

Ville Toivanen

RAKENNUSAUTOMAATION VALVOMOIDEN VIRTUALISOINTI

RAKENNUSAUTOMAATION VALVOMOIDEN VIRTUALISOINTI

Ville Toivanen
Opinnäytetyö
Kevät 2019
Sähkö- ja automaatiotekniikan
tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu

Sähkö- ja automaatiotekniikan tutkinto-ohjelma, Sähkövoimatekniikka

Tekijä: Ville Toivanen

Opinnäytetyön nimi suomeksi: Rakennusautomaation valvomoiden virtualisointi

Opinnäytetyön nimi englanniksi: Virtualization of Building Automation Control System

Työn ohjaajat: Heikki Kurki OAMK, Aleksi Holappa Caverion Suomi Oy

Työn valmistumislukukausi ja -vuosi: Kevät 2019

Sivumäärä: 39 + 3 liitettä

Opinnäytetyön tavoitteena oli valmistella ja toteuttaa Caverion Pyramid-automaatiojärjestelmän valvomoympäristö konesalissa. Etäyhteyksien muodostus valvomoon tuli olla asiakasystävällistä sekä turvallista. Työn tavoitteena oli myös kartoittaa uuden järjestelmän kustannuksia ja työstä tuli saada julkaisukelpoinen dokumentti mahdollisia asiakkaita varten. Opinnäytetyön tilaajana oli Caverion Suomi Oy:n Oulun toimipiste.

Opinnäytetyön teoriaosuudessa käsitellään automaatiojärjestelmien yleistä rakennetta, tiedonsiirtoprotokollia sekä tietoturvaan liittyviä asioita ja miten tietoturvaa voidaan parantaa automaatiojärjestelmissä. Opinnäytetyössä esitetään myös, miten valvomojärjestelmän käyttöönotto tapahtui. Opinnäytetyöhön kuului ohjelmistojen asentamista, tiedonsiirtoverkkojen suunnittelua sekä laitteiden asentamista asiakkaiden kiinteistöissä. Työhön sisältyi myös ulkopuolisten yritysten tekemiä ohjelmointitöitä konesalissa.

Työn lopputuloksena saatiin toimiva ja luotettava valvomoympäristö, johon voidaan ottaa etäyhteys tietokoneelta tai mobiililaitteesta ilman tarvetta asentaa ylimääräisiä ohjelmistoja. Järjestelmää testattiin koko kevään ajan ja sen todettiin olevan tehokas tapa toteuttaa rakennusautomaatioiden etävalvonta. Tulevaisuudessa etävalvomojärjestelmää voidaan tarjota asiakkaille Caverion automaatioratkaisujen ohella. Uusi valvomoratkaisu nimettiin Virtuaalivalvomoksi.

Virtuaalivalvomon käyttöönottoa käsittelevässä osiossa tuotettiin dokumentaatiota, joka luottamuksellisenä jää ainoastaan toimeksiantajan käyttöön. Kyseistä aineistoa ei julkaista tässä raportissa. Opinnäytetyön liitteet, lukuun ottamatta liitettä 1, ovat myös luottamuksellisia.

Asiasanat: automaatio, rakennusautomaatio, tiedonsiirtoprotokolla, virtuaalivalvomo, automaatiovalvomo, tietoturva

ABSTRACT

Oulu University of Applied Sciences
Electrical and Automation Engineering, Electrical Engineering

Author: Ville Toivanen

Title of thesis: Virtualization of Building Automation Control System

Supervisors: Heikki Kurki OAMK, Alekski Holappa Caverion Suomi Oy

Term and year when the thesis was submitted: Spring 2019

Pages: 39 + 3 appendices

The aim of this thesis was to prepare and implement a control system environment of the Caverion Pyramid automation system in data center. Remote access to the control room has to be as customer friendly and as secure as possible. The aim of the thesis was also to chart expenses of the system and create a publishable document about this system for potential customers. This thesis was commissioned by Caverion Suomi Oy, Oulu.

The theoretical part of the thesis contains information about the general structure of automation system, communication protocols and information security and how information security can be improved in automation systems. The work included installation of automation software, planning the transmission networks and equipment installation on the customer properties.

The result was functional and reliable web-based control system environment which can be accessed remotely from PC or mobile device without installing any extra software in them. The system was tested throughout the spring and it was found to be an efficient way to build a remote automation control system. New automation system can be provided to customers along with the Caverion automation solutions.

Keywords: Automation, Building Automation, Transfer Protocols, Virtualization, Automation Control System

ALKULAUSE

Tämän opinnäytetyön toimeksiantajana ja yhteistyökumppanina toimi Caverion Suomi Oy:n Oulun toimipiste. Työn ohjasivat Aleksi Holappa Caverion Suomi Oy:sta sekä Heikki Kurki Oulun Ammattikorkeakoulusta.

Opinnäytetyön tavoitteena oli valmistella ja käyttöönottaa Caverion Suomi Oy:n Oulun toimipisteen käyttöön automaation keskusvalvomo, jota ylläpidetään kone-salissa.

Haluan kiittää Caverion Suomi Oy:tä tästä toimeksiannosta. Kiitokset kuuluvat Aleksi Holapalle sekä Heikki Kurjelle, Oulun toimipisteen automaatoratkaisut-osaston työporukalle sekä Caverionin tuotekehityksen väelle. Lisäksi kiitokset kuuluvat myös vanhemmilleni ja ystävilleni kannustuksesta.

Oulussa, 18.5.2019

Ville Toivanen

SISÄLLYS

1 JOHDANTO	8
2 RAKENNUSAUTOMAATIOJÄRJESTELMÄT	10
2.1 Järjestelmien tavoitteet	10
2.2 Laitteiston kuvaus	10
2.2.1 Valvomotas	11
2.2.2 Alakeskustaso	12
2.2.3 Kenttälaitetaso	13
2.3 Tiedonsiirtoprotokollat	14
2.3.1 Langattomat kenttäväyläprotokollat	14
2.3.2 Langalliset kenttäväyläprotokollat	16
2.3.3 TCP/IP	17
2.4 Automaation tietoturva	23
2.4.1 Laitteiston ylläpito	23
2.4.2 Salasanat	24
2.4.3 Virtual Private Network	24
2.4.4 Tosibox	25
3 PYRAMID-AUTOMAATIOJÄRJESTELMÄ	28
3.1 Schneider Electric Citect SCADA	28
3.2 Citect Anywhere	30
3.3 Konesalit	30
3.4 Välityspalvelimet	31
3.5 Windows Server	32
4 VIRTUAALIVALVOMO	34
5 YHTEENVETO	35
Liite 1 Virtuaalivalvomo-esite	
Liite 2 Etäyhteyden muodostaminen Virtuaalivalvomoon (Luottamuksellinen)	
Liite 3 Pienkohteet Oulu vuokaavio (Luottamuksellinen)	

SANASTO

AD	Active Directory, toimialueen käyttäjätietokanta
ADDS	Active Directory Domain Services, Microsoft Server-käyttöjärjestelmän toimialuepalvelu
CWS	CompuTec Web Station, reititin/ohjelmoitava logiikka
Hardware	Tietokone-ohjelmistoa suorittava laitteisto
HMI	Human-Machine Interface, ihmisen ja laitteen välinen käyttöliittymä
LVI	Lämmitys-, vesijohto sekä ilmanvaihtotekniikka
MIO-52	Caverion Modbus I/O-kortti
OSI	Open Systems Interconnection, tiedonsiirtoprotokollien kerrosmalli
PLC	Programmable Logic Controller, ohjelmoitava logiikka
SCADA	Supervisory Control and Data Acquisition, prosessien ohjausjärjestelmäohjelmisto
Software	Tietokone-ohjelmisto
TCP/IP	Transmission Control Protocol/Internet Protocol, tietoliikenneprotokollien perhe
VAK	Valvonta-alakeskus
Virtuaalivalvomo	Oulun uuden valvomoympäristön nimi
VPN	Virtual Private Network, virtuaalinen erillisverkko
WAN	Wide Area Network, kiinteistön ulkopuolinen tiedonsiirtoverkko

1 JOHDANTO

Tietoteknisten laitteistojen sekä tiedonsiirtonopeuksien voimakas kehittyminen 2000-luvun aikana on tuonut internet-yhteydet yhä laajemmille alueille ja yhä useampaan laitteeseen. Kehittymisessä ei näy laantumisen merkkejä ja tulevaisuudessa esimerkiksi 5G-tekniikka tulee kasvattamaan tiedonsiirtonopeuksia ja laitteiden määrää internetissä entisestään. Kehityksen mukana myös rakennusautomaatiojärjestelmien ohjaus- ja valvomojärjestelmät ovat siirtyneet verkkopohjaisiin ratkaisuihin.

Opinnäytetyön toimeksiantajana toimi Caverion Suomi Oy. Caverion on suomalainen pörssiyritys, joka suunnittelee, toteuttaa, huoltaa ja ylläpitää teknisiä ratkaisuja kiinteistöille ja teollisuudelle. Caverion kattaa kaikki rakennuksen tekniset osa-alueet – yksittäisestä teknologiasta aina suurempiin kokonaisratkaisuihin. Caverion voi vastata teknisten ratkaisujen suunnittelusta ja asentamisesta sekä kiinteistön tai teollisuuslaitoksen huollosta ja kunnossapidosta. Caverion tarjoaa kiinteistötekniikan järjestelmiä ja tuotteita LVI:n, sähköistyksen, automaation, informaatio- ja viestintäteknologian sekä turvallisuuden osa-alueilla. (1.)

Caverion Pyramid-automaatiojärjestelmä on kiinteistöjen, teollisuuden ja vesihuollon automaatoratkaisu, jossa hyödynnetään SCADA-pohjaista ohjelmistoa. Nykyisin Pohjois-Suomen Pyramid-valvomot on toteutettu kiinteistöihin asennettuna kiinteässä valvontapäätelaitteessa tai valvonta on keskitetty Oulun toimipisteellä sijaitsevaan keskusvalvomoon, johon kiinteistönomistajat ja -huoltajat ovat ottaneet etäyhteyden.

Oulun toimipisteellä olevaan keskusvalvomoratkaisuun liittyy myös ongelmia. Keskusvalvomossa käytetyt laitteet ja käyttöjärjestelmät eivät ole ihanteellisia etäyhteyksien hallintaan ja valvomon ylläpitoon. Tämän lisäksi keskusvalvomo vaatii asianmukaisen tilan yrityksen toimitiloissa ja mahdollisten toimitilamuutosten yhteydessä tulisi keskusvalvomon siirto suunnitella hyvin tarkasti, ettei valvomoyhteyksiin tulisi pitkiä käyttökatoja.

