Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Lari Lindholm

Rakennusautomaatiojärjestelmän valvomon päivitystyö

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikka

Insinöörityö

6.5.2021

Tekijä Otsikko Sivumäärä Aika	Lari Lindholm Rakennusautomaatiojärjestelmän valvomon päivitystyö 26 sivua 6.5.2021
Tutkinto	Insinööri (AMK)
Tutkinto-ohjelma	Sähkö- ja automaatiotekniikka
Ammatillinen pääaine	Automaatiotekniikka
Ohjaajat	Asiakaspalvelupäällikkö Risto Keinänen Lehtori Reijo Leinonen

Tässä insinöörityössä perehdyttiin rakennusautomaation valvontajärjestelmän päivitykseen ja siirtoon konesaliympäristössä toimivaksi. Työn tilaajana oli eteläisessä Suomessa sijaitseva kunta ja toimittajana Caverion Suomi Oy. Tietoturvallisuuden takia tämä raportti on kirjoitettu niin, ettei asiakasta mainita eikä kaikkia käytettyjä ratkaisuja yksilöidä. Tämän työn tavoitteena oli suorittaa järjestelmän päivitys ja muutostyö asiakkaalle sekä oppia hahmottamaan työn kokonaisuus tulevaisuutta varten.

Työssä perehdyttiin teorian avulla automaatiojärjestelmien tiedonsiirtoon, tietoturvallisuuteen ja etäkäyttöön sekä konesaliympäristöihin. Työ eteni koneympäristön perustamisen kautta tietoturvallisten yhteyksien muodostamiseen ja järjestelmäversion päivitykseen. Työ tehtiin yhteistyössä Caverion Suomi Oy:n tuotekehityksen kanssa, joten kaikki tässä työssä tehdyt työvaiheet eivät ole allekirjoittaneen tekemiä.

Työn tuloksena järjestelmäversio päivitettiin, ja jatkossa valvontajärjestelmä toimii konesalissa. Järjestelmä on etäkäytettävissä selaimen avulla alustasta riippumatta. Työn kautta saatu kokemus auttaa jatkossa seuraavissa järjestelmäpäivityksissä.

Avainsanat	Rakennusautomaatio, konesali, etäkäyttö, Tosibox

Author Title Number of Pages Date	Lari Lindholm Upgrading of a Building Automation System Control 26 pages 6 May 2021
Degree	Bachelor of Engineering
Degree Programme	Electrical and Automation Engineering
Professional Major	Automation Technology
Instructors	Risto Keinänen, Account Manager Reijo Leinonen, Senior Lecturer

In this engineering work, the upgrade and transfer of a building automation management system to operate in a data center environment was introduced. The client of the work was a municipality in southern Finland and the service provider was Caverion Suomi Oy. For security reasons, this report is written without the customer's name, and not all the used solutions have been presented. The aim of this work was to perform system upgrade and modification work for the customer and to learn how to outline the work as a whole for the future.

Theory section of this work was focused on the data transfer, data security and remote use of automation systems, as well as computer room environments. The work progressed through the establishment of a machine environment for establishing secure connections and updating the system version. The work was done in co-operation with Caverion Suomi Oy's product development department, so not all the steps of this work have been done by the author.

As a result of the work, the system version was updated and, in the future, the control system will work in the data center. The system can be accessed remotely via a browser, regardless of the platform. The experience gained through the work will help in future system upgrades.

Keywords	Building Automation, Data Center, Remote Access, Tosibox

Sisällys

Lyhenteet ja käsitteet

AD	Microsoft Active Directory. Windows Server -käyttöjärjestelmän käyttäjien tunnistautumis- ja hallintapalvelu.
ADDS	Active Directory Domain Services. AD-palvelun domain-palvelut.
APN	Access Point Name. Mobiilipohjainen yhdyskäytävä, joka yhdistää mobiiliverkon ja tietokoneverkon julkisessa internetissä.
DMZ	Demilitarized zone. Ulko- ja sisäverkon väliin tietoturvan lisäämiseksi sijoitettu fyysinen tai looginen aliverkko.
DNS	Domain Name System. Nimipalvelujärjestelmällä muunnetaan verkkotunnukset IP-osoitteiksi.
Domain	Internetin verkkotunnukset, joiden kirjaimista koostuvien nimien avulla niihin on helpompi viitata kuin numeroista muodostuvilla IP-osoitteilla.
Ethernet	Pakettipohjainen lähiverkkojen toteutustapa.
HTTPS	Hypertext Transfer Protocol Secure. Www-palvelinten ja selainten välisen liikenteen suojattu tiedonsiirtoprotokolla.
LAN	Local Area Network. Tietoliikenteen lähiverkko.
Palvelin	Käytetään myös nimeä serveri. Tietokoneessa oleva palvelinohjelmisto sekä sitä suorittava tietokone.
Pilvipalvelu	Pilvipalveluntarjoajan palvelimella oleva ohjelma, esimerkiksi Google Drive.
Protokolla	Yhteyskäytännöllä määritellään tai mahdollistetaan laitteiden tai ohjelmien väliset yhteydet.
Proxy	Välitys- eli välipalvelin. Käytetään varastoitaessa ja suodatettaessa verkossa siirrettäviä tiedostoja.

RAU	Rakennusautomaatio.
RDP	Remote Desktop Protocol. Microsoftin kehittämä protokolla etäkäyttöön.
RDS	Remote Desktop Services. Microsoft Windowsin komponentti, jonka avulla käyttäjä voi hallita etätietokonetta tai virtuaalikonetta verkkoyhteyden kautta.
TCP/IP	Transmission Control Protocol/Internet Protocol. Tietoliikenneprotokolla.
VAK	Valvontajärjestelmän alakeskus.
VPN	Virtual Private Network. Virtuaalinen erillisverkko.

1 Johdanto

Rakennusautomaation historia ulottuu sähkötekniikan historian kautta viime vuosisadan alkuun. Tekniikka on kehittynyt 1950-luvun analogisten säätimien ja 1960-luvulla hyväksytyn 4-20 mA analogisignaalistandardin ja suoran digitaalisen säädön eli DDC:n (Director Digital Control) kautta 1990-luvulla käyttöön otettuihin itsenäisiin alakeskusyksikköihin. Tämän vuosituhannen alun aikana otetut harppaukset tietoliikennetekniikan kehityksessä ovat jo tähän mennessä mahdollistaneet rakennusautomaatiojärjestelmien suuren kehityksen. Järjestelmien on mahdollista sijaita pilvipalveluna konesaleissa ja niitä voidaan käyttää lähes laiteriippumattomasti selaimen avulla. Tulevaisuudessa järjestelmien ja tekoälyn kehittyminen tarjoaa uudenlaisia rakennuksista kerättävien tietojen analysointitapoja. [1, s. 13-16.]

