Reijo Virtanen

Sähköasemien tiedonsiirron kehittäminen Helen Sähköverkko Oy:ssä

Metropolia Ammattikorkeakoulu

YAMK

Automaatioteknologia

Opinnäytetyö

23.5.2013

Metropolia

Tekijä Otsikko Sivumäärä Aika	Reijo Virtanen Sähköasemien tiedonsiirron kehittäminen Helen Sähköverkko Oy:ssä 62 sivua + 4 liitettä 23.5.2013
Tutkinto	Insinööri YAMK
Koulutusohjelma	Automaatioteknologia (YAMK)
Suuntautumisvaihtoehto	
Ohjaajat	DI Mika Loukkalahti Lehtori Kai Virta

Sähkövoimajärjestelmä on nykyaikaisen yhteiskunnan kriittisimpiä järjestelmiä, koska sähkönjakelun keskeytyminen voi aiheuttaa vakavia seurauksia. Tietoliikenneyhteyksillä mahdollistetaan sähköverkon luotettava ja turvallinen käyttö. Tietoliikenteen kehitys on ollut viime aikoina melko nopeaa, mikä on tarjonnut uusia mahdollisuuksia myös sähköasemien tiedonsiirtoon ja vastavuoroisesti sähköasematekniikan kehitys on tuonut sähköasemille uudenlaisia tiedonsiirtotarpeita.

Tässä työssä käsiteltiin kokonaisvaltaisesti Helen Sähköverkko Oy:n sähköasemien ulkoisia tiedonsiirtotarpeita; sähköasemien sisäinen liikenne rajattiin työn ulkopuolelle. Työssä perehdyttiin eri järjestelmien, kuten esim. 110 kV siirtoverkon suojauksen ja kaukokäyttöjen vaatimuksiin ja selvitettiin niiden nykytila. Luotiin yleiskatsaus suojausperiaatteisiin ja suojareleisiin sekä kaukokäyttöjärjestelmiin ja protokolliin. Työssä on esitelty myös eri tiedonsiirtotekniikoiden teoriaa ja periaatteita ja esiteltiin Helen-konsernin nykyiset tiedonsiirtojärjestelmät. Työssä käsiteltiin myös tietoturvaa yleisellä tasolla.

Työ jaettiin seuraaviin pääaiheisiin: Helen Sähköverkko Oy:n 110 kV siirtoverkon suojaus, kaukokäyttöyhteydet ja muut sähköasemilla käytetyt yhteydet, kuten sähkön laatumittaukset, kamera-valvonta ja kiinteistönvalvonta. Jokaisesta aihepiiristä selvitettiin nykytila ja esitettiin erilaisia kehitysmahdollisuuksia.

Avainsanat	sähköasema, tiedonsiirto, sähköverkon suojaus, kaukokäyttö

Author	Reijo Virtanen
Title	Developing Substation Communication in Helen Sähköverkko Oy
Number of Pages	62 pages + 4 appendices
Date	23 May 2013
Degree	Master of Engineering
Degree Programme	Automation Technology
Specialisation option	
Instructors	Mika Loukkalahti, M.Sc. Kai Virta, Principal Lecturer

The electric power system is one of the most critical systems in modern world because being without electricity can have severe consequences. Telecommunication enables safe and reliable use of the grid. Telecommunication has developed fast lately, which has offered new possibilities to data transmission between substations and control center. The technical development of substations has also created new needs for data transmission.

This thesis focuses exclusively on external data transmission needs of Helen Sähköverkko Oy's substations. The internal data transmission of the substations was not included. This thesis surveys the current state and requirements of different systems, for example protection and remote control for a grid of 110 kV. Principles for protection, protection relays, remote control systems and protocols were overviewed. This thesis introduces theory and principles of different data transmissions techniques as well as the current data transmission systems used within the Helen Group. Cyber security was discussed in general.

The thesis was divided into the following main topics: protection for the grid of 110 kV, remote control and other connections, such as quality measurements of electricity, video surveillance and building automation. The current state and development possibilities of each topic was introduced.

Keywords	substation, telecommunication, teleprotection, remote control

Sisällys

Liitteet

Liite 1. Helsingin Energian kuparikaapeliverkko

Liite 2. Helsingin Energian valokaapeliverkko

Liite 3. Helsingin Energian PCM-verkko

Liite 4. Helsingin Energian ProLAN-verkko

LYHENTEET

BGP - Border Gateway Protocol
CESoPSN - Circuit Emulation over PSN
CWDM - Coarse Wavelength Division Multiplex
DEMUX - Demultiplexer
DMZ - Demilitarized Zone
DSP - Digital Signal Prosessor
DWDM - Dense Wavelength Division Multiplex
EIA - Electronic Industries Association
EMI - Electromagnetic Interference
FDM - Frequency Division Multiplexing
GPRS - General Packet Radio Service
GPS - Global Positioning System
HSV - Helen Sähköverkko Oy
IEC - International Electrotechnical Commission
IEEE - Institute of Electrical and Electronics Engineers
IP - Internet Protocol
IS-IS - Integrated Intermediate System to Intermediate System
ISO - International Organization for Standardization
IT - Information Technology
MAC - Media Access Control
MPLS - Multiprotocol Label Switching
MUX - Multiplexer
NTP - Network Time Protocol
OSI - Open Systems Interconnection
OSPF - Open Shortest Path First
PCM - Pulse Code Modulaatio
PDH - Plesiochronous Digital Hierarhcy
PLC - Power Line Communication
PTP - Precision Time Protocol
PWE - Pseudowire Emulation
RADIUS - Remote Authentication Dial In User Service
RIP - Routing Information Protocol
SAToP - Structure Agnostic TDM over Packet
SCADA - Supervisory, Control and Data Acquisition

SDH - Synconous Digital Hierarchy

SHDSL - Symmetric High-bitrate Digital Subscriber Line

SSH - Secure Shell

TCP - Transmission Control Protocol

TC-PAM - Trellis Coded Pulse Amplitude Modulation

TDM - Time Division Multiplex

TDMoIP - TDM over IP

WDM - Wavelength Division Multiplex

VF - Voice Frequency

VKO - Verkonkäskyohjaus

VoIP - Voice over IP

WWDM - Wide Wavelength Division Multiplex

1 Johdanto

Sähkövoimajärjestelmä on nykyaikaisen yhteiskunnan kriittisimpiä järjestelmiä. Tietoliikenneyhteydet ja niiden päälle rakennetut kaukokäyttö- ja suojausyhteydet sekä esim. sähkön laadun mittaus, kunnonvalvonta ja rakennusten tilavalvonta ovat sähköverkon luotettavan ja turvallisen käytön kannalta erittäin tärkeitä.

Tietoliikenteen kehitys on ollut viime aikoina melko nopeaa, mikä on tarjonnut uusia mahdollisuuksia myös sähköasemien tiedonsiirtoon ja vastavuoroisesti sähköasematekniikan kehitys on tuonut sähköasemille uudenlaisia tiedonsiirtotarpeita. Kaukokäytöissä perinteisiä sarjaliikenneyhteyksiä on osittain korvattu IP-yhteyksillä, ja sähköverkon suojauksessa on siirrytty perinteisistä kuparikaapeliyhteyksistä valokuituyhteyksiin. Siirtyminen IP-pohjaisiin yhteyksiin on tuonut uusia haasteita mm. tietoturvaan. Tiedotusvälineissä viime aikoina esiintyneet kyber-uhkakuvat ovat nykypäivää.

Tässä työssä käsitellään Helen Sähköverkko Oy:n (HSV) sähköasemien tiedonsiirtotarpeita ja eri järjestelmien vaatimuksia. Työ on jaettu seuraaviin pääaiheisiin: sähköverkon suojaus, kaukokäyttöyhteydet ja muut sähköasemilla käytetyt yhteydet, kuten sähkön laatumittaukset, kameravalvonta, kiinteistönvalvonta ja verkkokäsky. Lisäksi luodaan yleiskatsaus tiedonsiirron perusteisiin ja Helenin tiedonsiirtoverkkoihin. Lopussa esitetään johtopäätökset ja periaatteet, joiden mukaan voidaan jatkaa tulevaisuuteen.

2 Työn tavoitteet ja rajaus

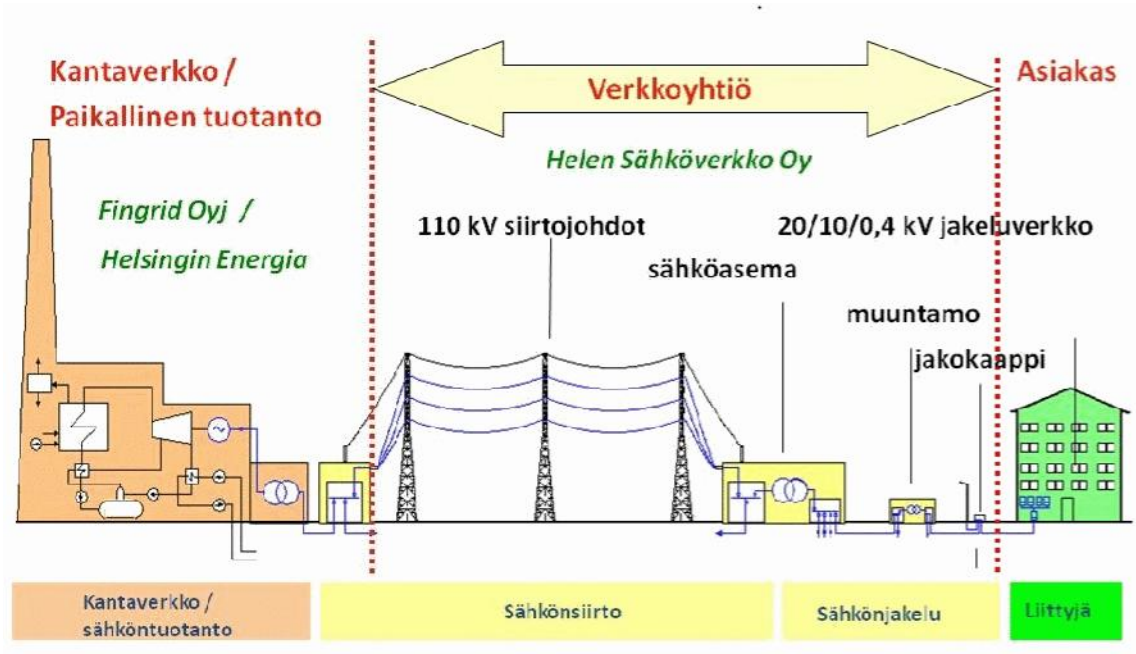
Työn tavoitteena on tarkastella HSV:n sähköasemien ulkoista liikennöintiä kokonaisvaltaisesti, selvittää yhteyksien nykytila sekä pohtia, miten liikennöintiä voisi tulevaisuudessa kehittää. Kehityskuvassa tärkeimmät katsantokannat ovat yhteyksien toimintavarmuus ja kustannustehokkuus.

Työ on rajattu käsittämään ainoastaan sähköasemien ulkopuolinen liikennöinti. Sähköasema-automaatiossa keskitytään kaukokäyttöyhteyksiin ja automaation etäkäyttöyhteyksiin, aseman sisäinen liikennöinti jätetään huomioimatta. Suojauksessa keskitytään ainoastaan differentiaalisuojaukseen ja distanssisuojaukseen sekä

keskijänniteaseman ja 110 kV aseman välisiin laukaisunsiirron viestiyhteyksiin. Sähköaseman sisällä tapahtuva releiden välinen liikennöinti on rajattu pois. Muita käsiteltäviä yhteyksiä ovat kameravalvonnan, sähkön laadun mittauksen, kunnon valvonnan ja verkkokäskyn yhteydet.

3 Helen Sähköverkko Oy

Helen-konserni on liiketoiminnallinen kokonaisuus, jonka konsernirakenteeseen kuuluu useita tytär- ja osakkuusyhtiöitä. Konsernin emoyhtiönä toimii Helsingin Energia (Helen). Helen Sähköverkko Oy (HSV) on Helen-konsernin tytäryhtiö ja yksi konsernin pääliiketoiminta-alueista. HSV vastaa sähkönsiirrosta ja sähköverkon hallinnasta Helsingin alueella, lukuun ottamatta 1.1.2009 Sipoosta Helsinkiin liitettyjä alueita. HSV:n tehtävänä on hoitaa sähköverkkoliiketoimintaa sekä tuottaa sähkön siirto- ja jakelupalveluja toimialueellaan. Asiakkaita HSV:llä on noin 360 000, ja vuosittainen sähkönkulutus toimialueella on noin 4600 GWh. HSV:n vastuualue on esitetty kuvassa 1. Yhtiö ylläpitää ja kehittää verkkoaan kulutuksen ja tuotannon tarpeita vastaaviksi. HSV:n merkittävimmät yhteistyökumppanit ovat Helenin lisäksi Mitox Oy, verkostourakoitsijat ja kantaverkkoyhtiö Fingrid Oyj. [1] [2] [3] [4]



Kuva 1. Vastuualuejako [1]

Helen Sähköverkko Oy (HSV) aloitti toimintansa 1.10.2006. Ennen tätä HSV tunnettiin Helsingin Energian HelenVerkko-yksikkönä. Yhtiön liikevaihto on noin 118,5 miljoonaa euroa ja henkilöstön määrä on noin 100 henkilöä. Päätoimipaikka sijaitsee Helsingissä Sörnäisissä, Sörnäistenkatu 1:ssä.

HSV:n sähköverkko on liittyneenä Suomen kantaverkkoon usealla sähköasemalla ja muodostaa kantaverkon kanssa rinnankäyvän verkon. Lisäksi HSV:n 110 kV verkkoon on liittyneenä paikallista tuotantoa, joka yhdessä kantaverkkoliityntöjen ja rengasmaisesti silmukoidun 110 kV verkon kanssa luo perustan sähkönjakelun käyttövarmuudelle Helsingissä. HSV:ssä on kuusi yksikköä johtoportaan lisäksi. Nämä on jaettu kuvan 2 mukaan. [1] [2]

Kuva 2. HSV:n organisaatiokaavio [1]

4 Yleistä tiedonsiirtotekniikoista

Erilaisilla siirtotekniikoilla pyritään minimoimaan etäisyyksistä ja yhteyksien määrästä aiheutuvia kustannuksia. Seuraavassa käsitellään lyhyesti eri tiedonsiirtotapojen periaatteet joihin myöhemmin esitetyt tekniikat perustuvat.

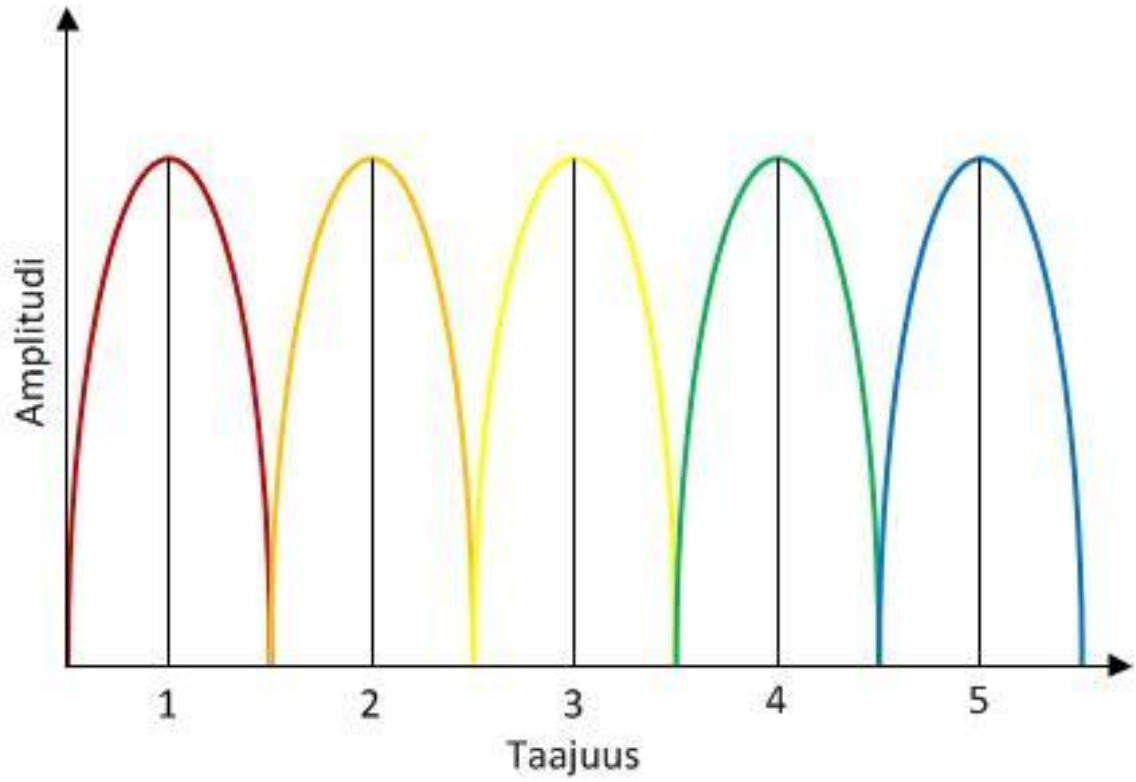
4.1 Tilajako

Jokaisella yhteydellä on oma johtonsa (kuva 3), ja yhteys tunnistetaan johdon numeron perusteella. Käytännössä esim. kaapeli, jossa jokainen pari/johdin/kuitu on erillinen yhteys. [5]

Kuva 3. Tilajako

4.2 Taajuusjako

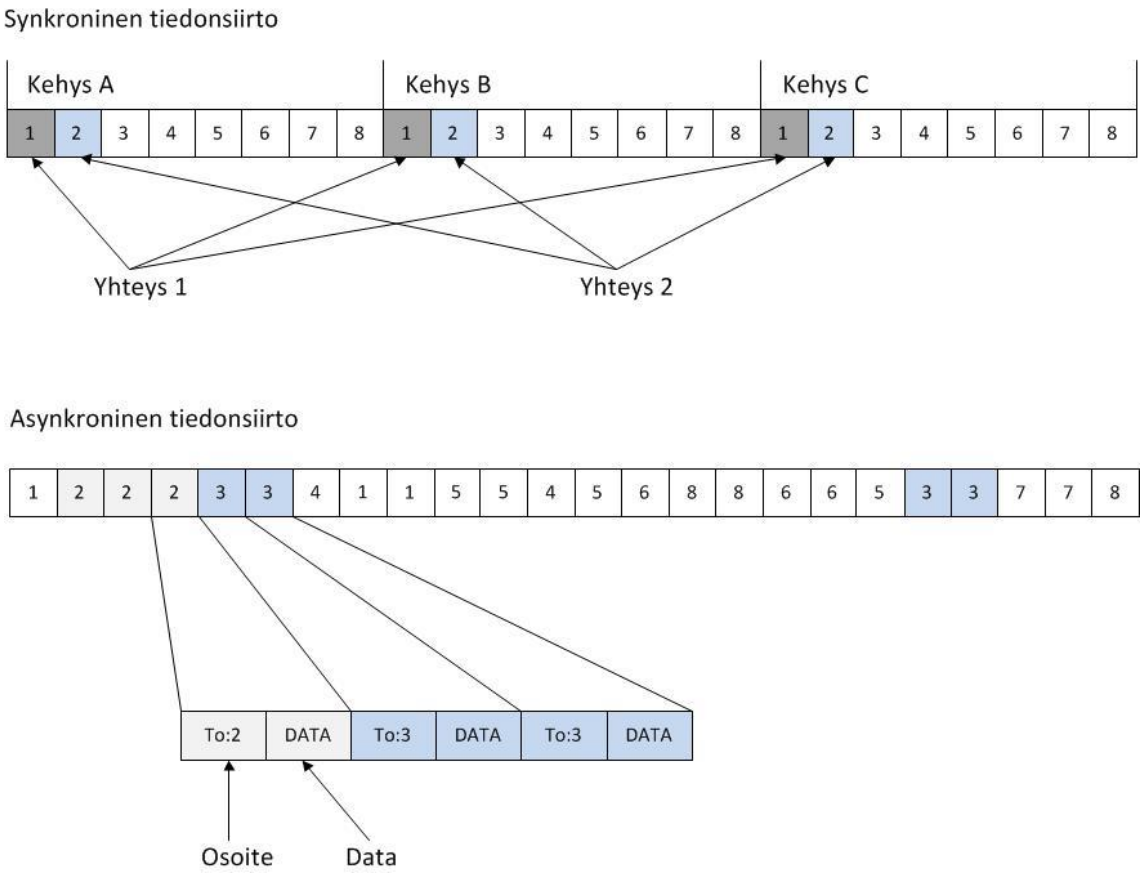
Taajuusjaossa FDM (Frequency Division Multiplexing) jokaisella yhteydellä on oma kantoaaltonsa (kuva 4), ja yhteys tunnistetaan kantoaallon perustaajuuden perusteella. Taajuusjakoa käytetään mm. radiotiellä ja valokuidussa aallonpituusjakona WDM (Wavelength Division Multiplexing). [5]



Kuva 4. Taajuusjako

4.3 Aikajako

Aikajakoinen TDM (Time Division Multiplexing) järjestelmä (kuva 5) voi olla joko synkroninen tai asynkroninen. Synkronisessa (esim. SDH tai PDH) järjestelmässä yhteys tunnistetaan sijainnin perusteella (tietyt bitit kehyksessä). Asynkronisessa (esim. IP-liikenne) järjestelmässä yhteys tunnistetaan paketissa olevan tiedon perusteella (yhteystunniste, kohdeosoite). [5]



Kuva 5. Aikajako

4.4 Yleistä tiedonsiirrosta kuparikaapeleissa

Ensimmäiset fyysisiin metallilankoihin perustuvat siirtoyhteydet Suomessa rakennettiin jo 1800-luvulla. Aluksi yhteydet olivat yksilankaisia teräslangoista rakennettuja avojohtoja, joissa kustannusten säästämiseksi paluutienä käytettiin maapotentiaalia. Ensimmäiset 2-johtimiset yhteydet otettiin käyttöön vuonna 1897. Ilma- ja maakaapeleiden käyttö Suomessa alkoi 1900-luvun alkupuolella, ja vähitellen kaikki avojohdot korvattiin kaapeliyhteyksillä. Kaapelit olivat aluksi paperieristeisiä ja niiden

ulkovaippa oli lyijyä. Tällaisia kaapeleita asennettiin 1950-luvulle saakka. Kaapelit olivat symmetrisiä nelikierre- tai parikaapeleita ja johtimien materiaali oli hehkutettua kuparia. Nelikierrekaapelit soveltuvat huonosti datasiirtoon suurehkon ylikuulumisen vuoksi. Nykyisin kaapeleiden rakenne on samantyyppinen, mutta eristemateriaalit ovat muovia ja kaapelit ovat parikaapeleita. [6] [7]

Nykyisin kuparikaapelissa siirretään pääsääntöisesti erilaisia datayhteyksiä eri tekniikoihin perustuvilla modeemeilla ja perinteinen puheensiirto on vähenemään päin. Lisäksi operaattorit ovat ajamassa kupariverkkojaan alas eivätkä enää rakenna uusia kuparikaapeliyhteyksiä. Jotkut operaattorit ovat jopa purkaneet aktiivisesti vanhoja kuparikaapeliyhteyksiään ja korvanneet niitä langattomilla tekniikoilla tai valokaapeliyhteyksillä.

