



Osaamista  
ja oivallusta  
tulevaisuuden  
tekemiseen

Eemeli Purmonen

# Selvitys veden tuotantojärjestelmän automaation tiedonsiirrosta

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikka

Insinöörityö

31.5.2019

Tekijä Otsikko Sivumäärä Aika	Eemeli Purmonen Selvitys veden tuotantojärjestelmän automaation tiedonsiirrosta 28 sivua 31.5.2019
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	Sähkö- ja automaatiotekniikka
Ammatillinen pääaine	Automaatiotekniikka
Ohjaajat	automaatioteknikko Timo Leppänen automaatiosuunnittelija Juha Arvas lehtori Jaana Wuorila-Stenberg
<p>Insinööriä tehtiin Kymen Vesi Oy:lle ja Kymenlaakson Vesi Oy:lle, jotka toimivat vesihuoltolaitoksina. Insinööriä tarkoituksena oli tutustua vesilaitosten käyttämiin tiedonsiirtoyhteyksiin sekä selvittää nykyisten järjestelmien tietoturvasuorituksia. Työn tarkoituksena oli antaa vesilaitoksille myös vaihtoehtoisia tapoja, miten nykyistä vedentuotanto ja -jakelu järjestelmää lähdetään päivittämään.</p> <p>Vesilaitosten tiedonsiirto toteutetaan pääsääntöisesti operaattorilta hankitulla yritysverkolla sekä omalla radioverkolla. Vesilaitosten alueilla on käytössä myös omia valokuituverkkoja. Työssä tutustutaan tarkemmin radiomodeemeilla toteutettavaan tiedonsiirtoon sekä yritysverkon hankinnassa huomioon otettaviin aiheisiin, kuten palveluntasosopimukseen. Radioverkon tiedonsiirrossa esimerkkinä toimivat Suomalaisen Satel Oy:n radiot. Työ toteutettiin nykyisen järjestelmän dokumentteihin tutustuen.</p> <p>Insinööriä tehtiin VTT:n tekemän kyber-turva-vesi-hankkeen johdosta. Hankkeessa syntyneiden dokumenttien pohjalta Kymen Vesi ja Kymenlaakson Vesi ovat havahtuneet tietoturvan merkitykseen ja haluavat parantaa oman toimintansa kyberturvallisuutta. Vesilaitosten toiminnassa onkin paljon erinäisiä kohteita, joiden tietoturvaa voidaan kehittää.</p> <p>Työn tuloksena Kymen Vesi ja Kymenlaakson Vesi voivat aloittaa automaatiojärjestelmän päivittämisen sekä käynnistää tietoturvasuoritusprosessin, joka kattaa vesilaitosten elinkaaren loppuun saakka.</p>	
Avainsanat	Vesilaitos, Yritysverkko, Radiomodeemi

Author Title	Eemeli Purmonen Exploration of Waterworks Automation Data Transfer
Number of Pages Date	28 pages 31 May 2019
Degree	Bachelor of Engineering
Degree Programme	Electrical and Automation Engineering
Professional Major	Automation Engineering
Instructors	Timo Leppänen, Automation Technician Juha Arvas, Automation Engineer Jaana Wuorila-Stenberg, Senior Lecturer
<p>This thesis study was commissioned by Kymi Water Ltd and Kymenlaakso Water Ltd, which are waterwork companies. The purpose of the project was to get to know how waterworks transfer their data and to find out the current security levels of the system. The purpose of the project was also to give waterworks some alternative ways on how they could update their system.</p> <p>Waterworks use mainly a corporate network and their own radio network to transfer their data. Corporate network is purchased from the operator. Water supply plants also use their own fiber optic networks. This study explores in detail the data transfer with radio modems and issues to be considered in the acquisition of corporate network, such as a service level agreement. Examples of radio networks include Finnish Satel Ltd products. This study was carried out by reviewing the documents of the current system.</p> <p>A cyber-safety-water -project done by VTT allowed Kymi Water and Kymenlaakso Water to have a better understanding of the importance of information security and want to improve the cyber security of their system. There are a lot of things in the water supply system that can be developed for information security.</p> <p>The results of the project allow Kymi Water and Kymenlaakso Water to start upgrading their automation system and launch an information security process, that covers the waterworks for the entire duration that it is operational.</p>	
Keywords	Waterworks, Corporate network, Radio modem

# Sisällys

## Lyhenteet

1	Johdanto	1
2	Kymenlaakson Vesi Oy ja Kymen Vesi Oy	2
3	Nykyinen automaatiojärjestelmä	6
3.1	Vedentuotannon ja -jakelun tiedonsiirtoyhteydet	7
3.2	Radiomodeemiyhteydet	7
3.3	Valvomot	8
3.4	Etäyhteydet	9
3.5	Yritysverkko	9
4	Tietoturva automaatiassa	10
4.1	Tietoturva vesihuollossa	10
4.2	Fyysinen tietoturva	11
4.3	Kyber-turva-vesi-hanke	12
5	Yritysverkko	13
5.1	Yritysverkon toiminta	13
5.2	Yritysverkon vaatimukset	14
6	Radiomodeemit ja langaton tiedonsiirto	15
6.1	Satel	16
6.2	Radiolinkit	18
6.3	4G-yhteys	18
7	Langattoman tiedonsiirron kehittäminen	19
8	Yritysverkon ja palvelimien hankinta	22
8.1	Valvomopalvelimet	22
8.2	Elinkaari	24
9	Yhteenveto	25



## Lyhenteet

ADSL	Asymmetric digital subscriber line. Epäsymmetrinen laajakaista.
AES	Advanced Encryption Standard. Edistynyt salausstandardi.
DMZ	Demilitarized zone. Demilitarisoitu alue.
GPRS	General Packet Radio Service. Pakettidatan siirtopalvelu GSM-verkossa.
IDS	Intrusion Detection System. Tunkeutumisenhavaitsemisjärjestelmä.
PLC	Programmable Logic Controller. Ohjelmoitava logiikka.
SCADA	Supervisory control and data acquisition. Valvomojärjestelmä.
SLA	Service Level Agreement. Palveluntasosopimus.
VPN	Virtual Private Network. Virtuaalinen yksityisverkko.

## 1 Johdanto

Insinööritö tehdään Kymen Vesi Oy:lle sekä Kymenlaakson Vesi Oy:lle. Yritykset toimivat vesilaitoksina, jotka tuottavat ja jakelevat puhdasta talousvettä kuluttajille sekä puhdistavat kuluttajien jätevedet. Tässä työssä keskitytään puhtasvesipuolen automaation tiedonsiirtoratkaisuihin sekä käytössä olevan automaatiojärjestelmän tietoturvaan.

Työn tarkoitus on selvittää vesilaitoksien nykyisten automaatiojärjestelmien tila sekä antaa kuva automaatiojärjestelmien tietoturvallisuudesta. Työssä tullaan myös esittelemään tarkemmin yritysverkon hankintaa sekä radiomodeemeilla toteutettavaa tiedonsiirtoa. Työ tehtiin VTT:n tekemän Kyber-Turva-Vesi-hankkeen johdosta, missä vesilaitoksille luotiin ohjeita ja työkaluja kyberturvallisuuden kehittämiseen.

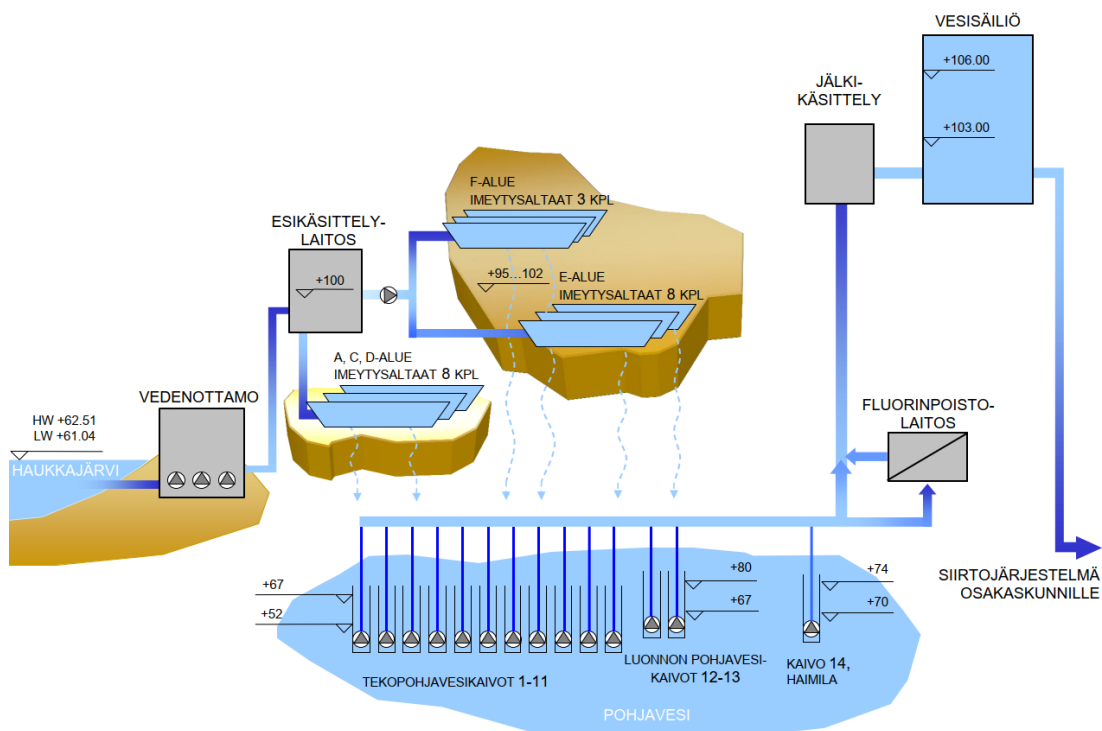
Tässä työssä esitellään ensin vedentuotantoa ja -jakelua sekä nykyisiä tiedonsiirtoratkaisuja. Näitä erilaisia tiedonsiirtotapoja ovat esimerkiksi yritysverkot, jotka ovat osa automaatioverkkoa, sekä käytettävät radiomodeemiverkot. Työn loppupuolella tullaan esittelemään eri vaihtoehtoja radiomodeemien hyödyntämiseen sekä huomioita siitä, mitä yritysverkon hankinnassa tulee ottaa huomioon. Kaikissa osa-alueissa pyritään painottamaan asiaa tietoturvan näkökulmasta. Tässä työssä ei käsitellä jätevesipuolen toimintaa.