Nykyisen Oulun toimipisteellä sijaitsevan keskusvalvomon tilalle haluttiin ratkaisu, jossa valvomo asennetaan konesalissa olevalle palvelimelle. Uudessa valvomoratkaisussa etäyhteyksien muodostamisen sekä järjestelmän käytön tuli olla asiakasystävällistä ja turvallista. Valvomon ylläpito tuli saada myös vaivattomaksi.

Opinnäytetyön tavoitteena oli suunnitella ja ottaa käyttöön Pyramid-automaatiojärjestelmä konesalin palvelimella. Työssä kartoitettiin myös uuden valvomoratkaisun kustannuksia. Palvelimelle asennettu Pyramid-automaatiojärjestelmä tuli saada käyttöön otettua niin, että uusien kohteiden valvonta voidaan ottaa käyttöön palvelimella sekä vanhan keskusvalvomon alla olevia kohteita voidaan alkaa siirtämään kyseisen järjestelmän alle.

Opinnäytetyössä käsitellään rakennusautomaatioon liittyvää laitteistoa, tiedonsiirtoprotokollia, rakennusautomaation tietoturvaa sekä uuden järjestelmän rakennetta ja käyttöä. Raportti ei sisällä yksityiskohtaisia tietoja valvomon käyttöönotosta tai automaatiojärjestelmien ohjelmoinnista.

2 RAKENNUSAUTOMAATIOJÄRJESTELMÄT

2.1 Järjestelmien tavoitteet

Rakennusautomaatiojärjestelmillä on rakennuksen elinkaarta ajatellen useita tärkeitä tavoitteita. Tärkeimmät niistä ovat rakennusten energiatehokkuuden lisääminen, sisäolosuhteiden ylläpitäminen optimaalisena sekä laitteistojen kunnan tarkkailu (2, s. 21).

Rakennusautomaatiojärjestelmillä tehdään eri säätö- ja ohjaustoimenpiteitä mittauksiin ja laitteiston tilatietoihin perustuen. Käyttäjä asettaa järjestelmälle tavoitteita, jotka pyritään eri toimenpiteillä täyttämään. Tällaisia tavoitteita voivat olla esimerkiksi sisäilmalämpötilan pitäminen asetusarvossa, valaistuksen ohjaaminen päälle ja pois tiettyyn vuorokauden aikaan tai keskeisten henkilöiden informointi vikatilanteen aikana. Automaatiojärjestelmällä voidaan kerätä mittausdataa sähkön- tai vedenkulutuksesta ja raportoida niistä käyttäjälle tietyllä ajanjaksolla. Rakennusautomaatiojärjestelmään tulee sisällyttää rakennusten haltijalle ja ylläpitäjälle selkeä ja helposti ymmärrettävä käyttöliittymä, josta järjestelmiä ja laitteita voidaan valvoa ja kontrolloida. (2, s. 21.)

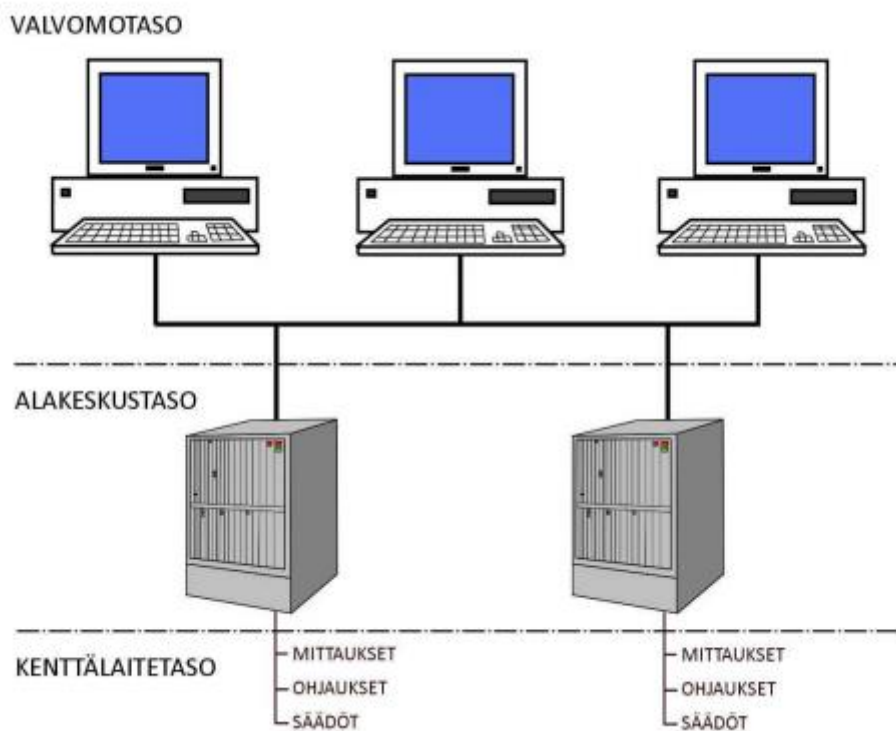
Nykyisin energiatehokkuus on hyvin tärkeä ominaisuus, kun laitteistoja hankitaan. Tulevaisuudessa energiankäyttöä halutaan hillitä entisestään ilmastonmuutoksen ja sen tuomien rajoitteiden vuoksi.

”Voidaan todeta, että investointikustannuksena rakennusautomaatiojärjestelmän osuus kokonaisuudesta on vähäinen, mutta sen merkitys rakennuksen elinkaaren aikaisiin kustannuksiin on ratkaiseva” (2, s. 21).

2.2 Laitteiston kuvaus

Rakennusautomaatiojärjestelmän laitteistot jaetaan yleisesti kolmeen päätasoon niiden sisältämien laitteiden tai toimintojen perusteella (kuva 1):

- valvomotaso
- alakeskustaso
- kenttälaitetaso

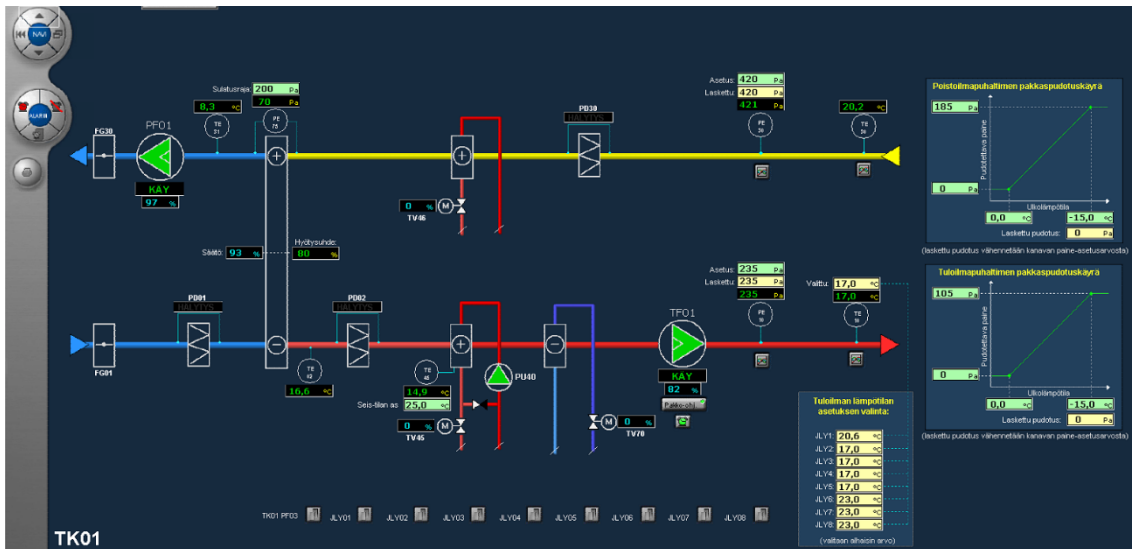


KUVA 1. Rakennusautomaationjärjestelmän hierarkia (3, s. 5)

2.2.1 Valvomotasoo

Valvomotasoo sisältää laitteiston, jolla luodaan käyttöliittymä ihmisen ja laitteiston välille (kuva 2). Tällaisesta käyttöliittymästä käytetään nimitystä HMI (Human-Machine Interface) (4, s. 12). Valvomotasoo sisältää tietokoneen käyttöjärjestelmän ja valvomo-ohjelmiston (Software) sekä ohjelmistoa suorittavan tietokone-laitteiston (Hardware) sekä palomuurin.

Valvomoympäristössä voidaan valvoa automaatiojärjestelmän toimintaa sekä tehdä tarvittavia muutoksia järjestelmään. Valvomotasoo on automaatiojärjestelmän näkyvin osa, joten käyttöliittymien suunnittelussa tulisikin panostaa käyttäjäystävällisyyteen sekä selkeään esitystapaan. Tätä varten käyttöliittymien suunnitteluun on olemassa ohjeistuksia ja hyväksi todettuja käytäntöjä.



KUVA 2. Valvomonäkymä Caverion Pyramid-automaatiojärjestelmässä.

2.2.2 Alakeskustaso

Alakeskustaso sisältää automaatiojärjestelmän ohjelmoitavan logiikan, PLC:n (Programmable Logic Controller), I/O-moduulit sekä virransyötön automaatiojärjestelmälle (kuva 3) (2, s. 60). Alakeskustasolla suoritetaan varsinaiset mittaus-, säätö- ja ohjaustoimenpiteet. Alakeskuksesta käytetään usein myös nimitystä VAK (valvonta-alakeskus).



KUVA 3. Alakeskuslaitteisto, Caverion CWS ja MIO-52

2.2.3 Kenttälaitetaso

Kenttälaitetasolle kuuluvat kaikki toimi- ja mittalaitteet, kuten anturit, venttiilimootorit, pumput ja puhaltimet. Mittalaitteet (kuva 4) välittävät reaaliaikaista tietoa prosessin tilasta automaation ohjausjärjestelmälle. Mittalaitteiden tietoja verrataan käyttäjän asettamiin tavoitteisiin ja automaatio-ohjausjärjestelmä säätää toimilaitteita siten, että järjestelmän tavoitteet voidaan saavuttaa (2, s. 61).



KUVA 4. Kenttätason mittalaitteita

2.3 Tiedonsiirtoprotokollat

Tiedonsiirtoprotokollat ovat oleellinen osa automaatiolaitteistoa. Eri tiedonsiirtoprotokollilla mahdollistetaan laitteistojen kommunikointi keskenään. Automaatiojärjestelmissä kommunikointiin automaatiotason ja kenttätason välillä on perinteisesti käytetty langallisia kenttäväyliä, mutta nykyisin myös langattomat tiedonsiirtoprotokollat ovat yleistyneet automaatiojärjestelmissä.