Seuraavassa luvussa on esitelty lyhyesti yleisesti käytetty SHDSL-modeemitekniikka, jolla kuparikaapelissa voidaan siirtää erityyppisiä datayhteyksiä.

Lyhenne SHDSL tule sanoista Symmetric High-bitrate Digital Subscriber Line eli symmetrinen nopea digitaalinen tilaajajohto. SHDSL on standardoitu versio aiemmin käytetyistä valmistajakohtaisista ratkaisuista. SHDSL on symmetrinen eli siirtonopeus on sama molempiin suuntiin. Koodauksena SHDSL-tekniikassa käytetään TC-PAM-tekniikkaa (Trellis Coded Pulse Amplitude Modulation). SHDSL-tekniikalla dataa voidaan siirtää yhdessä kupariparissa maksimissaan 2,3 Mbit/s nopeudella noin 3 km matkalla. Siirtomatkoja voidaan kasvattaa pienentämällä siirtonopeutta ja käyttämällä useampia pareja tiedonsiirtokapasiteettia voidaan nostaa (2-parilla 4,6 Mbit/s jne.). [8]

Tekniikasta on kehitetty edelleen valmistajakohtaisia sovelluksia, joilla yhden parin siirtokapasiteetti voi olla jopa 15 Mbit/s. SHDSL-laitteita valmistavat mm. Westermo, Phoenix Contact sekä kotimainen DCombus.

4.5 Yleistä optisesta tiedonsiirrosta

Optisella tiedonsiirrolla on monia hyviä ominaisuuksia, jotka ovat vauhdittaneet alan kehitystä nopeammin kuin kehityksen alkutaipaleella osattiin odottaa. Optisen kuidun tiedonsiirtokyky on suuri, ja se mahdollistaa erittäin pitkät siirtoyhteydet. Yksimuotokuidulla on mahdollista toteuttaa yli 100 km yhteysvälejä usean kymmenen gigabitin sekuntinopeudella. Pieni vaimennus ja suuri kaistanleveys ovat kuidun

ylivoimaiset siirtotekniset edut verrattuna kuparijohtimisiin siirtojärjestelmiin. Lisäksi kuidun materiaali lasi on sähköinen eriste, jonka ansiosta kuituyhteys on lähes immuuni sähkömagneettisille häiriöille eikä myöskään aiheuta ympäristölleen häiriöitä. Kuitujen pieni koko ja keveys mahdollistavat kaapeleiden pienen koon ja keveyden. Optisen kuidun pieni koko ja materiaali tuovat mukanaan myös joitakin haittatekijöitä. Ohuen kuidun käsittely vaatii tarkkuutta ja huolellisuutta, lisäksi lasilta materiaalina puuttuu lähes kokonaan elastiset ominaisuudet. Lasin käyttäytyminen tunnetaan kuitenkin hyvin, eikä ongelmia tule, kun se otetaan huomioon kuituja käsiteltäessä ja käytettäessä asianmukaisia suojarakenteita. [9]

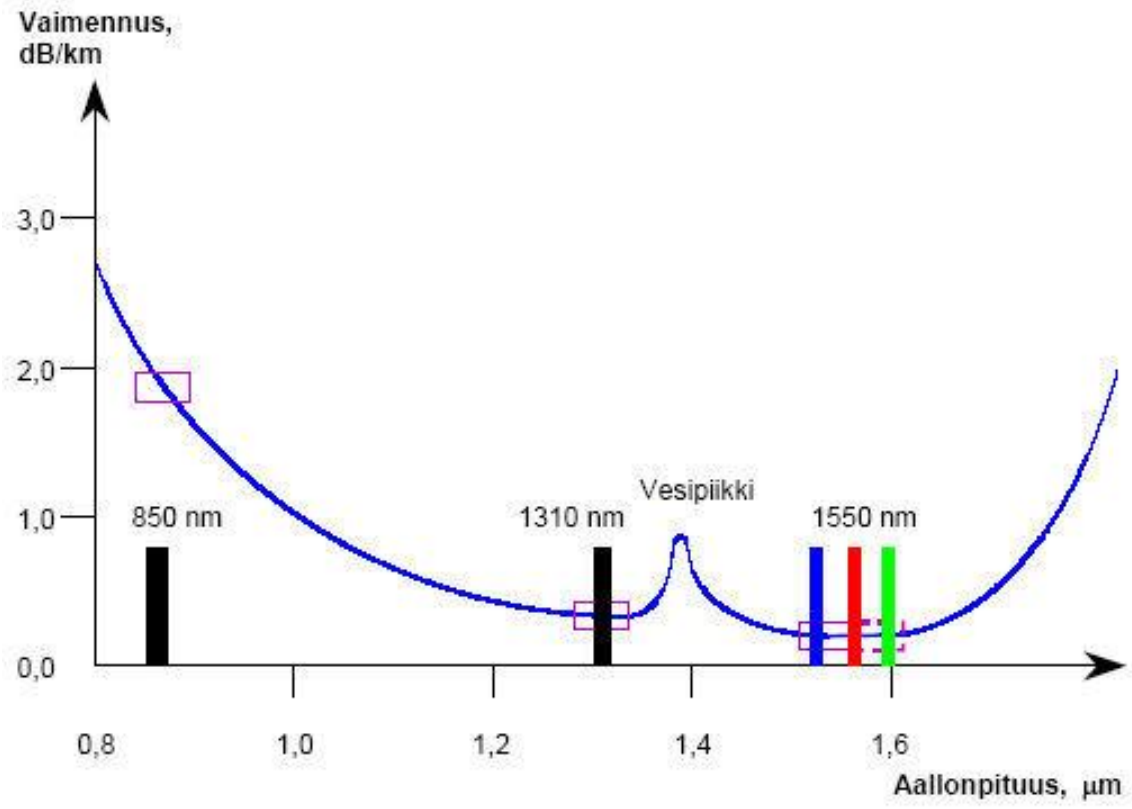
Optisessa tiedonsiirrossa signaali siirretään valon muodossa optista kuitua pitkin lähettimestä vastaanottimeen. Lähettimen tehtävänä on muuntaa sähköinen signaali valon muotoon ja sovittaa se optiseen kuituun. Lähettimessä käytetään joko laseria (pitkät yhteydet) tai valodiodia (lyhyet yhteydet). Vastaanottimessa vastaavasti muutetaan kuidulta tuleva valo takaisin sähköiseen muotoon. Kuituyhteydellä syntyy vaimennusta. Tiedonsiirtoyhteyden kokonaisvaimennus koostuu kuidun vaimennuksesta, jatkosvaimennuksista ja liitosten vaimennuksesta. Vaimennuksen lisäksi siirrettävään signaaliin vaikuttaa yhteyden kaistanleveys. Kaistanleveys määrittää suurimman yhteydellä siirrettävän taajuuden, joka puolestaan määrää suurimman tiedonsiirtonopeuden digitaalisessa siirrossa. Kaistanleveys riippuu kuidun ominaisuuksista. Määräävät ominaisuudet ovat monimuotokuidulla kaistanleveys ja yksimuotokuidulla dispersio. Koko siirtotien kaistanleveys riippuu myös lähettimen ominaisuuksista. [9]

Olennainen asia optisessa tiedonsiirrossa on tehobudjetti. Vastaanotettavan signaalin pitää olla riittävän suuri, jotta vastaanotin voi sen vielä tunnistaa. Tehobudjettiin vaikuttavat lähettimen teho, kuidun kokonaisvaimennus ja vastaanottimen herkkyys. Käytettäessä lyhyillä kuituyhteyksillä voimakkaita lähettimiä pitää yhteydelle lisätä sopivan kokoiset vaimentimet, jotta vastaanotettava signaali saadaan vaimennettua vastaanottimelle sopivaksi. Liian suuri teho vastaanottimessa saattaa lyhentää vastaanottimen käyttöikää huomattavasti. [9]

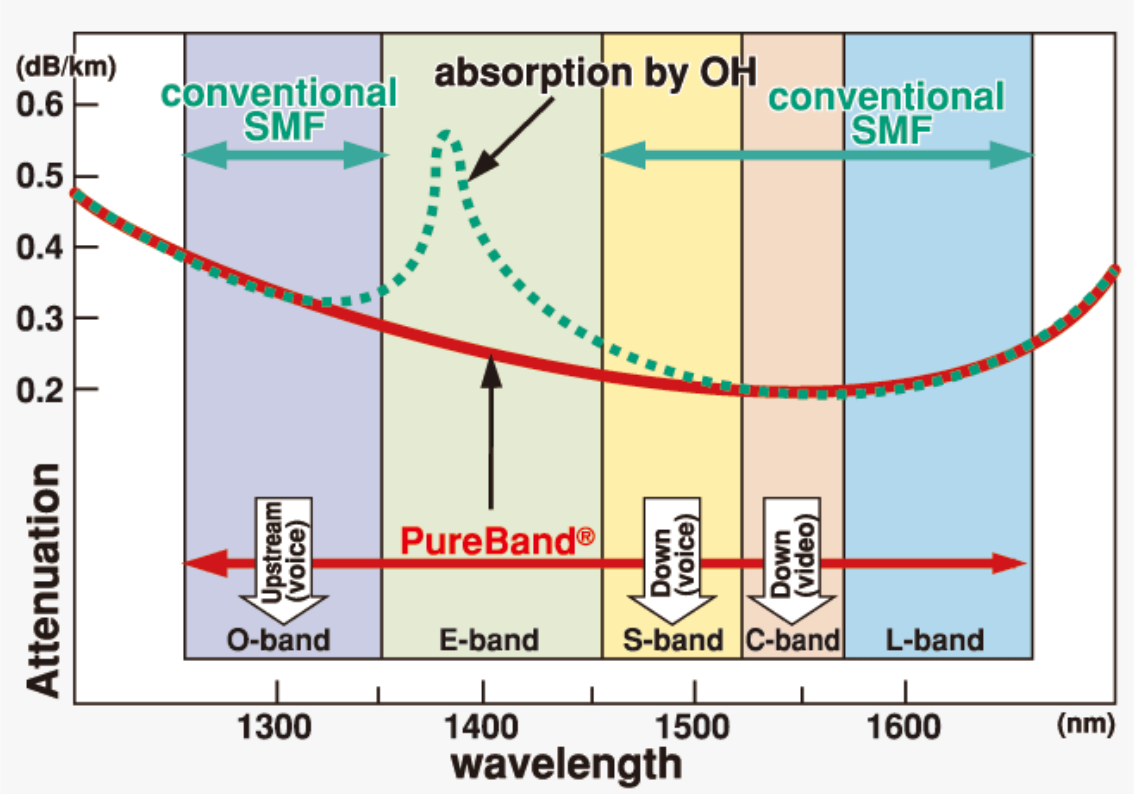
4.5.1 Valokuitujen vaimennus

Valokuidun vaimennus aiheutuu pääasiassa kahdesta syystä, sironnasta ja absorbtiosta. Absorptio aiheutuu valon imeytymisestä kuidun materiaaliin mm.

kuidussa olevien epäpuhtauksien takia. Suurin vaimennusta aiheuttava epäpuhtaus ovat OH-ionit. Sironta tarkoittaa kuidussa olevien mikroskooppisen pienten taitekerroinerojen aiheuttamaa heijastumista kaikkiin suuntiin. Teoreettisen epäpuhtauksista vapaan kuidun vaimennus määräytyy Rayleigh-sironnan perusteella, ja se on aallonpituudella 1550 nm noin 0,16 dB/km. Kvartsilasisista valmistetun kuidun vaimennus riippuu aallonpituudesta kuvan 6 mukaisesti. Kuvasta käy ilmi, että vaimennus on pieni 800 – 1700 nm aallonpituusalueella, lyhemmillä aallonpituusalueilla vaimennusta lisää ultraviolettiabsorbtio ja pidemmillä aallonpituusalueilla infrapuna-absorbtio. Vaimennuspiikki 1310 nm ja 1550 nm alueiden välissä on OH-ionista johtuva ns. vesipiikki. Alhaisen vesipiikin yksimuotokuiduissa (suositus: ITU-T G.652.D) tämä piikki on niin alhainen, että sitä voidaan käyttää myös vesipiikin aallonpituudella. Vesipiikittömän kuidun vaimennuskäyrä on esitetty kuvassa 7. [9]



Kuva 6. Kvartsilasista valmistetun kuidun vaimennus [10]



Kuva 7. Vesipiikittömän kuidun (ITU-T G.652.D) vaimennus [11]

Kuidun vaimennusta lisäävät myös makrotaipumat (säde >> 1 mm), mikrotaipumat (säde < 1 mm), vety sekä radioaktiivinen säteily. Nämä ovat lisävaimennusta aiheuttavia tekijöitä, jotka pyritään minimoimaan tai eliminoimaan kokonaan sopivilla kaapelirakenteilla ja oikeilla asennusmenetelmillä. [9]

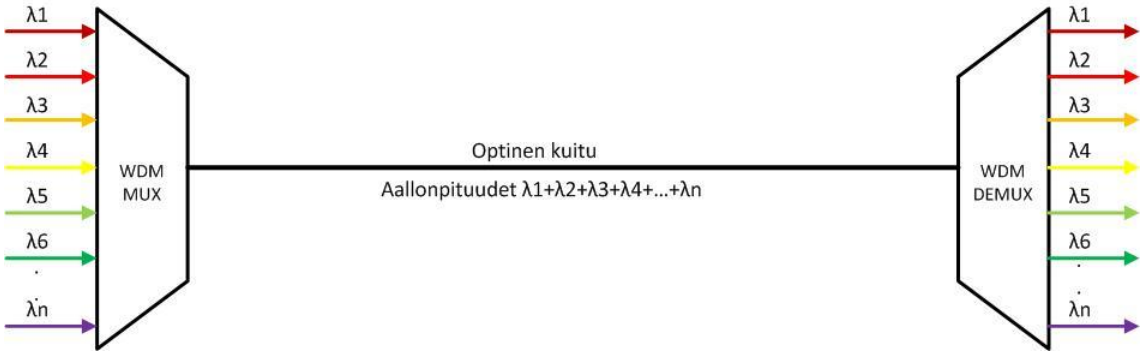
4.5.2 WDM-tekniikka

WDM eli aallonpituuskanavointi tarkoittaa sitä, että samassa kuidussa siirretään useampi signaali eri aallonpituuksilla niiden häiritsemättä toisiaan. Lyhenne WDM tulee sanoista Wavelength Division Multiplex. [9]

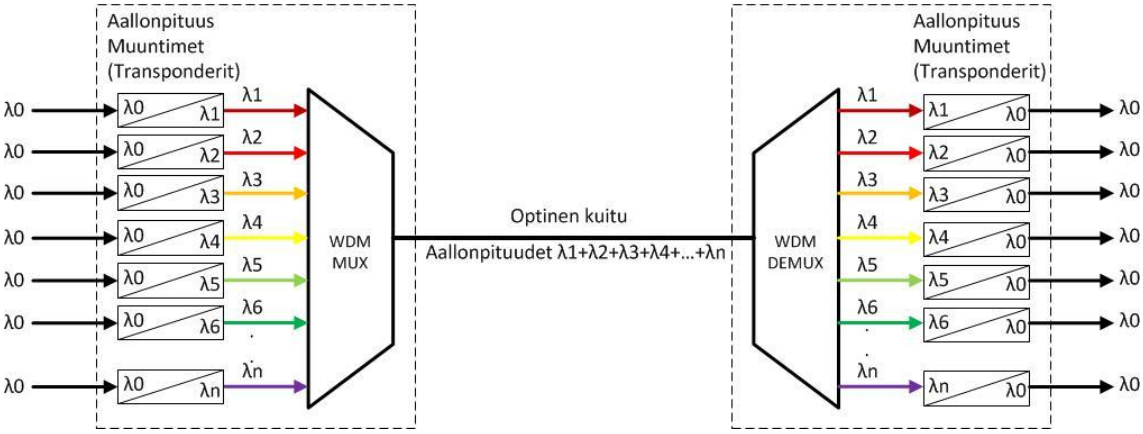
WDM-järjestelmä on periaatteeltaan optinen keskitin, joka yhdistää ja kanavoi usean siirtojärjestelmän signaalit yhteen kuituparin. Jos kaikki WDM-järjestelmään tuotavat signaalit ovat aallonpituuksiltaan yhteensopivia, voi WDM-laite olla rakenteeltaan ns. passiivinen eli se yhdistää ja jakaa kuituyhteyden signaalit ilman aallonpituusmuunnoksia. Kuvassa 8 on esitetty passiivisen WDM-järjestelmän periaate. Aktiivista WDM-järjestelmä tarvitaan silloin, kun yhdistetään samalla tai eri

aallonpituuksilla toimivia siirtojärjestelmiä. WDM:n ns. transponder-osassa suoritetaan kullekin erilliselle kanavalle aallonpituusmuunnokset ja sovitetaan ne standardin mukaiseen kanavarakenteeseen. Aktiivisen WDM-järjestelmän periaate on esitetty kuvassa 9. Aktiiviset WDM-järjestelmät ovat suhteellisen kalliita operaattoritason järjestelmiä. [12]

Multiplexer eli kanavointilaite on laite, jolla voidaan yhdistää yksi tai useampi erillinen kanava siirrettäväksi jaetulla siirtotiellä. Multiplexerillä (MUX) yhdistetään kanavat lähetyspäässä ja demultiplexerillä (DEMUX) vastaavasti erotetaan kanavat vastaanottopäässä. Käytännössä multiplexer- ja demultiplexer-toiminnallisuus ovat samassa laitteessa ja näistä käytetään yleisesti lyhennettä MUX. Kanavointi voi olla esimerkiksi taajuusjakoista esimerkiksi WDM-laitteet ja tietynlaiset radiolinkit tai aikajakoista kuten esimerkiksi PCM- laitteet. [13] [6]



Kuva 8. WDM-järjestelmän periaate



Kuva 9. Aktiivinen WDM-järjestelmä

WDM-tekniikassa käytetään kolmea perustyyppiä, WWDM (Wide Wavelength Division Multiplex), CWDM (Coarse Wavelength Division Multiplex) ja DWDM (Dense Wavelength Division Multiplex), jotka eroavat tosistaan lähinnä kanavajaoltaan.
WWDM on yksinkertaisin WDM-tekniikka, ja tässä käytetään kahta tai kolmea aallonpituutta. Käyttösovelluksena esim. yhden kuidun käyttö kahden päätelaitteen välillä, jolloin lähetys- ja vastaanottosuunnassa käytetään eri aallonpituutta. [9]

CWDM-tekniikassa käytetään 20 nm kanavajakoa alueella 1270 – 1610 nm, aallonpituudet on määritelty ITU-T-suosituksessa G.694.2. Tämä mahdollistaa 18 kanavan käytön yhdellä kuituparilla. Monesti käytetään kuitenkin laitteita, jossa on 8 CWDM-kanavaa 1470 – 1610 nm aallonpituuksilla sekä yksi laajakaistainen 1310 nm kanava. Tiedonsiirtolaitteissa yleistesti käytetty aallonpituus on 1310 nm.

Kun WDM-järjestelmän kanavat pakataan lähemmäksi toisiaan, kutsutaan järjestelmää nimellä DWDM (Dense Wavelegth Division Multiplex). ITU-T on laatinut suosituksen G.694.1, joka määrittelee kanavaväliksi 0,8 nm, 0,4 nm, 0,2 nm tai 0,1 nm, joilla yhteen kuitupariin saadaan mahtumaan vastaavasti 40, 80, 160 tai 320 alikanavaa kanavajaosta riippuen. [9] [12] [14]

4.6 Yleistä digitaalisista siirtotekniikoista

PCM-tekniikan toiminta perustuu pulssikoodimodulaatioon, jonka avulla analoginen informaatio voidaan muuttaa digitaaliseen muotoon informaation siirtämistä varten. Digitaalinen signaali muutetaan vastaanottopäässä takaisin analogiseksi. PCM-tekniikassa kanavointi on aikajakoista (TDM). Euroopassa käytetään 30-kanavaista 2,048 Mbit/s perusjärjestelmää (E1). Yhdessä aikavälissä, eli kanavassa, voidaan siirtää taajuuskaistaltaan 300-3400 Hz analogista signaalia tai 64 kbit/s dataa. PCM-järjestelmän peruskomponentti on 2M multiplekseri, jolla erilaisten kanavakorttien avulla sovitetaan käytettävät rajapinnat (äänikanavat ja erilaiset dataliitynnät) 2,048 Mbit/s perusjärjestelmän 64 kbit/s aikaväleihin. [6]

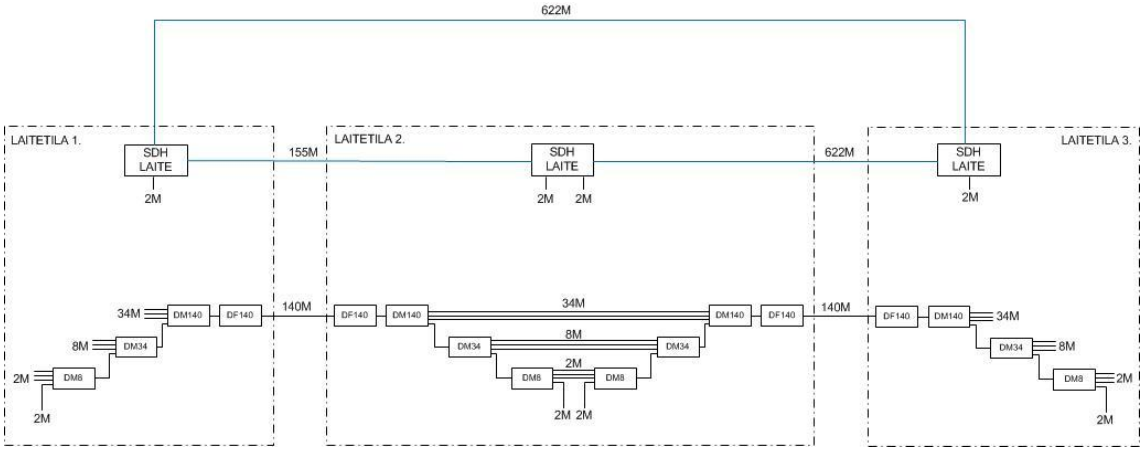
Perusjärjestelmän siirtokapasiteetti on suuremmissa siirtoverkoissa liian pieni. Tämän vuoksi on kehitetty perusjärjestelmää suurempia digitaalisia siirtojärjestelmiä. Euroopassa on käytössä PDH- ja SDH-siirtojärjestelmät. PDH-tekniikka on näistä vanhempi ja rajoittuneempi. Lyhenne PDH tulee sanoista Plesiochronous Digital Hierachy (plesiokroninen digitaalinen hierarkia). PDH-järjestelmässä ylempi järjestelmä

kanavoi neljä alemman tason järjestelmää. PDH-hierarkiatasot on esitetty taulukossa 1. PDH-järjestelmän haittapuolena on se, että järjestelmän ylempiin tasoihin (34 Mbit/s ylöspäin) ei pystytä suoraan liittymään 2 Mbit/s tasolla, vaan järjestelmä pitää aina rakentaa taso tasolta. PDH-järjestelmät on alun perin suunniteltu symmetrisille ja koaksiaalisille järjestelmille, optiset liitynnät on kehitetty myöhemmin. [6] [9]

Taulukko 1. PDH-hierarkiatasot

Nimi	Siirtonopeus [Mbit/s]	Selitys
E1	2,048	Koostuu 30 kanavasta joiden nopeus on 64 kbit/s
E2	8,448	4 x E1 kanavoituna aikajakoisesti (yhteensä 120 kanavaa)
E3	34,368	4 x E2 kanavoituna aikajakoisesti (yhteensä 480 kanavaa)
E4	139,264	4 x E3 kanavoituna aikajakoisesti (yhteensä 1920 kanavaa)
E5	564,992	4 x E4 kanavoituna aikajakoisesti (yhteensä 7680 kanavaa)

Lyhenne SDH tulee sanoista Synchronous Digital Hierarchy (synkroninen digitaalinen hierarkia). Se on PDH:ta joustavampi järjestelmä, joka on jo valmiiksi määritelty optisia liitäntöjä varten, ja sen hierarkiatasot on esitetty taulukossa 2. SDH-järjestelmässä on mahdollista liittyä 2 Mbit/s tasosta lähtien kaikilla tasoilla mihin tahansa ylempään hierarkiatasoon. SDH- ja PDH-järjestelmän hierarkiarakennetta on kuvattu kuvassa 10. SDH-järjestelmässä on mahdollisuus varmistaa yhteydet ennalta määritellyillä varareiteillä kaikilla hierarkiatasoilla, kytkentä varareitille tapahtuu alle 50 ms:ssa. SDH-järjestelmän etuja ovat myös suuremmat siirtonopeudet (10 Gbit/s asti), helppo laajennettavuus ja edistyksellinen verkonhallinta. [9]



Kuva 10. SDH- ja PDH-järjestelmän hierarkia.

