Mikko Takala

Tuotantokriittisen prosessiverkkoympäristön valvonta

Sähkötekniikan korkeakoulu

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 28.5.2012.

Työn valvoja:
Prof. Riku Jäntti

Työn ohjaaja:
FM, MBA Tapio Heinäaro

Aalto-yliopisto
Sähkötekniikan
korkeakoulu

AALTO-YLIOPISTO
SÄHKÖTEKNIIKAN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Mikko Takala

Työn nimi: Tuotantokriittisen prosessiverkkoympäristön valvonta

Päivämäärä: 28.5.2012 Kieli: Suomi Sivumäärä: 8 + 57

Tietoliikenne- ja tietoverkkotekniikan laitos

Professuuri: Tietoverkkotekniikka Koodi: S-38

Valvoja: Prof. Riku Jäntti

Ohjaaja: FM, MBA Tapio Heinäaro

Diplomityö on case-tutkimus Helsingin Energian tuotantokriittisen prosessiverkkoympäristön valvonnasta. Työssä esitellään Helsingin Energian tuotantokriittisille järjestelmille rakennettua nykyaikaista prosessiverkkoympäristöä (ProLAN) ja tutkitaan minkälaisia erityisvaatimuksia prosessiverkoilla on verkonvalvonnan kannalta. Työ tehtiin Helsingin Energialla ja tietolähteinä on käytetty olemassa olevia prosessiverkkoympäristöön liittyviä yrityksen sisäisiä dokumentteja. Lisäksi tutustuttiin verkon toimintaan käytännössä ja haastateltiin Helsingin Energian eri liiketoimintojen henkilöitä, jotka ovat järjestelmävastaavina eri prosessijärjestelmissä. Työn teoriaosuudessa tutkitaan kahta erilaista viitekehystä verkonvalvontaan sekä protokollia, joita verkonvalvontaa voidaan käyttää. Näihin liittyen lähdemateriaalina on käytetty standardointeja, suosituksia ja protokollakuvauksia.

Tutkimuksessa painotetaan verkonvalvontaa teknisessä mielessä ja sen avulla pyritään kehittämään ja edistämään verkonvalvontaa Helsingin Energian tarpeisiin. Diplomityön on tarkoitus olla apuna verkon ylläpitäjille esittelemällä verkkoympäristön arkkitehtuuria ja tarjota eväitä verkonvalvonnan jatkokehittämiselle.

Tuloksena on saatu määritettyä minkälaisia asioita prosessijärjestelmille tarkoitetusta verkkoympäristöstä pitäisi valvoa. Viitekehykset tarjoavat hyviä ohjeistuksia verkonvalvonnan eri osa-alueista ja liittävät ne hyvin liiketoimintaan ja sen jatkuvuuteen. Teknisessä mielessä riittävä kapasiteetti, liikenteen viiveettömyys ja toipuminen vikatilanteista ovat olennaisia asioita, joita on syytä painottaa prosessijärjestelmien luonteesta riippuen. Verkonvalvonta on tärkeä kokonaisuus monimutkaisissa ympäristöissä, jonka kehittämisen pitäisi olla jatkuvasti käynnissä oleva prosessi. Toimivan verkonvalvonnan ylläpitäminen vaatii sekä aikaa että resursseja.

Avainsanat: verkonvalvonta, prosessijärjestelmä, prosessiverkko

AALTO UNIVERSITY
SCHOOL OF ELECTRICAL ENGINEERING

ABSTRACT OF THE
MASTER'S THESIS

Author: Mikko Takala

Title: Monitoring production critical process network environment

Date: 28.5.2012 Language: Finnish Number of pages: 8 + 57

Department of Communications and Networking

Professorship: Networking Technology Code: S-38

Supervisor: Prof. Riku Jäntti

Instructor: MA, MBA Tapio Heinäaro

This master's thesis is a case-study of network monitoring of Helsingin Energia's production critical process network environment (ProLAN). Process network environment is introduced in general view and special requirements for network monitoring of process systems are examined. Master's thesis was done at Helsingin Energia and internal documents were used as sources. ProLAN-network's operation and performance was observed in practice and some of the internal business unit's system managers were interviewed. In the theoretical part of the thesis, two different frameworks for network management are studied. Also different protocols related to network monitoring are inspected.

In this thesis, focus is on the technical part of network monitoring. Purpose is to develop and enhance network monitoring in Helsingin Energia's ProLAN-network. Thesis is intended to ProLAN-network's administrators as comprehensive introduction to the network environment and offer ideas for developing network monitoring.

In the conclusions there are described what kind of parameters should be monitored in process network environment. Frameworks offer advisable guidelines on different areas of network management and also connects its relevance to business and continuation. In the technical aspect, sufficient capacity, low-latency and automatic recovery from different kind of faults are essential issues to monitor for process systems. Network management and monitoring is important and its development should be a constantly ongoing process. Fully operational and accurate network monitoring requires time and resources.

Keywords: network monitoring, process system, process network

Esipuhe

Haluan kiittää työn valvojaa professori Riku Jänttiä opastuksesta, kommenteista ja mahdollisuudesta tehdä tämä diplomityö Aalto-yliopistossa.

Suurimmat kiitokseni haluan antaa ohjaajalleni FM, MBA Tapio Heinäarolle, jolta sain jatkuvasti tukea ja ohjausta työtä tehdessä. Saamani ohjaus oli ensiluokkaista ja työn aikana käymämme keskustelut olivat hyvin hedelmällisiä. Onnistuneen ohjauksen merkitys työn valmistumiselle oli merkittävä.

Haluan kiittää myös vanhempiani ja lähimmäisiäni, jotka ovat tukeneet minua opiskeluissani. Kiitokset ansaitsevat myös työkaverini ja kollegat, jotka ovat edesauttaneet työn valmiiksi saattamisessa.

Lopuksi kiitos avopuolisolleni, joka on tukenut ja kannustanut minua työni tekemisessä alusta loppuun asti.

Espoossa, 28.5.2012

Mikko Takala

Sisällysluettelo

Symbolit ja lyhtenteet

AES	Advanced Encryption Standard
CMIP	Common Management Information Protocol
CMS	Central Monitoring System
DCS	Distributed Control Systems
FCAPS	Fault, Configuration, Accounting, Performance and Security Management
GPRS	General Packet Radio Service
GPS	Global Positioning System
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
ITU	International Telecommunications Union
L2L	Local Area Network to Local Area Network
LAN	Local Area Network
MIB	Management Information Base
NTP	Network Time Protocol
OSI	Open Systems Interconnection

PCM	Pulse Code Modulation
PLC	Programmable Logic Controller
RFC	Request for Comments
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIC	Secure Internal Communication
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TCP/IP	Transmission Control Protocol / Internet Protocol
TMN	Telecommunications Management Network
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications Service
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WWW	World Wide Web

1 Johdanto

Tietoliikenteen kehitys on ollut viimeisen parinkymmenen vuoden aikana valtavan nopeaa. Energia-alalla ja siihen liittyvissä prosessijärjestelmissä on tietoliikenteen osalta ollut käynnissä jo jonkin aikaa murrosvaihe, jossa prosessijärjestelmien vaatimukset tietoliikenteen osalta ovat muuttuneet.

Helsingin Energiassa erilaisten tietoliikenneverkkojen rooli on merkittävässä osassa esimerkiksi sähkön ja lämmön tuotantoa. Niiden toimintaa voidaan pitää elinehtona tuotannon sujuvan toiminnan ja jatkuvuuden kannalta. Erilaiset tuotantokriittiset prosessijärjestelmät kuten automaation ohjaus- ja mittausjärjestelmät voimalaitoksilta, sähköasemilta ja kaukolämpöverkon ala-asemilta tarvitsevat alleen tietoturvallisen ja toimintavarman verkon tiedonsiirtoon. Perinteisesti tällaisia yhteyksiä on toteutettu Helsingin Energialla sarjaliikenteenä modeemiyhteyksien tai PCM-siirtojärjestelmän (Pulse Code Modulation) yli eri toimipisteiden välillä.

Edellä mainittujen teknologioiden siirtonopeudet ja liityntärajapinnat eivät enää vastaa nykyaikaisten prosessijärjestelmien vaatimuksia. Tuotantokriittisille prosessijärjestelmille suunnitellulta verkolta vaaditaan mm. enemmän kapasiteettiä ja liityntärajapinnat ovat muuttuneet sarjaliikenteestä pääosin Ethernet-pohjaiseen ja IP:n (Internet Protocol) päällä toimivaan liikenteeseen. Prosessijärjestelmät käyttävät erilaisia protokollia mutta yhteinen tekijä niille on IP-pohjainen verkko ja Ethernet-liityntärajapinta. Uuden tyyppinen verkkoarkkitehtuuri asettaa luonnollisesti uusia vaatimuksia verkonvalvonnalle. Piirikytkentäisestä verkosta siirtyminen pakettikytkentäiseen ja IP-pohjaiseen verkkoon vaatii omat työkalunsa ja valvontamekanismit, joilla taataan sovelluksille toimintavarmuutta.

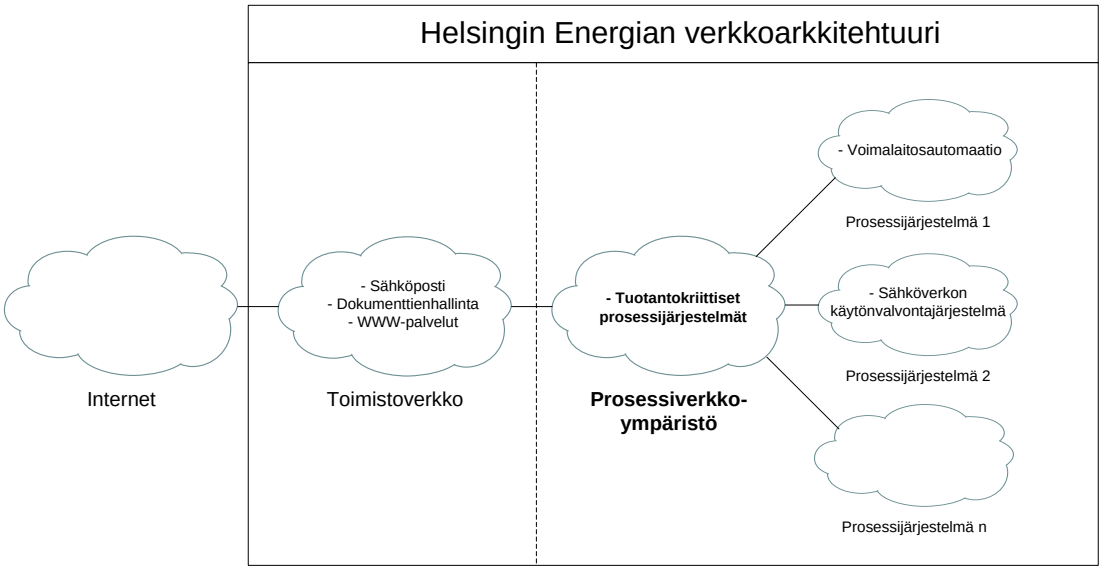
Tässä työssä tutustutaan Helsingin Energian prosessiverkkoympäristöön ja tutkitaan erilaisia verkonvalvontaan liittyviä teknologioita ja viitekehyksiä. Näistä pyritään löytämään potentiaalisia kehityskohteita ja parantamaan tätä kautta verkonvalvontaa Helsingin Energian prosessiverkkoympäristössä, jonka

myötä voidaan tarjota entistä luotettavampia verkkoja erilaisille tuotantokriittisille järjestelmille ja taata häiriöttömämpää toiminnan jatkuvuutta.

1.1 Taustat ja tutkimusongelma

Työn tilaajana on Helsingin Energia ja työssä tutkittiin miten prosessijärjestelmiä varten suunnitellun prosessiverkkoympäristön (ProLAN) verkonvalvontaa voidaan kehittää. Diplomityö tehtiin Helsingin Energialla yhdessä prosessiverkkoympäristön ylläpitäjien ja prosessijärjestelmistä vastaavien ja niiden kanssa operoivien henkilöiden kanssa. Lähdemateriaalina on käytetty paljon Helsingin Energian sisäistä dokumentaatiota ja näiden tueksi haastatteluja eri asiantuntijoiden ja järjestelmävastaavien kanssa.

Helsingin Energian tietoliikenneympäristö jakautuu kahteen erilliseen kokonaisuuteen. Alla olevassa kuvassa 1 on esitetty kokonaisuutta, joka koostuu toimistoverkosta ja tuotantokriittisille järjestelmille tarkoitetusta prosessiverkosta. Toimistoverkko on koko Helsingin Energian työntekijöille tarkoitettu tietoliikenneverkko toimistokäyttöön. Tyypillisiä sovelluksia ja järjestelmiä, joita on sijoitettu toimistoverkkoon ovat mm. sähköposti, dokumenttienhallinta ja yrityksen WWW-sivujen (World Wide Web) tuottamiseen tarvittavat palvelut. Toimistoverkkoon liitetyt työasemat ja palvelimet ovat vakioituja ja ympäristö on homogeeninen.



Kuva 1. Ylätason arkkitehtuurikuva Helsingin Energian tietoliikenneverkoista.

Helsingin Energian prosessijärjestelmille on rakennettu nykyaikainen ja uusiin tarpeisiin vastaava oma prosessiverkkoympäristönsä, joka on eriytetty muista verkoista. Tämä Ethernet-pohjainen korkean käytettävyyden ja tietoturvan verkkoympäristö on rakennettu vikasietoiseksi ja toimistoverkosta riippumattomaksi. Verkon runko on topologialtaan rengasmainen ja se kattaa suurimman osan Helsingin Energian toimipisteistä. Tähän runkoon on liitetty mm. voimalaitosten, sähköasemien ja kaukolämpöverkon ohjaamiseen ja käytönvalvontaan tarkoitettuja prosessijärjestelmiä. Eri prosessijärjestelmillä on toisistaan poikkeavia vaatimuksia verkon käytettävyydelle ja palveluiden saatavuudelle. Diplomityössä tutkitaan miten tällaisia prosessiverkkoja tulisi valvoa teknisessä mielessä ja minkälaisia haasteita ja erityisvaatimuksia niihin liittyy. Diplomityön aiheena on tuotantokriittisten prosessiverkkojen valvonta ja tutkimuskysymyksinä ovat:

1. **Mitä erityisvaatimuksia erilaisilla prosessijärjestelmillä on?**

2. **Mitä asioita verkonvalvonnalla halutaan nähdä?**

3. **Miten valvontaa voidaan toteuttaa ja kehittää Helsingin Energian ympäristössä?**

1.2 Työn rakenne

Työssä käydään läpi Helen-konsernin prosessiverkkoympäristön kannalta olennaisia IP-, tietoliikenne- ja valvontateknologioita. Kappale 1 toimii johdantona aiheeseen ja erityisesti alakappaleessa 1.3 syvennytään IT-ympäristöjen valvontaan ja tarkennetaan työn rajausta verkonvalvontaan, joka on siis yksi osa-alue IT-ympäristöjen valvonnassa.

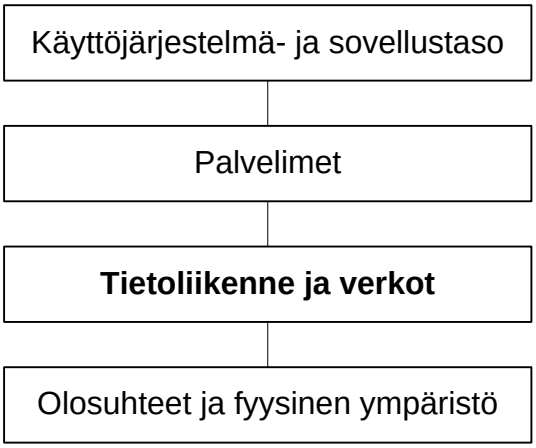
Kappaleessa 2 esitellään Helsingin Energiaa yrityksenä ja käydään läpi eri liiketoimintojen roolit. Lisäksi tässä kappaleessa kuvataan Helsingin Energian prosessiverkon, ProLAN:in verkkoarkkitehtuuria ja toimintaperiaatteita. Kappaleessa 3 käydään läpi yleisellä tasolla erilaisten prosessijärjestelmien erityisvaatimuksia verkonvalvonnan kannalta. Näissä kappaleissa pyritään löytämään vastauksia ensimmäiseen tutkimuskysymykseen, *mitä erityisvaatimuksia erilaisilla prosessijärjestelmillä on?*

Neljännessä kappaleessa lähestytään verkonvalvontaa ensin kahden yleisesti tunnetun viitekehyksen kautta ja sen jälkeen kuvataan erilaisia valvonta-arkkitehtuureja. Lopuksi syvennytään teknisemmällä tasolla erilaisiin protokolliin, joilla valvontaa voidaan toteuttaa ja jotka ovat oleellisia Helsingin Energian ympäristössä. Tässä kappaleessa haetaan vastauksia toiseen tutkimuskysymykseen, *mitä asioita verkonvalvonnalla halutaan nähdä?*

Lopuksi viidennessä kappaleessa esitetään johtopäätökset miten erilaisia verkonvalvonnan viitekehyksiä ja toisaalta teknisestä näkökulmasta, protokollia voidaan hyödyntää Helsingin Energian prosessiverkkoympäristössä. Tässä kappaleessa vastataan kolmanteen tutkimuskysymykseen, *miten valvontaa voidaan toteuttaa ja kehittää Helsingin Energian ympäristössä?*

1.3 IT-ympäristöjen valvonta ja työn rajaus

Työn aiheena on tuotantokriittisten prosessiverkkojen valvonta. Tässä kappaleessa käydään läpi työn rajausta ja peilataan verkonvalvontaa muihin osa-alueisiin IT-ympäristöjen valvonnassa. Alla olevaa kuvaa 2 tarkasteltaessa nähdään, että kokonaisuutena IT-ympäristön valvonta koostuu useista eri osa-alueista, joita on kaikkia syytä valvoa, jotta liiketoiminnan jatkuvuus voidaan taata. Jo lyhyet katkokset eri osa-alueilla voivat aiheuttaa tuotantokatkoksia ja täten suuria taloudellisia menetyksiä yrityksille. Hyvin suunniteltu ja tehokkaasti hallittu konesaliympäristö kasvattaa yrityksen tuottavuutta tarjoamalla luotettavan alustan tietoverkoille ja –järjestelmille. [1], [2], [3], [4] Työssä oletetaan, että palvelinkeskukset ovat jo olemassa ja niiden kehittämiseen, käyttöön ja turvallisuuteen on omat prosessinsa, joihin ei tässä tarkastelussa puututa. Seuraavaksi käydään läpi, mitä IT-ympäristön valvontaan liittyvät eri osa-alueet ovat ja minkälaisia asioita niissä tulisi valvoa teknisessä mielessä, taustalla tuotantokriittisten prosessijärjestelmien toiminta ja liiketoiminnan jatkuvuus.



Kuva 2. IT-ympäristön valvonta ja eri sen osa-alueet.