Automaatiojärjestelmissä käytettävät eri protokollat ovat useasti yhteensopivia toistensa kanssa. Kiinteistössä voidaan käyttää yhtä aikaa langallisia ja langattomia tiedonsiirtoprotokollia ja tiedonsiirto automaatiolaitteiden ja valvomotason välillä tapahtuu TCP/IP:n kautta.

2.3.1 Langattomat kenttäväyläprotokollat

Langattomien tiedonsiirtoprotokollien käyttö on yleistynyt rakennusautomaatiojärjestelmissä viime vuosina. Tekniikan kehittyminen on parantanut yhteyksien kantavuuksia sekä laitteiden käyttöaikaa. Langattomat tiedonsiirtoprotokollat eivät vaadi kaapelointia laitteiden välillä, joten niiden suotuisia käyttöympäristöjä ovat saneerauskohteet, joissa kaapelointi voi osoittautua haasteelliseksi. Myös suurissa kiinteistöissä, joissa välimatkat laitteiden välillä ovat pitkiä ja kaapelointi rakennuksessa ei ole kannattavaa, voidaan hyödyntää langattomia tiedonsiirtoprotokollia. Langattomien tiedonsiirtotapojen käytöllä voidaan välttää pitkät ja haasteelliset kaapeloinnit, mutta langattomien yhteyksien melko lyhyt kantavuus

voi johtaa siihen, että suuressa rakennuksessa joudutaan käyttämään vahvistimia tai toistimia, jos laitteiden etäisyydet ovat pitkiä tai niiden välissä on fyysisiä esteitä. Tämä voi aiheuttaa kustannuksien kasvamista ja johtaa tilanteeseen, jossa täytyy miettiä, onko langallisen tiedonsiirtotavan käyttö kannattavaa. (5, s. 4.)

Vaikka langattomat tiedonsiirtoprotokollat ovatkin yleistyneet ja niiden käytettävyys on parantunut, kriittisissä kohteissa niiden käyttö on kuitenkin vähäistä. Kohteissa, joissa tiedonsiirron luotettavuus ja suorituskyky ovat tärkeitä, suositetaan edelleen langallisia tiedonsiirtotapoja.

Rakennusautomaation käyttöön on kehitetty muutamia langattomia tiedonsiirtoprotokollia:

ZigBee on 2002 kehitetty langaton tiedonsiirtoprotokolla, jonka on kehittänyt ZigBee-allianssi ja se perustuu IEEE 802.15.4 -standardiin. ZigBee hyödyntää MESH-verkkorakennetta, jossa tiedonsiirtolaitteet pystyvät keskustelemaan minkä tahansa verkon sisällä olevan laitteen kanssa. Jos jokin laite rikkoontuu tai putoaa verkosta, laite etsii uuden tiedonsiirtoreitin verkon sisältä. ZigBee toimii 2,4 GHz:n taajuudella ja tiedonsiirron kantavuus on jopa yli 100 metriä laitteiden välillä. ZigBee-laitteet vaativat ulkoisen virransyötön toimintaa varten. ZigBeen kaupallinen käyttö vaatii lisensoinnin. (5, s. 18.)

EnOcean on Siemens AG:n vuonna 2008 kehittämä langaton tiedonsiirtoprotokolla ja sitä käytetään yleisesti valaistuksen ohjauksessa, huoneantureissa ja kulunvalvonnassa. EnOceanin lähettimen teho ja taajuus on pienempi kuin ZigBeessä, mutta laitteissa ei tarvita ulkoisia virtalähteitä, vaan laitteissa voidaan hyödyntää esimerkiksi aurinkoenergiaa. Kantavuus laitteiden välillä on noin 30 metriä. EnOceanissa ei hyödynnetä MESH-verkkorakennetta, joten yhden laitteen putoaminen verkosta voi aiheuttaa usean muun laitteen yhtäaikaisen toimintahäiriön. (5, s. 19.)

Suomalainen Proximal on myös kehittänyt oman langattoman tiedonsiirtolaitteiston, Proximal Proximan, jossa hyödynnetään ZigBeen tapaan MESH-verkkora-

kennetta, jossa laite pystyy kommunikoimaan minkä tahansa verkon sisällä olevan laitteen kanssa. Proximassa on käytössä Lumenradion kehittämä MiraOS-tiedonsiirtoratkaisu, jossa on yhdistelty eri langattomia tiedonsiirtomenetelmiä. Laitteet ovat täysin paristoilla toimivia, joten ulkoisia virtalähteitä laitteistossa ei vaadita. Proxima-laitteiston pariston kesto voi parhaimmillaan olla jopa 6–8 vuotta, riippuen mittauksista ja laitteiden optioista. (6.)

Proxima-laitteistoa hyödynnetään rakennusautomaatiossa huoneolosuhteiden mittaukseen. Proxima-laitteistoon kuuluu tukiasema (kuva 5) ja langattomat anturit. Proximassa on tuki Modbus RTU- ja Modbus TCP -protokollille (7).



KUVA 5. Proximal WBU-tukiasema langattomaan Proxima-verkkoon (7)

2.3.2 Langalliset kenttäväyläprotokollat

LON (Local Operating Network) on vuonna 1988 Echelonin kehittämä sarjaliikenneprotokolla, jolla pyrittiin luomaan yhteinen väyläratkaisu rakennusautomaatiolaitteille. LON-protokollaa käytetään miljoonissa laitteissa ympäri maailmaa. LON:ia pidettiin aikoinaan jopa tulevaisuuden ainoana väyläratkaisuna, mutta rakennuttajat huomasivat pian, että LON-protokollaan liittyi perustavanlaatuisia ongelmia, kuten kalliit lisenssimaksut ja heikko yhteensopivuus muiden protokollien kanssa. (8, s. 26.)

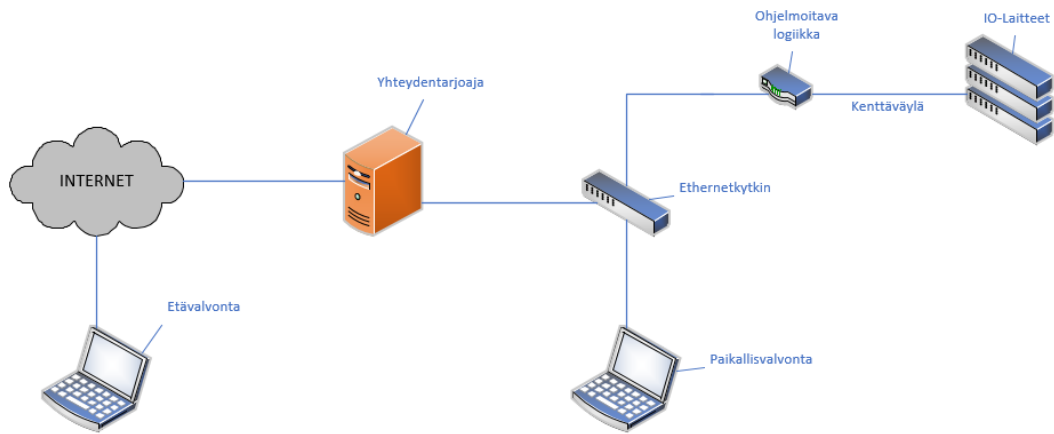
Modbus on Modiconin vuonna 1979 kehittämä sarjaliikenneprotokolla. Modbusia pidetään yleisesti väylätekniikan ”De facto” standardina. Modbus-protokollaa alettiin hyödyntää yleisesti teollisuuden automaatioissa sekä myöhemmin myös rakennusautomaation laitteistoissa. Euroopan ja Pohjois-Amerikan teollisuudessa arvioidaan olevan yli 7 miljoonaa Modbus-protokollaa hyödyntävää laitetta. (9.) Modbus on väyläratkaisuna kevyempi kuin LON johtuen väyläliikenteen vähemmästä salauksesta. Modbus-protokolla on myös lisenssimaksuton. (8, s. 26.)

BACnet on verkkoprotokolla, joka on kehitetty aikoinaan juuri rakennusautomaation tarpeita varten. Se kehitettiin vuonna 1987 Cornellin yliopistossa, Yhdysvalloissa. BACnet Testing Laboratories (BTL) testaa ja sertifioi BACnet-laitteet, jotta tuotteet olisivat yhteensopivia muiden BACnet-tuotteiden kanssa. (5, s. 7). BACnet on lisenssimaksuton ja sen lisäksi sen sarjaliikenne on paremmin salattu kuin LON:ssa tai Modbusissa (8, s. 27).

Langallisia väyläprotokollia on kehitetty näiden lisäksi useampia, kuten KNX, Dali sekä M-Bus. KNX on käytössä pääasiassa kotiautomaatioissa, Dali on valaistuksen ohjausjärjestelmiin suunniteltu tiedonsiirto-protokolla sekä M-Bus on käytössä veden- ja energiankulutusmittareissa. Usein näitä väyläprotokollia voidaan yhdensovittaa esimerkiksi Modbusin tai BACnetin kanssa. (5, s. 7–13.)

2.3.3 TCP/IP

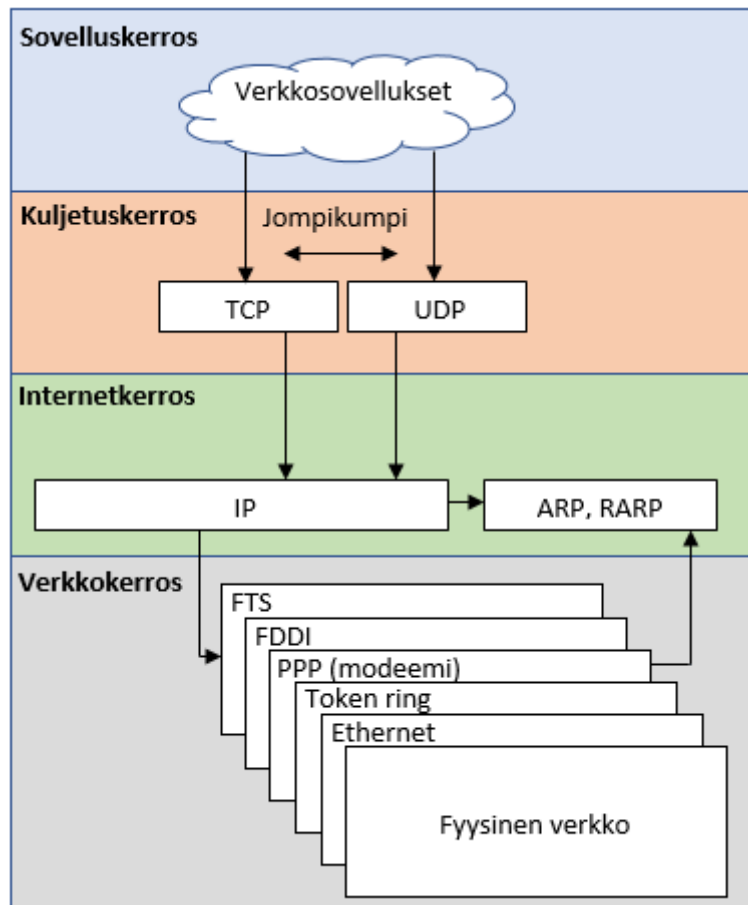
Automaatiotason ja valvomotason välinen kommunikointi perustuu tyypillisesti LAN-verkkoihin sekä TCP/IP-protokollaan (kuva 6). Tyypillinen rakennuksen paikallisverkko perustuu Ethernet-tekniikkaan, jossa kaapelointi on tehty kategorian 5 tai 6 kaapeloinnilla. (2, s. 60.)