Taulukko 2. SDH-hierarkiatasot

Nimi	Siirtonopeus [Mbit/s]	Selitys
STM-1	155,520	SDH:ssa on mahdollista liittyä 2Mbit/s-tasosta lähtien kaikilla tasoilla mihin tahansa ylempään hierarkiatasoon, STM = Synchronous Transport Module eli synkroninen kuljetusmoduli.
STM-4	622,080	
STM-16	2488,320	
STM-64	9953,280	

4.7 Yleistä Ethernet-pohjaisesta TCP/IP-tekniikasta

Alkuperäinen idea jaetusta siirtotiestä on peräisin Havaijin yliopiston ALOHA-radioverkkoprojektista 1960-luvun lopulta. Jaetulla siirtotiellä liikenne on aina vuorosuuntaista: kun yksi lähettää, niin muut kuuntelevat. Jaettuun siirtotiehen perustuva tekniikka ei kuitenkaan pystynyt palvelemaan riittävän hyvin jatkuvasti kasvavia liikennemääriä. 1990-luvun alkupuolella julkaistiin Kalpana-nimisen yrityksen toimesta kaksisuuntainen (full-duplex) Ethernet-tekniikka. Kaksisuuntaisuutta ja datavirran vuonohjausta koskeva standardi 802.3x julkaistiin IEEE:n toimesta vuonna 1997. Ethernet on muodostunut merkittäväksi teknologiaksi pakettikytkentäisissä verkoissa. Syynä Ethernetin suosioon on sen yksinkertaisuus. [15]

4.7.1 Kytkentäinen Ethernet

Kytkimen tehtävänä on välittää liikenne lähdeportista kohdeporttiin annettujen ohjeiden perusteella. Kytkentäisellä Ethernetillä tarkoitetaan IEEE 802.3x-standardin mukaiseen kaksisuuntaiseen tekniikkaan perustuvaa kytkintä, jossa datapakettien kytkentä tapahtuu OSI-mallin (kts. luku 4.7.3.) L2-tasolla (siirtokerros) laitteiden MAC (Media Access Control) -osoitteiden perusteella. Kytkentäisessä verkossa kytkin muodostaa yhteyden lähettävän ja vastaanottavan koneen välille yhden kehyksen ajaksi. Käytännössä kuitenkin nykypäivän L2-tason kytkimissä on myös yksinkertaisia reititysominaisuuksia. Näissä ns. reitittävissä kytkimissä pakettien välittäminen perustuu L3-tason IP-pakettien välittämiseen. [15]

4.7.2 Reititin ja reititys

Reititin on laite, jonka tehtävänä on ohjata liikennettä eri verkkojen välillä. Reititys tapahtuu OSI-mallin L3-tasolla eli verkkokerroksella. Reititin reitittää datapaketit IP-osoitteen perusteella vastaanottajalle ja tarvittaessa priorisoi ja suodattaa läpikulkevaa liikennettä. [15]

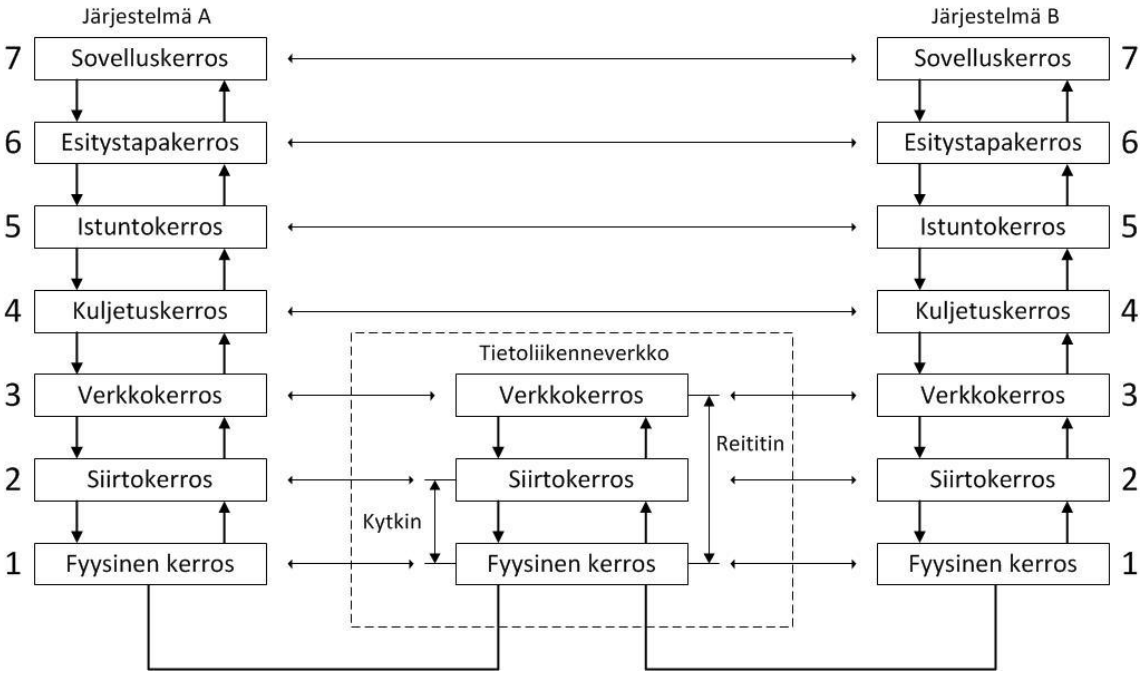
IP-reititys voidaan jakaa kahteen eri toimintoon: pakettien mekaaniseen reititykseen sisääntulosta ulostuloon ja reititystaulun tietojen välittämiseen reititysprotokollan avulla reitittimien kesken. Protokolla eli yhteyskäytäntö on sovittu käytäntö tai standardi, joka määrittelee laitteiden tai ohjelmien välisessä tiedonsiirrossa käytetyt menettelyt. Reitittimien reititystaulut voidaan määritellä myös staattisiksi, mikäli reititysprotokollia ei haluta tai voida käyttää. Staattisia reititystauluja ylläpidetään manuaalisesti. Reititysprotokollien tehtävänä on hoitaa yhteen liitettyjen IP-verkkojen välisen liikenteen reititystietojen jakelu siten, että reitit aliverkkojen välillä ovat järkeviä ja IP-paketit löytävät aina perille oikeaan osoitteeseen. Reititysprotokollan tehtävänä on myös huolehtia siitä, että reitityssilmukoita ei synny. Reitityssilmukka on tilanne, jossa IP-paketti jää pyörimään verkkoon löytämättä koskaan perille. Yleisimpiä reititysprotokollia ovat: RIP (Routing Information Protocol), OSPF (Open Shortest Path First), IS-IS (Integrated Intermediate System to Intermediate System) sekä BGP (Border Gateway Protocol). [15] [16]

4.7.3 OSI-malli

Tietoliikenteessä protokolla on säännöstö, jota noudattamalla lähettävän ja vastaanottavan laitteen välinen tiedonsiirto on mahdollista. Järjestelmästä riippuen protokolla voi sisältää määrittelyn mm. siirrettävän datan kehysrakenteesta, virheiden havaitsemisesta ja korjauksesta sekä pakettien reitityksestä laitteiden välillä. Käytännössä liikennöivä järjestelmä koostuu yleensä useista eri protokollista, jolloin tällaista kokonaisuutta voidaan kutsua protokollapinoksi. [17]

Kansainvälinen standardoimisliitto ISO (International Organization for Standardization) on luonut OSI-mallin (Open Systems Interconnection) ohjaamaan protokollien suunnittelua ja selkeyttämään valmistettavien järjestelmien rakennetta. OSI-mallissa tietoliikennejärjestelmä jaetaan toiminnallisiin osiin eli kerroksiin.

Kerrosten tehtävä on määritelty tarkkaan samoin rajapinnat muiden kerrosten kanssa. Kerrosten toteutus on sen sijaan jätetty valmistajalle. OSI-malli itsessään ei ole protokolla, vaan viitemalli tietoliikenteen standardoimistyölle ja protokollien suunnittelulle. OSI-malli on kuvattu kuvassa 11, OSI-mallissa Järjestelmän A Sovelluskerros (L7) kommunikoi Järjestelmän B Sovelluskerroksen kanssa, Esitystapakerros (L6) vastaavasti Esitystapakerroksen kanssa jne. [17]

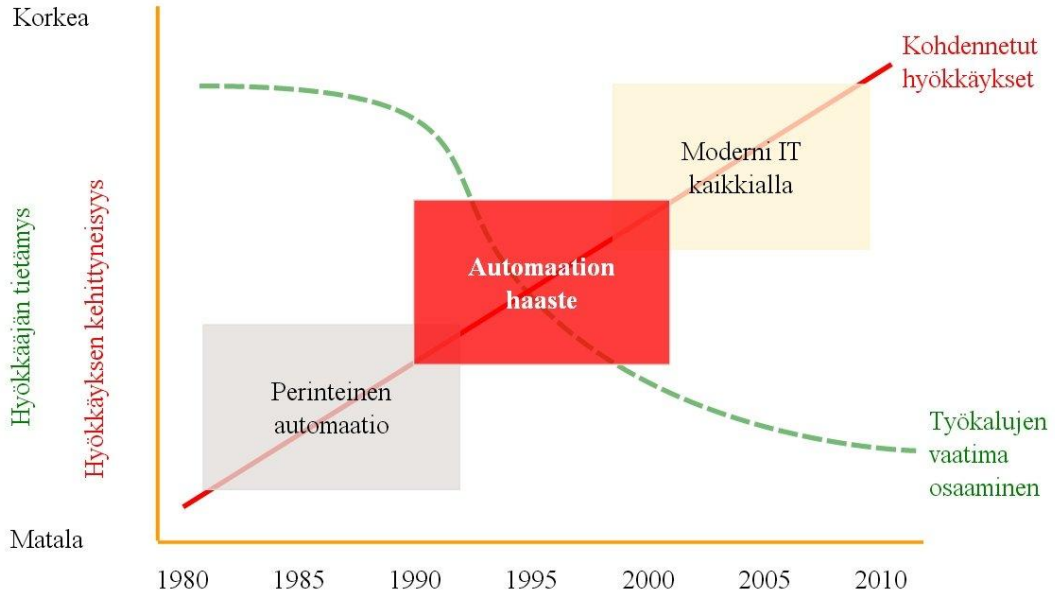


Kuva 11. OSI-malli

5 Tietoturva

Tietoturva on muodostumassa koko ajan tärkeämmäksi osaksi erilaisia automaatiojärjestelmiä. 1980-luvulla tietomurtoja tekivät harrastajat haastaessaan omaa osaamistaan yrittämällä murtautua valtionhallinnon ja armeijan palvelimiin. Nykyisin tietomurtoihin ovat erikoistuneet ammatilliset rikolliset ja valtiot tavoitellakseen rahallista tai muuta hyötyä. Samaan aikaan hyökkäys- ja murtautumistyökalut ovat muuttuneet helppokäyttöisemmiksi ja niitä voi ladata valmiina työkalupaketteina internetistä. Automaatiojärjestelmien haasteena ovat myös niiden pitkän käyttöiän aiheuttamat ongelmat nopeasti kehittyvässä IT-maailmassa. Toisin sanoen automaatiojärjestelmissä käytetään monesti vanhoja haavoittuvia versioita käyttöjärjestelmistä, ja niiden päivittäminen tuotannossa olevassa laitoksessa on

erittäin riskialtista ja vaikeaa. Kuvassa 12 on havainnollistettu, miten hyökkäysten vaatima tietotaito on pienentynyt samalla kun hyökkäysten kehittyneisyys on kasvanut viimeisen 30 vuoden aikana. [16]

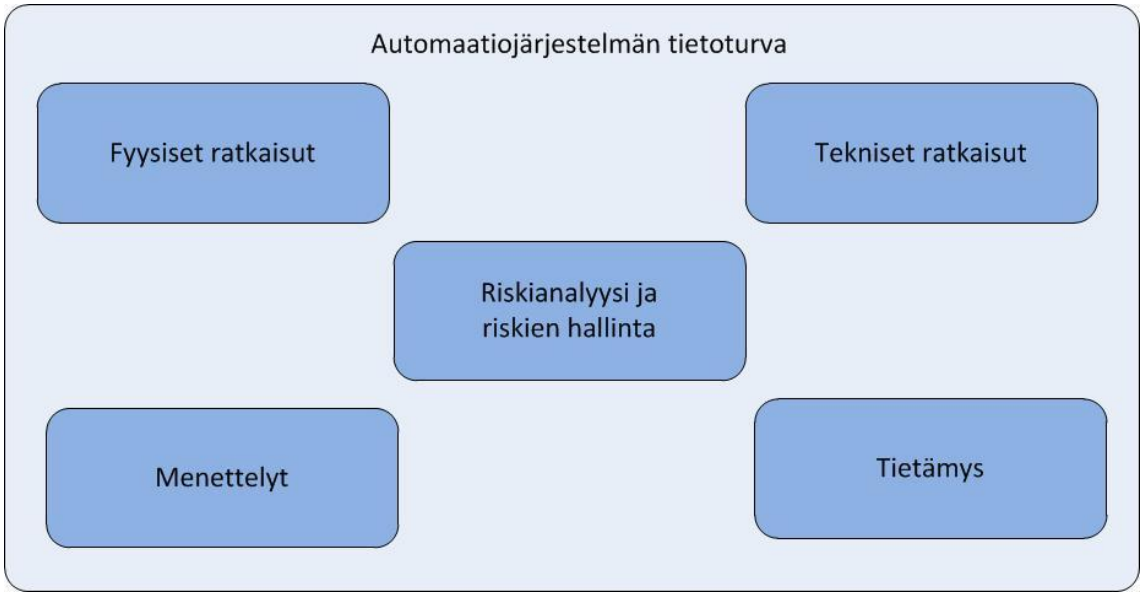


Kuva 12. Automaatiojärjestelmien riskikentän muuttuminen (© Jari Seppälä) [16]

Sähköverkon voidaan kokonaisuutena katsoa muodostavan yhden suuren automaatiojärjestelmän. Automaation tärkeimpinä tekijöinä voidaan pitää luotettavuutta ja käytettävyyttä. Näiden osa-alueiden aikaansaamisessa kriittisimmät tekijät ovat tietoturva ja toiminnallinen turvallisuus. Voidaan sanoa, että automaatiojärjestelmä on verkottunut ohjelmistotuote, joka väärin toimiessaan voi aiheuttaa fyysistä vahinkoa (esim. jos sähkö- tai kaukolämpöverkko lakkaa toimimasta 30 asteen pakkasella). [16]

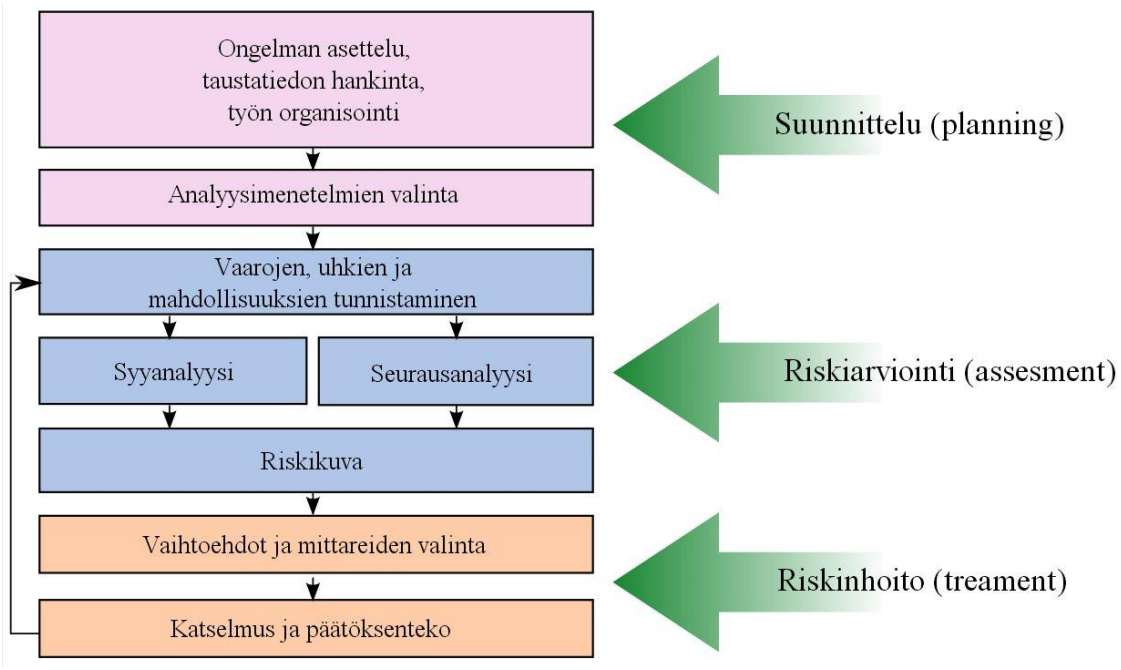
IP-verkkojen käytön lisääntyessä automaatiosovelluksissa tietoturva muodostuu yhä tärkeämmäksi osaksi kaikkia automaatiojärjestelmiä. Perinteisissä järjestelmissä, joissa tietoliikenne perustuu sarjaliikenteeseen ja virta- ja jänniteviesteihin, vaatii järjestelmän sabotoiminen enemmän viitseliäisyyttä ja tietoa. Tällöin pitää mennä paikan päälle esim. johonkin ristikytkentäpisteeseen tai laitetilaan päästäkseen käsiksi järjestelmiin. Aiheutettava vahinko voi olla silti yhtä suuri kuin moderneja järjestelmiä hyväksikäytettäessä. IP-pohjaisissa järjestelmissä hyökkäyksen tai tunkeutumisen voi tehdä etänä vaikka toiselta puolelta maapalloa helppokäyttöisiä työvälineitä käyttäen.

Tietoturva automaatiojärjestelmissä voidaan jakaa viiteen eri osa-alueeseen: fyysisiin ratkaisuihin, teknisiin ratkaisuihin, menettelyihin, tietämykseen sekä riskianalyysiin ja riskien hallintaan (kuva 13). Monesti tietoturva nähdään ainoastaan tekniikkana, vaikka tekniset ratkaisut ovat vain osa kokonaisuutta. Riskitietoisuus on yksi oleellisimmista osista kokonaistietoturvaa. Tärkeintä on tiedostaa riskien olemassaolo ja riskienhallinnan kautta tarkastella, onko riskin poistaminen tai siirtäminen mahdollista vai hyväksytäänkö riski sellaisenaan. Toteutunut turvallisuus on aina kompromissi, ja erilaiset tietoturvaratkaisut pitää valita tietoturvan tason ja järjestelmän käytettävyyden välimaastosta. Jos järjestelmän tietoturva kiristetään teknisillä ja fyysisillä ratkaisuilla äärimmilleen, sen käytettävyys pakosti kärsii. [16]



Kuva 13. Tietoturvan osa-alueet [16]

Riskianalyysi on tietoturvan parantamisessa tärkeä työkalu, riskianalyysin avulla voidaan rajalliset kehittämisresurssit ohjata oikeisiin ja mielekkäisiin hankkeisiin. Riskianalyysin avulla saadaan selville, mitkä ovat tietoturvatapahtumien taustalla vaikuttavat oikeat syyt, olivat ne sitten käytännön ongelmista johtuvia tai teknisiä. Tyypillinen riskianalyysimalli on esitetty seuraavassa kuvassa 14.



Kuva 14. Tyypillinen riskianalyysi (© Jari Seppälä) [16]

Riskianalyysissä tulee tiedostaa ainakin seuraavat asiat [16]:

- haavoittuvat komponentit
- miten hyökkääjät pääsevät sisälle
- miten onnistuneet hyökkäykset voidaan rajata [16]

Automaatioverkkoa voidaan suojata teknisesti esimerkiksi palomuureilla, yhteyksien salauksella ja vahvalla käyttäjien tunnistuksella (esim. muuttuvat salasanat verkkoon kirjauduttaessa). Automaatioverkon suojauksessa on yleisesti käytetty ns. syvyyssuuntaista suojausta (kts. luku 6.4 Helenin ProLAN- verkko). Tässä mallissa järjestelmä suojataan useammalla eri kerroksella (kts. kuva 18. Syvyyssuuntaisen suojauksen periaate), jolloin ulomman kerroksen murtaminen ei vielä lamauta koko järjestelmää. Hyökkäyksen sattuessa sisemmät kerrokset voidaan erottaa omaksi kokonaisuudekseen ja jatkaa tuotantoa. Tietoturvan tehtävänä on pidentää reaktioaikaa.

