bodo omogočale kasnejši vdor v sistem;
- napadi s poskusom dostopa: glavni cilj je izrabiti ranljivost IKS in pridobiti dostop do omrežja, s tem pa dostop do zaupnih informacij;
- napadi z zavrnitvijo storitve (DoS): namen teh napadov je onemogočanje delovanja IKS.

8.4 Gradniki zaščite informacijsko-komunikacijskega sistema

V tem poglavju bodo so na kratko predstavljeni glavni gradniki zaščite IKS. Katere gradnike bomo izbrali in kako jih bomo uporabili, je odvisno od namena IKS, njegove izpostavljenosti napadom in sredstev, ki smo jih pripravljeni plačati za zagotovitev (ustreznega nivoja) varnosti.

Tabela 8.1: Gradniki zaščite IKS

	Gradnik zaščite IKS	***Vloga in pomen gradnika***
1	Varnostna politika	Strategija zaščite; kdo/kaj (ne)sme, kako je sistem zaščiten, odgovornost za izvajanje aktivnosti za zagotavljanje varnosti
2	Avtentikacija, avtorizacija, zapisovanje	Zagotavljanje nadzorovanega dostopa do IKS in aplikacij, zapisovanje informacij o dostopu
3	Dinamična primarna zaščita	Primarna zaščita, zaznavanje in odgovarjanje na napade: usmerjevalniki, požarne pregrade, sistemi IDP; Segmentacija omrežja, t.j. delitev IKS glede na stopnjo potrebne zaščite.
4	VPN	»Navidezna privatna omrežja« zagotavljajo varno povezavo
5	Zaščita klientov	Zadnja obrambna linija, ugotavljanje nenormalnih aktivnosti in ustrezno ukrepanje
6	Varnost kot proces	Stalno učinkovito nadziranje pretoka podatkov, ugotavljanje nepravilnosti; Korelacija in iskanje trendov, t.j. primerjanje informacij o delovanju zaščitnih naprav s ciljem ugotavljanja razsežnosti napada; Proces stalnih izboljšav varnostnega sistema.

8.4.1 Varnostna politika

Načrtovanje in implementacija varnostne politike je specifična za vsako podjetje posebej. Vsestranska podpora vodstva podjetja je predpogoj za uspešno izvajanje katerekoli politike podjetja, še posebej varnostne politike.

Varnostna politika opredeljuje vse postopke in navodila za varno uporabo komunikacijskega omrežja. Nanaša se na vse procese in izvajalce procesov v podjetju in zunanje udeležence v procesih podjetja oziroma uporabnike IKS. Varnostna politika določa sprejemljivo uporabo IKS ter vlogo in pristojnosti uporabnika. Pri oblikovanju varnostne politike moramo upoštevati načela, ki so predstavljena v nadaljevanju.

Doslednost in celovitost

Varnostna politika mora obravnavati vse vidike uporabe IKS. V nobenem primeru ne sme biti prepuščeno uporabniku, da si sam določa pravila, po katerih se bo ravnal pri uporabi IKS. Izvajaje varnostne politike je naloga celotnega kolektiva v podjetju. Najvišje vodstvo mora varnostno politiko v celoti podpirati in jo tudi izvajati.

Razumljivost

Varnostna politika je namenjena vsem uporabnikom v podjetju, zato ne sme biti napisana kot tehnični dokument. Tudi ne-tehnikom mora biti razumljiva in nezapletena, uporabnikom ne sme povzročati težav pri njenem razumevanju in upoštevanju.

Enoumno določena odgovornost in pristojnost

Odgovornost in pristojnost uprave, uporabnikov in administratorjev mora jasno določena. Opredeljeni morajo biti ukrepi ob kršitvah varnostne politike.

Ukrepanje ob incidentih

Varnostna politika mora natančno obravnavati ravnanje ob pojavu posameznih oblik incidentov. Odgovornost in pristojnost uprave, uporabnikov in administratorjev mora biti jasno določena. Opredeljeni morajo biti ukrepi ob kršitvah varnostne politike.

Stalno izboljševanje varnostne politike

Varnostno politiko moramo nenehno nadgrajevati in izboljševati. Podjetje mora razumeti varnostno politiko kot enega od ključnih procesov, ki mora biti podvržen nenehnemu izboljševanju kakovosti.

8.4.2 Avtentikacija, avtorizacija, zapisovanje

Preverjanje identitete uporabnika je v elektronskem poslovanju ključnega pomena. Za zagotavljanje nemotenega poslovanja mora podjetje zagotoviti dostop do pomembnih podatkov in aplikacij različnim notranjim in zunanjim uporabnikom. Brez zanesljive

avtentikacije (overjanja) uporabnikov so ključne informacije podjetja izpostavljene poneverjanju, kraji in neupravičeni uporabi. Posebno pozornost je potrebno nameniti zaščiti pred nedovoljenim dostopom do podatkov in aplikacij s strani oseb, ki jim sicer dovoljujemo fizični stik z našimi napravami. To so pogodbeni izvajalci vzdrževanja, gostje podjetja, stranke, poslovni partnerji.

Preverjanje identitete temelji na avtentikaciji (angl. **A**vtentication), avtorizaciji (angl. **A**uthorization) in zapisovanju dogodkov (ang. **A**ccouting), ki jih s kratico označujemo AAA.

Avtentikacija je preverjanje veljavnosti identitete, s katero se predstavlja uporabnik. Mehanizmi preverjanja so: uporabniško ime in geslo, odzivi uporabnika, ipd. Zaradi svoje pomembnosti za varnost obravnavanega IKS je podrobneje predstavljena v poglavju 8.5.

Avtorizacija določa, do katerih virov je uporabnik upravičen in katere operacije lahko izvaja po uspešni avtentikaciji. Avtorizacija deluje s pomočjo preverjanja atributov, ki opisujejo avtorizacijo uporabnika z informacijami shranjenimi v podatkovni bazi.

Zapisovanje (Accouting) vseh dogodkov v povezavi z uporabnikom IKS, kot so začetni in končni čas povezave, izvedeni ukazi, število prenesenih podatkovnih paketov, identiteta uporabnika … izkoriščamo za zaračunavanje informacijsko-komunikacijskih storitev, z podrobno analizo tako pridobljenih podatkov pa lahko odkrijemo zlonamerna ravnanja posameznika ali posledice, ki jih je povzročil napad na IKS.

8.4.3 Dinamična primarna zaščita

V preteklosti je bilo zagotavljanje varnosti IKS osredotočeno predvsem na ločevanje »varnih« lokalnih omrežij (LAN) od ostalega omrežja (WLAN) s požarnimi pregradami[16]. Dandanes je z vedno bolj povezanimi IKS zagotavljanje varnosti preseglo okvir požarne pregrade. Nenazadnje predstavljajo največjo grožnjo varnosti nezadovoljni, zlonamerni ali neosveščeni zaposleni, ki povzročijo tudi največ varnostnih vdorov in nepooblaščenih dostopov do varovanih delov informacijskih sistemov. Zagotavljanje varnosti se mora zato osredotočiti na ugotavljanje in nadzorovanje groženj in ranljivosti informacijskega sistema. Pri varnosti informacijskega sistema gre predvsem za vzpostavitev preventivnih korakov, ki prispevajo k varovanju podatkov in zakrivanju ranljivosti informacijskega sistema pred grožnjami [33].

---

[16] Požarne pregrade (ang. firewall) se v gradbeništvu uporabljajo za ločevanje posameznih delov stavb z namenom, da ob izbruhu požara v enem delu stavbe preprečimo ali vsaj upočasnimo uničujoče širjenje požara. Požarna pregrada v zaščiti informacijsko komunikacijskih sistemov je sistem strojne in programske opreme, ki ločuje dele komunikacijskega omrežja z namenom preprečevanja prehoda zlonamernih podatkov.

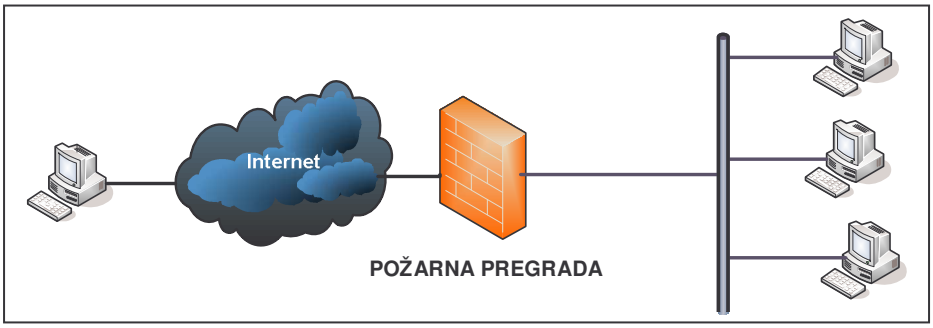
Dinamična primarna zaščita izvaja politiko kontrole dostopa do varovanega IKS. Kontrola dostopa do IKS je skoncentrirana na nekaj točk v IKS. Če je njena postavitev pravilno načrtovana, je uveljavljanje varnostne politike enostavno, skalabilno in robustno. Izvedena je v obliki t.i. **požarnih pregrad** in **sistemov za zaznavanje in preprečevanje napadov**, ki predstavljajo nadgradnjo požarnih pregrad.

Politika kontrole dostopa deluje na različnih nivojih:

- Kontrola povezljivosti določa, kdo lahko dostopa do varovanega IKS in kdo ne, preprečuje dostop nezaupanja vrednim uporabnikom;
- Kontrola protokola omejuje, kaj lahko uporabnik počne znotraj IKS; preprečuje izkoriščanje pomanjkljivosti v komunikacijskem protokolu;
- Kontrola podatkov omejuje izmenjavo podatkov; preprečuje pošiljanje zlonamernih podatkov strežnikom in klientom.

Požarna pregrada mora biti edina prehodna točka med dvema IKS. To pomeni, da mora celoten promet med zaščitenim sistemom in ostalimi sistemi potekati skozi požarno pregrado. Dosledna uporaba prehoda skozi požarno pregrado odpravlja grožnjo, ki jo sistemu predstavljajo stranska vrata (backdoor povezave).

S požarnimi pregradami lahko dosežemo tudi različne nivoje varovanja IKS, glede na potrebno stopnjo zaščite posameznega dela IKS (segmentacija IKS).



Slika 8.1 Požarna pregrada

Uporaba požarne pregrade pa lahko povzroča tudi težave, še posebej, če je napačno ali neoptimalno nastavljena. Tako imajo lahko nekatere aplikacije težave pri (varnem) delovanju ali pa pregrada predstavlja (pre)ozko grlo glede pretoka podatkov. Požarne pregrade je mogoče glede na sloj protokola, na katerem delujejo, razdeliti na tri vrste:

- paketni filter (packet filter),

- nadomestni strežnik, realizacija aplikacijskih prehodov (proxy server),
- paketno filtriranje z upoštevanjem vseh stanj (stateful inspection).

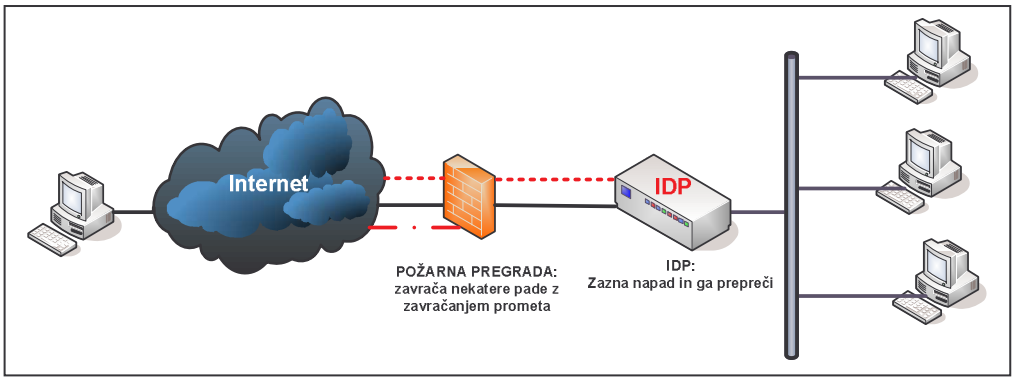
Običajno so požarne pregrade zgrajene na osnovi vseh zgoraj naštetih tehnologij.

Sistemi za odkrivanje in preprečevanje napadov

Napadi na IKS se dogajajo na različnih nivojih. Nekateri napadi so na omrežnem nivoju, drugi na aplikacijskem ali pa je napad usmerjen na več nivojev hkrati (hibridni napadi). Kakovostna zaščita sistema mora biti sposobna odkrivanja in preprečevanja napadov na vseh nivojih.

Za znane vzorce napadov obstajajo tudi zanesljive in preizkušene metode zaščite, vgrajene v požarne pregrade. Novi načini napadov pa se pogosto neodkriti prebijejo skozi požarno pregrado in jih moramo prepoznati še preden povzročijo (večjo) škodo našemu IKS.

Zaznavanje napada, ki je prešel požarno pregrado, predstavlja drugi nivo zaščite IKS. Sisteme za odkrivanje napadov, ki nimajo zmožnosti preprečevanja napadov, označujemo s kratico IDS (Intrusion Detection System). IDP sistemi (Intrusion Detection & Prevention System) so kompleksnejši, saj poleg odkritja napada le-tega lahko tudi preprečijo.



Slika 8.2 Drugi nivo zaščite – sistem za odkrivanje in preprečevanje napada (IDP)

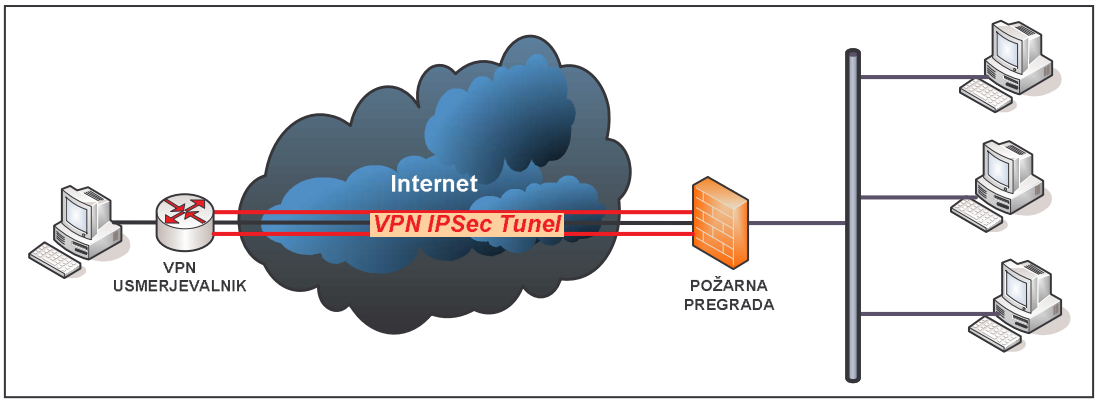
IDS sistemi običajno delujejo v kombinaciji s požarno pregrado. Ko IDS zazna napad, poda požarni pregradi zahtevo za prekinitev povezave z virom zlonamernih podatkov (TCP reset funkcionalnost). Velika pomanjkljivost sistema je omogočanje napadov z zavrnitvijo storitve (DoS).