1.3.1 Olosuhteet ja fyysinen ympäristö

Edellisellä sivulla esitetyn kuvan 2 mukaisesti alhaalta ylöspäin lähestyttäessä ensimmäisenä osa-alueena on olosuhdevalvonta. Palvelinkeskuksessa, jossa palvelimet ja tietoliikennelaitteet fyysisesti sijaitsevat, on syytä ottaa huomioon ja valvoa seuraavia asioita: [2]

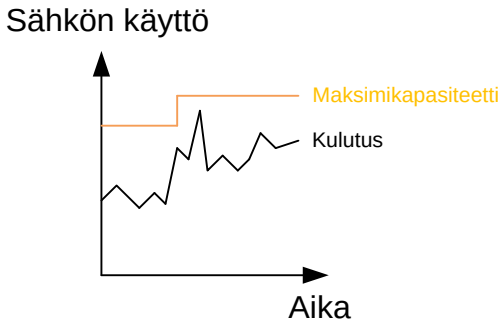
- Yleinen tilannekuva
- Sähkönsyötöt
- Jäähdytys
- Kosteus
- Paloturvallisuus

Näistä erityisesti sähkönsyöttö, jäähdytys ja kosteus ovat kriittisiä tekijöitä tietoliikennelaitteille, palvelimille, levyjärjestelmille ja muiden tietoteknisten laitteiden toiminnalle. Riittämättömyys sähkönsaannissa tai sulakkeiden palaessa esimerkiksi hetkellisen ylikuormituksen seurauksena seuraukset ovat välittömät, kun kaikki järjestelmät sammuvat samaan aikaan ja toiminta loppuu kokonaan. Vastaavasti liian korkea lämpötila ja ilmankosteus eivät ole hyväksi laitteiden toiminnan ja eliniän kannalta. [2]

IP-kamerat ovat yksi kätevä tapa saada yleistä kuvaa palvelinkeskuksen tilasta. Reaaliaikaisen videokuvan avulla nähdään yhdellä silmäyksellä tulviiko konesalissa tai tuleeko jostain esimerkiksi savua. Kamerat voidaan liittää olemassa olevaan verkkoinfrastruktuuriin ja niitä voidaan katsella samoilta valvontatyöasemilta mistä muitakin laitteita valvotaan. [2]

Sähkönsyöttöä voidaan valvoa asentamalla virrankulutusta mittaavat laitteet konesalin sähkökeskuksiin tai varavoimajärjestelmiin. Tällöin voidaan seurata hetkellisarvoja sähkönkulutuksesta ja esimerkiksi muutoksista kun tehdään isompia asennuksia. Lisäksi sähkönkulutusta on hyvä seurata pidemmällä aikavälillä, jotta osataan varautua varavoimalaitteiden mitoittamiseen tai maksimikapasiteetin kasvattamiseen riittävän ajoissa. Seuraavalla sivulla kuvassa 3 on esitetty esimerkki, jossa näkyy konesalin sähkönsyötön maksimikapasiteetti oranssilla kuvaajalla ja kulutus ajan suhteen mustalla kuvaajalla. Tämän

kaltainen seuranta on tärkeää, jotta sähkönsyötön tarpeisiin osataan varautua ajoissa. [2]



Kuva 3. Sähkönsyötön maksimikapasiteetti ja kulutuksen seuranta.

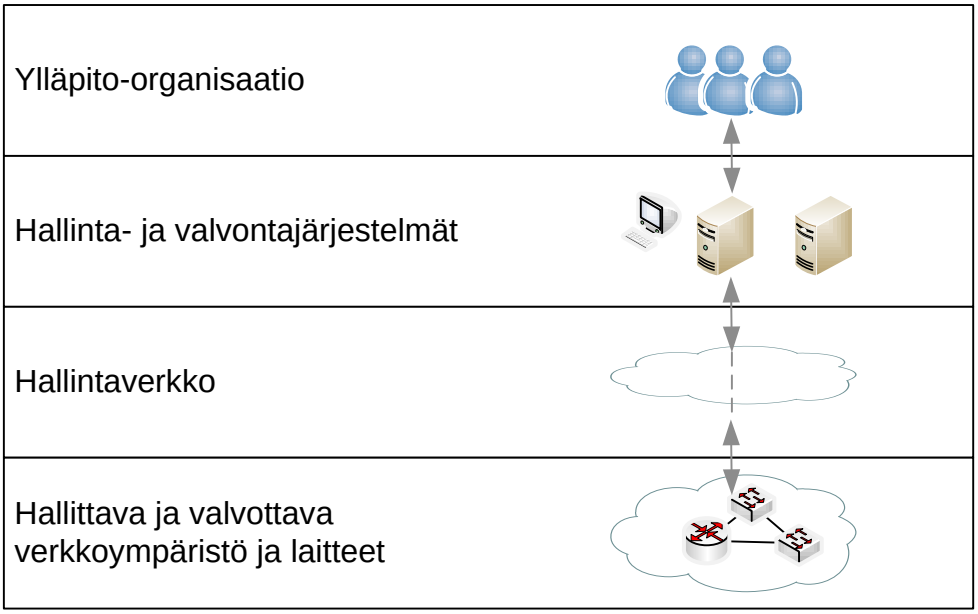
Lämpötilan ja kosteuden seuranta on myös olennaista olosuhdevalvonnassa, koska ne vaikuttavat laitteiden elinikään ja ääritapauksissa myös toimintaan. Jos äkillinen ja suuri lämpötilan nousu konesalissa huomataan riittävän ajoissa, osa vähemmän kriittisistä laitteista voidaan ajaa alas, jolloin lämmön tuotanto saadaan pienemmäksi. Tällöin kriittiset järjestelmät voidaan pitää yllä samanaikaisesti kun lämpöongelmaa korjataan. Pidemmän aikavälin trendeissä näkyvät lämpötilan muutokset konesalin eri osissa voivat paljastaa rikkoutumassa olevia ilmastointilaitteita tai ilmankierto-ongelmia. [2]

1.3.2 Tietoliikenne ja verkot

Fyysiset tietoliikenneyhteydet ja niiden päälle rakennettavat loogiset verkot luovat pohjan koko IT-ympäristölle ja –järjestelmille. Verkkojen kompleksisuuden kasvaessa verkonvalvonnan rooli korostuu entisestään. Jo lyhyet katkokset tietoliikenneyhteyksissä voivat aiheuttaa tuotannollisia häiriöitä yrityksille tai suuria taloudellisia menetyksiä. [4] Tästä saadaan perusteltu tarve ja motivaatio verkonvalvonnan toteuttamiseen ja jatkuvaan kehittämiseen.

Verkonvalvonnan ja –hallinnan perusarkkitehtuuri on esitelty seuraavalla sivulla kuvassa 4. Englanninkielinen termi *network management* tarkoittaa suomeksi verkonhallintaa. Verkonhallinta kattaa erilaisia aktiviteettejä, metodeita, prosesseja ja työkaluja, joilla operoidaan, ylläpidetään ja valvotaan

verkkoympäristöjä. [4] Verkonvalvonta on osa verkonhallintaa ja jatkossa työssä keskitytään pääasiallisesti verkonvalvontaan.

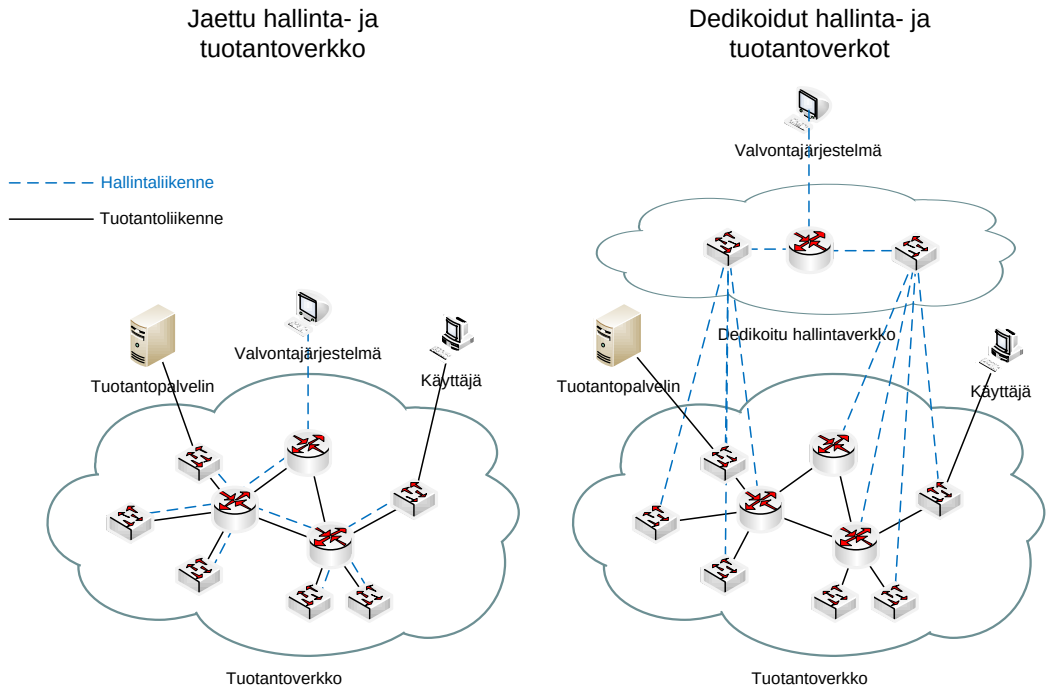


Kuva 4. Verkonhallinnan ja -valvonnan perusarkkitehtuuri. [4]

Kuvan 4 alimmassa laatikossa ensimmäisinä komponentteina verkonvalvonnassa ovat itse laitteet, jota valvotaan. Luonnollisesti suurissa verkoissa valvottavia laitteita on paljon, joten valvontaa on perusteltua toteuttaa automaattisilla järjestelmillä. Tyypillisiä laitteita ovat esimerkiksi kytkimet, reitittimet ja palomuurit. Valvottavat kohteet liitetään usein erilliseen valvontaverkkoon, jonka kautta ne keskustelevat valvontajärjestelmien kanssa. Tällöin valvonta- ja hallintaliikenne on eriytetty muusta tuotantoliikenteestä eivätkä ne rasita tai häiritse toisiaan. Samaan aikaan tämä on myös tietoturvakysymys, käyttäjille halutaan tarjota pääsy ainoastaan heidän tarvitsemille sovelluksille ja sulkea pois mahdollinen pääsy verkon hallintaan ja valvontaan liittyviin järjestelmiin. Kuvassa ylin laatikko kuvaa organisaatiota, joka vastaa verkon ylläpidosta. [4] On huomioitavaa, että verkonhallintaa ja –valvontaa voi toteuttaa automatisoitu järjestelmä, ihminen tai molemmat yhdessä. Joissakin tapauksissa riittävän hyvin konfiguroitu järjestelmä voi suoriutua tästä tehtävästä hyvin ja täyttää valvonnalle asetetut vaatimukset. Monimutkaisissa ympäristöissä valvontajärjestelmien jatkuva virittäminen tuo omat haasteensa. [5] Tässä työssä

pohditaan nimenomaan prosessiverkkoympäristön tuomia erityishaasteita ja yritetään löytää niitä kipupisteitä, joissa perinteinen verkonvalvonta ei riitä vaan tarvitaan ehkä kustomoituja ja kohdennettuja valvontamekanismeja joilla tarvittavaa informaatiota saadaan.

Hallinta- ja valvontaverkon eriyttäminen omaksi verkokseen (kuva 5) tulee erityisesti kysymykseen jos verkon koko on hyvin suuri tai sovelluksilla on kriittisiä vaatimuksia, joita ei haluta vaarantaa tuotantoliikenteen ja valvontaliikenteen sekoittumisen takia.



Kuva 5. Jaettu vs. dedikoidut hallinta- ja tuotantoverkot. [4]

Eriyttämisen hyviä puolia ovat: [4]

- *Luotettavuus.* Hallinta- ja valvontaliikenne kulkee omassa verkossaan eriytettynä tuotantoliikenteestä, jolloin se on paljon luotettavampaa.
- *Häiriöiden välttäminen.* Yhdessä jaetussa verkossa hallinta- ja valvontaliikenne kilpailee samoista resursseista tuotantoliikenteen kanssa. Suurissa verkkoympäristöissä liikennemäärät jo pelkistä valvontayhteyksistä saattavat kasvaa merkittäviksi. Tyypillisesti hallinta- ja valvontaliikenne on kuitenkin hyvin pientä verrattuna muuhun

liikenteeseen, esimerkiksi äänen ja videon siirtämiseen verkossa. Toisaalta se voi olla purskeista, esimerkisi vikatilanteissa tai kun laitteiden konfiguraatioita varmuuskopioidaan. Juuri tällöin on tärkeää, että hallinta- ja valvontaliikenne toimii, eikä katkeile ylikuormitusten vuoksi.

- *Verkon suunnittelun helppous.* Konfiguraation hallinta ja verkkoarkkitehtuuri yksinkertaistuu kun tuotanto- ja hallintaliikenne erotetaan toisistaan. Toisaalta hallintaverkkokin täytyy suunnitella, toteuttaa ja ylläpitää.
- *Tietoturva.* Hyökkääjien on hankalampi yrittää tunkeutua eriytettyyn verkkoon ja samalla se on myös helpompi suojata.

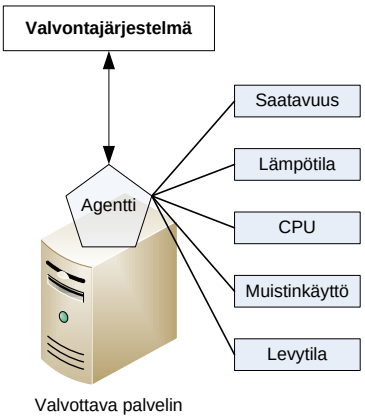
Eriyttämisen huonona puolena voidaan pitää kustannuksia. Fyysisesti eriytetty hallintaverkko vaatii omat laitteet ja ylläpitämisensä. Kustannukset kasvavat vastaavasti verkon koon kasvaessa kun hallintaverkkoakin täytyy laajentaa. Lisäksi ylimääräisien laitteiden kapasiteetteja ei pystytä hyödyntämään tehokkaasti, koska ne ovat omistettu ainoastaan hallinta- ja valvontaliikenteelle. Yhdistetty verkkoympäristö ei vaadi ylimääräisiä laitteita, tilaa tai kaapelointia. [4]

Oikein toteutettuna verkonvalvonnalla voidaan varmistaa, että verkkoa käyttävät palvelut toimivat kuten palvelutasosopimuksissa on luvattu. Lisäksi verkonvalvonta auttaa pitämään verkoista ja niiden ylläpidosta aiheutuvia kustannuksia kurissa.
Erilaisten verkonvalvontatyökalujen ja –järjestelmien avulla voidaan seurata verkon tilaa ja laitteita reaaliajassa. Laajempien valvontanäkymien avulla verkosta saadaan hyvä kokonaiskuva, jonka avulla verkon ylläpitoa ja kehittämistä voidaan ohjata ja suunnitella. [4]

Tämä diplomityö on rajattu tutkimaan tuotantokriittisten verkkojen valvontaa teknisestä näkökulmasta. Työssä käytetään viitekehyksiä verkonvalvonnan tukena mutta ei tutkita varsinaisesti verkonvalvontaprosesseja.

1.3.3 Palvelimet ja rautatason valvonta

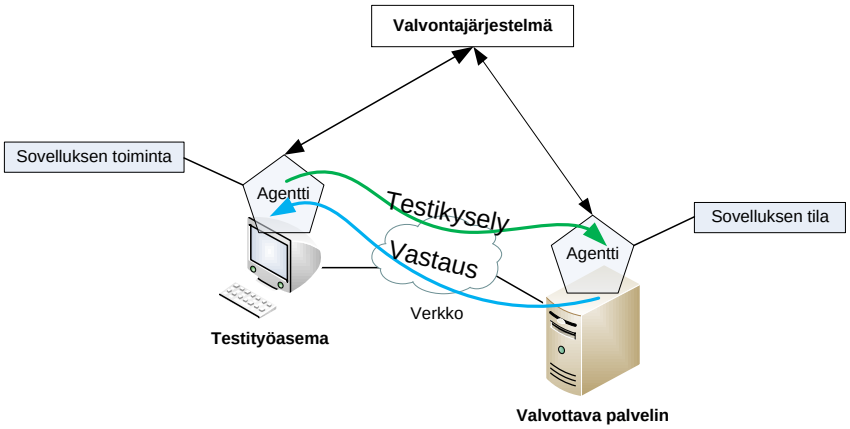
Palvelinten valvontaan on olemassa järjestelmiä, jotka valvovat rautatasolla palvelinten tilaa. Tyypillisiä asioita, joita yksittäisissä palvelimissa halutaan valvoa ovat palvelimen saatavuus, lämpötilat, prosessorikuormat, muistikuormat ja levytila. Alla olevassa kuvassa 6 on esitetty yleinen toimintaperiaate, jossa valvontajärjestelmä keskustelee palvelimeen asennetun agentin kanssa. [3]



Kuva 6. Palvelimen valvonta ja valvottavat asiat. [3]

1.3.4 Käyttöjärjestelmä- ja sovellustaso

Järjestelmien ja loppukäyttäjien näkökulmasta ketjun ylimpänä lenkkinä on itse sovellukset ja niiden valvonta. Sovellustason valvonta liittää yhteen kaikki edellä mainitut osa-alueet. Olennaisia komponentteja tässä on agentit käytettävillä työasemilla ja palvelimilla. Alla näkyvässä kuvassa 7 on esitetty kuvaus agenttien toiminnasta.



Kuva 7. Sovelluksen toiminnan valvonta. [3]

Agenttien avulla voidaan testata jonkin sovelluksen toimivuutta, esimerkiksi www-palveluna toimivaa sähköistä kaupankäyntijärjestelmää. Tällöin

automatisoitu valvontajärjestelmä ajaa ajastetusti testityöasemalta jonkin tapahtuman sähköiseen kaupankäyntijärjestelmään. Tällöin testatuksi tulee käyttöliittymä, palvelimen ja sovelluksen toiminta sekä niitä yhdistävä verkko. Tällaisissa valvonnoissa voidaan mitata esimerkiksi pyyntöihin liittyviä vasteaikoja. [3]

2 Helsingin Energian prosessiverkkoympäristö

2.1 Business-case

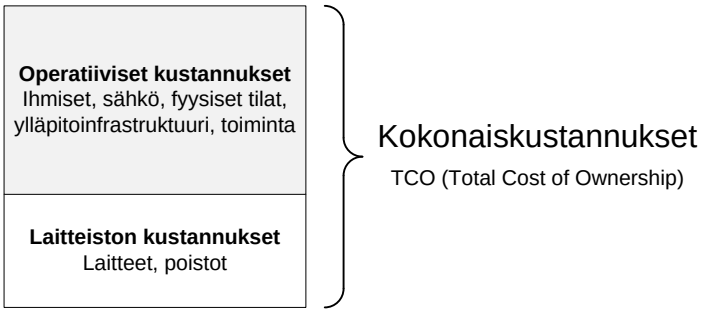
Helsingin Energia on pääosin Helsingin alueella toimiva energia-alan yhtiö, jolla on merkittävä rooli Helsingin alueen sähkön ja lämmön tuotannossa ja jakelussa. Helsingin Energia jakautuu erillisiin liiketoimintoihin, jotka vastaavat kukin omalta osaltaan energian tuotannosta, siirrosta ja jakelusta.