Teknisten ratkaisujen lisäksi, jopa näitä tärkeämpänä, tulee kiinnittää huomiota henkilötietoturvaan ja fyysiseen tietoturvaan. Henkilötietoturvalla käsitetään käyttäjien tekemiä toimenpiteitä, mm. muistitikkujen käyttäjät eivät monesti tule miettineeksi,

miten suuren riskin muistitikun työntäminen automaatiojärjestelmän laitteeseen aiheuttaa (esim. Stuxnet ja sen johdannaiset). Mikään palomuuri ym. ratkaisu ei pelasta tilannetta, mikäli järjestelmän käyttäjä tuo haittaohjelman muistitikulla suoraan järjestelmään. Henkilötietoturvaa voidaan parantaa kouluttamalla ja motivoimalla henkilökuntaa, usein erilaiset tietoturvariskit syntyvät vahingossa, johtuen käyttäjien ajattelemattomuudesta ja tiedon puutteesta. Muistitikkujen käytön riskiä taas voidaan pienentää järjestämällä mahdollisuus tikkujen virusskannaukseen ennen niiden työntämistä laitteistoon. [16]

Fyysisellä tietoturvalla tarkoitetaan esim. laitekaappien lukituksia ja kulunvalvontaa. Nykyaikaisessa IP-pohjaisessa verkossa on entistä tärkeämpää suojata tietoliikennelaitteet niin, etteivät asiattomat pääse niihin käsiksi. On melko turhaa suojata järjestelmää palomuureilla ym. teknisillä ratkaisuilla, mikäli tietoliikennelaitteet sijaitsevat tiloissa, joihin on suhteellisen vapaa pääsy.

6 Helsingin Energian tiedonsiirtoverkot

Helenin tiedonsiirtoverkkoja operoi ja hallinnoi erillisliiketoimintayksikkö ICT-palvelut. Helsingin Energian ICT-palvelut tuottaa tai hankkii ydinliiketoimintojen tarvitsemat tietotekniset ratkaisut. Seuraavassa katsaus ICT-palveluiden hallinnoimista tiedonsiirtoverkoista. [18]

6.1 Kupariverkko

Helenillä on oma telekaapeleilla rakennettu kupariviestiverkko. Verkko kattaa lähes kaikki toimipisteet ja sen kapasiteetti on noin 11 500 parikilometriä. Kaapeleita on asennettu usean vuosikymmenen ajan, vanhimmat kaapelit ovat paperieristeisiä lyijyvaippaisia puhelinkaapeleita, muovieristeisiin kaapeleihin siirryttiin 1950-luvulla niiden tultua markkinoille. Kaapelityyppeinä on käytetty mm. ARM-V- ja VMOHBU-kaapeleita, vanhimmat kaapelit ovat nelikierrekaapeleita ja uudemmat parikaapeleita. Kuparikaapeliverkko on esitetty liitteessä 1.

Kuparikaapeleita on asennettu erikseen kaukokäyttösovelluksiin ja puhelinsovelluksiin. Erona näissä on se, että puhelinkäyttöön rakennetuista kaapeleista osa on pupinoituja

eli kaapelin induktanssia on lisätty kytkemällä kaapeliin säännöllisin välein ns. pupinointikeloja. Induktanssin lisääminen parantaa kaapelin siirto-ominaisuuksia puhetaajuuksilla, ja näin ollen puhelimen siirtomatkaa voidaan kasvattaa. Nykytekniikalle pupinoinnista on lähinnä vain haittaa, koska pupinointi rajoittaa kaapelin siirtokaistaa ja näin ollen tekee siitä käyttökelvottoman esim. SHDSL-tekniikalle. [6]

Kaapelit on asennettu maahan joko suoraan hiekkaan tai betonikouruilla suojattuna ja myöhemmin putkiin. Yhteiskäyttötunneleissa kaapelit on sijoitettu kaapeliarinoille tai tunnelin lattiaan putkitettuna 110 kV kaapeliasennusten yhteydessä. Kupariverkkoa käytetään mm. kaukokäyttöyhteyksien varayhteyksinä, sähköverkon suojauksessa, lankapuhelimissa, erilaisissa suorissa mittauksissa (lähinnä Lämmitysmarkkinat-yksikön tarpeisiin) sekä IP-verkon reuna-alueilla käyttäen SHDSL-tekniikkaa.

Yhteiskäyttötunneleiden uusien turvallisuusmääräysten mukaan tunneleihin arinalle asennettavien kaapeleiden pitää olla halogeenittomia ja itsestään sammuvia. Markkinoilla ei ole yleisesti saatavilla tunneliolosuhteisiin sopivia palamattomia kaapeleita, joten nämä pitää teettää. Tämä pitää ottaa huomioon asennusaikatauluissa, koska erikoistilauksella tehtävien kaapeleiden toimitusaika on minimissään viisi viikkoa.

6.2 Valokuituverkko Helenillä

Helenillä on kaupungin kattava valokuituverkko, verkon kapasiteetti on noin 6750 kuitukilometriä. Valokuitukaapeleita on asennettu kuparikaapeleiden tapaan putkiasennuksilla maahan, yhteiskäyttötunneleihin arinoille ja maahan tunnelin lattialle putkiin 110 kV johtoasennusten yhteydessä, näiden lisäksi kaapeleita on asennettu myös 110 kV linjojen ukkosköysiin. Tietyillä yhteysväleillä vapaata kuitukapasiteettia on erittäin vähän tai ei ollenkaan. Kuituverkkoa rakennetaan kuitenkin koko ajan lisää, joten nämä ”pullonkaulat” tulevat poistumaan tulevaisuudessa.

Valokuitukaapelit ovat 8–192-kuituisia, joista vanhimmat 8-kuituiset asennukset ovat 1990-luvun alkupuolelta. 2000-luvun alkupuolella runkoyhteyksissä siirryttiin käyttämään 96-kuituisia kaapeleita, ja viime vuosina kuitukaapeleiden hinnan laskiessa ja kuitutarpeiden kasvaessa on siirrytty käyttämään 192-kuituisia kaapeleita. Useampikuituisten kaapeleiden käyttö ei ole tällä hetkellä järkevää, koska mahdollisen kaapelivaurion sattuessa kaapelin korjausaika yli 192-kuituislla kaapeleilla muodostuu

turhan pitkäksi. 192-kuituisen kaapelin jatkamiseen kuluu suurin piirtein yksi työpäivä. Kuitukaapelista on päätetty ainoastaan osa kuiduista, ja ylimääräiset kuidut on jätetty telineisiin ja jatkoskoteloille odottamaan tulevaisuuden tarpeita. Kaikki runkoverkossa käytetyt kuidut ovat yksimuotokuitua ja uusimmat (2000-luvulla asennetut) ovat vesipiikitöntä tyyppiä ITU-T G.652.D. Monimuotokuituja on käytetty jonkin verran kiinteistöjen sisäisessä kaapeloinnissa. Valokaapeliverkko on esitetty liitteessä 2.

Valokuituverkko toimii fyysisenä siirtotienä Helenin PCM-, toimisto- ja prosessiverkolle (ProLAN) sekä sähköverkon suojausyhteyksille (differentiaalisuojat). Tulevaisuudessa myös distanssisuojat ja varakaukokäyttöyhteydet on tarkoitus siirtää kuituyhteyksille.

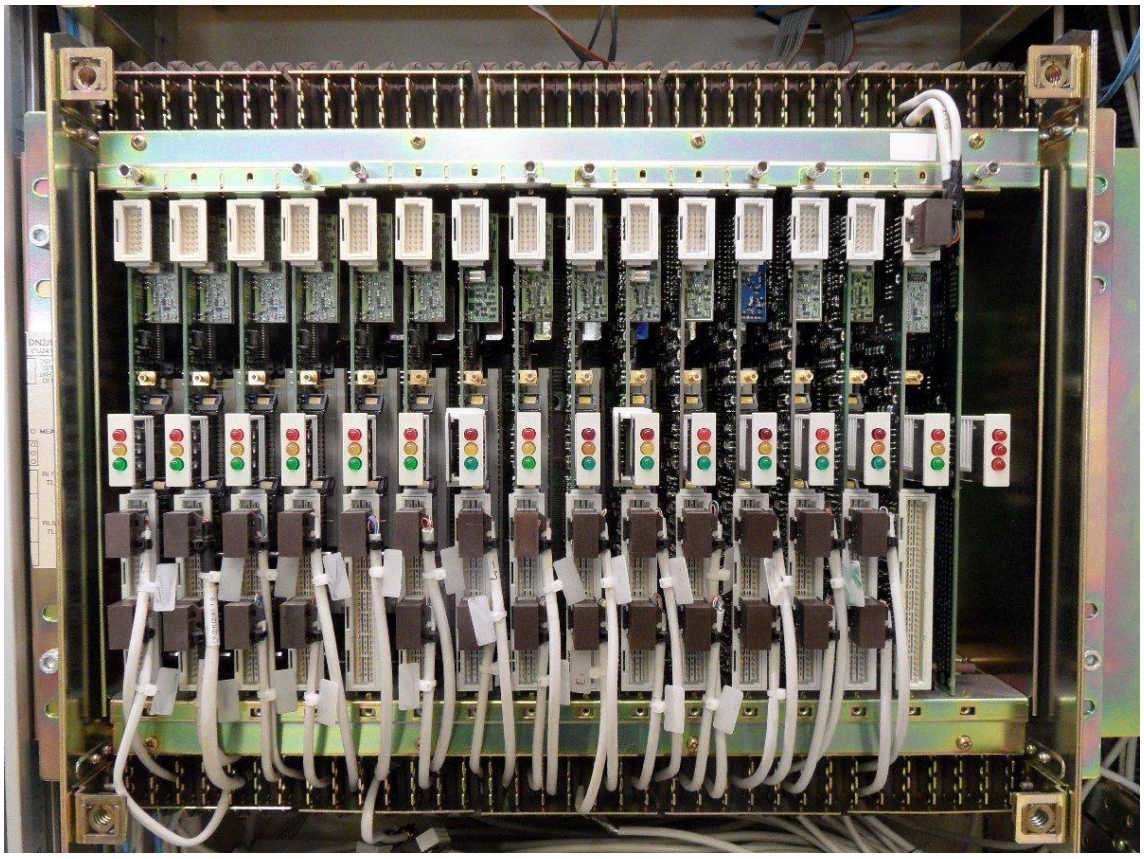
6.3 Helenin PCM-verkko

Helenillä PCM on yleisnimitys digitaaliselle siirtoverkolle. Helenin digitaalisen siirtoverkon runkoyhteydet on toteutettu PDH-tekniikalla, rungossa on käytetty 34 ja 8 Mbit/s.laitteita. Siirtoverkkoa valvotaan Nokian valmistamalla NMS-10-valvontaohjelmistolla. Ohjelmisto alkaa tulla elinkaarensa päähän ja sitä ollaan uusimassa.

Helenillä on käytössä NOKIAn (nykyisin Nokia Siemens Networks) valmistama PCM-järjestelmä, jolla voidaan siirtää sekä analogista että digitaalista tietoa. PCM-runkoverkko on rakennettu kattamaan lähes kaikki Helenin ja HSV:n toimipisteet (verkkokuva liitteessä 3.). Siirtotienä käytetään Helenin, HSV:n sekä Elisan omistamia valokuituja. Helenin runkoyhteydet on toteutettu PDH-tekniikalla pääasiassa 8 M ja 34 M hierarkiatasoilla käyttäen kuitulaitteita.

Runkoverkon asiakasrajapintoina ovat 2 Mbit/s G.703-liitynnät sekä 64 kbit/s aikavälit, jotka voidaan kytkeä erilaisiin rajapintoihin 2 Mbit/s DM2 MUX -laitteiden kanavakorttien avulla, rajapintoina mm. VF-kanavat (äänikanava), V.28-datakanavat sekä 64 kbit/s G.703-kanavat. 64 kbit/s aikavälien ristikytkennät tehdään digitaalisten ristikytkentälaitteiden DN2 sekä digitaalisten haaroituslaitteiden DB2 avulla. DN2-ristikytkentälaitteen maksimikytkentäkapasiteetti on 40 kpl 2 Mbit/s G.703/704/706-liityntää, laitteen kytkentämatriisi on estoton. DB2-laitteen kytkentäkapasiteetti on 3 kpl 2 Mbit/s liityntöjä ja kytkentämatriisissa on rajoituksia. DM2 MUX -laite kanavakortteineen on esitetty kuvassa 15 ja digitaalinen ristikytkentälaite DN2 kuvassa 16.

Kuva 15. 2Mbit/s MUX-laite DM2 ja 4 kpl kanavakortteja.



Kuva 16. Digitaalinen ristikytkentälaite DN2 täyteen kalustettuna.

Verkossa siirrettävät yhteydet ovat point-to-point-yhteyksiä tai point-to-multipoint-yhteyksiä. Jälkimmäistä käytetään verkkokäsky-yhteyksissä, joissa haaroitus on tehty DN2-ristikytkentälaitteilla.

PCM-verkossa ei ole käytössä minkäänlaisia automaattisia asiakasyhteyden varmistusmekanismeja. Kriittisimmät yhteydet on varmistettu käyttämällä varayhteytenä toista mediaa, esim. suoraa modeemiyhteyttä kupariverkossa.

PCM-laitteet sijaitsevat pääasiassa sähköasemilla. Näissä sähkönsyöttö on toteutettu sähköaseman akustosta 110-220 V/48 V DC/DC-muuntimilla tai aseman 48 V akustosta. Muissa kohteissa sähkönsyöttöön on käytetty 48VDC:n PoMo vaihtosuuntaajia tai muita akuilla varustettuja syöttölaitteita. Sähköasemien akustot on mitoitettu 10 h varakäyntiajan mukaan ja PoMo-vaihtosuuntaajat 2 h mukaan (täydellä kuormalla). PoMo- vaihtosuuntaajat on kytketty diesel-varmistettuihin sähkönsyöttöihin.

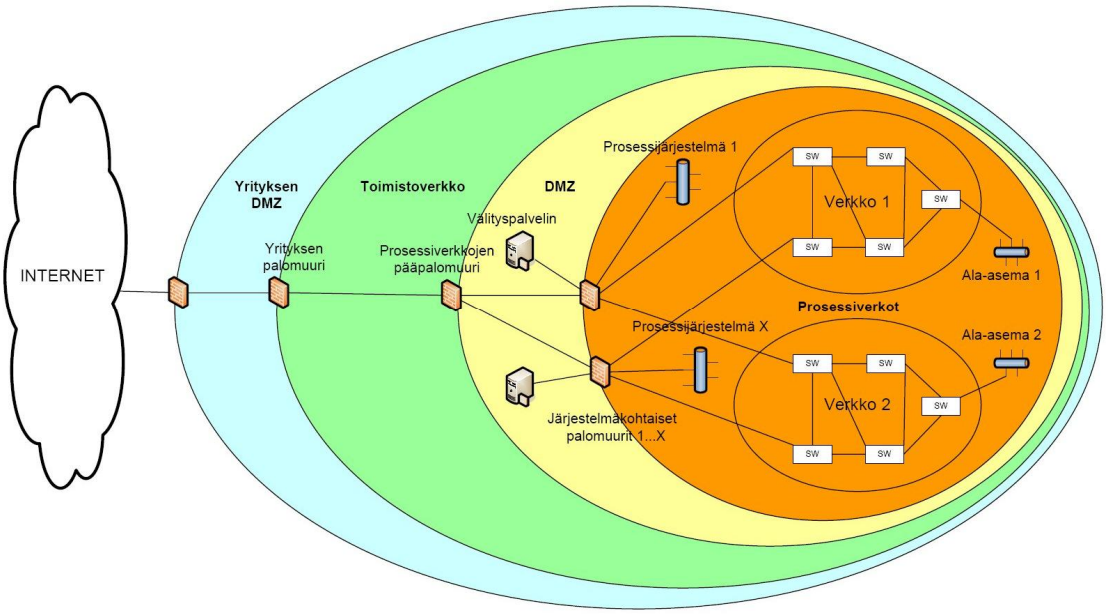
Tärkeimmät runkoyhteydet on tarkoitus korvata renkaaseen asennetuilla SDH-laitteilla, jolloin runkoverkon vikasietoisuus paranee uudelleenreititysominaisuuksien myötä (uudelleenreititys alle 50 ms ennalta määritellylle reitille). SDH-laitteiden myötä myös valokuituverkossa suoritetut muutostyöt aiheuttavat vähemmän haittaa asiakasyhteyksiin.

6.4 Helenin ProLAN-verkko

Prosessijärjestelmien kriittisyyden takia näitä järjestelmiä varten on Helenin ICT-palveluiden toimesta kehitetty erillinen ympäristö, jolle on annettu nimi ProLAN. ProLAN-palvelukokonaisuus on keskitetty verkkoympäristö omine palveluineen, johon eri liiketoimintojen tuotantokriittiset järjestelmät voidaan liittää. Ympäristö on skaalautuva kaikille Helen-konsernin liiketoiminnoille ja tytäryhtiöille. Tästä saadaan etuna keskitetty ylläpito ja tietoturva-arkkitehtuuri. ProLAN-verkko on esitetty liitteessä 4. [19]

ProLAN-kehityshankkeen suunnittelu käynnistettiin vuonna 2006, jolloin tiedostettiin kasvavat tarpeet uudenlaiselle verkkoympäristölle. Monien olemassa olevien prosessijärjestelmien elinkaaret olivat siinä vaiheessa, että uusia järjestelmäpäivityksiä olisi edessä lähivuosien aikana. Kehityshankkeen tuloksena syntyi malli kahdesta erillisestä, toisiaan varmentavasta, topologialtaan rengasmaisesta IP-verkosta, jotka

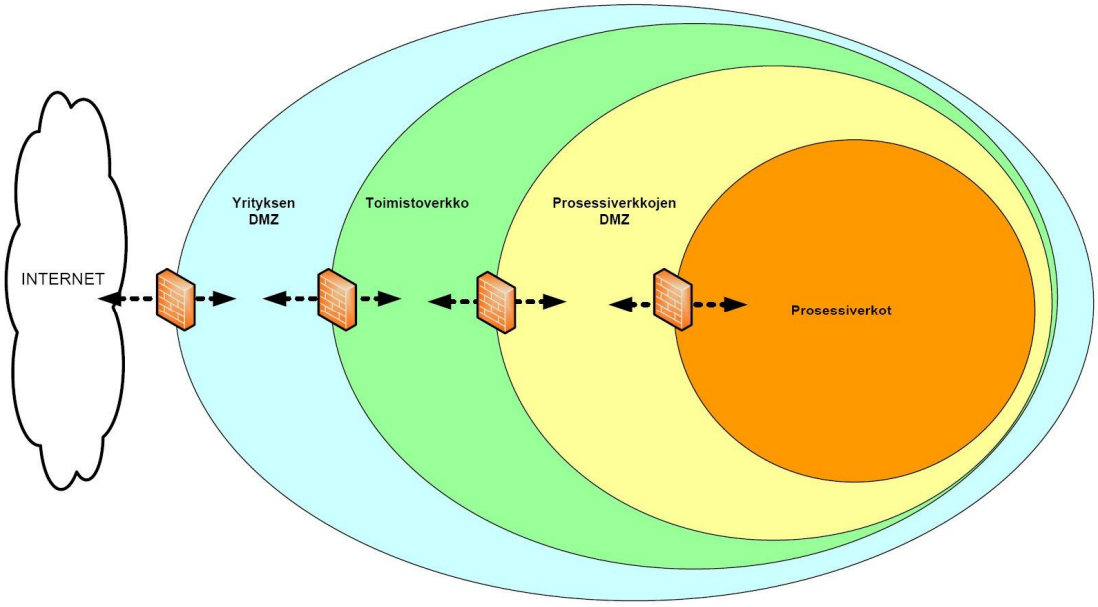
muodostavat ProLAN-verkon rungon. Eri asiakkaiden, järjestelmien tai järjestelmien eri toimintojen välinen liikenne erotetaan toisistaan VLAN-tekniikalla. Tätä hanketta lähdettiin viemään eteenpäin ja investointiprojekti ProLAN-verkon rakentamiseksi alkoi 2007. ProLAN-verkon verkkoarkkitehtuuri on esitetty kuvassa 17. [19] [15]



Kuva 17. ProLAN-verkkoarkkitehtuuri [15]

ProLAN-verkosta on tehty kaksi diplomityötä: Jukka Ristiniemen vuonna 2007 valmistunut ”Suunnitelma Ethernet-pohjaisen TCP/IP-verkon toteuttamiseksi prosessitietoliikenteen tarpeisiin Helsingin Energiassa” (Lappeenranta) ja Mikko Takalan vuonna 2012 valmistunut ”Tuotantokriittisen prosessiverkkoympäristön valvonta” (Aalto-yliopisto).

Verkon tietoturva on pyritty pitämään korkealla tasolla. Verkossa käytetään sotilasterminologiasta nimensä saanutta syvyyssuuntaista suojausta (Defence-in-Depth), jonka periaate on kuvattu kuvassa 18. Tässä turvallisuuden varmistaminen ei ole ainoastaan yhden suojauksen varassa, vaan suojattava alue on jaettu vyöhykkeisiin, joiden välissä käytetään erilaisia tietoturvamekanismeja. Ideana on se, että jos yksi kerros onnistutaan murtamaan, pitävät seuraavat vyöhykkeet vielä kriittisen toiminnan pystyssä. [15] [19]



Kuva 18. Syvyyssuuntaisen suojauksen periaate. [15]

ProLAN-palvelukokonaisuudelle on tehty oma politiikka, jossa on määritelty mm. menetelmät, joilla verkkoon voidaan liittyä, auditointikäytännöt ja eri osa-alueiden vastuuhenkilöt. Politiikassa on määritelty mm. seuraavanlaisia asioita:

- Kaikki laitekaapit on lukittu, lukot omalla sarjalla.
- Liikennöinti verkon ulkopuolelle on toteutettu palomuureilla.
- Käyttäjien tunnistamiseen käytetään vahvoja käyttäjäntunnistusmekanismeja.
- Verkkoon ei sallita suoria yhteyksiä ulkopuolelta.
- Sähkönsyötöt on kahdennettu. Sähkönsyötöt on toteutettu sähköasemien ja voimalaitosten UPS-laitteilta tai käyttämällä kaappikohtaisia UPS-laitteta, 2 kpl per kaappi.

