Teemu Ahoniemi

ENERGIAYHTIÖN SCADA-VERKON KEHITTÄMINEN

Opinnäytetyö
Tietotekniikka

2017

Kaakkois-Suomen ammattikorkeakoulu

Tekijä	Tutkinto	Aika
Teemu Ahoniemi	insinööri (AMK)	Toukokuu 2017

Opinnäytetyön nimi

Energiayhtiön SCADA-verkon kehittäminen

35 sivua
1 liitesivu

Toimeksiantaja

Kotkan Energia Oy

Ohjaaja

Lehtori Vesa Kankare, IT-asiantuntija Juha Heiskanen

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli perehtyä sähkönjakeluverkon käytönohjaus -ja valvontajärjestelmään (SCADA), sekä erityisesti kyseisen järjestelmän tietoverkkolaitteisiin ja niiden asetusmäärityksiin. Lisäksi verkon dokumentaatiota päivitettiin ja luotiin dokumenttipohjat, joita voidaan päivittää tarpeen mukaan.

Työssä pääpaino oli perehtyä laitevalmistaja Siemensin Ruggedcom-kytkimiin, sekä niissä tehtäviin asetusmäärityksiin häiritsemättä aikakriittisiä toimintoja. Kytkinten hallintaa varten asennettiin hallintakone, jolla etähallinta voitiin tehdä keskitetysti WhatsUp Gold -sovelluksen avulla. Varalaitteen avulla pystyttiin turvallisesti tutustumaan kytkinten ominaisuuksiin ja asetuksiin, sekä tekemään yhteyskokeilu toisen laitevalmistajan kytkimen kanssa. Tämän jälkeen asetusmääritykset tuotantoverkkoon tehtiin etänä hallintakoneelta.

Hallintakoneen ja sen ohjelmistojen asennus sujui ongelmitta, mutta SCADA-verkon palomuuriin tuli tehdä riittävät sääntömuunnokset yhteyden muodostamiseksi. Ongelmana työssä oli myös entuudestaan tuntemattomat Ruggedcom-kytkimet, joiden hallinnan opetteluun kului aikaa.

Työn lopputuloksena verkon tietoturvaa parannettiin, mutta parannettavaa jäi vielä esimerkiksi käyttöjärjestelmäpäivitysten ja fyysisen tietoturvan osalta. Tehtyjen laiteasetusten avulla uusien kytkimien käyttöönotto nopeutuu, sillä samat asetukset voidaan siirtää TFTP-protokollan avulla. Uusittujen dokumenttipohjien ansiosta verkkoon tehtävät muutokset saadaan selkeämmin ja helpommin kirjattua.

Asiasanat

automaatiojärjestelmät, dokumentointi, SCADA, sähköverkot, tietoturva

South-Eastern Finland University of Applied Sciences

Author	Degree	Time
Teemu Ahoniemi	Bachelor of Engineering	May 2017

Thesis Title

Development of SCADA Network of an Energy Company

35 pages
1 appendix page

Commissioned by

Kotkan Energia Oy

Supervisors

Vesa Kankare, Senior Lecturer; Juha Heiskanen, ICT-specialist

Abstract

This thesis examines supervisory control and data acquisition (SCADA) networks. The focus was on the telecommunications equipment and its device configurations. Additionally, the documentation of the network was updated and it was made so that changes could be made to the documentation when new equipment was added.

The main objective was to research Ruggedcom switches which are manufactured by Siemens. The configuration settings of these devices had to be made in such a a way that time-critical services were not disturbed. A network management computer was installed with additional software that made remote management of the switches easier. By using a backup device, it was possible to test different settings and features of a Ruggedcom switch and see how it would work in conjunction with a switch of a different manufacturer. After the testing phase, the configuration changes were made to the devices in production network.

There were no problems in the installation of the management computer or the software, but some access list rule changes had to be made on the SCADA firewall so that successful connection was achieved. The great challenge during the thesis study was the Ruggedcom switches and how to configure them correctly.

Configuration changes improved the information security of the network, but there are still improvements to be made in the physical security and upgrades in operating systems. Once the device configurations were completed and transferred to the management computer via TFTP-protocol, they could be used when a new switch is added to the network. The updated documentation is clearer than before and easier to manage.

Keywords

automation system, documentation, SCADA, power-distribution network, data security

SISÄLLYS

LIITTEET

Liite 1. Kaaviokuva verkon perusrakenteesta

LYHENTEITÄ JA MÄÄRITELMIÄ

ARP	Address Resolution Protocol, protokolla, jonka avulla voidaan selvittää IP-osoitetta vastaava MAC-osoite.
CAN	Controller Area Network, teollisuuslaitteissa ja koneissa käytettävä automaatioväylä.
CMS	Central Monitoring System, keskusvalvontayksikkö.
DCS	Distributed Control Systems, hajautetut automaatiojärjestelmät.
GPS	Global Positioning System, maailmanlaajuinen paikallistamisjärjestelmä.
HMI	Human Machine Interface, ihmisen ja ohjelmoitavan logiikan välinen käyttöliittymä.
I/O	Input/output, siirräntä.
IED	Intelligent Electronic Device, älykäs sähköverkkolaite.
LAN	Local Area Network, paikallisverkko.
PLC	Programmable Logic Control, ohjelmoitavat logiikkajärjestelmät.
RTU	Remote Terminal Unit, etäasema.
SCADA	Supervisory Control And Data Acquisition, käytönohjaus- ja valvontajärjestelmä.
SSH	Secure Shell, protokolla, jolla tietoliikenne voidaan salata.
TFTP	Trivial File Transfer Protocol, protokolla tiedostojen siirtämistä varten.
WAN	Wide Area Network, laaja lähiverkko.

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena oli perehtyä Kotkan Energian sähköverkon käytönohjaus- ja valvontajärjestelmään. Työn tavoitteena oli dokumentoida järjestelmässä käytetyt tietoverkkolaitteet, sekä perehtyä niiden tietoturvaominaisuuksiin. Tämän jälkeen tavoitteena oli parantaa verkon tietoturvaa siten, etteivät aikakriittiset toiminnot häiriintyisi. Muina tavoitteina oli suunnitella ja budjetoida järjestelmän tulevia laitehankintoja.

Työn aihe löytyi kesätyön aikana Kotkan Energialla. Työssä perehdyttiin aluksi yleisimpiin teollisuusautomaatiojärjestelmiin (SCADA, DCS, PLC), tämän jälkeen syvemmin käytönohjaus- ja valvontajärjestelmiin (SCADA). Tämä johtuen siitä, etteivät kyseisten järjestelmien ratkaisut tietoverkoissa olleet aikaisemmassa koulutuksessa tulleet tutuiksi. Työn suunnitteluvaiheessa työnantajalta sain selkeät tavoitteet työn suhteen. Lähteinä käytetyt materiaalit olivat pääosin verkkojulkaisuja esim. laitevalmistajilta ja virallisilta tahoilta, kuten Siemens ja Yhdysvaltain Kotimaan turvallisuus (Homeland Security).

Kotkan Energia Oy

Kotkan Energia Oy on kotkalainen energiakonserni, jonka liiketoimintaan kuuluu sähköverkot, energiantuotanto sekä kaukolämpöpalvelut. Yritys on perustettu vuonna 1993. Päätuotteina ovat jätteidenhyötykäyttöpalvelu, kaukolämpö sekä teollisuushöyry ja -sähkö. Valtaosa Kotkassa käytettävästä kaukolämmöstä tuotetaan Hovinsaaren voimalaitoksessa. Energian-tuotanto hyödyntää lähialueilta saatavia polttoaineita, puuta ja turvetta. Lisäksi lämpöä ja sähköä tuotetaan maakaasusta, tuulivoimasta sekä kierrätykseen kelpaamattomasta jätteestä. Yritys on solminut energiatehokkuussopimuksen, jolla pyritään vähentämään energiankulutusta ja parantamaan energiatehokkuutta. (Kotkan Energia 2016.)

Yritys omistaa kaksi tytäryhtiötä, Karhu Voima Verkko ja Karhu Voima Palvelu. Nämä yhtiöt harjoittavat sähköverkon liiketoimintaa sekä maakaasun siirtoliiketoimintaa Karhulan teollisuusalueilla. Maakaasun yritysmyyntiä tehdään myös valtakunnallisesti. Näiden lisäksi Karhu Voima Palvelu tuottaa sähköverkkojen huolto-

ja kunnossapitopalveluita, sekä erilaisia projektinhoito- ja asiantuntijapalveluita. (Kotkan Energia 2016.)

2 AUTOMAATIOJÄRJESTELMÄT TEOLLISUUDESSA

Verkottuneen teollisuusautomaation katsotaan saaneen alkunsa 1940–1950-lukujen vaihteessa. Noin kymmenen vuotta myöhemmin 1960-luvulla sähköisesti ohjattujen kytkinten (rele) rinnalle tulivat mekaanisesti ohjelmoidut logiikat sekä binääriset ohjauslogiikat, joita ohjattiin tietokoneiden avulla. Tietokoneiden avulla tuotantoprosesseja voidaan hallita ja valvoa paremmalla tarkkuudella, kuin mitä ihminen kykenee. (Suomen Automaatioseura 2010, 51.)

1970-luvulla yleistyivät tietokoneet, jotka perustuivat mikroprosessoreihin. Näiden avulla pystyttiin rakentamaan prosessiasemia hajautetusti tuotantolaitoksille, joita ohjattiin valvomoista prosessitietokoneilla. Tällä tavoin saatiin automatisoitua prosessiasemien mittauksia, sekä niihin perustuvia säätötoimenpiteitä. 1980–1990-luvuilla nopeasti kehittyneet paikallisverkot (LAN) pyrittiin ottamaan käyttöön myös teollisuusautomaatiossa, mutta sen aikaiset tiedonsiirtomenetelmät eivät soveltuneet riittävän tehokkaasti automaation vaatimuksiin. Vuonna 2007 julkaistu ns. kenttäväylästandardi IEC 61158 mahdollisti aiempaa laajemman hajautuksen kenttälaitteille, jotka kommunikoivat paikallisverkon välityksellä. (Pyyskänen 2009, 21–22.)

Laitteiden välisissä kytkennöissä automaatioverkoissa on vähitellen siirrytty sarjaporteista (esim. RS-232/422/485) Ethernetin sekä langattoman tiedonsiirron käyttöön. Tiedonsiirtoprotokollia on kuitenkin käytössä laajasti, kuten esim. Modbus, Profibus, Profinet, Ethernet/IP ja DeviceNet.