Opinnäytetyön työkohteena on eteläisessä Suomessa sijaitsevan kunnan rakennusautomaatiojärjestelmän päivittäminen kunnan tiloissa olevalta fyysiseltä pöytätietokoneelta Caverion Suomi Oy:n pilvipalvelussa sijaitsevalle palvelimelle. Järjestelmän päivittäminen on ajankohtainen, koska pöytätietokone on jo kahdeksan vuoden ikäinen, ja riski hajoamiseen on todellinen. Järjestelmän toimittaja Caverion Suomi Oy ja tilaajana toimiva kunta sopivat, että Caverion Suomi Oy suorittaa automaatiojärjestelmän päivittämisen sekä huolehtii järjestelmän ylläpidosta jatkossakin. Kunta vastaa omalta osaltaan kunnan verkon ylläpidosta, jotta järjestelmään liitetyistä kohteista saadaan katkeamattomasti olosuhteista kertovat tarvittavat tiedot automaatiojärjestelmään.

Automaatiojärjestelmään on liitetty yhteensä yli viisikymmentä erilaista rakennusta, kuten perusopetuksen, varhaiskasvatuksen ja terveydenhuollon kiinteistöjä sekä kunnantalo. Järjestelmän etäkäytön avulla kohteiden olosuhteista vastaavien huoltohenkilöiden on mahdollista tarkkailla ja osittain myös parantaa kohteiden olosuhteita etäyhteyden välityksellä käymättä kohteessa fyysisesti paikan päällä.

Tämän opinnäytetyön tavoitteena on päivittää rakennusautomaatiojärjestelmä ja siirtää se tietokoneelta konesalissa sijaitsevalle serverikoneelle. Työn toisena tavoitteena on

oppia hahmottamaan järjestelmän päivitystyön kokonaisuus. Tähän kuuluvat muun muassa järjestelmäsaneerauksen tarvittavat työtunnit ja tehtävät, kustannukset sekä tarpeet asiakkaan ja tilaajan näkökulmista.

Insinöörityön alussa käsitellään rakennusautomaatiota, -järjestelmiä, pilvipalvelua ja tietoturvaa yleisellä tasolla. Tämän jälkeen käydään läpi asiakkaan näkökulmia, järjestelmän lähtötilannetta sekä itse päivitystyö alusta käyttöönottoon saakka.

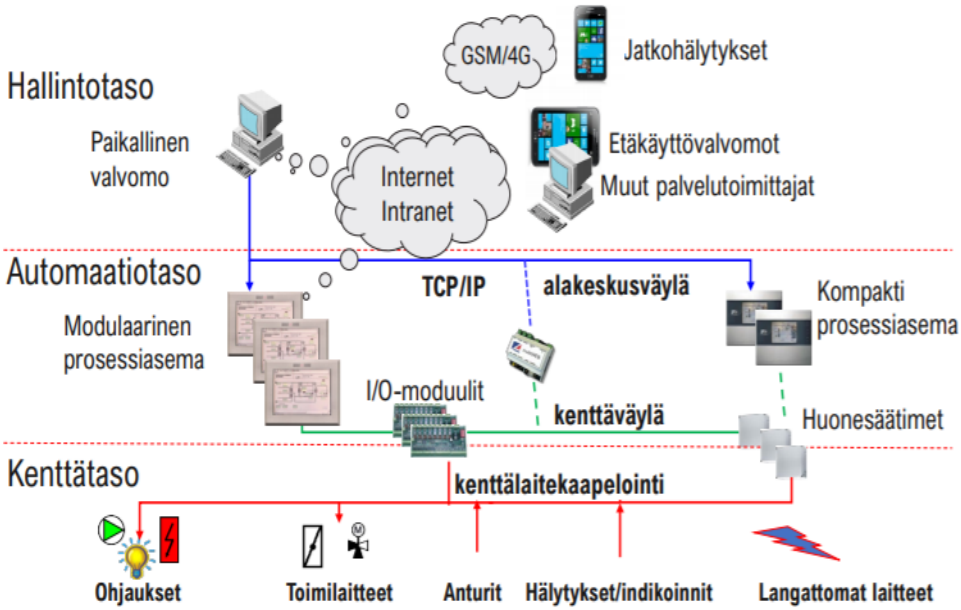
Päivityksen kannustimena on järjestelmässä olevien tietojen nopeampi päivittäminen ilman käyttökatkoja, järjestelmän etäkäyttäminen laitteesta riippumatta, tietoturvan huomattava parantuminen sekä käyttövarmuuden ylläpitäminen.

2 Rakennusautomaatio

Rakennusautomaatiolla (RAU) tarkoitetaan talotekniikan järjestelmien automaattista ohjausta. Siihen liitetään yleensä vähintään kiinteistön lämmitys- ja ilmanvaihtojärjestelmät. [2, s. 9.] Järjestelmän avulla hallitaan monesti kulunvalvontaa ja valaistusta [3]. Hyvin usein rakennusautomaation avulla mitataan ja säädetään myös jäähdytysjärjestelmän toimintaa sekä välitetään edellä mainittujen järjestelmien aiheuttamat hälytykset eteenpäin. Edellä mainittujen järjestelmien mittaamisen ja hallitsemisen kautta rakennusten energiatehokkuus paranee ja käyttöikä kasvaa. Rakennusautomaatiosta käytetään myös synonyymia kiinteistöautomaatio. [2, s. 9.]

2.1 Rakennusautomaatiojärjestelmien hierarkkinen rakenne ja tiedonkulku

Rakennusautomaation ohjauksessa olevien LVIS (lämpö-, vesijohto-, ilmanvaihto- ja sähkötekniikka) -tekniikkojen avulla on mahdollista saada merkittäviä hyötyjä ilmanvaihdon parantuessa sekä veden ja sähkön kulutuksen pienentyessä. Rakennusautomaatiojärjestelmän ja siihen liitettyjen laitteiden säännöllinen ja oikea-aikainen huolto on tärkeässä osassa, jotta kaikki laitteet toimivat halutulla tavalla. [2, s. 9.]



Kuva 1. Tyypillisen rakennusautomaatiojärjestelmän hierarkiarakenne [1, s. 60].

Yllä olevassa Kuvassa 1 on esitetty tyypillisten rakennusautomaatiojärjestelmän hierarkkiset rakennetasot, jotka ovat hallinto-, valvontajärjestelmän automaatio- ja kenttälaitetaso. Rakenne kehitettiin keskitettyjen järjestelmien aikana, ja älyn hajauduttua yhä enemmän eri laitteisiin rakenteen rajat ovat hälventyneet. Tasojen välillä on aina jokin ratkaisu tiedonsiirtoon. [1, s. 59.]