HelenVoima vastaa sähkön ja kaukolämmön tuotannosta Helsingin Energian voimalaitoksilla. **HelenSalkunhallinta** vastaa Helsingin Energian voimalaitosten ja voimaosuuksien kaupallisesta toiminnasta ja hyödynnettävyydestä. **HelenSähkö** vastaa sähköenergian vähittäismyynnistä kotitalouksille, yrityksille sekä muille energiayhtiöille valtakunnallisesti. Liiketoiminto on jakautunut suuryrityksiä ja pk-yrityksiä sekä pientaloissa ja kerrostaloissa asuvia palveleviin yksiköihin. **HelenLämpö** vastaa kaukolämmön myynnistä ja jakelusta sekä huolehtii riittävästä huippu- ja varalämmön tuotannosta. Näiden liiketoimintojen lisäksi Helen-konserniin kuuluva **Helen Sähköverkko Oy** vastaa sähkön siirrosta ja jakelusta lähes koko Helsingin kaupungin alueella. [6]

Suomen sijainti pohjois-Euroopassa asettaa lämmitykseen tarvittavan energian määrän henkeä kohti maailman suurimpien maiden joukkoon. Suomen energiahuolto perustuu hajautettuun ja monipuoliseen tuotantoon. Sekä sähköä että kaukolämpöä tuotetaan monipuolisesti erilaisilla menetelmillä. Helsingin Energia myy sähköenergiaa noin 400 000 asiakkaalle Suomessa ja kaukolämpötuotanto kattaa yli 90 prosenttia pääkaupungin lämmitystarpeesta. Kaukolämmön tuotanto Helsingin alueella on kuitenkin sähköntuotantoa paikallisempaa ja tässä mielessä se on huoltovarmuuskriittisempi järjestelmä. Kun kaukolämpöverkon ohjaamiseen käytetään tietoverkoissa toimivia erilaisia järjestelmiä, seuraa tästä luonnollisesti se, että näiden tietoteknisten järjestelmien jatkuvuus on yhtenä edellytyksenä häiriöttömälle saatavuudelle. Tämä asettaa alla toimivalle tietoverkolle korkeat vaatimukset käytettävyyden suhteen. [7] [6]

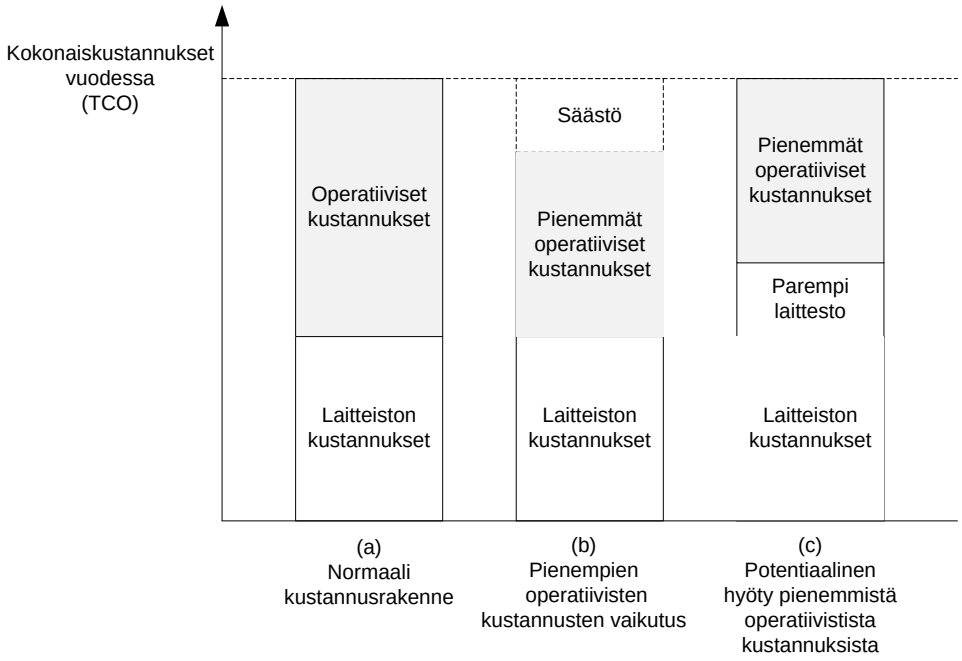
Helsingin Energian sisäinen erillisliiketoimintayksikkö ICT-palvelut on rakentanut ja ylläpitää tuotantokriittisille järjestelmille suunniteltua tietoturvallista prosessiverkkoympäristöä, ProLAN:ia, jossa edellä mainittujen liiketoimintojen tietotekniset järjestelmät toimivat eriytettyinä muista järjestelmistä.

Verkonhallinnan ja –valvonnan yhtenä tarkoituksena on suoranaisen valvonnan lisäksi tehdä verkon operoinnista tehokkaampaa ja ylläpitäjistä tuottavampia. Taloudellisesta näkökulmasta verkonhallinnalla pyritään pienentämään ja minimoimaan kokonaiskustannuksia, joita verkosta aiheutuu. Kuvassa 8 on esitetty verkkoympäristöstä aiheutuvia kokonaiskustannuksia, jotka voidaan jakaa operatiivisiin ja laitteistosta johtuviin kustannuksiin. [4]



Kuva 8. Verkkoympäristön omistuksen kokonaiskustannukset. [4]

Operatiiviset kustannukset voivat olla suuremmat kuin laitteistoon kuluvat kustannukset. Jos tehokkaammalla verkonhallinnalla ja –valvonnalla voidaan tehdä asioita suunnitelmallisemmin, voidaan periaatteessa ylläpidosta aiheutuvia operatiivisia kustannuksia laskea. Tällöin kokonaiskustannuksissa (TCO, Total Cost of Ownership) saadaan aikaiseksi säästöjä, jotka voidaan käyttää johonkin muuhun tai vastaavasti panostaa tehokkaampiin tai parempiin laitteisiin. Tätä ilmiötä on havainnollistettu seuraavalla sivulla kuvassa 9. [4]



Kuva 9. Operatiivisten kustannusten pienentämisen merkitys. [4]

Toisaalta ennakoimattomat katkokset verkossa voivat aiheuttaa ylimääräisiä kustannuksia. Seuraavassa yksinkertaisessa esimerkissä tarkastellaan tilannetta, jossa yrityksen www-pohjainen kauppapalvelu on kriittinen järjestelmä joka on saatavilla normaalisti 24 tuntia vuorokaudessa ja 7 päivää viikossa. Kauppapalvelu tuottaa keskimäärin tunnissa 4000 euroa tuloja asiakastilauksista. Kuukaudessa palvelu tuottaa 2,88 miljoonaa euroa. Jos tässä palvelussa, jossa tietoliikenneverkkoa voidaan ajatella yhtenä osa-alueena, tapahtuisi esimerkiksi 14 tunnin mittainen katkos, tarkoittaisi tämä keskimääräisesti 56 000 euron suoraa tappiota. Tämä luku perustuu keskimääräisiin arvoihin mutta tyypillisesti asiakastilauksia tulee tiettyinä vuorokauden aikoina enemmän kuin toisina, jolloin menetetyt tulot voivat olla paljon suuremmat. Vikatilanteita sattuu tyypillisesti usein siihen aikaan kun järjestelmät ja verkot ovat muutenkin kovemmalla rasitusasteella ja niihin kohdistuu piikkejä. Kun kasvavia trendejä jatkuvista ylikuormituksista ei huomata, voi tämä johtaa pahimmillaan edellä mainitun kaltaisiin pitkiin katkoksiin, joista edelleen aiheutuu rahallisia menetyksiä. [3]

Seuraavissa kappaleissa 2.2-2.3 esitellään Helsingin Energian yleisellä tasolla prosessiverkkoympäristöä, sen eri osia ja toimintaperiaatteita. Kappaleet 2.3.1 – 2.3.4 on merkitty salassa pidettäviksi niiden sisältävän salaiseksi merkityn materiaalin takia.

2.2 Prosessiverkkoympäristön esittely

Helsingin Energian ICT-palvelut on erillisliiketoimintayksikkö, jonka tarkoituksena on tuottaa tai hankkia ydinliiketoimintojen tarvitsemat tietotekniset ratkaisut. Prosessijärjestelmien kriittisyyden takia näitä järjestelmiä varten on kehitetty erillinen ympäristö, jonka nimi on 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. [8]

ProLAN-kehityshanke ja suunnittelu käynnistettiin vuonna 2006. Tuohon aikaan tiedostettiin kasvavat tarpeet uudenlaiselle verkkoympäristölle ja 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 verkosta, jotka muodostavat ProLAN-verkon rungon. Tätä hanketta lähdettiin viemään eteenpäin ja investointiprojekti ProLAN-verkon rakentamiseksi alkoi 2007. [9]

Seuraavassa kappaleessa esitellään ja käydään läpi Helsingin Energian ICT-palveluiden ylläpitämä prosessiverkkoverkkoympäritöä.

2.3 Prosessiverkkoarkkitehtuuri

Tänä päivänä tietoturvamekanismit ja suojaavat laitteet pelkästään yrityksen verkon ulkoreunalla eivät riitä. Tietomurrot ja –hyökkäykset voivat tapahtua usein myös verkon sisäpuolelta, madot, virukset ja troijalaiset voivat tulla turvallisena pidettyyn verkkoon sisäpuolelta, esimerkiksi huonosti suojattujen langattomien WLAN-verkkojen (Wireless Local Area Network) kautta tai huolimattomien käyttäjien mukana muistitikuilta. [10], [11] Suoraan tiettyihin organisaatioihin kohdennettuja hyökkäyksiä on havaittu jo useiden vuosien ajan. Perinteisten palvelunestohyökkäysten lisäksi yritysten tietoturvaa uhkaavat hyvin tarkkaan kohdennetut hyökkäykset. Kohdennetun hyökkäyksen tavoitteena on päästä käsiksi jonkin tietyn organisaation järjestelmiin. Tyypillisesti tämän kaltaisissa hyökkäyksissä käytetään tähän tarkoitukseen erikseen kehitettyjä haittaohjelmia, jotka käyttävät hyväkseen hyvin tuoreita haavoittuvuuksia, joita virustorjuntaohjelmistot eivät useinkaan tunne. Hyökkääjä ei pyri levittämään haittaohjelmia laajamittaisesti ja mielivaltaisesti vaan niitä lähetetään pienin määrin valikoidulle kohdejoukolle. Tällä tavoin hyökkääjä tavoittelee sitä, ettei sen toimintaa havaita ja vastatoimiin huomata ryhtyä. Energia-alalla tämän kaltaisia hyökkäyksiä on myös ja niiden torjuntaan täytyy kehittää jatkuvasti uusia ratkaisuja. [12] Yhtenä olennaisena osana puolustautumisessa voidaan pitää tarkkaa ja moniulotteista verkonvalvontaa, jonka avulla voidaan mahdollisesti havaita poikkeavia tapahtumia.

Edellä mainitun kaltaisilta hyökkäyksiltä suojauduttaessa voidaan käyttää hyväksi niin sanottua syvyyssuuntaista puolustusstrategiaa, *defense-in-depth*. Yrityksen verkkoa ei pidä ajatella yhtenä homogeenisena alueena, jonne käyttäjät voivat liittyä mistä tahansa ja saada samanlaiset pääsyt kaikkiin resursseihin. Sen sijaan yrityksen verkko pitäisi pilkkoa pienempiin osiin ja ottaa erilaisia tietoturvamekanismeja käyttöön näiden eri osien välille. Syvyyssuuntaisen puolustuksen perusajatuksena on, että jos yksi kerros onnistustaan murtamaan, niin seuraava kerros pitää vielä kriittisen toiminnan pystyssä ja mahdollisesti estää täydellisen järjestelmään tunkeutumisen ja sen kokonaisvaltaisen käyttöön saamisen. Tämä monikerroksinen suojausmalli antaa myös aikaa

puolustautumiseen ja joissain tapauksissa mahdollistaa hyökkäyksen analysointia ja helpottaa hyökkääjän jäljille pääsemistä. [13], [10], [11]

Yhden määritelmän mukaan syvyyssuuntainen puolustusstrategia koostuu kuudesta eri kokonaisuudesta: [10]

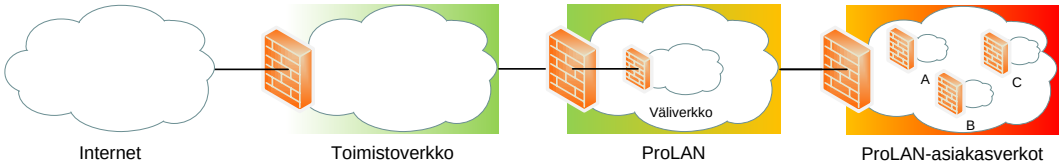
1. Kaikkien käyttäjien autentikointi verkossa.
2. Karkean tason eriytys verkkoliikenteelle esim. VLAN-tekniikkaa (Virtual Local Area Network) käyttäen.
3. Nykyaikainen palomuuriteknologia tarkempaan eriyttämiseen kriittisten osien kohdalla.
4. Verkkoliikenteen salaus.
5. Hyökkäysten havainnointi ja estäminen.
6. Työasemien ja palvelimien koventaminen.

Jos tuotantokriittisen verkkoympäristön rakentamisessa huomioidaan edellisellä sivulla listatut asiat, saadaan niistä johdettua vastaavasti valvottavia asioita. Alla listatut asiat ovat yleisiä asioita, joita jokaisessa verkossa tulisi valvoa eivätkä niinkään prosessijärjestelmistä tulevia erityisvaatimuksia.

1. Väärät autentikointiyritykset suhteessa hyväksyttyihin autentikoitumisiin.
2. Kytkinten, reitittimien ja palomuurien valvonta.
3. Salauslaitteisiin liittyvien väärinkäyttöyritysten seuranta.
4. Lokienkeruu, tapahtumien korrelointi ja niistä muodostuvat trendit.

Kokonaisuutta ajatellen nämä ovat kuitenkin olennaisia asioita. Kappaleessa 4 tullaan käymään läpi erilaisia protokollia, joilla yllä mainittuja asioita voidaan toteuttaa.

Kuvassa 10 on ylätason esitys ProLAN-verkkoarkkitehtuurista. Kokonaisuus jakautuu erillisiin vyöhykkeisiin, jotka ovat suojattu toisistaan palomuureilla. Vyöhykkeet ovat ulkoa päin turvattomammasta vyöhykkeestä turvallisempaan vyöhykkeeseen: *ProLAN-väliverkko, ProLAN-runkoverkko ja ProLAN-asiakasverkot*.



Kuva 10. ProLAN-verkkoarkkitehtuuri.

ProLAN-verkkoympäristössä toteutetaan syvyyssuuntaista puolustusstrategiaa, engl. d*efense-in-depth,* jolla pyritään ylläpitämään korkeampaa tietoturvaa ja käytettävyyttä. Tällä hajautetulla mallilla ja eri toimintojen eriyttämisellä saadaan seuraavia etuja: [14], [15], [16]

- Eri käyttäjillä on rajoitettu pääsy järjestelmiin koko verkkoympäristössä ja niiden toimia voidaan valvoa.
- Tietyille käyttäjäryhmille kuten ulkopuolisille kumppaneille tai järjestelmätoimittajille voidaan tarjota hyvin rajoitettu pääsy vain joihinkin järjestelmän osiin.
- Tietoturvamurto asiakasverkossa rajoittuu vain kyseiseen murrettuun alueeseen.
- Uhkaavassa tilanteessa kokonaisia vyöhykkeitä voidaan fyysisesti irrottaa toisistaan, jolloin ulkoiset hyökkäykset verkkoa pitkin ovat käytännössä mahdottomia.
- Ylläpitotyö jakautuu pienempiin osakokonaisuuksiin ja on täten helpompi hallinnoida.