IDP sistemi omogočajo uporabniško odločitev glede odgovora na zaznan napad (dovoli promet, prekini promet, zabeleži dogodek …). Delujejo za požarno pregrado in lahko ustavljajo napade na aplikacijskem nivoju. IDP sistemi nadzirajo omrežni promet od drugega

do sedmega sloja ISO –OSI modela, medtem ko požarne pregrade nadzirajo le promet od drugega do četrtega sloja.

8.4.4 Navidezno privatno omrežje – VPN

Internet se je razvil v (skoraj) povsod prisotno telekomunikacijsko okolje, ki omogoča izmenjavo velikih količin podatkov. Postavlja se vprašanje ali lahko uporabljamo Internet tudi za vzpostavljanje privatnih omrežij, ne da bi fizično gradili ločena privatna omrežja. Odgovor na to vprašanje so navidezna privatna omrežja (VPN). VPN je torej sredstvo za varno komunikacijo med dvema lokacijama, ki sta s pomočjo »varnega tunela« povezani preko javne infrastrukture (Internet) Gradnjo varnega tunela omogoča IPSec protokol, ki je eden od t.i. tunelskih protokolov.



Slika 8.3 Tunelski način prenosa podatkov - IPSec VPN

IPSec tunel sestavlja par enosmernih varnostnih povezav[17] (SA), ki opravlja naslednje varnostne funkcije:

- zasebnost s pomočjo enkripcije,
- vsebinsko celovitost s pomočjo avtentikacije,
- pošiljateljevo pristnost.

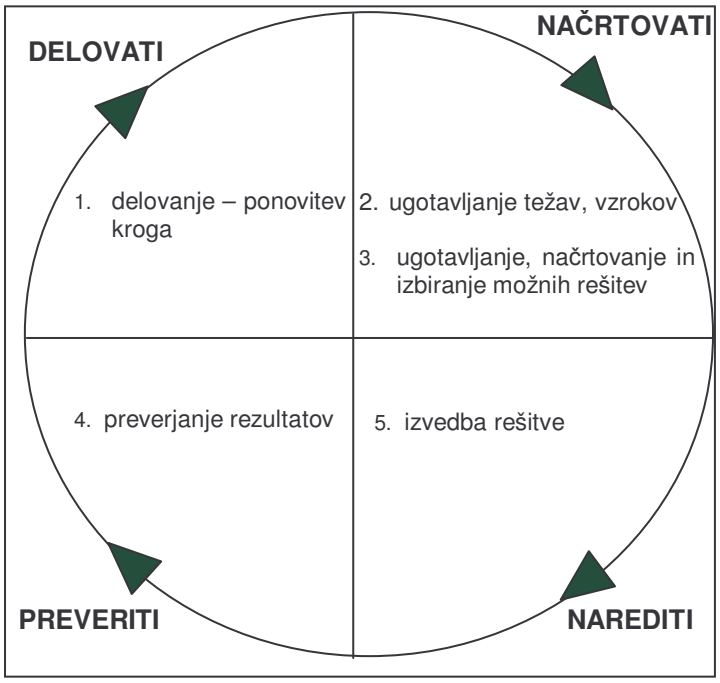
IPSec temelji na šifriranju in ovijanju (ang. encapsulation) prometa za namen prenosa preko IP omrežja. V tunelskem načinu delovanja IPSec je izvornemu IP paketu dodana nova glava AH (Avtentication Header). S tem je zagotovljena avtentikacija izvora IP paketa in preverjanje celovitosti vsebine.

[17] Varnostne povezave – (ang. Security Associations; SA) so nabor politik in ključev, ki se uporabljajo za zaščito informacij med dvema sogovornikoma.

8.4.5 Varnost kot proces

Varnost omrežja moramo razumeti kot proces, v katerem se na vseh nivojih nenehno izvajajo naslednje aktivnosti:

- zaščita, ki vključuje avtentikacijo in preverjanje identitete, enkripcijo, delovanje VPN…
- nadzor, ki ga izvajamo z zaznavanjem in preprečevanjem vdorov v sistem ter zaznavanjem in odstranjevanjem sumljive vsebine sporočil;
- preverjanje ranljivosti varnostnega stanja z izvajanjem podrobnega pregledovanja delovanja sistema, preverjanje aplikacij in testiranje popravkov aplikacij;
- upravljanje omrežne varnosti, varnostnih naprav in izvajanje analize dogodkov in podatkov o delovanju omrežja in omrežnih naprav.



Slika 8.4: Demingov krog stalnih izboljšav

Filozofija neprestanih izboljšav (varnostnih) procesov mora vključevati sodelovanje vsakega posameznika v organizaciji. Uporablja se koncept inovativnih izboljšav[18], t.i.

[18] Programe za izboljšanje poslovnih procesov opredeljujejo standardi ISO. Elektro Gorenjska, d.d., je pridobila certifikate ISO9001:2000, ISO 14001, OHSAS 18001. Poteguje se tudi za priznanje RS za poslovno odličnost po evropskem modelu EFQM.

Demingov krog: načrtovati – narediti – preveriti – delovati (angl: plan – do – check – act: PDCA) (Slika 8.4) [34].

8.5 Vloga avtentikacije pri zagotavljanju varnosti IKS

Varnostni sistemi v lokalnem omrežju, kot so IDS in IDP sistemi, vsekakor prispevajo k zagotavljanju varnosti IKS. Ključnega problema, to je nadzora nad uporabo aplikacij in dostopa do podatkov, pa ne rešujejo v celoti. IDS in IDP sistemi nadzirajo podatkovni promet v lokalnem omrežju, pa tudi prenos podatkov med posameznimi aplikacijami. Vendar pa ostaja odprto vprašanje, ali ima uporabnik, ki navidez korektno uporablja neko aplikacijo ali dostopa do podatkov, tudi pravico, da to počne.

Dodaten problem predstavljajo brezžična lokalna omrežja (WLAN). Prenosni medij pri teh omrežjih ni zaseben. Za razliko od ožičenih lokalnih omrežij, kjer mora imeti uporabnik fizičen dostop do omrežnega priključka, se v WLAN priključi vsak, ki se nahaja v dosegu radijskega signala brezžične dostopovne točke. Zaradi možnosti prisluškovanja lokalnemu podatkovnemu prometu je v brezžičnih omrežjih nujno potrebno zagotoviti tudi šifriranje podatkov.

Pravico dostopa in način uporabe aplikacij in podatkov v informacijskem sistemu nekega podjetja predpisuje *varnostna politika*. Za vsakega uporabnika, tako notranjega kot zunanjega, morajo biti pravice natančno določene. Uporabniku je potrebno omogočiti dostop do podatkov in uporabo le tistih podatkov in aplikacij, ki jih potrebuje. Zatorej morajo biti pravice uporabnika IKS individualno določene. **Avtentikacija**, to je preverjanje identitete uporabnika IKS, je predpogoj za **avtorizacijo**[19]**,** t.j. dodeljevanje individualnih pravic uporabnika.

Izvajanje avtentikacije vseh uporabnikov zahteva drugačno arhitekturo lokalnih omrežij in uvajanje novih tehnologij.

V naslednjih poglavjih bo predstavljen splošen princip avtentikacije, sledila pa bo predstavitev nekaj značilnih metod avtentikacije za specifična področja uporabe, njihove prednosti in pomanjkljivosti.

---

[19] SSKJ: **avtorizacija -e ž (a)** uradno dovoljenje; potrdilo, pooblastilo: dobiti avtorizacijo … * jur. uradno dovoljenje za zasebno opravljanje kake dejavnosti, zlasti tehnične

8.5.1 Splošni princip in metode avtentikacije

Danes predstavlja avtentikacija začetek vsake uporabe IKS. Pri avtentikaciji v osnovi ločimo dva pristopa: avtentikacijo virov sporočanja in avtentikacijo samih sporočil.

Avtentikacija vira pomeni ugotavljanje identitete uporabnika IKS ali storitve, pri kateri želimo z veliko verjetnostjo zagotoviti, da je uporabnik (vir) resnično oseba, za katero se predstavlja. Preverjanje se mora izvesti v realnem času ob prijavi uporabnika (vira) in velja le za čas med uspešno avtentikacijo in prekinitvijo prijave uporabnika. Na ta način je preprečen poskus vrivanja neavtenticiranih uporabnikov.

Pri **avtentikaciji sporočil** ni nevarnosti vrivanja, kot pri avtentikaciji virov, saj vedno avtenticiramo sporočilo v celoti. Preverjanje avtentičnosti sporočila lahko tudi odložimo (ni potrebe po preverjanju v realnem času), opravimo ga takrat, ko sporočilo potrebujemo.

Za avtentikacijo virov lahko uporabljamo naslednje metode:

- **metode s fiksnim geslom:** najbolj razširjena in pogosto uporabljana metoda; dokazovalec posreduje overitelju kombinacijo osebnega imena (user name) in fiksnega gesla (password); overitelj preveri, če kombinacija imena in gesla ustreza in s tem je avtentikacija zaključena; uporaba te metode zagotavlja le šibko avtentikacijo;
- **metode izziv - odgovor:** spada med močne avtentikacijske metode; dokazila o avtentičnosti dokazovalec ne pošilja overitelju preko komunikacijskega kanala, kar v veliki meri preprečuje možnost prevzema identitete dokazovalca s prisluškovanjem komunikacijskega kanala; dokazovalec na izziv (vprašanje) pošlje overitelju odgovor, na podlagi katerega overitelj lahko sklepa, da je dokazovalec resnično vir, za katerega se predstavlja. Izzivi se s časom spreminjajo. Algoritem izračunavanja odgovorov je poznan tako overitelju kot pravemu viru; overitelj torej ve, kakšen odgovor pričakuje od vira, katerega avtentičnost preverja; varnost in s tem moč avtentikacijske metode lahko povečamo s časovnim spreminjanjem parametrov, npr. izziva in (ali) s kriptiranjem avtentikacijskih sporočil, t.j. izzivov in odgovorov;
- **metode brez razkritja znanja (Zero Knowledge):** osnovna ideja protokolov brez razkrivanja znanja je posredovanje odgovorov, ki sami po sebi ne izdajajo rezultatov skrivnega algoritma za izračun odgovorov na izzive, ampak na podlagi več odgovorov na zastavljena vprašanja (izzive), omogočajo overitelju, da z zadostno verjetnostjo sklepa, da dokazovalec pozna algoritem za izračun

odgovorov; overitelj se na podlagi odgovorov odloča ali jih bo upošteval kot zadosten dokaz v postopku avtentikacije ali pa bo posredovane dokaze zavrnil.

- **metode s simetričnimi ključi:** pošiljatelj in prejemnik sporočila razpolagata z identičnim ključem, ki služi tako za kriptiranje kot za dekriptiranje sporočila; v smislu avtentikacije se uporablja prej predstavljene metode, uspešno dekriptiranje pa je dodaten dokaz, da je dokazovalec resnično oseba, za katero se predstavlja; protokoli avtentikacije po metodi izziva in odgovora z uporabo simetričnih ključev so opisane v standardu ISO/IEC 9798-2;
- **metode z uporabo asimetričnih ključev:** problematiko izmenjave in dodeljevanja simetričnih ključev za kriptiranje sporočil odpravlja uporaba asimetričnih ključev - dveh parov privatnega in javnega; javna ključa overitelj in dokazovalec javno objavita; s tema ključema kriptirano sporočilo lahko dekriptiramo le s tajnim ključem, ki pa ga ni potrebno izmenjevati preko komunikacijskega kanala;
- **metode z elektronskim podpisom:** uporabo med drugim predpisujeta standarda ISO/IEC 9798-3 in ITU-T X.509; sistem elektronskega podpisovanja temelji na digitalnih potrdilih (certifikatih), ki jih izdajajo »zaupanja vredne« institucije, npr. SiGen-CA [35].

Za avtentikacijo sporočil so primerne predvsem zadnje tri navedene metode, saj avtentikacija po prvih treh metodah zahteva izmenjavo avtentikacijskih sporočil v realnem času. Elektronski podpis je nasprotno pripet sporočilu in ga prejemnik lahko preveri kasneje.

Vsi postopki avtentikacije uporabnika (vira podatkov) temeljijo na specifičnih lastnostih ali značilnostih uporabnikov IKS, ki so lastni samo posamezniku in se po teh lastnostih ali značilnostih tudi enoumno razlikuje od ostalih oseb. Uporabnost razlikovalnih značilnosti za avtentikacijo je seveda odvisna od namena in metode avtentikacije ter tehnološke opremljenosti izvajalca avtentikacije [36].

Slika 8.5: Splošni postopek avtentikacije

Avtentikacija poteka na podlagi avtentikacijskih protokolov. V procesu avtentikacije sodelujeta dokazovalec in overitelj. Dokazovalec na osnovi nekega dokaza po naprej določenem postopku (protokolu) želi dokazati svojo resnično identiteto, naloga overitelja pa je, da dokaz preveri in nedvoumno ugotovi, ali je dokazovalec resnično oseba, za katero se predstavlja.

8.5.2 Vzroki za napade na avtentikacijo in njihove posledice

Napad na avtentikacijo ima preprost namen; zlorabiti identiteto nekoga drugega in izkoristiti njegove pravice do uporabe informacijsko-komunikacijskih storitev. Posledice uspešnega napada na avtentikacijo so lahko dokaj nedolžne, npr. zgolj osebna potrditev »strokovnosti« napadalca ali pa katastrofalne za posameznika ali organizacijo, npr. kraja zelo občutljivih poslovnih ali osebnih podatkov, kraja večjih vsot denarja …

Profilov napadalca na avtentikacijo je mnogo; od računalniškega nadobudneža, ki potrebuje nekaj samopotrditve, do resnih primerov e-kriminalitete in terorizma.

Načini napadov na avtentikacijo so pogojeni predvsem z uporabljeno metodo avtentikacije in opremljenostjo ter izkušnjami napadalca. Bolj napredne metode avtentikacije zahtevajo mnogo več znanja, izkušenj in opreme za uspešen napad. Zato je ključnega pomena, da avtentikacijske metode prilagodimo stopnji ogroženosti našega sistema in da dosledno upoštevamo varnostno politiko v podjetju.