KUVA 6. Yksinkertaistettu verkon rakenne rakennusautomaatiojärjestelmässä

TCP/IP-tiedonsiirtoprotokollien kehittäminen alkoi 1970-luvulla Yhdysvaltojen puolustusministeriön hankkeena. Nykyinen TCP/IP juontuu kahdesta suuresta kehityslinjasta, internetistä sekä paikallisverkoista. TCP/IP-protokollat määrittelevät verkossa tapahtuvaa liikennettä ja sen, miltä tietopakettien tulee näyttää sekä mitä tietoa niiden tulee sisältää. TCP/IP-protokollaperheen rakenne on esitetty kuvassa 7. (10, s. 10, 12.)

TCP/IP-protokollien toiminnan kohtuullinen ymmärtäminen on automaatiojärjestelmien tiedonsiirron kannalta tärkeää. Perustietotaidot helpottavat verkkojen rakentamista sekä mahdollisten vikatilanteiden sattuessa vian paikallistaminen helpottuu.



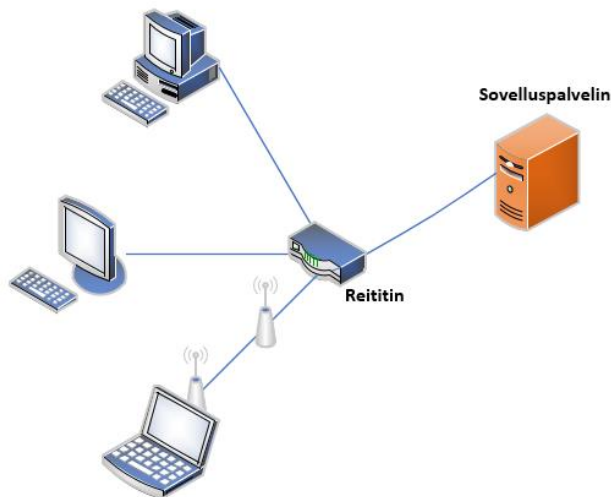
KUVA 7. TCP/IP-verkon rakenne ja protokollamalli (10, s. 29)

TCP/IP:n toimintaan liittyvä oleellisesti seuraavat käsitteet:

- looginen osoitteisto
- reititys
- nimipalvelu
- virheiden havaitseminen ja tiedonsiirron valvonta
- sovellustuki.

Jokaiselle verkkolaitteelle on annettu tehtaalla ainutkertainen ja pysyvä fyysinen osoite. Paikallisverkkoon kuuluvat laitteet lähettävät tietoa toisilleen ja laitteisto kuuntelee, mitkä viestit on tarkoitettu vastaanotettavaksi. Suuressa verkossa tämä ei ole mahdollista. Laitte ei voi esimerkiksi kuunnella koko internetin sisällä liikkuvaa tietomäärää, joten verkot pitää jakaa pienempiin ryhmiin. TCP/IP:ssä verkot jaetaan aliverkkoihin (subnet), jotka määritellään loogisten osoitteiden avulla. Näitä loogisia osoitteita kutsutaan IP-osoitteiksi. (10, s. 12.)

Reititys tarkoittaa tiedon siirtämistä määränpään loogisten osoitteiden avulla. Reititys toteutetaan reitittimillä (router). Internet koostuu valtavista määristä reitittimiä, joissa tieto voidaan siirtää useita vaihtoehtoisia reittejä pitkin. Reitityksen periaate on esitetty kuvassa 11. (10, s. 13.)



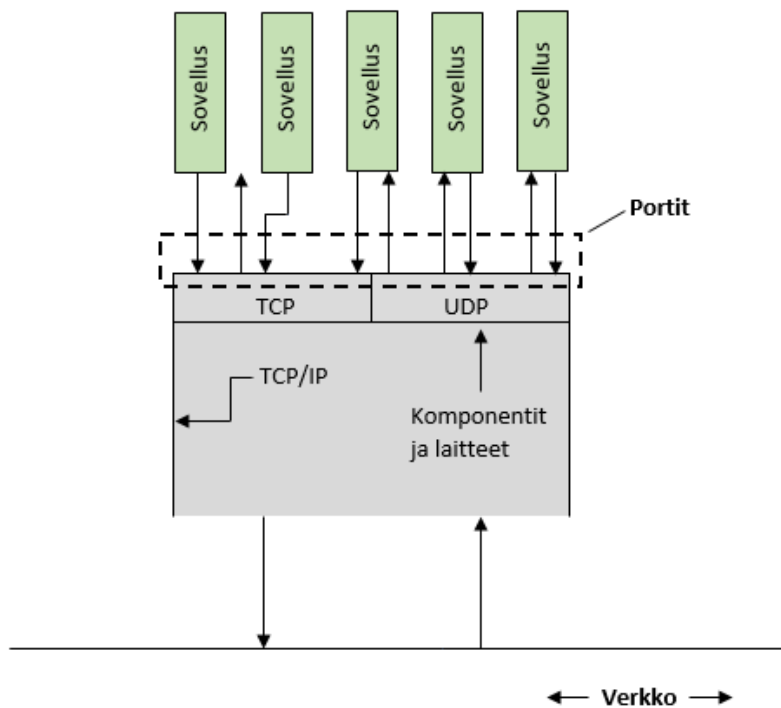
KUVA 8. Havainnekuva reitityksestä (11)

Koska ihmisten on hankala muistaa eri internetissä olevia IP-osoitteita, on TCP/IP:ssä vaihtoehtoinen tapa ilmoittaa osoitteet. Puhutaan toimialueen nimi-palvelusta (Domain Name Service, DNS). Verkon IP-osoite muutetaan tällöin ihmisystävällisempään muotoon. Sähköpostin ja WWW:n (World Wide Web) yhteydessä käytetään DNS-nimityksiä, esimerkiksi www.caverion.fi. (10, s. 14.)

Virheiden havaitsemisella ja tiedonsiirron valvonnalla tarkoitetaan sitä, että TCP/IP-protokolla sisältää useita ominaisuuksia, joilla valvotaan tiedonsiirron toimivuutta sekä havaitaan virheet tiedonsiirrossa. Tiedonsiirrossa oleellisinta on se, että lähtevä tieto säilyy samassa muodossa perille asti. Luotettavan tiedonsiirron takaamiseksi on lähettävän ja vastaanottavan tietokoneen osattava havaita ja korjata virheelliset sanomat ja valvottava tietovuota. (10, s. 15, 22.)

Sovellustuki tarkoittaa protokollaperheen rajapintaa, jossa sovellukset voivat kutsua protokollaohjelmiston palveluja ja siten olla yhteydessä verkkoon. Tämä ky-

seinen rajapinta sijaitsee TCP/IP:ssä paikallisessa tietokoneessa ja se toteutetaan loogisten kanavien, porttien avulla. Esimerkiksi automaatiovalvomo-sovellukset kommunikoivat verkon kanssa tiettyjen porttien kautta. Kyseiset rajapinnat ovat TCP (Transmission Control Protocol) sekä UDP (User Datagram Protocol). TCP on yhteydellinen protokolla, jolla on paremmat vuonohjaus- sekä virheenkorjaustoimenpiteet kuin UDP:llä. UDP on yhteydetön protokolla, joka on TCP:tä nopeampi, muttei yhtä luotettava. UDP jättää virheentarkistuksen kokonaan sovellusohjelman vastuulle. TCP- ja UDP-porttien toiminta sovellustasolla on esitetty kuvassa 9. (10, s. 15, 28.)



KUVA 9. Sovellukset ja verkon käyttö (10, s. 15)

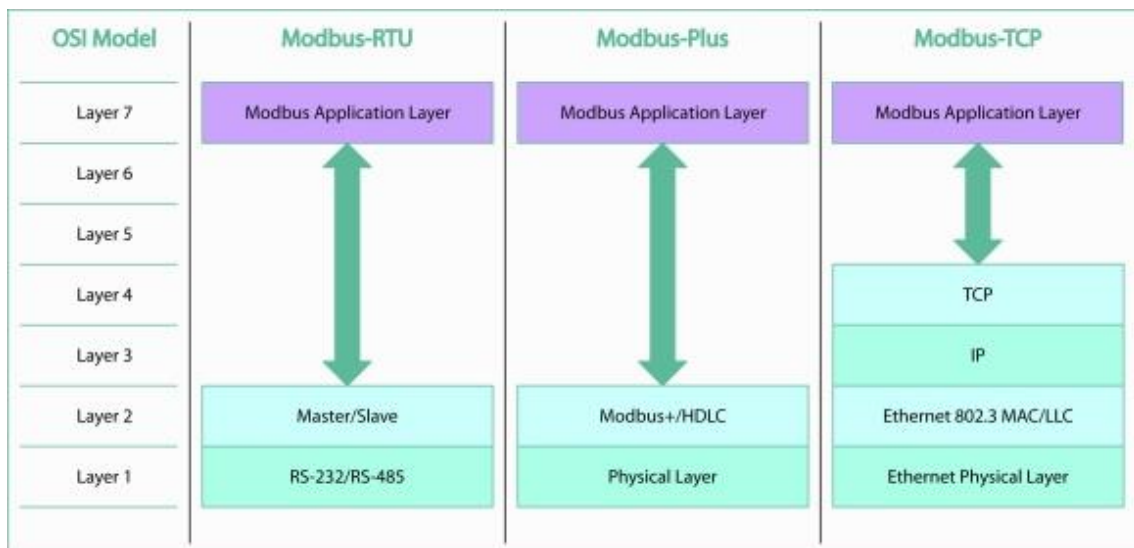
Verkkomaailmassa on käytössä seitsenkerroksinen standardimalli kuvaamaan protokollarakenteita. Sitä kutsutaan OSI-malliksi (Open Systems Interconnection). OSI-mallin on laatinut kansainvälinen standardisointiorganisaatio ajatuksena yhdenmukaistaa verkkoprotokollajärjestelmiä sekä auttaa muiden protokollien liittämistä toisiinsa. OSI-malli on monelta osin yhtäläinen TCP/IP-protokollamallin kanssa, vaikka ne eivät virallisesti vastaakaan toisiaan. Huomionarvoista on kuitenkin se, että OSI-malli on vain standardi, ei toteuttamistapa. Todelliset

verkko-ohjelmistot eivät välttämättä vastaa täysin OSI-mallia, joka on esitetty kuvassa 10. (10, s. 25–26.)