Hallintotasoon kuuluvat mahdolliset paikallis- ja etäkäyttövalvomot. Tason tehtävänä on toimia rajapintana järjestelmän ja käyttäjän välillä. Käyttäjärajapinta tarkoittaa paikallista PC:llä tai etänä olevaa valvomoa, josta käyttäjä voi tarkistaa kiinteistön järjestelmistä tulleet hälytykset, katsoa prosesseja kuvaavia grafiikoita, muokata asetusarvoja sekä tarkastella raportteja. Näitä tietoja analysoinnissa hyödyntämällä kiinteistöjen energiankäyttöä ja olosuhteita voidaan optimoida. Valvomoon liitettyjen kohteiden taloteknisten järjestelmien aiheuttamat hälytykset välitetään valvomosta eteenpäin huoltohenkilöille sähköpostien tai tekstiviestien avulla. Päivystävät huoltohenkilöt vastaanottavat hälytyksiä ympäri vuorokauden ja voivat ratkaista ongelmia etäkäytön avulla tai tiedon saatuaan lähteä paikan päälle kohteeseen. On erittäin tärkeää suunnitella ja toteuttaa etävalvonta niin, että valvomoa voidaan käyttää päätelaitealustasta riippumatta selaimella. [1, s. 59-60, 66-67.]

Kommunikaatio tällä tasolla perustuu pakettipohjaiseen Ethernet-väylään, ja etävalvonnassa hyödynnetään laajakaistayhteyksiä, jotka pohjautuvat TCP/IP (Transmission Control Protocol/Internet Protocol) -protokollaan. Etävalvontaan saavutetaan joustavuutta avoimilla tiedonsiirtoratkaisuilla, joka toisaalta asettaa tietoturvahaasteita. Pääosin tiedonsiirto-ongelmia on vain vähän ja mahdollisten ongelmien vaikutukset rajautuvat valvomoon. Itsenäiset alakeskukset ja säätimet jatkavat prosessien ohjauksia sekä säätöjä valvomon tiedonsiirto-ongelmista huolimatta. [1, s. 60.]

Alakeskukset ja niissä sijaitsevat I/O (Input/Output) -moduulit kuuluvat automaatiotasoon. Moduulien I/O-pisteisiin kytkettyjä kenttälaitteita ohjaavat ohjelmat sijaitsevat alakeskuksissa. Yleensä alakeskusten välillä ja niistä valvomoon tapahtuva kommunikaatio perustuu LAN (Local Area Network) -verkkoon ja TCP/IP-protokollaan. Esimerkiksi yhtä ulkovalovoimakkuuden anturia tai lämpötila-anturinlukemaa hyödynnetään useissa alakeskuksissa. Paikallisverkko on kaapeloitu standardien mukaisesti CAT-6-kaapelilla. Langatonta verkkoa (WLAN, Wireless Local Area Network) hyödynnetään myös tiedonsiirtoon. [1, s. 60-61.]

Anturit ja toimilaitteet, huonesäätimet ja toisiin laitteisiin integroidut säätimet muodostavat kenttälaitetason. Anturien avulla saadaan ajantasaista tietoa esimerkiksi prosessien, kuten ilmanvaihtokoneen lämpötiloista ja ilmavirran nopeudesta tai kiinteistön huoneiden lämpötiloista. Alakeskuksissa sijaitsevat ohjelmat lukevat antureiden arvoja ja vertaavat niitä ennalta-asetettuihin tavoitteisiin sekä ohjaavat toimilaitteita toimimaan tavoitteiden saavuttamiseksi. Myös hajautettua I/O:ta voidaan sijoittaa kentälle, mikä tarkoittaa alakeskuksen väylän avulla kommunikoivia I/O-moduuleja. Kentällä voi olla myös itsenäisesti toimivia huonesäätimiä tai pakettiratkaisuja, joihin on integroitu oma säädin, kuten IV (ilmanvaihto) -kone- ja lämmönvaihdinpaketeissa. [1, s. 61, 103-104.]

Taajuusmuuttajilla ohjatut pumput ja puhaltimet sisältävät omat ohjauslogiikkansa, jotka välittävät ja vastaanottavat tietoa alakeskukselle. Kommunikointi tapahtuu kenttäväylän avulla alakeskusten, hajautetun I/O:n ja säätimien välillä. Kenttäväylien, anturien, toimilaitteiden ja säätimien kytkentä alakeskuksiin toteutetaan suojatulla NOMAK- tai JAMAK-2x2x0,5+0,5 ja MMJ 3x1,5 S -kaapeleilla. [1, s. 61, 103-104.]

Kenttäväylät ovat standardisoituja ja tunnetuimpia niistä ovat ModBus, M-Bus, KNX, BACnet, LON ja DALI. Väylä valitaan sen mukaan, mitkä sovellukset ja laitteet on kohteeseen valittu. Sovelluksia ja laitteita ovat esimerkiksi kylmiöiden ohjauskeskukset, väyläohjatut pumput, ilmanvaihtokoneet sekä vedenjäähdytyskojeikot. [1, s. 61, 103-104.] Seuraavana on esitelty tarkemmin tunnetuimmat kenttäväylästandardit.

ModBus-tietoliikenneprotokollaa käytetään laajasti liitettäessä laitteita automaatiojärjestelmiin. Se on avoimen lähdekoodin protokolla, jota hyödyntää lähes kaikki LVIA-alojen yritykset. Protokolla perustuu perinteiseen master-slave (isäntä-orja) -ratkaisuun. Laitteet tallentavat analogiset arvot ja binääriarvot rekistereihin, joista ne luetaan valvomoon. [5.]

M-Bus eli Meter-Bus-protokolla on kustannustehokas kenttäväyläratkaisu, joka on suunniteltu mittaustietojen siirtämiseen. Tämän takia väylä ei sovellu suoraan sovellu hälytysten lähettämiseen, vaan hälytystiedot muutetaan rakennusautomaatiojärjestelmissä hälytyksiksi. [6, s. 3.]

KNX on avoin maailmanlaajuisessa käytössä oleva rakennusautomaatiostandardi sähköisten toimintojen ohjaukseen. Sen avulla on mahdollista yhdistää satojen laitevalmistajien tuotteita yhteiseksi kokonaisuudeksi. Hyväksytyt ja testatut tuotteet tunnistetaan KNK-logosta. KNX täyttää EN50090- sekä ISO/IEC14543-standardien vaatimukset. [7.]

BACnet eli Building Automation and Control networks on valmistajasta ja raudasta riippumaton dynaaminen protokolla. Se tarjoaa ratkaisun, jonka avulla eri laitevalmistajien laitteet ja järjestelmät sekä valvomot voidaan liittää yhteen. BACnet ei ole kenttäväylä, vaan se on kommunikointiprotokolla. [8.]

LonWorks eli Local Operating Network (paikallinen toimintaverkko) on protokolla, jonka avulla monenlaiset ohjauslaitteet, kuten toimilaitteet ja anturit, voivat kommunikoida keskenään yhteisen yhteyskäytännön avulla. [9.]

DALI eli Digital Addressable Lightning Interface on digitaalinen ohjausväylä, jonka avulla tietoa siirretään esimerkiksi valaistuksien sekä niitä ohjaavien laitteiden ja liiketunnistimien välillä. [10.]