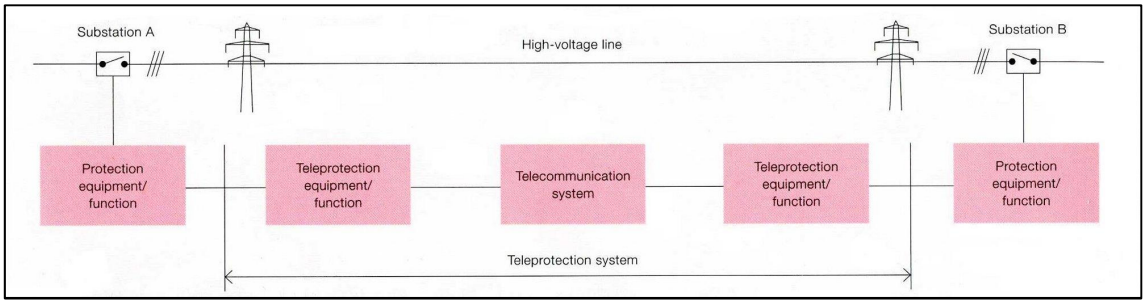
7 Sähkön siirtoverkon suojaus

Sähköverkon suojauksen tarkoituksena on havaita viat siirtoverkossa ja erottaa siirtoverkon viallinen osa muusta verkosta selektiivisesti nopeasti ja luotettavasti. Tähän päästään käyttämällä kahta tai useampaa laitetta, jotka voivat kommunikoida keskenään. Korkeilla jännitetasoilla vian havaitseminen ja virtapiirin erottaminen pitäisi ideaalitapauksessa tapahtua alle yhden aikajakson, joka tarkoittaa 50 Hz järjestelmässä alle 20 ms toiminta-aikaa. Käytännössä kuitenkin katkaisijoiden

toiminta-aika on noin 40-60 ms, minkä vuoksi vian erottamista ei pystytä tekemään alle 20 ms:ssa, vaikka suojarele voikin havahtua ja toimia tuossa ajassa. Siirtoverkkojen suojauksen kokonaistoiminta-aikatavoite on 100 ms. Suojausviestiyhteydessä ei sallita katkoksia tai muutoksia johdon ollessa käytössä. [20] [3]

Nykyisin sähkön siirtoverkon suojaus on riippuvainen tiedonsiirtoverkon ominaisuuksista. Odottamattomat muutokset tiedonsiirtoverkossa saattavat aiheuttaa vikalaukaisun suojausjärjestelmässä, mikä ääritapauksissa voi johtaa laajoihin sähkökatkoihin, turvallisuusongelmiin ja taloudellisiin menetyksiin. [20]

Tyypillinen korkeajännitejohdon suojausjärjestelmä (kuva 19) koostuu kolmesta pääkomponentista: suojareleestä, kaukosuojauslaitteesta (teleprotection) ja tiedonsiirtojärjestelmästä. Kaukosuojauslaite toimii fyysisenä liitäntänä suojareleen ja tiedonsiirtojärjestelmän välillä. [21] Kaukosuojauslaite voi olla erillinen laite tai integroitu suojareleeseen.



Kuva 19. Tyypillinen korkeajännitejohdon suojausjärjestelmä. [21]

7.1 Tiedonsiirtojärjestelmien vaatimukset sähköverkon suojauksessa

Eri suojaustekniikoilla on erilaiset vaatimukset tiedonsiirtojärjestelmille. Jotkut tekniikat käyttävät ”käsky”-tietoa (ON/OFF-tieto), toiset tarvitsevat jatkuvan datavirran, jossa siirretään voimajärjestelmän mittaustietoja releeltä toiselle ja näiden avulla analysoidaan johdon tilaa. Käytännössä suojausyhteys voidaan toteuttaa kuparikaapelilla, voimajohdoilla (PLC-tekniikka), erilaisilla siirtojärjestelmillä (PDH/SDH), radiolinkeillä tai suoralla valokuituyhteydellä. Yhteys voi olla toteutettu omassa verkossa, jolloin yhteys on omassa hallinnassa tai se voidaan vuokrata operaattorilta. Tiedonsiirtoverkon parametrit kuten viive, viiveen vaihtelu, siirtovirheet,

saatavuus ym. voivat kasvattaa suojauslaitteiden toiminta-aikoja tai jopa estää niiden toiminnan. [20] [22]

7.2 Tiedonsiirtojärjestelmien ongelmia

Tiedonsiirtojärjestelmän virheiden vaikutusta suojauksen toimintakykyyn voidaan tarkastella taulukon 3 avulla. Ongelmien aiheuttajat on listattu alla.

.

Taulukko 3. Tiedonsiirtojärjestelmän vikojen vaikutus suojaukseen. [20]

	Vika suojatulla alueella	Vika suojatun alueen ulkopuolella	Ei vikaa
Vika havaittu	Oikea toiminta	C1 - Väärät asetukset C2 - Väärä suojaus C3 - EMC ongelmat, liittimet & kaapelit	B1 - Ajan epäjohdonmukaisuus B2 - Muut virheet
Vikaa ei havaittu	A1 - Datan eheys A2 - Yhteysvika	Oikea toiminta	Oikea toiminta

A1: Datan eheys – Suojauslaite vastaanottaa virheellistä dataa.
A2: Yhteysvika – Tiedonsiirtoyhteys vialla

B1: Ajan epäjohdonmukaisuus – Eri aikaan otettujen näytteiden vertailu, esim. differentiaalisuojauksessa tulkitaan väärästä kohtaa otettua näytettä.
B2: Muut virheet – Väärä data tulkittu käskyksi tai mittausarvoksi ym.

Muut suojausjärjestelmän viat, jotka eivät johdu tiedonsiirrosta:
C1: Väärät asettelut, esim. suojaus aseteltu liian herkäksi
C2: Väärän tyyppinen suojaus
C3: Asennuksesta johtuvat virheet, esim. elektromagneettiset häiriöt

7.2.1 Signaalin kulkuaikaviive ja viiveen vaihtelu

Signaalin kulkuaikaviive kasvattaa laukaisuaikoja. Viiveen vaihtelu vaikuttaa joihinkin nykyisiin differentiaalireleisiin, jotka vaativat vakion siirtoviiveen kellojen synkronointiin. Mikäli nämä releet havaitsevat viiveen vaihtelun siirtotiellä, synkronointi lukitaan, kunnes viive taas palaa vakioksi. Toiminnan tarkoituksena on pitää siirtoviiveen mittaus luotettavana ja suodattaa esim. siirtotien uudelleenkytkennän (esim. SDH-verkko)

aiheuttamat transientit pois. Vaikka kellojen synkronointi lukitaan, voivat releet toimia jonkin aikaa normaalisti. Jotkut releet mittaavat synkronointiprosessin aikana kellojen tarkkuutta toisiinsa nähden, ja tätä tietoa voidaan käyttää pidentämään aikaa, jolloin releiden synkronointi on lukittu. Mikäli signaalin siirtoviiveen vaihteluita tapahtuu usein, voi synkronointiprosessi keskeytyä pitkäksikin ajaksi ja aiheuttaa suojien lukittumisen. [20]

7.2.2 Epäsymmetrinen viive

SDH-siirtoverkossa käytetään itsestään toipuvia rengasmaisia verkkoarkkitehtuureita. Näissä liikenne siirtyy toiselle reitille, mikäli jokin laite tai siirtotie vioittuu. Reitinvaihto voi olla joko yksisuuntainen, jolloin ainoastaan vioittunut reitti korvataan uudella ja vioittumaton reitti jää ennalleen, tai vaihto voi olla kaksisuuntainen, jolloin sekä lähetys- että vastaanottosuunta siirretään uudelle reitille riippumatta siitä, onko ainoastaan toinen siirtosuunta vialla. Yksisuuntainen reitinvaihto saattaa aiheuttaa siirtotielle epäsymmetrisen viiveen. Differentiaalireleiden kellojen synkronointi tehdään tiedonsiirtoyhteyden läpi, olettaen että lähetys- ja vastaanottoviive ovat samansuuruisia (kulkuaikaviive lasketaan jakamalla signaalin meno-paluuaika kahdella). Epäsymmetria meno- ja paluureittien viiveissä aiheuttaa virheen kellojen synkronointiin, joka taas tulkitaan vaiheensiirtona paikallisen ja etäpään virtojen välillä. Tämä vaiheensiirto jäljittelee virtojen eroa, joka taas saattaa aiheuttaa releiden laukaisun. [20]

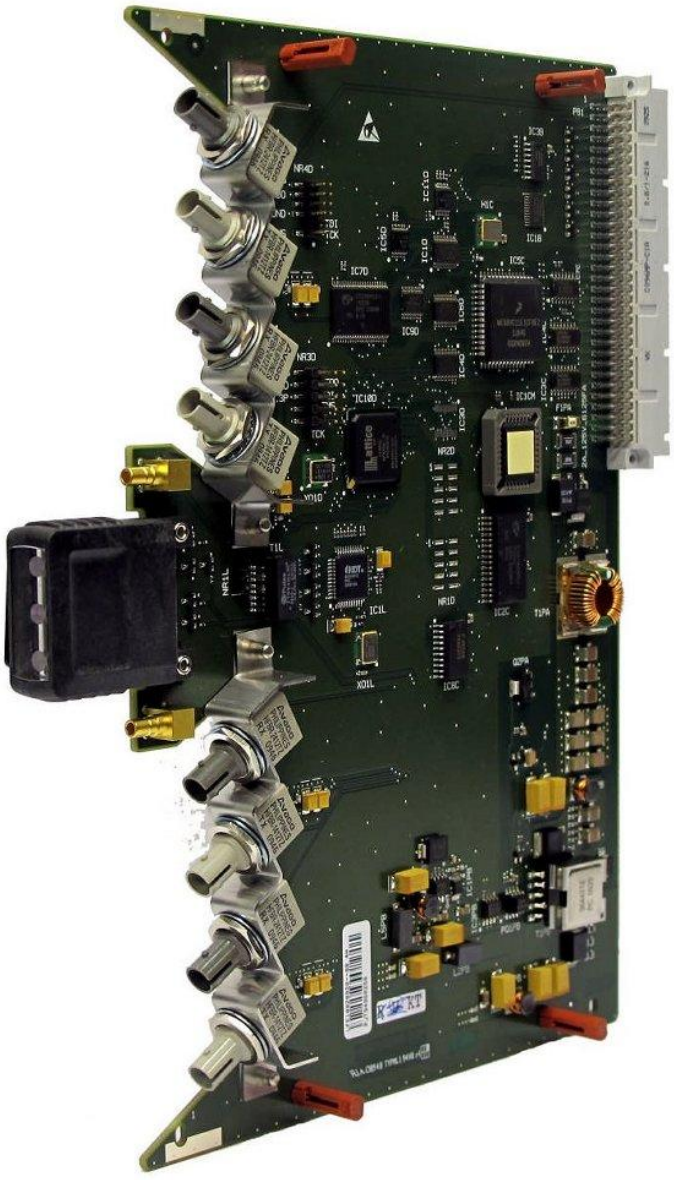
7.3 Suojareleiden liitännät

Nykyiset differentiaalireleet on yleensä varustettu kuituliitännöillä, joilla releet on tarkoitettu liitettäväksi toisiinsa suoralla valokuituyhteydellä. Yleensä tämä kuituliitäntä on valmistajakohtainen, jolloin relettä ei voi kytkeä suoraan mihinkään siirtojärjestelmään. Mikäli näin halutaan tehdä, tarvitaan valmistajakohtainen sovitin, jolla optinen signaali muutetaan siirtojärjestelmälle sopivaksi standardoiduksi liitännäksi, esim. vastasuuntaiseksi 64 kbit/s G.703-, V.28/V.24- tai E1-liitännäksi.

Vuonna 2002 on standardoitu suojareleiden optinen liitäntä IEEE C37.94. Standardi määrittelee suojareleen ja digitaalisen multiplekserin (esim. Nokia DM2) välisen optisen Nx64 kbit/s rajapinnan, jossa N=1-12, eli 64-768 kbit/s. Standardi mahdollistaa eri valmistajien suojareleiden liittämisen suoraan siirtojärjestelmän multiplekserin C37.94-

kanavakorttiin 50 tai 62,5 mikrometrin monimuotokuidulla, kuituyhteyden maksimipituus on 2 km. Näin ollen ei tarvita erillistä laitetta optisen signaalin muuttamiseksi sähköiseksi. [23]

Nokia Siemens Networksin DM2-multiplekseriin on saatavilla TPSO-kanavakortti (kuva 20) jossa on 4 kpl optisia C37.94-liitäntöjä. [24]



Kuva 20. TPSO-kanavakortti [24]

7.4 Yleiset siirtoverkon suojausperiaatteet

7.4.1 Distanssisuojaus

Distanssireleiden toiminta perustuu impedanssin laskemiseen mitattujen virtojen ja jännitteiden perusteella. Virran ja jännitteen perusteella rele pystyy määrittämään vian suunnan ja etäisyyden mittauspisteestä, jolloin voidaan toteuttaa silmukoidussa verkossa selektiivinen suojaus. Distanssireleelle asetellaan ns. vyöhykkeet, joille määritellään ulottuma ja aikahidastus. Eri asemilla sijaitsevien distanssireleiden vyöhykkeet menevät osittain päällekkäin, jolloin ne toimivat myös toistensa varasuojina. [25]

Distanssireleillä viestiyhteys ei ole välttämätön, mutta sen avulla voidaan kauempana vikapaikasta olevan releen toimintaa nopeuttaa ja estää virhelaukaisuja. Kun suojausalueen toisessa päässä oleva rele havahtuu ja lähettää tästä signaalin, osaa oikea rele silloin laukaista nopeammin. Distanssisuojauksen apuyhteydellä voidaan käyttää kahta eri viestitapaa, laukaisun vapauttavaa ja laukaisun lukitsevaa. HSV:llä käytetään vapauttavaa periaatetta. [26] [3]

Laukaisun vapauttavassa tapauksessa rele toimii vian sattuessa lähellä johdon toista päätä vain, jos kaukosuojauskäsky vastaanotetaan. Käskyn tarkoituksena on tällöin vahvistaa, että vika todella sijaitsee suojattavalla johdolla. Laukaisun lukitsevassa tapauksessa rele toimii vastaavasti vain kaukosuojauskäskyn puuttuessa. Tässä tapauksessa kaukosuojauskäsky lähetetään, jos vika sijaitsee suojattavan johdon ulkopuolella ja sitä käytetään siksi releen toiminnan estämiseksi. Laukaisun lukitsevissa sovelluksissa vaaditaan korkeaa luotettavuutta eli alhaista käskyn estymisen todennäköisyyttä. [27]

7.4.2 Differentiaalisuojaus

Differentiaalisuojausta voidaan soveltaa kaikkien verkon osien eli muuntajien, koneiden, kiskostojen sekä johtojen suojaukseen. Differentiaalisuoja vertaa suojattavan kohteen tulevia vaihevirtoja siitä lähteviin. Jos nämä virrat poikkeavat toisistaan joko amplitudin tai vaihekulman tai näiden molempien suhteen enemmän kuin suojaan aseteltujen arvojen verran, seuraa laukaisu. Mittausperiaatteen ansiosta suojaus toimii ainoastaan suojausalueella tapahtuvissa vioissa, jolloin suojaus on absoluuttisesti

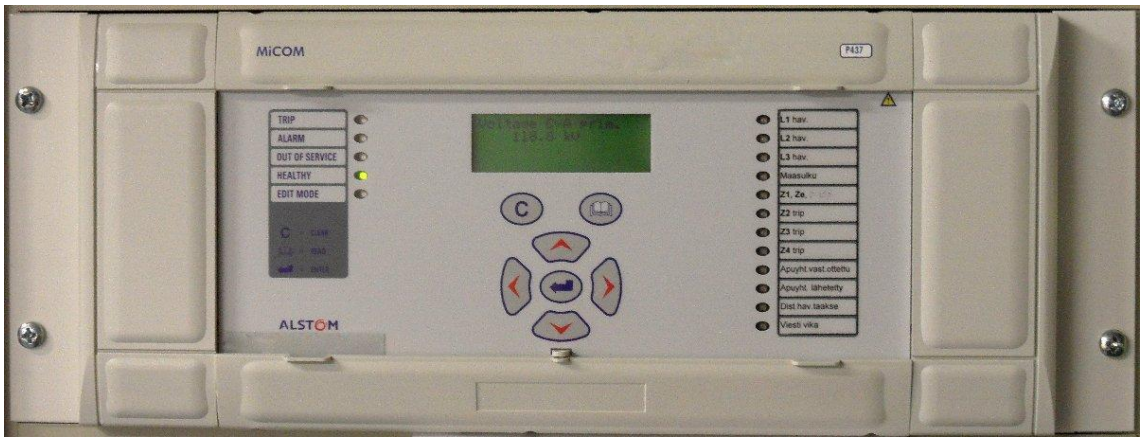
selektiivinen. Tästä syystä releen toimintanopeus on erittäin hyvä, jopa alle puolijakson, käytännössä ei kuitenkaan päästä näin nopeaan toiminta-aikaan. Suojausalue muodostuu virranmittauspaikkojen väliin jäävästä alueesta. Toinen mittausperiaatteen tuoma etu on suuri herkkyys: suojaus voi toimia jopa muutaman prosentin nimellisvirrasta olevilla vikavirroilla. Saavutettava herkkyys riippuu toimintanopeuden tavoin käytetystä releтyypistä, virtamuuntajien ominaisuuksista sekä suojattavasta kohteesta. [28]

7.5 Releteknikka

Releteknikka on muuttunut suuresti viimeisen 30 vuoden aikana. Elektromekaaniset releet kaikissa muodoissaan on korvattu lähes täysin staattisilla, digitaalisilla ja numeerisilla releillä, releet ovat pienentyneet ja niiden ominaisuudet ovat lisääntyneet, analogiatekniikka on korvattu digitaalitekniikalla. Samalla releiden luotettavuus on pysynyt samalla tasolla tai jopa parantunut, myös käytettävyys on parantunut huomattavasti uuden tekniikan myötä. Kuvassa 21 on Alstomin valmistama numeerinen distanssirele MiCOM ja kuvassa 22. Siemensin numeerinen differentiaalirele SIPROTEC 7SD5. [22]

Nykyisin kaikki uudet suojareleet ovat numeerisia releitä. Numeerisissa releissä käytetään tähän tarkoitukseen kehitettyjä digitaalisia signaaliprosessoreja (DSP), joilla sisään tulevat analogiset signaalit muutetaan digitaalisiksi ja toteutetaan varsinaiset mittaus- ja suojaustoiminnot. Numeeristen releiden toimintatarkkuus ja pitkän ajan stabiilisuus ovat erittäin hyviä. Numeeristen releiden asetusarvot ovat hyvin monipuoliset, ja releiden sisältämien loogisten toimintojen avulla rele voidaan sopeuttaa erilaisiin käyttötilanteisiin. Numeeristen releiden hyvänä puolena voidaan pitää myös integroituja häiriö- ja tapahtumantallennusominaisuuksia, jotka auttavat häiriötilanteiden jälkiselvityksessä. [3]

Suojausteknisesti numeeristen releiden merkittävin ominaisuus on itsevalvonta, mikä lisää oleellisesti suojauksen luotettavuutta. Aiheettomien toimintojen todennäköisyys pienenee, sillä itsevalvonta estää viallisen releen toiminnan. Itsevalvonta indikoi myös viallisen yksikön, jolloin releen toimintakuntoon saattaminen nopeutuu. [22] [29]



Kuva 21. Numeerinen Distanssirele Alstom MiCOM.

Kuva 22. Numeerinen differentiaalirele Siemens SIPROTEC 7SD5

7.6 Siirtojohtojen suojaus HSV:ssä

110 kV siirtojohdot on koko verkossa suojattu kahdella eri suojalla. Pääsuojauksena käytetään differentiaalisuojausta tai vertosuojausta ja varasuojina distanssisuojausta. Avojohdoilla on lisäksi varalla herkkä maasulun suuntasuojaus. [3]

Differentiaalireleiden välinen viestiyhteys on toteutettu suorilla valokuituyhteyksillä tai PCM-verkossa, joko sarjaliikenteellä tai äänikanavassa (vanhemmat releet).

Distanssireleiden välinen tiedonsiirtokytkintieto on toteutettu kuparikaapelilla tai PCM-verkon avulla, joko äänikanavissa tai TPS64-kaukosuojauslaitteilla.

Perustoteutusperiaatteena uusilla suojausyhteyksillä on ollut toteuttaa differentiaalisuojauksen yhteydet suorilla valokuiduilla ja distanssisuojien yhteydet kuparikaapelilla ja mahdollisuuksien mukaan vielä eri reiteille. Tällä tavoin on varmistettu, että suojausyhteydet kulkevat eri kaapeleissa eikä näin ollen yhden kaapelin vioittuminen ole estänyt suojien toimintaa. Käytännössä kuitenkin kuparikaapeliyhteydet tulevat monesti liian pitkiksi suojareleille, joten tätä mallia ei voida joka paikassa toteuttaa. Pitkillä distanssisuojayhteyksillä tai kohteissa, joissa ei ole käytettävissä kuparikaapeleita, on käytetty TPS64-kaukosuojauslaitteita ja siirtotienä PCM-verkkoa.

Vanhoilla suojausyhteyksillä on käytössä vaihtelevasti PCM-ääni- ja datakanavia sekä kuparikaapeliyhteyksiä. Näissä on pyritty myös käyttämään eri reittejä pää- ja varasuojauksen yhteyksillä silloin, kun se on mahdollista. Näiden vanhojen suojausyhteyksien periaate on tarkoitus yhdenmukaistaa releuusintojen yhteydessä.

7.7 Suojausyhteyksien kehitysnäkymät HSV:ssä

Kuten edellisessä kappaleessa mainittiin, HSV:ssä on ollut periaatteena, että ensimmäinen pääsuojaus (differentiaalisuojaus) toteutetaan suorilla valokuituyhteyksillä ja toinen pääsuoja (distanssisuojaus) kuparikaapeliyhteyksillä. Nämä kaksi toisiaan varmentavaa suojausyhteyttä pyritään mahdollisuuksien mukaan sijoittamaan fyysisesti eri reiteille. Tällöin yhden kaapelin vioittuminen tai laitevika ei katkaise molempia yhteyksiä. [30]

7.7.1 Differentiaalisuojaus

Kaikki uudet ja uusittavat differentiaalisuojien viestiyhteydet toteutetaan suorilla valokuiduilla. Differentiaalisuojien yhteydet reititetään mahdollisimman lyhyttä reittiä pitkin ja kuitujen ristikytkentäpaikat pyritään minimoimaan. Differentiaalisuojien kuituyhteydet pyritään siis hitsaamaan päästä päähän, jolloin voidaan minimoida reitillä olevien liitosten määrä ja samalla minimoidaan riski mahdollisista käytön aikaisista virhekytkennöistä kuituverkossa. Differentiaalisuojille varataan aina oma kuitu/kuitupari

koko matkalla, eikä yhteydellä käytetä esim. aallonpituusmultipleksointia (WDM). Releissä käytettävät kuitumoduulit on valittava niin, ettei välivahvistimia tarvita.

Digitaalisessa siirtoverkossa on tarkoitus korvata keskeisimmissä ristikytkentäpaikoissa vanhat PDH-siirtolaitteet renkaaseen kytketyillä SDH-laitteilla. Tämä parantaa verkon luotettavuutta automaattisen uudelleenreititysominaisuutensa ansiosta. Reitin pituuden muuttuminen vikatilanteessa vaikuttaa kuitenkin yhteyden kulkuaikaviiveeseen, ja tämä aiheuttaa ongelmia sellaisille differentiaalisuojille, jotka liikennöivät sarjaliikenteellä digitaalisen siirtoverkon läpi. Kulkuaikaviive on aseteltu kiinteästi releen parametreihin, ja jos viive muuttuu, rele ei välttämättä enää toimi niin kuin on suunniteltu. Näin ollen on varmistettava, että kyseisenlaisia yhteyksiä ei ole SDH-renkaaseen liitetyissä laitteissa. Vanhempiin äänikanavassa liikennöiviin differentiaalisuojiin ja distanssisuojiin ei siirtojärjestelmän laitetyypin vaihdolla ole merkitystä.