KUVA 10. OSI-malli (12)

OSI-mallilla voidaan havainnollistaa myös automaation kenttäväyläprotokollien kommunikointia verkon yli. Kuvassa 11 on esitetty, mitkä Modbus-protokollan kerrokset vastaavat OSI-mallin kerroksia.



KUVA 11. Modbus-protokollapinot OSI-mallissa (13)

2.4 Automaation tietoturva

Automaatiojärjestelmissä tietoturva on yksi sen tärkeimmistä ominaisuuksista. Mahdollisia automaatioon liittyviä tietoturvariskejä ovat mm. järjestelmään tunkeutuminen, erilaiset haittaohjelmat, puskuriylivuodot, palvelunestohyökkäykset tai tietojen kalastelu mm. sähköpostin kautta (14, s. 18–23).

Yleisradion esittämässä Docstop: Team Whack – Kaikki on hakkeroitavissa -ohjelman jaksossa 1 ryhmä onnistui murtautumaan tunnetun suomalaisen rakennusautomaatiojärjestelmiä kehittävän yrityksen laitteeseen sisään mm. komentokehotteiden kautta. Tämän jälkeen ryhmä etsi kyseisen yrityksen automaatiolaitteita julkisesta verkosta Shodan-palvelun kautta ja löysi niitä ympäri Suomea, mm. asunto-osakeyhtiöiden, apteekkien sekä jäähallin rakennusautomaatiolaitteita. Näiden järjestelmien väärinkäyttö voisi aiheuttaa mittavia omaisuusvahinkoja ja mahdollisia ihmisiin kohdistuvia vaaratilanteita. (17.)

Automaatiojärjestelmien verkottuminen on mahdollistanut niiden etähallinnan, mutta myös sen, että niihin voidaan murtautua vahingontekomielessä. Tälläkin hetkellä on valtava määrä julkisessa verkossa kiinni olevia laitteita, jotka ovat kaikkien verkonkäyttäjien saavutettavissa, myös niiden, jotka voisivat omilla toimenpiteillä saada isoja vahinkoja aikaiseksi. Viime vuosina rakennusautomaatiojärjestelmiä on alettu poistaa julkisesta verkosta tietoturvan takia.

2.4.1 Laitteiston ylläpito

Jotta mahdolliset tietoturva-avoittuvuudet voidaan mahdollisimman hyvin välttää, on laiteohjelmistot pidettävä ajan tasalla. Tarpeen vaatiessa ohjelmistot tulee päivittää uusimpiin versioihinsa. Tietoturvapäivityksiä ei tulisi koskaan sivuuttaa, koska niissä voi olla korjauksia mahdollisesti löytyneisiin tietoturva-aukkoihin tai ne voivat parantaa tietoturvaa yleisellä tasolla.

Ohjelmiston testausversioiden, esimerkiksi alfa- tai betaversioiden käyttöä tulee tarkoin harkita. Varhaiset ohjelmistoversiot saattavat sisältää tietoturvariskejä, joita ei ole mahdollisesti huomattu. Jos mahdollisia tietoturva-aukkoja havaitaan, tulisi niistä tiedottaa ensi tilassa ohjelmiston kehittäjille.

2.4.2 Salasanat

Salasanat ovat yksi tärkeimmistä tunnistautumisen keinoista. MWR Infosecurityn Ben Barkowitz havaitsi riippumattomassa tutkimuksessaan, että yleisimmät salasanat vuonna 2018 ovat edelleen "123456", "password", "123456789", "12345678", "12345" ja "qwerty" (15). Tällaiset salasanat ovat helposti arvattavissa tai salasanat voidaan murtaa nykyajan laskentatehoilla minuuteissa, jopa sekunneissa.

Asiantuntijat neuvovat, että salasana tulisi olla vahva ja uniikki. Samaa salasanaa ei tulisi käyttää koskaan kahdessa eri palvelussa. F-Securen tietoturva-asiantuntija neuvoo, että hyvä salasana on kuin salalause. Kun salalause on keksitty, sitä voidaan muokata lisäämällä sinne isoja ja pieniä kirjaimia, numeroita ja ääkkösiä. (16.)

Valitettavan usein myös automaatiojärjestelmiin tunnistautumiseen käytetään salasanoja, jotka ovat muotoa "1234", "admin", "root" tai esimerkiksi "huolto". Tämän kaltaisten salasanojen käytöstä tulisi luopua pikimmiten. Vaikka järjestelmiin päästäisiinkin käsiksi verkon yli, voidaan vahvan salasanan käytöllä vielä estää pääsy automaation ohjausjärjestelmiin.

Monesti mielletään, että hyvä tietoturva ja nopea ja helppo käytettävyys ovat ristiriidassa. Kun nämä kaksi asiaa ovat vaakakupissa, tulisi tietoturvan mennä edelle. Hieman vaivalloisempi käyttö ei ole yhtä huono vaihtoehto kuin mahdollinen tietoturvariski.

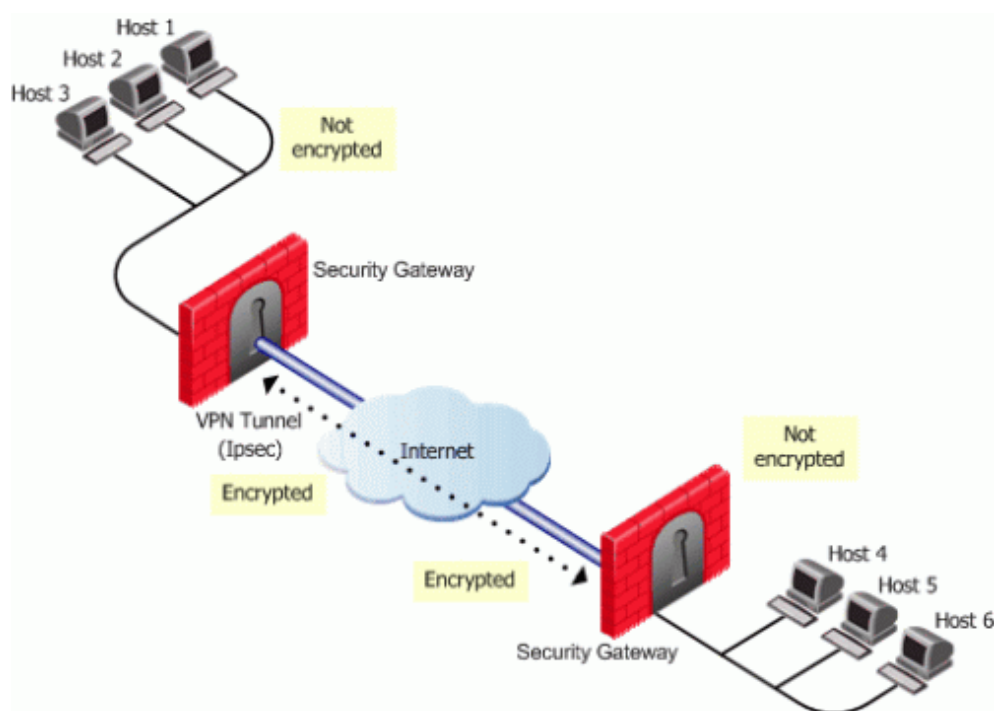
2.4.3 Virtual Private Network

Rakennusautomaatiojärjestelmiä ei tulisi järjestelmällisesti liittää julkiseen verkkoon, vaan yhteydet tulisi piilottaa julkisesta verkosta. Rakennusautomaatiojärjestelmien ja etähallinnan välille on luotava salattu yhteys. Tähän tarkoitukseen on käytössä eritasoisia protokollia hyödyntävä VPN-tekniikka (Virtual Private Network). (18, s. 16.)

VPN toimii siten, että lähettäjän ja vastaanottajan välille luodaan "tunneli", jossa tieto kulkee. Lähettäjän tiedot viedään VPN-palvelimelle, jossa tiedot salataan ja

lähetetään internetin kautta vastaanottajalle. Vastaanottajan päässä salaus puretaan ja tiedot voidaan käsitellä. Vastaanottaja lähettää myös omat tietonsa VPN-palvelimelle, jossa tiedot taas salataan ja lähetetään alkuperäiselle lähettäjälle. Lähettäjän päässä salaus puretaan ja tieto voidaan sen jälkeen taas hyödyntää. (19.)

VPN voidaan ajatella eräänlaisena tunnelina, johon pääsee käsiksi vain tunnelin päistä. Vaikka tunnelin sisällä olevat tiedot saataisiin kaapattua, ei siihen voi tehdä muutoksia vastaanottajan huomaamatta. Tiedon avaamiseen tarvitaan aina salausavaimet, jotta tieto saadaan selkokieliseksi. VPN:n toimintaperiaatetta on havainnollistettu kuvassa 12. (18, s. 17–18.)



KUVA 12. VPN:n toimintaperiaate (20)

2.4.4 Tosibox

Valvomotason sekä kohteiden automaatiolaitteistojen välinen salattu yhteys voidaan luoda käyttämällä Tosibox-etäyhteyslaitteita.

Tosibox on vuonna 2011 perustettu oululainen yritys, joka valmistaa VPN-etäyhteyslaitteistoja automaatio- ja turvallisuusaloille. Tosibox on maailman ensimmäinen Plug & Go -tekniikalla toimiva etäyhteyslaitteisto. Tosibox-etäyhteyslaitteet

täyttävät ISAE3000-, ISO 27001:2013 -standardit ja laitteita on käytössä Euroopassa, Yhdysvalloissa, Aasiassa, Lähi-Idässä sekä Australiassa. (21.)