2.2 Automaation fyysiset I/O-pistetyypit

Kentällä olevat laitteet liitetään alakeskuksissa sijaitseviin I/O-moduuleihin, kuten kuvassa 2 olevaan DI-16-moduuliin. Liityntäpisteitä on olemassa kahdenlaisia: fyysisiä ja ohjelmallisia pisteitä. Jälkimmäisiä kutsutaan myös pehmopisteiksi, jotta ne erotetaan fyysistä pisteistä. Fyysisiä I/O-pistetyyppejä on neljä:

- DI-pisteet (Digital Input) eli digitaaliset tulopisteet, joiden avulla relekosketintietona saatavat hälytykset ja tilatiedot liitetään alakeskukseen [1, s. 72].

- DO-pisteet (Digital Output) eli digitaaliset lähdöt, joiden avulla ohjataan 24 V:n ja 230 V:n toimilaitteita ja konvektoreita [1, s. 73].

- AI-pisteet (Analog Input) eli analogiset tulopisteet. AI-pisteisiin liitetään NTC-vastusarvoantureita ja paineantureita, joista saadaan arvo 0-10V DC viestinä. [1, s. 73.]

- AO-pisteet (Analog Output) eli analogiset lähdöt. Niiden avulla ohjataan portaattomalla yleensä 0-10 V jänniteviestillä peltien ja venttiilien toimilaitteita. [1, s. 74.]

Kuva 2. Fidelix DI-16-moduuli [11].

2.3 Tietoturvallisuus automaatiojärjestelmissä

Tieturvan merkitys on korostunut viime vuosina entisestään, kun verkossa olevien laitteiden määrä sekä pilvipalveluiden ja järjestelmien etäkäyttö on kasvanut. Julkisessa internetissä toimiessa tietoturva-asiat korostuvat verrattuna vain paikallisesti käytettäviin järjestelmiin. Valvomo- ja rakennusautomaatiojärjestelmät voivat altistua ympäri maailmaa tuleville hyökkäyksille, mikäli niitä ei suojata riittävästi. [4, s. 117.]

Tietoturva voidaan esittää C-I-A-mallilla, joka tulee sanoista confidence, integrity ja availability. Suomennettu versio on L-E-S (luottamuksellisuus, eheys ja saatavuus) -

malli. Luottamuksellisuus ylläpidetään pitämällä tietojen käsittelyoikeus vain ennalta määritetyillä henkilöillä. [4, s. 117.]

Eheys tarkoittaa tallennettujen tietojen säilymistä tarkoituksenmukaisesti. Tiedon eheys vaarantuu, jos ei-toivottu henkilö pääsee muokkaamaan anturitietoja tai saattamaan järjestelmän muille laitteille tai ihmisille vaaralliseen tilaan. [4, s. 117.]

Saatavuudella tarkoitetaan rakennusautomaatiojärjestelmissä olevien tietojen saavutettavuutta tarvittaessa niille tahoille ja henkilöille, joille on annettu oikeudet. Jos laitteiden ja valvomon välinen kommunikaatio häiriintyy ja tietoja jää siirtymättä, saavutettavuus vaarantuu. Palvelunestohyökkäyksillä yritetään vaarantaa saatavuutta lähettämällä niin paljon sanomia, ettei niitä järjestelmä pysty enää käsittelemään ja käyttö estyy. Saavutettavuus voi vaarantua myös, mikäli valvomokoneen kovalevy hajoaa. Myös tahattomat toimet aiheuttavat tietoturvariskejä. Tällaisia ovat esimerkiksi tietojen käsittelyoikeuksien omaavien henkilöiden liikkuminen kalasteluyrityksiä sisältävillä internetsivuilla tai vapaa-ajalla käytössä olevien salaamattomien USB-tikkujen käyttäminen työajalla. [4, s. 117.]

Rakennusautomaation tietoturvallisuus ja kyberturvallisuus kulkevat käsi kädessä. On hyvin tärkeää suojautua järjestelmään tunkeutumisyrityksiltä, jotta esimerkiksi kiinteistöjen ilmanvaihtoon tai lämmitykseen ei pystytä vaikuttamaan. Tietoturvaa ja suojattavien tietojen tasoja mietittäessä tehdään usein riskianalyysi. Siinä käydään läpi ulkoisten ja sisäisten riskitekijöiden todennäköisyyttä ja vaikutuksia riskien konkretisoituessa. On hyvä ottaa huomioon esimerkiksi valvomojärjestelmän tai siihen liitettyjen laitteiden rikkoontumiset, tietoverkkojen kautta tulevat tunkeutumisyritykset, järjestelmässä olevien tietojen päätyminen väärin käsiin ja mahdolliset sähkökatkot. [4, s. 118.]

Yksi suurimmista riskeistä automaatiojärjestelmien tietoturvassa konkretisoituisi, jos suora liikenne avoimesta internetistä laitteisiin avautuisi. Järjestelmiä ei yleensä ole tarkoitettu suoraan internetiin kytkettäväksi, koska vähäiselläkin IT-osaamisella laitteisiin tunkeutuminen voi olla helppoa. Siksi internetyhteydet tulee toteuttaa aina esimerkiksi VPN (Virtual Private Network) -yhteydellä, joka on tietoturvallinen ratkaisu. VPN:llä eli virtuaalisella erillisverkolla voidaan muodostaa julkisen verkon yli näennäisesti yksityinen verkko, jonka avulla voidaan yhdistää yrityksen verkkoja. Yhteys käyttäjän ja VPN-palvelimen yli salataan erityisillä avaimilla. Tietoliikenne liikkuu salattuna yhteyden luomisen jälkeen. [4, s. 119.]

2.4 Järjestelmien suojaaminen fyysisesti ja käyttöoikeuksien avulla

Tietoturvallinen rakennusautomaatiojärjestelmien suojaaminen käsittää myös niiden fyysisen suojaamisen. Valvomo, alakeskukset, verkon aktiivilaitteet ja ristikytkennät, verkkoliitynnät ja -pisteet on korostetun tärkeää sijoittaa lukittuihin tiloihin, joihin on vain valvotusti ja tietyille henkilöille rajattu pääsy. Esimerkiksi valvomon ja verkossa olevien laitteiden sijoittaminen julkiseen tilaan, kuten kauppakeskusten aulaan ei ole suotavaa. Joskus voi tulla kuitenkin sellainen tilanne, että on tarve sijoittaa jäähdytyksen tai valaistuksen ohjauspaneeli avoimeen tilaan. Tällaisissa tilanteissa kyseinen verkkopiste eristetään talotekniikkaverkosta tai käytetään laitekohtaista tunnistautumista. [4, s. 120.]