## 2 Kymenlaakson Vesi Oy ja Kymen Vesi Oy

Kymenlaakson Vesi Oy on vesilaitos, joka tuottaa puhdasta talousvettä asiakkailleen. Kyseinen vesilaitos toimii tukkuvesilaitoksena, jonka asiakkaita ovat osakaskunnat Kotka, Hamina ja Kouvola. Osakaskuntien tehtävä on huolehtia talousvedenjakelusta loppukäyttäjille. Varsinaisia talousveden kuluttajia Kymenlaakson Vedellä ei siis ole asiakkainaan. Kymenlaakson Veden tukkuvesilaitos sijaitsee Kuivalassa, Valkealassa. Kymenlaakson Veden tekopohjavesilaitoksen ohjaus on pitkälle automatisoitu ja täten henkilökunnan tarve on vähäinen. [1.]

Kuvassa 1 on esitetty Kuivalan tekopohjavesilaitoksen eri vaiheet, joita ovat:

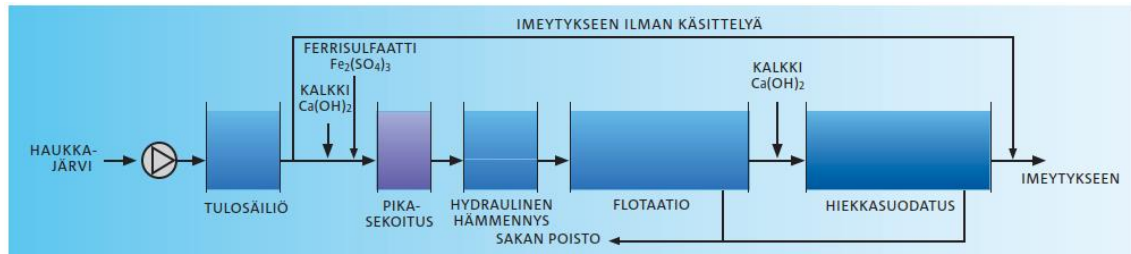
- raakaveden pumppaus
- esikäsittely
- imeytys
- tekopohjaveden pumppaus
- fluorinpoisto
- jälkikäsittely. [1.]



Kuva 1. Vedenpuhdistusprosessin eri vaiheet [1, s. 3].



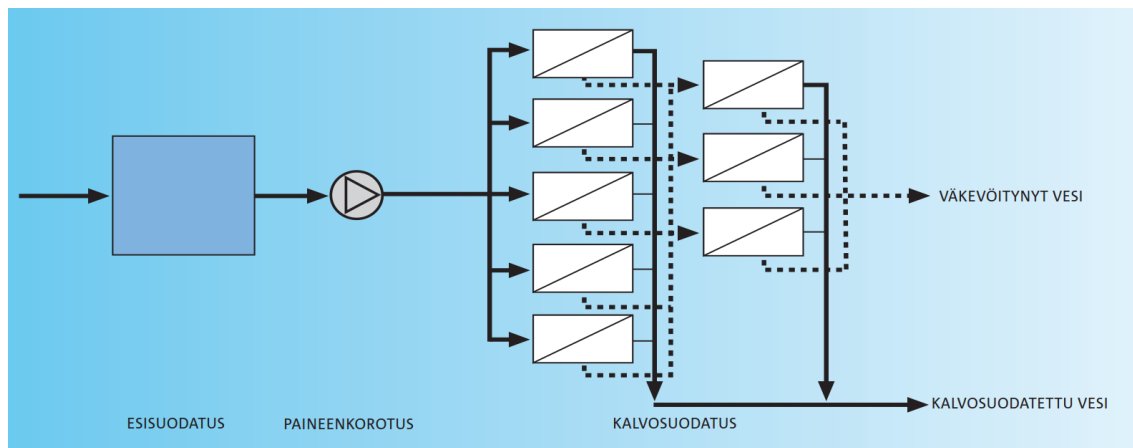
Tukkuvesilaitoksena toimiva Kymenlaakson Vesi käyttää raakavetenään Haukkajärven pintavettä. Tekopohjavesilaitokselle pumpatusta raakavedestä noin puolet esikäsitellään ennen sen imeyttämistä Kuivalan soraharjuun. Esikäsitelyllä saadaan parannettua tekopohjaveden laatua sekä kevennettyä epäpuhtauksien aiheuttamaa kuormaa maaperälle. Kuvasta 2 voi havaita esikäsitelyyn liittyvät vaiheet. [1.]



Kuva 2. Esikäsitelyn eri vaiheet [1, s. 4].

Tekopohjavesilaitoksella on 19 eri imeytysallasta, joista vesi imeytetään maaperään. Imeytyminen kestää noin 30–50 vuorokautta, jonka aikana vedestä poistuu muun muassa bakteereja. Kun vesilaitos käyttää raakavetenä pohjavettä tai tekopohjavettä, on veden puhdistusprosessi huomattavasti kevyempi maaperän puhdistusominaisuuksien ansiosta. Imeytetty raakavesi pumpataan 11:sta eri siiviläputkikaivosta takaisin vesilaitokselle tekopohjavedenä. Vesilaitokselle pumpataan myös luonnon pohjavettä kolmesta kaivosta. [1.]

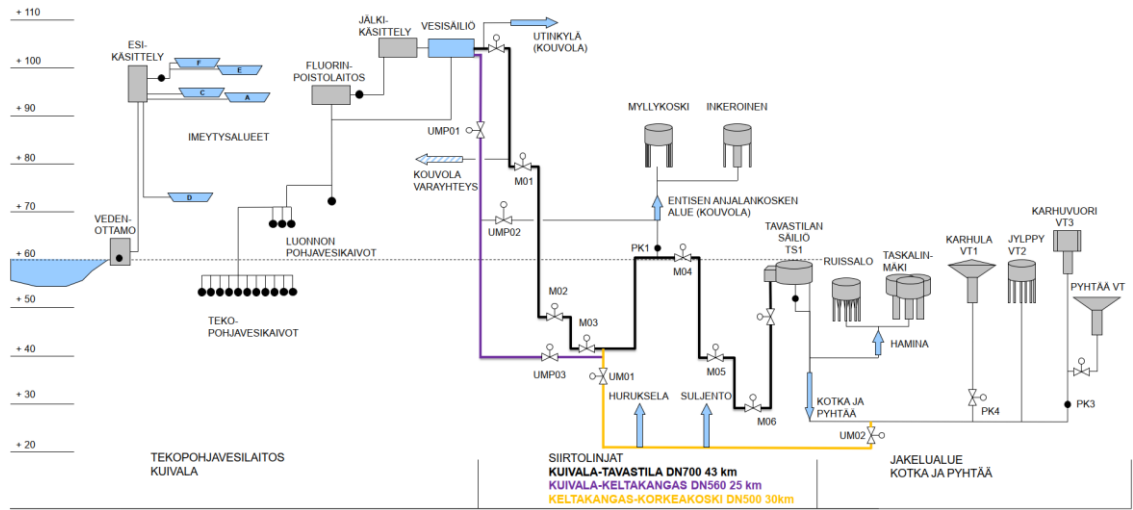
Tekopohjaveden käsittely aloitetaan fluoridipitoisuuden vähentämisellä. Fluoridi on maaperästä imeytynyt aine, jonka pitoisuus talousvedessä saa olla enintään 1,5 mg/l. Fluoridipitoisuutta vähennetään kalvosuodatuslaitoksessa. Kuvassa 3 näkyy kalvosuodatukseen kuuluvat kokonaisuudet. Fluoridi saadaan poistettua käänteisosmoosiin perustuvalla käsittelyllä, missä tekopohjavesi johdetaan paineella puoliläpäisevien kalvojen läpi. [1.]



Kuva 3. Fluoridin poisto [1, s. 4].

Ennen veden johtamista verkostoon se alkaloidaan kalkilla ja hiilidioksidilla sekä desinfioidaan klooriamiinikloorauksella. Alkaloinnin tarkoitus on vähentää veden syövyttävyyttä, missä veden pH-arvo säädetään sopivaksi vedenjakeluverkoston korroosion estämiseksi. Klooriamiinikloorauksessa veteen syötetään ammoniumsulfaattia ja natriumhypokloriittia. Klooriamiinikloorauksella varmistetaan desinfiointin tehokkuus erityisesti hyvin pitkillä viipymillä vesijohtoverkossa. Lopuksi vesi johdetaan Kuivalan lähtösäiliölle, mistä se siirretään osakaskunnille ja edelleen kuluttajille.

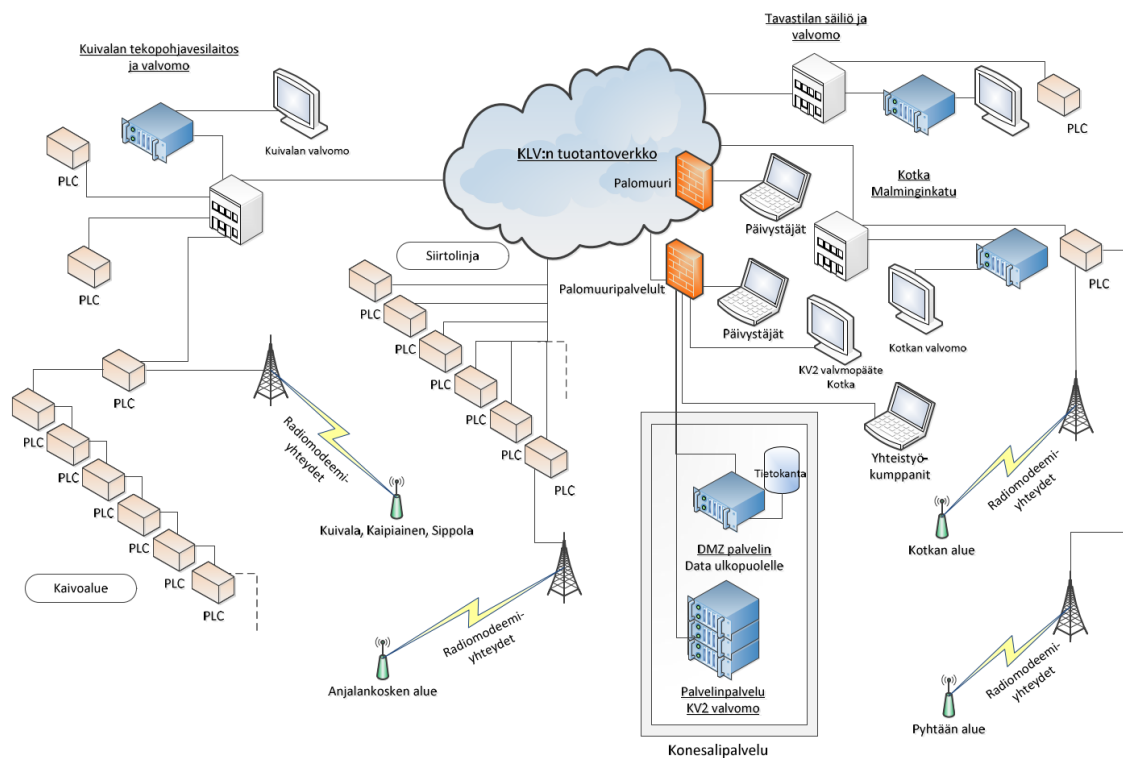
Talousveden jakamisesta asiakkaille huolehtii Kymen Vesi Oy. Talousvesi johdetaan painovoimaisesti kahdella runkolinjalla Kotkaan, mistä se johdetaan edelleen Kotkan, Haminan ja Pyhtään vesitorneille. Runkolinjoista ohjataan talousvettä myös Valkealaan ja Etelä-Kouvolan alueelle. Kuivalan lähtösäiliöstä lähtevän veden virtaama on keskimäärin noin  $830 \text{ m}^3/\text{h}$ , jolloin päivittäinen veden tarve on noin 20 miljoonaa litraa. Veden siirto vesitorneille sekä osakaskunnille on kuvattuna kuvassa 4. [1; 2.]