3 Prosessijärjestelmien erityisvaatimukset

Tässä kappaleessa tutustutaan erilaisiin prosessijärjestelmätyyppeihin ja tutkitaan minkälaisia erityisvaatimuksia niillä on. Näiden myötä pyritään löytämään vastauksia ensimmäiseen tutkimuskysymykseen, *mitä erityisvaatimuksia erilaisilla prosessijärjestelmillä on?*

Nykyään monenlaisia tuotanto- ja prosessijärjestelmiä voidaan liittää IP-pohjaisiin tietoverkkoihin suoraan Ethernet-tekniikkaa käytäen. Mahdollisuudet erilaisten laitteiden ja ohjelmistojen verkottamiseen ovat kasvaneet valtavasti, toisaalta vastaavasti tarpeet etähallita näitä järjestelmiä ovat myös yleistyneet. Tällöin valvottava alue laajenee entisestään kun siirtotienä käytetään esimerkiksi kolmannen osapuolen matkapuhelinverkkoa. Näistä tarpeista nousee erityisvaatimuksia verkoille, joihin järjestelmiä liitetään. [17]

Teollisuuden automaatiojärjestelmät, kuten esimerkiksi voimalaitosten, sähköverkkojen tai kaukolämmön ohjaamiseen tarkoitetut järjestelmät ovat osa yhteiskunnan kriittistä infrastruktuuria. Tämän takia niiden toiminnan mahdollistavien verkkojen toiminta on kriittisessä asemassa. Verkon tilaa ja käytettävyyttä on pysyttävä seuraamaan jatkuvasti ja luotettavasti, mutta tämän lisäksi tietoturvan merkitys on suuri. [18]

Kriittiseen infrastruktuuriin liittyvillä tietojärjestelmillä on erityispiirteitä, joilla ne erottuvat muista tietojärjestelmistä on listattu alla: [18], [17]

- Häiriöiden vakavat seuraukset
- Automaatiojärjestelmien pitkä elinkaari
- Erityisohjelmistot
- Erilaiset käyttäjäryhmät
- Järjestelmätoimittajien asenteet virustorjuntoja ja tietoturvapäivityksiä kohtaan

Esimerkiksi järjestelmä 1 on latenssiriippuvainen järjestelmä, jossa hallinta-asema liikennöi ala-asemille eri puolelle kaupunkia. Verkosta pitäisi pystyä

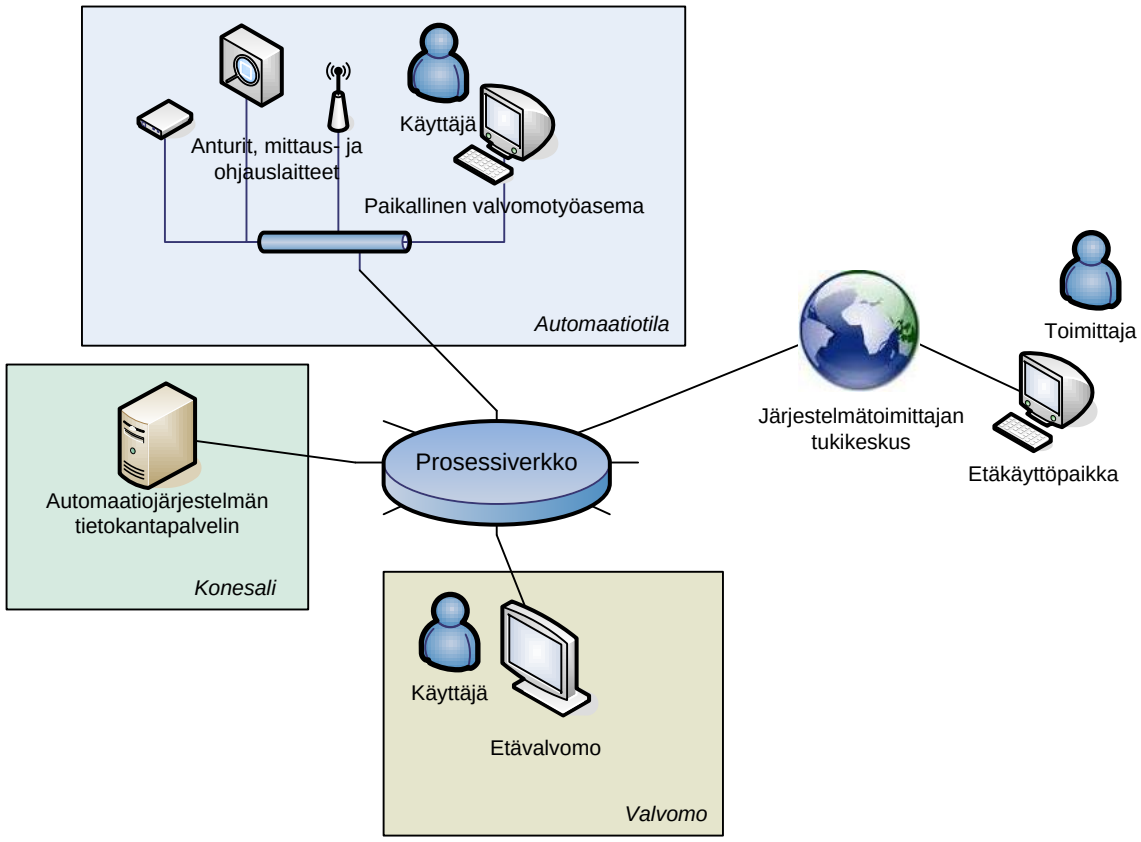
mittaamaan näitä latensseja, jolloin voidaan tarkkailla asiakkaalle luvattua latenssia tiedonsiirrossa. [17]

Toinen esimerkkijärjestelmä 2 voi vaatia tietyn määrän liikennekapasiteettia toimiakseen kunnolla. Esimerkiksi videokuvan toisto verkon yli vaatii tyypillisesti tietyn määrän kapasiteettia, jotta videokuvaa pystytään siirtämään reaaliajassa, hyvällä kuvanlaadulla ja kuvanopeudella. Tässä tapauksessa mitattavia asioita olisivat eri noodien välisten linkkien kuormitusasteet. [17]

Kolmantena esimerkkinä olisi verkon tarjoamien palveluiden valvonta. Dynaamiset reititysprotokollat ja varmistavat yhteydet eivät hyödytä verkkoon liitettyjä järjestelmiä, jos ne eivät toimi automaattisesti vikatilanteissa niin kuin on suunniteltu. Varayhteyksiä, reititysprotokollia ja tapahtumia tämän tyyppisissä asioissa olisi pystyttävä myös tarkkailemaan. Lisäksi tärkeäksi asiaksi prosessijärjestelmissä on aikatiedon tuottaminen eri sovelluksille, palvelimille ja tietoliikennelaitteille. Mm. kahdennetut järjestelmät vaativat, että eri noodien kellot käyvät samaa aikaa. Monimutkaisissa ympäristöissä vianselvityksen kannalta on oleellista, että lokimerkintöjen aikaleimat ovat samassa ajassa, jolloin eri paikoissa syntynyttä tietoa voidaan liittää toisiinsa ja päästä nopeammin ongelmiin käsiksi. Palvelinten, tietoliikennelaitteiden ja muiden verkkoon liitettävien prosessijärjestelmien laitteiden kellonaikoja voidaan synkronoidata NTP-protokollalla (Network Time Protocol). [19] Eri laitteiden kellon ajassa pysymisen tarkkuutta olisi hyvä pystyä seuraamaan. [17]

3.1 Automaatio- ja prosessinohjausjärjestelmät

Alla olevassa kuvassa 11 on esitetty automaatiojärjestelmän toimintaympäristöä. Tyypillisesti automaatiojärjestelmissä on esimerkiksi antureita, joilla kerätään dataa kentältä tai ohjataan toimilaitteita. Mittaus- ja ohjauslaitteilla voidaan tehdä säätöjä järjestelmään ja tietokantapalvelimeen kerätään data talteen. Näitä toiminnallisuuksia halutaan käyttää joko paikallisesti tai usein myös esimerkiksi etävalvomosta. Järjestelmän eri osat sijoittuvat fyysisesti eri tiloihin ja näiden välisille yhteyksille on erilaisia vaatimuksia käytettävyyden ja tietoturvan suhteen. Joissain tapauksissa prosessiverkkoon on myös pystyttävä toteuttamaan järjestelmätoimittajan etäyhteys tuen saamiseksi. [17]



Kuva 11. Automaatiojärjestelmän tietoverkko.

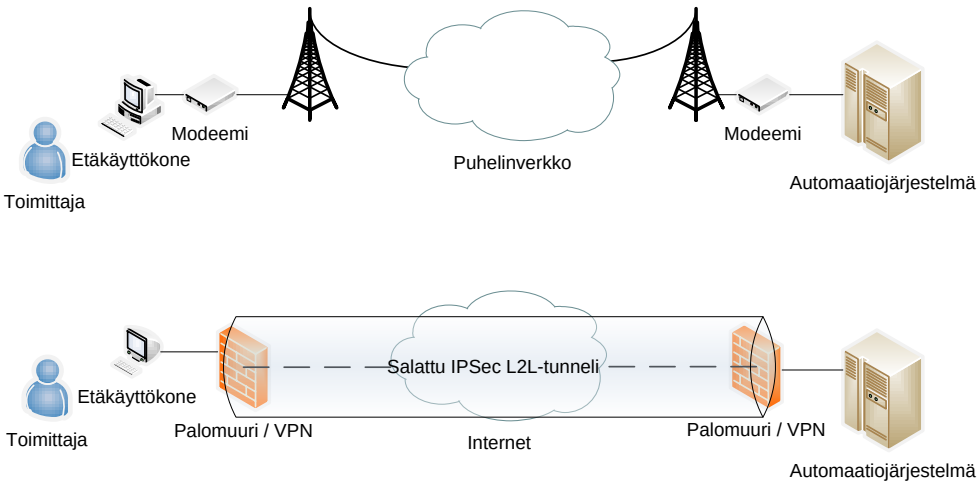
Nykyaikaiset teollisuuden automaatiojärjestelmät, ICS-järjestelmät (Industrial Control System) voidaan jakaa karkeasti kolmeen ryhmään verkkoarkkitehtuurin perusteella: [17]

1. Hajautetut ohjausjärjestelmät (Distributed Control Systems, DCS)
2. SCADA-käytönvalvontajärjestelmät (Supervisory Control and Data Acquisition Systems)
3. Ohjelmoitavat logiikkajärjestelmät (Programmable Logic Control, PLC)

Seuraavaksi avataan lyhyesti näitä erityyppisiä teollisuuden automaatiojärjestelmämalleja.

3.2 Hajautettu ohjausjärjestelmä

Energia-alalla hajautettuja järjestelmiä käytetään tyypillisesti laajojen ja monimutkaisten kokonaisuuksien kuten voimalaitosjärjestelmien ohjaamiseen. Hajautettu ohjausjärjestelmä (DCS) on jaettu ohjaustasoon ja yhteen tai useampiin hajautettuihin ohjausyksikköihin, kuitenkin niin, että ne sijaitsevat saman voimalaitosalueen sisällä. Hajautetut ohjausyksiköt ohjaavat tuotantoprosessien toimintoja ohjausyksikön kautta ja keräävät palautetta erilaisilta antureilta. [17]



Kuva 12. Salatun etäyhteyden muodostaminen automaatiojärjestelmään. [21]

Hajautetun järjestelmän ohjausyksikköinä käytetään erilaisia ohjelmoitavia ohjauslaitteita, joihin perinteisesti on järjestetty pääsy suoraan modeemin kautta. Tämän yhteyden kautta toimittaja tai voimalaitoksen työntekijät ovat pystyneet

keräämään diagnostiikkaa ja tekemään huoltotoimenpiteitä järjestelmään (edellisellä sivulla kuva 12). [17] Nykyään on mahdollista käyttää modeemien sijasta IP-pohjaista (Internet Protocol) L2L-tunnelia (Lan-to-Lan), joka tarjoaa paremmat mekanismit yhteyksien päästä päähän suojaukseen ja käyttäjän autentikoimiseksi. IPSec-protokollalla (Internet Protocol Security) voidaan muodostaa salattu tunneli julkisen verkon yli kahden päätepisteen välille. [20], [21] Prosessijärjestelmien tyypillinen elinikä on keskimäärin 8-15 vuottaja joissain tapauksissa paljon pidempi, esimerkiksi ydinvoimateollisuudessa pääautomaatiojärjestelmät voivat olla 20-30 vuotta vanhoja ja silti edelleen tuotannossa. Näiden järjestelmien elinkaarien aikana tietoliikenneteknologiat kehittyvät useita sukupolvia. Tämä tuo omat haasteensa eri järjestelmien ja teknologioiden yhteensovittamisessa. [22]

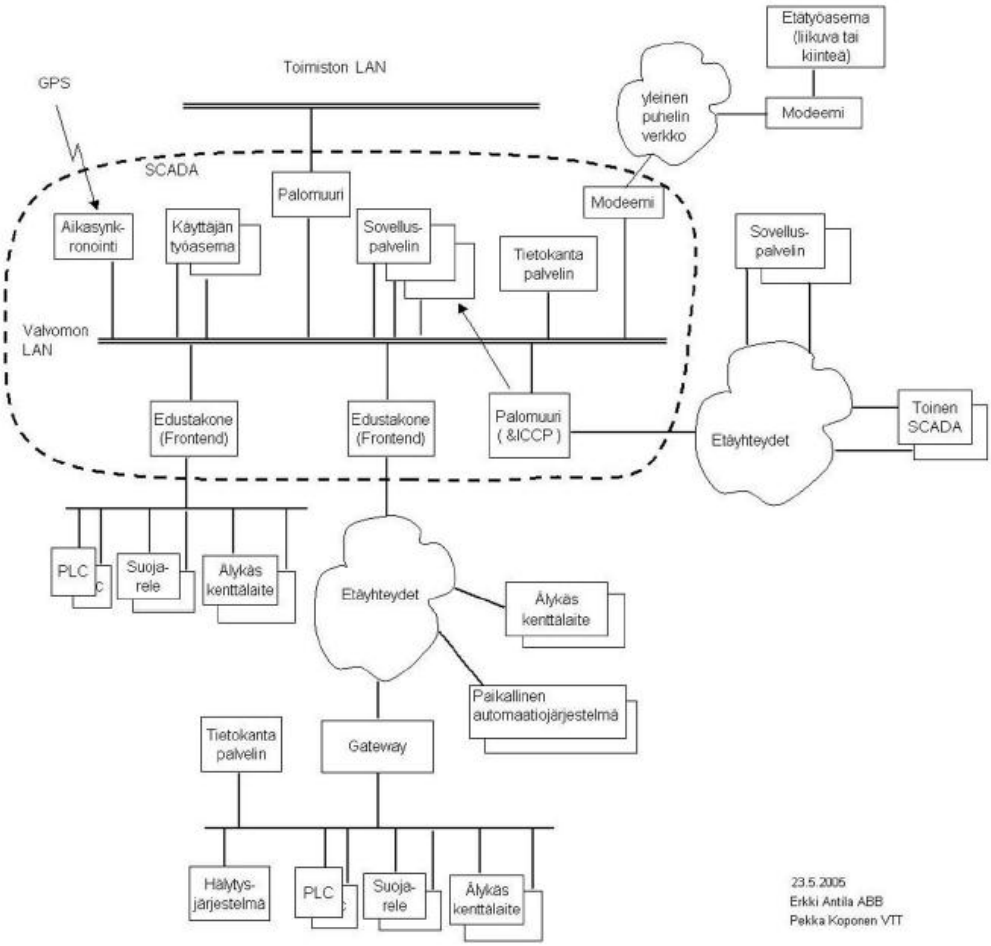
3.3 SCADA-käytönvalvontajärjestelmät

SCADA-järjestelmät (Supervisory Control and Data Acquisition Systems) ovat DCS-järjestelmiä hajaantuneempia ja niitä käytetään pääasiassa maantieteellisesti hajautettujen järjestelmien ohjaukseen. Energia-alalla tyypillisiä käyttökohteita olisivat esimerkiksi sähkön siirtoon ja jakeluun liittyvät järjestelmät. Niissä olennaista on keskitetty tietojen hankinta ja SCADA-järjestelmään liitettyjen alijärjestelmien (ala-asemien) etäohjaus. [17]

Seuraavalla sivulla olevassa kuvassa 13 esitelty arkkitehtuuri on tyypillinen esimerkki sähkönsiirron ja –jakelun SCADA-järjestelmille. SCADA-järjestelmän sisäisiin yhteyksiin ei paneuduta tässä työssä syvällisemmin mutta oleellista on, että laajan infrastruktuurin eri osia palvelevien toimintojen välillä on oltava tietoliikenneyhteydet. Nykyaikaisissa ympäristöissä protokollat on sovitettu toimimaan TCP/IP –pohjaisissa verkoissa. Yhteydet muihin SCADA-järjestelmiin ja yrityksen toimistoverkkoon on toteutettu liittämällä palomuureilla suojatut verkot toisiinsa. Verkon tietoturvan kannalta SCADA-verkot ja niissä käytettävät protokollat ovat haasteellisia tietoturvalaitteisiin saatavien tunkeutumisen havainnointiin ja estoon kehitettyjen IDS/IPS –järjestelmien (Intrusion Detection System / Intrusion Prevention System) kannalta, koska ne

eivät käytännössä tunne näitä protokollia. [17] Verkkoliikenteen seurannalla ja erilaisten hyökkäysten tunnistaminen ja torjunta parantaisi verkon tietoturvaa huomattavasti, mutta tämä osa-alue vaatii lisätutkimusta.

Yksi olennainen vaatimus SCADA-järjestelmissä on eri osien välinen aikasynkronointi. Kokonaisuuteen kuuluu keskusvalvontayksikkö (Central Monitoring System, CMS) ja yksi tai useampia ala-asemia (Remote Terminal Unit, RTU). Ala-asemien ohjaus ja niissä tapahtuvat muutokset vaativat usein reaaliaikaista näkymää ja tämän takia laitteiden kellot ovat oltava synkronoituina. Perinteisesti aikasynkronointi on tehty GPS-kelloilla (Global Positioning System) järjestelmän eri osissa mutta tulevaisuudessa IEC 61850 –viitekehyksen mukaisesti on mahdollista tehdä hyvinkin tarkkaa aikasynkronointia Ethernet-verkossa IEEE1588-standardin (Institute of Electrical and Electronics Engineers) mukaisesti. [17] ProLAN-verkon yhtenä palveluna on tarjota tarkkaa aikaa eri järjestelmille NTP-protokollalla (Network Time Protocol).



Kuva 13. Maantieteellisesti hajautettu SCADA-tyyppinen järjestelmä. [18]

3.4 Helsingin Energian prosessijärjestelmät

Helsingin Energian ProLAN-verkkoon on liitetty useita erityyppisiä prosessijärjestelmiä, joilla on omia erityisvaatimuksia verkon suhteen. Alla on listattu keskeisimpiä prosessijärjestelmiä, joilla on omat vaatimuksensa tietoliikenteen suhteen:

- Tuotannonohjausjärjestelmät
- Voimalaitosautomaatio
- Kaukolämpöverkon kaukokäyttö
- Sähköverkon käytönvalvonta
- Kameravalvontajärjestelmät
- Kulunvalvonta

3.5 Yhteenveto prosessijärjestelmien erityisvaatimuksista

Kappaleessa 3 tutkittiin mitä erityisvaatimuksia prosessijärjestelmillä on verkonvalvonnalle. Yleisesti ottaen energia-alalla automaatio-käytönvalvontajärjestelmillä ohjataan yhteiskunnan kriittistä infrastruktuuria kuten lämmön tuotantoa ja sähkön siirtoa. Verkon tilaa ja käytettävyyttä on pystyttävä seuraamaan reaaliaikaisesti, koska vakavien vikatilanteiden seuraukset ovat välittömät ja saattavat johtaa jopa sähkökatkoksiin. Erityyppisiä järjestelmiä tarkemmin avattaessa havaittiin, että verkon latenssi on olennainen asia niiden toiminnan kannalta. Toinen tärkeä asia SCADA-järjestelmien luotettavan toiminnan kannalta on aikasynkronointi järjestelmän eri osien välillä. Varsinaisten järjestelmien lisäksi aikatarkkuus on tärkeää klusteroiduille verkon komponenteille, joilla parannetaan vikasietoisuutta. GPS-signaalista saatavaa tarkkaa kellonaikaa voidaan jakaa NTP-protokollalla ja sen tarkkuutta on pystyttävä seuraamaan niin lyhyellä kuin pitkälläkin aikavälillä. Prosessijärjestelmät ovat tyypillisesti suunniteltu ja rakennettu niin, että ne toimivat itsenäisesti vaikka ulkoiset yhteydet niihin menetetäänkin. Ulkoisten yhteyksien vikaantuessa järjestelmiin ei voida ottaa huoltoyhteyksiä etäisesti vaan huoltotyöt joudutaan tekemään paikallisesti. Lisäksi jos järjestelmät keräävät historiatietoa ulkoisiin raportointi- ja tiedonkeruupalvelimille, myös näihin tietoihin tulee katkoksia. Nämä eivät kuitenkaan vaikuta järjestelmän toimintaan, jolloin ne eivät ole niin kriittisiä ominaisuuksia.