Odtujitev gesel in identifikacijskih številk je najpogostejša oblika napada na avtentikacijo. Načini odtujitve so lahko zelo različni: prisluškovanje (nekriptiranega) prometa po omrežju, »brskanje prek rame«, socialni inženiring (… »zaupaj mi tvoje geslo, da ti bom lahko sam uredil zadeve« ...), kraja datotek z gesli ipd. Posledice odtujitve gesla so kritične predvsem pri enostavnih enostopenjskih avtentikacijskih metodah, kot je avtentikacija s fiksnim geslom. Tudi močnejše avtentikacijske metode, ki uporabljajo pametne kartice z elektronskimi certifikati, generatorji enkratnih gesel ali certifikati, shranjenimi na disku računalnika, ne pomagajo dosti, če napadalec pozna fiksno geslo za aktiviranje certifikata, generatorja gesel …

Obramba pred odtujitvijo gesla je predvsem natančno upoštevanje primerne varnostne politike. Varnostna politika mora določiti kriterije za izbiro gesla, ki otežujejo njegovo razkritje. Pomembno je, da uporabnik ne izbere gesla, ki ga je preprosto uganiti, npr. znanih pojmov, lastnih imen … saj obstajajo učinkoviti načini za ugibanje preprostih gesel, t.i.

napadi s slovarjem. Gesla morajo biti dovolj dolga (npr. 6 – 8 znakov), sestavljena morajo biti iz številk in črk, pomembna je (različna) velikost črk. Geslo moramo menjavati čim bolj pogosto. Tabele gesel na strežniku overitelja morajo biti kriptirana. Z gesli moramo previdno ravnati, jih ne zapisovati in ne zaupati drugim uporabnikom sistema. Pomembna je tudi uporaba kriptiranih povezav med uporabnikom in avtentikacijskim strežnikom, kar zmanjšuje uspešnost prisluškovanja. Nekateri postopki avtentikacije vključujejo t.i. začinjanje gesel, to je avtomatizirano dodajanje znakov geslu ob vnosu, s čimer se zmanjšuje možnost uspešnega napada »s slovarjem« kljub temu, da je uporabnik izbral preprosto geslo. Overitelj pred preverjanjem gesla po skritem postopku očisti geslo dodatnih znakov, preden ga uporabi.

8.5.3 Avtentikacija v različnih sistemih

Metode avtentikacije, ki so bile predstavljene v poglavju 8.5.1, se množično uporabljajo v sodobnih IKS. Nemogoče je natančno našteti vse primere uporabe avtentikacije, tudi če bi pod drobnogled postavili samo eno področje uporabe. Področja se tudi med seboj prepletajo. Prenosni računalnik, ki je vključen v poslovno informacijski sistem podjetja, lahko uporablja mobilni komunikacijski sistem, uporablja Windows okolje, z njim je mogoč dostop do interneta in do spletnih storitev, npr. elektronskega bančništva. Prenos podatkov večinoma poteka po TCP/IP protokolu preko Ethernet omrežij. V nadaljevanju bodo zato izpostavljeni samo tisti vidiki avtentikacije, ki so pomembnejši z vidika zaščite obravnavanega IKS.

Avtentikacija v Ethernet omrežjih

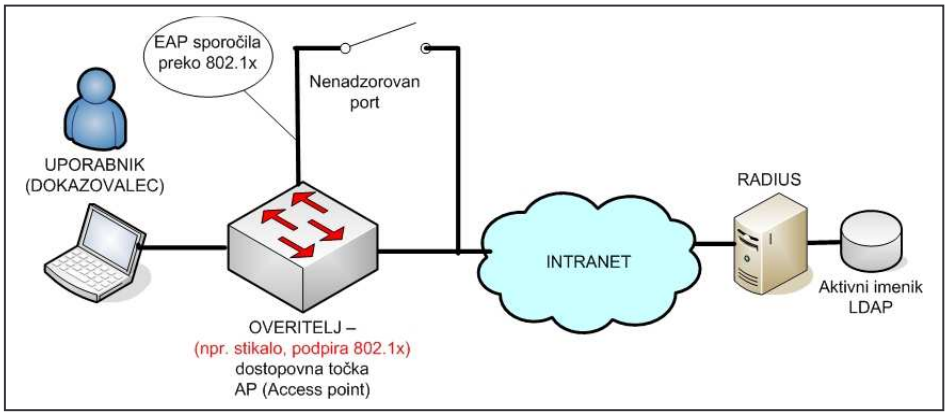
Z naraščanjem pomena in uporabe Ethernet omrežij tudi izven industrijskih okolij se je pojavila potreba po standardiziranem pristopu k avtentikaciji uporabnikov. Avtentikacijski sistem v Ethernet okolju sestavljajo:

- odjemalec (dokazovalerc),
- overitelj, ki je lahko stikalo, usmerjevalnik ali brezžična dostopovna točka,
- avtentikacijski strežnik, ki poleg avtentikacije omogoča tudi avtorizacijo in obračunavanje (Accounting) – AAA.

Uporablja se standardiziran in razširljiv avtentikacijski protokol EAP (Extensible Authentication Protocol), ki podpira različne metode avtentikacije. Transport sporočil preko Ethernet medija zagotavlja protokol IEEE 802.1x. Avtentikacija dejansko poteka med

avtentikacijskim strežnikom in odjemalcem, overitelj (dostopovna točka, stikalo) pa je samo posrednik avtentikacijskih sporočil.

Protokol IEEE 802.1x deluje na 2. plasti OSI referenčnega modela. Zasnovan je na nadzorovanem dostopu do omrežja na nivoju vrat. Protokol 802.1x sam po sebi ne zagotavlja avtentikacije, ampak le prenaša avtentikacijska EAP sporočila.



Slika 8.6: Mehanizem delovanja IEEE 802.1x protokola

Odjemalec zahteva dostop do lokalnega omrežja preko dostopovne točke (stikala), ki ima vlogo overitelja. Avtentikacijska sporočila se prenašajo preko nadzorovanega porta. Po uspešni avtentikaciji, overitelj omogoči promet preko nenadzorovanega porta, do zaključka seje, ko je potrebna ponovna avtentikacja (Slika 8.6) [37].

EAP zagotavlja le standardiziran in nadgradljiv način prenosa avtentikacijskih sporočil, zato je potrebno izbrati še metodo avtentikacije:

- LEAP (Lightweight EAP) uporablja šibko avtentikacijsko metodo uporabniškega imena in (fiksnega) gesla;
- EAP-MD5(EAP-Message Digest5) uporablja metodo šifriranega izziva - odgovora,
- EAP-MSCHAPv2 (EAP Microsoft Challenge Handshake Authentication Protocol v2) temelji na metodi izmenjave gesel,
- EAP-TLS (EAP-Transport Layer Security) uporablja metodo avtentikacije z digitalnimi certifikati po standardu x.509v3,
- EAP-OTP (EAP-One Time Password) avtentikacija z enkratnimi gesli,
- EAP-GTC (EAP-Generic Token Card) avtentikacija z žetonskimi karticami.

Za dodatno zaščito lahko uporabimo tehniko tuneliranja (navidezni varni komunikacijski kanali) EAP avtentikacijskih sporočil:

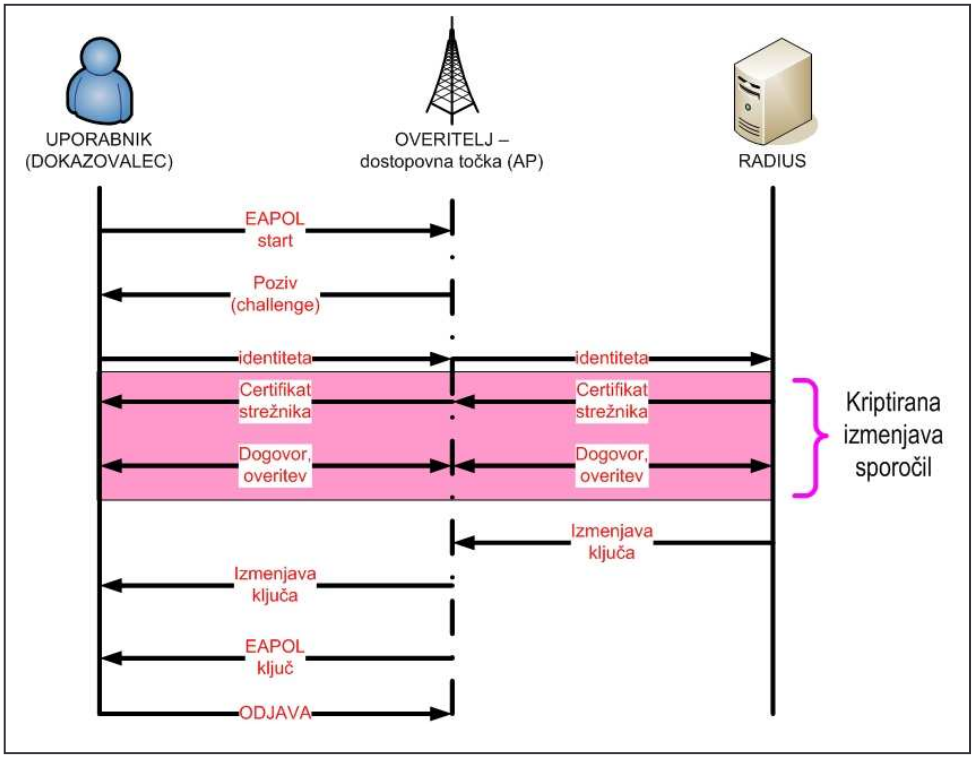
- PEAP (Protected EAP), naprimer PEAP/EAP-MSCHPv2,
- EAP-TTLS (Tunneled Transport Layer Security).

Avtentikacijo uporabnika v omrežjih WLAN predpisuje standard IEEE 802.1x, ki zagotavlja nadzor glede na vstopno točko (angl. port-based access control). Standard IEEE 802.11 tako predvideva AES (Advanced Encription Algorithm), ki uporablja 128, 192 ali 256 bitni ključ. Za avtentikacijo se uporablja EAP ali novejši PEAP (Protected EAP).

Avtentikacijski strežnik je običajno RADIUS (Remote Authentication Dial-In Services). Njegova naloga je kontrola dostopa do omrežja [38]. RADIUS strežnik preveri ali se je uporabnik pravilno prijavil v omrežje. Dostopovna točka (AP – Access Point) sprejme zahtevo po avtentikaciji od potencialnega uporabnika omrežja. Zahtevo posreduje RADIUS strežniku, ki glede na pravice, zapisane v aktivnem imeniku (LDAP), preveri uporabnika. RADIUS strežnik omrežnim napravam posreduje politiko dostopa za prijavljenega uporabnika.

Postopek avtentikacije WLAN uporabnika vsebuje naslednje korake (Slika 4.3):

- potencialni uporabnik se poskuša povezati z dostopovno točko (AP) preko nekontroliranega porta, AP ustvari izziv (challenge) in ga pošlje uporabniku;
- uporabnik odgovori s svojo identiteto;
- AP pošlje identifikacijsko sporočilo na avtentikacijski strežnik (RADIUS);
- RADIUS preveri identiteto in določi pravice, ki jih ima uporabnik; ugotovljena informacija se pošlje uporabniku;
- uporabnik pošlje svoje dostopovne pravice na nekontroliran port AP;
- RADIUS pravice preveri, če so v redu, pošlje avtentikacijski ključ na AP; ključ je kriptiran tako, da ga lahko uporabi le AP;
- AP dekriptira ključ in z njim kreira unikatni ključ za novega uporabnika. Ta ključ se nato pošlje uporabniku. Ključ se uporablja samo znotraj ene seje.



Slika 8.7: Postopek avtentikacije 802.1x/EAP-PEAP

Kot aventikacijska metoda se uporablja sitem izziv – odgovor. Uporabnik in overitelj poznata skrito vsebino, na podlagi katere se izračunavajo parametri odgovora in preverja njegova pravilnost glede na izziv. Uporabnik ima shranjeno skrivno vrednost na SIM kartici. V osnovi gre za 128 bitno vrednost, ki služi izračunu 32 bitnega odgovora. Za kriptiranje avtentikacijskih podatkov se uporablja 64 bitni ključ. Dostop do skrite vrednosti na SIM kartici je zaščiten z uporabniško številko (PIN).

Mobilna omrežja so zaradi enostavnega brezžičnega dostopa še posebej problematična s stališča napadov. Še posebej so občutljiva zasebna brezžična omrežja (WLAN, WiFi) saj njihovi načrtovalci pogosto zanemarijo pomen kriptiranja podatkov in s tem na široko odpirajo vrata tudi napadom na avtentikacijo. Razvoj novih varnostnih mehanizmov je v mobilnih komunikacijah še posebej intenziven. V zadnjem času so bili predstavljeni novi mehanizmi za doseganje večje varnosti v mobilnih komunikacijah, kot so WPA in nadgradnja WPA2.

Sodobni standard za zagotavljanje varnosti WLAN, WPA2 predstavlja nadgradnjo starejših protokolov za zagotavljanje varnosti: WEP (Wired Equivalent Privacy) in kasnejšega WPA (Wi Fi Protected Access). Slabost starejšega WPA je uporaba statičnega ključa za avtentikacijo in šifriranje podatkov, ki ga je s pasivnim opazovanjem radijskega prometa

mogoče relativno hitro ugotoviti. WPA temelji na šifrirnem algoritmu TKIP (Temporal Key Integrity Protocol), avtentikaciji po standardu 802.1x, dolžina (dinamičnega) ključa je 128 bitov, uporabljen je EAP.

Pri WPA2 kontrolo identitete oz. overjanje uporabnika (avtentikacijo) predpisuje standard 802.1x, ki zagotavlja nadzor glede na vstopno točko (angl. port-based access control) (Slika 5.2). Standard 802.11 tako predvideva AES (Advanced Encription Standard), ki uporablja ključe spremenljive dolžine (128, 192 ali 256 bitni ključ). Za overjanje po standardu 802.1x se uporablja industrijski standard EAP ali novejši PEAP. PEAP je t.i. dvostopenjski protokol, ki v prvi stopnji zagotavlja zaščito povezave, v drugi pa avtentikacijo uporabnika. V prvi stopnji se vzpostavi TLS (Transport Layer Security) tunel, pri čemer se avtentikacijski strežnik predstavi uporabniku z digitalnim potrdilom. Po vzpostavitvi varnega kanala se izvede še avtentikacija uporabnika [39].