Kuva 4. Veden siirtoverkoston korkeuserot [1, s.7].

### 3 Nykyinen automaatiojärjestelmä

Nykyinen vesilaitosta ohjaava järjestelmä koostuu kuvassa 5 näkyvistä osista. Järjestelmän automaatio hyödyntää verkko-operaattorin tarjoamaa yritysverkkoa sekä Kymen Veden ja Kymenlaakson Veden omia radiomodeemiyhteyksiä. Automaatiojärjestelmä koostuu Kymen Veden ja Kymenlaakson Veden valvomoista sekä pääasemien ja alasemien ohjelmoitavista logiikoista, joita ovat kuvassa 5 olevat PLC:t (Programmable Logic Controller). Järjestelmässä on kolme erillisestä päävalvomoa sekä yksi virtuaalikoneella toteutettu valvomo. Vesilaitoksen valvomot sekä maastossa olevat pääasemat ovat yhteydessä toisiinsa operaattorin tarjoaman yritysverkon kautta. Maastossa hajallaan olevien ala-asemien tiedonsiirto on toteutettu pääsääntöisesti radiomodeemeilla. Muutamii ala-asemiin tiedonsiirtoyhteydet on toteutettu ADSL-yhteyksillä (Asymmetric digital subscriber line). Ala-asemiin kuuluvat vesilaitoksen pumppaamot, paineenkorotusasemat, mittausasemat, vesitornit ja mittakaivot. Kymenlaakson Vedellä on myös LoRa-tiedonsiirrolla toimivia mittalaitteita. Mittalaitteita käytetään sähköttömillä paikoilla, joissa halutaan seurata esimerkiksi pohjavesien tasoja. [3; 4.]



Kuva 5. Vedentuotannon automaatio ja tietoliikenne [5].

### 3.1 Vedentuotannon ja -jakelun tiedonsiirtoyhteydet

Vedentuotantoon liittyvät tiedonsiirtoyhteydet koostuvat verkko-operaattorin tarjoamista yritysverkon valokuitukaapeleista sekä Kymen Veden ja Kymenlaakson Veden omistamista radioverkoista. Kuivalan tekopohjavesilaitokselta on radiomodeemiyhteyksiä Kuivalan, Kaipiaisten ja Sippolan alueiden ala-asemiin. Ala-asemiin kuuluvat muun muassa vesitorni, kaivo ja vedenottamo. Tekopohjavesilaitoksen alueella sijaitseville kaivoille sekä raakavedenpumppaamolle tiedonsiirtoyhteydet on luotu omilla valokuituyhteyksillä. Vedentuotannon kannalta kriittisiin pisteisiin, kuten raakavedenpumppaamoon valokuituyhteydet ovat kahdennettuja tiedonsiirtoyhteyksien varmistamiseksi. [3; 4; 6.]

Vedenjakeluun tarvittavaan tiedonsiirtoon käytetään verkko-operaattorilta vuokrattuja kupariyhteyksiä sekä Kymen Veden ja Kymenlaakson Veden omistamia radioverkkoja. Verkko-operaattorin kuparikaapeleilla on luotu ADSL-yhteydet vedensiirtolinjalla oleviin ala-asemiin, joista yksi on jouduttu korvaamaan 4G-modeemilla operaattorin poistettua puhelinverkon kaapeleita alueelta. Operaattorin tarjoamissa yritysverkon yhteyksissä on käytössä GPRS-palvelu (General Packet Radio Service), jota käytetään asemien varayhteytenä. Radiomodeemeilla luotua radioverkkoa käytetään tiedonsiirtoon maastossa sijaitsevan pääaseman ja entisen Anjalankosken alueen ala-asemien välillä. Radiomodeemiyhteydet ovat myös Kotkan valvomosta Kotkan ja Pyhtään alueen ala-asemille. Vedenjakelussa ala-asemilla tarkoitetaan lähinnä vedenottamoita, paineenkorotusasemia, mittausasemia sekä vesitorneja. [3; 4; 6.]

### 3.2 Radiomodeemiyhteydet

Kymen Vedellä ja Kymenlaakson Vedellä on käytössä kymmeniä radiomodeemeja. Kaikki käytössä olevat radiomodeemit ovat Suomalaisen radiomodeemivalmistaja Satel Oy:n tuotteita. Radiomodeemeilla toteutettu radioverkko on käyttöön otettu noin 10 vuotta sitten, jolloin tiedonsiirto päätettiin toteuttaa Satelline tuoteperheen radiomodeemeilla. Kuntaliitosten myötä ala-asemia on tullut lisää ja radioverkkoa on laajennettu myös Satellar-tuoteperheen radiomodeemeilla. Näiden radiomodeemien suurin ero on käytettävä tiedonsiirtoprotokolla. Satellar-radiomodeemit tukevat sekä sarja että IP-tiedonsiirtoa toisin kuin Satelline-radiomodeemit, jotka toimivat vain sarjaliikenteellä. Kymen Veden ja Kymenlaakson Veden käyttämät radiomodeemit käyttävät luvanvaraisia radiotaajuuksia.

Luvanvaraisiin radiotaajuuksiin vaadittavasta radioluvasta sekä radiomodeemien toiminnasta kerron lisää työn loppupuolella. [3; 4; 6; 7; 8.]

### 3.3 Valvomot

Järjestelmää ohjataan kolmelta fyysiseltä valvomolta, joista yksi sijaitsee Kouvolassa ja kaksi Kotkassa. Valvomoiden ensisijainen tehtävä on toimia käyttöpäätteinä operaattoreille, jotka voivat ohjata järjestelmää valvomoiden näytöiltä. Toissijainen tehtävä on toimia varavalvomona. Normaalisissa tilanteissa, kun kaikki kolme valvomot ovat toiminnassa, Kuivalan valvomon tehtävä on huolehtia tekopohjavesilaitoksen toiminnasta sekä veden siirrosta Tavastilan vesisäiliölle. Tavastilan valvomon tehtävä on toimia varavalvomona. Kotkan päävalvomon ensisijainen tehtävä on huolehtia vedenjakeluun liittyvistä toiminnoista. Vedentuotannon ja -jakelun kriittisyyden vuoksi järjestelmän tulee olla riittävän luotettava ja varmistettu. Tästä syystä valvomot ovat toistensa kopioita pystyen tarvittaessa hoitamaan ensisijaisen ja toissijaisen tehtävänsä. Jokaiselle valvomolle on täten luotu myös omat yhteydet kaikkiin ohjattaviin asemiin. Tällä on mahdollistettu jokaisen valvomon mahdollisuus huolehtia koko järjestelmän ohjauksesta. Näin ollen yhden tai jopa kahden valvomon vikaantuminen ei estä vedentuotantoa ja -jakelua kuluttajille. [3; 4.]

Valvomoita käytettäessä käyttäjä tunnistetaan ennalta määritettyjen menetelmien mukaan. Käyttäjät jakautuvat katselijoihin, päivystäjiin ja pääkäyttäjiin. Katselijoilla on oikeudet vain järjestelmän seurantaan. Päivystäjällä on oikeudet ohjata järjestelmää asetettujen rajojen sisällä. Esimerkiksi linjan virtaamaa päivystäjä voi muuttaa sille asetettujen minimi ja maksimi arvojen välillä. Mikäli tulee tarve muuttaa kyseisen linjan virtaaman raja-arvoja, on se mahdollista vain pääkäyttäjän oikeuksilla. Automaatiojärjestelmätoimittajalla on järjestelmään rajoittamattomat oikeudet. Rajoittamattomia oikeuksia tarvitaan huolto- ja vikatilanteissa, jolloin mahdolliset rajoitukset estäisivät töiden tekemisen. [3; 4; 9.]

Kotkaan on sijoitettu myös virtuaalikoneella toteutettu valvomopääte. Valvomon palvelimet sijaitsevat fyysisesti palveluntarjoajan konesalissa. Konesalissa käytössä olevat virtuaalipalvelimet hakevat datansa suoraan pääasemilta. Haetuilla tiedoilla luodaan vedenjakelujärjestelmän seurantaan käytettävä valvomo. Virtuaalivalvomoa ei käytetä

vedentuotannon seurantaan eikä siihen ole myöskään rakennettu mahdollisuutta kirjoittaa pääasemille uusia arvoja. Konesalissa olevilla virtuaalipalvelimilla luotua valvomoa käytetään Kotkan toimiston valvomopäätteeltä. Pääasemien logiikoille tehtyjä hälytyksiä ja muita toiminnollisuuksia ei siis hyödynnetä virtuaalisessa valvomossa. Esimerkiksi mittaustietojen raja-arvohälytykset luodaan virtuaalivalvomossa pääasemilta haettujen arvojen perusteella niin sanottuina valvomotoimintoina. Virtuaalivalvomon käyttö vaatii myös tunnistautumisen, jolloin käyttäjälle määritetyt oikeudet mahdollistavat halutut toiminnot. Virtuaalisesta valvomosta voidaan myös turvallisesti siirtää tietoja ulos esimerkiksi kolmansille osapuolille. [3; 4; 10.]