3 ERILAISIA AUTOMAATIOJÄRJESTELMIÄ

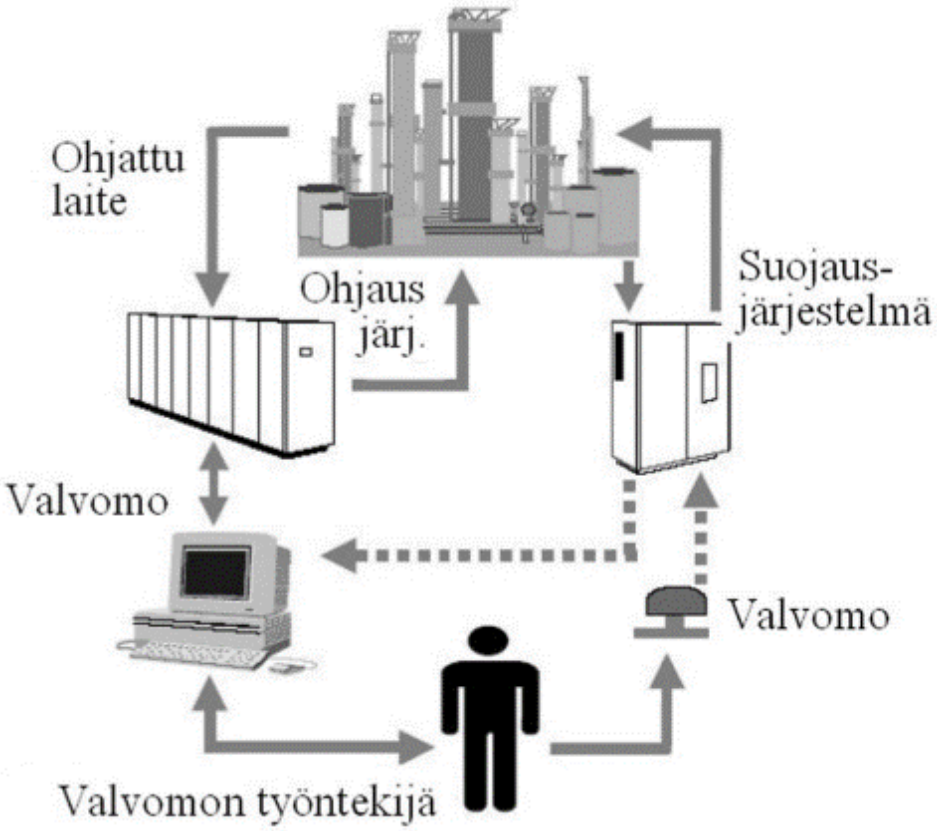
Nykypäivänä teollisuusautomaatiojärjestelmät voidaan jakaa kolmeen pääryhmään:

- hajautetut automaatiojärjestelmät (DCS, Distributed Control System)
- käytönohjaus- ja valvontajärjestelmä (SCADA, Supervisory Control And Data Acquisition)

- ohjelmoitavat logiikat (PLC, Programmable Logic Controller)

3.1 Hajautetut ohjausjärjestelmät

Hajautetuilla ohjausjärjestelmillä hallitaan yleensä yhdellä alueella sijaitsevia laitoksia, kuten öljynjalostuksen, elintarvikealan ja paperiteollisuuden laitoksia. Ohjausjärjestelmään kuuluu yleensä ohjaustaso sekä yksi tai useampi hajautettu ohjausyksikkö. Valvontayksikön toiminta tapahtuu ohjauspalvelimessa ja kommunikointi ala-asemien välillä tapahtuu omissa aliverkoissa. Ohjausyksikkö suorittaa tarvittavat säätötoimenpiteet ja kerää tietoja hajautetuilta ohjausyksiköiltä, jotka ohjaavat prosessitoimintoja annettujen käskyjen mukaisesti. Kommunikointi anturien ja toimilaitteiden kanssa tapahtuu kenttäväylän avulla. Etähallinta ohjausjärjestelmän yksiköihin tapahtuu yleensä modeemien avulla, jolloin laitteita voi hallita ja huoltaa laitosten työntekijöiden lisäksi esim. laitetoimittajat. Suojausjärjestelmiä prosessiautomaatiossa tarvitaan vain poikkeustilanteiden hallinnassa, joten niiden vaatimustaso on perusjärjestelmää korkeampi (kuva 1). (Suomen Automaatioseura 2010, 53.)



Kuva 1. Yksinkertaistus prosessin perus- ja suojausjärjestelmästä (Suomen Automaatioseura 2010, 54)

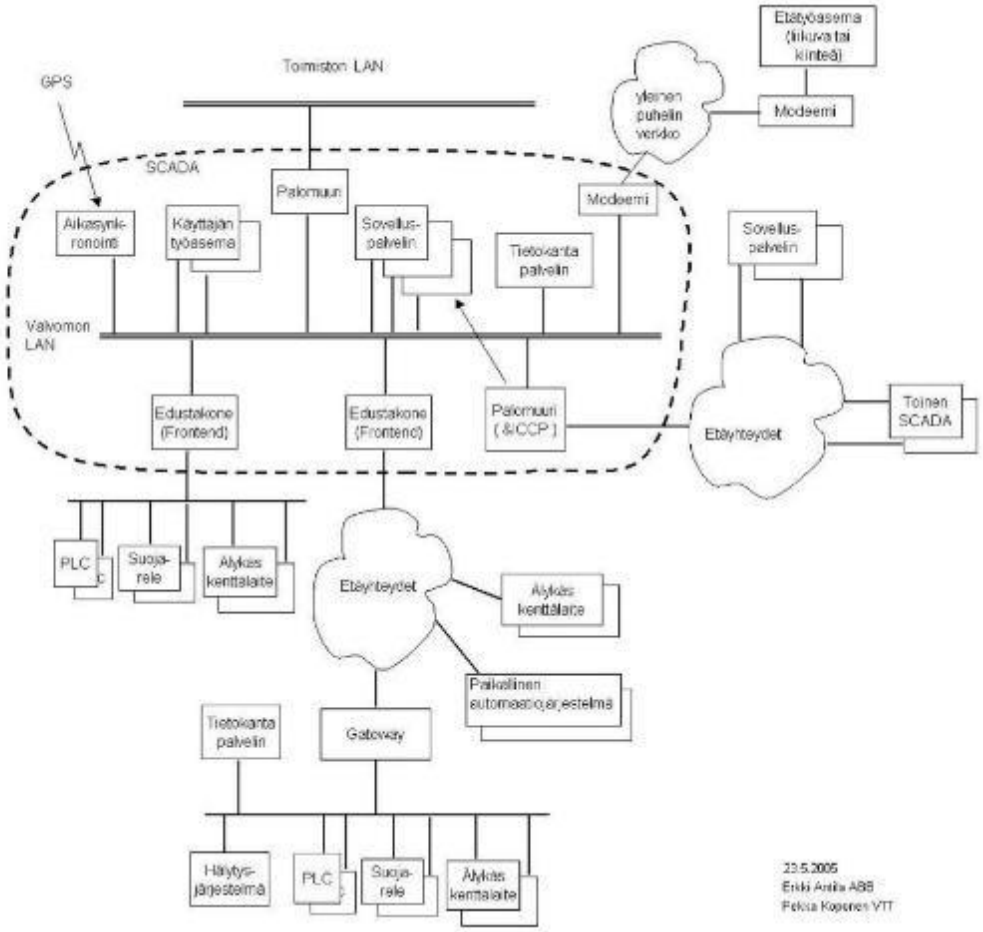
Hajautetut ohjausjärjestelmät eivät toimi itsenäisesti, vaan vaativat toimintojen suorittamiseen ja päätöksien tekoon ihmisen (operaattori). Operaattori pystyy valvomosta käsin esim. sulkemaan tai avaamaan venttiilejä tai muokkaamaan tuotannossa käsiteltävien materiaalien määriä. Valvomoon välitetään tuotannon kriittisimmistä pisteistä hälytykset, joihin operaattorin tulee reagoida. (DCS or PLC? - Seven Questions to Help You Select the Best Solution 2007, 5.)

3.2 Käytönohjaus- ja valvontajärjestelmä

SCADA-järjestelmillä tarkoitetaan maantieteellisesti hajautettuja järjestelmiä, joilla hallitaan yleensä laajempia kokonaisuuksia kuin DCS-ohjausjärjestelmissä. Tällaisia voivat olla esim. sähköverkot, vesijärjestelmät ja kaasulinjat. Maantieteellisen laajuuden lisäksi suurena erona SCADA-järjestelmällä DCS-järjestelmään on sen päätarkoitus. SCADA-järjestelmän avulla kerätään tietoja etäasemista tietokantoihin ja suurin osa järjestelmässä tapahtuvista säätötoimenpiteistä ovat automatisoituja. (Suomen Automaatioseura 2010, 54.)

SCADA-järjestelmä koostuu yleensä keskusvalvontayksiköstä (CMS) sekä yhdestä tai useammasta etäasemasta (RTU tai PLC). Ohjauspalvelimessa sijaitseva ohjausjärjestelmä kerää tiedot etäasemista ja suorittaa säätötoimenpiteet mittausten perusteella. Säätötoimenpiteet on myös mahdollista hoitaa etäasemilla kenttäoperaattorin tai ohjelmoitavan logiikkayksikön (PLC) toimesta. (Stouffer, Pillitteri, Lightman, Abrams & Hahn 2015, 20.)

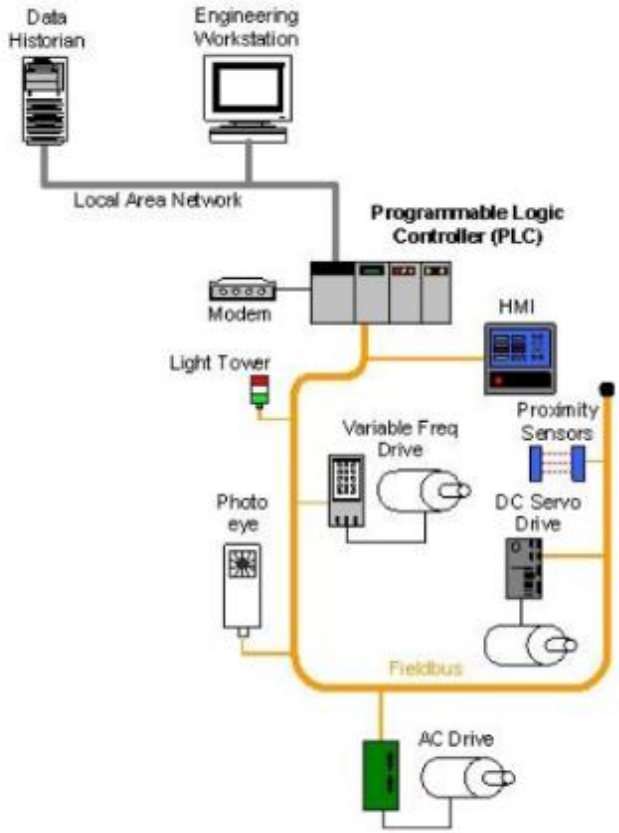
Yleensä SCADA-järjestelmät eristetään omiin aliverkkoihin ja suoraa yhteyttä normaaliin internetliikenteeseen ei ole. Yhteys esim. toimistoverkkoon yhdistetään palomuurin kautta ja yleensä myös toimistoverkon liikenne kulkee Internetin suuntaan palomuurin läpi (kuva 2). Tällä pyritään karsimaan kaikki turha tietoliikenne SCADA-järjestelmistä pois.



Kuva 2. Tyypillinen esimerkki sähkönsiirron SCADA-järjestelmästä. Kriittisin ja parhaiten suojattu osa verkosta on merkitty katkoviivalla, yhteydet muihin paikallisverkkoihin eristetään yleensä palomuurien ja edustakoneiden avulla (Suomen Automaatioseura 2010, 55)

3.3 Ohjelmoitavat logiikat

Ohjelmoitavat logiikat eroavat hajautetuista ja käytönvalvontajärjestelmistä siten, että niistä yleensä puuttuu keskusohjauspalvelin (engl. central control server) sekä käyttöliittymät (HMI). Tyypillisesti ohjelmoitavat logiikat toimivat osana SCADA ja DCS järjestelmiä, jolloin niiden tehtävänä on hoitaa hallintatehtäviä eri puolilla prosessia. Koska logiikoista puuttuvat käyttöliittymät, niitä hallitaan erillisillä työasemilla, jotka ovat samassa lähiverkossa (Kuva 3). Työasemien kautta logiikat voidaan ohjelmoida suorittamaan tarvittavat tehtävät, joita voivat olla esim. siirräntälaitteiden ohjaus (I/O), ajoitukset, laskutehtävät ja tietojenkäsittely. (Stouffer ym. 2015, 27–28.)