9 NAČRTOVANJE VARNEGA IKS ZA AKTIVNA OMREŽJA V DEE

Kot osnovo za načrtovanje varnega IKS vzamemo ISO - OSI model in glede na nivo modela načrtujemo ustrezno zaščito:

- fizična plast; nadzor nad vozlišči, uporaba standardov ožičenja …
- povezovalna plast; nadzor in upravljanje nad aktivno mrežno opremo drugega nivoja (koncentratorji, stikala …);
- omrežna in transportna plast; nadzor in upravljanje nad aktivno mrežno opremo tretjega in četrtega nivoja (usmerjevalniki, požarne pregrade, IPSec VPN …);
- ostale višje plasti: nadzor nad podatki in aplikacijami, zaupnost in integriteta podatkov.

Izbira gradnikov zaščite IKS je pogojena predvsem z namenom IKS, ki je predmet zaščite. Obravnavan IKS za aktivna omrežja v DEE ima z vidika zaščite omrežja naslednje pomembne značilnosti:

- telekomunikacijski sistem je strogo namenski in ni namenjen prenosu podatkov med neznanimi uporabniki;
- IKS v veliki meri uporablja lastno infrastrukturo podjetja, t.j. lastno optično komunikacijsko omrežje, lastne radijske zveze, ki niso predvidene za javno uporabo;
- dostop nepooblaščenim osebam do večine komunikacijske opreme je precej otežen, saj se nahaja v elektroenergetskih objektih (TP, RTP), poseganje vanje pa je lahko smrtno nevarno;
- optično omrežje poteka večinoma v strelovodnih vrveh 110 kV daljnovodov (OPGW) ali v kabelskih kanalizacijah ob 20 kV SN kablovodih, kar otežuje pristop nepooblaščenim osebam;
- IKS deloma uporablja tudi javna komunikacijska omrežja (mobilno omrežje GPRS/UMTS, Internet);
- podatki o količini porabljene električne energije, trenutnih obremenitvah TP, parametrih kakovosti napetosti … niso tako zanimivi kot npr. osebni podatki, stanje na bančnih računih, številke kreditnih kartic… zato obravnavan IKS ni najbolj iskana tarča potencialnih napadalcev.

Na podlagi prej navedenih dejstev je za zaščito obravnavanega IKS predvideno:

- zagotovitev zaščite telekomunikacijske infrastrukture;
- tunelski način prenosa podatkov na principu VPN IPSec tehnologije za zagotovitev varnega prehoda skozi javna TK omrežja;
- požarni zid na meji med intranetom podjetja kot edina dovoljena točka povezave z zunanjimi deli komunikacijskega omrežja in kot točka zaključevanja VPN povezav;
- zagotavljanje varnosti WLAN omrežja z uporabo sodobnih komunikacijskih standardov (WPA2) in RADIUS strežnika za avtentikacijo, avtorizacijo in zapisovanje TK prometa (AAA);
- dopolnitev varnostne politike podjetja s pravili za uporabo razširjenega IKS podjetja;
- izobraževanje vseh uporabnikov sistema za pravilno uporabo sistema in izvajanje varnostne politike podjetja.

9.1 Zaščita telekomunikacijske infrastrukture

Kot fizični nivo varovanja infrastrukture razumemo mehansko zaščito infrastrukture, naprav in kontrolo dostopa do komunikacijskih naprav in omrežja. Potencialnim vsiljivcem moramo v največji možni meri preprečiti nedovoljen dostop do omrežja in omrežnih naprav. Poleg tega moramo v prostorih, v katerih se nahaja telekomunikacijska oprema, zagotoviti ustrezne klimatske pogoje in sisteme rezervnega napajanja.

Da bo telekomunikacijsko omrežje zanesljivo delovalo, moramo pri uporabi posameznega komunikacijskega medija (optika, bakreni vodi, WLAN …) upoštevati:

- standarde proizvajalcev medija in komunikacijske opreme ter
- tehnične predpise s področja elektrotehnike.

9.1.1 Izbira prenosnega medija

Z vidika varnosti imajo optične zveze več prednosti pred bakrenimi vodniki (paricami) in koaksialnimi kabli. Omogočajo doseganje velikih pasovnih širin, z njimi je mogoče (brez vmesnih ojačitev signala) dosegati večje razdalje. V primerjavi z bakrenimi in koaksialnimi vodniki je težje izvesti prisluškovanje na samem vodniku, odcep na vodniku je precej teže

realizirati kot na bakreni parici. Prisluhi so seveda mogoči tudi na optiki, jih je pa mogoče odkriti s posebnimi orodji, t.i. optičnimi reflektometri (OTDR – Optical Time Domain Reflectometer). Prisluškovanje poveča slabljenje na optičnem vlaknu, reflektometer pa meri slabljenje na dolžino vlakna.

V Elektro Gorenjska v zadnjih letih gradimo fiksne telekomunikacijske zveze izključno na osnovi optike. Starejših bakrenih vodnikov (paric) je še zelo malo; večina jih je bila že nadomeščenih z optičnimi vlakni. Za zanesljivo in varno delovanje optičnih povezav je potrebno še posebej paziti na:

- maksimalne dolžine in radije krivljenja,
- izvedbo in nadzor stičnih mest,
- polaganje vodnikov v zaščitne cevi.

Povsod tam, kjer (še) ne obstaja privatno optično omrežje, je za prenos merilnih podatkov predvidena uporaba brezžičnih komunikacij, tako javnih (GPRS/UMTS) kot zasebnih (WLAN na osnovi WiMax ali WiFi).

Nevarnosti prisluškovanja se ne moremo popolnoma izogniti. Pomembno je, da prisluškovalec ne bo mogel razbrati vsebine podatkovnih paketov, ki potujejo po komunikacijskem omrežju. Rešitev je varno kodiranje podatkov (enkripcija). Pomembno je, da kriptiramo podatke na vsej poti med uporabniki omrežja, še posebej je to pomembno pri bolj izpostavljenih delih omrežja, kot so brezžični deli (privatnega) omrežja ali internet. Eno boljših rešitev tega problema predstavlja IPSec VPN, predstavljen v poglavju 9.2.

Za doseganje primerne zanesljivosti delovanja in varnosti komunikacijskega sistema je pomembna tudi topologija omrežja, t.j. fizična pot medija za prenos podatkov. Pomembno je graditi strukturirana omrežja in zagotavljati redundantne poti med vozlišči, s čemer precej zmanjšano možnost izpada sistema (downtime). Optično omrežje smo v Elektro Gorenjska vedno gradili tako, da smo zagotavljali veliko stopnjo razpoložljivosti sistema, saj se komunikacijski sistem v osnovi uporablja za vodenje in nadzor elektroenergetskega sistema, kjer si izpada nadzora nad omrežjem praktično ne moremo privoščiti.

9.1.2 Varovanje in pogoji delovanja komunikacijske opreme

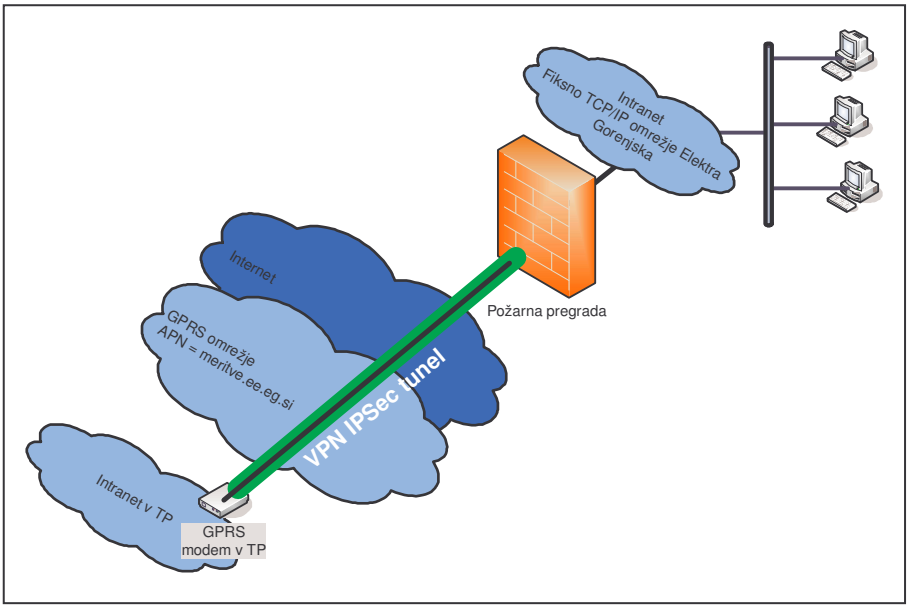
Posebej kritično je zagotavljanje varnosti dostopa in pogojev delovanja pomembnih mrežnih elementov, kot so strežniki, usmerjevalniki prometa, požarne pregrade … V konkretnem primeru se vsa komunikacijska oprema nahaja v posebej varovanih prostorih, kjer

so zagotovljeni tudi potrebni klimatski pogoji in sistemi rezervnega napajanja. Zagotovljena je kontrola temperature in vlažnosti prostora, nameščena je ustrezna zaščita pred vplivi atmosferskih razelektritev, požarna zaščita, zaščita pred premočnimi elektromagnetnimi polji in zaščita pred prahom.

Bolj kritična je zaščita komunikacijske opreme v TP. Dostop je sicer »varovan« že s tem, ker je komunikacijska oprema nameščena v energetskem objektu, je pa v manjših (jamborskih) TP težje zagotoviti primerne klimatske pogoje za zanesljivo delovanje opreme. Nekatere TP so močno izpostavljene visokim oz. nizkim temperaturam, prahu, v vseh je prisotno tudi povečano elektromagnetno sevanje. Pri izbiri komunikacijske opreme moramo upoštevati mesto vgradnje in vplive, ki so na njem prisotni.

9.2 VPN IPSec prehod skozi javna komunikacijska omrežja

Uporaba zasebne komunikacijske infrastrukture, predvsem optičnega omrežja, zagotavlja poleg ostalih ukrepov visoko stopnjo varnosti. Varnost podatkov pri prehodu skozi javno komunikacijsko omrežje pa mora biti zagotovljena z vzpostavitvijo varnega zasebnega IP omrežja (VPN). Podlaga za aktiviranje prenosa podatkov je vzpostavitev povezave med GPRS omrežjem mobilnega operaterja in intranetom podjetja. Povezava se vzpostavi skozi IPSec tunel preko interneta. Mobilni operater uporabniku dodeli dostopno točko (APN), na katero se naveže VPN IPSec povezava med operaterjem in uporabnikom.



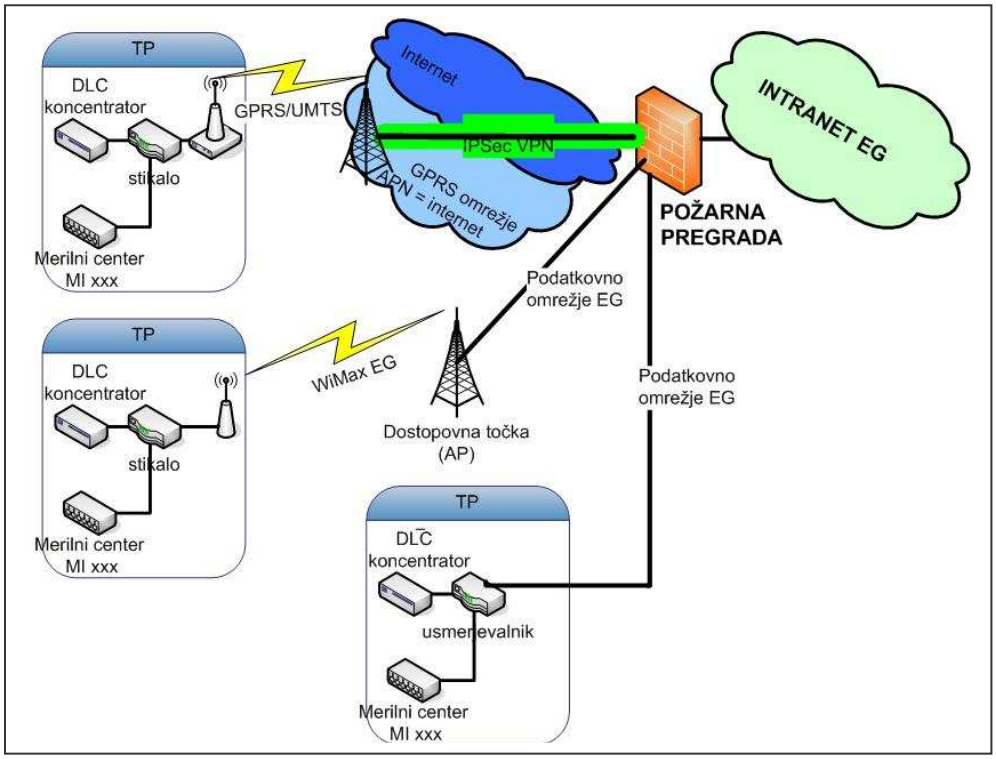
Slika 9.1: Shematski prikaz prenosa podatkov preko javnega omrežja

Mobilnemu operaterju je za vzpostavitev varne povezave potrebno podati pisno zahtevo za aktiviranje varnega dostopa do izbranih SIM kartic. Dostop do teh SIM kartic je drugim uporabnikom omrežja onemogočen [40]. Shematski prikaz infrastrukture je podan na sliki 9.1.

V predhodnih poglavjih je bilo na več mestih poudarjen otežen dostop do komunikacijske infrastrukture v lasti podjetja, saj je le-ta v veliki meri zgrajena paralelno z energetskimi vodi pod visoko napetostjo. Načeloma je le malo možnosti, da bi prišlo do prisluškovanja komunikacijskemu prometu na privatnem delu omrežja. Kljub temu bo tudi pri prenosu podatkov preko privatnega optičnega omrežja za dosego še večje varnosti uporabljeno kriptiranje podatkov in avtentikacija v skladu z IPSec standardom. Pomembno je, da tako kot požarna pregrada tudi komunikacijska oprema v TP (usmerjevalnik, WLAN komunikator) omogoča vzpostavitev (zaključevanje) varnih privatnih omrežij (IPSec VPN) [41].

9.3 Požarna pregrada

Požarna pregrada bo edina prehodna točka med internim omrežjem Elektra Gorenjska in IKS, ki bodo omogočali prenos podatkov iz TP v merilni center (Slika 9.2). Predvidena je uporaba strojne požarne pregrade. Na trgu obstaja široka paleta produktov, ki vključujejo različne funkcionalnosti.