### 3.4 Etäyhteydet

Järjestelmää voidaan ohjata ja valvoa myös etäyhteydellä. Fyysisiin valvomoihin, joista järjestelmää ohjataan, voidaan luoda etäyhteys käyttäjien tableteilta sekä päivystäjän kannettavalta tietokoneelta. Yhteys luodaan ensin muodostamalla VPN-yhteys (Virtual Private Network) operaattorin tarjoamalle hyppykoneelle. Hyppykoneella tarkoitetaan DMZ-alueella (demilitarized zone) sijaitsevaa palvelinta, jossa etäyhteyden luoja tunnistetaan ja yhteys sallitaan jatkumaan automaatiojärjestelmään. Etäyhteydellä käyttäjä kirjautuu järjestelmään samalla tavalla kuin valvomoonkin. Etäyhteyden luotuaan käyttäjä voi tehdä muutoksia valvomoon sekä järjestelmään käyttäjälle määritettyjen oikeuksien mukaan. Myös virtuaalivalvomoon voidaan luoda etäyhteys. Yhteys luodaan samalla tavalla kuin fyysisiin valvomoihin. [3; 11.]

### 3.5 Yritysverkko

Verkko-operaattorin tarjoamat yhteydet yhdistävät koko järjestelmän tiedonsiirron luoden Kymen Vedelle ja Kymenlaakson Vedelle yritysverkon. Yritysverkko on julkisesta internetistä operaattorin toimesta eriytetty verkko, jonka kautta valvomoiden ja pääasemien tiedot siirretään. Yritysverkon sopimus on laadittu noin 10 vuotta sitten, jolloin määriteltiin yhteydet, tiedonsiirtonopeudet sekä tarvittavat varayhteydet. Sopimuksessa verkko-operaattori veloitettiin myös järjestämään palomuu- ja etäyhteysspalvelut. [3.]

## 4 Tietoturva automaatiossa

Automaatiojärjestelmässä tietoturva on toiminnan elinehto. Tietoturvan pettämisellä voi olla tuhoisia seurauksia, ja tämän vuoksi automaatiojärjestelmien tietoturvaan tulee kiinnittää erityistä huomiota. Usein automaatiojärjestelmät on suojattu eristämällä ne muista verkoista fyysisesti tai tiukoilla palomuurisäännöillä. Automaation laitteet on myös sijoitettu paikkaan, missä saavutetaan riittävä fyysinen suojaus. Paikka voi olla esimerkiksi laitoksen vartioitu tuotantoalue. Automaatiojärjestelmässä toimivat laitteet vaativat virheettömän tiedonsiirron lisäksi jatkuvan saatavuuden, ja tästä syystä automaatiojärjestelmän suojaamiseen ei yleisesti voida hyödyntää kaikkia toimistoverkoissa käytettyjä tietoturvaominaisuuksia, kuten automaattista yhteyden estämistä poikkeavan toiminnan johdosta. Automaatiojärjestelmän suojaamiseen liittyy myös palautuminen mahdollisesta häiriöstä, joten järjestelmälle on hyvä olla valmiina suunnitelma tilanteen palauttamiseksi normaaliin tilaan. [12.]

### 4.1 Tietoturva vesihuollossa

Vesihuollossa on lukuisia kohteita, joiden tietoturvasuus tulee ottaa huomioon koko järjestelmän suojauksen toteutumiseksi. Ensisijaisesti tulee pyrkiä pitämään järjestelmä erillään julkisesta verkosta. Järjestelmän verkko tulee segmentoida toimintojen mukaisesti sopiviin kokonaisuuksiin. Segmentoinnilla saadaan kokonaisuus hallittavammaksi ja siten turvallisemmaksi. Järjestelmässä on myös hyvä käyttää haittaohjelmien torjuntaan soveltuvaa ohjelmaa. Virustorjuntaohjelman toiminnan varmistamiseksi tulee päivitykset hoitaa säännöllisesti, koska ohjelman toiminta perustuu tunnettujen haittaohjelmien vertailuun. Järjestelmän ollessa julkisesta verkosta erotettu tulee usein tarpeelliseksi etäyhteyden mahdollisuus. Sen luomiseksi tulee määrittää etäyhteyteen käytettävä laitteisto sekä käytäntö, miten yhteys luodaan. Käytännön tulee olla riittävän helppokäyttöinen. Helppokäyttöisyys ei kuitenkaan saa heikentää etäyhteyden tietoturvasuutta. [13.]

Vesihuollon käyttämissä verkoissa on hyvä olla myös järjestelmät, jotka tarkkailevat verkon liikennettä. IDS-järjestelmä (Intrusion Detection System) on hyökkäyksiä havainnoiva järjestelmä, jonka tarkoitus on tunnistaa verkossa tapahtuvia poikkeamia sekä reagoida niihin. Järjestelmän toiminta voi perustua esimerkiksi lokitietojen tarkkailuun tai



tiedostojärjestelmien muutosten havainnointiin. IDS-järjestelmällä on mahdollista estää poikkeamaksi tulkittu yhteys tai toiminta, mutta tämän ominaisuuden käyttö automaatioverkoissa voi aiheuttaa ongelmia normaalissa toiminnassa. Järjestelmä tulee esimerkiksi estäneeksi vääriä yhteyksiä luullessaan harvoin tapahtuvan hälytyksen olevan poikkeama. Järjestelmän havaitsemista poikkeamista on hyvä luoda hälytys, jonka perusteella ryhdytään tarvittaviin jatkotoimenpiteisiin. [14, s.15–20.]

Vesilaitoksilla tyypillinen ympäristö, jossa IDS-järjestelmä toimii, on SCADA-ohjausjärjestelmä (Supervisory control and data acquisition). SCADA-järjestelmän liikenne on toistuvaa ja siksi helposti opittavissa, koska automaatioverkossa olevat laitteet eivät vaihda toimintatapaansa. Esimerkkinä valvomon toistuvat kysymykset ala-asemille, joihin ala-asemien logiikat vastaavat. Automaatioverkossa tapahtuvat muutokset käyttäytymisessä on siis mahdollista havaita helpommin kuin toimistoverkoissa. [15, s.6.]

Automaatiojärjestelmän tietoturvaa voidaan parantaa koventamalla yksittäiset laitteet. Koventamisella tarkoitetaan laitteen toiminnallisuuksien rajaamista vain niihin toimintoihin, joita kyseinen laite tarvitsee toimintaansa. Kaikki palvelut ja ominaisuudet, joita ei käytetä, tulee poistaa käytöstä. Jokainen laite voi tahollaan toimia verkon niin sanottuna takaporttina eli tietoturva-aukkona. Kovennettavia laitteita ovat järjestelmän ohjaukseen käytettävät tietokoneet ja tabletit sekä verkon aktiivilaitteet, kuten palomuurit, kytkimet ja reitittimet. Koventamisen lisäksi laitteet tulee myös suojata riittävän vahvalla salasanalla sekä rajoittaa laitteiden etäyhteydet vain tarpeellisiin yhteyksiin. [16, s.73.]

## 4.2 Fyysinen tietoturva

Vesilaitoksilla on useita fyysisiä paikkoja, jotka sijaitsevat laajalla alueella. Fyysisen turvallisuuden mahdollistamiseksi onkin tärkeä tiedostaa kaikki paikat, joihin automaatioverkko tai -laitteet ulottuvat. Varsinkin ala-asemien fyysiseen turvallisuuteen tulee kiinnittää huomiota. Ala-asemalla sijaitsevat laitteet tulee suojata riittäväällä fyysisellä suojauksella sekä varautumalla mahdolliseen ilkivaltaan tarvittavalla varalaitteella sekä suunnitelmalla toiminnan palauttamiseksi. [17, s.4.] Ala-asemien fyysistä turvallisuutta voidaan tehostaa esimerkiksi automaattisella ilmoituksella aina, kun ala-aseman ovi avataan tai ala-aseman sisällä oleva liiketunnistin havaitsee liikettä. Näin saataisiin valvomon tieto, mikäli ala-aseman ovi murretaan tai sisälle on muuten onnistuttu

pääsemään. Sovitut ala-asemakäynnit olisivat kuitattavissa puhelulla tai vastaavalla, mutta tällä tavalla saataisiin tieto ala-asemaan kohdistuvasta hyökkäyksestä ennen kuin aseman tiedonsiirto häviää.

Fyysisen turvallisuuden aukkoja ovat myös esimerkiksi valvomoiden avoimet USB-portit. Portin kautta voidaan järjestelmään saada siirrettyä haittaohjelma, ja siksi tuntematonta USB-tikkua ei saa missään tilanteessa liittää automaatiojärjestelmään. Hyvä keino suojautua on estää USB-porttien käyttö joko ohjelmallisesti tai fyysisesti. [17, s.6.]

#### 4.3 Kyber-turva-vesi-hanke

Teknologian tutkimuskeskus VTT toteutti vuosina 2016–2018 kyber-turva-vesi-hankkeen, jonka rahoittivat Vesilaitosyhdistyksen kehittämisrahasto, Huoltovarmuuskeskus sekä hankkeeseen osallistuneet vesilaitokset. Hankkeessa luotiin ohjeita sekä kaksi arviointityökalua vesilaitoksille. Ohjeiden ja työkalujen avulla vesilaitokset voivat kehittää toimintaansa tietoturvaluottelu huomioiden. Ostopalveluiden tietoturva-vaatimusten arviointityökalun avulla voidaan arvioida nykyisten palveluiden tietoturvan tila sekä havainnoida, mitä eri vaatimuksia palveluilta on hyvä vaatia. Hankkeessa luotiin myös työkalu automaation tietoturvan arviointiin. Työkalun avulla vesilaitokset voivat arvioida automaatiojärjestelmänsä tietoturvaluottelu ja löytää siitä parannettavia kohteita. Hankkeessa luoduilla työkaluilla vesilaitokset saavat ymmärryksen, mitä vaatimuksia ostopalveluiden ja automaation kyberturvaluotteluun liittyy sekä mitä vesilaitosten tulee ottaa huomioon kehittäessään toimintaansa turvallisemmaksi. [17.] VTT:n luomat dokumentit ja työkalut ovat kaikkien vesilaitosten saatavilla, ja pyydetessä ne toimitetaan myös muille asiasta kiinnostuneille [18].

## 5 Yritysverkko

### 5.1 Yritysverkon toiminta

Yritysverkolla tarkoitetaan verkkoa, joka yhdistää yrityksen eri toimipisteet toisiinsa. Verkon tarjoaa verkko-operaattori, joka myös huolehtii yhteyksien toimivuudesta. Verkko-operaattori toimittaa liityntärajapinnan asiakkaan tarvitsemiin toimipisteisiin sekä tekee tarvittavat konfiguroinnit omaan verkkoonsa. Yritysverkolla voidaan siis yhdistää maantieteellisesti erillään olevat pisteet verkko-operaattorin tarjoamalla yhteydellä.