Automaatiojärjestelmiä suojataan myös käyttöoikeuksien avulla. Järjestelmiin luodaan eritasoisia oikeuksia, joilla on laajuudeltaan erilaiset käyttöoikeudet. Yleensä järjestelmissä on vähintään pääkäyttäjä, jolla on täydet oikeudet käyttää järjestelmää ja lisätä sekä poistaa käyttäjiä ja heidän järjestelmänkäyttöoikeuksia. Kohteista riippuen voi olla käyttöoikeustarpeita kiinteistöjen omilla tai ulkopuolisilla huoltohenkilöillä, työmaanaikaisilla urakoitsijoilla ja energia-asiantuntijoilla. Koska käyttäjiä voi olla hyvinkin paljon, on erityisen tärkeää, että on jatkuvasti tiedossa, ketkä järjestelmiä käyttävät. Jokaisella käyttäjällä on oma henkilökohtainen tunnus ja salasana. Niiden huolellinen säilyttäminen ja salassa pitäminen sekä salasanan vaihtaminen säännöllisesti vaikeuttaa tunkeutujien esiintymistä luvallisena henkilönä. Tunnukset voivat kuitenkin päätyä inhimillisenkin erehdyksen kautta vääriin käsiin. Tämän takia monissa rakennusautomaatiojärjestelmissäkin on otettu käyttöön kaksivaiheinen tunnistautuminen. Siinä tunnuksen ja salasanan syöttämisen jälkeen henkilöllisyys tunnistetaan esimerkiksi lähettämällä ennalta määrättyyn puhelinnumeroon tekstiviesti, joka syötetään järjestelmään. [4, s. 122.]

3 Konesalin merkitys automaatiojärjestelmän taustalla ja TOSIBOX®

Useita kiinteistöjä hallinnoivat tahot haluavat usein keskittää kiinteistöjen valvonnan ja parantaa sitä kautta kustannustehokkuutta. Tällainen tilanne on esimerkiksi huoltoyhtiöillä, kaupungeilla ja kunnilla. Kiinteistöjen teknisten järjestelmien etävalvonta keskitetään keskusvalvomoon. Se voi sijaita fyysisesti tietokoneella huoltoyhtiön tai kaupungin tiloissa. Yksittäisten kiinteistön omistajat voivat ostaa myös keskitettyjä valvomopalveluita. Niitä tarjoavat monet kiinteistö- ja automaatiopalveluita tuottavat yritykset. Palvelun avulla saadaan parempaa asiantuntemusta kiinteistöjen ylläpitoon ja ongelmatilanteiden ratkaisuihin. [1, s. 66-67.]

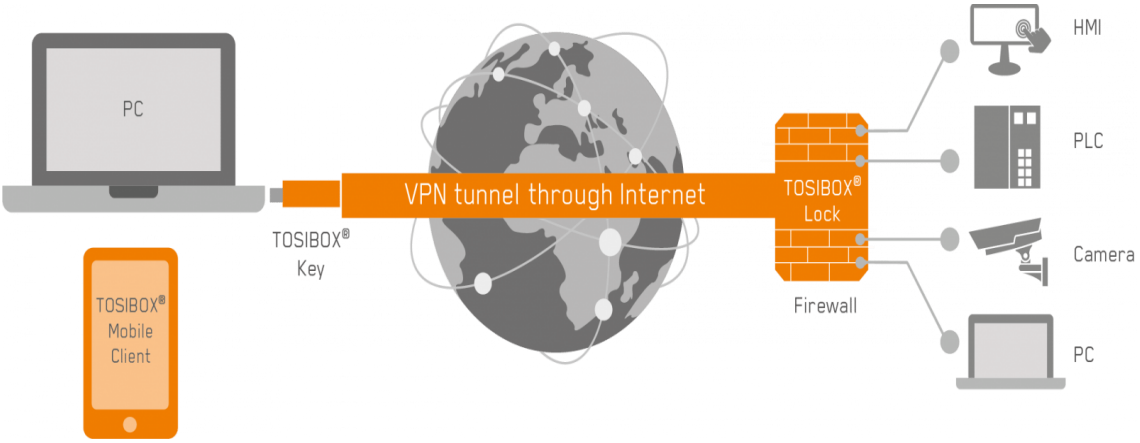
Valvomojärjestelmä voidaan hankkia myös ohjelmistoresurssipalvelun (SaaS, Software as a Service) avulla tuotettuna pilvivalvomona. Tällöin järjestelmä pyörii palvelun tarjoajan tai sen yhteistyökumppanin konesalissa. [1, s. 66-67.] Ne ovat hyvin suojattuja tiloja, joiden ovia sekä kulkureittejä valvotaan ja kulkuoikeuksia annetaan vain tarvittaville henkilöille. Saleihin on myös varmistettu sähkönsyötön katkeamattomuus ja jäähdytyksen toiminta kaikissa tilanteissa. Sähkönsyöttöä ja tehokasta jäähdytystä tarvitaan konesaleissa sijaitsevien isoja datamääriä käsittelevien tietokoneiden ja tarvittavien oheislaitteiden ympärivuorokautisen toiminnan turvaamiseksi. [12.] Konesalissa olevan pilvivalvomon käyttäjällä on käytettävissään täydet valvomotoiminnot, mutta palveluntarjoaja vastaa valvomolaitteista, -ohjelmistoista sekä -järjestelmän ylläpidosta. [1, s. 66.]

3.1 Yhteydet alakeskuksista konesaliin

Yhteydet alakeskuksista konesaliin hoidetaan internetin, asiakkaan paikallisverkon tai esimerkiksi 3G/4G-modeemien avulla. Yhteyksiä alakeskuksista konesaliin voidaan tehdä myös mobiilipohjaisen yhdyskäytävän eli APN:n (Access Point Name) avulla. Sen tehtävänä on yhdistää mobiiliverkko ja tietokoneverkko julkisessa internetissä. Operaattorit myyvät suljettuja APN-verkkoja ja yhteyksiä. Kohteessa on tämänlaisessa tapauksessa kyseiseen APN:ään omistettu SIM (Subscriber Identity Module) -kortti, joka laitetaan reitittimeen, jolloin tieto pääsee alakeskuksilta liikkumaan APN:n kautta. APN-verkon sisällä kyseiseen laitteeseen ei muualta pääse kuin kyseisestä APN:stä. Tieto APN-verkoissa liikkuu eriteltynä samoissa tietoliikennemastoissa muun tietoliikenteen kanssa.

3.2 Yhteyksien muodostaminen TOSIBOX®-tuotteiden avulla

Yksi tapa muodostaa suojattuja yhteyksiä asiakkaan paikallisverkon ja konesalin välille on hyödyntää TOSIBOX®-tuotteita. TOSIBOX® luo patentoidun etäyhteysteknologian avulla VPN-tunnelin laitteiden välille. Ratkaisussa hyödynnetään modulaarisia komponentteja, jotka ovat yhteensopivia keskenään sekä laitteista, operaattorista ja verkkoyhteyksistä riippumattomia. Käytettävien komponenttien avulla saavutetaan joustavuus ja rajaton laajennettavuus. Ratkaisua voidaan hyödyntää sekä sisäisessä että ulkoisessa verkossa niin modernien kuin iäkkäämpienkin järjestelmien kanssa. [13.]