Kuva 3. Esimerkki ohjelmoitavan logiikan toteutuksesta (Stouffer ym. 2015, 28)

3.4 Järjestelmien eroavaisuudet ja kehittyminen

Aiemmin näiden pääryhmien erot toisiinsa nähden olivat selkeät, mutta viime vuosien aikana niiden rajat ovat hämärtyneet. Vielä 1990-luvulla SCADA-järjestelmien päätarkoitus oli tiedonkeruu ja tietokantojen ylläpito. Tiedonkeruu ja järjestelmien hallinta tapahtuivat maantieteellisesti laajassa, hitaassa ja usein epävakaassa tietoverkossa. DCS-järjestelmissä pääpaino oli laitosten eri laitteiden hallinnassa. Tietokannoille ja tiedonkeruulle ei ollut tarvetta ja operaattorille välitetyt tiedot olivat vain osa järjestelmän tehtävää. Tuotannon hallittu ylläpito oli tärkeintä. Yleisesti DCS-järjestelmä suoritti prosessitehtävät ja raportoi tulokset laajempaan SCADA-järjestelmään.

Tekniikan kehityksen myötä rajoitukset esim. tietoliikennenopeuksissa ja tietokoneiden laskentatehoissa ovat muuttuneet. Kehityksen ansiosta monia ominaisuuksia SCADA-järjestelmistä on otettu käyttöön DCS-järjestelmiin ja päinvastoin. Modernissa SCADA-järjestelmässä on aiempaa älykkäämpiä etälaitteita

(RTU ja PLC), joiden ansiosta verkon saatavuus (engl. availability) säilyy, vaikka yhteys keskusvalvontayksikköön katkeaa. DCS-järjestelmissä prosessinhallinnan lisäksi kerätään tietoa esim. laitoksen sähkönjakelusta ja turvalaitteiden toiminnasta (Essentials of the Modern DCS 2015, 2). Hallintajärjestelmät ovat myös helpompi yhdistää laitoksen tai yrityksen muuhun tietoliikenneverkkoon. Pääpaino onkin nyt siirtynyt teknisistä ongelmista tietoturvan parantamiseen.

4 SCADA-VERKKOJEN TIETOTURVA

Samalla, kun automaatiojärjestelmien etäohjaus ja valvonta on siirtynyt TCP/IP-pohjaiseen verkkoon, niiden tietoturvariskit ovat kasvaneet. Vielä vuosituhannen vaihteessa automaatiojärjestelmät olivat fyysisesti eristettyjä, eikä niiden tietoturvaa pidetty merkittävänä. Järjestelmissä käytetään usein kaupallisia ohjelmistoja ja laitteita, jotka vaativat yhteyden ulkopuolisiin verkkoihin. Tämä muodostaa vakavan uhan tuotannon eri järjestelmiin. (Suomen Automaatioseura 2010, 58–59.)

Laite- ja ohjelmistovalmistajien itsemääritellyt protokollat ja usein vanhentuneet turvallisuusasetukset eivät suojaa riittävästi nopeasti kehittyviltä kyberhyökkäyksiltä. Vasta viime vuosien aikana suurimmat laitevalmistajat ovat havahtuneet parantamaan laitteidensa turvallisuusominaisuuksia jo niiden valmistusvaiheessa. (Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies 2016, 31, 34.)

Tavanomaisiin IT-järjestelmiin verrattuna automaatiojärjestelmien laitteistojen elinkaaret ovat pidempiä ja niiden mahdolliset päivitykset ja laitemuutokset tulee tehdä hallitummin ja turvallisemmin. Vaikka laitteet ja ohjelmistot ovat hankintavaiheessa nykyään paremmin suojattuja, tulisi niiden tietoturvaominaisuudet huomioida koko elinkaaren ajalle. Etenkin vanhempien järjestelmien osalta tämä on yleensä tutkittava tapauskohtaisesti. (Suomen Automaatioseura 2010, 89–90.)

Suurien tietomurtojen jälkeen on havahduttu parantamaan tietoturvaa esim. virusturvalla ja perusasetusten muutoksilla, eli koventamisella. Koventamiseen kuuluu muun muassa oletussalasanojen muuttaminen, turhien palveluiden poistaminen

ja käyttämättömien tiedonsiirtoporttien sulkeminen Lisäksi tietoturvaa on pyritty parantamaan lukuisten standardien ja ohjeistusten avulla.

4.1 Tyypillisimmät riskit ja niiltä suojautuminen

Yleisimpiä tapoja verkkoon tunkeutujalle on löytää verkosta huonosti määritelty laite tai turvaton protokolla, jolla laitteeseen yhdistetään. Yleisesti käytetyissä käyttöjärjestelmissä on oletuksena käytössä palveluita, joiden takia avoimeksi jää useita haavoittuvia portteja. Kun tarpeellinen ohjelmisto on asennettu, tulisi tämän jälkeen huolehtia ylimääräisten palveluiden sulkemisesta. Vanhentuneiden protokollien käyttöä tulisi välttää niiden turvattomuuden vuoksi. Esimerkiksi käytettäessä Telnet-protokollaa yhteyden muodostamiseen laitteiden välillä, salasanat lähetetään selkokielisenä. (Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies 2016, 37.)

Henkilöstön riittävästä kouluttamisesta ja ohjeistamisesta tulisi huolehtia, sillä se muodostaa yhden suurimmista riskeistä tietoturvalle. Luvattomat laitteet, kuten USB-muistit ja kannettavat tietolaitteet, ovat hyvin tyypillisiä välineitä viruksen levittämiselle tai tietoliikenteen jumiuttamiselle. (Suomen Automaatioseura 2010, 21.)

Laitetilojen valvonta on myös tärkeässä osassa. Lukittujen ovien lisäksi tulisi hyödyntää esimerkiksi kulunvalvontaa ja kameravalvontaa. Kuten palvelintilat yleisesti, tulisi kriittisimmät tilat olla myös ikkunattomia. Koulutettu henkilöstö tulee esiin myös fyysisessä tietoturvassa, sillä heidän vastuullaan on myös huolehtia, että asiattomat henkilöt eivät pääse sisään laitetiloihin ja aiheuttamaan fyysistä vahinkoa laitteille.

4.2 Toipuminen häiriötilanteista

Mahdollisten tietoturvahäiriöiden varalle tulisi aina olla toipumissuunnitelma. Suunnitelman tulisi sisältää muun muassa kovalevyjen ja laiteasetusten varmennukset. Näiden avulla mahdollistetaan verkon nopea palautuminen. Varmennuksia ei tulisi säilyttää samassa tilassa tuotannossa olevien laitteiden kanssa, vaan

eristettynä esimerkiksi toiselle koneelle johon ei ole suoraa yhteyttä. Kaikkien varmennusratkaisujen toimintavarmuutta tulisi myös testata sopivin aikavälein, jotta voidaan varmistua niiden toimivuudesta. (Suomen Automaatioseura 2010, 76–77.)

Kattavaan suunnitelmaan kuuluu myös ajan tasalla oleva verkon kaaviokuva, josta selviää laitteiden sijoitukset ja kytkennät. Lisäksi tulisi suunnitella lista vastuuhenkilöistä ja heidän rooleista häiriötilanteiden aikana. Myös lista muun muassa yhteyshenkilöistä eri laitevalmistajille ja verkon ylläpitäjille nopeuttaa toipumista. (Stouffer ym. 2015, 94.)

5 TYÖN TOTEUTUS

Työn aloitusvaiheessa oli ensin perehdyttävä aikaisempaan verkkodokumentaatioon, joka oli tehty energiayhtiö Loisteen toimesta. Tämän jälkeen tutustuttiin verkossa käytössä olleisiin verkkolaitteisiin ja niihin määritettyihin asetuksiin. Lisäksi tehtiin esittelykierros tärkeimmillä ala-asemilla, joilla näytettiin verkkolaitteiden sijoituspaikat sekä esiteltiin sähköverkon etäohjattavia laitteita. Näiden tietojen pohjalta pystyttiin tekemään riittävät parannukset verkon dokumentaatioon tietoverkkolaitteiden osalta.

Perehtymisvaiheen jälkeen käytiin läpi kaikkien hallittavien kytkimien asetukset ja tutkittiin, minkälaisilla asetusmuutoksilla tietoturvaa voitaisiin parantaa. Ala-asemavierailun jälkeen mietittiin myös mahdollisia parannuksia fyysiseen tietoturvaan.

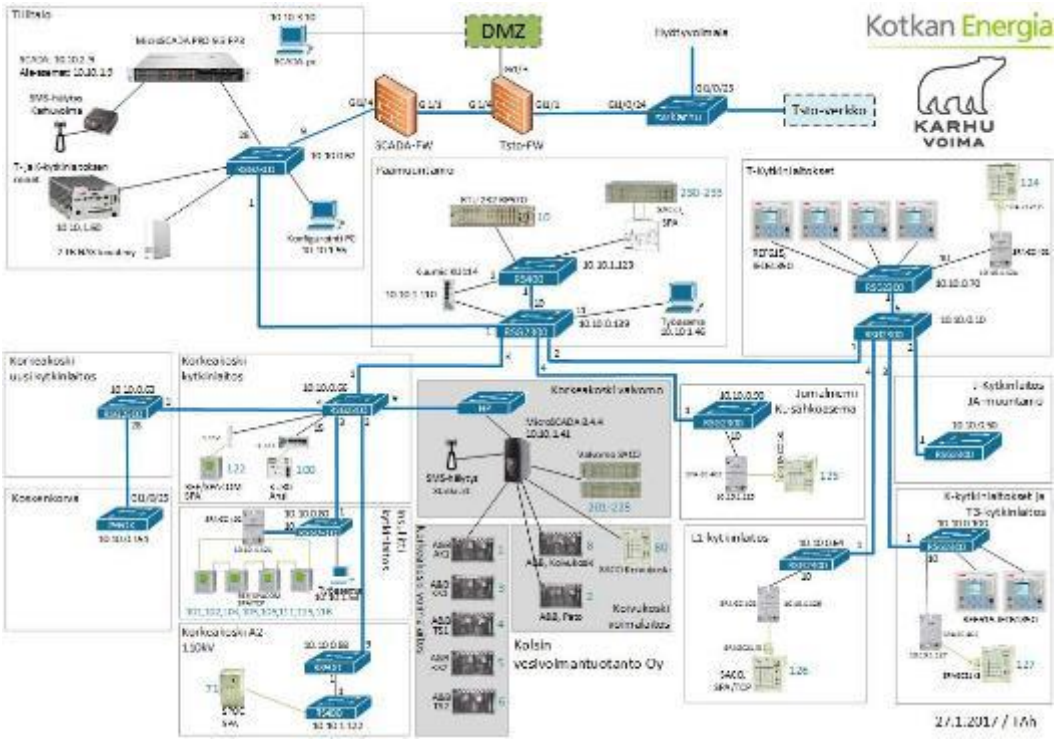
Verkkolaitteiden hallintaa varten asennettiin erillinen virtuaalikone, johon asennettiin verkon hallintaa helpottavia ohjelmistoja. Tätä virtuaalikonetta varten tuli tehdä riittävät muutokset palomuuriin, koska kone oli Kotkan Energian hallintaverkossa.

5.1 Verkon dokumentointi

Aiempien dokumenttien perusteella selvisivät käytössä olleet IP-osoitteet, jotka oli jaettu kuuteen aliverkkoon niiden käyttötarkoitusten mukaan. Käytetyt IP-osoitteet olivat listattuna yhteen Word-dokumenttiin, jossa oli myös selostettu verkkoon tehdyt suuremmat muutostyöt. IP-osoitetaulukko tässä dokumentissa oli sekava, sillä vain etämittarien aliverkon osalta oli tehty oma taulukko ja muiden aliverkkojen laitteet olivat sekaisin erillisessä taulukossa.