SDH-laitteissa on myös ominaisuus, jolla vikatilanteessa ainoastaan vioittunut liikennesuunta käännetään varareitille. Tämä aiheuttaa epäsymmetrisen kulkuaikaviiveen, joka myös häiritsee suojausyhteyksien toimintaa. Laitteet on siis parametroitava niin, että vian sattuessa yhteyden kumpikin suunta käännetään varareitille, vaikka vain toinen suunta olisi vioittunut. Yhteyden uudelleenreititys on myös aseteltava niin, ettei reittiä palauteta automaattisesti primäärireitille yhteyden palautuessa kuntoon. Tämä saattaa aiheuttaa yhteyden turhaa pätkimistä, mikäli primääriyhteyden vika on sen luontoinen, että se välillä palaa toimintaan ja on välillä poikki.

7.7.2 Distanssisuojaus

Käytäntö on osoittanut, että käytettäessä kuparikaapeliyhteyksiä muodostuvat matkat monessa tapauksessa ongelmaksi. Nykyiset distanssisuojissa käytetyt kuparikaapelimuuntimet toimivat max. 8 km yhteydellä ja varsinkin tavoiteltaessa reittivarmennusta matka monesti ylittyy. Vaihtoehtona on luopua reittivarmennuksesta tai sijoittaa yhteysvälille toistin. Kumpikin vaihtoehto on huono ajatellen yhteyden kriittisyyttä. Vaihtoehtona on käyttää siirtotienä esim. PCM-verkkoa ja TPS64-kaukosuojauslaitteita tai suoria valokuituyhteyksiä myös distanssisuojauksessa. Kummallakin vaihtoehdolla voidaan eliminoida etäisyydestä aiheutuvat ongelmat.

Helenillä käytössä oleva PCM-siirtoverkko alkaa olla käyttöikänsä loppupuolella, ja sen varaosien toimitus loppuu vuoden 2014 aikana. Näin ollen uusia suojausyhteyksiä ei kannata enää rakentaa PCM-järjestelmän päälle. Nykyiset jo käytössä olevat PCM-yhteydet saadaan pidettyä toiminnassa käyttöikänsä loppuun hankkimalla riittävästi varaosia varastoon. PCM-siirtoverkon elinkaarta voidaan jatkaa myös australialaisen Avara Technologies-nimisen valmistajan laitteilla. Avara on toiminut aiemmin Nokia Siemens Networksin (NSN) alihankkijana ja valmistanut joitain Dynanet-tuotteita ja jatkaa edelleen näiden valmistamista ja kehittämistä, vaikka NSN lopettaa kyseisen tuoteperheen. Avaran verkkoratkaisut ovat osittain yhteensopivia vanhojen Dynanet-tuotteiden kanssa. Runkoverkon tiedonsiirtotekniikkana on Ethernet perinteisten PDH- ja SDH-tekniikoiden sijaan. [31] [32]

Käytettäessä suoria valokuituyhteyksiä myös toisella pääsuojalla ongelmaksi muodostuu joissain tapauksissa kuituverkon kapasiteetti. Tietyillä väleillä valokuituverkossa on käytettävissä ainoastaan 4-8 kuitua, ja näihin on jo kytketty differentiaalisuojien tarvitsemat kuituyhteydet sekä kaukokäyttöjen tarvitsemat PCM- ja ProLAN-yhteydet, eli ylimääräistä kapasiteettia ei ole. Tällä hetkellä ahtailla kuituväleillä on käytössä CWDM-multipleksereitä, joilla kuidun kapasiteettia voidaan kasvattaa. Nämä käytössä olevat passiiviset laitteet vaatisivat kuitenkin releisiin tietyllä aallonpituudella olevat kuitumodulit. Tiedusteltaessa relevalmistajilta (Siemens, ABB ja Schneider Electric) sopivia CWDM-kuitumoduleita ilmeni, että näitä ei juurikaan ole saatavilla. Siemensin uusimpiin releisiin on saatavana WDM-tekniikkaan perustuvia (lähetys ja vastaanotto eri aallonpituudella) yksikuituisia moduuleita, mutta näitä ei voi käyttää CWDM multipleksereiden kanssa. [33] [34]

Kuituverkkoa rakennetaan koko ajan lisää mm. 110 kV kaapelitöiden yhteydessä ja uusimalla nykyisiä valokuitu-ukkosköysiä. Näin ollen kuituverkon kapasiteettiongelmat poistuvat jollakin aikajänteellä. Uusimman sähköasemaspesifikaation mukaan uusille sähköasemille ei enää vedetä kupariviestikaapelointia, vaan kaksi kuitukaapelia. Kuitukaapelit sijoitetaan 110 kV johtoreitin eri puolille, jolloin kaapeleiden samanaikainen vaurioitumistodennäköisyys pienenee. Valokuidun käyttöä voidaan perustella myös seuraavan vertailun avulla.

Valokuitu:

+ immuuni häiriöille
+ pitkät siirtoetäisyydet
+ kaapelin hinta
+ kuitupäätelaitteiden hinta laskenut ja tarjonta parantunut
- kaapelin päättäminen ja jatkaminen kallista

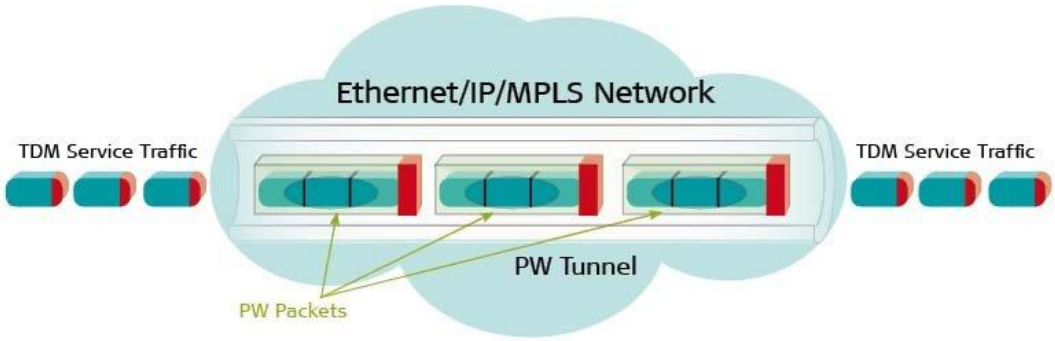
Kuparikaapeli:

+ kaapelin päättäminen ja jatkaminen edullista
- rajoitettu siirtoetäisyys
- kaapelin hinta
- häiriöherkkä

7.7.3 IP-verkko suojausyhteyksillä

IP-verkot ovat viime vuosina kehittyneet rajusti ja ne ovat syrjäyttämässä ja osittain jo syrjäyttäneet perinteiset siirtojärjestelmät kuten SDH- ja PDH-järjestelmät. Tämän vuoksi on alettu tutkia, miten IP-verkkoa voitaisiin käyttää suojausyhteyksillä. Perinteisen IP-verkon perusominaisuudet asettavat suuria haasteita suojausyhteyksille. Suojausyhteydet vaativat nopeaa ja luotettavaa tiedonsiirtoa, symmetristä kulkuaikaviivettä (kts. luku 7.2.2.) ja pientä viiveen vaihtelua (jitter). Mikään näistä ei ole ominaista perinteiselle IP-verkolle. Nykytekniikka tarjoaa kuitenkin erilaisia mekanismeja, joilla nämä tekijät voidaan ohittaa. [35]

Nykyisin tyypillisin tapa siirtää aikajakoisia piirikytkettyjä yhteyksiä (kuten suojausyhteydet SDH- tai PDH-verkon päällä) IP-verkon yli on käyttää eräänlaista keinojohto- emulointia (engl. pseudowire emulation, PWE). Tämä on menetelmä, jolla rakennetaan suora yhteys kahden laitteen välille luomalla looginen linkki tai tunneli IP-verkon yli. Tässä tekniikassa siirrettävä datavirta paketoidaan lähtöpäässä ja lähetetään luotua tunnelia pitkin kohdepäähän, jossa paketit puretaan ja liikenne synkronoidaan uudelleen (kuva 23.). Synkronointitiedon siirtämiseen käytetään PWE-tekniikan ominaisuuksia. Näin syntyy reaaliaikainen läpinäkyvä yhteys IP-verkon yli. [35]



Kuva 23. Keinojohtoemuloinnin periaate [35]

Tyypillisiä PWE-tekniikoita ovat:

- SAToP Structure Agnostic TDM over Packet
- CESoPSN Circuit Emulation over PSN
- TDMoIP TDM over IP [35]

Kehitteillä on myös tapoja, jolla liikenne saadaan ohjattua suoraan IP-verkon yli haluttua reittiä pitkin. Tällöin ei tarvita erillistä laitteita yhteyden emulointiin. [35]

IP-verkon käyttäminen HSV:llä suojausyhteyksiin ei ole järkevää, koska käytössä on lähes kaikki sähköasemat käsittävä kuituverkko ja toimitaan maantieteellisesti suhteellisen pienellä alueella. IP-verkon käyttöön ei siis ole taloudellisia eikä teknisiä perusteita.

IEC 61850 -protokollaan ollaan kehittämässä ominaisuuksia, joilla releiden välinen suojausyhteys voitaisiin toteuttaa IP-verkossa. Tämä standardoitu rajapinta mahdollistaisi tulevaisuudessa eri valmistajien releiden käytön suojattavan johdon eri päissä. Tämä ei kuitenkaan ole vielä valmis ratkaisu, ja vie vuosia, ennen kuin järjestelmä on otettavissa tuotantokäyttöön. Toteutusmalli asettaa myös tietoliikenneverkolle suuria haasteita. [36]

IEC 61850 -protokolla on kansainvälinen standardi Tietoliikenneverkot ja -järjestelmät sähköasemalla (Communication networks and systems in substations). Sen tavoitteena on päästä eroon valmistajakohtaisista ratkaisuista ja ylimääräisistä muunnoksista eri protokollien välillä. Standardissa on pyritty erottamaan tietojen ja palveluiden käsittely

käytettävästä tiedonsiirtotavasta, jolloin standardia on mahdollista käyttää myös tulevaisuudessa kehitettävien tiedonsiirtotapojen yhteydessä. Tällä hetkellä IEC 61850:n tiedonsiirto perustuu Ethernet-tekniikkaan. IEC 61850 -protokolla on käytössä sähköaseman sisäisessä liikenteessä, mutta sitä ollaan kehittämässä kattamaan myös sähköasemien välistä liikennettä. [25]

8 Kaukokäyttöyhteydet

8.1 Yleistä kaukokäytöistä

Suomessa sähköasemat ovat olleet jo pitkään miehittämättömiä, kaukovalvottuja ja kauko-ohjattuja järjestelmiä. Sähkön siirto- ja jakeluverkot ovat jakautuneet laajalle alueelle. Valvomalla ja ohjaamalla verkkoja keskitetysti voidaan parantaa sekä verkon ja sen käytön teknistä laatutasoa, esim. toimintavarmuutta ja häiriöiden lyhytaikaisuutta, henkilöstömenojen säästämiseksi. Tällaisesta keskitetystä ja osin automaattisesta ohjauksesta ja valvonnasta käytetään nimitystä kaukokäyttö. Siihen liittyy usein muitakin tehtäviä, kuten tietojen tallennusta, laskentaa ja raportointia. [37]

Verkon käytön tehtävänä on hallita energian siirtoprosessia suorien valvonta- ja ohjaustoimenpiteiden avulla. Tämä tarkoittaa tuotetun ja kulutetun sähkön tasapainon ylläpitämistä sekä sähkön siirron ohjaamista mahdollisimman käyttövarmasti ja taloudellisesti. Tämä vaatii verkon tietojen keräämistä, prosessointia ja tietojen vaihtoa muiden yhtiöiden ja toimijoiden kanssa. Kerättävien ja siirrettävien tietojen määrä on suuri koostuen mm. jännitteistä verkon eri osissa, johtojen virroista ja tehoista sekä kytkinlaitteiden asennoista ja niissä tapahtuvista muutoksista. Tällaisesta laajasta tiedonkeruujärjestelmästä käytetään nimitystä SCADA-järjestelmä (Supervisory, Control and Data Acquisition System). [37]

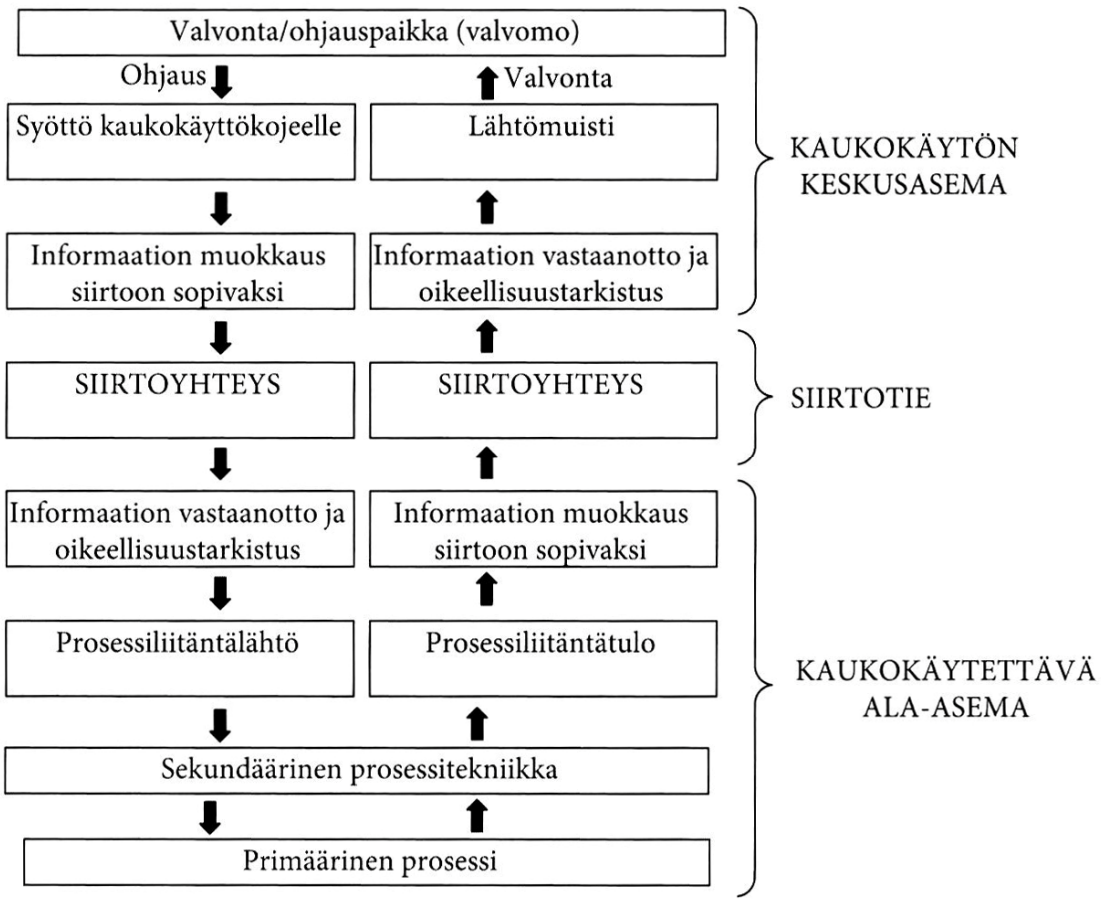
Alkuvaiheessa kaikki valvonta- ja ohjausjärjestelmät olivat langallisia kahden pisteen välisiä järjestelmiä. Tämä tarkoitti suurta toisiokaapeleiden määrää, sillä tietty mittaustieto saatettiin viedä esim. kymmeneen eri kohteeseen, kuhunkin omalla johdinparillaan. Tietotekniikan kehittyminen on tarjonnut mahdollisuuden rinnakkaisten johdinparien vähentämiseen kaukoyhteyksissä sekä asematasolla, jossa ala-aseman ja kenttätason välinen kuparikaapelointi on korvattu sarjaliikenne- ja Ethernet-pohjaisella

tiedonsiirrolla. Elektroniikan kehittyminen ja yleistymien yhdessä tiedon digitalisoinnin kanssa ovat radikaalisti muuttaneet ja edelleen muuttamassa sähkönsiirron ohjauksessa, säädössä ja valvonnassa käytettyjä ratkaisuja. [37] [3]

8.2 Kaukokäyttöjärjestelmät

Kaukokäyttöjärjestelmän periaatteellinen toimintakaavio on esitetty kuvassa 24. Valvottavaa prosessia koskevat tiedot kerätään digitaalisina- tai analogisina viesteinä kaukokäyttölaitteelle. Kaukokäyttölaitteessa suoritetaan esim. näytteenotto, signaalin valinta ja kanavointi, koodaus sekä osoitteenmuodostus, minkä jälkeen muodostettu sanoma muunnetaan siirtoon sopivaksi. Informaatio siirretään edelleen siirtotien välityksellä valvomoon, jossa sanomalle suoritetaan dekoodaus ja virheentarkastus. Tämän jälkeen tiedot ovat käytettävissä jatkokäsittelyyn tai nähtävissä valvomon näyttölaitteilla.

Ohjaustilanteessa tapahtumat kulkevat samaan tapaan, mutta vastaavasti valvomosta prosessin suuntaan. [37]



Kuva 24. Kaukokäyttöjärjestelmän toimintakaavio [37]

Kaukokäyttöjärjestelmä toimii yleensä reaaliajassa, jolloin käyttäjä on jatkuvasti selvillä prosessin tilasta ja ohjauskäskyt menevät nopeasti ja luotettavasti perille. Tiedonsiirrolle ja kaukokäyttöjärjestelmien tietoliikenneohjelmille on asetettava suuret vaatimukset, jotta edellä mainitut tavoitteet saavutetaan. [37]

8.3 Kaukokäyttöjen liikennöintiprotokollat

Kaukokäyttöprotokollia käytetään pääsääntöisesti ala-aseman ja käytönvalvontajärjestelmän väliseen kommunikaatioon. Uudemmissa järjestelmissä käytetään IP-pohjaista tiedonsiirtoa ja vanhemmissa sarjaliikennettä. Vanhemmat sarjaliikenneprotokollat ovat monesti järjestelmätoimittajien itsensä kehittämiä. Standardointijärjestö IEC on luonut ja kehittää edelleen yhteisiä liikennöintiratkaisuja ja –malleja. Kaksi yleisesti käytössä olevaa liikennöintiprotokollaa ovat IEC 60870-5-101 ja IEC 60870-5-104. [38]

8.3.1 IEC 60870-5-101

IEC 60870-5-101-protokolla on suunniteltu sarjaliikenne-pohjaiseen kommunikointiin ala-aseman ja käytönvalvontajärjestelmän välillä. Fyysisellä kerroksella IEC 60870-5-101-protokolla tarjoaa ITU-T-standardin mukaisen rajapinnan, joka on yhteensopiva EIA-standardien RS-232 ja RS-485 kanssa. [38]

IEC 60870-5-101 -protokolla mahdollistaa kaksi erilaista kommunikointitapaa ala-aseman ja käytönvalvontajärjestelmän välillä. Protokollaa voidaan käyttää linkkikerroksella kahdessa eri siirtotilassa, balansoidussa ja balansoimattomassa. Balansoimattomassa tiedonsiirrossa master-asema eli käytönvalvontajärjestelmä kontrolloi viestiliikennettä pollaamalla ala-asemia kutakin vuorollaan. [38]

Balansoidussa tiedonsiirrossa jokainen ala-asema voi aloittaa liikennöinnin ilman erillistä kyselyä. Ala-asemat voivat siis liikennöidä samanaikaisesti toistensa kanssa. Balansoidusti toimivassa järjestelmässä tieto tapahtumasta siirtyy välittömästi, kun taas balansoimattomassa vasta seuraavan kyselyn yhteydessä. Balansoimaton järjestelmä on taas yksinkertaisempi toteuttaa ja hallita, koska käytönvalvontajärjestelmä voi vapaasti päättää, milloin ja miltä ala-asemalta tietoa pyydetään. [38]

8.3.2 IEC 60870-5-104

IEC 60870-5-104 on IP-verkoissa käytettävä käytönvalvontaprotokolla. Protokolla mahdollistaa pakettikytkentäisten TCP/IP-verkkojen käytön ala-aseman ja käytönvalvontajärjestelmän välillä. [38]

IEC 60870-5-101- ja IEC 60870-5-104 -protokollien toiminnallisuus sovelluskerroksella on lähes sama. Kyseiset protokollat jakavat saman tason ASDU-kehyksen (Application Service Data Unit) viestinnässä, mutta eroavat toisistaan linkkitasolla. Edellä mainittujen protokollien peruserona voidaan pitää sitä, miten ne käsittelevät tietoja ja tapahtumia. IEC 60870-5-104 -protokolla mahdollistaa tapahtumien lähettämisen symmetrisesti. Tämä tarkoittaa sitä, että ala-asemat pystyvät käsittelemään ja lähettämään samanaikaisesti tapahtumia ja pyyntöjä, kun käytönvalvontajärjestelmä suorittaa taustalla toimintaansa. [38]

IEC 60870-5-104 -protokollan suurimpana etuna voidaan pitää mahdollisuutta standardoidun verkon käyttöön, jonka kautta tiedonsiirto onnistuu useiden laitteiden ja palveluiden välillä. Tämän ansiosta saadaan tieto esim. hälytyksistä toimitettua nopeammin. [38]

8.4 Kaukokäytöt HSV:ssä

Sähköaseman ja käytönvalvontajärjestelmän (GE XA/21) välillä liikennöidään pääsääntöisesti IEC 60870-5-101 tai IEC-60870-5-104 -protokollalla, kahdella asemalla on vielä käytössä I33-protokolla. IEC-60870-5-101- ja I33-protokollaa käytettäessä liikennöintimuoto käytönvalvontajärjestelmän ja aseman kaukokäyttölaitteen välillä on sarjaliikennettä. IEC-60870-5-101 -protokollalla sarjaliikenteen nopeus on 9600 bit/s ja I33-asemilla 1200 bit/s. IEC-60870-5-104 -asemien liikenne on IP-pohjaista, ja kaukokäyttölaite on liitetty sähköasemalla olevaan ProLAN-kytkimeen 10 Mbit/s tai 100 Mbit/s Ethernet-liitynnällä.

Kummassakin tapauksessa kaukokäyttöyhteydet on kahdennettu. Sarjaliikenneasemilla kaukokäytön pääyhteys on toteutettu PCM-verkossa ja varayhteys kupariverkossa käyttäen sarjaliikennemodeemeita. IP-pohjainen liikenne on

kahdennettu ProLAN-verkossa niin, että kaukokäytön pääyhteys on kytketty ProLAN1-renkaaseen ja kaukokäytön varayhteys on kytketty ProLAN2-renkaaseen.