Slika 9.2 Požarna pregrada v IKS za aktivna omrežja

V našem primeru mora imeti požarna pregrada naslednje lastnosti:

- možnost izbire načina delovanja, kot na primer:
  - paketni filter (packet filter),
  - nadomestni strežnik, realizacija aplikacijskih prehodov (proxy server),
  - paketno filtriranje z upoštevanjem vseh stanj (stateful inspection).
- omogoča vzpostavitev (zaključevanje) varnih privatnih omrežij (IPSec VPN).

Izbira načina delovanja in s tem stopnje zaščite bo natančno določena v varnostni politiki. Pri izbiti bo potrebno poiskati primeren kompromis med čim večjo varnostjo (zahtevnejšim preverjanjem prometa) in prepustnostjo požarne pregrade (glede na potreben pretok podatkov).

9.4 Zagotavljanje varnosti v javnih mobilnih in zasebnih WLAN omrežjih

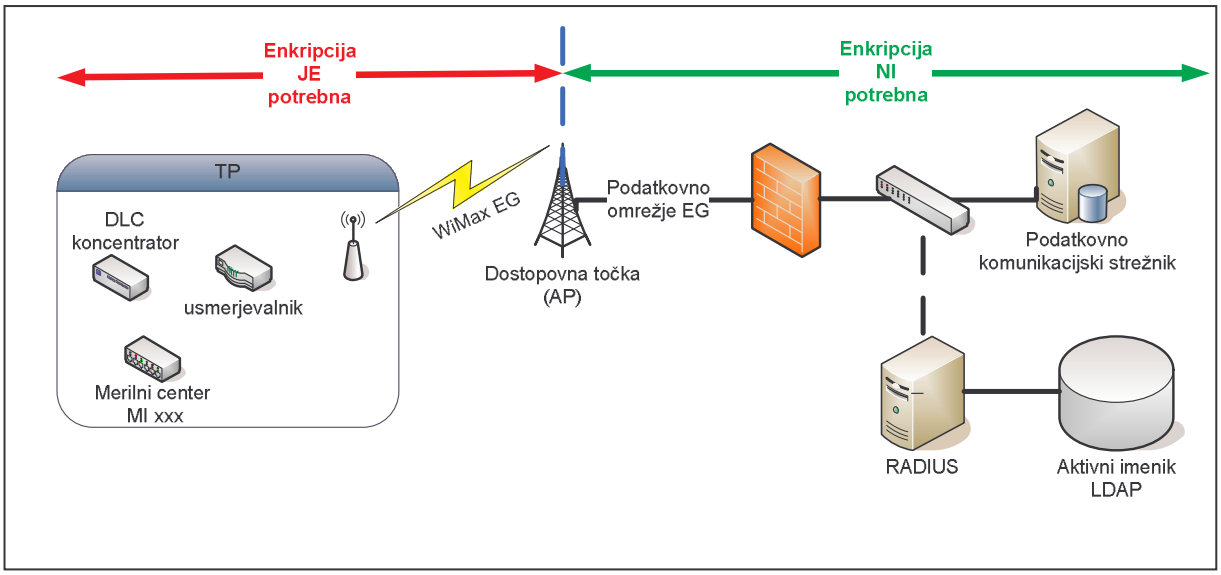
Obravnavan IKS v veliki meri uporablja lastno infrastrukturo (optično omrežje), za končni dostop do »inteligentnih enot« aktivnega omrežja pa bo v večini primerov uporabljeno mobilno omrežje (GPRS/UMTS) ali lastno WLAN omrežje (WiMax EG). Ravno brezžični deli »zadnje milje« IKS predstavljajo najverjetnejšo točko vdora v predmetni sistem. Dejansko lahko kdorkoli v bližini dostopne točke sprejema signal, zato je treba ves brezžični promet kriptirati. To še posebej velja za privatna WLAN omrežja, saj mobilni operaterji ponujajo bolj ali manj ustrezne varnostne mehanizme. Razvoj varnostnih mehanizmov je na področju WLAN intenziven, v nadaljevanju je navedenih nekaj značilnosti novejših standardov za zagotavljanje varnosti, ki jih bo potrebno pravilno uporabljati .

9.4.1 Sodobni standardi za zagotavljanje varnosti WLAN omrežij: WPA2

WPA2 predstavlja nadgradnjo starejših protokolov za zagotavljanje varnosti: WEP (Wired Equivalent Privacy) in kasnejšega WPA (Wi Fi Protected Access). Slabost starejšega WPA je uporaba statičnega ključa za avtentikacijo in šifriranje podatkov, ki ga je s pasivnim opazovanjem radijskega prometa mogoče relativno hitro ugotoviti. WPA temelji na šifrirnem algoritmu TKIP (Temporal Key Integrity Protocol), avtentikaciji po standardu 802.1x, dolžina (dinamičnega) ključa je 128 bitov, uporabljen je EAP.

Pri WPA2 kontrolo identitete oz. overjanje uporabnika (avtentikacijo) predpisuje standard 802.1x, ki zagotavlja nadzor glede na vstopno točko (angl. port-based access control) (Slika 9.3). Standard 802.11 tako predvideva AES (Advanced Encription Standard), ki uporablja ključe spremenljive dolžine (128, 192 ali 256 bitni ključ). Za overjanje po standardu 802.1x se uporablja industrijski standard EAP (Extensible Authentication Protocol) ali novejši PEAP (Protected EAP). PEAP je t.i. dvostopenjski protokol, ki v prvi stopnji zagotavlja zaščito povezave, v drugi pa avtentikacijo uporabnika. V prvi stopnji se vzpostavi TLS (Transport

Layer Security) tunel, pri čemer se avtentikacijski strežnik predstavi odjemalcu z digitalnim potrdilom. Po vzpostavitvi varnega kanala se izvede še avtentikacija odjemalca [39].



Slika 9.3 Zaščita WLAN omrežij

9.4.2 RADIUS strežnik za avtentikacijo, avtorizacijo in zapisovanje (AAA)

Za avtentikacijo, avtorizacijo in zapisovanje prometa je predvidena uporaba avtentikacijskega strežnika RADIUS. RADIUS preveri, ali se je uporabnik IKS pravilno prijavil v omrežje. Dostopovna točka (AP) sprejme zahtevo po overjanju od potencialnega uporabnika omrežja. Zahtevo posreduje RADIUS strežniku, ki glede na pravice, zapisane v aktivnem imeniku (LDAP), preveri uporabnika. RADIUS strežnik omrežnim napravam posreduje politiko dostopa za prijavljenega uporabnika.

Pravice vsakega uporabnika omrežja bodo morale biti individualno določene. Z določitvijo individualnih pravic uporabnikov IKS za aktivna omrežja se bo postavila jasna pravila uporabe IKS, s tem pa bo omogočen tudi nadzor nad samim podatkovnim prometom.

9.5 Varnostna politika

Vsak večji poseg ali razširitev IKS podjetja zahteva dopolnitev varnostne politike v segmentih, ki se nanašajo na novo opremo razširjenega sistema. Pri tem moramo paziti, da ne porušimo integritete obstoječe varnostne politike podjetja. V nadaljevanju je nanizanih nekaj področij varnostne politike, ki se jih obravnavan IKS najbolj dotika.

Politika fizičnega dostopa do omrežja določa pravila za izbiro, nameščanje, povezovanje in vzdrževanje komunikacijske infrastrukture. V osnovi mora varnostna politika določati:

- nameščanje mrežne opreme v komunikacijskih omarah v skladu s požarno – varnostnimi pravili, zaščiteno pred atmosferskimi vplivi in poseganjem nepooblaščenih oseb,
- uporabo rezervnih sistemov napajanja (UPS),
- beleženje dostopov in vzdrževalnih posegov na opremi,
- način gradnje / nadgradnje omrežja, pri čemer je potrebno strogo upoštevati tipizacijo omrežne opreme in uporabo predpisanih nastavitev.

Politika omrežnega dostopa določa, katere omrežne povezave so dovoljene glede na varnostno politiko organizacije. Realizirana je z nastavitvami parametrov požarne pregrade. V okviru politike kontrole dostopa tako določimo:

- kdo se lahko poveže v omrežje (kontrola povezljivosti),
- kaj lahko uporabnik počne znotraj aplikacije (kontrola protokola),
- kateri podatki se lahko preko omrežja izmenjujejo (kontrola podatkov).

Pod povezljivostjo so zajeti različni aspekti komunikacije:

- omrežne seje med klienti in strežniki,
- aplikacije, ki uporabljajo omrežne seje,
- podatki, ki se prenašajo znotraj aplikacijskih sej.

Postavitev požarne pregrade je z vidika varnostne politike še posebej občutljiva, saj predstavlja mejo »varnega« dela omrežja. Natančno moramo določiti:

- kdo bo z napravo upravljal,

- pravila spreminjanja osnovnih nastavitev, ki vplivajo na upravljanje: administratorsko geslo, servisni porti …
- mesta, s katerih se lahko požarna pregrada upravlja,
- obrambne mehanizme naprave, če obstajajo,
- nastavitev SNMP nadzora in prijavljanja, alarmiranja
- shranjevanje podatkov o konfiguraciji požarne pregrade na varno mesto.

Politika preverjanja identitete in dodeljevanja pravic temelji na avtentikaciji, avtorizaciji in zapisovanju dogodkov na omrežju (AAA). Varnostna politika mora biti dopolnjena z jasnimi pravili glede:

- načina preverjanja identitete uporabnika,
- načina dodeljevanja uporabniških imen in gesel,
- pravic dostopa do podatkov in aplikacij, še posebej pogodbenih izvajalcev vzdrževanja in zunanjih uporabnikov (obračunskih) podatkov,
- metod zapisovanja dogodkov v povezavi z uporabo IKS.

9.5.1 Usposabljanje in motiviranje uporabnikov za varno uporabo IKS

Tehnično varovanje IKS je z uporabo sodobnih tehnologij relativno enostavno zagotoviti. Tehnično delovanje naprav je znano in dokaj predvidljivo. Bistveno večji izziv pri zagotavljanju varnosti predstavlja »človeški faktor«. Problematična je organizacija pravilne uporabe uporabljenih tehnoloških virov in dosledno upoštevanje varnostne politike. Uporabniški vidik varnosti telekomunikacijskega sistema je pogojen z *usposobljenostjo, motivacijo, kooperativnostjo in pogoji poslovanja* zaposlenih v podjetju in drugih uporabnikov sistema.

Usposabljanje uporabnikov za pravilno in varno uporabo telekomunikacijskega sistema predpostavlja izvedbo različnih tečajev in usposabljanj, možnost dostopa do uporabniških priročnikov, neposredno uvajanje uporabnikov za varno delo in zagotavljanje pomoči v primeru težav na delovnem mestu.

Motivacija je pomemben del organizacije poslovanja, saj zagotavlja delovanje uporabnikov v dogovorjenih in predpisanih okvirih. Pri tem je denarno in nedenarno nagrajevanje zaposlenih zelo pomemben dejavnik varnosti.

Kooperativnost pogojuje uspešno delovanje in servisiranje komunikacijskega sistema, saj le uporabniki s pravilnim odnosom do svojega delovnega okolja prispevajo k zanesljivemu delovanju celotnega sistema.

Pogoji poslovanja, kot so urejen status zaposlenih, urejeno delovno okolje… pozitivno vplivajo na delovno klimo v podjetju in na lojalnost zaposlenih [22].

Zagotoviti moramo, da varnostna politika obravnava vse vidike uporabe IKS. Vsi zaposleni v podjetju morajo razumeti varnostno politiko kot enega od ključnih procesov, ki mora biti podvržen nenehnemu izboljševanju kakovosti. Le na ta način bomo zagotovili varno in zanesljivo delovanje obravnavanega in vseh ostalih IKS, brez katerih si sodobnega poslovanja ne moremo več predstavljati.

9.6 Standardi na področju varnosti IKS v aktivnih omrežjih

V predhodnih poglavjih predstavljene posamezne tehnične rešitve zaščite IKS za aktivna omrežja morajo biti uporabljene na sistematičen način. V nasprotnem primeru obstaja tveganje »lukenj« v varnostnem sistemu. Tudi na tem področju obstajajo in se dopolnjujejo standardi, ki predpisujejo vrste zaščite, njihove povezave in nastavitve. Standard, ki se v zadnjem času najpogosteje omenja v povezavi s protokolom IEC 61850, je IEC 62351.

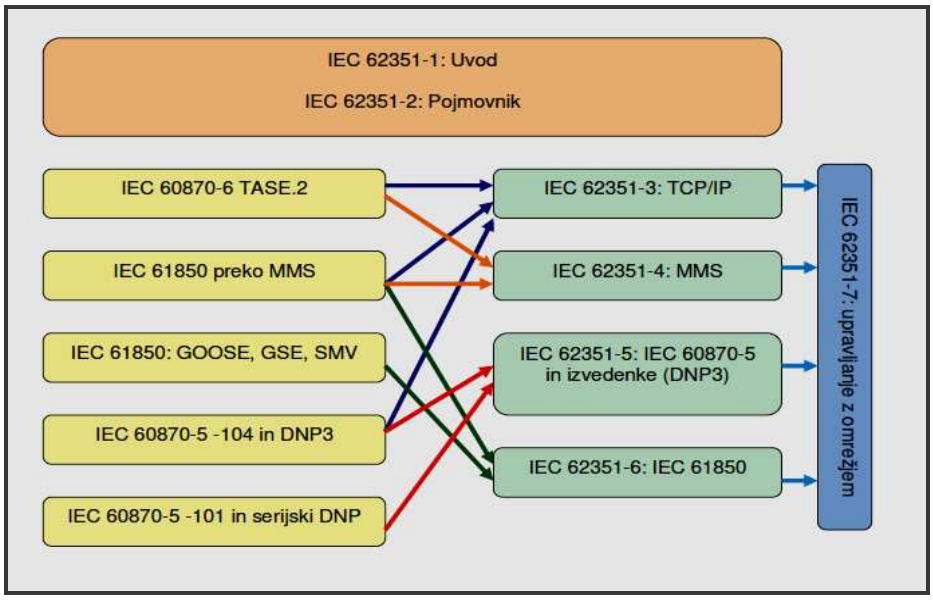
9.6.1 Standard IEC 62351

Standard IEC 62351 je nastal in se razvija pod okriljem IEC TC57 WG15 (IEC tehnična komisija št. 57, delovna skupina 15). Standard IEC 62351 določa varnostna pravila naslednjih komunikacijskih protokolov: IEC 60870-5, DNP, IEC 60870-6 (ICCP) in tudi IEC 61850. Ti protokoli se med seboj razlikujejo tudi z vidika potrebnih varnostnih mehanizmov. Ker se zaradi neprestanega dograjevanja sistemov vodenja v distribuciji EE uporablja več zgoraj naštetih protokolov istočasno, je še toliko bolj pomembna uporaba standarda, ki obravnava varnost vseh uporabljenih komunikacijskih protokolov.