Vanhasta taulukosta etsittiin kaikki etähallittavat laitteet ja varmistettiin niiden IP-osoitteiden pitävän edelleen paikkansa. Tämän jälkeen tehtiin Excel-ohjelmalla uusi työkirja, johon luotiin jokaiselle aliverkolle omat taulukot ja listattiin laitteet niille kuuluville osoitepaikoille.

Microsoft Visio -ohjelmalla luotiin kaavio, johon piirrettiin kuva verkon perusrakenteesta ja sijoitettiin laitteet paikoilleen Loisteen dokumentaation perusteella (Kuva 4). Kaaviokuvasta tarkempi versio löytyy liitteestä 1. Koska edellinen dokumentaatio oli vuodelta 2015, piti uuteen kaaviokuvaan lisätä verkkoon liitetyt uudet ala-asemat, Koskenkorva ja Korkeakosken uusi sähköasema, sekä niiden verkkolaitteet.



Kuva 4. Kaavio SCADA-verkon perusrakenteesta. Tämän työn kannalta oleellisimmat kytkimet merkittiin erottuvasti sinisinä laatikoina

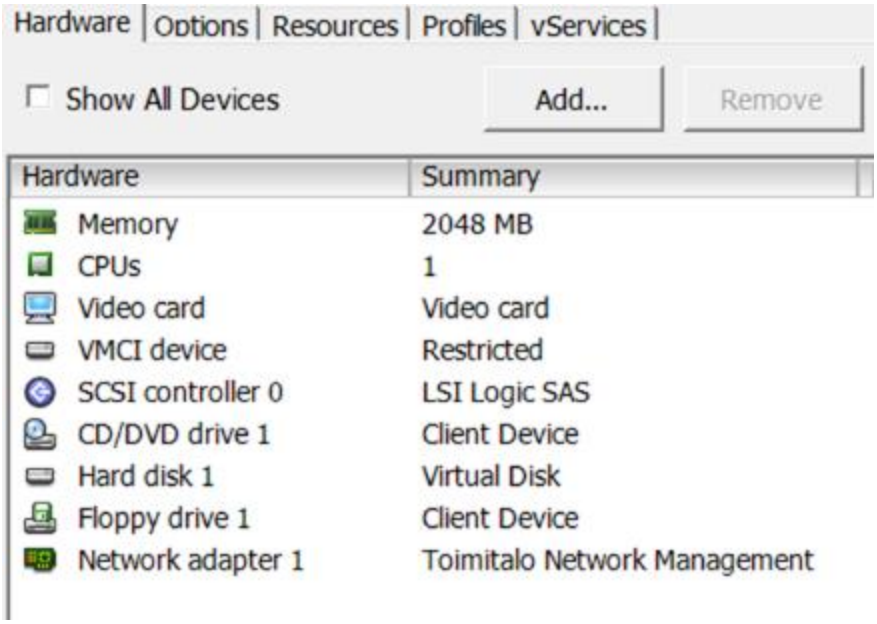
Kaavioon on merkitty seuraavat asiat:

- ala-asemien nimet ja numerointi (siniset numerot)
- IP-osoitteet
- mallinumerot
- laitteiden väliset porttikytkennät

Dokumentaatiota tehdessä selvisi, että jotkut laitteista oli siirretty ala-asemilta toiselle ja vanhat tiedot eivät pitäneet enää paikkaansa. Näiden laitteiden uudet sijoitukset pystyttiin selvittämään kytkimien MAC-osoitetaulukoiden, sekä ARP-kyselyiden avulla, jotka tehtiin reititystä hoitaneessa palomuurissa. Tämä vaihe esitellään tarkemmin laitteiden asetusten määrittelyssä.

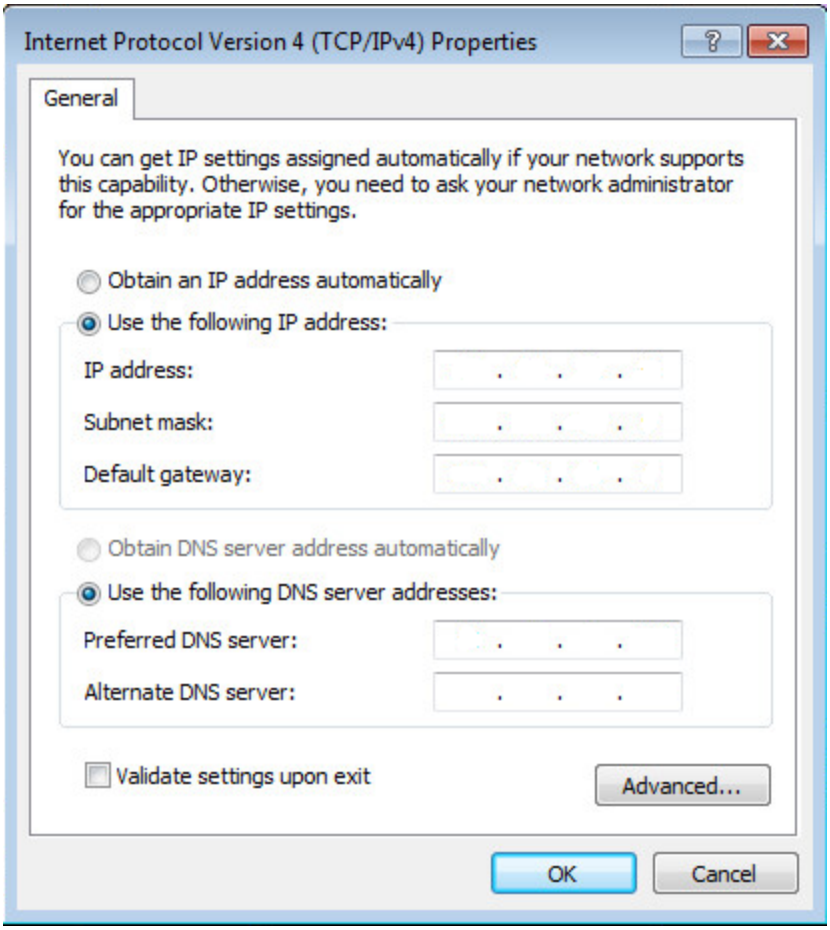
5.2 Verkonvalvontakone

Verkon valvontaa pyrittiin helpottamaan ja automatisoimaan asentamalla siihen tarkoitukseen oma tietokone. Tietokone asennettiin virtuaalikoneena VMwaren vSphere-alustalle. Koska verkonvalvontaa varten tarvittiin vain muutama ohjelmisto, virtuaalikoneelle määritettiin pienet resurssit (kuva 5).



Kuva 5. Virtuaalikoneen resurssimääritykset

Virtuaalikoneen käyttöjärjestelmäksi valittiin Windows 7 Professional, 64-bittinen versio. Valinta tehtiin sen perusteella, että kaikki asennettavat ohjelmat tiedettiin toimivan ongelmitta kyseisessä käyttöjärjestelmässä. Lisäksi käyttämättömiä tuoteavaimia oli heti saatavilla. IP-osoitteeksi valittiin vapaa osoite Kotkan Energian aliverkosta, joka on tarkoitettu verkon hallintaan (kuva 6). Myös DNS-palvelinten osoitteet määritettiin Kotkan Energian verkosta. Virtuaalikoneen nimeksi määritettiin KAR-NMC (Karhuvoima Network Management Center).



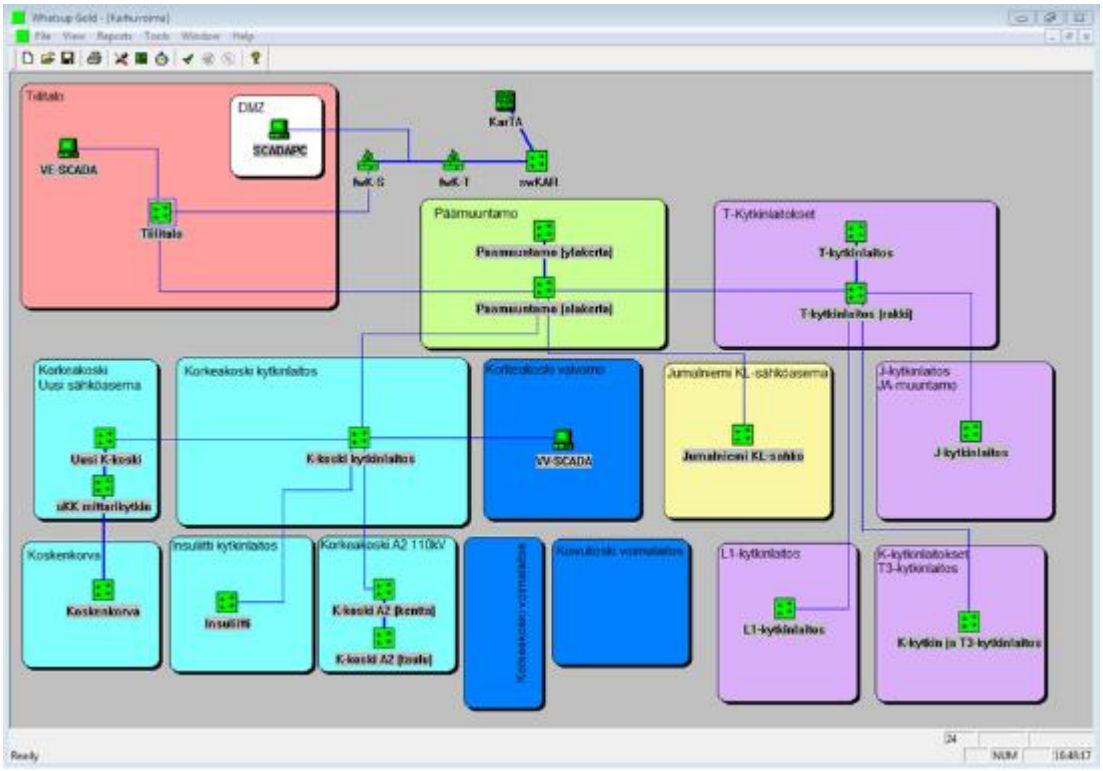
Kuva 6. IP-osoitteen ja DNS-palvelinten määritys

Koneelle asennettiin seuraavat ohjelmat:

- PuTTY
- Kiwi Syslog server
- Tftpd32
- WhatsUp Gold Network Monitoring
- UltraVNC Server
- Cisco -palomuurien hallintaohjelmisto ASDM

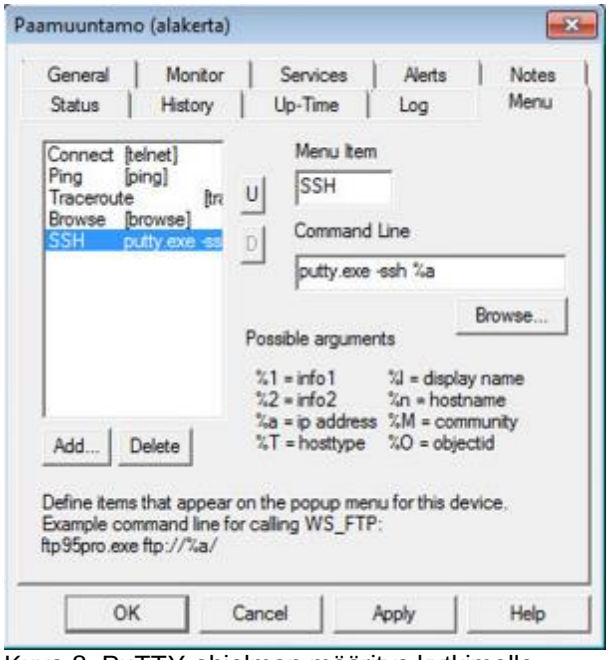
Näistä ohjelmista WhatsUp Gold vei eniten aikaa käyttöönotossa. Kyseessä oli ohjelmasta vanhempi versio, mutta sen käyttö oli ilmaista. Lisäksi Kotkan Energian verkossa oli muualla käytössä sama ohjelma, josta pystyi hyödyntämään ohjelmassa tehtyjä määrityksiä. Oikein määritettynä se on tehokas työkalu verkon valvonnassa, sekä nopeuttaa etäyhteyksien muodostamista verkon eri laitteisiin. Ohjelman käyttöönotossa ensimmäinen vaihe on verkon kaaviokuvan piirtäminen, sekä verkkolaitteiden sijoitus kuvaan. Koska dokumentaatiovaiheessa verkosta luotiin ajan tasalla oleva kaaviokuva, sitä pystyttiin hyödyntämään myös

tässä työvaiheessa. Lopputulos muistuttaa alkuperäistä kaaviokuvaa, mutta yksinkertaistetumpi, sillä kaikkia laitteita ei tarvittu liittää valvontaan (kuva 7).