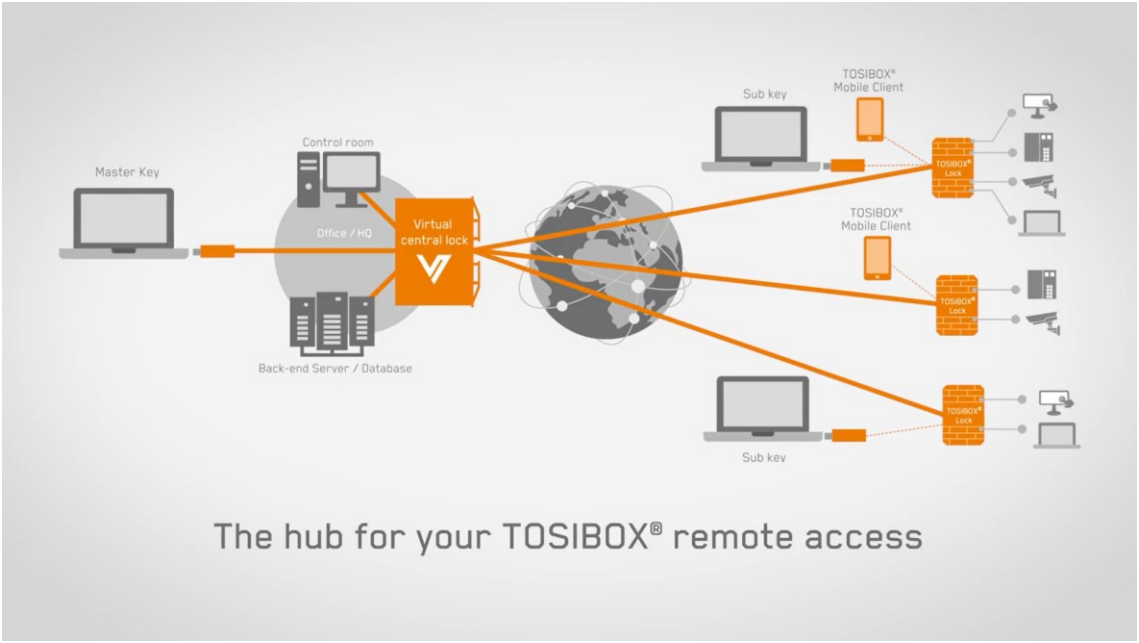


Kuva 3. TOSIBOX®-toimintaperiaate [13].

Yhteyden muodostamiseen tarvitaan TOSIBOX®-lukko, verkkoyhteys ja TOSIBOX®-avain kuvan 2 mukaisesti. TOSIBOX®-lukko on palomuurin sisältävä reititin, jonka avulla pääsy laitteisiin avautuu. Lukkoja on sekä fyysisiä että virtuaalisia eli Lukko, joka on laitteen sisään asennettu ohjelmisto. TOSIBOX®-verkkolaiteavainta käytetään verkkoon kirjautumiseen. Avaimia on kahdenlaisia: USB-porttiin laitettava fyysinen salausavain sekä ohjelmallinen TOSIBOX® Softkey. TOSIBOX® MatchMaker -taustapalvelu auttaa käyttäjiä löytämään lukot, joihin heidän avaimillaan on pääsyoikeudet. [13.]

Kuva 4. Fyysinen TOSIBOX® Lukko 200 [13].

Kuvassa 3 oleva TOSIBOX® Lukko 200 on älykäs reititin, joka toimii yhteyksien päätepisteenä. Lukkoon liitetään halutut laitteet ja niihin päästään kiinni salatulla VPN-yhteydellä. [13.]



Kuva 5. Virtuaalisen TOSIBOX®-keskuslukon toimintaperiaate [13].

TOSIBOX® Virtual Central Lock on VPN-yhteyksien keskitin, joka kokoaa halutut etäyhteydet yhteen paikkaan kuvan 4 esittämällä tavalla. Tästä paikasta voidaan reaaliajassa hallita verkon käyttäjiä ja heidän käyttöoikeuksiaan. [13.]

Kuva 6. Fyysinen TOSIBOX®-Avain sekä ohjelmallinen TOSIBOX® SoftKey[13].

Kuvassa 5 ovat TOSIBOX®-avaimet. Fyysisen TOSIBOX®-salausavaimen avulla muodostetaan yhteys TOSIBOX®-lukkojen ja tietokoneen välille, minkä avulla voidaan hallita lukkoon liitettyjä verkkolaitteita. TOSIBOX® SoftKeyn toimintaperiaate on sama kuin fyysisellä avaimella, mutta se asennetaan haluttuun tietokoneeseen. Kun Softkey on kerran asennettu, sitä ei voida enää kopioida tai siirtää toiseen tietokoneeseen, vaan tietokoneen rikkoutuessa on hankittava uusi avain. [13.]

4 Automaatiojärjestelmän päivitystyön eteneminen

Tässä luvussa käsitellään rakennusautomaatiojärjestelmäpäivityksen sopimuksen syntymistä ja itse päivitystyön etenemistä. Päivitystyö eteni koneympäristön perustamisesta yhteyksien luomiseen asiakkaan automaatiojärjestelmäverkosta konesaliin. Tämän jälkeen vanhasta valvomosta siirrettiin vanhan valvomojärjestelmäversion varmuuskopio konesalissa olevalle koneelle. Luvun lopussa avataan järjestelmän etäkäyttöä, hälytysten siirtymistä valvomosta huoltohenkilöille sekä käyttöönottoa.

4.1 Asiakkaan näkökulma

Sopimusta päivitystyöstä aloitettiin laatimaan jo hyvissä ajoin ennen varsinaisen työn aloitusta. Asiakas arvosti sopimusta laadittaessa muun muassa sitä, että palvelun mahdollisista käyttökatkoista tulevat sanktiot ja hyvitykset. Ne pohjautuvat sopimuksessa olleeseen SLA (Service Level Agreement) -liitteeseen. Se tarkoittaa asiakkaan sekä palveluntarjoajan välistä palvelutasosopimusta. Siinä määritellään kyseisen palvelun vaatimustasot ja erityyppiset mittarit palvelun toimivuuden seuraamiseksi sekä sanktiot tilanteisiin, jossa palvelu ei vastaa sovittua. Palveluntarjoajan eli Caverion Suomi Oy:n vastuulla on tarjota toimiva palvelu sekä seurattava ja raportoitava, mikäli palvelu ei toimi odotusten mukaisesti. [14; 15.]

Asiakkaalle oli myös tärkeää, että sopimuksessa on selkeästi ja ymmärrettävästi esitetty palvelukuvaus. Siinä kerrotaan, mitä palvelua ollaan ostamassa ja mitä palvelu pitää sisällään sekä mitkä asiat kuuluvat hintaan. Asiakas myös korosti palvelukuvauksen selkeyden tärkeyttä varsinkin pitkien sopimuksien yhteydessä, koska palvelut voivat olla asiakkaalla käytössä vuosiakin ja kyseisen sopimuksen tehneet henkilöt ovat saattaneet vaihtaa eri yritykseen ennen sopimuksen voimassaolon päättymistä. Tämä tarkoittaakin sitä, että käytännössä muidenkin kuin vain sovittuun asiaan perehtyneiden tulisi ymmärtää sopimuksen sisältö ja sovitut asiat. [14; 15.]