Käytännössä IEC 60870-5-104 -protokollalla toteutettujen asemien käyttöönotto ja järjestelmän muutokset ovat osoittautuneet hankalemmiksi verrattuna IEC 60870-5-101-protokolla toteutettuihin ala-asemiin. Johtuen lähinnä kaukokäyttöyhteyksillä käytettävästä IP-tekniikasta ala-asemille pitää määrittää IP-osoitteet ja muutoksissa näitä pitää joskus vaihtaa. IEC 60870-5-101 -protokollaa käytettäessä vastaavia toimenpiteitä ei tarvita. [36]

Näiden lisäksi on käytössä varakaukokäyttöyhteys, joka on tällä hetkellä toteutettu kupariverkossa käyttäen sarjaliikennemodeemeita. Uusilla ja uusituilla asemilla on käytössä myös kaukokäytön etäohjauspiste, joka käyttää siirtotienä ProLAN-verkkoa. [3]

Sähköaseman sisäinen liikenne on toteutettu uusilla ja uusituilla sähköasemilla IEC 61850 -standardin mukaisesti, tällä hetkellä näitä on 6 kpl, IEC 61850 -toteutuksia on tulossa lisää 1-2 kpl vuodessa. Käytössä on myös ILSA-, LON- ja IEC 60870-5-103-protokollia. [3]

8.5 Pääkaukokäyttöyhteyksien kehitysnäkymät HSV:ssä

Sähköasemien kaukokäyttöyhteyksiä siirretään IP-verkkoon IEC 60870-5-104 -protokollaan siirtymisen myötä sähköasemien saneerausten yhteydessä, näin ollen tarve sarjaliikenneyhteyksille vähenee ja päästään eroon vanhenevasta modeemikannasta ja PCM-yhteyksistä. Tämän hetkisen tiedon perusteella Nokia Siemens Networks lopettaa Dynanet-tuotteiden (Helenillä käytössä olevat PCM-laitteet) myynnin 2013 jouluna ja huollon 2016. Näin ollen on päätetty, ettei uusia sarjaliikenneyhteyksiä enää rakenneta PCM-järjestelmään. Siirtymäaikana tarvitaan kuitenkin myös sarjaliikenneyhteyksiä, ja luvussa 8.5.4 on esitelty käytönvalvontajärjestelmän uusinnan myötä käyttöönotettava ratkaisu. [31]

Tarpeet erilaisten automaatiolaitteiden turvalliseen liittämiseen IP-verkkoon ovat tuoneet markkinoille myös erilaisia sähköasemaympäristöön sopivia tietoliikenneratkaisuja. Seuraavassa on esitelty lyhyesti Helenillä kehitetyn ProLAN-

verkon kehitysnäkymiä sekä esitellään kahden eri kaupallisen valmistajan näkemys aiheesta.

8.5.1 ProLAN-verkko

IP-yhteyksien kehityksessä noudatetaan ProLAN-verkon kehityspolkua. ProLAN-verkon kehityksestä vastaa Helenin ICT-palvelut. ProLAN-verkon seuraavan kehitysversion rakentaminen on suunniteltu alkavan noin vuonna 2015, tekniikkana reitittävä L3- tai MPLS-tekniikka. MPLS on menetelmä, jolla kuljetetaan esimerkiksi IP-paketteja ennalta määriteltyjen reittien läpi nopean runkoverkon solmujen kautta ilman, että solmujen tarvitsee tehdä reititystä. [39]

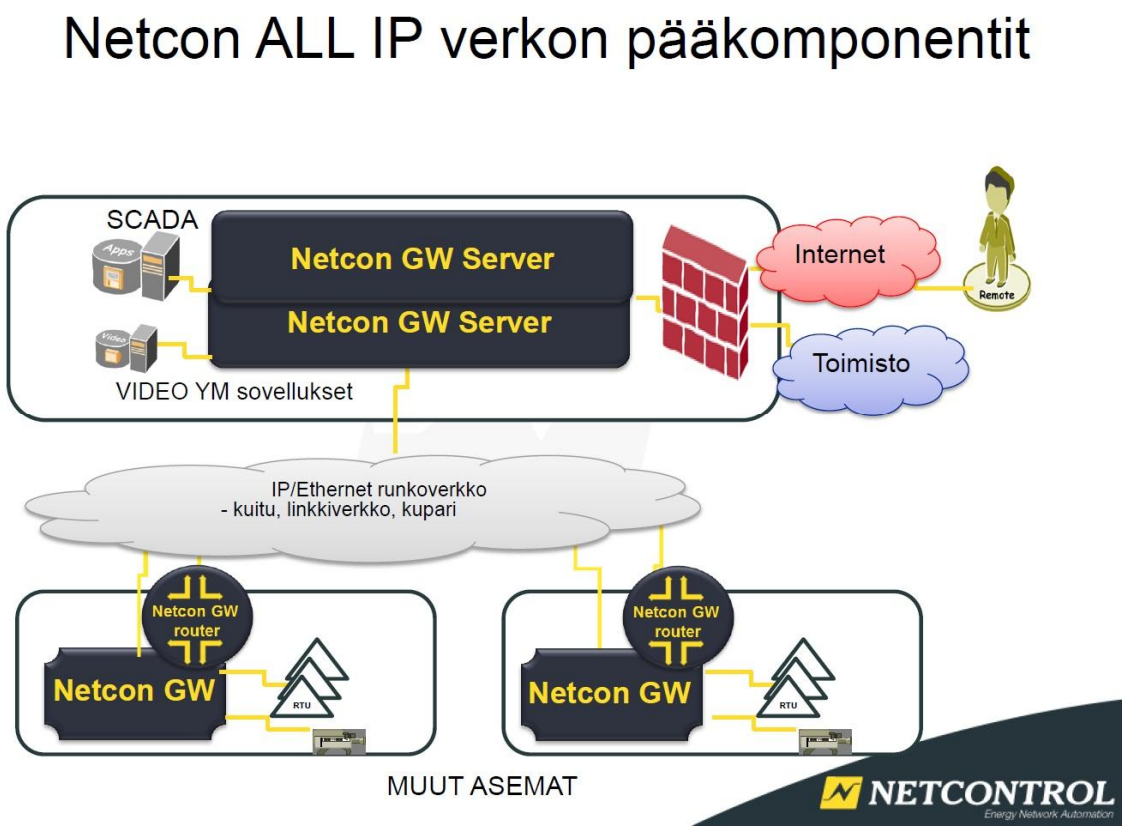
8.5.2 Netcontrol Oy:n ALL-IP-ratkaisu

Netcontrol Oy on suomalainen vuonna 1991 perustettu yritys, joka tarjoaa ratkaisuja tietoliikenteeseen, verkostoautomaatioon, sähköasema-automaatioon sekä valvomoihin. [40]

Netcontrol Oy:n Netcon ALL-IP-ratkaisu on sähköyhtiöille kehitetty kattava viestiliikennearkkitehtuuri. ALL-IP-järjestelmässä voidaan siirtää kaikki sähköasemilla tarvittava liikenne, kuten kaukokäyttöyhteydet, puhe, video, mittarinluku ym. tietoliikenneyhteydet IP-verkon päällä. Siirtomediana voi olla kupari, valokuitu tai jokin langaton ratkaisu. Verkon liikenne jaetaan neljään palveluluokkaan, kriittiseen, korkeaan, keskitasoon ja normaaliin. Kriittiseen palveluluokkaan kuuluu mm. reititys, NTP (aikapalvelu) sekä linkkiverkon hallinta. Korkeaan palveluluokkaan kuuluvat mm. SCADA-kaukokäyttö sekä VoIP (Voice over IP). Keskitason palveluluokkaan kuuluvat mm. mittarinluenta ja erilaiset etäkäytöt. Normaaliin palveluluokkaan kuuluvat toimistoverkkoyhteydet, kamera- ja kulunvalvonta sekä esim. sähkönlaadun mittaukset. Järjestelmässä ylemmän luokan palvelujono ohittaa matalamman. Järjestelmän laitteiden sisääntulossa sovellukset tunnistetaan ja liikenne ohjataan lähdössä palveluluokan mukaisiin jonoihin. [41]

Netcon ALL IP-järjestelmä koostuu Netcon GW Serveristä, joka on sijoitettu esim. käyttökeskukseen sekä sähköasemille sijoitetuista Netcon GW laitteista. Netcon GW Server voidaan kahdentaa ”Hot Standby”-menetelmällä, eli toinen GW server on

aktiivinen ja toinen varalla, vikatilanteessa liikenne siirtyy automaattisesti varalaitteelle. Muille laitteille kahdennettu GW server näkyy yhtenä laitteena. Järjestelmän pääkomponentit on kuvattu kuvassa 26. [41]



Kuva 26. ALL IP-verkon pääkomponentit.

Järjestelmään on saatavilla muunnin, jolla perinteinen sarjaliikenne voidaan siirtää IP-verkon yli. Laitteessa voidaan tehdä myös protokollamuunnoksia, esim. muuntaa sarjaliikenneprotokolla IEC 60870-5-101 IP-pohjaiseksi IEC 60870-5-104 -protokollaksi. Järjestelmä tukee yli 50 protokollaa. [41]

Järjestelmän tietoturva on rakennettu käyttäen syvyyssuuntaista suojausmallia, jossa kriittiset järjestelmät ovat usean sisäkkäisen palomuurin takana. Yhteydet eri toimipisteiden välillä voidaan salata (256-bittinen SSL-salaus). Järjestelmän laitteet voidaan kytkeä renkaaseen, jolloin jonkin linkin vioittuessa liikenne siirretään automaattisesti ehjälle reitille. Järjestelmässä käytetään standardin mukaista OSPF-reititystä. [41]

HSV:llä on käytössä Netcontrolin ALL-IP-järjestelmä muuntamoautomaation tietoliikenteessä. Tiedonsiirto on toteutettu langattomasti matkapuhelinverkon välityksellä. [42]

8.5.3 RADiFlow-ratkaisu.

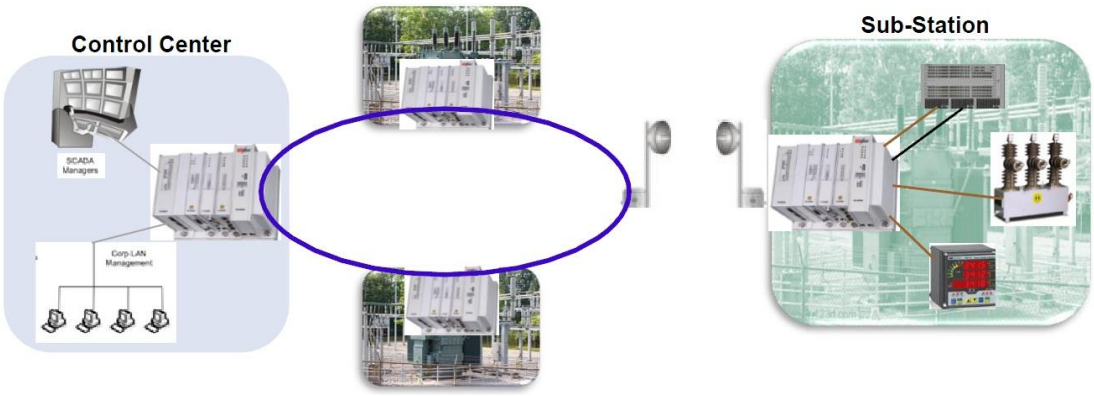
RADiFlow Ltd on osa israelilaista RAD Groupia, RAD valmistaa erilaisia tietoliikennelaitteita, protokollamuuntimia, mittalaitteita, radiolinkkejä ja muita tietoliikennelaitteita. RADiFlow on kokonaiskonsepti erilaisiin kaukokäyttösovelluksiin. [43]

RADiFlow-järjestelmä on kriittisille automaatioverkoille kehitetty tietoturvallinen verkkoratkaisu. Laitteet ovat modulaarisia DIN-kiskoon asennettavia (kuva 27). Niiden käyttölämpötila-alue on -40 - +75 °C ja suojausluokka IP30. Jotkut laitemallit voidaan varustaa kahdennetulla virtalähteellä. Laitteet täyttävät sähköasemakäytön vaatimukset standardin IEC 61850-3 EMI mukaisesti. Rajapintoina Ethernet- ja sarjaliikennemoduulit (RS-232/RS-485). [43] [44]

Kuva 27. RADiFlow-laitetyypit. [44]

Laitteiden verkkoyhteytenä voidaan käyttää Ethernet-liitäntöjä (kuitu/kupari), erilaisia kupariverkkomodemeja (SHDSL) sekä langattomia matkapuhelinverkkoja (GPRS, 3G). Laitteissa on kytkin sekä IP-reititysominaisuudet. Esimerkki laitteiden käyttökohteesta on kuvassa 28. Laitteiden avulla voidaan myös tunneloida sarjaliikenne IP-verkon yli. Laitteessa on protokollamuunnin, jolla sarjamuotoinen IEC 60870-5-101 -protokolla voidaan muuttaa IEC 60870-5-104-protokollaksi. Laitteet voidaan kytkeä renkaaseen ja

liikenne voidaan priorisoida ja salata. Laitteiden kellojen synkronointi voidaan toteuttaa IEEE 1588v2 PTP –protokollalla, jolloin ei tarvita asemakohtaista GPS-laitteistoa kellojen synkronointiin. Samaa kelloa voidaan käyttää sähköaseman automaatiolaitteissa. [43]



Kuva 28. RADiFlow-käyttöesimerkki. [43]

IEEE 1588 -protokolla on tarkan kellonajan synkronointiin kehitetty Ethernet-pohjainen protokolla, jonka avulla päästään alle 1 µs tarkkuuteen. Järjestelmä perustuu laitepohjaiseen menetelmään, jossa kello synkronoidaan uudelleen joka hypyssä ja aikasanomaan lisätään korjausarvo. Näin ollen IP-verkossa esiintyvät viiveet ja viiveen vaihtelut eivät vaikuta kellon tarkkuuteen. Järjestelmä vaatii toimiakseen IEEE 1588 -laitetuen kaikilta verkon laitteilta. [45]

Tietoturvaratkaisuina järjestelmässä on kytkinporttien MAC/IP-filtteröinti ja hajautettu porttikohtainen palomuuri, joka tunnistaa yleisesti käytetyt kaukokäyttöprotokollat. Verkossa siirrettävä data voidaan salata yhteyskohtaisesti. Laitteiden etähallintayhteydet on salattu SSH-protokollalla ja käyttäjientunnistukseen käytetään keskitettyä RADIUS-palvelua. [43] [44]

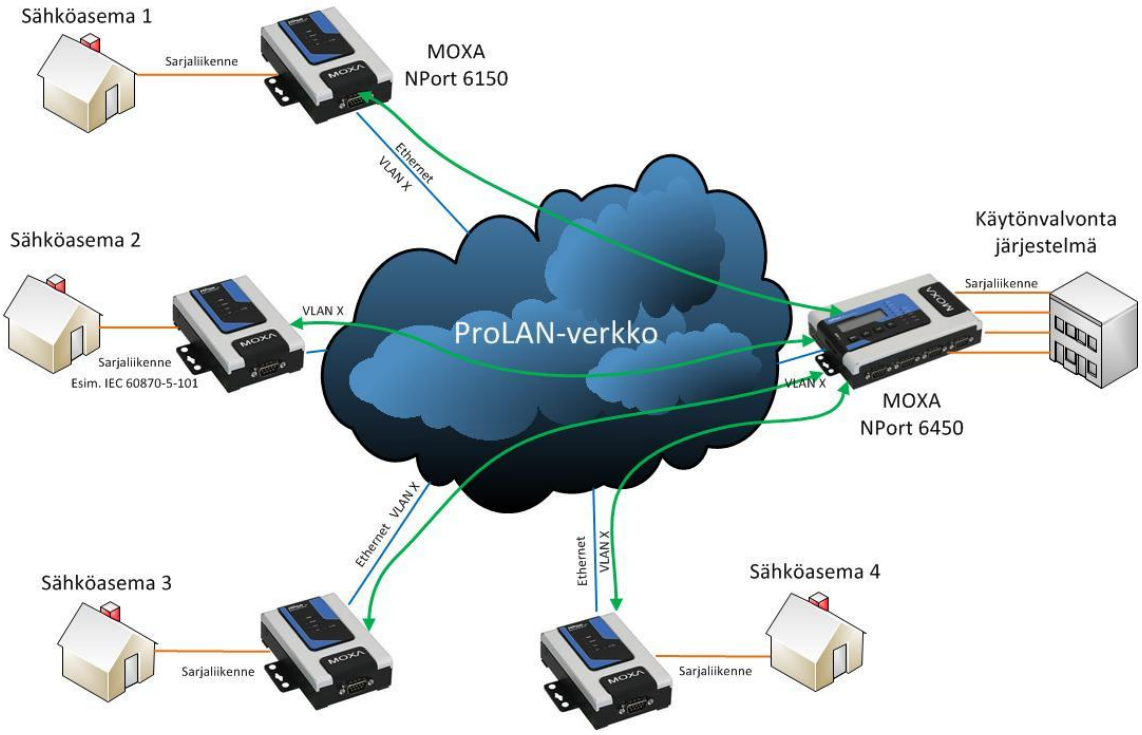
RADiFlow-järjestelmä on siis sähköasemakäyttöön kehitetty tietoturvallinen verkkoratkaisu, pääkäyttötarkoituksena kaukokäytöt ja automaatiojärjestelmän etäkäyttö. Laitteisto on valmistajakohtaista tekniikkaa, eikä siihen voi liittää toisen valmistajan laitteita ilman, että järjestelmän ominaisuudet kärsivät.

8.5.4 Sarjaliikenteen siirto ProLAN-verkon yli

Käytönvalvontajärjestelmän uusimisprojekti valmistui keväällä 2013. Uusi järjestelmä on hajautettu fyysisesti kahteen eri paikkaan, minkä vuoksi myös kaukokäyttöyhteydet pitää saada järjestettyä kahteen eri paikkaan. IEC 60870-5-104 -asemien osalta tämä ei vaadi suuria järjestelyitä. Riittää, että varajärjestelmälle rakennetaan ProLAN-verkon liitynnät, jolloin kaikkien IEC 60870-5-104 -asemien liikenne saadaan tarvittaessa ohjattua varajärjestelmälle.

Sarjaliikennettä käyttävien IEC 60870-5-101- ja I33-asemien osalta yhteydet vaativat enemmän työtä. Tällä hetkellä sarjaliikenneyhteydet on toteutettu PCM-verkossa ja kupariverkossa luvun 8.4 mukaisesti. Sähköasemalla on sarjaliikennekytkin, jolla liikenne ohjataan normaalitilanteessa päälinjalle ja päälinjan vioittuessa varalinjalle. Yhteyksien toinen pää on käyttökeskuksessa. Käytönvalvontajärjestelmän hajautuksen myötä tarvitaan ainakin yksi yhteys lisää viidelletoista sähköasemalle, ja sähköasemalta varajärjestelmälle. Vaihtoehtoina olivat perinteiset PCM- ja/tai modeemiyhteys, joissa vaihtoehdoissa työn määrä ja investoinnit olisivat olleet suhteellisen suuret ja laitteet ovat muutenkin jo elinkaarensa loppupuolella. Yhteydet päätettiin toteuttaa modernimmalla tekniikalla käyttämällä Ethernet-sarjaliikennemuuntimia ja siirtoverkkona ProLAN-verkkoa. Näillä laitteilla saadaan sarjaliikenne kuljetettua IP-verkon yli. Laitteiksi valittiin MOXA NPort -muuntimet, joita on käytetty kulunvalvontasovelluksissa jo useamman vuoden ajan, näin ollen laitteista on jo käyttökokemuksia. Tätä kirjoitettaessa laitteita on jo testattu yhdellä sähköasemalla ja yhteys toimii luotettavasti.

Kuvassa 25 on esitetty järjestelmän periaate. ProLAN-verkossa on NPort-laitteille oma VLAN, jossa ne liikennöivät. Sähköasemilla laitteina ovat MOXA NPort 6150 -laitteet joissa on yksi sarjaliikenneportti. Käytönvalvontajärjestelmän päähän on valittu MOXA NPort 6450 -laite, jossa on 4 kpl sarjaliikenneportteja. Käyttämällä useampiporttista laitetta käytönvalvontajärjestelmän päässä säästetään kaapelointia ja myös jonkin verran tilaa verrattuna yksittäislaitteisiin.



Kuva 25. Ethernet-sarjaliikennemuuntimien periaate.

Muuntimia käytettäessä säästetään suuri määrä fyysistä kytkentätyötä ja aikaa verrattuna perinteisiin yhteystapoihin, myös laitteiden investointihinta on huomattavasti pienempi.

8.5.5 Johtopäätökset (pääkaukokäyttö)

Jos verrataan Netcontrolin ja RADiFlow'n ratkaisua tämänhetkiseen toteutukseen ProLAN-verkossa ainoa suurempi ero on tiedonsiirtolinkkien salauksessa. Tällä hetkellä ProLAN-verkossa ei pystytä salaamaan toimipisteiden välisiä linkkejä. Ottaen huomioon, että lähes kaikki yhteydet ovat konsernin omissa kaapeleissa ja laitekaapit ovat lukittuja ja sijaitsevat omissa kulunvalvotuissa tiloissa, salauksen puuttumista ei voida pitää kovin suurena riskinä. ProLAN-verkon seuraavassa kehitysversiossa salaus saattaa olla jo mahdollista. Valmistajakohtaisissa laitteistoissa on myös oma riskinsä, koska tällöin sitoudutaan yhteen laitevalmistajaan ja sen kehityspolkuun sekä hinnoitteluun. Järjestelmän laajennusten kilpailuttaminen on hankalaa, jos on ainoastaan yksi valmistaja/toimittaja. Lisäksi valmistajakohtaisten laitteistojen käyttö ja ylläpito vaatii erityisosaamista. ProLAN-verkko on toteutettu standardien mukaisilla laitteilla, jolloin ei ole sitouduttu yhteen laitevalmistajaan. Myös kustannuksien kannalta nykymalli on parempi, koska samoja laitteita käytetään myös toimistoverkossa, jolloin

varaosa- ym. asiat saadaan järjestettyä kustannustehokkaasti. Lisäksi ei olla riippuvaisia yhdestä laitetoimittajasta. Netcontolin ja RADiFlow'n kaltaisten järjestelmien hyvinä puolina voidaan pitää liikenteen priorisointimahdollisuutta sekä protokollakohtaisia hajautettuja palomuureja.