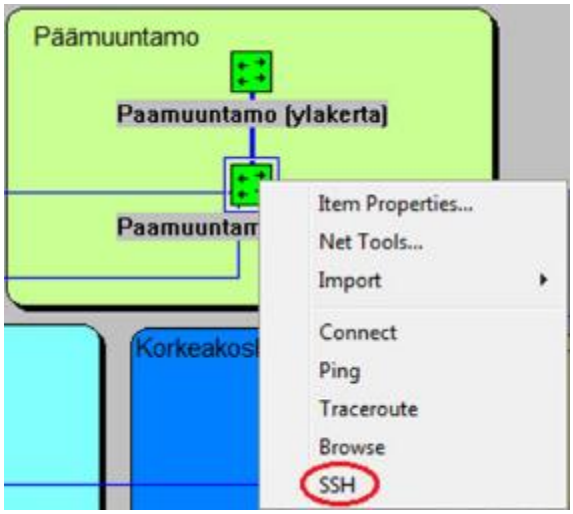


Kuva 7. Ruutukaappaus WhatsUp Gold -ohjelmasta työn loppuvaiheessa. Hallittavina laitteina ohjelmassa ovat vain kriittisimmät laitteet, esimerkiksi verkon suojareleitä ei lisätty. Valvontaan voitaisiin lisätä mikä tahansa laite, jossa on IP-osoite

WhatsUp Gold -ohjelma pystyy hyödyntämään PuTTY-etähallintaohjelmaa siten, että määrityksen jälkeen klikkaamalla verkkolaitetta kaaviokuvassa voidaan muodostaa hallintayhteys (kuva 8 ja 9).



Kuva 8. PuTTY-ohjelman määritys kytkimelle



Kuva 9. Kaaviokuvassa avautuva valikko määrityksen jälkeen

5.3 Palomuurisääntöjen lisäys

Jotta verkonhallintakoneelta saatiin yhteys SCADA-verkon laitteisiin, piti SCADA-palomuuriin lisätä kuvan mukaiset säännöt (kuva 10). Näiden sääntöjen lisäksi palomuurissa oli määritykset muun muassa muutamalle VPN-yhteydelle ja toisen SCADA-verkon hallintakoneelle.

#	Enabled	Source Criteria: Source	...	S...	Destination Criteria: Destination	Sec...	Service	Action	Hits
Global (32 rules)									
3	☑	any			KAR-NMC		syslog	Permit	147
4	☑	any			KAR-NMC		tftp	Permit	8
13	☑	KAR-NMC			VV-SCADA		VPN_SERVICES_ICMP_RDP_...	Permit	3
14	☑	KAR-NMC			HALLINTAVERKKO-network/24		NETWORKACCESS-SERVICES	Permit	168
15	☑	KAR-NMC			KORKEAKOSKIVALVOMO-NETWORK		NETWORKACCESS-SERVICES	Permit	10

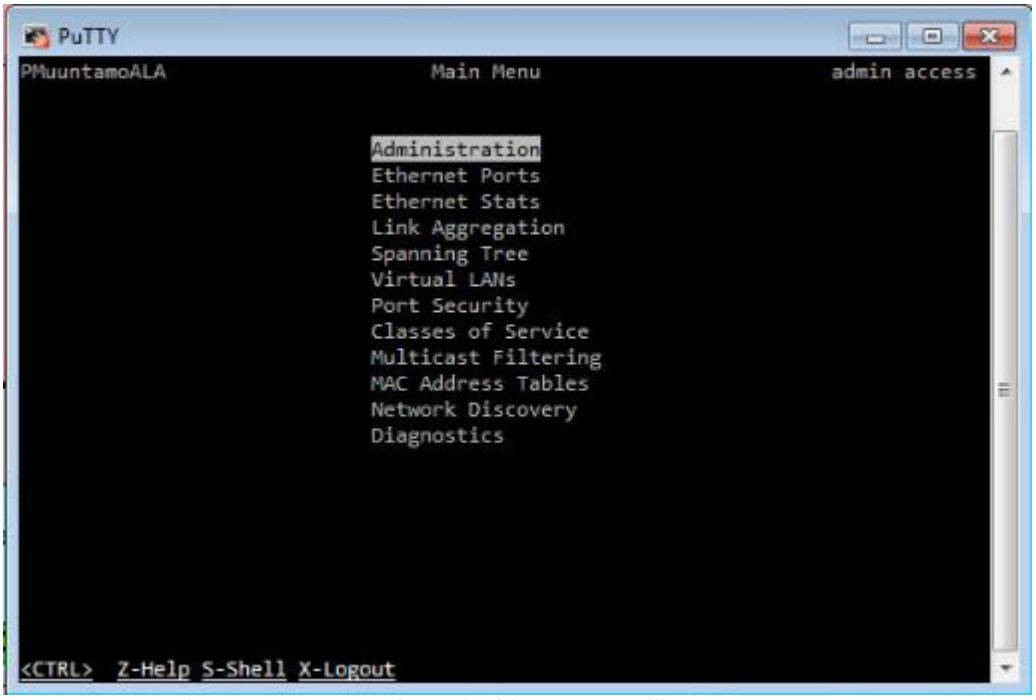
Kuva 10. Lisätyt palomuurisäännöt hallintakoneen osalta

Syslog- ja TFTP-palveluiden osalta sääntöihin määritettiin lähdeosoitteeksi mikä tahansa osoite SCADA-verkosta ja kohdeosoitteeksi hallintakone KAR-NMC. Kytkinten hallintaa ja etätyöpöytähallintaa varten lisättiin säännöt, joissa lähdeosoitteena olivat verkonhallintakone ja kohdeosoitteena olivat muun muassa SCADA-kytkimet.

5.4 Kytkinten asetusmäärittelyt

Työn aloitusvaiheessa käytössä olleet tietoverkkolaitteet koostuivat laitevalmistaja Siemensin Ruggedcom-kytkimistä. Nämä kytkimet sopivat hyvin etenkin sähkönjakeluverkon tiedonsiirtoon, sillä ne tukevat IEC 61850 kommunikointiprotokollaa ja ovat suojattuja sähkömagneettisilta häiriöiltä ja suurilta virtapiikeiltä. Lisäksi laitteet ovat tärinäsuojattuja ja ne kestävät suuriakin lämpötilavaihteluita (-40 °C…+85 °C) (RUGGEDCOM RSG2300 2017). Laitteiden asetukset olivat pääosin tehdasasetusten mukaiset, sillä niihin oli määritetty vain IP-osoitteet ja ylläpitäjän salasana oli muutettu.

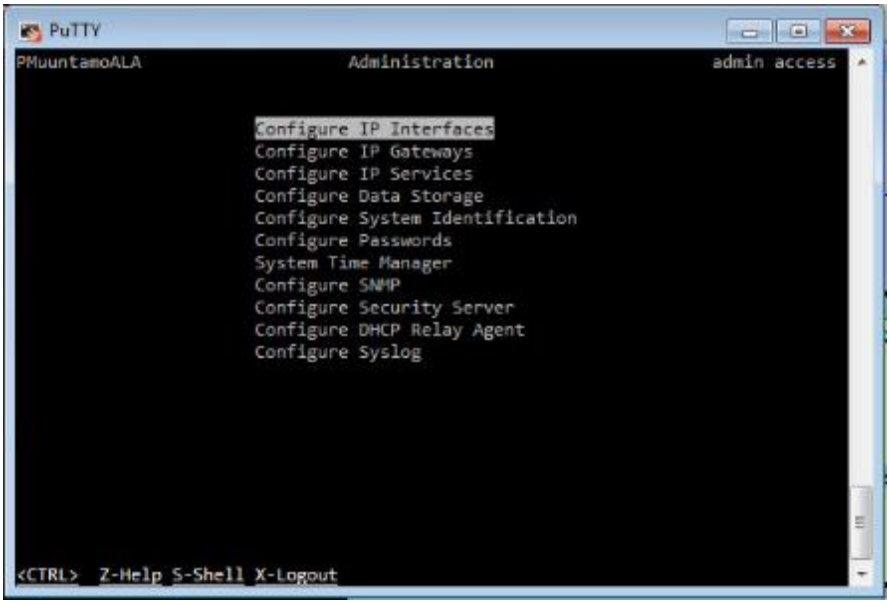
Ruggedcom-kytkimien käyttöjärjestelmänä on RUGGEDCOM Operating System (ROS®). Tässä käyttöjärjestelmässä asetusmuutokset tehdään valikkojen avulla (kuva 11), komentorivin kautta onnistuu esim. kaiutuspyyntöjen lähettäminen ja laiteasetusten siirto TFTP:n avulla.



Kuva 11. Ruutukaappaus Ruggedcom-kytkimen päävalikosta

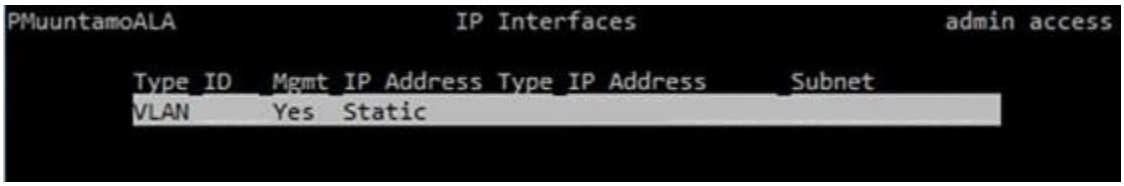
5.4.1 Muutokset tehdasasetuksiin

Koska kytkinten asetukset olivat pääosin tehdasasetusten mukaiset, piti kaikki kytkinten asetukset käydä läpi ja tehdä ne yhdenmukaiseksi. Tärkeimmät asetukset perusasetuksiin liittyen löytyi Main Menu -valikon Administration-alavalikosta (kuva 12).



Kuva 12. Ruutukaappaus Administration-alavalikosta

Configure IP Interfaces- ja IP Gateways -alavalikoissa muutoksia ei tarvittu tehdä, sillä niihin oli kaikissa laitteissa määritetty oikeat asetukset, eli laitteen hallinta IP-osoite (kuva 13) ja yhdyskäytäväosoite (kuva 14). Yhdyskäytävänä tässä verkossa toimi palomuuri, johon oli määritetty jokaiselle aliverkolle oma aliliityntäporttinsa (subinterface).