Verkon turvallisuuden vuoksi toimistosta, automaatiosta ja turvallisuudesta vastaavien laitteiden tulee olla omissa verkoissaan. Kokonaisuudet on myös hyvä eriyttää toisistaan fyysisesti erillisillä laitteilla. Toimistoverkkoon tulevia laitteita ovat muun muassa yrityksen työntekijöiden mobiili- ja tablet-laitteet. Automaatioverkossa ovat kaikki ne laitteet, jotka liittyvät jollain tavalla vedentuotantoon ja -jakeluun. Turvalaitteilla tarkoitetaan esimerkiksi kamera- ja kulunvalvontaan liittyviä toimintoja. Mikäli turvalaitteille ei hankita omia fyysisiä verkkolaitteita, kuten kytkimiä, on ne syytä laittaa toimiston verkkoon. Automaatioverkkoon tulee liittää vain ne laitteet, jotka ovat automaation kannalta olennaisia. Turvallisuuteen liittyvien laitteiden määrittäminen omaan verkkoon sekä fyysisiin laitteisiin helpottuu tulevaisuudessa, mikäli päätetään esimerkiksi hankkia kameravalvonta ulkoisena palveluna. Tällöin laitteet ovat jo valmiiksi erotettuna ja helposti jaettavana palveluntarjoajan käyttöön. [19.]

Verkko-operaattorin toimipisteisiin toimittaman liitännäraajapinnan lisäksi verkkoon tarvitaan reitittämiä, palomuureja sekä kytkimiä. Nämä edellä mainitut laitteet vaativat säännöllistä ylläpitoa verkon turvallisuuden ylläpitämiseksi. Ylläpidolla tarkoitetaan esimerkiksi laitteiden ohjelmistojen päivitysten ajantasaisuutta. Ylläpito on syytä hankkia palveluna, mikäli vesilaitoksella ei ole omaa ICT-osastoa huolehtimassa verkkolaitteiden ylläpidosta. Hankkiessa verkkolaitteiden ylläpitopalvelua tulee vastaan myös itse laitteiden hankkiminen palveluna. Kun hankitaan verkon aktiivilaitteet palveluna, tulee sopimuksessa huomioida tilanne, jossa verkon ylläpitopalvelu kilpailutetaan. Käytössä olevien laitteiden sisältämät konfiguroinnit tulee siis pystyä siirtämään uuden ylläpitäjän käyttöön, jolloin vältytään laitteiden peruskonfigurointien uudelleen tekemiseltä. Olivatpa verkkolaitteet omia tai vuokrattuja, tulee niiden ylläpidosta silti huolehtia. [19.]

## 5.2 Yritysverkon vaatimukset

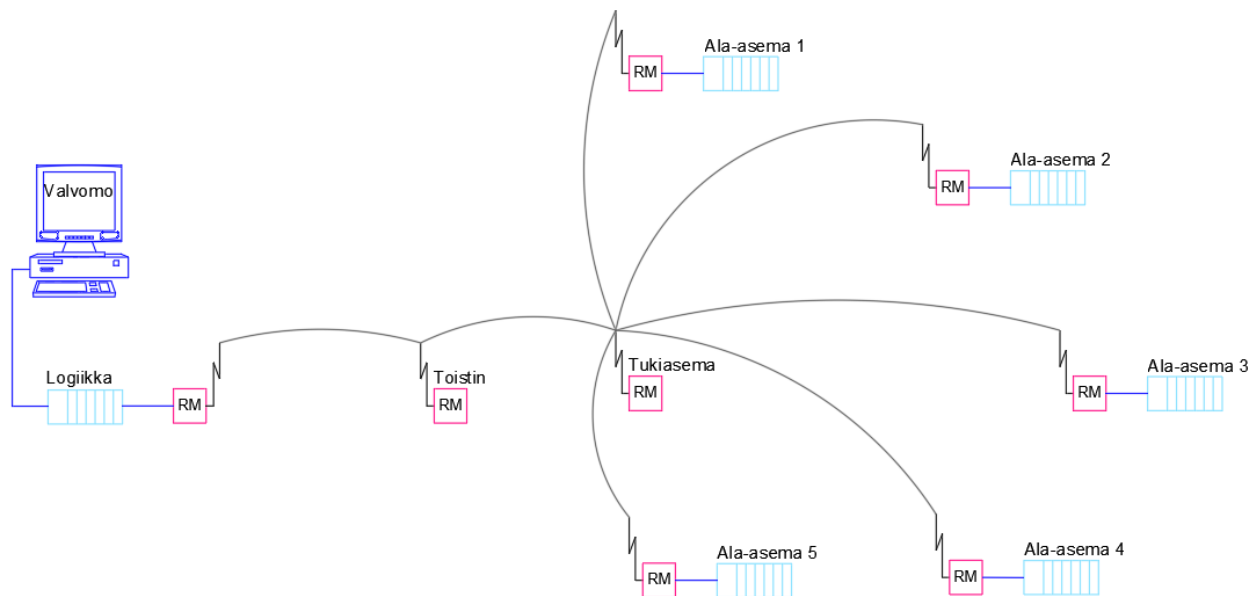
Kun ryhdytään hankkimaan tai kilpailuttamaan yritysverkkoa, tulee ensin selvittää nykyisen verkon laajuus sekä verkkoon liitettävät laitteet. Tarvittavista yhteyksistä tulee ilmetä myös, minkä tasoisia yhteydet ovat. Mikäli käytössä olevan järjestelmän dokumentaatio on hyvin hoidettu ja ajantasainen, ei tämä aiheuta juurikaan työtä. Yritysverkon hankinnassa asiakkaan tulee myös määrittää verkolle vaatimukset, joiden täytyessä verkkoon liitetyt laitteet toimivat suunnitellusti. Vaatimuksina on tyypillisesti verkon laajennettavuus, käytettävyys, turvallisuus ja hallittavuus. Tulevaisuuden tarpeita ei voida tietää, joten verkko on syytä suunnitella siten, että sitä voidaan aina tarvittaessa laajentaa. Verkon käytettävyyden taso riippuu siitä, kuinka kriittisiä toimintoja verkolla yhdistetään. Verkon toimittaja tekee tarvittavat toiminnot verkon käytettävyyden tason mahdollistamiseksi. Verkko tulee myös suunnitella ja toteuttaa niin, että voidaan suojautua verkkoon tai verkkoon liitettyihin laitteisiin kohdistuvia hyökkäyksiä vastaan. Verkon hallittavuudella tarkoitetaan verkon konfiguroinnin ja valvonnan toteutusta helpolla ja mahdollisella tavalla. Lisäksi on tärkeää velvoittaa verkon tarjoaja raportoimaan vaatimusten täyttymisestä säännöllisesti sekä mahdollisten poikkeamien johdosta. Yritysverkon tarjoaja on myös hyvä velvoittaa huolehtimaan verkon turvallisuudesta esimerkiksi IDS-järjestelmällä. Sovittaessa verkon vaatimuksista kirjataan tiedot palvelutasosopimukseen, joka on esitetty seuravaksi. [19.]

### Palvelutasosopimus

SLA (Service Level Agreement) eli palvelutasosopimus on asiakkaan ja palvelun tarjoajan välinen sopimus. Sopimuksessa määritetään tarkasti asiakkaalle tarjottavat palvelut sekä niiden tasot. Sopimuksessa tulee määritellä myös mittarit, joilla palvelun tasoa mitataan sekä sanktiot mikäli palvelu ei yllä sovitulle tasolle. Palveluntarjoajalta on myös hyvä vaatia säännöllistä raportointia toteutuneesta palvelusta. Sopimuksen ollessa määrittämiseltään selkeä, on sen noudattaminen huomattavasti tehokkaampaa. Palvelutasosopimuksen ajantasaisuudesta tulee huolehtia ja päivittää sitä muun järjestelmän mukana. [20; 21.]

## 6 Radiomodeemit ja langaton tiedonsiirto

Radiomodeemi on laite, joka toimii reitittimen tavoin lähettäen ja vastaanottaen saamansa datan radiotaajuuksien avulla. Radiomodeemi voi toimia lähettimenä, vastaanottimena, tukiasemana ja toistimena. Radioyhteyden tarvitaan aina lähetin ja vastaanotin. Edellä mainittujen komponenttien etäisyyden kasvaessa voidaan lähettimen lähettämää viestiä vahvistaa toistamalla se, jolloin yhteyden kantama pitenee. Radiomodeemin toimiessa tukiasemana pienennetään myös radiotaajuuksien aiheuttamaa peittoa luomalla yksi runkoyhteys tukiasemaan. Tukiaseman kattamalla alueella olevat radiomodeemit yhdistyvät automaatiojärjestelmään tukiaseman kautta. Kuvassa 6 on esitetty esimerkki radioverkon toteutuksesta. [22.]



Kuva 6. Radioverkko esimerkki.

Tieto saadaan siis siirrettyä radiotaajuuksien avulla ilman fyysistä yhteyttä esimerkiksi alueelta, johon ei kannata rakentaa kiinteää tiedonsiirto yhteyttä.

Tiedonsiirto radiotaajuuksilla

Langattomassa tiedonsiirrossa on mahdollista käyttää vapaita taajuuksia tai radioluvan vaativia taajuuksia. Vapaiden taajuuksien käytössä päällekkäisyys on mahdollista ja yhteydet saattavat estyä eri radiolaitteiden taajuuksien sotkiessa radiosignaalit.

Varmistaakseen oman radioverkon toiminnan on parempi käyttää luvanvaraisia taajuuksia. Radiolupaun ilmoitetaan muun muassa laitteiden käyttämät taajuusalueet, lähetysteho sekä antennien sijainnit. Traficomille ilmoitettujen tietojen perusteella myönnetään lupa kyseisellä alueella vapaana olevaan taajuuteen. Alueittain päällekkäisiä taajuuksia ei siis pääse syntyämään ja radioyhteydet toimivat oikein. Samaa taajuutta voidaan käyttää myös muualla sillä tavoin, etteivät radiotaajuudet häiritse toisiaan. [23, s. 12–13.]

Radioyhteyksien tietoturva saavutetaan tuntemalla omassa verkossa olevat laitteet, salaamalla radiomodeemien välinen tiedonsiirto sekä suojaamalla laitteet riittävällä fyysisellä suojauksella. Laitteet tulee konfiguroida siten, että vain tunnetut modeemit voivat olla yhteydessä toisiinsa radioverkossa olevien modeemien kanssa. Näin estetään tuntemattomien laitteiden liittyminen radioverkkoon. Liikenteen salauksella on samat tarkoitukset kuin tietokoneiden välisessä tiedonsiirrossa. Tarkoitus on estää tiedon salakuuntelu sekä varmistaa tiedon eheys ja muuttumattomuus. Radiomodeemeja käytetään usein alueilla, jotka ovat turvattomia ja valvomatta. Tästä syystä niiden fyysiseen turvallisuuteen tulee kiinnittää erityistä huomiota. Fyysinen suojaus voidaan toteuttaa sijoittamalla modeemi esimerkiksi lukittuun tilaan tai lukittavaan koteloon. Radiomodeemien sisältämät tiedot tulee olla suojattuna omalla salasanalla, jolloin käytössä olevia konfiguraatio tietoja ei voida saada selville ilman laitteen salasanaa. [23, s. 14.]