8.6 Varakaukokäyttö

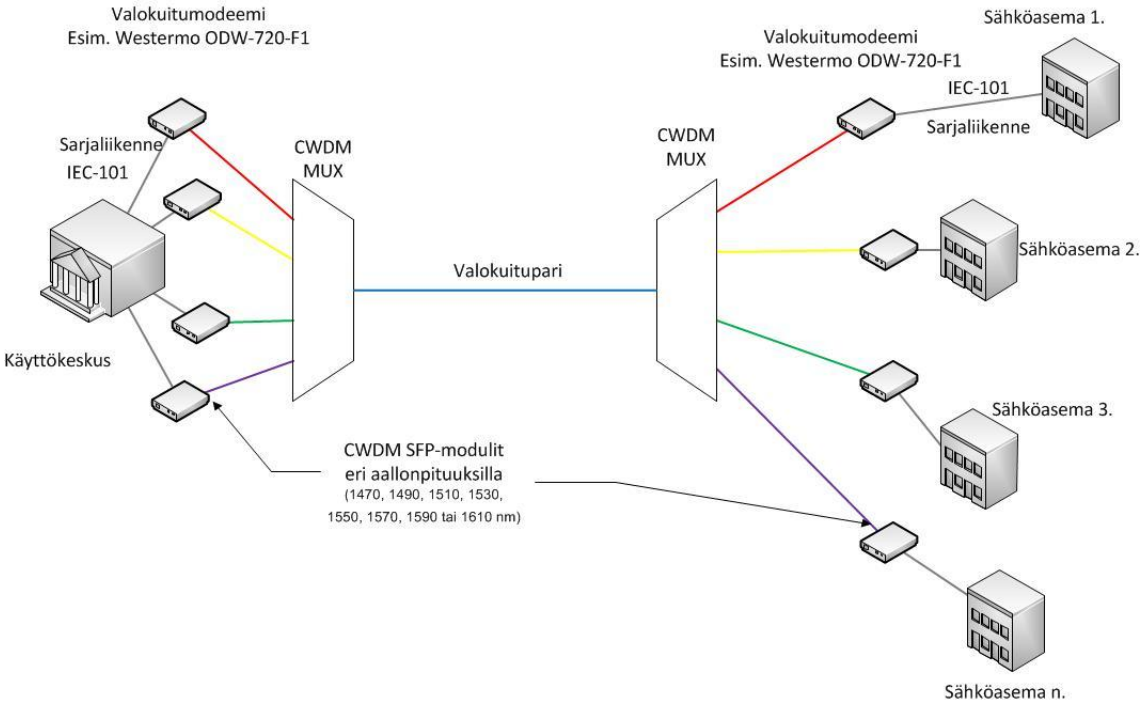
Varakaukokäyttöjärjestelmä on eräänlainen kevyt kaukokäyttölaitetta varmistava järjestelmä. Järjestelmällä ei voida ohjata asemaa, mutta sen kautta saadaan joitain yleishälytyksiä, joista nähdään onko asemalla kaikki kunnossa. [36]

Varakaukokäyttöyhteydet on tällä hetkellä toteutettu kuparikaapeliverkossa käyttäen sarjaliikennemodeemeita. Käytännön ongelmakohdaksi ovat muodostuneet sopivien hyvälaatuisten modeemien huono saatavuus, pitkät siirtotiet ja joillain reiteillä olevat huonolaatuiset kuparikaapelit. Tähän asti on käytetty Nokian valmistamia BB2W-modeemeita, mutta näiden valmistus on lopetettu jo useita vuosia sitten eikä näin ollen varalaitteita enää ole saatavilla.

Viime vuosien laajat valokuituinvestoinnit mahdollistavat valokuitujen käytön myös varakaukokäyttöyhteyksillä. Markkinoilla on useita erilaisia valokuitumodeemeja, joilla varakaukokäyttöyhteydet voidaan toteuttaa. Näin eliminoidaan ongelmat liian pitkistä kupariyhteyksistä ja suppeasta laitetarjonnasta. Valokuitumodeemeita on saatavilla 1-kuituisina versioina, jolloin kuituverkon kapasiteettia säästyy muihin käyttötarkoituksiin. Modeemeita voidaan kytkeä myös renkaaseen, jolloin kuituverkon käyttöä voidaan entisestään tehostaa. Esimerkkinä on valokuitumodeemi Westermo ODW-720-F1 point-to-point kuvassa 29.

Kuva 29. Valokuitumodeemi Westermo ODW-720-F1. [46]

Westermo Teleindustri AB:n kanssa on selvitetty CWDM-moduulien ottamisesta tuotevalikoimaan ja moduulit ovat tällä hetkellä testausvaiheessa. Kun moduulit tulevat tuotevalikoimaan (kesä 2013), kuituverkon kapasiteettirajoitukset saadaan kokonaan eliminoitua. Periaate näkyy kuvassa 30. [47]



Kuva 30. CWDM-yhteyksien käyttö varakaukokäyttöyhteyksillä.

Varakaukokäyttöyhteydet voitaisiin siirtää valokuiduille suhteellisen nopealla aikataululla (edellyttäen, että välillä on vapaata kuitukapasiteettia). Varakaukokäyttöhuoneeseen pitää rakentaa kuituyhteydet nykyisistä ristikytkentäpisteistä, kaksi reittiä kahdesta eri pisteestä. Kuitupaneeli on hyvä sijoittaa nykyiseen modeemikaappiin, jolloin laitteiden kytkentä on helppoa ja kytkentäkuituina voidaan käyttää normaaleita kytkentäkuituja. Mikäli käytetään esim. Westermo ODW-720-F1 -modeemia, pitää laitteille järjestää DC-sähkönsyöttö (käyttöjännite 12-48 VDC). Sähköaseman päässä pitää vetää suojattu kytkentäkuitu (esim. Tietosähkö Oy, BX-sarjan kaapeli tai vastaava) ristikytkentätelineeltä automaatiokaappiin ja järjestää sopiva sähkönsyöttö käyttämällä esim. DIN-kiskoon asennettavaa 24 V:n Traco Power TBL 060-124 -virtalähdettä varmistettuun sähkönsyöttöön kytkettynä.

Pääkaukokäyttöyhteyksien reitit pitää ottaa huomioon suunniteltaessa varakaukokäyttöyhteyksien reittejä kuituverkkoon ja pyrkiä mahdollisuuksien mukaan sijoittamaan varakaukokäyttöyhteydet eri reiteille.

9 Muut yhteydet

Seuraavassa on esitelty lyhyesti muita HSV:n sähköasemayhteyksiä ja kirjattu näiden kehityspolkuja.

9.1 Automaation etäyhteydet

Automaation etä-/huoltoyhteyttä käytetään mm. häiriötallentimien tietojen tarkasteluun. Yhteydellä voidaan myös kaukokäyttää sähköasemaa, mikäli varsinaiset kaukokäyttöyhteydet ovat vioittuneet. Etäyhteyden kautta voivat myös laitetoimittajat suorittaa erilaisia huoltotoimenpiteitä. Etäyhteyksiä on toteutettu vanhemmilla sähköasemilla suorilla point-to-point-modeemiyhteyksillä ja soittomodeemeilla, ja uudemmilla sähköasemilla ProLAN-verkon kautta. Uusilla rakennettavilla sähköasemilla ja saneerattavilla sähköasemilla etäyhteys toteutetaan ProLAN-verkon kautta.

9.2 Sähkön laatumittaukset

Sähkön laatumittauksia on tällä hetkellä käytössä ainoastaan yhdellä sähköasemalla. Yhteys on toteutettu ProLAN-verkossa. Uudet asennettavat sähkönlaadun mittauslaitteet kytketään ProLAN-verkkoon.

9.3 Rakennusautomaatio

Uudiskohteisiin ja saneeratuille sähköasemille asennettu rakennusautomaatiojärjestelmä on liitetty ProLAN-verkkoon, ja tässä noudatetaan ProLAN-kehityspolkua.

9.4 Kunnonvalvonta

Primäärilaitteiden jatkuva-aikaisen kunnonvalvonnan tietoliikenne on tällä hetkellä toteutettu toimistoverkossa tai ProLAN-verkossa. Periaatteena on ollut, että jos kunnonvalvontaohjelmistolla pystytään tekemään ohjauksia, jotka vaikuttavat primäärilaitteiden toimintaan, esimerkiksi ohjaamaan muuntajien jäähdytystä, on

tietoliikenne toteutettava ProLAN-verkossa. Kunnonvalvontatietojen keruu ja katselu voidaan toteuttaa toimistoverkossa. [30]
Tulevaisuudessa kaikki kunnonvalvontayhteydet siirretään ProLAN-verkkoon ja kehityksessä seurataan ProLAN-kehityspolkua.

9.5 Kulun- ja kameravalvonta

Kulunvalvontayhteydet on vanhoissa kohteissa toteutettu sarjaliikennemodeemeilla ja uudiskohteissa toimistoverkossa. Saneerausten yhteydessä vanhoja sarjaliikenneyhteyksiä on korvattu toimistoverkkoyhteyksillä. Joitain kohteita, joissa ei ole ollut käytettävissä toimistoverkkoyhteyttä, on toteutettu ProLAN-verkon yli sarja/Ethernet-muuntimien avulla. Kulunvalvontayhteydet tuottaa Helen-konsernin turvallisuuspalvelut ja tämän kehityksessä noudatetaan turvallisuuspalveluiden kehityspolkua.

Sähköasemien kameravalvontajärjestelmä on liitetty ProLAN-verkkoon ja yhteyksien kehityksessä noudatetaan ProLAN-kehityspolkua. [30]

9.6 Sähköasemien puhelimet

Sähköasemien puhelimet on liitetty Helenin omaan puhelinvaihteeseen kuparikaapeliyhteyksillä. Kahdella asemalla, jolla ei ole käytettävissä omia kuparikaapeliyhteyksiä, on puhelimet tuotu PCM-järjestelmän avulla. Puhelimien osalta noudatetaan Helenin puhelinvaihteen kehityspolkua. Uusille asemille, joille ei enää asenneta kuparikaapeleita, puhelinliittymät toteutetaan IP-puhelimilla tai vaihtoehtoisesti laitteilla, joilla puhelinliittymät saadaan kuljetettua valokaapeliyhteyden yli.

9.7 Verkkokäskyohjaus

Verkkokäskyohjausta on käytetty tariffin- ja ulkovalaistuksen ohjaukseen. Tariffinohjaus hoidetaan nykyisin etäluettavilla mittareilla ja ulkovalaistuksen ohjaukseen ollaan hankkimassa uutta järjestelmää, joten järjestelmä alkaa olla elinkaarensa päässä.

Verkkokäskyohjauksen yhteydet on toteutettu PCM-verkossa käyttäen hyväksi DN2-ristikytkentälaitteen haaroitusominaisuutta. Verkkokäskyohjauksen yhteydet on jaettu kahteen osaan, toisessa haarassa ovat 10 kV sähköasemat ja toisessa haarassa 20 kV sähköasemat. Käyttökeskuksen päässä rajapintana VKO-järjestelmään on kaksi BaseBand-modeemia, (yksi kummallekin haaralle), jotka on liitetty PCM-järjestelmän BaseBand-kanavakorttiin. Näistä modeemeista yhteydet viedään PCM-järjestelmän avulla sähköasemille, joissa vastaavat BaseBand-modeemit rajapintana PCM-järjestelmän ja VKO-ala-aseman välillä. Järjestelmä kommunikoi vuorollaan jokaisen ala-aseman kanssa eli yhteys muodostetaan yhteen ala-asemaan kerrallaan.

Edellä mainitun toteutustavan hyvänä puolena voidaan pitää sitä, että käyttökeskuksen päässä ei tarvita kuin yksi modeemi haaraa kohti ja huonona puolena sitä, että viestiyhteyksien vianhaku on erittäin hankalaa ja aikaa vievää. Nykyinen modeemikanta on myös erittäin vanhaa ja modeemien valmistus on lopetettu jo vuosia sitten.

VKO-järjestelmä on poistumassa käytöstä, eikä vuoden 2010 jälkeen uudiskohteisiin ole rakennettu verkkokäskyohjausta. Näin ollen kehitysnäkymänä on ainoastaan ylläpitää nykyistä järjestelmää yllä sen elinkaaren loppuun, tämänhetkisen tiedon mukaan vuoteen 2015. [30]

10 Yhteenveto

Tämän työn tarkoituksena oli luoda kokonaiskuva Helen Sähköverkko Oy:n sähköasemien tiedonsiirtoon. Työssä selvitettiin, miten tiedonsiirtoyhteydet on toteutettu tällä hetkellä, ja tutkittiin eri järjestelmien erityisvaatimuksia. Näiden perusteella on etsitty sopivia ratkaisumalleja yhteyksien toteuttamiseksi tai todettu, että nykyinen toimintamalli on jo valmiiksi käyttökelpoinen.

Työssä syvennyttiin eri tiedonsiirtotekniikoihin, järjestelmiin sekä fyysisiin tiedonsiirtoyhteyksiin (valokuitu, kuparikaapeli). Sähköasemanäkökulmasta keskityttiin pääasiassa 110 kV siirtoverkon suojaukseen ja sen vaatimiin yhteyksiin sekä kaukokäyttöyhteyksiin. Muut yhteydet kuten kamera-/kulunvalvonta, sähkönlaatumittaukset, verkkokäsky ym. on käsitelty kevyemmin, lähinnä kommentoimalla niiden nykytilaa ja yhteyksien kehityssuuntaa.

110 kV siirtoverkon suojausyhteyksissä tullaan siirtymään kokonaan valokuitujen käyttöön. Täten eliminoidaan nykyisten kuparikaapeliyhteyksien ongelmat siirtomatkan suhteen sekä varmistetaan siirtotien häiriöttömyys. Releuusintojen yhteydessä siirrytään käyttämään suoria kuituyhteyksiä, jolloin nykyiset PCM-verkossa olevat yhteydet poistuvat ja päästään eroon vanhentuneesta ja poistuvasta tekniikasta ja samalla yhteydeltä poistuu huomattava määrä aktiivilaitteita. Suorien valokuituyhteyksien käytölle on vielä joillain yhteysväleillä esteenä valokuituverkon kapasiteetti, mutta tämä voitaisiin kiertää käyttämällä yhteyksillä WDM-tekniikkaa. Valitettavasti relevalmistajat eivät tehtyjen tiedustelujen mukaan ole kovin innokkaita WDM-tekniikan käyttöön. Valmistajien kiinnostus voisi herätä, mikäli esim. releuusintojen tarjouspyyntövaiheessa tarjouspyyntöön lisättäisi vaatimus WDM-moduulien käytöstä. Valokuituverkon rakentamisen myötä verkon kapasiteetti tulee vuosien mittaan paranemaan ja kapasiteettiongelmat poistuvat.

Kaukokäyttöyhteyksien kohdalla jatketaan nykymallilla. Uudet asemat liitetään suoraan ProLAN-verkkoon (Helenillä kehitetty IP-pohjainen palvelukonsepti prosessijärjestelmille) ja vanhojen sähköasemien saneerauksien yhteydessä siirretään kaukokäyttöyhteyksiä nykyisiltä sarjaliikenneyhteyksiltä ProLAN-verkkoon. Varakaukokäyttöyhteyksillä siirrytään myös vähitellen käyttämään valokuitumodeemeita. Näin päästään eroon vanhenevista kuparimodeemeista, joiden valmistus on jo lopetettu, sekä kuparikaapeliyhteyksien matkarajoituksista.

Valokuitumodeemien laitevalmistajien kanssa on käyty keskusteluja WDM-moduulien saatavuudesta, ja tätä kirjoitettaessa näyttää siltä, että moduulit ovat tulossa tuotantoon. WDM-moduuleita käyttämällä saadaan varakaukokäyttöyhteydet toteutettua kaikille sähköasemille valokuidulla.

Työn edetessä tietämys sähköasemien järjestelmistä syveni, ja tämä auttaa tulevaisuudessa ottamaan järjestelmien erityistarpeet huomioon tiedonsiirtoyhteyksiä suunniteltaessa ja kehitettäessä. Työ tuo myös HSV:lle tietoa tiedonsiirtotekniikoista ja niiden mahdollisuuksista sähköasemayhteyksiä kehitettäessä.

Lähteet

[1] Helsingin Energia. 2011. Helsingin Energian vuosikertomus. 2011,yhteiskuntavastuun raportti.

[2] Helsingin Energia. 2012. Helen Intra. http://intra/hsv/yritystietoa/Sivut/Default.aspx Luettu 4.10.2012.

[3] Loukkalahti, Mika. 2013. Helen Sähköverkko Oy. Sähköpostiviesti Reijo Virtaselle 5.1.2013.

[4] Helsingin Energia. 2013. Helsingin Energia lyhyesti. http://www.helen.fi/yritys/helen.html. Luettu 18.5.2013.

[5] Luoma, Marko. 2000. Siirtotekniikat. http://www.netlab.tkk.fi/opetus/s38118/s00/luennot/pdh_sdh_synkronointi_handout.pdf. Luettu 22.3.2013.

[6] Volotinen, Vesa. 1991. Teitoliikenne, Verkot ja päätelaitteet. Porvoo. WSOY.

[7] Draka, Prysimian Group. 2013. Kuparijohtimiset liityntäverkon kaapelit. http://www.draka.fi/draka/Countries/Draka_Finland/Languages/suomi/navigaatio/UutiseU/Arkisto/KuparijohtimisetLiityntaverkonKaapelit.html. Luettu 3.4.2013.

[8] Roimola, Taneli. 2007. Laajakaistayhteyksien vertailua käyttäjän ja rakennuttajan näkökulmasta. Diplomityö. Lappeenrannan Teknillinen Yliopisto. Tietotekniikan Osasto.

[9] Optiset liityntäverkot. 2006. Teletekno Oy. Helsinki.

[10] Flash Cord 2001 Valokaapelit tele- ja tietoverkossa. 2003. Helkama Bica Oy. Tampere. Tammer-Paino Oy.

[11] Sumitomo Electriv Industries Ltd. 2010. Optical Fibers & Cables. http://global-sei.com/fttx/product_e/ofc/fiber.html Luettu 11.1.2013.

[12] Virtanen, Reijo. 2001. DWDM laitteiden alkukokoonpanon valintaperusteet. AMK Projektityö. Helsingin Ammattikorkeakoulu.

[13] Janssen, Cory. 2013. Multiplexer (MUX). Tecopedia. http://www.techopedia.com/definition/24124/multiplexer-mux. Luettu 2.4.2013.

[14] ITU-T G.694.1. 2012. Spectral grids for WDM applications: DWDM frequency grid. http://www.itu.int/rec/T-REC-G.694.1/. Luettu 8.12.2012.

[15] Ristiniemi, Jukka. 2007. Suunnitelma Ethernet-pohjaisen TCP/IP-verkon toteuttamiseksi prosessitietoliikenteen tarpeisiin Helsingin Energiassa. Diplomityö. Lappeenrannan Teknillinen Yliopisto. Tietotekniikan osasto.

[16] Salmenperä, Mikko – Seppälä, Jari. 2013. Kurssimateriaali. Automaation tietoturva (omin käsin). https://ae.ase.tut.fi/csst/kurssit/tty/Helen-201303/. Luettu 26.3.2013.

[17] Vuola, Jukka. 2006. Verkostoasiantuntijan koulutusohjelma, Johdanto IP-verkkoihin. Kurssimateriaali. Teleware Oy.

[18] Helsingin Energia. 2008. Helsingin Energian vuosikertomus 2008. www.helen.fi/vuosi2008/Hel_En_vuosikertomus_2008.pdf. Luettu 30.11.2012.

[19] Takala, Mikko. 2012. Tuotantokriittisen prosessiverkkoympäristön valvonta. Diplomityö. Aalto-yliopisto. Tietoliikenne- ja tietoverkkotekniikan laitos.

[20] Samitier, Carlos. 2010. Comminication issues using line protection scemes. CIGRE JWG B5/D2.30.

[21] Comino, Romeo – Strittmatter, Michael. 2011. Advanced power grid protection, Next generation teleprotection solutions. ABB review. 3/2011, s. 19-25.

[22] Network Protection & Automation Guide. 2005. Areva.

[23] IEEE C37.94. 2003. IEEE Standard for N Times 64 Kilobit Per Second Optical Fiber Interface between Teleprotection and Multiplexer Equipment. The Institute of Electrical and Electronics Engineering.

[24] Dynanet TPSO. 2009. Esite. Nokia Siemens Networks.

[25] Ojavalli, Paavo. 2011. Relekoestuksissa käytettävä kytkinlaitesimulaattori. Diplomityö. Tampereen Teknillinen Yliopisto. Sähkötekniikan koulutusohjelma.

[26] Koivunen, Tiina. 2011. Tuulipuiston sähköverkon suojaus. Diplomityö. Tampereen Teknillinen Yliopisto. Sähkötekniikan koulutusohjelma.

[27] Tulkki, M. 1993. TPS 64 Kaukosuojauslaite. Käyttökirja. Nokia Telecommunications.

[28] ABB. 2004. TTT-käsikirja 2000-07 Luku 7: Oikosulkusuojaus.

[29] ABB. 2004. TTT-käsikirja 2000-07 Luku 10: Mittaus-, ohjaus- ja suojauslaitteistot.

[30] Helen Sähköverkko Oy. 2010. Sähköasemaspesifikaatio D02 Tietoliikenne. Sisäinen dokumentti.

[31] Jääskeläinen, Jouni. 2012. Saab Systems Oy. Sähköpostiviesti Reijo Virtaselle 20.12.2012.

[32] Dynanet Evolution. 2013. Esite. CommTel Network Solutions.

[33] Tiesmäki, Ville. 2013. Siemens Oy. Sähköpostiviesti Reijo Virtaselle 21.1.2013.

[34] Pöhö, Jarmo. 2013. ABB Oy. Sähköpostiviesti Reijo Virtaselle 21.1.2013.

[35] RAD Data Communications Ltd. 2011. Teleprotection over Packet. http://www.rad.com/12/Teleprotection-over-Packet/23080/. Luettu 26.3.2013.

[36] Loukkalahti, Mika. 2013. Helen Sähköverkko Oy. Keskustelu 28.3.2013.

[37] Elovaara, Jarmo & Haarla, Liisa. 2011. Sähköverkot II Verkon suunnittelu, järjestelmät ja laitteet. Helsinki. Otatieto.

[38] Tamsi, Toni. 2010. Verkkokatkaisija-aseman liittäminen MicroSCADA-käytönvalvontajärjestelmään. Insinöörityö. Vaasan Ammattikorkekoulu. Sähkötekniikan koulutusohjelma.

[39] Wikipedia. 2013. MPLS. http://fi.wikipedia.org/wiki/MPLS. Luettu 18.4.2013.

[40] Netcontrol Oy. 2013. Netcontrol yhtiö. http://www.netcontrol.com/fin/tietoa-meistae/netcontrol-yhtioe/. Luettu 18.4.2013.

[41] Netcon ALL-IP. 2013. Esite. Netcontrol Oy.

[42] Loukkalahti, Mika. 2013. Helen Sähköverkko Oy. Keskustelu 15.5.2013.

[43] Barda, Ilan. 2011. Secure Industrial Networks for Critical Applications. Seminaarimateriaali. RADiflow.

[44] Secure Communication for Critical Infrastructure Services. 2010. Esite. RADiFlow.

[45] Goraj, Maciej. 2011. Introduction to IEEE1588 v2. Seminaarimateriaali. Ruggedcom Inc.

[46] Point-to-Point Fibre Converter RS-232. 2013. Esite. Westermo Teleindustri AB. http://www.westermo.com/web/web_en_idc_com.nsf/alldocuments/291976B6728CCC33C12578930034B860. Luettu 14.1.2013.

[47] Eriksson, Lars – Lock, Ray, Westermo Teleindustri AB – Salmela, Markku, Salmetek Oy. Keskustelu 20.2.2013.