Kuva 13. Esimerkki kytkimen hallinta IP-osoitteen määrittämisestä

Kuva 14. Esimerkki kytkimen yhdyskäytäväosoitteen määrittämisestä

Configure IP Services -alavalikossa (kuva 15) määritettiin etähallintaan liittyviä seuraavia asioita:

- istunnon aikakatkaisu
- samanaikaisten Telnet-istuntojen lukumäärä
- samanaikaisten SSH-istuntojen lukumäärä

Kuva 15. Esimerkki IP Services -asetusten määrityksistä

Osassa laitteista, joissa oli vanhempi käyttöjärjestelmäversio käytössä, ei ollut mahdollista kytkeä SSH-määritystä käyttöön, vain Telnet-yhteys oli mahdollinen. Jatkossa tulisi harkita ainakin näiden vanhempien käyttöjärjestelmäversioiden

päivittämistä, sillä salaamaton Telnet-etäyhteys on tietoturvariski. Tästä esimerkkinä nähdään jo etäyhteyttä muodostettaessa kytkimeen: SSH-yhteydellä nähdään vain kirjautumistiedot (kuva 16), Telnet-yhteydellä nähdään esim. laitteelle määritetty nimi, laitteen versionumero ja MAC-osoite (kuva 17).

Kuva 16. Kirjautuminen kytkimeen SSH-yhteydellä

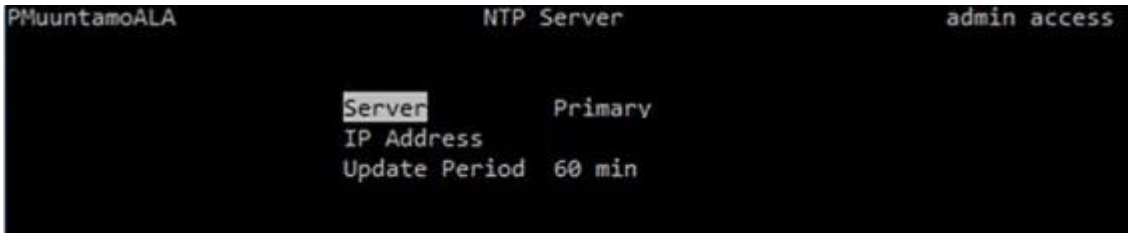
Kuva 17. Kirjautuminen kytkimeen Telnet-yhteydellä

Ruggedcom-kytkimissä on oletuksena käytössä kolme käyttäjätiliä, joissa on eritasoiset käyttöoikeudet. Guest-tason tilillä näkee määritetyt asetukset, mutta niitä ei voi muuttaa. Operator-tason tilillä näkee kaikki asetukset ja on mahdollista muuttaa laitteet perusasetuksia. Admin-tason tilillä on mahdollista muuttaa kaikkia laitteen asetuksia. (RUGGEDCOM RS900 ROS v4.3 User Guide 2016, 112–113.)

Näistä tileistä otettiin pois käytöstä kaksi alemman tason tiliä, Guest ja Operator, sillä niille ei ollut tarvetta. Tilit poistettiin käytöstä siirtymällä Configure Passwords -alavalikkoon ja tyhjentämällä kentät Guest Username ja Operator Username (kuva 18). Admin-tilin kohdalla muutettiin vain oletussalasana.

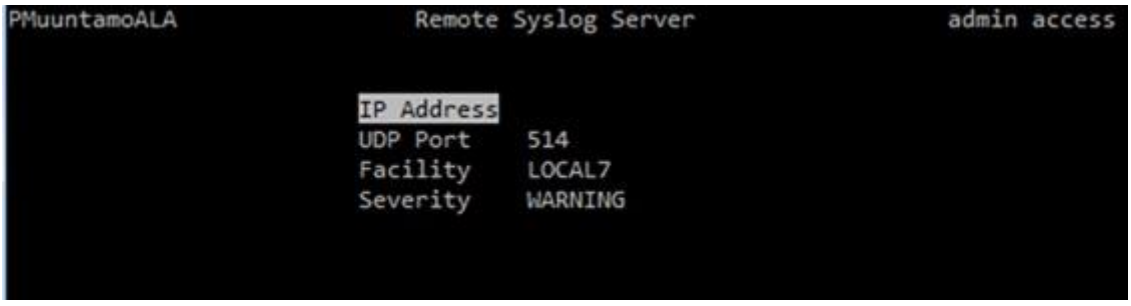
Kuva 18. Käyttäjätilien ja salasanojen määritysvalikko

Kytkimien aika-asetukset muutettiin niiden oletusarvoista (UTC-05:00) vastaamaan paikallista aikaa (UTC+02:00). Lisäksi kytkimet määritettiin tahdistamaan kellonaika kerran tunnissa NTP-palvelimelta (kuva 19).



Kuva 19. Esimerkki NTP-palvelinmäärityksestä

Configure Syslog -alavalikossa kytkimet määritettiin välittämään Syslog-viestit verkonvalvontakoneelle. Näistä viesteistä määritettiin kerättävän Warning-tason ja sitä vakavammat viestit (kuva 20).



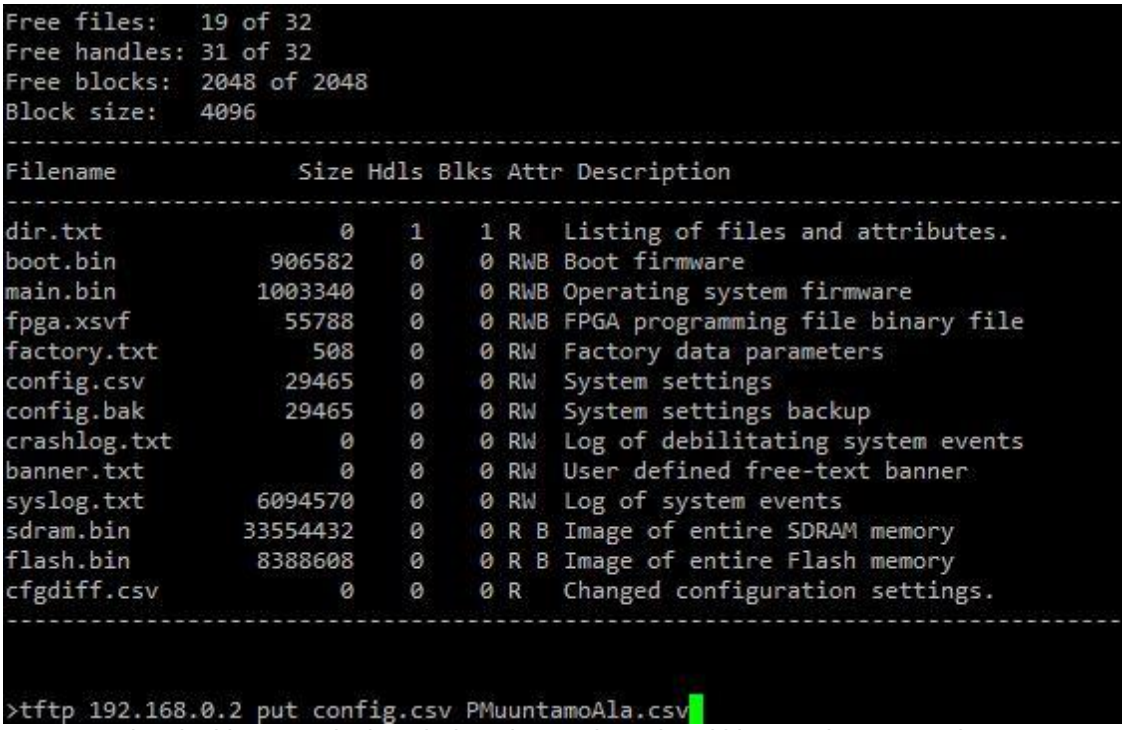
Kuva 20. Syslog-palvelimen määritys

5.4.2 Laiteasetusten tallennus TFTP-palvelimelle

Kun edellä mainitut asetusmuutokset oli tehty, komentorivin kautta kerättiin TFTP:n avulla kaikista kytkimistä laiteasetukset talteen verkonvalvontakoneelle. Tämä tapahtui komentorivin kautta, johon siirryttiin päävalikosta painamalla näppäinyhdistelmää CTRL + S (kuva 21).

Kuva 21. Vaihto valikkonäkymästä komentoriville

Dir-komennolla selvisi tiedosto, johon kytkimet tallensivat laiteasetukset. Kuvassa olevalla komennolla tiedostot siirrettiin valvontakoneelle (kuva 22).



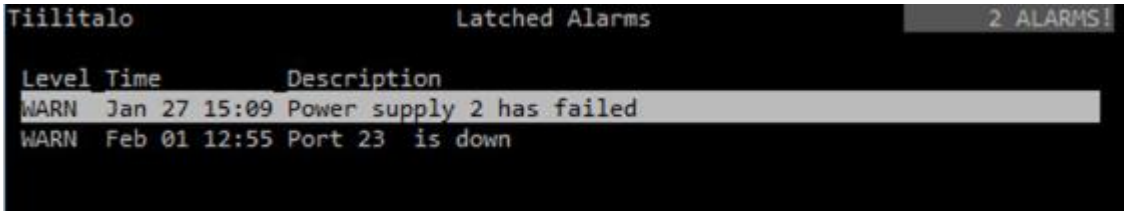
Kuva 22. Lista kytkimessä olevista tiedostoista, sekä esimerkki TFTP-komennon käytöstä

TFTP-komennossa käytetyt eri muuttujat tarkoittavat seuraavia asioita: IP-osoite 192.168.0.2 on kohdeosoite, johon TFTP-tiedostot lähetetään. Put-käskyllä määritetään tiedoston lähetys (get-käskyllä voidaan hakea tiedosto). Config.csv on tiedosto, joka halutaan lähettää. PMuuntamoAla.csv on itsemääritetty nimi, jolla tiedosto tallennetaan palvelimen päässä.

Koska kytkimissä on toisiinsa verrattuna samankaltaiset asetukset, vikatilanteessa tai uutta kytkintä käyttöönotettaessa olisi mahdollista ladata minkä tahansa kytkimen asetusmääritykset valvontakoneelta. Asetusmuutokset tulisi tehdä hallinta IP-osoitteen ja laitteen nimen osalta.

5.4.3 Hälytykset kytkimissä

Ruggedcom-kytkimissä on oletuksena käytössä laitekohtaiset hälytykset. Jos laitteessa on jokin laukaissut hälytyksen, niin siitä näkyy ilmoitus päävalikossa. Myös laitteessa itsessään syttyy punainen LED-valo hälytyksen aikana. Hälytyksen tarkemmat tiedot löytyivät siirtymällä ensin Diagnostics, sitten Latched Alarms -alavalikkoon (kuva 23).



Kuva 23. Laitteen aktiiviset hälytykset

Useassa laitteessa oli aiemmin tapahtuneen sähkökatkon takia hälytyksiä, joiden paikkansapitävyys tuli tutkia. Esimerkiksi niissä laitteissa, joissa oli kahdennettu virransyöttö, saattoi toinen virtalähteistä hälyttää kuvan 22 mukaisesti. Kun varmistuttiin laitteiden toimivan normaalisti, hälytykset poistettiin Diagnostics-alavalikossa valitsemalla Clear Alarms. Ainoastaan Tiilitalo-nimisessä kytkimessä jäi voimaan hälytys laitteen toisesta virtalähteestä. Tämä johtui siitä, ettei siihen oltu kytketty sähkövirtaa.