## 6.1 Satel

Satel on suomalainen radiomodeemeita valmistava ja myyvä yritys. Yritys on perustettu 1986 Salossa, jossa yrityksen toiminta jatkuu vielä tänäkin päivänä. Tuotannosta suurin osa menee vientiin ulkomaille yli sataan maahan. Satelin radioilla on mahdollista toteuttaa jopa 100 kilometrin yhteysväli, mutta silloin vaaditaan 35 watin lähetysteho. Yhteysvälin pituuteen vaikuttaa lähetystehon lisäksi antennin vahvistus, maston korkeus sekä ympäristö. [22.]

Satelilla on tarjolla useita tiedonsiirtoratkaisuja laitteille, jotka käyttävät sarjaliikennettä. Vesilaitoksille soveltuvia laitteita ovat muun muassa Satelline-tuoteperheen modeemit Easy ja 3AS, joita Kymen Vedellä ja Kymenlaakson Vedellä on käytössä. 3AS-mallin valmistus tullaan lopettamaan vuoden 2019 aikana. Korvaavana radiomodeemina tulevat toimimaan Easy+ -tuotteet. Haastaviin olosuhteisiin on tarjolla Easy-Proof -

radiomodeemi, jonka kotelointiluokka on IP69K, mikä tarkoittaa kuuman korkeapaineistetun vesisuihkun kestoä. Easy-Proof -radiomodeemi soveltuu tiiveytensä puolesta varsin hyvin esimerkiksi kaivoon sijoitettavaksi. Etä-I/O-ratkaisulle on myös vaihtoehto, jolloin ala-asemalle ei tarvitse sijoittaa omaa logiikkaa, vaan voidaan käyttää useamman ala-aseman ohjaukseen samaa logiikkaa. Vesilaitoksilla ala-asemien tulee pystyä ohjaamaan itsensä turvalliseen tilaan, vaikka yhteys valvomoon on katkennut. Silloin ala-aseman logiikalle ohjelmoidut toiminnot toteuttavat tarvittavat ohjaukset. Keskitettyä logiikkaa käytettäessä tulee varmistaa ala-aseman turvallinen toiminta myös yhteyden katketessa. Satelin LP-I/O toimii kenttäväylään kytketyn etä-IO:n tavoin mutta langattomasti. [22.]

Mikäli käytössä on laitteita, jotka käyttävät IP-tiedonsiirtoa, on vaihtoehtona käyttää XPRS -radioreitittimiä. XPRS -radioreititin tukee sarja- ja IP-tiedonsiirtoa, jolloin samalla radiomodeemilla voidaan muodostaa yhteys XPRS IP -radioreitittimien lisäksi myös Easy -radiomodeemeihin. XPRS IP -radioreitittimen toiminta perustuu älykkääseen IP-radioreititykseen. XPRS IP -radioreititin on varmennettu omalla varavirralla, jolloin tiedonsiirtoyhteys ei katkea edes sähkökatkon aikana. [24.]

Satel tarjoaa myös verkkosuunnittelua, johon vaaditaan vain asiakkaan määrittämät fyysiset sijaintipisteet modeemeille. Asiakas siis ilmoittaa Satelille olemassa olevien sijaintien tarkat koordinaatit ja mahdolliset olemassa olevat mastot, joita voidaan hyödyntää. Näiden tietojen pohjalta asiakkaalle pystytään määrittämään tarvittavat antennit sekä niiden korkeudet. Lisäksi verkkosuunnittelussa määritetään modeemien määrät, ja mikäli ilmenee tarve toistimille niin niiden sijainnit ja määrät. Satel avustaa asiakasta myös Traficomille lähetettävässä radiolupahakemuksessa. Satel täydentää lupahakemukseen käytettävien antennien ja modeemien tehot, säteilyalueet, suunnat, voimakkuudet sekä sijainnit. Nämä ovat pääasialliset tiedot, joita radiolupaan radioiden osalta tarvitaan. Satelilta tilatut modeemit myös toimitetaan valmiiksi konfiguroituina, jolloin niiden käyttöönotossa kytketään vain tarvittavat tiedonsiirtokaapelit, antenni sekä virtalähde. [22.]

Verkon konfigurointiin on olemassa sovellus, jonka graafisessa käyttöliittymässä luodaan haluttu verkko ja määritellään verkossa käytettävät radioluvan mukaiset taajuudet. Ohjelmaa voidaan käyttää niin uuden laitteen lisäyksessä kuin vanhan vikaantuessa. Ohjelmasta ladataan halutun modeemin konfigurointitiedosto ja asennetaan se uudelle modeemille. [22.]

## 6.2 Radiolinkit

Radiolinkillä tarkoitetaan kahden pisteen välille luotavaa tiedonsiirtoyhteyttä. Radiolinkeillä toteutetuilla yhteyksillä saavutetaan huomattavasti paremmat tiedonsiirtonopeudet kuin radiomodeemeilla. Siksi radiolinkit soveltuvat varmentamaan verkko-operaattorin tarjoamaa valokuituyhteyttä tai muodostamaan täysin oman runkoyhteyden. Radiolinkkejä on saatavilla luvanvaraisilla sekä luvasta vapailla taajuuksilla. Enkom Active Oy tuo maahan muun muassa Radwinin luvasta vapaita radiolinkkejä sekä Aviat Networksin luvanvaraisia radiolinkkejä. Radwinin luvasta vapailla radioilla voidaan saavuttaa jopa 750 Mbit/s tiedonsiirtonopeus. Aviatin luvanvaraisilla radioilla tiedonsiirtonopeudet voivat nousta jopa 2.5 Gbit/s. [23, s.15; 31.]

## 6.3 4G-yhteys

Tiedonsiirto valvomoiden, pääasemien ja ala-asemien välillä on toteutettavissa myös 4G-yhteydellä. Tiedonsiirtoyhteyksien toteuttaminen 4G:llä vaatii jokaiselle asemalle oman modeemin sekä SIM-kortin. Asemalla logiikka liitetään modeemiin, joka luo tiedonsiirtoyhteyden vesilaitoksen käyttämään yritysverkkoon. 4G-modeemilla toteutetun yhteyden tiedonsiirtonopeudet ovat huomattavasti nykyisiä radiomodeemiyhteyksiä paremmat. Yhteys on myös helppo hankkia, eikä siihen tarvita suuria alkuinvestointeja. Kuukausittaiset kustannukset ovat kuitenkin huomattavasti korkeammat kuin nykyisten radiomodeemiyhteyksien kuukausittaiset kustannukset. [3.]



## 7 Langattoman tiedonsiirron kehittäminen

### Satellite-verkon päivitys

Nykyisen radioverkon Easy-radiomodeemit tulee päivittää AES 128 (Advanced Encryption Standard) salausta tukevaksi. Salaus voidaan tehdä vain Easy-modeemeille, joten nykyiset 3AS-modeemit tulee päivittää Easy-malleihin. Modeemien päivityksellä saadaan nykyiset suojaamattomat radioyhteydet salattua estäen viestien salakuuntelun ja vääristelyn. Nykyisellä järjestelmällä on mahdollista, että tunkeutuja kuuntelee verkossa liikkuvia tietoja sekä vääristelee niitä esimerkiksi kaivon ja valvomon välillä. 3AS-modeemin korvaaminen uudella Easy-modeemilla kustantaa noin 1100 euron laitehankinnan sekä tarvittavat asennus- ja konfigurointitoista syntyvät kustannukset. Easy-modeemeihin tehtävä päivitys maksaa noin 200–400 euroa kappaleelta riippuen radioverkon laajuudesta. [3; 22; 25.]

### Satellar-verkon päivitys

Satellar-modeemeihin tulee myös päivittää salattu tiedonsiirtoyhteys. Nykyiset radiomodeemit tukevat AES-128-salausta, mikä tulee vähintään ottaa käyttöön. Laitteet voidaan myös päivittää Satelin XPRS IP -radioreitittimiin, jolloin teoreettiset tiedonsiirtomäärät nousevat nykyisestä noin 20 kbps:tä noin 120 kbps:ään. Uudessa XPRS IP -radiomodeemissa myös tietoturvaominaisuudet ovat paremmat. Radiomodeemin tietoturvasta huolehtii muun muassa AES-256-salaus, sisäinen palomuuuri sekä käyttäjän todennus. Liikenteen salaus on vahvempi kuin Easy-mallissa, mutta nykyisillä tietokoneilla molempien modeemien luoman salauksen purkamiseen kuluva aika on niin pitkä, ettei tieto ole enää hyödyllistä. Laitteen hinta on noin 2000 euroa kappaleelta, ja päivittäessä Satel ohjelmoi radioreitittimet verkkosuunnitelman mukaan valmiiksi, joten käyttöönotossa ei ohjelmointikustannuksia muodostu. Nykyiset Satellar-radiomodeemit voidaan myös päivittää Easy-radiomodeemeiksi, jolloin kaikki käytössä olevat modeemit ovat samasta tuotepiheestä. Modeemien päivitys kustantaa noin 13 000 euroa. [26.]

### Siirtolinjan yhteydet

Nykyisellä siirtolinjalla olevien verkko-operaattorilta hankittujen tiedonsiirtoyhteyksien korvaaminen XPRS IP -radioreitittimillä vähentää kuukausittaisia kuluja huomattavasti.

Nykyiset siirtolinjan ala-asemien yhteydet aiheuttavat kuukausittaisia kuluja, kun taas radioverkon käytöstä aiheutuu alkuinvestoinnin jälkeen vuosittain noin 20 euron radiolupamaksu jokaista laitetta kohden. Siirtolinjan tiedonsiirto toteutettaisiin ketjuna, jolloin jokaisella asemalla olisi kaksi erillistä yhteyttä automaatiojärjestelmään. Näin ollen yhden aseman yhteyden katketessa ketjun muiden asemien yhteydet vielä toimivat. [27; 28.]

Siirtolinjan tiedonsiirtoyhteyksien korvaaminen radioreitittimillä vaatii jokaiselle asemalle noin 15 metriä korkean maston. Mastojen rakentamisen lisäksi alkuinvestointeja syntyy laitehankinnan osalta noin 28 000 euroa, mihin sisältyy tarvittavat antennit sekä radioreitittimet. Lukuun ottamatta mastojen hankinnasta koituvia kustannuksia, maksavat radioreitittimet alkuinvestointinsa takaisin muutamassa vuodessa. [29.]