Preslikave posameznih komunikacijskih protokolov so shematsko prikazane na Sliki 9.5. Podrobnosti standarda IEC 62351 so predstavljene v naslednjih dokumentih:

- IEC 62351-1: Varnost podatkov in komunikacij – uvod
- IEC 62351-2: Pojmovnik
- IEC 62351-3: Varnostni načini in nastavitve za TCP/IP

- IEC 62351-4: Varnostni načini in nastavitve za MMS
- IEC 62351-5: Varnostni načini in nastavitve za IEC 60870-5 in DNP 3.0
- IEC 62351-6: Varnostni načini in nastavitve za IEC 61850
- IEC 62351-7: Varnost omrežja in upravljanje s sistemom



Slika 9.5: Preslikave komunikacijskih standardov v varnostne standarde IEC 62351-x

IEC 62351-3 vsebuje varnostne nastavitve za protokole, ki temeljijo na paketnem prenosu skladno s TCP/IP. Predpisane so nastavitve TLS (Transport Layer Security), ki se običajno uporablja na nižjih plasteh zaščite Internetnih komunikacij, pri čemer so nastavitve prilagojene zahtevam prenosa podatkov v IKS za elektroenergetske sisteme. Pozornost je usmerjena predvsem v zaščito pred prisluškovanjem, avtentikaciji, ne ščiti pa proti napadom tipa DoS.

IEC 62351-4 obravnava varnostne nastavitve sistema pri sporočilih MMS (ISO 9506), ki jih uporabljata protokola TASE.2 (ICCP) in IEC 61850. Tudi tu gre za nastavitve TLS s poudarkom na avtentikaciji.

IEC 62351-5 zagotavlja varnostne mehanizme in nastavitve serijskih protokolov (IEC 60870-5-101) in protokolov, ki temeljijo na paketnem prenosu podatkov ((IEC 60870-5-104 in DNP 3.0). Komunikacija po protokolu IEC 60870-5-101 velikokrat uporablja nizko hitrost prenosa podatkov, zato IEC 62351-5 predvideva le avtentikacijo, kriptiranje sporočil (TLS) pa

ne pride v poštev. Za IEC 60870-5-104 in DNP 3.0 je mogoče uporabiti tudi kriptirane sporočil. Kot alternativa kriptiranju sporočil se predvideva uporaba VPN povezav.

IEC 62351-6 podaja rešitve za časovno kritična sporočila v okviru IEC 61850, ki morajo biti prenesena znotraj 4 ms časovnega okna. V teh primerih je potrebno iskati drugačne varnostne rešitve, saj kripriranje in drugi varnostni ukrepi zaradi časovnih omejitev niso dopustni. Avtentikacija je zato edini varnostni mehanizem, kar zagotavlja minimalni čas za obdelavo in prenos podatkov.

IEC 62351-7 določa zahteve za celovito upravljanje omrežja in varnostnih mehanizmov komunikacijskega sistema od izvora podatkov do prejemnika (point to point). MIB (Management Information Base) je prirejen uporabi v elektroenergetskih sistemih. MIB vsebuje stanja posamezne informacijsko-komunikacijske opreme, aplikacij in sistemov. Upravljaje omrežja temelji na SNMP (Simple Network Management Protocol). Protokol podpira celovitost komunikacijskega omrežja, skrbi za pravilno delovanje sistema in aplikacij, IDS sistema in za druge varnostne nastavitve, ki so specifične za elektroenergetske sisteme.

10 SKLEP

Proizvodnja, prenos in distribucija električne energije imajo pomembno vlogo pri zagotavljanju večjega deleža energije iz obnovljivih virov in posredno zmanjšanja izpustov toplogrednih plinov ter racionalizacijo porabe energije. Pričakuje se pospešen razvoj in večja uporaba električnih vozil ter zmogljivejših hranilnikov električne energije. Vedno večje so zahteve po daljinskem odčitavanju števcev električne energije, pa tudi toplotne energije, vode, plina ... kar vse prinaša precejšnje spremembe v logiko obratovanja distribucijskega omrežja. Nadzor in vodenje posledično mnogo bolj »aktivnega« distribucijskega omrežja postaja vedno večji izziv.

Uporaba informacijsko-komunikacijskih sistemov (IKS) ima v slovenski elektrodistribuciji dolgo zgodovino. Uvajanje IKS je sledilo razvoju tehnike in vedno ostrejšim zahtevam po nadzoru in vodenju distribucijskega omrežja. Dandanašnji distribucijski centri vodenja (DCV) omogočajo daljinski nadzor in vodenje RTP, RP ter posameznih daljinsko vodenih stikalnih naprav na SN omrežju. Izziv za bližnjo prihodnost je informatizacija celotnega distribucijskega omrežja, torej implementacija takšnih IKS, ki bodo:

- zadostili sedanjim in tudi prihodnjim potrebam po nadzoru in vodenju celotnega distribucijskega omrežja,
- omogočali nadzor in upravljanje množice razpršenih virov energije,
- zagotavljali potrebno komunikacijsko infrastrukturo sodobnim AMI sistemom ter
- sistemom za upravljanje porabe električne energije pri odjemalcih (DSM).

Pri tem je ključno vprašanje izbire optimalne komunikacijske tehnologije, standardov in komunikacijskih protokolov.

Kljub dolgi tradiciji uporabe IKS v distribuciji EE pa ravno ti sistemi postajajo zaradi svoje heterogenosti, strogo namenske uporabe, nepovezanosti in drugih tehničnih omejitev, ozko grlo in ovira hitrejšemu razvoju v smeri aktivnih omrežij za distribucijo električne energije.

10.1 Celovit pristop k izgradnji IKS za aktivna omrežja

Evolucijo klasičnih omrežij v aktivna omrežja za distribucijo električne energije bo narekoval tempo razvoja IKS v distribuciji električne energije. Da bi presegli slabosti obstoječih IKS je potreben celovit pristop k njihovi izgradnji, pri čemer je potrebno upoštevati naslednje:

- IKS morajo temeljiti na nadgradnji obstoječih sistemov,
- uporabljene morajo biti sodobne standardizirane rešitve (Ethernet, IEC 61850, CIM IEC 61970/61968),
- uporabiti je potrebno vse razpoložljive TK tehnologije predvsem lastnih telekomunikacijskih sistemov (optične in radijske zveze, WiMax),
- varnost IKS mora temeljiti na sodobnih standardih (IEC 62351).

10.2 Pilotni projekti EG s področja aktivnih omrežij

V iskanju primernih rešitev so poleg spremljanja trendov v svetu najpomembnejše lastne izkušnje. V Elektro Gorenjska smo zato po letu 2005 pristopili k preizkušanju različnih informacijsko-komunikacijskih rešitev, temelječih na Ethrenet tehnologiji. V nadaljevanju je predstavljenih nekaj ključnih pilotnih projektov, ki smo jih že izvedli ali pa so še v teku.

10.2.1Informatizacija TP SN/NN (2006–2008)

V sodelovanju s podjetjem Iskra Sistemi smo prvi v slovenski distribuciji praktično preizkusili prenos obračunskih in obratovalnih meritev v TP preko Ethernet povezav (optika, GPRS/UMTS, WiMax) v merilni center obračunskih meritev, obratovalnih meritev in naprej v DCV [22],[23].

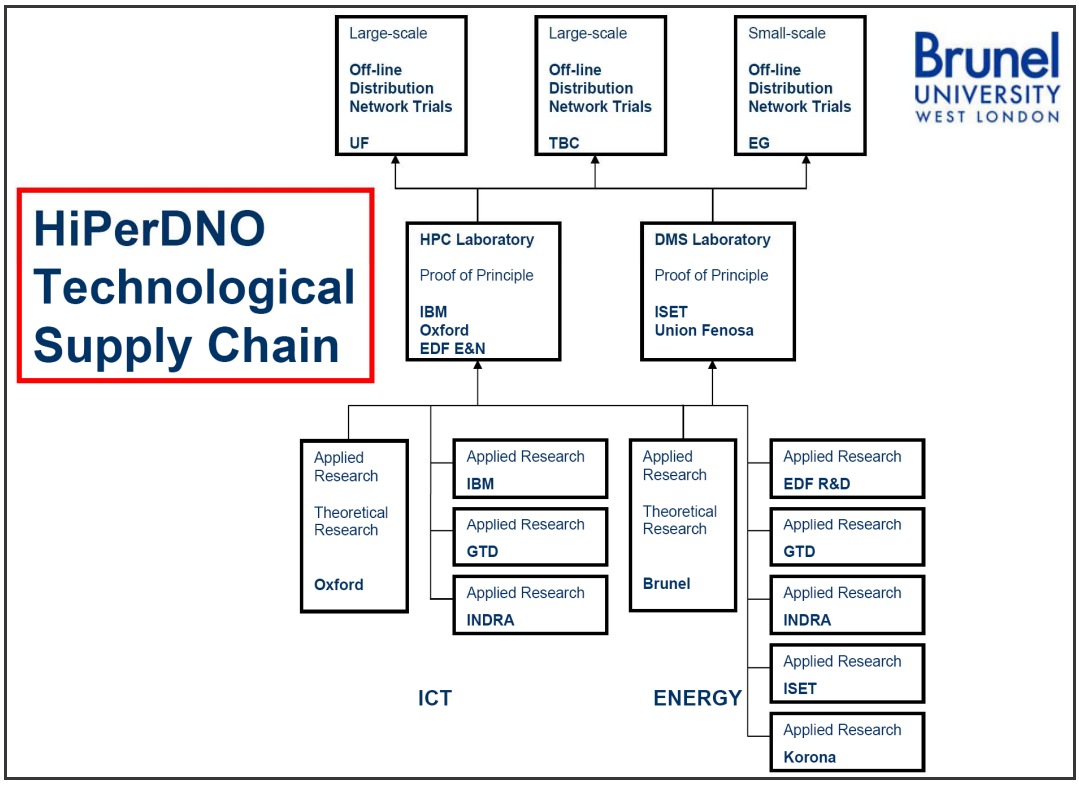
10.2.2 Uvajanje sistemov obračunskih meritev v EG (AMI)

Leta 2009 smo s proizvajalcema naprednih merilnih sistemov Iskra Emeco in Landis+Gyr podpisali pogodbo, po kateri je v naslednjih petih letih predvidena zamenjava števcev vseh gospodinjskih odjemalcev s sodobnimi AMI števci. Pomembna je naša zahteva po interoperabilnosti, s katero smo veliko prispevali k standardizaciji merilne opreme. Poleg tega je potrebno poudariti, da so na Gorenjskem praktično vsi odjemalci s priključno močjo 41kW ali več že dve leti daljinsko odčitani, večinoma s klicno povezavo (CSD) preko mobilnega

omrežja s centrom obračunskih meritev. Poleg tega na vzorcu 300 odjemalcev z vgrajenimi AMI števci preizkušamo tudi daljinsko odčitavanje plina, vode in tople vode.

10.2.3 Mednarodni razvojno raziskovalni projekt HiPerDNO (2010–2013)

HierDNO (High Performance Computing Technology for Smart Distributon Network Operation) je mednarodni projekt znotraj Sedmega okvirnega programa Evropske Unije za raziskave in tehnološki razvoj.



Slika 10.1: Organizacija in osnovne naloge članov konzorcija projekta HiPerDNO

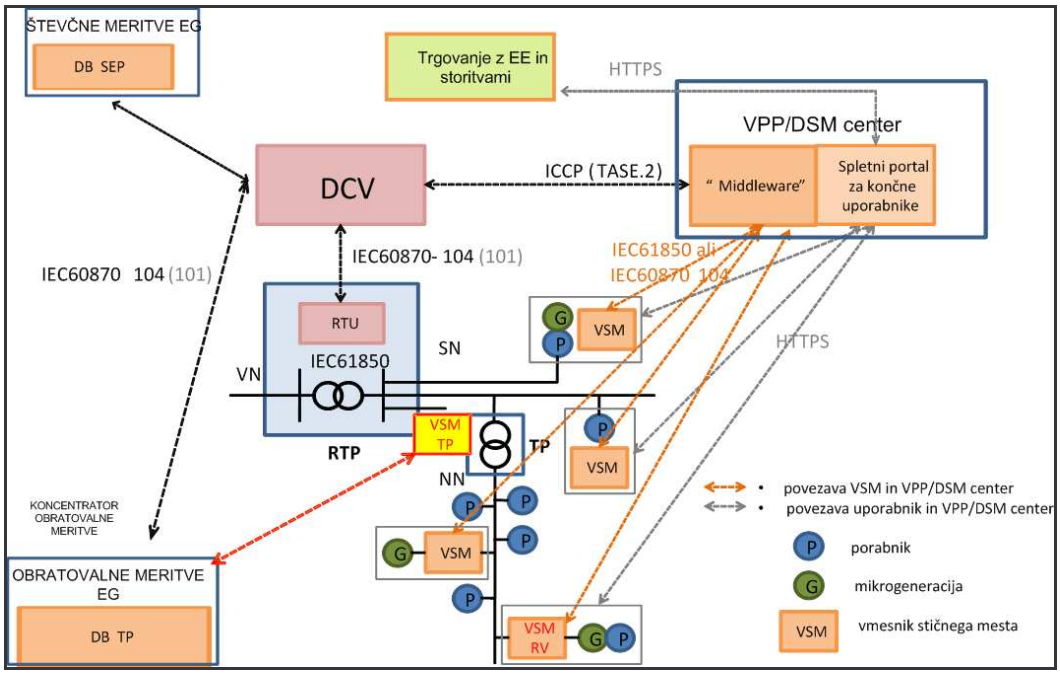
EG sodeluje z res eminentnimi znanstveno raziskovalnimi institucijami in podjetji, saj so v konzorciju poleg Elektra Gorenjska še: Brunel University, London, Velika Britanija, EDF (R&D), Pariz, Francija, IBM Israel – Science & Technology, Haifa, Izrael, University of Oxford, Oxford, Velika Britanija, Union Fenosa, Španija, (distribucija EE), Indra, Španija (IKT in energetika), GTD, Španija (IKT in energetika), Korona, Slovenija (inženiring, energetika, svetovanje) in Fraunhofer IWES/ISET, Nemčija (raziskovalna organizacija).