Työn tilaajan ollessa kunta on sopimusta laadittaessa otettava huomioon myös JIT:it eli julkisen hallinnon IT-hankintojen sopimusehdot. Asiakkaan näkökulmasta sopimuksen tekoa helpottaa, kun JIT:it on lisätty ja otettu huomioon jo tarjouspyynnössä. JIT:it on valmiiksi neuvoteltu kuntien kanssa, ja ne turvaavat kunnan näkökulmasta hyvin kunnan etuja. Siinä on määritelty muun muassa, milloin ostettavan palvelun hintaa saa korottaa

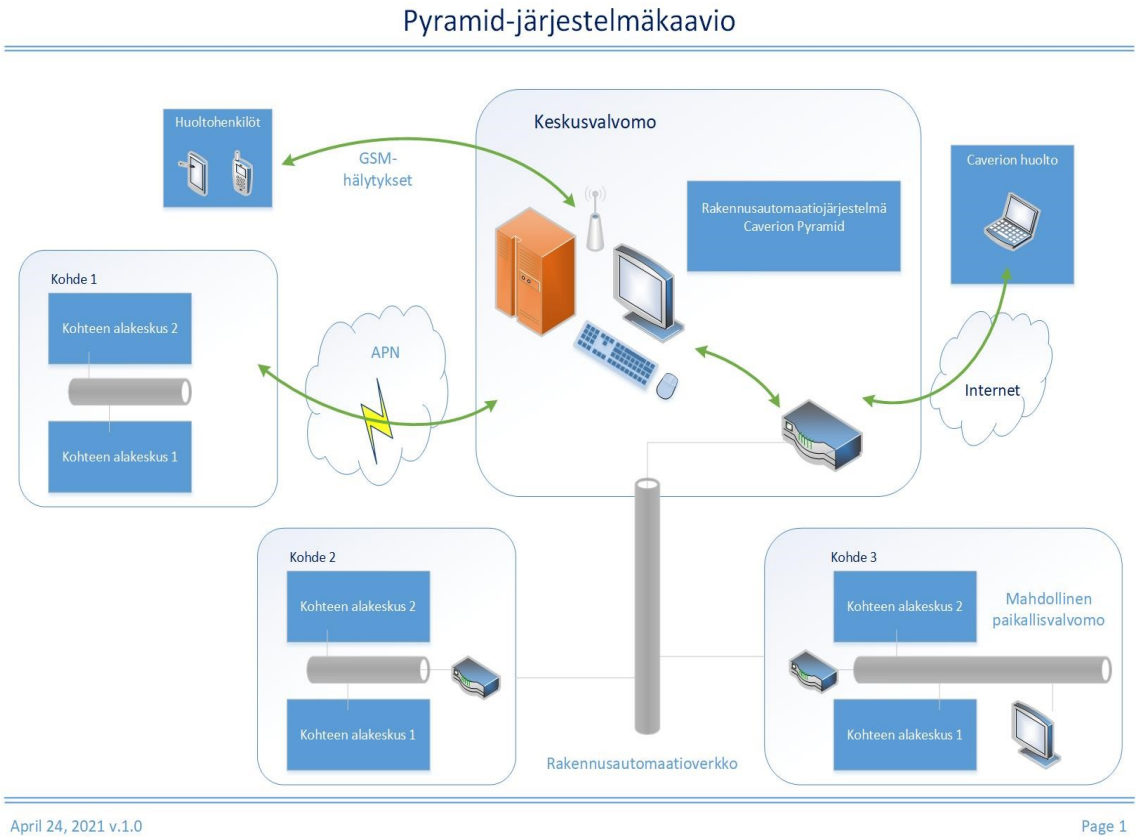
ja kuinka paljon. Mikäli kunta on ostamassa pelkkää palvelua, sopimus voi olla muotoa toistaiseksi voimassa oleva. Jos sopimus sisältää palvelun lisäksi myös laitehankintoja, asiakkaan näkökulmasta sopimuksen voimassaolon olisi tällöin hyvä olla laitteiden oletetun toimintakeston ajan. Kunnan näkökulmasta lyhyt irtisanomisaika on parempi ja mahdollistaa siten muiden markkinoilla olevien vastaavien palveluntarjoajin hintojen ja palveluiden kehittymisen seurannan. JIT:it määrittävät SaaS-palveluiden irtisanomisajan pituuden. Irtisanomisaika on kuusi kuukautta asiakkaalla ja 12 kuukautta toimittajalla sopimuksen allekirjoituksesta. [14; 15.]

Sopimuskeskusteluissa käytiin myös läpi tietoturvan merkitys. Molemmille oli selvää, että tietoliikenneyhteyksien tulee olla turvallisia ja datan varmistettua. Caverion vastaa omalta osaltaan tietoturvallisuudesta sekä kantaa kokonaisvastuun ostetun palvelun raudasta ja softasta sekä niiden ylläpistosta. [14; 15.]

4.2 Lähtötilanne

Asiakkaan automaatiojärjestelmä on ollut jo vuosia Caverionin toimittama Aveva Citect SCADA (myöhemmin pelkkä Citect) -ohjelmistoalustan päälle rakennettu Pyramid. Automaatiojärjestelmän viimeisin versio oli päivitystyötä aloittaessa 7.8. Citect-versio täytyy päivittää uudempaan versioon, koska edelliset eivät tue HTML5-kieltä. Tätä tarvitaan, jotta etäkäyttö selaimella alustasta riippuen on mahdollista.

Pyramid on pyörinyt asiakkaan tiloissa olevalla tietokoneella jo kahdeksan vuotta. Järjestelmän toimivuuden kannalta käyttöikänsä päässä ollut tietokone muodosti kasvavan uhkan. Tietokone on ollut avoimessa tilassa yhden lukitun oven takana, mikä on muodostanut tietoturvariskin. Edellä mainittujen riskin poistaminen olivat osa niistä eduista, jotka päivitystyön kautta saavutettiin.