4 Verkonvalvonta

Tässä kappaleessa käydään läpi verkonvalvontaan käytettäviä viitekehyksiä ja valvonnan erilaiset arkkitehtuurilliset ratkaisut. Näistä haetaan hyviä ja huonoja puolia ja peilataan niitä Helsingin Energian tarpeisiin. Alakappaleessa 4.3 listataan mitä asioita verkonvalvonnalla yleensä halutaan saada näkyviin valvottavasta verkosta ja pohditaan, että riittävätkö ne täyttämään prosessijärjestelmien erityisvaatimukset. Alakappaleessa 4.4 käydään läpi tarkemmin oleellisia protokollia, joilla verkonvalvontaa voidaan toteuttaa ja millä valvontajärjestelmät ja valvottavat kohteet keskustelevat keskenään. Näillä haetaan vastauksia toiseen tutkimuskysymykseen, *mitä asioita verkonvalvonnalla halutaan nähdä?*

Verkonvalvonnassa on syytä myös huomioida erilaiset tavat toteuttaa sitä. *Passiivinen* valvonta tarkoittaa sitä, että valvontaa ei käytännössä tehdä ollenkaan ja vaikka indikaatioita joistakin tapahtumista tulisi, niihin ei kuitenkaan reagoitaisi. *Reaktiivisessa* valvonnassa ei valvota mitään aktiivisesti mutta tapahtumiin reagoidaan niiden sattuessa. *Interaktiivinen* valvonta käsittää kohteiden aktiivisen valvonnan mutta tapahtumia ja vikoja selvitellään käsityönä ja erillisinä tapahtumina. *Proaktiivisessa* valvonnassa valvotaan komponentteja aktiivisesti ja valvontajärjestelmä pyrkii tarjoamaan juurisyyt ongelmille yhdistäessään erilaisia tapahtumaketjuja toisiinsa. Lisäksi komponentit voivat käynnistää automaattisesti palautumis- tai vikatilanneprosesseja järjestelmän alahallaoloajan minimoimiseksi. [23], [4]

4.1 Viitekehykset

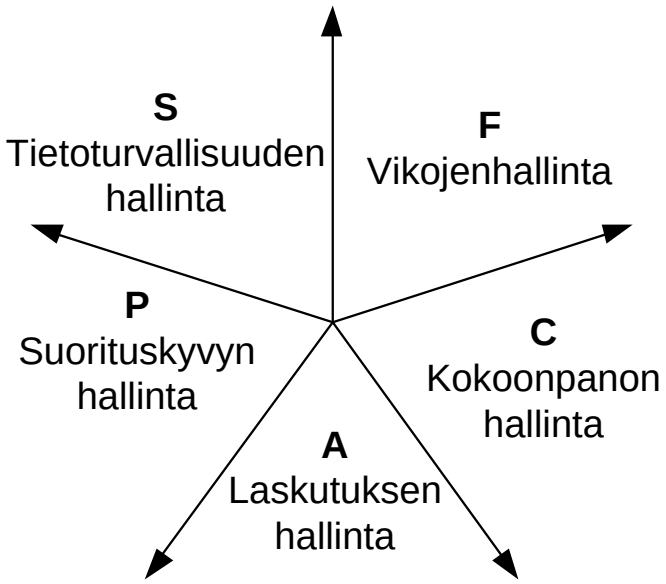
Verkonhallintaan ja –valvontaan on olemassa ITU:n (International Telecommunication Union) määrittelemiä standardointeja ja suosituksia, joiden avulla valvontaa voidaan toteuttaa. ITU-T:n suositukset muodostavat hierarkkisen kokonaisuuden, jossa eri osa-alueita on käsitelty. Diplomityön aiheen kannalta olennaisia suosituksia ovat ITU-T X.700, joka kattaa tietoliikenneverkot, avointen systeemien yhteydet ja niiden tietoturvan sekä ITU-

T M.3010, jossa käsitellään tietoliikenneverkkojen hallinnan periaatteita. [24], [25]

Seuraavaksi käydään läpi kaksi erilaista verkonhallintaan ja –valvontaan soveltuvaa viitekehystä, FCAPS- (Fault, Configuration, Accounting, Performance and Security Management) ja TMN-viitekehykset (Telecommunications Management Network). Nämä viitekehykset ovat yleisesti tunnettuja malleja ja tarjoavat hyviä ohjeita verkonhallintaan ja –valvontaan. FCAPS kuvaa hyvin prosesseja ja funktioita, joita sen eri osa-alueilla toteutetaan. TMN liittää verkonvalvonnan liiketoiminnan tarpeisiin ja siksi nämä kaksi viitekehystä tuovat oman hieman erilaisen näkökulmansa verkonvalvontaan.

4.1.1 FCAPS

FCAPS on ISO:n (International Organisation for Standardization) tuottama yleinen viitekehys verkonhallintaan. Alla olevan kuvan 14 mukaisesti malli jakautuu viiteen eri osaan ja se määrittelee minkälaisia asioita näillä eri osa-alueilla tulisi hallita ja valvoa. Tämä malli on osa ISO:n tekemää OSI-mallia ja sillä on laaja hyväksyntä eri verkonhallintajärjestelmien vaatimusten määrittelyssä. [26], [1]



Kuva 14. FCAPS-viitekehyksen eri osa-alueet. [27]

Vikojenhallinta *(Fault Management)* sisältää verkossa esiintyvien vikojen havaitsemisen, eristämisen ja korjaamisen. Käytännössä tämä tarkoittaa laitteiden lokien ylläpitoa ja seurantaa virheiden havaitsemisen kannalta, erilaisten toimenpiteiden määrittelyt vikahavaintojen perusteella, testaamista ja mittaamista vikojen todentamiseksi ja itse vikojen korjaamista. Laitteista saatavien erilaisten tapahtumien talteenotto ja analysointi on oleellista proaktiivisessa valvonnassa. Mahdollisten vikojen havaitseminen ennen kuin ne pääsevät syntymään todellisiksi ongelmiksi, vaatii oleellisen tiedon poimimisen ja esiin nostamisen kaiken muun seasta. [27], [1]

Vikatilanteen sattuessa vikojenhallinnan mukaan toimintamalli on seuraava: [26], [1]

1. Vian tunnistaminen ja paikallistaminen.
2. Toiminnan jatkuvuuden säilyttäminen mahdollisuuksien mukaan eristämällä vika.
3. Vikaantuneen komponentin korjaus tai vaihto.
4. Verkon tilan palautus normaaliin tilaan.

Kokoonpanon hallintaa *(Configuration Management)* käytetään verkon fyysisten ja loogisten osien yksilöimiseen, konfigurointiin ja dokumentointiin. Fyysisiä osia ovat esimerkiksi verkkokortit, kytkimet ja reitittimet. Loogisia osia ovat näiden päälle tehtäviä VLAN-verkkoja (Virtual Local Area Network), reititysmäärityksiä ja pääsylistoja. VLAN-tekniikalla tarkoitetaan yhden fyysisen verkon sisällä toteutettuja useampia virtuaalisia verkkoja IEEE 802.1Q – standardin mukaisesti. [28] Kokoonpanon hallinnan yksi olennainen osa on laitteiden säännöllinen varmuuskopiointi ja niiden palautukset. Verkon konfigurointiin tarkoitettujen työkalujen merkitys kasvaa mitä suurempia verkkoja hallitaan. Esimerkiksi muutosten tekeminen muutamiin tietoliikennelaitteisiin yhden kiinteistön sisällä on vielä hallittavissa käsityönä ilman varsinaisia verkonhallintaan tarkoitettuja työkaluja. Kun tarkastellaan monimutkaisempia verkkoja jotka jakautuvat esimerkiksi useisiin eri kiinteistöihin tai sijainteihin, pitkien etäisyyksien päässä toisistaan, keskitetty

etähallinta tuo merkittäviä etuja hallintaan ja valvontaan sekä nopeuttaa konfigurointia. [27], [26], [1]

Laskutuksen hallinta *(Accounting Management)* käsittää ja mahdollistaa laskutuksen verkon palveluiden käytöstä. Sen tarkoituksena on mitata verkkopalveluiden kustannukset ja määritellä niiden hinta käyttäjille. [29] Laskutuksen hallinnalla ei ole niin suurta merkitystä verkonhallinnassa teknisessä mielessä, joten sitä ei tässä työssä käsitellä tarkemmin.

Suorituskyvyn hallinta (*Performance Management)* käsittelee nimensä mukaisesti verkon suorituskykyä. Verkossa on rajattu määrä resursseja ja niiden käyttöä on voitava seurata, jotta asiakkaille ja käyttäjille luvattu palvelutaso voidaan tuottaa vaatimusten mukaisesti. Joidenkin reaaliaikaisten palveluiden kohdalla, kuten esimerkiksi puheen tai videon välittämisessä verkon yli voidaan määritellä alhaisin suoritustaso, joka palvelun tuottamiseen tarvitaan. Verkon eri osista ja komponenteista on siis pystyttävä keräämään ja analysoimaan tietoa niin hetkellisistä kuin pidemmän aikavälin muutoksista suorituskykyarvoissa. [27], [1] Suorituskykyyn liittyviä oleellisia kohtia ovat: [26]

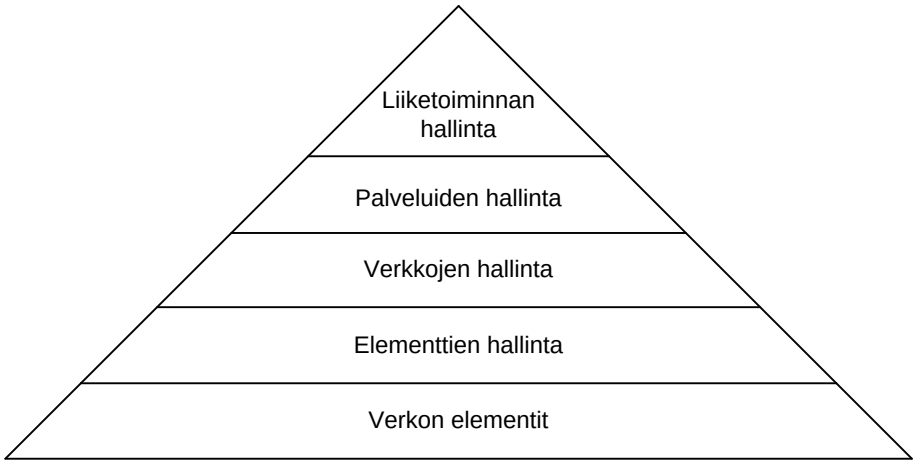
- Verkon kapasiteetin käyttöaste ja kasvu- tai laskutrendit.
- Liikenteen ruuhkautuminen tietyissä verkon osissa.
- Suorituskyvyn riittävä taso ajettaville sovelluksille.
- Vasteaikojen muuttumiset verkon eri osien välillä.

Viides osa FCAPS-mallia on tietoturvallisuuden hallinta *(Security Management)*. Se tarjoaa keinot joilla verkon resurssit ja käyttäjien tiedot turvataan siten, että tiedetään kenellä, mistä ja milloin on oikeus päästä ja käyttää mitäkin verkossa tarjottavaa palvelua. Turvallisuuden hallinta on käytännössä eri lokeista saatavan datan keräämistä ja analysointia sekä pääsynhallintaa. [27], [1]

On hyvä huomioida, että FCAPS-mallin tarkoituksena on tarjota ainoastaan kehyksiä valvottaville ja hallittaville asioille edellä mainituilla osa-alueilla. Painopisteiden asettaminen ja resurssien kohdentaminen niihin jää verkkoa ylläpitävän organisaation vastuulle.

4.1.2 TMN

TMN on ITU-T:n (International Telecommunications Union) määrittelemä viitekehys tietoliikenneverkkojen hallintaan. TMN-malli koostuu hierarkisesta rakenteesta toisin kuin edellä esitelty FCAPS. Alla olevassa kuvassa 15 näkyy hierarkian eri tasot. Tasot ovat alhaalta ylöspäin; verkon elementit, elementtien hallinta, verkkojen hallinta, palveluiden hallinta ja liiketoiminnan hallinta. [4]



Kuva 15. TMN-viitekehys verkonhallintaan. [4]

TMN tarjoaa standardeja laaja-alaisesti yksittäisistä verkon elementeistä lähtien aina ylimälle tasolle liiketoimintaan ja sen avulla yrittää liittää ne toisiinsa. Seuraavaksi käydään läpi tarkemmin mitä nämä eri tasot tarkoittavat. [4]

Verkon elementit kuvaavat varsinaisia fyysisiä komponetteja, joista koko verkko rakentuu. Siinä ei varsinaisesti oteta kantaa minkälainen elementti on kyseessä tai minkälaisella verkonhallintajärjestelmällä sitä voidaan hallita ja valvoa. Elementeillä on tiettyjä ominaisuuksia, joita se itsestään tukee ja joiden kautta sitä voidaan hallita. Valvonnan kannalta tämä tarkoittaa esimerkiksi kytkintä ja siinä olevaa porttia, joka pystyy kytkimen käyttöjärjestelmän kautta tarjottavan rajapinnan myötä tuottamaan itsestään esimerkiksi portin tilatietoa, käyttöastetta tai virheiden määrää. [4]

Seuraava taso, *elementtien hallinta* kokoaa elementit yhteen ja se kattaa käytännössä sellaiset prosessit, joilla elementtejä hallitaan. Toisin sanoen verkonhallintajärjestelmillä voidaan lukea ja muokata elementtien

konfiguraatioita, valvoa niiden hälytyksiä tai komentaa elementit tekemään jotakin haluttua toimintoa. [4]

Verkkojen hallinta –tasolla otetaan edelleen askel kerrosta ylemmäs. Tämä taso tarkoittaa erilaisten suhteiden ja riippuvuuksien hoitamista verkon eri osien ja elementtien välillä. Käytännössä verkkojen hallinnalla pyritään ylläpitämään verkon yhteyksiä ja toiminnallisuutta päästä päähän. Esimerkiksi kun reitittävässä verkossa halutaan tarjota yhteyttä jostakin aliverkosta toiseen, täytyy jokainen verkon elementti, tässä tapauksessa reititin, konfiguroida erikseen, jotta yhteys päästä päähän toimisi. Muutoin reitti alkupisteestä loppupisteeseen ei toimi, jollei kaikkia sen varrella olevia elementtejä ole konfiguroitu oikein tätä toiminnallisuutta varten. Valvonnan kannalta olennaisia asioita tälle kerrokselle ovat mm. liikennevuon tarkastelu jollakin yhteysvälillä. Tämä tarkoittaa sitä, että liikenteen viivettä ja kapasiteettia on voitava valvoa. Verkkojen hallinta –taso käyttää siis hyväksi elementtien hallintaa, jonka avulla elementtejä hallitaan ja tuottaa tämän lisäksi näkyvyyden kokonaisuudesta verkkotasolla. [4]

Neljäntenä tasona on *palveluiden hallinta.* Siellä hallitaan niitä palveluita, joiden tuottamiseen alla oleva verkko osallistuu. Edellä esitetty esimerkki yhteyden muodostamisesta pisteestä A pisteeseen B voisi olla VoIP-puhelinyhteyttä (Voice over IP) varten, joka tarvitaan yrityksen työntekijälle puhelinyhteyttä varten. Palveluiden hallinta kattaa tässä tapauksessa VoIP-palveluun liittyvät toiminnot, jotka tarvitaan, että puhelinyhteys on käytettävissä. Tämä tarkoittaa puhelinnumeron allokointia, yrityksen sisäisen puhelinluettelojärjestelmän päivittämistä ja VoIP-järjestelmän konfigurointia uutta liittymää varten. Vasta näiden toimintojen jälkeen palvelu on vasta käytettävissä, lisäksi alla oleva verkko ja sen elementit on tietysti oltava konfiguroitu oikein tätä palvelua varten. [4]

Ylin kerros, *liiketoiminnan hallinta* liittää yrityksen liiketoiminnan näihin kaikkiin edellä esitettyihin tasoihin. Tämä tarkoittaa mm. laskutuksen hallintaa. [4]

TMN-viitekehyksessä FCAPS:iin verrattuna verkonhallintaa lähestytään hyvin liiketoimintalähtöisesti. Tietoteknisten järjestelmien avulla toteutetaan monenlaista liiketoimintaa ja monesti niiden kriittisyys yritykselle on merkittävä. Esimerkiksi sähköä tuottava energiayhtiö tarvitsee erilaisia tietojärjestelmiä sähkön tuotantoon, jakeluun ja myyntiin liittyen. Eri liiketoimintojen tarpeiden mukaisesti verkkojen pitää voida tuottaa niiden tarvitsemat palvelut. Liiketoiminta määrittelee siis tarpeet ja politiikat verkoille. Verkonvalvonnan kannalta on mielekästä tarkastella kolmea ensimmäistä tasoa: elementtejä, elementtien hallintaa ja verkonhallintaa. Mutta TMN-malli liittää ne vahvasti liiketoiminnan tarpeisiin, joka siis ohjaa näitä alempia tasoja. [29]

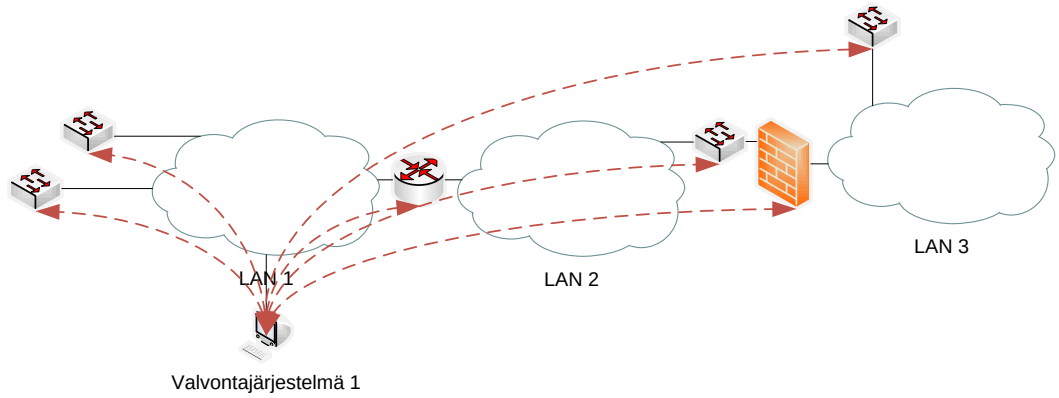
4.2 Valvonta-arkkitehtuuri

Verkonvalvontaa suunniteltaessa on huomioitava olemassa oleva tietoliikenneverkkoarkkitehtuuri sekä valvontaan käytössä olevat järjestelmät ja niiden ominaisuudet.

Verkon ja siihen liitettyjen järjestelmien luonteesta riippuen on olennaista miettiä, voidaanko valvontaliikennettä ajaa samassa verkossa tuotantoliikenteen kanssa vai onko tarpeellista eriyttää ne täysin omiksi verkoikseen. Suuremmissa verkkoympäristöissä valvontaliikenne voi aiheuttaa jo kohtalaisia liikennemääriä joihinkin verkon osiin, ne voivat olla jossain mielessä haitallisia tuotantoliikenteelle. Toinen olennainen asia on valvontamalli, tehdäänkö se keskitetysti yhdestä pisteestä vai hajautetusti eri puolilta verkkoa. Näitä malleja vertaillaan seuraavissa alakappaleissa.