### Varayhteys

Nykyisen verkko-operaattorin tarjoama varayhteys valvomoiden välille voidaan korvata omalla radioverkolla. Radioreitittimillä luotu varayhteys on täysin muista tiedonsiirroista riippumaton tiedonsiirtoyhteys. Yhteys toteutettaisiin XPRS IP -radioreitittimillä Kuivalasta vesitornien kautta Tavastilan vesisäiliölle, mistä yhteys jatkuisi Kotkan valvomoon. Suunnitelluilla mastoilla tiedonsiirtonopeus rajoittuisi noin 60 kilobittiin sekunnissa. Antennivälejä pienentämällä ja mastoja korottamalla voidaan tiedonsiirtonopeus saada nostettua radioreitittimen maksimiin, joka on 121 kilobittiä sekunnissa. Varayhteyden luomiseen tarvittavat laitteet, kuten radioreitittimet ja antennit, kustantavat noin 14 000 euroa. Lisäksi kustannuksia syntyy tarvittavien mastojen rakentamisesta. [27; 28; 30.]

Radioreitittimillä toteutettavan varayhteyden tiedonsiirtonopeus jää liian pieneksi, joten varayhteys kannattaa toteuttaa lisenssitajuisilla radiolinkeillä. Aviatin 13 GHz:n radiolinkeillä voidaan toteuttaa varayhteys Kuivalan ja Kotkan välille siten, että jännevälejä on kolme. Yksi toistinasema sijoitetaan noin puolessa välissä sijaitsevan vesitornin päälle, jolloin erillistä mastoa ei tarvitse rakentaa. Vesitornin päälle riittää kevyempi masto, joka mahdollistaisi antennin riittävän korkeuden. Varayhteyttä suunniteltaessa tulee myös huomioida Kuivalan tekopohjavesilaitoksen läheisyydessä sijaitsevan Utin lentokentän aiheuttamat rajoitteet rakennettavan maston korkeudelle ja sijainnille. Radiolinkeillä toteutettavaan varayhteyteen tarvittavien laitteiden, kuten radioiden ja antennien kustannukset olisivat hieman radiomodeemeilla toteutettavaa yhteyttä pienemmät. Tosin radiolinkit tarvitsevat korkeammat mastot kuin radiomodeemit, minkä johdosta

kokonaiskustannukset nousevat radiomodeemiyhteyttä korkeammiksi. Vaikka kokonaiskustannus on korkeampi, saavutetaan radiolinkeillä huomattavasti parempi tiedonsiirtonopeus. Enkom Active arvioi tiedonsiirtonopeudeksi vähintään 100 Mbit/s, mikä riittäisi jo hyvin valvomoiden väliseen tiedonsiirtoon. [31.]

## 8 Yritysverkon ja palvelimien hankinta

Kymen Veden ja Kymenlaakson Veden kilpailuttaessa nykyistä yritysverkkoa tulevat verkkoon liitettävät laitteet olemaan hyvin pitkälti samoja kuin nykyisetkin. Yritysverkko-sopimukseen tulee sisällyttää vähintään toimisto- ja automaatioverkot sekä toimipisteisiin sijoitettavat verkon reitittimet. Uuteen sopimukseen määritetään molemmille verkoille omat fyysiset aktiivilaitteet, jotka tulee sijoittaa erillisiin laitekaappeihin. Verkkoysteik-sien lisäksi sopimukseen lisätään tarvittavia palveluita verkon turvallisuuden mahdollis-tamiseksi. Nykyisen sopimuksen sisältämiä palveluita, kuten etäyhteys- ja palomuuripal-velu, tulee tarkentaa vastaamaan uusia vaatimuksia. Lisäksi on hyvä hankkia myös IDS-järjestelmä havaitsemaan verkossa tapahtuvia poikkeamia. Yritysverkon sopimuskau-den tulee suosia säännöllistä verkko-operaattorin kilpailutusta, millä mahdollistetaan ver-kon pysyminen kehityksen mukana sekä viimeisimmän teknologian hyödyntäminen. [3; 4.]

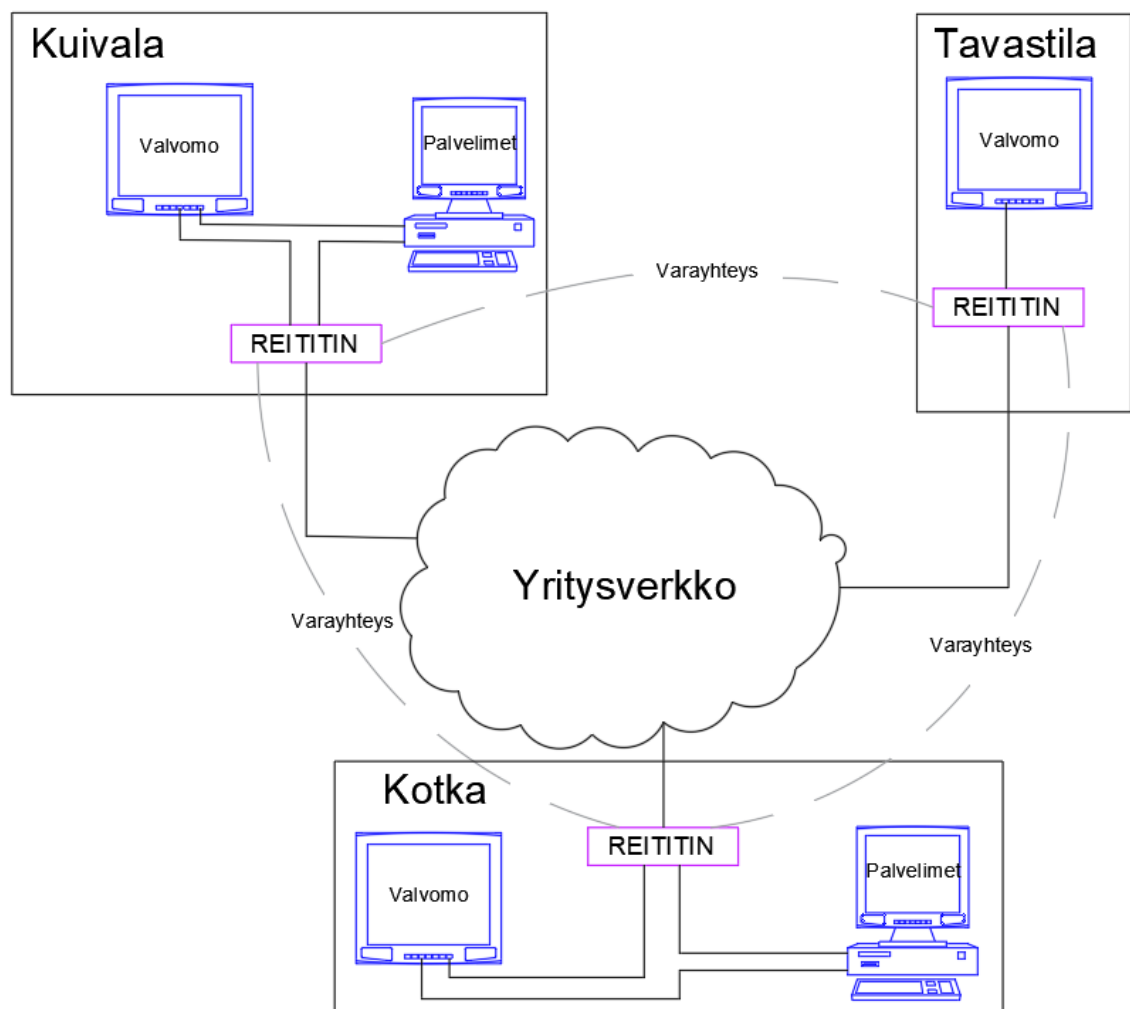
Verkkoa hankittaessa on myös hyvä varautua käytettävien verkon aktiivilaitteiden ylläpi-toon. Jos omalla henkilökunnalla ei ole mahdollisuutta huolehtia ylläpidosta, tulee ylläpito hankkia palveluna. Tällöin on usein kokonaisuuden kannalta edullisinta hankkia laittei-den ylläpito verkontarjoajalta. Laitteiden ylläpitopalvelu on hyvä hankkia myös automaa-tiojärjestelmässä oleville aktiivilaitteille. Verkko-operaattorin tulee tällöin tehdä yhteis-työtä automaatiojärjestelmän toimittajan kanssa, jotta automaation häiriötön toiminta mahdollistetaan. Mikäli päädytään ulkoistamaan myös verkon fyysiset aktiivilaitteet, ku-ten kytkimet, tulee sopimuksessa määrittää verkon konfigurointitiedot asiakkaan omista-miksi. [3; 4.]

### 8.1 Valvomopalvelimet

Nyt, kun on tarkoitus uusia yritysverkon sopimusta, on samalla myös hyvä selvittää vaih-toehtoja, miten nykyiset valvomoiden fyysiset palvelimet tullaan tulevaisuudessa uusi-maan. Fyysisten laitteiden elinikä rajautuu laitevalmistajan myöntämään takuuseen, joka on usein kolmesta viiteen vuotta. Takuuajan jälkeen vastuu laitteiden toimivuudesta siir-tyy asiakkaalle eli vesilaitokselle. Tämän takia on hyvä selvittää kustannukset vuokra-tuille palvelimille. Vuokratuissa laitteissa palveluntarjoaja on veloitettu huolehtimaan laitteiden toimivuudesta. Nykyistä Kymen Veden vedenjakeluverkoston valvontaan

käytettävää virtuaalista valvomoa voidaankin pitää yhtenä vaihtoehtona. Erona nykyiseen on kuitenkin fyysisten laitteiden sijoittaminen vesilaitoksen kriittisille alueille, kuten Kuivalan tekopohjavesilaitokselle. Tekopohjavesilaitoksen tulee pystyä toimimaan myös ulkoisten yhteyksien puuttuessa. Nykyiset palvelimet on toimittanut automaatiourakoitsija, jonka tehtäväksi on myös määritetty ohjelmistojen ajantasaisuudesta huolehtiminen. Valvomopalvelimien päivityksessä tulee myös huomioida se, miten ulkoistettujen palvelimien päivitykset toteutetaan häiritsemättä itse tuotantoa. [3; 4.]

Nykyiset Kymenlaakson Veden omistamat palvelimet ovat noin viiden vuoden ikäisiä, minkä johdosta ne tulee päivittää. Valvomoiden palvelinlaitteita päivittäessä on suositeltavaa hyödyntää nykyisen virtuaalivalvomoratkaisun tapaista toteutusta. Kuvassa 7 on havainnollistettu valvomoiden toteutusvaihtoehtoa.