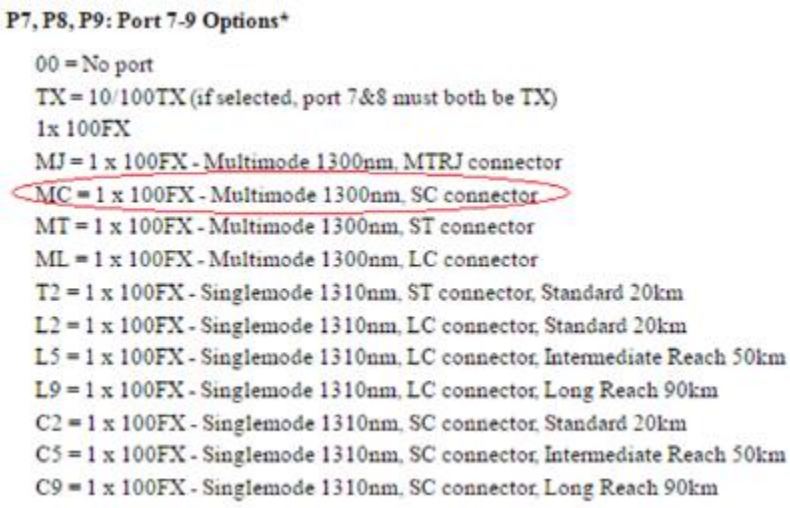
5.4.4 Koskenkorvan sähköaseman kytkin

Vuoden 2016 aikana sähköverkkoon liittyneelle Koskenkorvan sähköasemalle tarvittiin oma kytkin. Koska käytettävissä ei ollut Ruggedcom-kytkimiä, päätettiin sen sijaan käyttää laitevalmistaja Ciscon C2960X-sarjan kytkintä. Ennen varsinaista käyttöönottoa oli varmistettava, että kyseinen kytkin on mahdollista kytkeä

Ruggedcom-kytkimeen. Tämä tapahtui hallitussa testiympäristössä ja kytkimiä ei yhdistetty muihin verkkoihin.

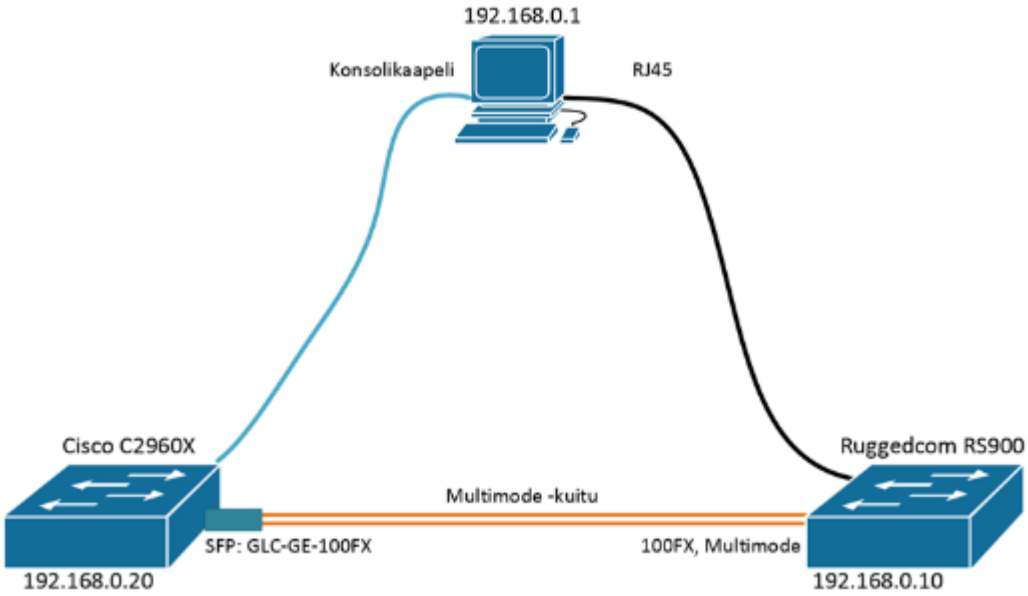
Kytkiminä testissä oli Ciscon C2960X, sekä Ruggedcom RS900 -kytkimet. Testauksessa käytettiin kytkinten lisäksi tietokonetta, jolla asetusmääritykset tehtiin. Koska yhteyttä ei onnistuttu muodostamaan RS900-kytkimen ja tietokoneen välillä konsolikaapelilla, määritettiin tietokoneelle osoite samasta aliverkosta. Tämän jälkeen kytkin ja tietokone kytkettiin toisiinsa RJ45-kaapelilla. C2960X-kytkin ja tietokone kytkettiin toisiinsa Ciscon konsolikaapelilla.

Testin tavoitteena oli yhdistää kytkimet valokaapelilla ja tätä varten tuli selvittää RS900-kytkimeen kiinnitetyn valokuitumoduulin tekniset tiedot. Tätä moduulia ei voitu irrottaa laitteesta, mutta C2960X-kytkimeen voitiin valita yhteensopiva moduuli. RS900-kytkimessä Product Information -alavalikossa selvisi käytössä ollut moduulin tuotekoodi ja laitteen ohjekirjasta tuotekoodia vastaava moduulitieto, joka on kuvassa ympyröitynä (kuva 24).



Kuva 24. RS900-kytkimeen asennettavat kuitumoduulit

C2960X-kytkimeen moduuliksi valittiin GLC-GE-100FX. Tämän jälkeen laitteet kytkettiin toisiinsa monimuotokuidulla (kuva 25).



Kuva 25. Kaaviokuva testikytkennästä

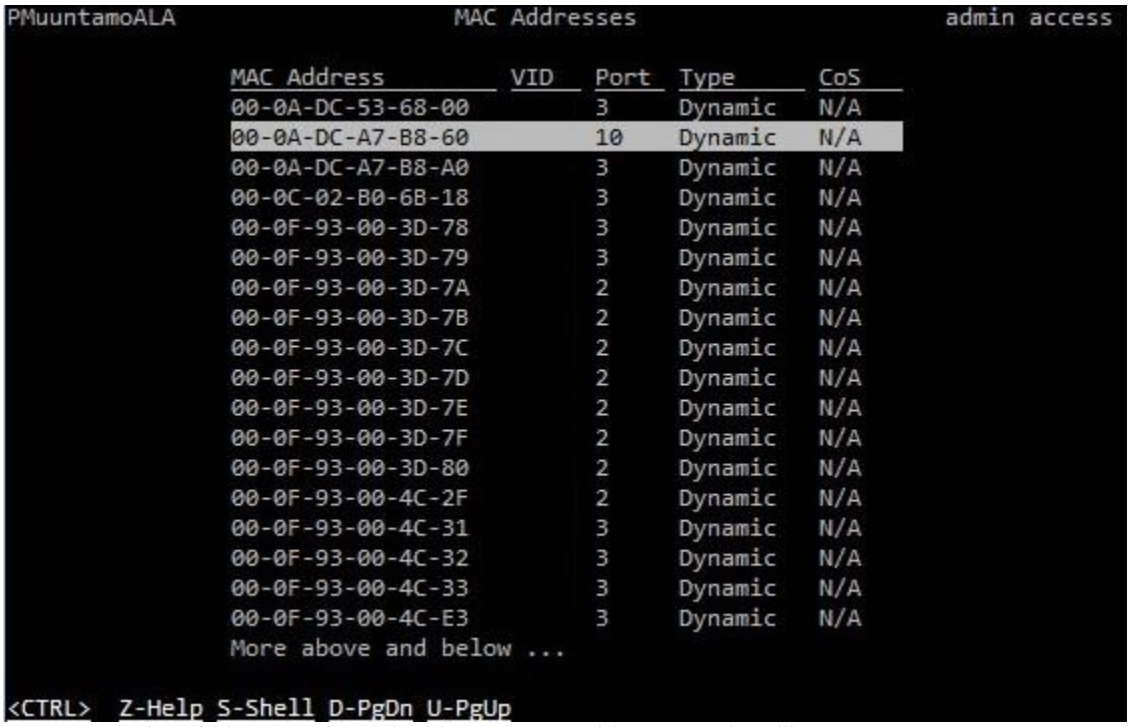
Testikytkennässä ei ilmennyt ongelmia ja tiedonsiirto laitteiden välillä onnistui. Tämän jälkeen tarkasteltiin C2960X-kytkimen sijoitusta kentällä ja todettiin, että kytkennän toisessa päässä oli Ruggedcom RSG2300 -kytkin ja linkkivälillä käytettiin yksimuotokuitua. RSG2300-kytkimessä oli kuitumoduulina 100FX. C2960X-kytkimeen ei ollut käytettävissä tähän sopivaa yksimuotokuitumoduulia, joten päädyttiin käyttämään 1000Base-LX moduulia. Jotta kytkentä kentällä onnistui, asennettiin laitteiden välille CTC Unionin valmistama mediamuunnin, joka muuntaa kuitusignaalin kupari-signaaliksi ja toisinpäin (kuva 26).

Kuva 26. Lopullinen kytkentä kentällä

5.4.5 Porttikytkentöjen selvittäminen

Aiemmasta verkkodokumentaatiosta ei selvinnyt laitteiden välisiä porttikytkentöjä. Nämä tuli selvittää, sillä mahdollisissa vikatilanteissa tieto tehdyistä kytkennöistä nopeuttaisi vian löytämistä. Apuna tässä käytettiin kytkimien ARP-kyselyjä, joiden avulla voidaan selvittää laitteen IP-osoitetta vastaava MAC-osoite.

Ruggedcom-kytkimissä MAC Addresses -alavalikossa oli listattuna taulukkoon kaikki MAC-osoitteet, joiden kanssa kytkin oli kommunikoinut. MAC-osoitteen jälkeen taulukossa oli virtuaalinen lähiverkko, johon kohdelaite kuului. Lisäksi selvisi portti, mitä kautta laite löytyi (kuva 27). Koska verkon yhdyskäytävänä käytettiin SCADA-palomuuria, selvitettiin MAC-osoitetta vastaava IP-osoite sen avulla (kuva 28).



Kuva 27. Esimerkki Ruggedcom-kytkimen MAC Addresses -alavalikosta

Kuva 28. Esimerkki palomuurissa tehtävästä ARP-kyselystä

Vastaavilla kyselyillä saatiin selville tärkeimpien porttikytkentöjen tiedot, mutta osassa laitteista ei löytynyt MAC-osoitetta vastaavaa IP-osoitetta. Tämä saattoi johtua esimerkiksi siitä, että laitteiden välillä ei ollut tietoliikennettä, mutta MAC-osoitetaulukkoon oli jäänyt merkintä aiemmasta kommunikoinnista. MAC Address Tables -alavalikossa oli toiminto Purge MAC Address Table, joka olisi tyhjentänyt kytkimen MAC-taulukon, mutta tämän toimintaa ei kokeiltu tuotantoverkossa.

5.5 Fyysinen tietoturva

Lähes kaikkien asemien fyysisestä tietoturvasta oli huolehdittu hyvin. Useat kohteet olivat aidattuja ja laitetilojen ovet olivat lukittuina, eikä laitteiden sijainti ollut helposti löydettävissä. Muutamaan kohteeseen oli verrattain helppo pääsy, sillä laitteet olivat sijoitettu ikkunan läheisyyteen. Näille laitteille tulisi suunnitella suojatummat paikat, etenkin kriittisimmissä solmupisteissä, kuten Tiilitalolla ja Päämuuntamolla.

Kameravalvontaa ei ollut käytössä missään. Toisaalta kameravalvontaa ei olisi suositeltavaa otettavan käyttöön SCADA-verkon kytkimissä johtuen sen aikakriittisistä tehtävistä. Myöskään nykyisten käytössä olevien kytkimien porttinopeudet eivät ole riittävät kameraliikennekäyttöön. Paras ratkaisu tähän olisi varata vain kamerakäyttöön omat kytkimet ja niissä ei tulisi liikkua SCADA-verkkoon kuuluvaa tietoa.