4.2.1 Keskitetty valvonta

Keskitetystä valvonnasta puhutaan silloin, kun kaikki valvontaliikenne verkon eri komponenteille kohdistuu yhteen pisteeseen. Tyypillisesti tämän mallin valvontajärjestelmä on suuri ja se on rakennettu mahdollisimman vikasietoiseksi. Alla olevassa kuvassa 16 on esitetty keskitettyä verkonvalvontamallia ja siinä on kuvattu punaisilla katkoviivoilla valvonnan aiheuttamat liikennevuot.



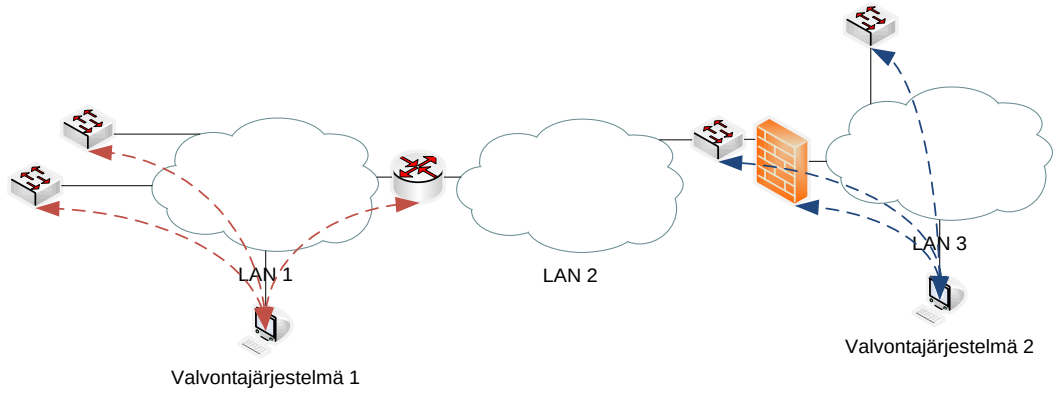
Kuva 16. Keskitetty valvontamalli. [1]

Keskitetyn valvonnan ilmeinen hyöty on sen pienet kustannukset, koska vain yksi järjestelmä tarvitaan kattamaan koko verkonvalvonta. Toisaalta suuressa ja kriittisessä verkkoympäristössä keskitetty valvontamalli muodostuu yksittäiseksi vikapisteeksi ja kun se pettää, niin koko valvontanäkymä menetetään kerralla. Lisäksi suuremmissa verkkoympäristöissä, joissa valvottavien laitteiden määrä koostuu tuhansista kytkimistä ja reitittimistä, voi valvontaliikenne aiheuttaa ongelmia muulle verkkoliikenteelle. [1]

4.2.2 Hajautettu valvonta

Hajautetulla valvonnalla tarkoitetaan ympäristöä, jossa valvontajärjestelmiä on asetettu useampia eri puolille verkkoa. Strategisesti valituilla sijanneilla voidaan saada erilaisia etuja keskitettyyn valvontaan nähden.

Alla olevassa kuvassa 17 on esitetty hajautettu valvontamalli, jossa näkyy lokalisoitunut valvontaliikenne ja eriytetyt valvonta-alueet. Lokalisoitunut valvontaliikenne vähentää siirrettävän valvontadatan määrää ympäri koko verkkoa. Eriytetyillä valvonta-alueilla voidaan saavuttaa parempi vikasietoisuus kun toisen järjestelmän pettäessä saadaan verkon tilasta vielä osittainen kuva. Tarvittaessa valvontajärjestelmät voidaan konfiguroida myös niin, että ne pystyvät vikatilanteessa hoitamaan oman alueensa lisäksi myös toisen alueen. [1]

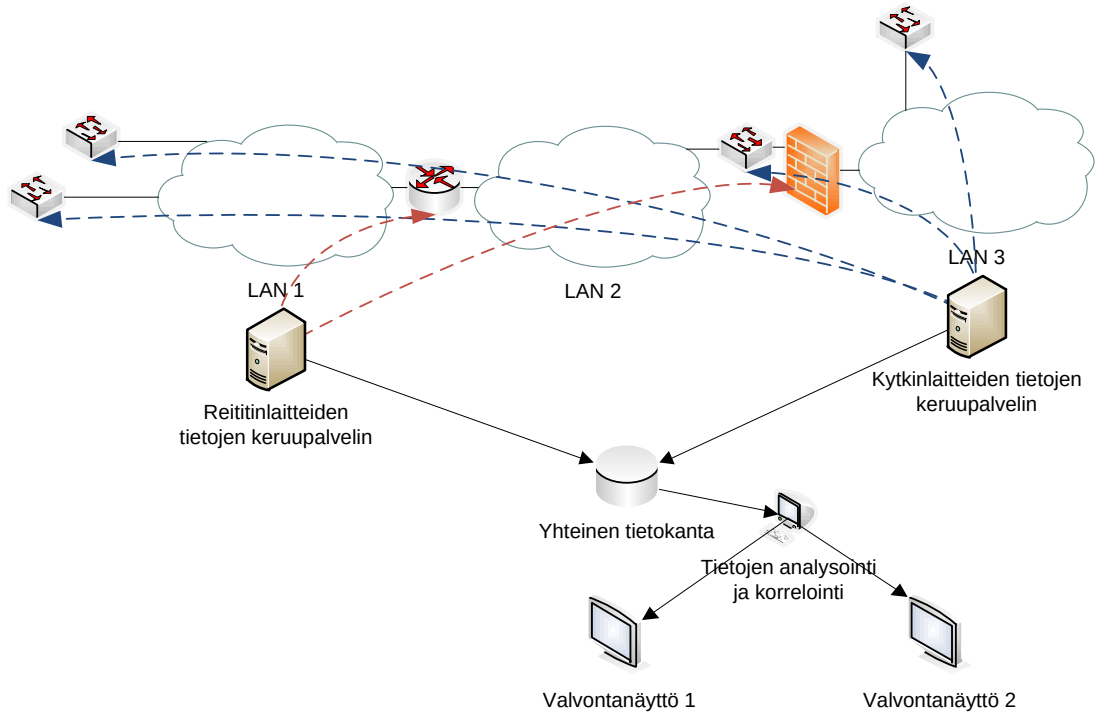


Kuva 17. Hajautettu valvontamalli. [1]

Hajautetussa mallissa valvontajärjestelmiä tarvitaan useampia, jolloin hankinta- ja ylläpitokustannukset ovat luonnollisesti korkeammat. Myös koko valvontasysteemin kompleksisuus kasvaa kun järjestelmiä on useampia.

4.2.3 Hierarkkinen valvontamalli

Kolmantena mallina edellä esiteltyjen lisäksi on olemassa hierarkkinen valvontamalli. Tällä tarkoitetaan valvontaan sisältyvien eri prosessien eriyttämistä eri laitteisiin ja mahdollisesti hajauttamista eri puolille verkkoa. Valvontaan liittyviä prosesseja ovat laitteiden monitorointi, valvontadatan prosessointi, säilytys ja esittäminen.



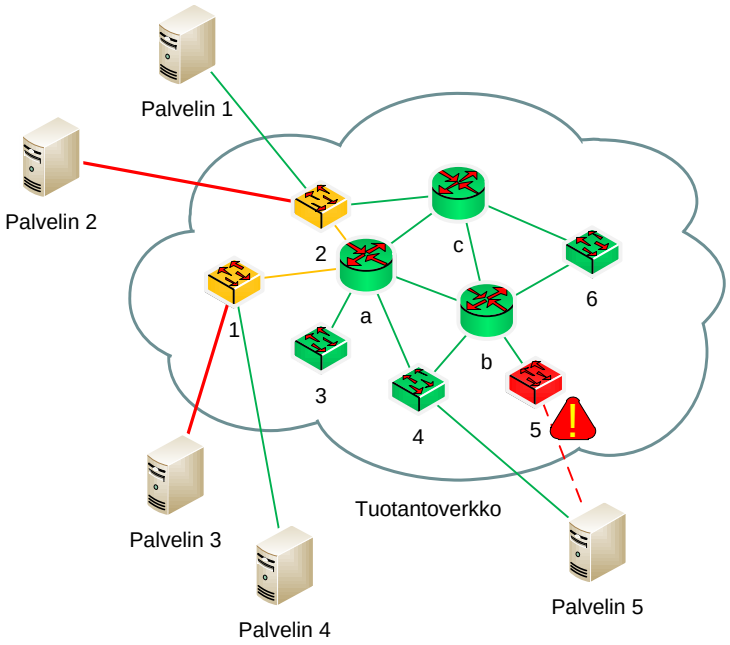
Kuva 18. Hierarkkinen valvontamalli, jossa on hajautettu eri toimintoja erillisille tasoille. [1]

Hierarkkisessa mallissa verkkoympäristöön istutetaan kerääviä komponentteja, jotka monitoroivat verkon laitteita ja lähettävät keräämänsä datan tietokantaan, jossa dataa säilytetään. Korrelointikomponentit prosessoivat dataa edelleen loppukäyttäjälle ystävällisempään muotoon suodattamalla siitä olennaisen osan ja lopuksi ne päätyvät yksinkertaisempiin valvontatyöasemiin, joiden tarkoituksena on vain näyttää valvontadataa. [1] Yllä olevassa kuvassa 18 on havainnollistettu hierarkkisen mallin eri komponentit ja niiden väliset relaatiot.

Tässä mallissa hyvänä puolena on mahdollisuus korkeaan vikasietoisuuteen ja räätälöintiin monimutkaisiin ja erittäin suuriin verkkoympäristöihin. Haittapuolena ovat korkeat kustannukset ja hyvin kompleksinen valvontaympäristö. [1]

4.3 Valvottavat ja mitattavat asiat

Verkkolaitteissa tapahtuu jatkuvasti erilaisia tapahtumia, joista toiset ovat kriittisyysasteeltaan vähäisempiä ja toiset suurempia. Jotta verkkoon liitetyille prosessijärjestelmille voidaan taata luotettava toimintavarmuus ja jatkuvuus, täytyy verkon eri ominaisuuksia pystyä valvomaan. Verkosta ja siihen liittyviltä laitteilta on pystyttävä mittaamaan mm. tavoitettavuutta, liikenteen määriä, liikenteen kulkuaikaviiveitä verkon eri osissa ja siirtovirheiden määriä. Tietoa on pysyttävä keräämään ja näyttämään hetkellisarvoina mutta myös pidemmän aikavälin trendeinä, jotta kokonaiskuva ja kehityssuuntaa voidaan seurata. [4]



Kuva 19. Verkkolaitteiden valvonta ja näkymä.

Kytkimissä, reitittimissä, palomuureissa ja muissa tietoliikennelaitteissa on syytä pystyä tekemään seurantaa porttitasolle asti. Tällöin voidaan havaita pullonkauloja tai ennakoida kasvavien liikennemäärien perusteella mahdollisia kapasiteetin lisäyksiä. Yllä olevassa kuvassa 19 on esimerkkitilanne, jossa verkonvalvontajärjestelmistä saatavien tietojen perusteella on syntynyt kuvitteellinen tilannekuva. Kuvassa punaiset linkit esittävät suurta käyttöastetta ja keltaiset keskitason käyttöastetta. Vihreät linkit toimivat normaalisti asetettujen raja-arvojen sisällä. Kuvasta voidaan havaita, että kytkimiin 1 ja 2 liitetyt palvelimet 2 ja 3 aiheuttavat suurta liikennemäärää ja niiden välisiin yhteyksiin pitäisi lisätä kapasiteettia, jotta muissa verkkoon liitetyissä

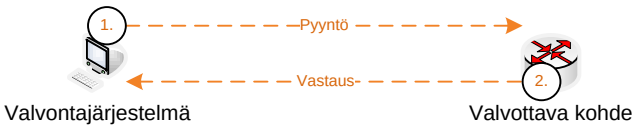
palvelimissa toiminta ei häiriintyisi. Lisäksi palvelimeen 5 on menetetty yhteys kokonaan linkkivian takia. Verkonvalvontajärjestelmän pitäisi pystyä esittämään tilanne esimerkkikuvan mukaiseti, jossa punainen tarkoittaa kriittistä hälytystä, keltainen jonkinlaista poikkeustilannetta ja vihreä kuvaa normaalia toimintatilaa. Kriittisyys ja hälytysrajat erilaisten tapahtumien perusteella on pysyttävä asettamaan tapauskohtaisesti.

Tämän kaltaisia tilannekuvia verkonvalvonnalla halutaan saada, jotta ylläpitäjät pystyvät muodostamaan vikatilanteissa nopeasti tilannekuvan ja käynnistämään oikeat toimenpiteet tilanteiden korjaamiseksi. Verkon topologia- ja tilannekuvien täytyy olla riittävän selkeitä ja helppolukuisia, jotta ylläpitäjät pystyvät nopeasti erottamaan kriittiset viat vähemmän kriittisimmistä reagoimaan niihin tarpeen mukaan.

Seuraavissa alakappaleissa on käsitelty tarkemmin erilaisia verkonvalvontaan käytettäviä protokollia, joilla verkon tilaa voidaan valvoa. Lisäksi työhön on nostettu kaksi muuta protokollaa, jotka ovat tärkeässä asemassa verkon ja siihen liitettyjen järjestelmien toiminnan ja vikasietoisuuden kannalta.

4.3.1 Valvontaliikenne

Kappaleessa 4.2 käytiin läpi erilaisia arkkitehtuureja, joiden päälle varsinainen järjestelmä rakentuu ja joka toteuttaa valvontaa. Kaikille valvonta-arkkitehtuureille on yhtenäistä valvontajärjestelmän ja valvottavan kohteen välinen tiedonvaihto. Tapoja valvoa laitteita tai saada tietoa niiltä on itse asiassa kaksi, kysely- ja tapahtumapohjainen. [4]



Kuva 20. Kyselypohjainen valvonta. [4]

Yllä olevassa kuvassa 20 on yleinen esitys pyyntö- ja vastausinteraktiosta. Tyypillisesti valvontajärjestelmästä lähetettävistä pyynnöissä (kuva 20, kohta 1) määritellään vähintäänkin seuraavat asiat: [4]

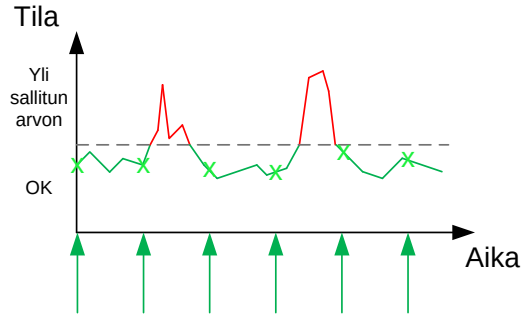
- Pyynnön tyyppi.
- Pyyntöön liittyvät parametrit, joilla siihen voidaan vastata.
- Muita valvontaan liittyviä parametreja, esimerkiksi tunnistautumiseen vaadittavat tiedot tai salausavaimet, joilla voidaan varmentua pyynnön lähettäjän oikeellisuudesta.

Vastaavasti valvottava kohde vastaa viestillä (kuva 20, kohta 2), josta ilmenee vähintäänkin seuraavat asiat: [4]

- Vastauskoodi, josta ilmenee oliko lähetetty pyyntö onnistunut. Jos pyyntö oli virheellinen, palautetaan jokin syy mistä virhe johtui.
- Vastaus pyyntöön. Esimerkiksi palautetaan jokin pyydetty lukuarvo.
- Muita valvontaan liittyviä parametreja, mm. tunniste, jolla valvontajärjestelmä osaa sovittaa saamansa vastaukset lähettämiinsä pyyntöihin.

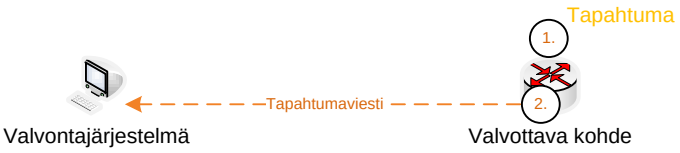
Tämän tyyppisillä viesteillä voidaan helposti saada reaaliaikaista tietoa laitteen tilasta, diagnosoida sitä erilaisissa vianselvitystilanteissa tai kohdentaa kyselyitä johonkin erityiseen asiaan ja mitata sitä. Kyselemällä esimerkiksi kytkimen portin käyttöastetta säännöllisin väliajoin, esimerkiksi 15 minuutin välein, voidaan helposti tuottaa seuraavalla sivulla näkyvän kuvan 21 mukaista kuvaajaa. Kuvaajasta voidaan seurata liikennemäärää ja sen kehitystä. Toisaalta kuvasta nähdään myös kyselypohjaisen valvonnan yksi merkittävä ongelmakohta. Jos mittausväli on liian suuri, niin kyselyiden väliin voi jäädä kriittinen tilanne kun portin liikennemäärä ylittää sille asetetun raja-arvon.

Valvontajärjestelmä ei huomaa tätä, eikä täten pysty generoimaan siitä merkintää, jonka myötä kapasiteettia voitaisiin tarvittaessa kasvattaa. [4]



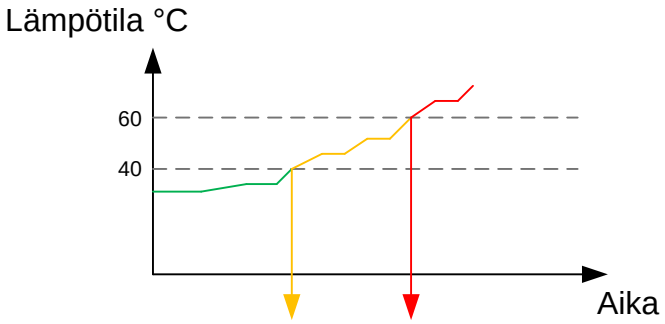
Kuva 21. Kyselypohjaisen valvonnan ongelma. [4]

Toinen tapa, jolla valvontajärjestelmä ja valvottava kohde keskustelevat on tapahtumiin perustuva valvottavalta kohteelta lähtevä viestitys. Tapahtumapohjainen valvonta perustuu valvottavassa kohteessa esiintyviin tapahtumiin, joista osa määritellään sellaisiksi, että kun niissä tapahtuu muutoksia tai jokin sallittu raja-arvo ylitetään, käynnistetään jokin toimenpide. (kuva 22)



Kuva 22. Tapahtumapohjainen valvonta. [4]

Valvontamielessä tyypillisesti toimenpide tarkoittaa tiedon lähettämistä valvontajärjestelmälle, mutta laitteet voivat myös tarvittaessa tehdä automaattisesti itsenäisiä toimia tilanteen korjaamiseksi. [4]



Kuva 23. Tapahtumapohjainen valvonta laitteen lämpötilasta ja hälytysten laukaisu ennalta määrättyjen raja-arvojen kohdilla. [4]

Yllä olevassa kuvassa 23 on esimerkkitilanne laitteesta, joka valvoo itse itsensä lämpötilaa. Valvontajärjestelmässä on määritetty normaaliksi lämpötilaksi alle 40 astetta. Lisäksi on määritelty kaksi raja-arvoa 40 ja 60 astetta. Ensimmäisen raja-arvon ylittyessä laite voi lähettää valvontajärjestelmälle hälytyksen koskien nousevaa lämpötilaa. Jos tähän ei reagoida ja lämpötila jatkaa nousuaan, voidaan laite määritellä sammuttamaan itsensä jos lämpötila nousee yli 60 asteen, jolloin vältytään mahdollisesti suuremmilta ongelmilta. Tapahtumapohjainen valvonta auttaa siis reagoimaan tilanteisiin välittömästi kun ne syntyvät ja antavat verkon ylläpitajille enemmän aikaa reagoida ja aloittaa toimet. Toisaalta tämänkaltainen äly ja ohjelmoitavuus vaativat valvottavalta laitteelta enemmän ominaisuuksia.