Tosibox-etäyhteydet perustuvat lukko-etäyhteyslaitteeseen sekä Tosibox-avaimen. Näiden kahden laitteen välille luodaan VPN-yhteys. Tosibox-lukko ja avain toimivat VPN-tunnelin ääripäinä. Tosibox-lukon ja -avaimen parittaminen tapahtuu fyysisesti asettamalla avain lukkolaitteen USB-porttiin. Lukkolaite sekä avain vaihtavat salausavaimensa keskenään. Tämän lisäksi Tosibox-avain suojataan aina salasanalla (21).

Tosibox-lukkolaite ja avain vaativat toimiakseen aina internet-yhteyden. Yhteys internetiin voidaan hoitaa kohteessa kiinteillä WAN-yhteyksillä tai 4G-mobiiliverkon avulla.

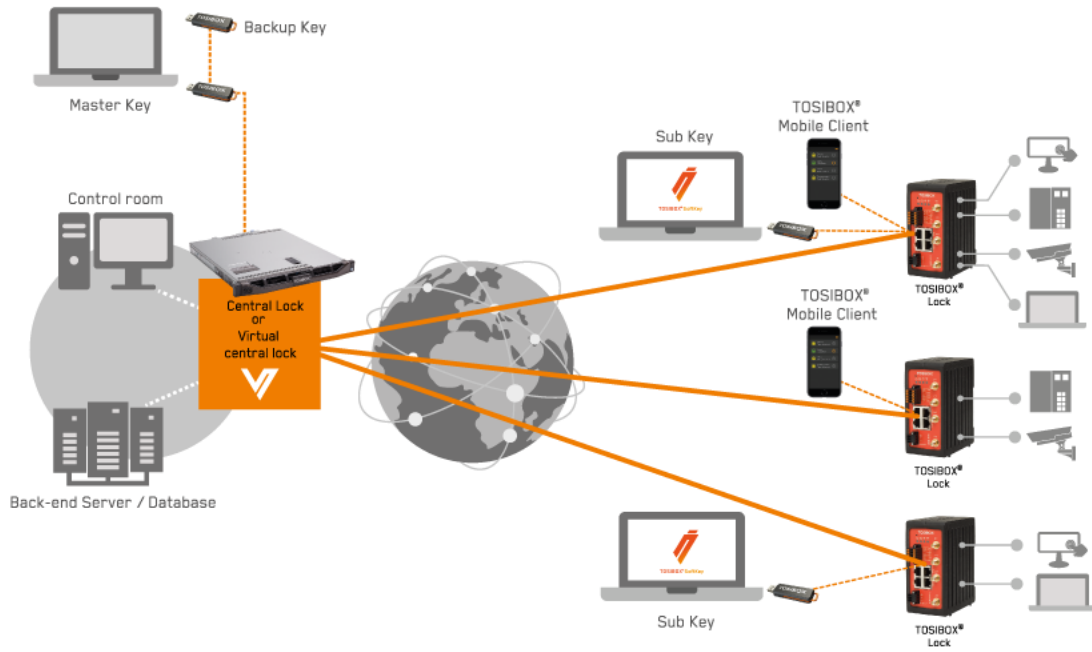
Kuvassa 13 on esitetty toimintaperiaate, miten yhteydet mm. automaatiojärjestelmien sekä etävalvomon välillä voidaan muodostaa. Lukkolaitteeseen kytketään kaikki etähallittavat kohteet sekä internet-yhteys. Tämän jälkeen sarjoitettu avain kytketään käyttöpäätteeseen, jolloin VPN-yhteys muodostuu avaimen ja lukon välille. (18, s. 31.)



KUVA 13. Tosibox-etäyhteyksien toimintaperiaate (21)

Oulun Virtuaalivalvomossa on konesalissa Tosibox-keskuslukko (Central Lock). Keskuslukon tiedonsiirto- sekä salauskapasiteetti mahdollistaa jopa tuhansien eri lukkolaitteiden tai avaimien yhtäaikaisen käytön. Keskuslukosta voidaan helposti hallinnoida yhteyksiä eri lukkolaitteiden sekä avaimien välillä. (18, s. 41.)

Virtuaalivalvomon kohteissa olevat lukkolaitteet kommunikoivat konesalissa sijaitsevan keskuslukon kautta palvelimelle. Kuvassa 14 on havainnollistettu keskuslukon käyttöä etäyhteyksissä.



KUVA 14. Tosibox-keskuslukon toimintaesimerkki (21)

3 PYRAMID-AUTOMAATIOJÄRJESTELMÄ

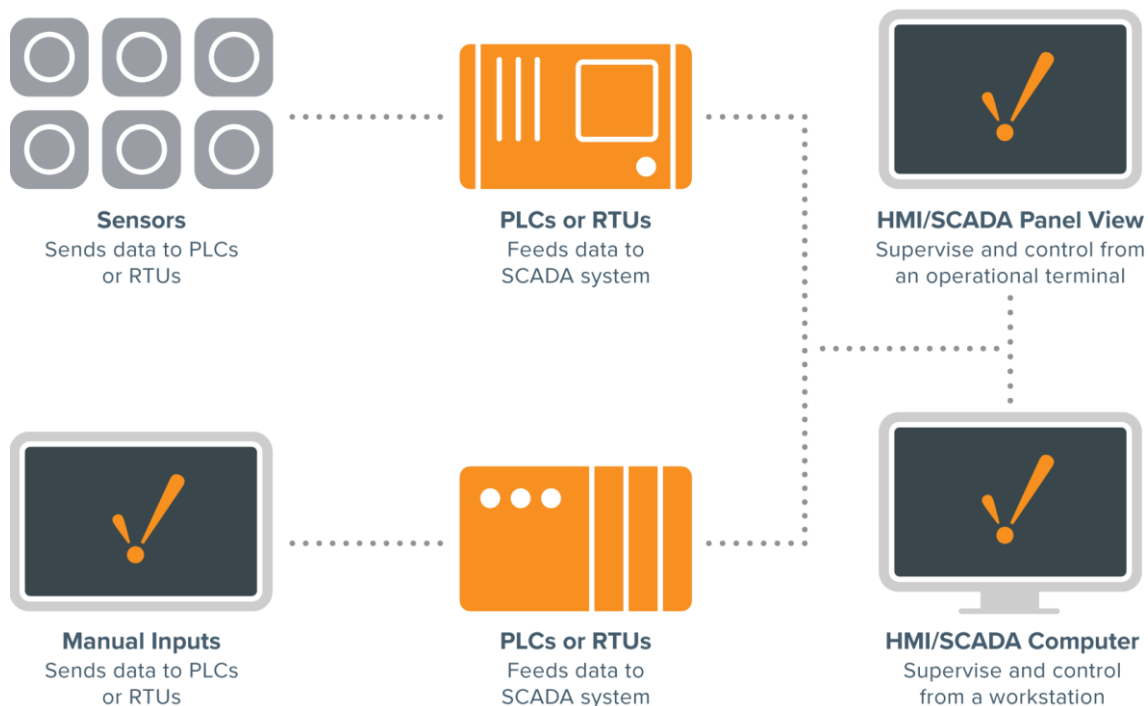
3.1 Schneider Electric Citect SCADA

SCADA (Supervisory control and data acquisition) tarkoittaa ohjelmistoja, joilla luodaan käyttöliittymä käyttäjän sekä automaatiolaitteiston välille. SCADA-ohjelmistolla voidaan suorittaa käskyjä sekä tarkkailla ja kerätä reaaliaikaisia tietoja automaatiolaitteistosta. Voisi sanoa, että SCADA muuntaa automaatiojärjestelmän sähköiset viestit ihmiselle helposti tulkittavaan muotoon. (22.)

SCADA-konsepti luotiin jo 1920-luvun puolivälissä. Ennen SCADA-ohjelmistoja prosesseja ohjattiin ja seurattiin paikan päällä käytännössä fyysisten painikkeiden sekä analogisten mittareiden avulla. Kun laitteistot ja tehtaot kasvoivat, aiheutti prosessien ylläpitäminen ongelmia, koska prosessien ohjaaminen kohteesta hankaloitui. Ajastimet ja releiden käyttö helpotti hieman tilannetta, mutta niiden uudelleenohjelmointi tuotti vaikeuksia. Tarvittiin tehokkaampi tapa ohjata ja seurata prosessien tilaa. (22.)

SCADA-ohjelmiston kehittyminen voidaan katsoa alkaneeksi 1950-luvulla, kun ensimmäiset tietokoneet saapuivat teollisuuden käyttöön. Mikroprosessorien ja ohjelmoitavien logiikoiden yleistyminen vauhditti automaatiojärjestelmien käyttöliittymien kehitystä. 1990- ja 2000-luvulla SCADA-järjestelmät alkoivat siirtyä internetiin. Tätä voidaan pitää etävalvomoiden kehityksen alkuna. (22.)

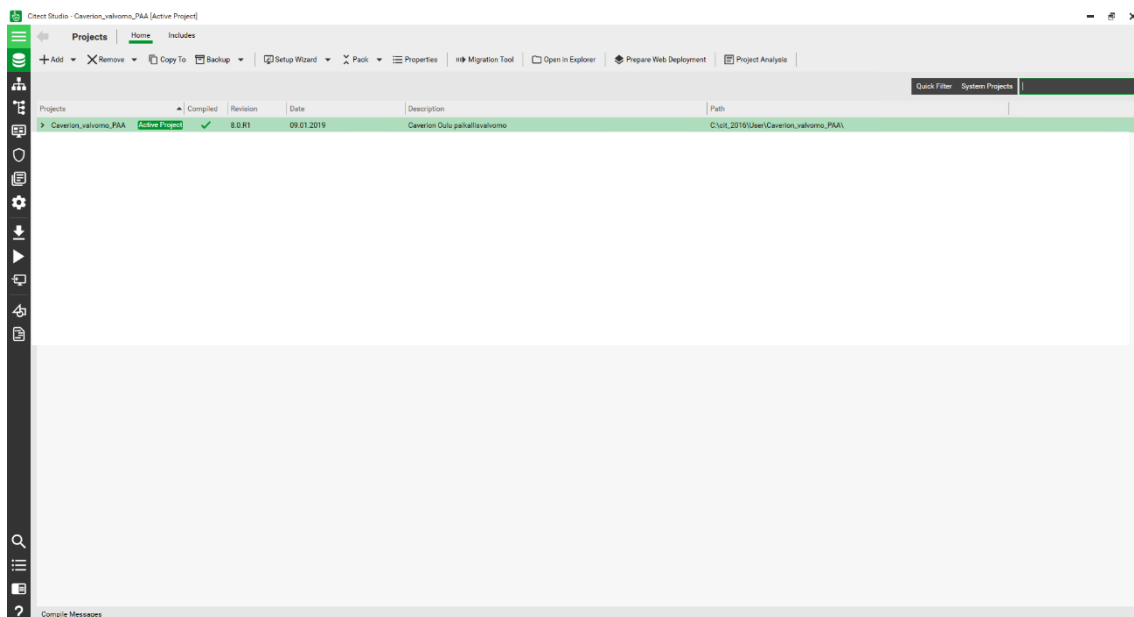
Nykyaikainen SCADA-ohjelmisto mahdollistaa reaaliaikaisen prosessien seurannan lähes joka paikasta maailmassa, vaatimuksena on käytännössä enää vain internet-yhteys valvomon ja käyttöpaatteen välillä. Ilman nykyaikaisia SCADA-ohjelmistoja olisi datan kerääminen sekä automaatiojärjestelmien käyttö todella haastavaa (22). Kuvassa 15 on havainnollistettu nykyaikaisen SCADA-järjestelmän toimintaa automaatiojärjestelmässä.