6 LOPPUPÄÄTELMÄT

Kokonaisuudessaan työ oli onnistunut, vaikka osa alkuperäisistä tavoitteista ei toteutunut. Tämä johtui osittain siitä, että aiheeseen oli perehdyttävä teoriatasolla ennen työvaiheen aloittamista. Työssä aikaa kului kytkimiin ja niiden asetuksiin tutustuessa. Verkonhallintakoneen käyttöönotossa aikaa kului eniten WhatsUp Goldin asennuksessa, mutta se osoittautui yhdeksi tärkeimmistä työkaluista verkonvalvonnassa. Dokumentaatiota tehdessä oli suuri apu aiemmista kaaviokuvista ja IP-taulukoista, mutta oli tärkeää tehdä niistä paremmat pohjat, joita voidaan päivittää jatkossa. Alkuperäisen suunnitelman mukaan tarkoitus oli myös suunnitella sähköverkon laitteiden päivitystä siten, että kaikki laitteet olisivat käyttäneet IEC 61850 standardia, mutta tähän ei aika riittänyt.

Lopputuloksena verkon tietoturvaa saatiin parannettua laiteasetusten kautta, sekä verkonhallintakoneen avulla. Hallintakoneen hyöty nähtiin jo pian sen käyttöönoton jälkeen, kun verkossa tapahtui jatkuvia sähkökatkoja yhdellä ala-asemista ja siitä saatiin hälytykset sähköpostitse. Koska Karhuvoiman henkilöstö oli mukana hälytysten sähköpostijakelulistalla, he pystyivät aloittamaan selvityksen

ja korjaustyöt aiempaa nopeammin. Syslog-palvelimesta saatiin myös uusi työväline verkon vikatilanteiden selvittämiseen. Työn aikana tehtyjä asetusmäärityksiä voidaan jatkossa hyödyntää kytkinten käyttöönotossa, joka osaltaan säästää aikaa. Kytkinten hallinnasta saatiin turvallisempaa kytkemällä turhat käyttäjätilit pois ja kun salasanat yhdenmukaistettiin. Päivitetyn dokumentaation avulla häiriötilanteiden selvitys nopeutuu, kun laitteiden oikeat sijainnit ja porttikytkennät ovat tiedossa.

Jatkokehityksenä verkossa voisi olla kameravalvonnan käyttöönotto, sekä kytkinten käyttöjärjestelmäpäivitykset tai päivittäminen kokonaan uusiin laitteisiin. Jos päätetään pitäytyä nykyisissä kytkimissä, olisi hyvä perehtyä niiden muihinkin ominaisuuksiin, kuten esimerkiksi Spanning Tree -protokollan asetuksiin. Ruggedcom-kytkimissä olisi mahdollista käyttää Siemensin kehittämää eRSTP-protokollaa (enhanced Rapid Spanning Tree), mutta sitä ei tällä hetkellä hyödynnetä verkossa lainkaan. Sen avulla verkossa tapahtuvista mahdollisista katkoista toivuttaisiin nopeammin. Kytkinten porttisuojausasetusten käyttöä olisi mahdollista ottaa käyttöön ainakin niissä porteissa, joissa tiedetään pysyvän samat kytkennät pitkään. Kytkinten hallinnassa turvallisuutta voitaisiin parantaa nykyisten käyttäjätunnusten ja salasanojen lisäksi käyttämällä RADIUS tai TACACS+ -tunnistuspalvelinta. Myös linkkivälien kahdennuksia tulisi suunnitella ja toteuttaa, ainakin kriittisimmillä väleillä.

LÄHTEET

670 series 2.0 IEC - IEC 61850 Edition 2 Communication Protocol Manual, 2014. ABB AB, Substation Automation Products. Saatavissa: https://library.e.abb.com/public/d12b928653b5c627c1257d940039f26a/1MRK511303-UEN_-_en_Communication_protocol_manual__IEC_61850_Edition_2__670_series_2.0__IEC.pdf [viitattu 3.10.2016].

DCS or PLC? - Seven Questions to Help You Select the Best Solution. 2007. Laitevalmistaja Siemensin kotisivut. Saatavissa: http://w3.siemens.com/mcms/process-control-systems/SiteCollectionDocuments/efiles/pcs7/support/marktstudien/PLC_or_DCS.pdf [viitattu 24.10.2016].

Essentials of the Modern DCS. 2015. Laitevalmistaja Rockwell Automation kotisivut. Saatavissa: http://literature.rockwellautomation.com/idc/groups/literature/documents/sp/proces-sp050_-en-e.pdf [viitattu 2.11.2016].

Kotkan Energia Oy. 2016. Yrityskuvaus. Kotkan Energia Oy:n kotisivut. Saatavissa: http://www.kotkanenergia.fi/fi/yritys-0 [viitattu 16.11.2016].

Pyyskänen, S. 2009. Teollisuusautomaatio- ja ohjausjärjestelmät – standardien valinta ja käyttö. Verkkojulkaisu. Suomen Automaatioseura ry:n internetsivut. Saatavissa: http://www.automaatioseura.fi/site/assets/files/1367/standardikirja.pdf [viitattu 5.10.2016].

Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. 2016. Verkkojulkaisu. U.S. Department of Homeland Security. Saatavissa: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf [viitattu 8.11.2016].

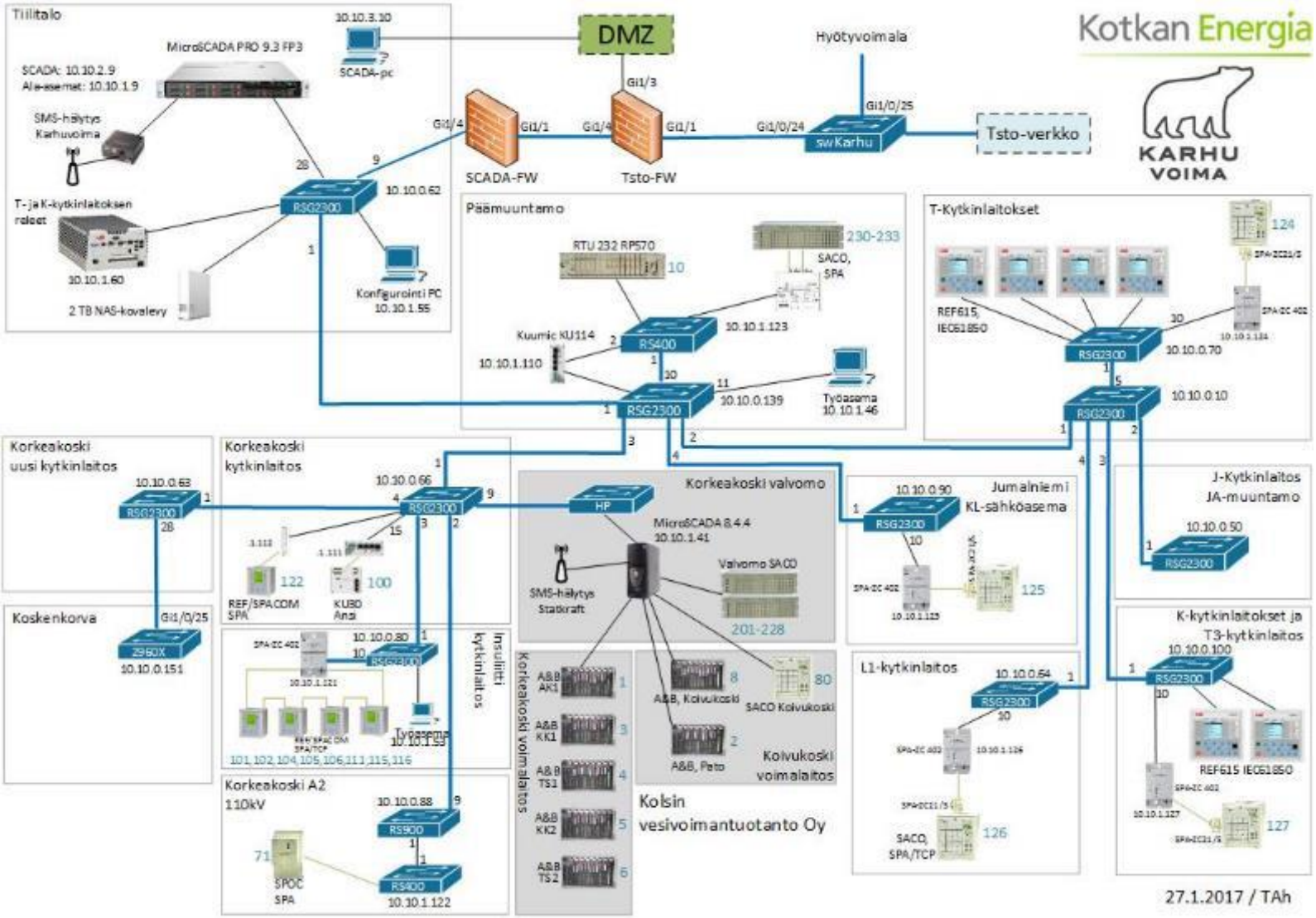
RUGGEDCOM RS900 ROS v4.3 User Guide. 2016. Käyttöohje. Laitevalmistaja Siemensin kotisivut. Saatavissa: https://cache.industry.siemens.com/dl/files/197/109737197/att_889252/v1/ROS_v4.3_RS900_User-Guide_EN.pdf [viitattu 7.3.2017].

RUGGEDCOM RSG2300. 2017. Verkkolaitteen tuote-esittely. Laitevalmistaja Siemensin kotisivut. Saatavissa: http://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/products/switches-routers-layer-2/pages/rsg2300.aspx [viitattu 22.4.2017].

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. & Hahn, A. 2015. Guide to Industrial Control Systems (ICS) Security. Verkkojulkaisu. Saatavissa: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf [viitattu 28.10.2016].

Teollisuusautomaation tietoturva - verkottumisen riskit ja niiden hallinta. 2010. Suomen Automaatioseuran julkaisusarja nro 29. Helsinki: Suomen Automaatioseura ry. Saatavissa: https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf [viitattu 4.10.2016].

Liite 1/1


Tiilitalo
10.10.3.10
SCADA-pc
MicroSCADA PRO 9.3 FP3
SCADA: 10.10.2.9
Ala-asemat: 10.10.1.9
SMS-hälytys
Karhuvoima
T- ja K-kytkinlaitoksen releet
10.10.1.60
2 TB NAS-kovalevy
RSG2300
10.10.0.62
Konfigurointi PC
10.10.1.55
DMZ
SCADA-FW
Tsto-FW
Hyötyvoimala
swKarhu
Tsto-verkko
Kotkan Energia
KARHU VOIMA
Päämuuntamo
RTU 232 RP570
10
230-233
SACO, SPA
Kuumic KU114
10.10.1.110
RS400
10.10.1.123
RSG2300
10.10.0.139
Työasema
10.10.1.46
T-Kytkinlaitokset
124
REF615, IEC61850
RSG2300
10.10.0.70
10.10.0.10
Korkeakoski uusi kytkinlaitos
10.10.0.63
Korkeakoski kytkinlaitos
10.10.0.66
122
REF/SPACOM SPA
100
KUBO Ansi
Korkeakoski valvomo
HP
MicroSCADA 8.4.4
10.10.1.41
SMS-hälytys Statkraft
Valvomo SACO
201-228
Jumalniemi KL-sähköasema
10.10.0.90
125
J-Kytkinlaitos JA-muuntamo
10.10.0.50
Koskenkorva
Gi1/0/25
2960X
10.10.0.151
Insulitti kytkinlaitos
10.10.0.80
RS400
10.10.1.121
101,102,104,105,106,111,115,116
Korkeakoski voimalaitos
A&B AK1
A&B KK1
A&B TS1
A&B KK2
A&B TS2
A&B, Koivukoski
SACO Koivukoski
A&B, Peto
Koivukoski voimalaitos
Kolsin vesivoimantuotanto Oy
L1-kytkinlaitos
10.10.0.64
SACO, SPA/TCP
126
K-kytkinlaitokset ja T3-kytkinlaitos
10.10.0.100
REF615 IEC61850
127
Korkeakoski A2
110kV
10.10.0.88
RS900
RS400
10.10.1.122
71
SPOC
SPA
27.1.2017 / TAh