Tässä kappaleessa käytiin läpi valvontaliikenteen anatomiaa ja vertailtiin kysely- ja tapahtumapohjaisia malleja. Seuraavissa alakappaleissa 4.4.1 – 4.4.3 käydään läpi valvontaprotokollia, joista osa toimii kyselypohjaisesti ja osa tapahtumapohjaisesti.

4.4 Valvontaan soveltuvia protokollia

Valvontajärjestelmät keskustelevat valvottavien kohteiden kanssa erilaisilla protokollilla. Protokollia tarvitaan valvontadatan siirtoon ja varsinaisiin valvontaan liittyviin mittauksiin ja ohjauksiin, joita voidaan tehdä useilla eri tavoilla. Seuraavissa kappaleissa käydään tarkemmin läpi eri protokollia ja pyritään löytämään niistä olennaiset asiat verkonvalvonnan kannalta. Seuraavaksi läpi käytävät protokollat ovat käytössä Helsingin Energian prosessiverkkoympäristössä ja niillä on suuri merkitys valvonnan toiminnan kannalta.

4.4.1 ICMP

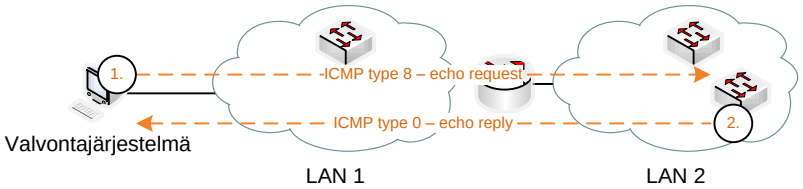
ICMP (Internet Control Message Protocol) on IP-protokollaan (Internet Protocol) sisäänrakennettu ominaisuus, jolla laitteet voivat verkossa informoida erilaisista vika- ja poikkeustilanteista.Käytössä olevia erilaisia ICMP-viestityyppejä on 11 ja ne ovat listattuna alla olevassa taulukossa 1. [30]

Taulukko 1. Yhteenveto eri ICMP-viestityypeistä. [30]

0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply

IP-protokollaa ei itsessään ole suunniteltu täysin luotettavaksi protokollaksi. ICMP-viestien tarkoitus on välittää tietoa erilaisista ongelmista IP-verkoissa. Näiden ominaisuuksien ja yksinkertaisuutensa myötä se on erinomainen protokolla myös verkonvalvontaan ja mm. viiveiden mittaamiseen. [30]

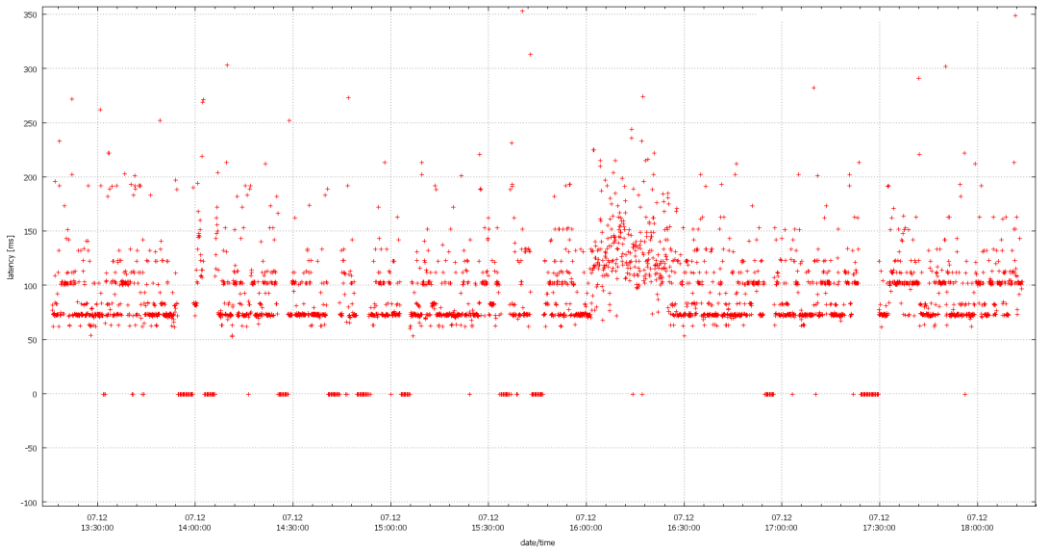
Yksi hyvin tyypillinen tapa, miten valvontajärjestelmät käyttävät ICMP-protokollaa hyväkseen on lähettää tyypin 8 viestejä, eli echo request –paketteja valvottavalle kohteelle. Normaalitilanteessa kohde vastaa tyypin 0 viestillä, echo reply -viestillä. (kuva 24)



Kuva 24. ICMP echo request ja echo reply.

Seuraavalla sivulla kuvassa 25 on esitetty mittaustuloksia Helsingin Energian kulunvalvontajärjestelmään liittyvän palvelimen ja ala-aseman välisen liikenteen kulkuaikaviiveestä. Mittaus on toteutettu Linux-pohjaiselta palvelimelta

erillisellä tätä tarkoitusta varten tehdyllä skriptillä. Tämä yksinkertainen skripti mittaa kulkuaikaviivettä kohdekoneeseen ja ottaa tuloksen ylös aikaleimattuna. Jos mitattava kohde ei vastaa, skripti kirjaa arvon ”-1”. Kuvasta nähdään, että siirtotienä käytettävän UMTS-verkon normaali viive on noin 70ms. Tämä viive sisältää 256-bittisen AES-salauksen (Advanced Encryption Standard). Toinen selkeä kohta, johon viive näyttäisi asettuvan on 100 ms. Tämä ilmiö johtunee UMTS-verkon ominaisuuksista, joilla se säätelee verkossa kulkevia yhteyksiä erilaisia kuormitustilanteissa. Lisäksi nähdään, että yhteydessä esiintyy noin 4 minuutin mittaisia katkoksia keskimäärin tunnin välein.



Kuva 25. ICMP-mittauksia palvelimelta ala-asemalle, joiden välinen yhteys toteutettu IPSec L2L-tunnelina UMTS-verkon yli.

Kun mittaustulosten perusteella tiedetään mikä on verkosta johtuva latenssi ja pakettihäviö, niin näitä tietoja voidaan käyttää hyväksi päällä ajettavan kulunvalvontasovelluksen virittämiseen tälle kohteelle. Jos sovellus vaatisi normaalisi, että ala-aseman ja palvelimen välinen viive ei saa olla yli 100 ms niin tästä nähdään välittömästi, että tällä yhteydellä kulunvalvontajärjestelmä ei tulisi toimimaan kyseisessä paikassa kovin luotettavasti. Kulunvalvontajärjestelmää voidaan teoriassa kuitenkin muokata niin, että se sallii suurempia viiveitä ja voi toimia itsenäisesti jonkin aikaa, vaikka sillä ei olisikaan yhteyttä palvelimelle.

Edellä mainittujen tietojen avulla kulunvalvontajärjestelmän virittäminen antaa joustavuutta ja mahdollistaa sovelluksen käytön verkon yli, jossa viive vaihtelee

ja paketteja häviää kohtalaisen paljon. Näillä muokkauksilla kulunvalvontajärjestelmä saadaan toimimaan ja tästä muodostuu myös konkreettinen tarve valvoa siihen liittyviä tietoliikenneyhteyksiä.

4.4.2 SNMP

SNMP (Simple Network Management Protocol) on IETF:n (Internet Engineering Task Force) kehittämä protokolla verkonhallintaan. SNMP perustuu muutamaan yksinkertaiseen operaatioon, jotka tarjoavat ylläpitäjille mahdollisuudet hallita ja valvoa IP-pohjaisia laitteita. Tyypillisiä SNMP:n käyttötarkoituksia voisi olla esimerkiksi kytkimen portin sulkeminen tai avaaminen, portin nopeuden tarkastaminen, läpi kulkevan liikenteen seuraaminen tai laitteen lämpötilan tarkkailu. [23]

SNMP:n ensimmäinen versio 1 kehitettiin vuonna 1988 vastaamaan kasvaviin tarpeisiin hallita IP-pohjaisia laitteita. 1990-luvulla kehitettiin myös toista, vahvasti OSI-malliin pohjautuvaa verkonhallintaan tarkoitettua CMIP-protokollaa (Common Management Information Protocol). OSI-mallin raskaudesta johtuen ja toisaalta SNMP:n yksinkertaisuuden takia CMIP jäi taka-alalle IP-pohjaisissa verkoissa ja SNMP vakiinnutti asemansa verkonhallintaprotokollana IP-pohjaisissa tietoliikennelaitteissa. [5], [31]. SNMP versio 2 ja nykyinen versio 3 ovat kehittyneempiä versioita protokollasta, joissa on panostettu erityisesti tietoturvaominaisuuksiin. SNMP:n viimeisin versio 3 on julkaistu vuonna 1999 ja siinä on kehitetty erityisesti seuraavia osa-alueita: [23], [32]

- Autentikointi ja yksityisyys (salattu tiedonsiirto).
- Valtuutus ja katseluperusteinen pääsynhallinta.
- Standardoitu etähallinta.

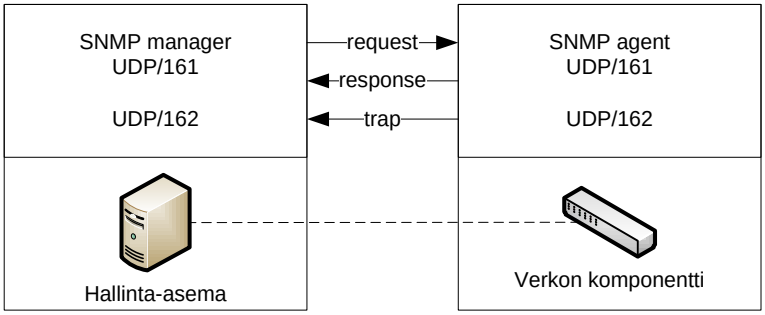
Näillä kehitystoimenpiteillä on pyritty parantamaan erityisesti tietoturvaa, sillä enää ei voida olettaa, että uhat tulisivat ainoastaan yrityksen verkon ulkopuolelta. Verkon sisäpuoleltakin voi kohdistua tietomurtoja ja hyökkäyksiä verkon infrastruktuuriin. Varsinaisesti protokollan toiminnassa ei ole tapahtunut suuria muutoksia. [23]

SNMP toimii yhteydettömän UDP-protokollan (User Datagram Protocol) päällä. UDP ei varmista pakettien perille menoa päästä päähän joten se jää SNMP:n vastuulle. Tyypillisesti tämä on huomioitu valvontajärjestelmissä aikakatkaisujen avulla. SNMP on suunniteltu helposti käyttöönotettavaksi ja vähän laitteiden ja verkon resursseja kuluttavaksi. SNMP:n perusoperaatiot ovat listattu alla olevassa taulukossa 2.

Taulukko 2. SNMP-operaatiot ja niiden merkitykset. [23]

Operaatio	**Merkitys**
Get	Hallinta-asema hakee tietueen operoitavan kohteen MIB-tietokannasta.
Set	Hallinta-asema asetettaa tietueelle jokin arvo operoitavan kohteen MIB-tietokantaan.
Trap	Verkon komponentti lähettää viestin (hälytyksen) hallinta-asemalle.
Inform	Hallinta-asema lähettää viestin (hälytyksen) toiselle hallinta-asemalle.

Alla olevassa kuvassa 26 on kuvattu SNMP:n toimintaperiaate, jossa näkyy miten hallinta-asemalta voidaan lähettää pyyntö valvottavalle komponentille, joka vastaa siiheen response-sanomalla. Lisäksi verkon komponentit voivat lähettää trap-sanomia erilaisten tapahtumien myötä, jotka voidaan erikseen määritellä laitekohtaisesti. Objektit, joita SNMP:n avulla voidaan valvoa ja hallita verkkolaitteissa, määritellään laitteiden paikallisissa MIB-tietokannoissa (Management Information Base). [23]



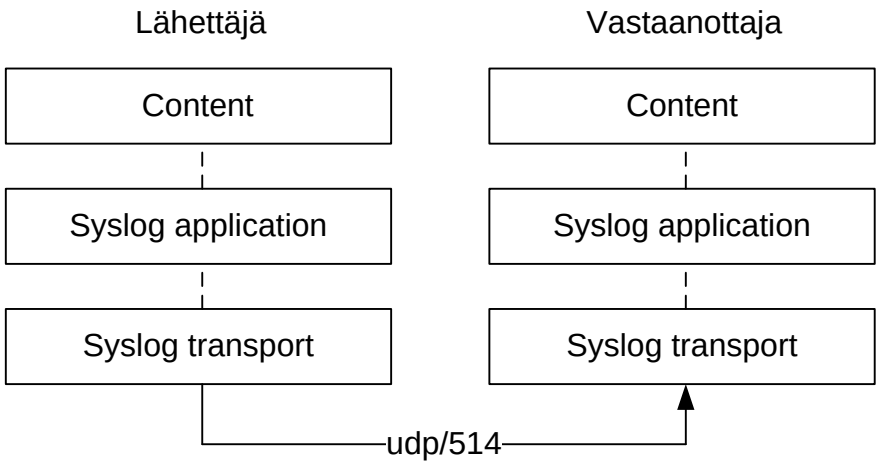
Kuva 26. SNMP:n toimintaperiaate, request, response ja trap -sanomat. [23]

MIB on hierarkkinen tietokanta valvottavan komponentin objekteista, jossa määritellään tietueet esimerkiksi verkkolaitteiden rajapintojen nopeuksille, lähetetyille ja vastaanotetuille tavuille sekä porttien tiloille. [23]

4.4.3 Syslog

Syslog on protokolla, jonka tarkoituksena on kirjoittaa järjestelmäviestejä (system messages) lokiin. Syslog on sovellustason protokolla ja se tarjoaa kehyksen erilaisille järjestelmäviesteille, joita eri laitevalmistajat voivat hyödyntää laitteissaan. Standardoidun protokollan avulla eri laitevalmistajien viestit voidaan rakentaa jäsenneltyyn formaattiin ja koota yhteen. [33]

Syslogin toiminta perustuu kolmeen eri kerrokeen, joilla on jokaisella oma tehtävänsä viestien välityksessä. Nämä kerrokset ovat esitetty alla kuvassa 27 ja ne ovat *syslog content* eli viestin sisältö, *syslog appliaction*, joka viittaa viestejä käsittelevään sovellukseen sekä *syslog transport*, jonka alla viestit lähetetään ja vastaanotetaan käyttäen hyväksi jotakin siirtotietä.

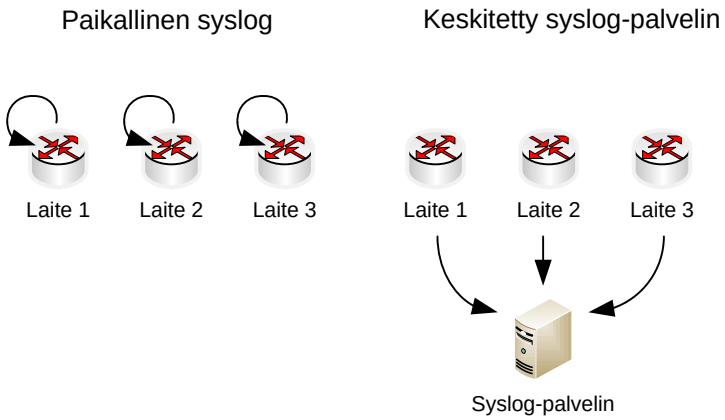


Kuva 27. Syslog-protokollan toimintaperiaate ja eri kerrokset. [33]

Sisältö käsittää valvottavaan tai hallittavaan järjestelmään liittyvän informaation, joka halutaan kerätä talteen lokiin.

Syslog voi toimia paikallisesti laitteen sisällä, jolloin se kerää järjestelmäviestejä paikalliseen tiedostoon tai tietokantaan. Monet verkkolaitteet tekevät usein hyvin paljon ja erilaisia syslog-viestejä, alkaen kriittisistä hälytyksistä ja päättyen hyvinkin informatiivisiin viesteihin, joilla ei välttämättä ole kovinkaan paljon arvoa. Jotta syslog-viestien keruu ja analysointi olisi suuremmissa verkkoympäristöissä järkevää, kannattaa ne ohjata keskitetylle syslog-palvelimelle. Alla olevassa kuvassa 28 on esimerkiksi ohjattu kaikki viestit

erilliselle syslog-palvelimelle, jossa niitä voidaan säilyttää pidemmältä ajanjaksolta ja jalostaa niistä oleellinen informaatio eteenpäin.