Kuva 7. Ehdotus uudesta valvomo ratkaisusta.

Kuivalaan ja Kotkaan sijoitetaan fyysiset palvelimet, jotka virtualisoidaan. Nykyiset valvomot, jotka ovat kopioita toisistaan, siirretään toimimaan virtuaalisilla palvelimilla. Tavastilan valvomo jää siis käyttämättä, minkä johdosta lisenssejä tarvitaan vähemmän. Uusia virtuaalisia valvomoita käytetään valvomopäätteiltä Kuivalasta, Tavastilasta tai Kotkasta.

Virtuaaliset palvelimet koostuvat useammasta fyysisestä laitteesta, millä mahdollistetaan riittävä vikasietoisuus. Tällä toteutuksella virtuaalisen palvelimen ja valvomopäätteen välinen yhteys on todella kriittinen, minkä johdosta yhteydet tulee varmentaa riittäväällä varayhteydellä.

## 8.2 Elinkaari

Automaatiojärjestelmien elinkaari arvioidaan yleisesti kymmeniksi vuosiksi, jolloin tulee huolehtia järjestelmän tietoturvallisuudesta koko elinkaaren ajan. Kun järjestelmää päivitetään, tulee ottaa huomioon kaikki järjestelmään kuuluvat osat ja niiden elinkaari. On otettava huomioon, miten nykyisen tiedonsiirtoyhteyden päivitys johonkin tasoon on käyttökelpoinen vielä, kun muuta järjestelmää myöhemmin päivitetään. On siis hyvä olla jokin suunnitelma, jonka mukaan järjestelmä päivitetään. Uusien ominaisuuksien tulee tukea vanhaa toteutusta antaen silti lisäarvoa järjestelmän toiminnalle. Päivitettäessä ei välttämättä kannata ottaa käyttöön viimeisintä mallia, jossa on kaikki hienot ominaisuudet, jos vanhat laitteet eivät niitä voi hyödyntää. Tosin tulee myös muistaa, että vanhemmat laitteet tulevat jossain vaiheessa elinkaarensa päähän, jolloin nekin päivitetään uusiin markkinoilla oleviin soveltuviin laitteisiin. Tällöin uusien laitteiden tulee olla soveltuvia aikaisemmin päivitettyjen yhteyksien kanssa tuoden ehkä jotain uutta ominaisuutta tai vain korvaamalla vanhat laitteet.

## 9 Yhteenveto

Insinööriyön tarkoitus oli selvittää Kymen Veden ja Kymenlaakson Veden automaatiojärjestelmän tiedonsiirtoyhteydet, joihin kuuluvat nykyinen yritysverkko, ala-asemien käyttämät radiomodeemit sekä Kymen Veden omistamat valokuituyhteydet. Lisäksi oli tarkoitus selvittää nykyisten valvomoiden elinkaari sekä ratkaisu, miten valvomoita tulevaisuudessa tullaan päivittämään. Työn yhtenä osana oli tarkoitus selvittää, miten tietoturva on nykyisessä järjestelmässä otettu huomioon sekä miten sitä voidaan kehittää.

Insinööriyötä aloitettaessa käsitykseni Suomen vesihuollosta oli suppea. Työn ansiosta sain hyvin kattavan näkemyksen Kymen Veden ja Kymenlaakson Veden toiminnasta vesilaitoksina sekä pääsin tutustumaan vedentuotantoprosessin eri vaiheisiin. Erityisesti yllätyin, miten paljon järjestelmien välistä tiedonsiirtoa toteutetaan vesilaitoksien omilla radioverkoilla. Radiomodeemien käyttö vaikuttaakin hyvin soveltavalta tiedonsiirtotavalta ala-asemille, missä tiedonsiirtonopeudet ovat alhaiset.

Työssä selvitettiin nykyisiä yhteyskäytäntöjä, joista kattavin katsaus koski radioverkkoa sekä sen päivittämistä. Lisäksi työssä annettiin perusteita yritysverkon hankinnalle. Työtä tehdessäni huomasin dokumentaation olevan hyvin olennaisessa roolissa esimerkiksi tietoturvan ylläpitämisessä. Tietoturvaa kehitettäessä tulee tunnistaa kaikki käytettävät yhteydet ja tekniikat, jotta niiden heikkouksia voidaan parantaa. Ennen kuin Kymen Vesi ja Kymenlaakson Vesi ryhtyy päivittämään nykyisiä tiedonsiirtojärjestelmiä, tulee heidän laatia tietoturvapoliittikka, josta saadaan suuntaviivat, miten yritysten tietoturva tullaan ottamaan huomioon. Poliittikan pohjalta voidaan myös luoda tarkennettuja ohjeita esimerkiksi automaatiojärjestelmän etäyhteyksille. Tietoturvallisuus tulee olemaan oma prosessi vesilaitoksien normaalin toiminnan ohella. Tietoturvallisuusprosessilla huolehditaan kokonaisuuden turvaaminen aina elinkaaren loppuun saakka.

## Lähteet

1. Vettä, luonnollisesti. 2007. Yrityksen sisäinen dokumentti. Kymenlaakson Vesi Oy.
2. Talousvesigraafi\_A1\_13.3.2019.pdf. 2019. Yrityksen sisäinen dokumentti. Kymenlaakson Vesi Oy.
3. Leppänen, Timo. 2019. Automaatioteknikko, Kymen Vesi Oy, Kuivala. Keskustelut 8.2.2019–29.3.2019.
4. Juha, Arvas. 2019. Automaatiosuunnittelija, Pöyry Finland Oy, Vantaa. Keskustelu 21.1.2019–12.4.2019.
5. Vedentuotannon automaatio ja tietoliikenne. 2019. Yrityksen sisäinen dokumentti. Kymen Vesi Oy.
6. Järjestelmäkaavio. 2017. Yrityksen sisäinen dokumentti. Kymenlaakson Vesi Oy.
7. Sateline Easy radiomodeemi. 2019. Verkkoaineisto. Satel Oy. <<https://www.satel.com/products/radio-modems/sateline-easy/>>. Luettu 15.2.2019
8. SATEL-TA12 User manual. 2019. Verkkoaineisto. Satel Oy. <<https://www.cleancss.com/user-manuals/MRB/SATEL-TA12>>. Luettu 15.2.2019
9. Valvomot. 2009. Yrityksen sisäinen dokumentti. Kymenlaakson Vesi Oy.
10. Virtuaalivalvomohanke. 2018. Yrityksen sisäinen dokumentti. Kymenlaakson Vesi Oy.
11. Nopanen, Teemu. 2019. Projekti-insinööri, Mipro Oy, Vantaa. Keskustelu 22.3.2019.
12. Eerola, Risto. 2012. Automaatiojärjestelmien tietoturvaan liittyviä erityishaasteita. Verkkoaineisto. TUTWiki. <https://wiki.tut.fi/Tietoturva/Tutkielmat/AutomaationTietoturva>>. 20.4.2012. Luettu: 1.4.2019.
13. Pentikäinen, Heimo & Raitio, Pia. VTT. 2018. Lyhyet kyberturvallisuusohjeet vesihuoltolaitoksille. Kyber-turva-vesi -hanke. Huoltovarmuusorganisaatio, Vesi-huoltopooli.
14. Karppinen, Jukka. 2019. Verkon tietoturvakontrollit. Luentomateriaali. Metropolia Ammattikorkeakoulu.



15. Sailio, Mirko. VTT. 2018. AI-tekniikat IDS-järjestelmien tukena vesilaitosten tietoturvan parantamisessa. Kyber-turva-vesi -hanke. Huoltovarmuusorganisaatio, Vesihuoltopooli.
16. Suomen Automaatioseura ry. Teollisuusautomaation tietoturva, Verkottumisen riskit ja niiden hallinta. 2010. 1. Verkkopainos.
17. Pentikäinen, Heimo. VTT. 2018. Vesihuoltolaitosten kyberfyysinen turvallisuus. Kyber-turva-vesi -hanke. Huoltovarmuusorganisaatio, Vesihuoltopooli.
18. Liikanen, Riina. 2019. Vesiasian päällikkö, Vesihuoltopoolin valmiuspäällikkö, Suomen Vesilaitosyhdistys ry, Vantaa. Puhelu 21.3.2019.
19. Kankkunen, Petri. 2019. ICT osastopäällikkö, Pöyry Oy, Vantaa. Keskustelu 28.2.2019.
20. Pervilä, Markku. 2017. Tämän vuoksi palvelutasosopimus on niin tärkeä – mitata lupausten toteutumisen. Verkkoaineisto. Tivi. <<https://www.tivi.fi/CIO/tamanvuoksi-palvelutasosopimus-on-niin-tarkea-mittaa-lupausten-toteutumisen-6671699>>. 25.8.2017. Luettu 20.3.2019.
21. Stephanie, Overby; Lynn Greiner & Lauren Gibbons Paul. 2017. What is an SLA? Best practices for service-level agreements. Verkkoaineisto. CIO. <<https://www.cio.com/article/2438284/outsourcing-sla-definitions-and-solutions.html>>. 5.7.2017. Luettu 23.3.2019.
22. Kotirinta, Samuli. 2019. Myyntipäällikkö, Satel Oy, Vantaa. Tuote-esittely 28.2.2019.
23. Kylänpää, Markku & Pentikäinen, Heimo. VTT. 2018. Vesihuoltolaitosten radio-, mobiili- ja IoT-laitteiden kyberturvallisuus. Kyber-turva-vesi -hanke. Huoltovarmuusorganisaatio, Vesihuoltopooli.
24. Satel XPRS radioreititin. 2019. Verkkoaineisto. Satel Oy. <<https://www.satel.com/xprs/#SATELLAR-XT-5RC>>. Luettu 15.2.2019
25. Satelline modeemien päivitys. 2019. Yrityksen sisäinen dokumentti. Kymen Vesi Oy.
26. Satellar modeemien päivitys. 2019. Yrityksen sisäinen dokumentti. Kymen Vesi Oy.
27. Kari, Seppo. 2019. Tekninen Tuki, Satel Oy, Vantaa. Puhelu 15.3.2019.
28. Kotirinta, Samuli. 2019. Myyntipäällikkö, Satel Oy, Vantaa. Puhelu 15.3.2019

29. Siirtolinjan päivitys. 2019. Yrityksen sisäinen dokumentti. Kymen Vesi Oy.
30. Varayhteys. 2019. Yrityksen sisäinen dokumentti. Kymen Vesi Oy.
31. Junninen, Seppo. 2019. Tuotealuepäällikkö, Enkom Active Oy, Vantaa. Puhelu 15.4.2019