Glavni cilji projekta je razvoj algoritmov, ki bodo omogočili izdelavo ocenjevalca stanj distribucijskega omrežja (Distribution State Estimator) v skoraj realnem času. Ocene stanj bodo vhodni podatki za izdelava novih DMS funkcionalnosti centrov vodenja in

informacijskih rešitev za aktivna omrežja. Vloga EG v projektu je določitev zahtev za podatke o stanju omrežja, priprava poligona za testiranje algoritmov in končni prikaz delovanja celotnega sistema.

10.2.4 Strateški raziskovalni razvojni projekt SUPERMEN (2009-2012)

Na razpis Javne agencije za tehnološki razvoj Republike Slovenije iz sredstev Operativnega programa krepitve regionalnih razvojnih potencialov za obdobje 2007 – 2013 se je Elektro Gorenjska prijavila v konzorciju s podjetji Iskra MIS, Solvera Lynx in Gorenjske elektrarne. Projekt z naslovom Inteligentna elektroenergetska platforma za nadzor in vodenje razpršenih virov in porabnikov (krajše SUPERMEN) je bil odobren v mesecu oktobru 2009.



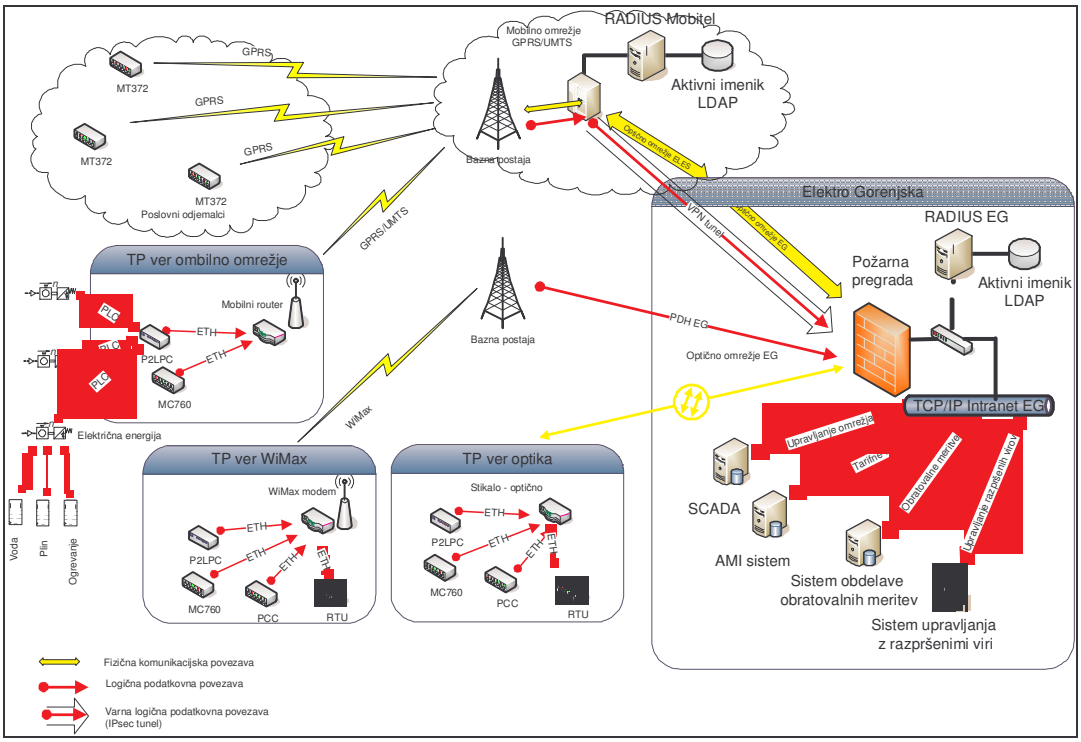
Slika 10.2: Shematski prikaz projekta SUPERMEN

Osnovni namen projekta je razvoj in demonstracija uporabe izdelkov in rešitev upravljanja z viri ter porabo električne energije, s katerimi bo operaterjem, lastnikom razpršenih virov ter uporabnikom, ob zaostrenih pogojih glede dobave in kakovosti električne energije, novih standardih in pravilnikih ter ob vse večjemu številu razpršenih (obnovljivih) virov, omogočeno poslovati uspešno, konkurenčno ter tehnološko napredno. EG v projektu sodeluje na področju analize vpliva razpršenih virov, pripravi specifikacije merilnika za razpršene vire, razširitve in testiranja SCADA sistema v DCV in na koncu tudi pripravi specifikacije testnega scenarija za nadzor in vodenje distribucijskega elektroenergetskega sistema s pomočjo novo razvite opreme.

10.2.5 Preizkušanje komunikacijskih tehnologij za aktivna omrežja

Preizkušanje novih tehnoloških rešitev, komunikacijskih standardov, varnostnih standardov in sistemov se nadaljuje. Trenutno preizkušanje poteka na treh področjih:

- lastno optično omrežje: v enem TP priključen merilni center MC750 in koncentrator obračunskih meritev,
- vodenje RP Cerklje preko WiMax omrežja; priključeni merilni center MI750 in MOSCAD RTU,
- mobilno omrežje (GPRS/UMTS); priključeni merilni centri MI750 oziroma MC760 v devetih TP in eni RP.



Slika 10.3: Simbolična shema IKS za aktivna omrežja

Namen teh preizkušanj je ugotoviti primernost posameznih tehničnih rešitev in opreme v realnem sistemu. Pred množičnim uvajanjem AMI sistema v naslednjih letih poskušamo kar najbolj pravilno določiti kriterije za izbor optimalne komunikacijske opreme.

10.3 Nadaljnji koraki pri zagotavljanju IKS za aktivna omrežja

Tudi v prihodnje bo potrebno nadaljevati s pilotnim preizkušanjem komunikacijskih standardov in informacijsko-komunikacijske opreme. Posebno pozornost bomo namenili možnosti izgradnje lastnega WiMax omrežja, saj je to precej obetajoča tehnologija za zagotavljanje temeljne komunikacijske infrastrukture. Povečevali bomo obseg in zmogljivost lastnega optičnega omrežja, komercialna (mobilna) omrežja pa bomo uporabljali predvsem na področjih, kjer zahteve po zanesljivosti niso visoke (samo nadzor, ni vodenja) ali pa lastno telekomunikacijsko omrežje ne obstaja.

V okviru slovenske distribucije bomo v sodelovanju z znanstveno raziskovalnimi ustanovami (Fakulteta za elektrotehniko, Elektroinštitut Milan Vidmar ...) usmerjali izdelavo sistemskih študijskih nalog distribucije v raziskovanje primernosti in načinov uporabe sodobnih komunikacijskih, informacijskih in varnostnih standardov (IEC 61850, CIM IEC 61970 in IEC 61968, IEC 62351). Poskušali bomo nadgraditi bazo tehničnih podatkov o omrežju v smeri CIM. Pri obnovi ali izgradnji sistemov vodenja bomo izbirali opremo, ki omogoča uporabo komunikacijskega protokola IEC 61850. V naslednjih letih bomo zamenjali opremo DCV in pri tem posebno pozornost namenili funkcionalnostim, ki bodo omogočale upravljanje z velikim številom majhnih enot za proizvodnjo električne energije in upravljanju porabe pri odjemalcih (DSM).

Nadaljnji razvoj IKS v distribuciji električne energije bo zagotovo dinamičen in zelo zanimiv.

Znanja in volje za delo imamo v Sloveniji dovolj, samo želimo pa si lahko, da omejena finančna sredstva in toga zakonodaja ne bosta preveliki oviri tehnološkemu napredku, ki ga uporabniki distribucijskega omrežja od nas upravičeno pričakujejo.

11 SEZNAM UPORABLJENIH VIROV

[1] E. Košnjek, Poslovni načrt OE Distribucijsko omrežje 2008-2011, Elektro Gorenjska, d.d., Kranj, 2008.

[2] Spletna stran podjetja SODO, d.o.o., www.sodo.si.

[3] Mihai Paun, at all., Smart Grids and Networks of the Future – EURELECTRIC Wiews, EURELECTRIC, Brussels, 2009.

[4] E. Turk, WG Smart Grid in projekti po EU, predstavitev, Skupščina GIZ distribucije EE, Ljubljana, marec 2010.

[5] T. Mohar, J. Golob, L. Andrejaš, Razvoj in uporaba programskega paketa GREDOS, Zbornik CIRED, 5. konferenca slovenskih energetikov, 2001.

[6] SIST EN 50160, Značilnosti napetosti v javnih distribucijskih omrežjih (istoveten EN 50160:1999), druga izdaja, marec 2001.

[7] Načrt razvoja distribucijskega omrežja Elektro Gorenjska d.d. za desetletno obdobje od leta 2009 do 2018, Elektro Gorenjska, d.d., Kranj, 2008.

[8] Spletna stran podjetja Iskra MIS, d.d., www.iskra-mis.si.

[9] J. Rosina, M. Mavrar, DCV Elektro Gorenjska, idejni projekt, IBE, d.d, Ljubljana, 2006.

[10] A. Souvent, G. Omahen, B. Derganc, J. Kosmač, Strateško tehnološko–ekonomska študija uvedbe sodobnega sistema merjenja električne energije (AMM sistema) v slovenski distribuciji, EIMV, ref 1849, Ljubljana, 2007.

[11] Spletna stran Energy Savig Trust (VB), http://www.energysavingtrust.org.uk/

[12] M. Kojc, Vpliv učinkovite rabe energije na emisije ogljikovega dioksida v Sloveniji, magistrsko delo, Univerza v Ljubljani, FE, 2005.

[13] Vlada RS, Energetski zakon – EZ, uradno prečiščeno besedilo EZ-UPB2, Ur.l. RS 27/2007, Ljubljana, 2007.

[14] Vlada RS, Zakon o spremembah in dopolnitvah EZ-C, Ur.l. RS 70/2008, Ljubljana 2008.

[15] Vlada RS, Nacionalni akcijski načrt za energetsko učinkovitost za obdobje 2008-2016 (AN-URE), Ljubljana, 2008.

[16] Spletna stran EFR – Europaische Funk-RundSteuerung, www.efr-funk.eu/

[17] D. Crossley, Evaluation and Acquisition of Network-driven DSM Resources, Research report No 4, Task XV of the IEA DSM Programme, IEADSM, 2008.

[18] D. Crossley, Worldwide Survey of Network-driven DSM Projects, Research report No 1, Task XV of the IEA DSM Programme, IEADSM, 2008.

[19] L. Hull, A Practical Guide to Demand Side Bidding, Task VIII of the IEA DSM Programme, IEADSM, 2005.

[20] M. Vodušek, Načrt razvoja distribucijskega omrežja električne energije v Republiki Sloveniji za desetletno obdobje od leta 2009 do 2018, SODO,d.o.o., Maribor, 2009.

[21] D. Crossley, Incorporation of DSM Measures into Network Planning, Research report No 3, Task XV of the IEA DSM Programme, IEADSM, 2008.

[22] D. Gerbec, E. Košnjek, J. Smukavec, Informatizacija TP SN/NN na osnovi Ethernet tehnologije, zbornik CIRED, 8. konferenca slovenskih energetikov, Čatež, 2007.

[23] D. Gerbec, J. Curk, E. Košnjek, J. Smukavec, Implementation of Ethernet in LV/MV transformer stations, International Conference on Electricity Distribution, Vienna, 2007.

[24] T. Vidmar, Informacijsko–komunikacijski sistem, Založba Pasadena, Ljubljana, 2002.

[25] IEEE-SA Stadards Board, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridget Local Area Networks, IEEE 802.1q, IEEE, New York, USA, 1999.

[26] A.W. McMorran, An Introduction to IEC 61970-301 & 61968-11, The Common Information Model, Institute for Energy and Environment, Department of Electronic and Electrical Engineering, University of Strathlyde, Glasgow, UK, 2007.

[27] R. Mackiewicz, The impact of Standardized Models, Programming Interfaces and Protocols on Substations, SISCO, Inc., Michigan, USA, 2003.

[28] http://www.simobil.si/sl/inside.cp2?cid=B0850770-48AD-C0FA-B6B6-931CADEDC3C7&linkid=article

[29] http://www.mobitel.si/slo/Ponudba/GSMnarocniki/OMobitelGSM/Osnovnipodatki/PokritostSlovenije/zemljevid.asp

[30] http://www.tusmobil.si/index.php?option=com_content&task=view&id=171&Itemid=211

[31] http://www.mobitel.si/slo/Ponudba/GSMnarocniki/OMobitelUMTS/Pokritost.asp

[32] E. Košnjek, Varnost telekomunikacijskega sistema na primeru sistema za prenos obratovalnih in obračunskih meritev v DEE, seminarska naloga, Fakulteta za elektrotehniko, Ljubljana, 2008.

[33] E. Mainvald, Network security, McGraw-Hill/Osborne, 2001.

[34] A. Kovačič, V. Vukšić-Bosilj, Management poslovnih procesov: Prenova in informatizacija poslovanja s praktičnimi primeri, GV Založba, Ljubljana, 2005.

[35] S. Tomažič, Varnost v telekomunikacijah in kako jo zagotoviti, članek, Fakulteta za elektrotehniko, Ljubljana, 2006.

[36] W.E. Burr, D.F. Dodson, W.T. Polk, Information securitiy, Electronic Authentication Guideline, NIST, Gaithersburg, 2004.

[37] J. Vollbrecht, at all, 802.11b Wireless Networking and Why It Needs Authentication, Interlink Networks Inc., 2002.

[38] M. Ladava, Navodila za postavitev, konfiguracija RADIUS strežnika za poslovni GPRS, V1.0, Microsoft Services, 2006.

[39] K. Albreht, R. Sušnik, J. Sodnik, S. Tomažič, WLAN – brezžična lokalna omrežja, Fakulteta za elektrotehniko, Univerza v Ljubljani, 2004.

[40] Spletna stran podjetja Mobitel, d.d., www.mobitel.si.

[41] R. Kolar, Varnost v IP VPN omrežjih z uporabo tehnologije IPSec, Štirinajsta delavnica o telekomunikacijah VITEL, Brdo pri Kranju, 2003.

[42] Spletna enciklopedija Wikipedia, http://sl.wikipedia.org/.