KUVA 15. Yksinkertainen SCADA-kaaviokuva (22)

Citect SCADA on Schneider Electricin kehittämä SCADA-ohjelmistoratkaisu prosessienhallinnan asiakkaille. Citect SCADA sisältää kaikki tarvittavat projektihallinta- sekä grafiikanpiirtotyökalut, joilla kohteen valvomoympäristöt voidaan luoda. (23).

Uusimmassa SCADA 2016 -versiossa on yhdistetty kaikki tarvittavat toiminnot yhteen sovellukseen, jota kutsutaan nimellä Citect Studio (Kuva 16). Aiemmissa versioissa projektihallinta- sekä grafiikanpiirtotyökalut olivat erillisiä sovelluksia. Tärkein Citect SCADA:n työkalu on kuitenkin Cicode Editor, jolla valvomon ohjelmistot luodaan. Caverion Pyramid-lähdekoodi on luotu Cicodella. Pyramid-lähdekoodi on kokonaisuudessaan Caverion Suomi Oy:lle kuuluvien tekijänoikeuksien alaista omaisuutta.



KUVA 16. Citect SCADA Studio 2016 -projektinhallintaohjelmisto

3.2 Citect Anywhere

Citect Anywhere on Windowsin etätyöpöytäyhteyksiin perustuva lisäosa Citect SCADA-ohjelmistoon. Citect Anywhere mahdollistaa valvomon etäyhteydet kaikista HTML5-yhteensopivista selaimista. Etävalvomon käyttöön ei vaadita ollenkaan ohjelmistoja, vaan nykyaikainen nettiselain riittää valvomon käyttöön. Citect Anywhere vaatii toimiakseen Windows Server-käyttöjärjestelmän, jossa täytyy olla asennettuna AD-toimialue- (Active Directory) sekä RDS-etätyöpöytäpalvelut (Remote Desktop Services). (24.)

3.3 Konesalit

Caverion Virtuaalivalvomo sijaitsee fyysisesti Etelä-Suomessa sijaitsevassa konesalissa. Konesali tarkoittaa tietoteknistä käyttöä varten erityisesti varustettua ja rajattua tilaa tai rakennusta, jossa on paljon suurien tietomäärien käsittelyyn tarvittavia tietokoneita sekä laitteita.

Konesali käsittää pääasiassa sähköisiä laitteita datan prosessointiin. Näitä kutsutaan palvelimiksi (kuva 17). Konesalit sisältävät myös levyjärjestelmät tiedon varastointiin sekä kommunikointiin vaadittavat verkkojärjestelmät. (25, s. 3.)

Konesalin etuina voidaan pitää hyvää tilaturvaa. Tilaturvalla tarkoitetaan sitä, että tietotekniset laitteistot sijaitsevat hyvin suojatuissa tiloissa, jonne ulkopuolisten pääseminen on käytännössä mahdotonta. Konesaleissa on myös varavoimalaitteisto mahdollisen sähkön syötön katkeamisen varalta. Konesaleissa olevat tiedot ovat myös varmennettuja, mahdollinen tallennusjärjestelmien hajoaminen ei aiheuta mittavia tuhoja, vaan tiedot on varmuuskopioitu ja niitä voidaan hyödyntää mahdollisessa vikatilanteessa.



KUVA 17. Konesalilaitteistoja (26)

3.4 Välityspalvelimet

Välityspalvelimet (Proxy Server) reitittävät tietoja internetissä tiedon lähettäjän ja vastaanottajan välillä. Normaalisessa tilanteessa verkkokäyttäjä lähettää tietoja suoraan vastaanottajalle ja vastaanottaja myös vastaa takaisin suoraan tietojen alkuperäiselle lähettäjälle. Kun käytetään välityspalvelimia, tietojen lähetys tapahtuu niin, että tiedot ohjataan ensin välityspalvelimelle, josta tiedot ohjataan vastaanottajan luokse. Vastaanottajan lähettämät tiedot kulkevat myös välityspalvelimien kautta takaisin alkuperäiselle lähettäjälle. Välityspalvelimien käytössä on hieman samoja piirteitä kuin VPN-yhteyksissä, mutta ne eivät silti vastaa toisiaan. (27.)

Välityspalvelimet toimivat verkossa hieman samaan tapaan kuin palomuurit tai filterit. Niillä pystytään ehkäisemään esimerkiksi tiedonkaappausyrityksiä lähet-

täjän ja vastaanottajan välisessä tiedonsiirrossa. Välityspalvelin pystyy muokkaamaan lähettäjän tietoja siten, että lähettäjää on vaikeaa tunnistaa, mutta tiedot saapuvat vastaanottajalle toivotussa muodossa. Kun välityspalvelimeen otetaan yhteyttä jollain tietyllä IP-osoitteella, voi välityspalvelin lähettää tiedot eri IP-osoitteella vastaanottajalle, jolloin vastaanottaja ei välttämättä pysty tunnistamaan lähettäjää. Tällä tavoin identiteetti voidaan salata paremmin verkossa. (27.)

Hyvät välityspalvelimet ovat yleensä maksullisia ja ilmaisiin välityspalvelimiin kannattaa suhtautua varauksella. Niissä ei välttämättä löydy tietojen suojaamiseen tarvittavia ominaisuuksia tai tiedot voidaan pahimmassa tapauksessa vuotaa tahallisesti ulkopuolisille.

Oulun Virtuaalivalvomossa yhteyden luominen Tosibox-keskusluvon ulkopuolisesta verkosta konesalin palvelimelle luodaan Caverion Oneportal-välityspalvelimen kautta. Caverion Oneportalin käyttö on täysin turvallista ja se vaatii vain käyttäjätunnukset, joilla palveluun pääsee kirjautumaan. Onnistunut kirjautuminen ohjaa käyttäjän konesalin palvelimelle, jossa voidaan avata etävalvomoyhteys Citect Anywhere -sovelluksen kautta.

3.5 Windows Server

Konesalin palvelin-PC:llä käytettiin Virtuaalivalvomo-projektissa Microsoft Windows Server 2012 R2-käyttöjärjestelmää. Windows Server-käyttöjärjestelmät eroavat perinteisistä Windows-käyttöjärjestelmistä siten, että ne on optimoitu suurten tietomäärien jakamiseen sekä suurempien käyttäjämäärien hallinnoimiseen.

Windows Server-käyttöjärjestelmän käyttö on pakollista, jos etäyhteyksien luontiin käytetään Citect Anywhere -sovellusta. Citect Anywhere vaatii kaksi toimintoa, jotka toimivat Windows Server-käyttöjärjestelmässä. Nämä toiminnot ovat ADDS (Active Directory Domain Services) sekä Windows RDS (Remote Desktop Services).

ADDS-palvelulla voidaan luoda Windowsin toimialue, jolla hallinnoidaan järjestelmän tietokoneita, käyttäjiä sekä sovelluksia. Virtuaalivalvomossa toimialuetta kutsutaan Pyramid-toimialueeksi. Tälle toimialueelle on luotu kaikki etäyhteyksiin vaadittavat käyttäjät sekä toimialuetta hallinnoi järjestelmänvalvoja. (28.)

RDS-palvelulla mahdollistetaan haluttujen käyttäjien etätyöpöytäyhteyksien luonti isäntäpalvelimelle. Isäntäpalvelimena toimii Virtuaalivalvomossa Pyramid 8-valvomo-PC. Käytännön tasolla, kun käyttäjä ottaa etäyhteyden Virtuaalivalvomon, lataa käyttäjä selaimelleen näkymän räätälöidystä Windows Server-käyttöliittymästä, jossa näkyy ainoastaan Pyramid-valvomosovellus.

4 VIRTUAALIVALVOMO

Luottamuksellinen.

5 YHTEENVETO

Opinnäytetyön tavoitteena oli ottaa käyttöön konesalissa uusi Pyramid 8 -automaatiojärjestelmä, jonka käyttö olisi mahdollisimman asiakasystävällistä sekä turvallista. Työssä oli tarkoitus kartoittaa uuden valvomojärjestelmän kustannuksia sekä opinnäytetyöstä tuli saada julkaisukelpoinen, jotta sitä voitaisiin esitellä mahdollisille asiakkaille.

Työ eteni kohtuullisen nopeasti eteenpäin, suurempia ongelmia työn aikana ei tullut eteen. Pienellä avustuksella pienistä ongelmista selvittiin nopeasti. Työtä helpotti huomattavasti tuotekehityksen pitämä lyhyt koulutus ja se, että Etelä-Suomessa kyseistä järjestelmää oli keretty jonkin verran jo testata, joten täysin puhtaalta pöydältä ei tarvinnut aloittaa.

Työn lopputuloksena saatiin luotua konesaliin Pyramid -automaatiojärjestelmä, joka nimettiin Virtuaalivalvomoksi. Siihen pystytään ottamaan etäyhteys laitteesta riippumatta. Ainoa vaatimus on toimiva internet-yhteys sekä HTML5-yhteensopiva selain. Jos etävalvomoa käytetään Oneportal-etätyöpöytäyhteyksien kautta, käyttömukavuus hieman kärsii, kun joudutaan kirjautumaan sivustoilla pariin otteeseen, mutta järjestelmään voidaan tehdä automaattinen kirjautumisprofiili, jolloin vältytään useilta kirjautumisilta.

Usealla kirjautumisella myös hyvät puolensa tietoturvaa ajatellen. Useampi kirjautuminen vaikeuttaa järjestelmiin murtautumista. Tietoturvan takia myös kaikissa kohteissa käytettiin Tosibox-etäyhteyslaitteita. Asiaton järjestelmien käyttö tulee kaikissa tilanteissa pyrkiä estämään.