Kuva 28. Syslog-viestien keruu paikallisesti tai keskitetyn syslog-palvelimen käyttö. [33]

Systemaattinen syslog-viestien keräämiselle voidaan keksiä useita tarpeita. Ne helpottavat vikatilanteissa ongelman selvittelyä tai niiden avulla voidaan seurata eri asioiden kehittymistä tai muuttumista pidemmällä aikavälillä. Usein verkkoympäristöissä tulee vastaan tilanteita, joissa on tärkeää saada koottua eri laitteiden viestit yhteen näkymään, joiden avulla pystytään tekemään oikeita johtopäätöksiä ja niistä edelleen tarvittavia toimenpiteitä tilanteen korjaamiseksi. [33], [4]

5 Johtopäätökset

Diplomityössä tutkittiin tuotantokriittisten verkkojen valvontaa, kahta erilaista viitekehystä, joita voidaan käyttää verkonvalvonnan tukena sekä esiteltiin Helsingin Energian tuotantokäytössä olevaa prosessiverkkoympäristöä. Tässä kappaleessa esitetään johtopäätökset ja pohditaan erilaisia näkökulmia kolmanteen tutkimuskysymykseen, *miten valvontaa voidaan toteuttaa ja kehittää Helsingin Energian ympäristössä?*

Helsingin Energian tuotantokriittisten prosessijärjestelmien kannalta verkkoympäristön käytettävyys- ja luotettavuusvaatimukset ovat erittäin korkealla tasolla. Prosessijärjestelmät, joita verkossa ajetaan, liittyvät hyvin olennaisesti kriittiseen infrastruktuuriin, mm. sähkön- ja lämmön tuotantoon. Tämän kaltaisissa tietojärjestelmissä häiriöillä voi olla erittäin vakavia seurauksia. Saatavuutta, käytettävyyttä ja luotettavuutta on pysyttävä seuraamaan ja niistä on voitava luoda raportteja pidemmän aikavälin trendejä. Reaaliaikaiset tuotannonohjausjärjestelmät ja sähkökauppajärjestelmät sähköpörssissä vaativat liikenteen kulkuajan suhteen viiveettömyyttä ja stabiiliutta eri verkkojen välillä. Turvallisuuteen liittyvissä kamera- ja kulunvalvontajärjestelmissä verkon on pystyttävä tarjoamaan riittävästi kapasiteettia mm. reaaliaikaiseen videovalvontaan ja kiinteistönohjaukseen. Monimutkaisessa verkkoympäristössä tämänkaltaisten asioiden valvominen ei ole aivan yksiselitteinen asia.

Jotta edellä mainitun kaltaisia asioita voidaan valvoa, verkonvalvontajärjestelmillä on kerättävä dataa useista eri lähteistä ja niistä on pystyttävä koostamaan se olennainen tieto luettavaan ja ymmärrettävään muotoon. Helsingin Energian prosessiverkkoympäristössä on kehitettävä verkonvalvontaa reaktiivisesta valvonnasta proaktiiviseen valvontaan, jossa osana ovat erilaiset automatisoidut verkon valvontajärjestelmät. Kun verkkoympäristön koko ja monimutkaisuus kasvaa useista sadoista laitteista koostuvaksi kokonaisuuksiksi, on automatisoitujen järjestelmien käyttö perusteltua. Vaikka niistä aiheutuukin kustannuksia ja ne vaativat ylimääräistä työpanosta, saadaan niiden avulla tarvittavaa tietoa, jolla ylläpitäjät pystyvät tarjoamaan prosessijärjestelmien vaatimaa luotettavuutta ja käytettävyyttä.

Verkonvalvonnan on pystyttävä tuottamaan eritasoisia näkymiä verkon tilasta. Ylätason näkymässä on pyrittävä yksinkertaiseen tilannekuvaan, josta nähdään helposti yhdellä silmäyksellä onko verkossa kaikki kunnossa, jokin matalan tason vikatilanne päällä vai korkean tason vika, joka vaatii välitöntä reagointia. Tällaisesta näkymästä on voitava pureutua verkon eri osiin ja aina yksittäisiin laitteisiin asti. Verkon kehityksessä ja laitevalinnoissa on syytä huomioida niiden yhteensopivuus verkonvalvontajärjestelmien kanssa, jotta laitteet ja valvontajärjestelmät integroituvat toisiinsa myös tulevaisuudessa. Verkonvalvontaan on kehitetty erilaisia viitekehyksiä, jotka antavat ohjeistuksia ja kehyksiä valvottaville asioille eri osa-alueilla. FCAPS-malli on hyvä lähtökohta, joka tarjoaa laaja-alaisesti ohjeistuksia viidellä eri osa-alueella vikojen, kokoonpanon, laskutuksen, suorituskyvyn ja tietoturvallisuuden hallintaan. Verkonvalvonnan pitää olla olennaisena osana jokaisessa näissä osa-alueessa. FCAPS-mallin sisältö on hyvin konkreettisella tasolla esitetty ja sitä voidaan käyttää tukena erilaisten prosessien kehittämiseen näillä osa-alueila. TMN-mallissa sen sijaan on onnistuttu esittämään hyvin verkkojen ja niiden valvonnan liittyminen ja vaikutukset liiketoimintaan. Tämä on olennainen asia Helsingin Energian, ja etenkin ICT-palveluiden kannalta, jonka tarkoituksena on tuottaa ydinliiketoiminnoille niiden tarvitsemia palveluita. Yhteys tuotettavasta palvelukokonaisuudesta aina liiketoiminnan jatkuvuuteen liittyviin kysymyksiin auttaa nostamaan verkonvalvonnan tärkeyttä.

Helsingin Energialla prosessiverkkoympäristö on eriytetty omaksi kokonaisuudekseen toimistoverkosta. Tämä on linjassa työssä esitetyn hajautetun valvontamallin kanssa. Toimistoverkkoympäristö ja prosessiverkkoympäristö ovat kaksi erillistä kokonaisuutta, omine fyysisine verkkoineen ja valvontajärjestelmineen.

Työssä käytiin läpi yksityiskohtaisesti ProLAN-verkkoarkkitehtuuria, sen toimintaperiaatteita ja erilaisia protokollia, jotka mahdollistavat valvontaan käytettävän datan keräämistä verkosta ja verkkolaitteilta. Tarkemmin analysoitaessa ja prosessijärjestelmien erityisvaatimukset taustalla pitäen voidaan todeta, että verkonvalvontajärjestelmät täytyy virittää Helsingin Energian tarpeita

vastaaviksi. ProLAN-verkkoympäristössä yhtenä olennaisena perusperiaattena on tarjota kahdennettu ja automaattisesti vikatilanteista toipuva alusta eri järjestelmille. Tällaisissa ratkaisuissa on käytetty dynaamisia reititysprotokollia. Reititystietojen valvontaan pitäisi jatkokehittää jonkinlaisia mekanismeja, joilla aktiiviset reitit, uudelleen reititykset ja niihin liittyviä muutoksia voidaan valvoa ja todentaa. Vianselvityksen kannalta on olennaista tietää, mitkä verkon komponentit ovat olleet aktiivisina vikatilanteiden aikana ja tätä kautta päästä nopeammin ongelman jäljille ja selvittää se.

Työn edetessä selkeni kokonaiskuva Helsingin Energialla käytössä olevista verkonvalvontajärjestelmistä ja mihin kaikkeen niitä voidaan mahdollisesti käyttää. Ongelmana eivät ole niinkään puuttuvat tai huonosti toimivat valvontajärjestelmät vaan näiden järjestelmien suunnitelmallinen käyttö ja valvontaan liittyvät prosessit. Tämä tarkoittaa automatisoitujen järjestelmien ja ylläpitäjien toimintaa erilaisissa tilanteissa ja tapahtumien suodatusta. Kappaleessa 1.3.2 on esitetty, että valvontaa voi toteuttaa ihminen, automatisoitu järjestelmä tai tilanteen mukaan molemmat yhdessä. Helsingin Energialla ei ole erillistä verkkovalvomoa tai -keskusta. Automaattiset järjestelmät eivät tuota lisäarvoa ylläpitäjille, jos niitä ei kohdenneta oikein tai niistä saatavaa tietoa ei käytetä mihinkään. Verkonvalvontaa pitää kehittää siihen suuntaan, että sen avulla pystytään ennakoidusti havaitsemaan nousevat liikennemäärät tai viiveet eri verkon osissa. Tämänkaltaisten tietojen avulla ylläpitäjät pystyvät käynnistämään tarpeelliset muutokset verkon parantamiseksi ennen kuin tilanne pääsee siihen pisteeseen, jossa se ei enää pysty tarjoamaan sille asetettuja luotettavuus- ja käytettävyysvaatimuksia. Verkonvalvontajärjestelmien toimivuuden varmistamiseksi on oltava prosessit, joilla hälytystietojen edelleenlähetys päivystäjille voidaan taata. Tämä on ehdoton edellytys sille, että tapahtumiin voidaan reagoida. Kokonaisuutena tämänkaltainen kehityssuunta tarkoittaisi valvomotoiminnan ja valvomon kehittämistä Helsingin Energian prosessiverkkoympäristössä.

Verkonvalvonnan tarkoituksena ei ole ainoastaan palvella sen ylläpitäjiä vaan valvontajärjestelmät tulee toteuttaa niin, että niistä on mahdollista saada tietoa myös sellaisessa muodossa, että sillä voidaan raportoida asiakkaille palveluiden

saatavuudesta ja luotettavuudesta. Optimaalisessa tilanteessa eri prosessijärjestelmien vaatimukset verkolle olisi pystyttävä kuvaamaan hyvinkin tarkasti ja näiden vaatimusten täyttymistä voitaisiin seurata säännöllisillä raporteilla ja auditoinneilla. Käytännössä näin ei useinkaan ole vaan vaatimukset ovat yleisemmällä tasolla ja tuotettava palvelu ja siihen liittyvä verkko toteutetaan tapauskohtaisesti. Systemaattisesti infrastruktuurin mukana tuleva verkonvalvonta pystyisi kuitenkin tarjoamaan lähtökohdat tarkemmalle raportoinnille kun sellaiselle on tarvetta.

Johtopäätöksenä voidaan todeta, että verkonvalvonta ja verkkoliikenteessä tapahtuvien muutoksien seuraaminen on kriittisessä asemassa kun halutaan tuottaa palvelua jollakin asetetulla palvelutasolla. Luvattu palvelutaso voidaan ainoastaan saavuttaa jos se on riittävän tarkasti määritelty ja se voidaan todentaa erilaisilla mittauksilla. Tässä työssä on käsitelty verkonvalvontaa lähinnä siirto- ja suorituskykymielessä. Loppukäyttäjien kannalta on kuitenkin samantekevää, että mistä syystä kriittiset järjestelmät eivät ole käytettävissä. Verkon kapasiteetin loppuminen, linkkiviat tai esimerkiksi ulkopuolinen tietoturvamurto, jonka myötä tietoturvamekanismit on murrettu ja ympäristö on ulkopuolisen hyökkääjän hallussa ovat kaikki kriittisiä tapahtumia järjestelmien toiminnan kannalta. Verkonvalvonnan avulla voidaan havaita muutoksia liikenteessä mutta tietoturvatapahtumien seuraaminen on myös erittäin olennainen asia. Koska kyseessä on hyvin pitkälti samoista laitteista, palomuureista, VPN-yhdyskäytävistä, reitittimistä ja kytkimistä, olisi näitä valvontatoimintoja mahdollista yhdistää. Tietoturvatapahtumien valvonta ja tietojen korrelointi muun verkonvalvonnan kanssa on yksi asia, jonka tutkimusta voisi jatkaa tämän työn pohjalta.

Jatkotutkimuksena aihetta voisi laajentaa juurikin tietoturvanäkökulmasta. Minkälaisia tietoturvatapahtumia pitäisi valvoa ja miten ne voidaan esittää ja liittää yhteen muun verkonvalvonnan kanssa? Olennaista on, että kun jotakin hälyttävää tapahtuu, voidaan se havaita useista eri näkökulmista ja tasoilla jos niihin on kohdistettu oikeanlaista valvontaa.

Verkkoympäristöille on myös mahdollista toteuttaa matemaattisiin malleihin liittyviä luotettavuuslaskentoja. Tällainen analyysi ProLAN-verkon eri osille olisi myös mielenkiintoinen projekti ja sen avulla voitaisiin mahdollisesti löytää heikkouksia, joihin panostamalla verkon toimintavarmuutta ja vikasietoisuutta voitaisiin parantaa entisestään.

Verkonvalvonta vaatii itse järjestelmien ylläpitoa ja niistä saatavan tiedon vastaanottamista ja aktiivista seurantaa. Tämä vaatii aikaa ja resursseja mutta saadun tiedon perusteella voidaan havaita muutoksia ja käynnistää oikeanlaisia toimenpiteitä ennekuin tapahtumat ehtivät muuttua todellisiksi ongelmiksi ja aiheuttaa pahimmassa tapauksessa laajoja katoksia kriittisissä järjestelmissä.

6 Lähteet

[1] **McCabe, J. D.** 2007. *Network Analysis, Architecture, and Design*. Elsevier. Burlington, USA.

[2] **Alger, D.** 2005. *Build the Best Data Center Facility for Your Business*. Cisco Press. Indianapolis, IN. USA. 408 s.

[3] **Fuller, C., Joyner, J., Meyler, K.** 2008. *System Center Operations Manager 2007 unleashed.* Sams publishing. USA. 1385 s.

[4] **Alexander, C.** 2006. *Network Management Fundamentals.* Cisco Press. Indianapolis, IN 46240 USA. 532 s.

[5] **Leon-Garcia, A., Widjaja, I.** 2004. *Communication Networks, Fundamental Concepts and Key Architectures 2nd edition.* McGraw-Hill Companies, Inc.

[6] **Helsingin Energia** 2011. *Helsingin Energia lyhyesti* (online, saatavilla www-muodossa: http://www.helen.fi/yritys/helen.html) [viitattu: 15.9.2011]

[7] **Huoltovarmuuskeskus** 2011. *Energiahuolto | Toimialat | Huoltovarmuuskeskus.*(online, saatavilla www-muodossa: http://www.huoltovarmuus.fi/toimialat/energiahuolto/toiminnan-perusteet/) [viitattu: 15.9.2011]

[8] **Helsingin Energia** 2008. *Helsingin Energia vuosikertomus 2008* (online, saatavilla www-muodossa: http://www.helen.fi/vuosi2008/Hel_En_vuosikertomus_2008.pdf) [viitattu: 14.5.2012]

[9] **Ristiniemi, J.** 2007. Diplomityö: *Suunnitelma Ethernet-pohjaisen TCP/IP-verkon toteuttamiseksi prosessitietoliikenteen tapreisiin Helsingin Energiassa.* Lappeenrannan teknillinen yliopisto. Helsinki. Suomi. 79 s.

[10] **Snyder, J.** *Six Strategies for Defense-in-Depth. Securing the Network from the Inside Out.* 9 s. (online, saatavilla www-muodossa: http://www.arubanetworks.com/pds/technology/whitepapers/wp_Defense-in.depth.pdf) [viitattu: 26.11.2011]

[11] **Gervais, A., Hyppönen, M., Kuivalainen J, et al.** (**monta).** 2011. *White Paper on Industrial Automation Security in Fieldbus and Field Device Level.* 41 s.

[12] **Viestintävirasto.** 2007. *CERT-FI Tietoturvakatsaus 3/2007.* (online, saatavilla www-muodossa: http://www.cert.fi/katsaukset/2007/tietoturvakatsaus_3-2007.html) [viitattu: 27.2.2012]

[13] **McGraw, G., Viega, J.** 2002. *Building Secure Software: How to Avoid Security Problems the Right Way. Addison-Wesley.* Boston. USA.

[14] **Anderson, R.** 2008. *Security Engineering.A Guide to Building Dependable Distributed Systems. 2nd edition.* Wiley. Indianapolis, IN. USA. 1040 s.

[15] **Santos, O.** 2008. *End-to-End Network Security. Defense-in-depth.* Cisco Press. Indianapolis, IN. USA. 469 s.

[16] **Anon.** 2001. *Achieving Defense-in-Depth with Internal Firewalls.* SANS Institute, InfoSec Reading Room. 8 s. (online, saatavilla www-muodossa: http://www.sans.org/reading_room/whitepapers/firewalls/achieving-defense-in-depth-internal-firewalls_797) [viitattu: 26.11.2011]

[17] **Suomen automaatioseura ry.** 2005. *Teollisuusautomaation tietoturva – verkottumisen riskit ja niiden hallinta*. Suomen Automaatioseura ry. Helsinki, Suomi.

[18] **Ahonen, P.** 2010. *TITAN-käsikirja – VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektissa*. Edita Prima Oy. Helsinki, Suomi. 152 s.

[19] **Mills, D.L.** 1985. RFC 958 *Network Time Protocol (NTP).* (online, saatavilla www-muodossa: http://www.ietf.org/rfc/rfc958.txt) [viitattu: 14.5.2012]

[20] **Atkison, R., Kent, S.** 1998. RFC 2401 *Security Architecture for the Internet Protocol.* (online, saatavilla www-muodossa: http://www.ietf.org/rfc/rfc2401.txt) [viitattu: 14.5.2012]

[21] **Shaw, W.** 2006. *Cybersecurity for SCADA Systems*. PennWell. Oklaholma, USA.

[22] **Barnes, K., Johnson, B., Nickelson, R.** 2004. *Review Of Supervisory Control And Data Acquisition (SCADA) Systems.* Idaho National Engineering and Environmental Laboratory. USA. (online, saatavilla www-muodossa: http://www.inl.gov/technicalpublications/Documents/3310858.pdf) [viitattu: 20.11.2011]

[23] **Mauro, D., Schmidt, M.** 2005. *Essential SNMP 2nd Edition.* O'Reilly. 460 s.

[24] **ITU-T Recommendation X.700**. 1992. *Management Framework for Open System Interconnection (OSI).* (online, saatavilla www-muodossa: http://www.itu.int/rec/T-REC-X.700-199209-I/en) [viitattu: 7.2.2012]

[25] **ITU-T Recommendation M.3010**. 2000. *Principles for a telecommunications management network.* (online, saatavilla www-muodossa: http://www.itu.int/rec/T-REC-M.3010-200002-I) [viitattu: 7.2.2012]

[26] **Hautaniemi, M.** 1994. Diplomityö: TKK/Atk-keskuksen TCP/IP-verkon valvonta ja hallinta. (online, saatavilla www-muodossa: http://www.netlab.tkk.fi/julkaisut/tyot/diplomityot/611/) [viitattu: 8.11.2011]

[27] **Jaakonhuhta, H.** 2002. *Lähiverkot - Ethernet. 3. uudistettu painos*. Edita Publishing Oy. IT Press.

[28] **Dykes, B., McPherson, D.** 2001. RFC 3069 *VLAN Aggregation for Efficient IP Address Allocation.* (online, saatavilla www-muodossa: http://www.ietf.org/rfc/rfc3069.txt) [viitattu: 14.5.2012]

[29] **Claise, B., Wolter R.** 2007. *Network Management: Acoounting and Performance Strategies.* Cisco Press. Indianapolis, USA.

[30] **Postel, J**. 1981. RFC 792 *Internet Control Message Protocol*. (online, saatavilla www-muodossa: http://www.ietf.org/rfc/rfc792.txt) [viitattu: 4.12.2010]

[31] **ITU-T Recommendation X.711**. 1997. *Common Management Information Protocol: Specification.* (online, saatavilla www-muodossa: http://www.itu.int/rec/T-REC-X.711-199710-I/en) [viitattu: 13.5.2012]

[32] **Case, J., Mundy, R., Partain, D.**, 1999. RFC 2570 *Introduction to Version 3 of theInternet-standard Network Management Framework* . (online, saatavilla www-muodossa: http://www.ietf.org/rfc/rfc2570.txt) [viitattu: 9.11.2010]

[33] **Gerhards, R.** 2009. RFC 5424 *The Syslog Protocol*.(online, saatavilla www-muodossa: http://www.ietf.org/rfc/rfc5424.txt) [viitattu: 23.1.2012]