12 PRILOGE

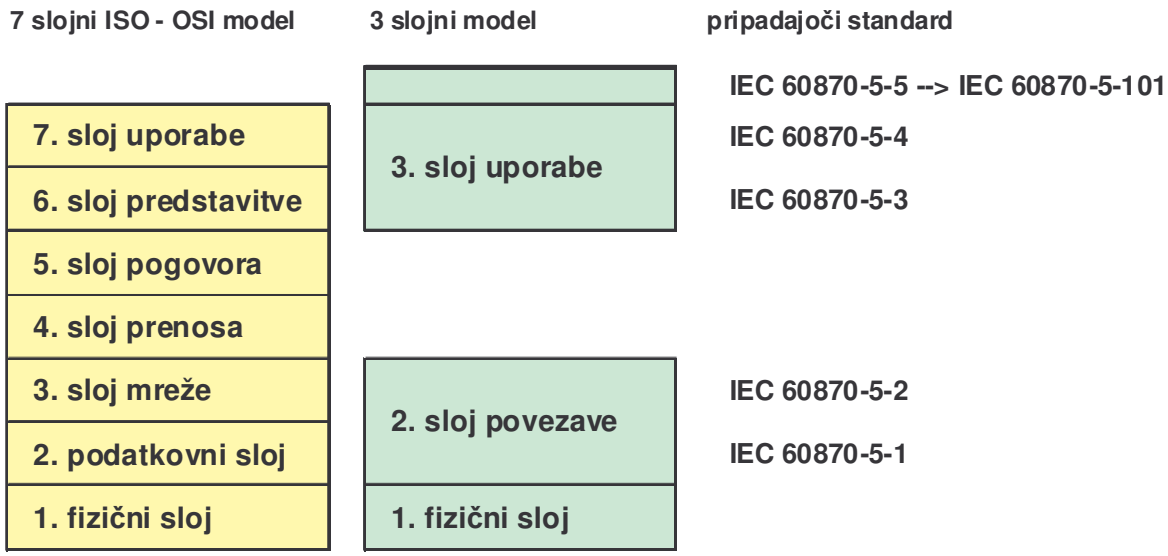
KAZALO PRILOG

Priloga 1: Kratka predstavitev protokola IEC 60870–5–101

Družina protokolov **IEC 60870-5** spada med najbolj razširjene komunikacijske protokole v sistemih daljinskega vodenja, zaščite in nadzora v elektroenergetiki. Med njimi po razširjenosti še posebej izstopa **IEC 60870-5-101** protokol, ki je namenjen povezavi med SCADA sistemi in končnimi postajami (Remote Control Unit – RTU). Standard IEC 60870-5 opredeljuje pet dokumentov:

- IEC 60870-5-1 …… Oblika okvirja podatkov,
- IEC 60870-5-2 …… Storitve prenosa podatkov,
- IEC 60870-5-3 …… Osnovna struktura aplikacijskih podatkov,
- IEC 60870-5-4 …… Definicija in kodiranje informacijskih elementov,
- IEC 60870-5-5 …… Osnovne aplikacijske funkcije.

Družina protokolov IEC 60870-5 temelji na standardnem tri slojnem referenčnem modelu. V primerjavi s standardnim sedem slojnim referenčnim modelom ISO (Internatonal Organization for Standardization) prinaša tri slojni model določene poenostavitve pri mehanizmu prenosa podatkov, ki pa glede na ožji namen uporabe ne predstavlja nikakršnih težav. Primerjava tri slojnega modela s sedem slojnim OSI modelom je prikazan na Sliki 1.



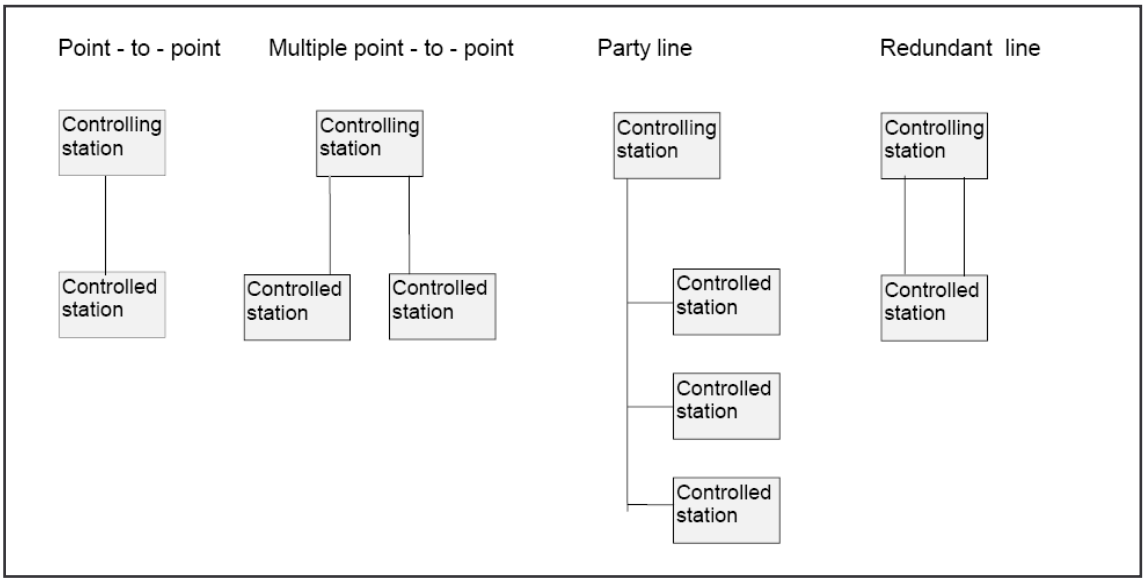
Slika 1: Primerjava 3 slojnega modela s sedem slojnim ISO-OSI modelom

Na Sliki 1 je tudi razvidno, na katere sloje protokola se nanašajo posamezni dokumenti IEC 60870-5-1 do 5.

IEC 60870-5-5 definira aplikacijske funkcije, zato je umeščen na najvišje mesto tri slojnega modela. Gre za osnovne funkcije sistemov daljinskega vodenja. Celoten nabor funkcij je osnova, na podlagi katere se z izborom parametrov (nekaterih) funkcij oblikujejo t.i. uporabniški profili, ki predstavljajo standardizirano uporabo funkcij za določen namen. Enega od takih standardnih profilov opredeljuje tudi IEC 60870-5-101.

Na nivoju fizičnega sloja IEC 60870-5-101 dopušča izbiro RS232 ali RS485 standarda priključevanja, podpira pa tudi uporabo optičnih zvez. Možni načini povezav so prikazani na Sliki 2.

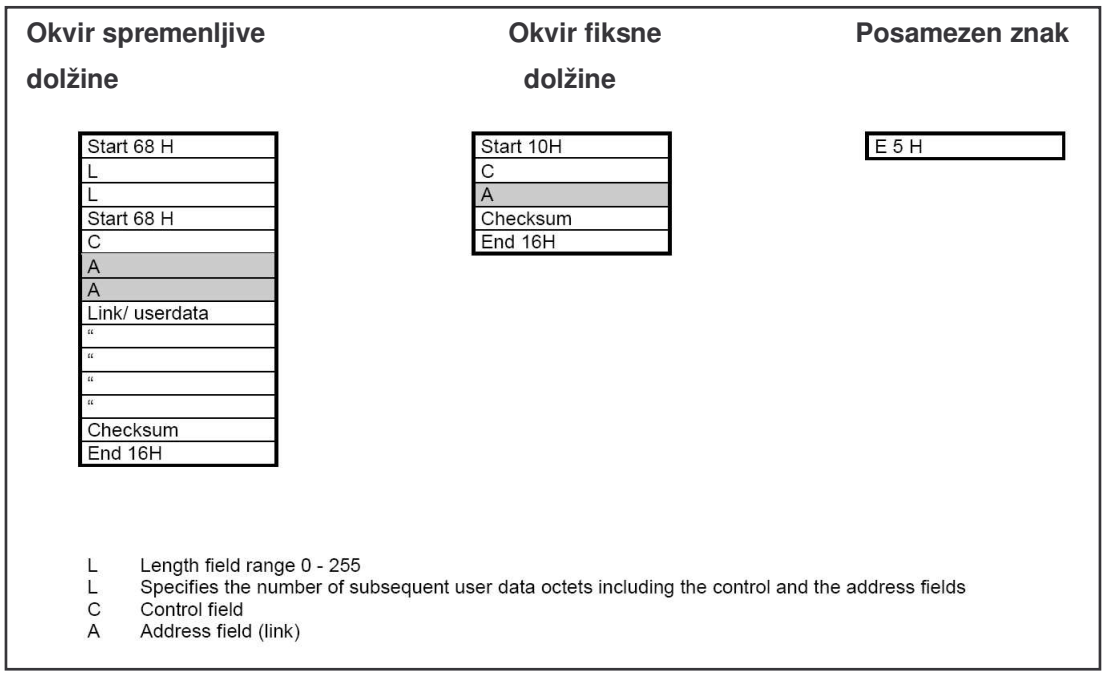
Na nivoju sloja povezave je določen okvir podatkov FT 1.2, ki zagotavlja visoko stopnjo integritete podatkov ob maksimalni učinkovitosti. FT 1.2 je v osnovi namenjen asinhroni komunikaciji in je prirejen standardnim univerzalnim asinhronim sprejemno oddajnim enotam (Universal Asynchronous Receiver/Transmitter - UART). Različne oblike okvirjev prikazuje Slika 3, obliko podatkovnega znaka pa Slika 4.



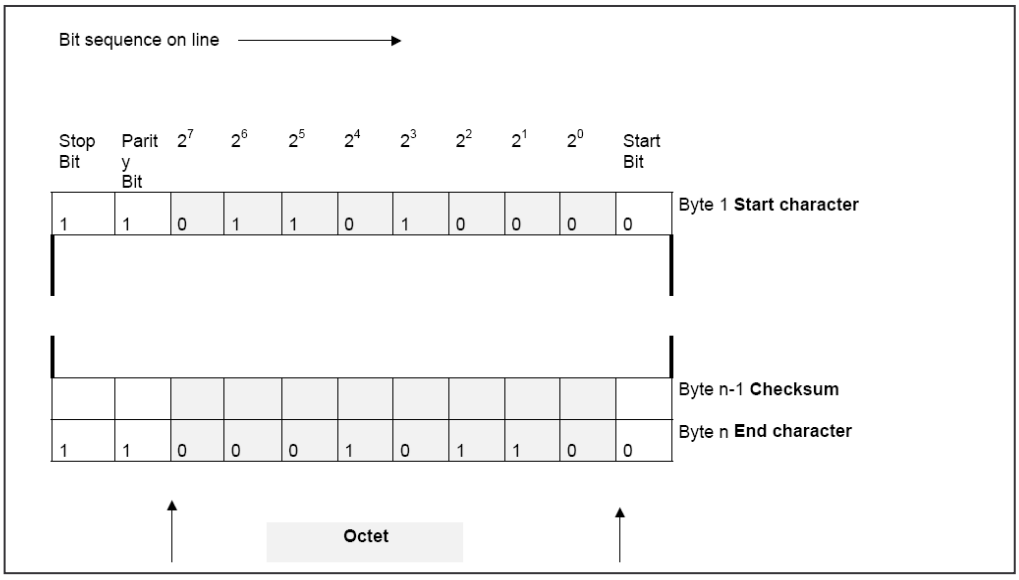
Slika 2: Možni načini omrežnih povezav po protokolu IEC 60870-5-101

Podatkovni znak je sestavljen iz enajstih bitov (Slika 3):

- 1 startni bit,
- 8 podatkovnih bitov (bit1….LSB, bit 8…MSB),
- 1 paritetni bit (soda pariteta),
- 1 stop bit.



Slika 3: Oblike podatkovnih okvirjev po FT 1.2



Slika 4: Sestava podatkovnega znaka po protokolu IEC 60870-5-101

Na nivoju sloja uporabe določa Standardni profil 101 uporabo funkcij, ki so potrebne za zagotovitev komunikacijske povezave med RTU in SCADA sistemom. V elektroenergetiki je tipično mesto uporabe zveza med komunikacijskim računalnikom v RTP in DCV.

Nabor funkcij, ki jih določa IEC 60870-5-101, je naslednji:

- inicializacija postaje (RTU),
- ciklični (krožni) prenos podatkov,
- splošni poziv,
- prenos ukazov,
- pridobivanje podatkov na poziv,
- pridobivanje dogodkov (alarmov),
- nastavitve parametrov,
- prenos datotek,
- sinhronizacija časa,
- testni postopki.

Priloga 2: Temeljne značilnosti protokola IEC 60870–5–104

IEC 60870-5-104 je mednarodni standard, ki ga je leta 2000 izdala Mednarodna elektrotehnična komisija (IEC). Iz polnega poimenovanja »Omrežni dostop za IEC 60870-5-101 s standardnimi transportnimi profili« (Network access for IEC 60870-5-101 using standard transport profiles) izhaja bistvo tega protokola, to je uporaba aplikacijske plasti protokola IEC 60870-5-101 z drugačno izvedbo plasti povezave in fizične plasti.

IEC 60870-5-104 omogoča komunikacijo med distribucijskim centrom vodenja (DCV) in razdelilno transformatorskimi postajami (RTP) preko standardnega **TCP / IP** omrežja.

IEC 60870-5-104 vsebuje nekatere omejitve parametrov in podatkovnih tipov, opredeljenih v IEC 60870-5-101, kar pomeni, da vse funkcije, ki jih podpira IEC 60870-5-101, niso na voljo v IEC 60870-5-104 (npr. kratke časovne značke, omejitve pri izbiri dolžine naslovov ...). Te omejitve ne preprečujejo pogoste souporabe obeh protokolov, previdnost pa vsekakor ni odveč.

Največja prednost IEC 60870-5-104 je, da omogoča komunikacijo prek standardnih Ethernet omrežij, kar zagotavlja istočasen prenos podatkov med več napravami in storitvami. Ob tem pa ne smemo pozabiti na varnostna tveganja, ki so še posebej velika v primeru uporabe javnih omrežij. ISO/OSI model je prikazan na Sliki 6.

7	Application Layer	IEC 60870-5-104 Companion Standard IEC 60870-5-5, IEC 60870-5-4	
6	Presentation Layer	n/a	
5	Session Layer	n/a	
4	Transport Layer	TCP (RFC 793)	
3	Network Layer	IP (RFC 791)	
2	Link Layer	PPP (RFC 1661 & RFC 1662)	Transmission of IP datagrams over ethernet network (RFC 894)
1	Physical Layer	X.21	Ethernet (IEEE 802.3)

Slika 6: Prikaz ISO/OSI modela protokola IEC 870-5-104 (vir: www.ipcomm.de)

I Z J A V A

Izjavljam, da sem magistrsko delo izdelal samostojno pod vodstvom mentorja prof. dr. Stanislava Kovačiča, univ. dipl. inž. el.

Izkazano pomoč drugih sodelavcev sem v celoti navedel v zahvali.

Edvard Košnjek, univ. dipl. inž. el.

_____