Pyramid-automaatiojärjestelmää ei alun perin ole suunniteltu käytettäväksi mobiililaitteissa, jotkut ominaisuudet tarvitsevat vielä hienosäätöä, että käytettävyys paranisi. On keskusteltu, että järjestelmää tullaan tulevaisuudessa kehittämään siten, että mobiilikäyttö paranisi.

Täydellistä kustannuslaskentaa ei järjestelmän pystyttämisestä ja ylläpidosta ole vielä tehty, mutta kartoitus tehdään tarvittaessa, kun saadaan kohteita hieman

lisää Virtuaalivalvomoon. Tämä opinnäytetyö pyrittiin pitämään julkaisukelpoisena. Tämän vuoksi opinnäytetyöhön ei voitu lisätä yksityiskohtaisia tietoja valvomojärjestelmästä, automaatiolaitteiston verkkoihin liittyvistä toiminnoista tai automaatiojärjestelmien ohjelmoinnista.

Kaiken kaikkiaan projekti oli haastava ja mielenkiintoinen. Työssä pääsi perehtymään mm. tietoliikenneverkkoihin, automaatio-ohjelmointiin sekä konesalitekniikkaan. Vaikka tietoteknisiä taitoja hieman jo löytyi, opiskeltavaa oli paljon, mutta tulevaisuutta ajatellen tästä opinnäytetyöstä on varmasti hyötyä. Virtuaalivalvomon kehitystä jatketaan tulevaisuudessa kohti parempaa valvomojärjestelmää.

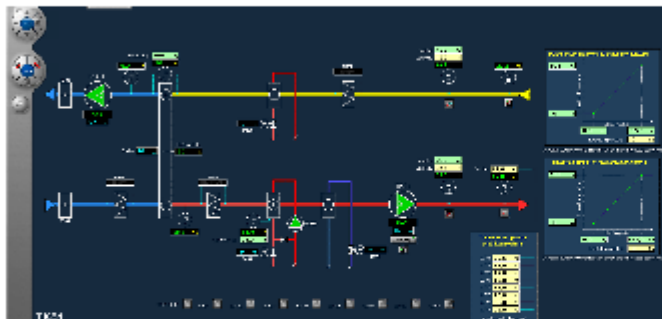
LÄHTEET

1. Caverion 2019. Liiketoiminta ja palvelut. Saatavissa: <https://www.caverion.fi/tietoa-caverionista/liiketoiminta-ja-palvelut> Hakupäivä 4.3.2019
2. ST-käsikirja 17. Sähkötieto ry 2018. Rakennusautomaatiojärjestelmät. Espoo: Sähköinfo Oy
3. Pirhonen, Tero 2011. Kiinteistöautomaation peruselementit ja -toiminnot sekä kiinteistöautomaatioprojektin toteutus. Opinnäytetyö. Helsinki: Metropolian ammattikorkeakoulu, automaatiotekniikka
4. ST-käsikirja 22. Sähkötieto ry 2017. Kiinteistöjen valvomojärjestelmät. Espoo: Sähköinfo Oy
5. Schneider Electric 2019. Guide to Open Protocols in Building Automation. Saatavissa: https://blog.schneider-electric.com/wp-content/uploads/2015/11/SE-Protocols-Guide_A4_v21.pdf Hakupäivä 28.4.2019
6. Pro dual Pump. Langattomat rakennusautomaatioratkaisut kehittyvät. Blogikirjoitus. Saatavissa: <http://www.produal.com/fi/pump/blog/langattomat-rakennusautomaatioratkaisut-kehittyvat/> Hakupäivä 13.5.2019
7. Pro dual 2019. WBU-tukiasema. Saatavissa: http://www.produal.com/fi/shop/web_wireless_proxima_mesh/sku-54011W0000 Hakupäivä 13.5.2019
8. Ikonen, Matti 2011. Rakennusautomaatiojärjestelmien toimintaympäristöt ja järjestelmäkehityksen tavoitteet. Opinnäytetyö. Jyväskylä: Jyväskylän ammattikorkeakoulu, automaatioteknologian koulutusohjelma
9. Modbus Organization 2019. Modbus FAQ: About the Protocol. Saatavissa: <http://www.modbus.org/faq.php> Hakupäivä 28.4.2019
10. Casad, Joe – Willsey, Bob 1999. TCP/IP Trainer. Jyväskylä: Gummerus Kirjapaino Oy

11. Wikipedia 2018. Reititin. Saatavissa: <https://fi.wikipedia.org/wiki/Reititin> Hakupäivä 2.5.2019
12. Wikipedia 2018. OSI-malli. Saatavissa: <https://fi.wikipedia.org/wiki/OSI-malli> Hakupäivä 2.5.2019
13. Johnson, Glenn 2009. Determinism in Industrial Ethernet: A technology Overview – Part 2. Saatavissa: <https://www.processonline.com.au/content/industrial-networks-buses/article/determinism-in-industrial-ethernet-br-a-technology-overview-part-2-966929628> Hakupäivä 2.5.2019
14. Suomen Automaatioseura ry 2005. Teollisuusautomaation tietoturva, Verkottumisen riskit ja niiden hallinta. Helsinki: Painomerkki Oy
15. Rantalainen, Tuomas 2018. Yksinkertaiset ohjeet yksinkertaisen salasanan parantamiseksi. Blogikirjoitus. Saatavissa: <https://blog.f-secure.com/fi/yksinkertaiset-ohjeet-yksinkertaisen-salasanan-parantamiseksi/> Hakupäivä 3.5.2019
16. Uusi Suomi 2008. F-Securen asiantuntija neuvoo: Näin muodostat hyvän salasanan. Saatavissa: <https://www.uusisuomi.fi/kotimaa/16389-f-securen-asiantuntija-neuvoo-nain-muodostat-hyvan-salasanan> Hakupäivä 3.5.2019
17. Yleisradio 2019. Docstop: Team Whack – Kaikki on hakkeroitavissa, Jakso 1: Team Whack iskee taloyhtiöön. Video. Saatavissa: <https://areena.yle.fi/1-4664683> Hakupäivä 3.5.2019
18. Niemisalo, Heikki 2016. Etävalvomon tietoliikenneyhteyksien kehitysprojekti. Opinnäytetyö. Oulu: Oulun ammattikorkeakoulu, talotekniikan tutkinto-ohjelma
19. Crawley, Kim 2018. Explain How VPN Works. Saatavissa: <https://www.alienvault.com/blogs/security-essentials/explain-how-vpn-works> Hakupäivä 4.5.2019

20. Vaughan-Nicholas, Steven J. 2017. How Does A VPN Work? Saatavissa: <https://www.ign.com/articles/2017/08/11/how-does-a-vpn-work> Hakupäivä 4.5.2019
21. Tosibox 2019. Saatavissa: <https://www.tosibox.com> Hakupäivä 4.5.2019
22. Inductive Automation 2018. What is SCADA? Saatavissa: <https://inductiveautomation.com/resources/article/what-is-scada> Hakupäivä 6.5.2019
23. Schneider Electric 2018. Citect SCADA: SCADA Software for Industrial Processes. Saatavissa: <https://www.schneider-electric.com.au/en/product-range-presentation/1500-citect-scada/#tabs-top> Hakupäivä 6.5.2019
24. Schneider Electric 2015. Citect Anywhere. Saatavissa: <http://www.con-trosys.hu/download/Citect/Citect-Anywhere-Brochure.pdf> Hakupäivä 6.5.2019
25. Karjalainen, Unto 2017. Energiätehokkuuden merkitys konesaleille. Opinnäytetyö. Kajaani: Kajaanin ammattikorkeakoulu. Tradenomi, tietojenkäsittely
26. Elisa 2015. Yrityksen kokoinen ja turvallinen konesali. Saatavissa: <https://hub.elisa.fi/yrityksen-kokoinen-ja-turvallinen-konesali/> Hakupäivä 6.5.2019
27. Petters, Jeff 2019. What is Proxy Server and how does it work? Blogikirjoitus. Saatavissa: <https://www.varonis.com/blog/what-is-a-proxy-server/> Hakupäivä 6.5.2019
28. Microsoft 2018. Active Directory Domain Services. Saatavissa: <https://docs.microsoft.com/en-us/windows/desktop/ad/active-directory-domain-services> Hakupäivä 6.5.2019

Caverion



Paikallisvalvomo, Pohjois-Suomi

(Caverion Pyramid-automaatiojärjestelmä)

onePortal

Yleiskuvaus

Caverionin paikallisvalvomo on suunniteltu kiinteistöjen etävalvontaan Pohjois-Suomen alueelle.

Pohjois-Suomen paikallisvalvomo hyödyntää uutta Caverion Pyramid 8-automaatiojärjestelmää. Pyramid 8 tukee Citect Anywhereä, jossa valvomosovellusta voidaan käyttää mistä tahansa HTML5-pohjaisista selaimista.

Valvomosovelluksen käyttö ei vaadi erillisiä valvomo-ohjelmistoja tai kiinteitä valvomopäätteitä. Valvomoa voidaan käyttää mobiililaitteissa sekä tietokoneissa käyttöjärjestelmästä riippumatta.

Pohjois-Suomen paikallisvalvomoa ylläpidetään Caverionin konesalin palvelimilla. Konesalin käytöllä parannetaan tietoturvaä sekä helpotetaan valvomon huoltotöitä. Yhdistäminen konesaliin voidaan tehdä turvallisesti Caverion Oneportal-palvelun avulla.

Caverion Oulun paikallisvalvomo on lähtökohtaisesti tarkoitettu Pohjois-Suomen alueen asiakkaiden tarpeisiin, mutta Pyramid-8 automaatiojärjestelmä voidaan toteuttaa asiakkaan tarpeiden mukaisesti paikkakunnasta riippumatta.

Ominaisuudet

- Valvomon käyttö on mahdollista kaikissa HTML5-yhteensopivissa laitteissa.
- Reaaliaikainen valvomon käyttö paikasta riippumatta
- Ei vaadi erillisiä valvomo-ohjelmistoja.
- Tietoturvallinen kiinteistöautomaatiojärjestelmä.

Lisätietoja automaatiojärjestelmästä:



Aleks Holappa, Huoltopäällikkö
p. 0505600661
aleksi.holappa@caverion.com



Jari Jussinniemi, Myyntipäällikkö
p. 0505185020
jari.jussinniemi@caverion.com



Luottamuksellinen.

Luottamuksellinen.