Kuva 7. Asiakkaan rakennusautomaatiojärjestelmän periaatekuva

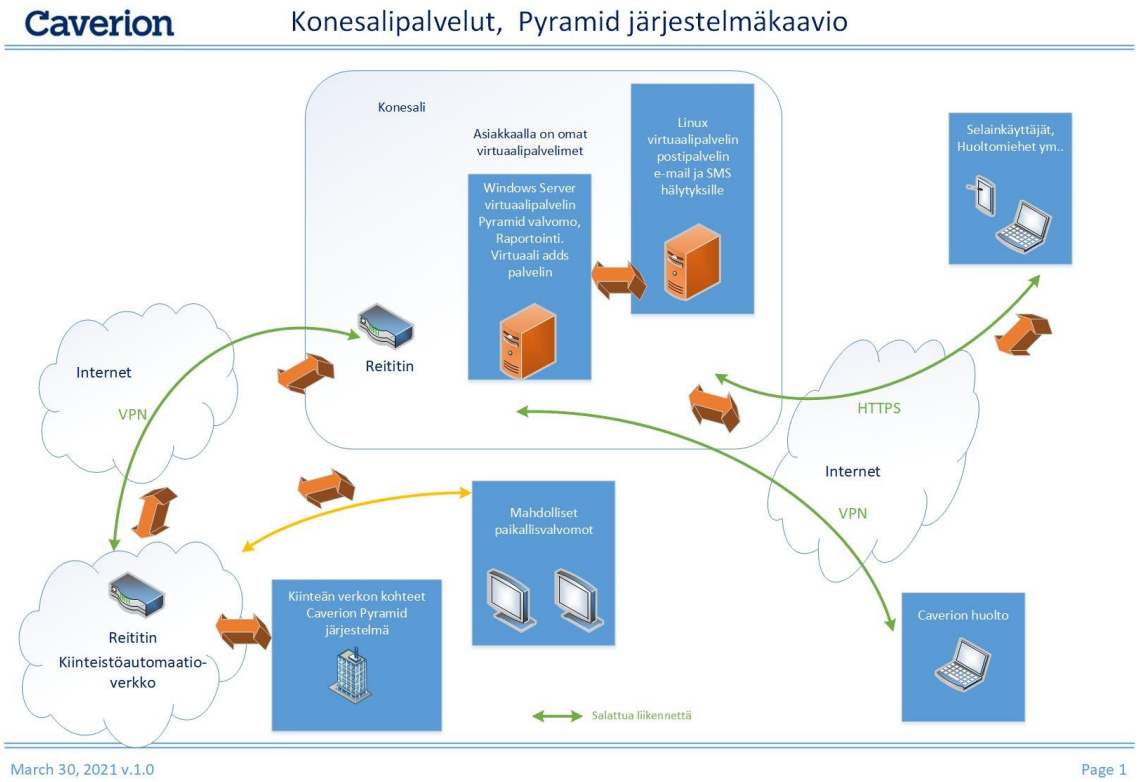
Yllä oleva Kuva 7 havainnollistaa asiakkaan rakennusautomaatioverkkoa ja tietojen liikkumista keskusvalvomon ja kohteiden välillä. Tiedot asiakkaan kiinteistöjen alakeskuksista Pyramid-järjestelmään liikkuvat asiakkaan verkon kautta. Kiinteistöissä on alakeskusten välillä Ethernet-kaapelointi ja tarvittavat kytkimet. Osa VAK:eista (valvontajärjestelmän alakeskus) on liitetty asiakkaan verkkoon mobiiliyhteyksien avulla. Näissä kohteissa alakeskukseen on sijoitettu SIM-kortilla varustettu WLAN-reititin. Kyseiset rakennukset sijaitsevat hieman kauempana muista kohteista, eikä niihin ole rakennettu esimerkiksi valokuituyhteyksiä. Jatkohälytykset vanhasta valvomosta huoltohenkilöille lähtivät valvomokoneen sarjaportissa olleen gsm-moduulin avulla.

Vanhassa valvomossa oli yksi käytettävyyttä alentava ominaisuus. Järjestelmä piti sammuttaa ja käynnistää uudelleen, kun oli tarve saada näkyviin grafiikoille järjestelmään tehdyt muutokset tai kun järjestelmästä otettiin varmuuskopioita. Tämä tietysti tarkoitti sitä, ettei uudelleen käynnistyksen aikana käyttäjät pystyneet ohjelmaa käyttämään. Ominaisuus johtui siitä, että etäkäyttö oli rakennettu WebClientin avulla. Käynnistyessään se siirtää itselleen muuttumatonta dataa, joita ovat esimerkiksi grafiikkakuvat, eikä

se käy kysymässä palvelimelta dataa enää uudestaan muuten kuin seuraavan käynnistyksen yhteydessä. Etäkäytön toiminnallisuus perustuu ActiveX-sovelluskomponenttiin, jonka tuki löytyy käytännössä vain Microsoftin Internet Explorer -selaimesta. Tämän takia etäkäyttö rajautui Internet Explorer -selaimeen. [16.]

4.3 Järjestelmäkaavio

Alla olevan Kuvan 8 järjestelmäkaaviossa on kuvattu Caverionin konesalin ja asiakkaan kohteiden sekä konesalin ja käyttäjien välisiä yhteyksiä. Niitä tarvitaan, jotta tiedot toimilaitteilta liikkuu alakeskuksiin ja eteenpäin rakennusautomaatioverkkoa pitkin konesaliin. Yhteyksiä tarvitaan myös konesalin ja käyttäjien välillä ja niitä voivat olla esimerkiksi asiakkaan huoltohenkilöt sekä Caverionin työntekijät. Yhteyksien mahdollistamiseksi tarvitaan muun muassa reitittimiä, suojattuja yhteysmuotoja, kuten VPN, sekä Ethernet-kaapelointia. Kohteita voidaan liittää kiinteistöautomaatioverkkoon myös APN:n eli mobiiliyhteyksien avulla.



Kuva 8. Caverionin konesalipalvelut ja erilaiset yhteydet konesaliin [17].

4.4 Päivitystyön aloitus

Päivitystyö aloitettiin taustalla samaan aikaan vanhan valvomon toimiessa alkuperäisenä päivitystyön loppuun saakka. Caverionin konesaliin perustettiin koneympäristö. Konesalikäytöllä oleva Pyramid-Citect Anywhere -ohjelmisto vaatii, että Pyramidia pyörittävä kone on domainissa. Tämä tarkoittaa sitä, että koneella on IP-osoitteen lisäksi verkkotunnus eli domain. Tämän takia konesaliin piti luoda toinenkin kone, jotta siitä saadaan asiakkaan oma ADDS (Active Direcory Domain Services) -ympäristö eli domain-ympäristö. [16.]

Citect Anywhere (myöhemmin pelkkä Anywhere) on ohjelma, joka käyttää hyödykseen Microsoftin palveluita pystyäkseen näyttämään selainikkunassa jotain sovellusta. Tässä projektissa näytettävä sovellus on Pyramid-rakennusautomaatiovalvomo. Anywhere-ohjelma itsessään mahdollistaa serverin päässä sen, että moni eri henkilö voi käyttää Citect Pyramidia samaan aikaan eli käyttäjäistuntoja voi olla useampia.

Microsoftin RDS (Remote Desktop Services) -palvelu muodostaa linkin selaimen ja Anywhere-Pyramid-paketin välille. RDS on komponentti, jonka avulla verkkoyhteyden kautta voidaan hallita etä- ja virtuaalikoneita. Anywhere-kirjautuminen on käytännössä Microsoftin Windows -kirjautumista ja -tunnistautumista. Anywhere siirtää kirjautumistiedon Microsoftin kirjautumisiin. [16.]

4.5 Koneympäristön perustaminen

Caverionilla on virtuaaliympäristössään valmis mallipohja (engl. Template). Sitä monistamalla saatiin luotua tarvittavat koneet virtuaaliympäristöön. Ennen kuin mallipohjaa aletaan monistamaan, siihen tehdään tarvittavat Microsoft Windows -järjestelmäpäivitykset. Mallipohjien avulla koneiden luonti nopeutuu, kun jokaista vaihetta ei tarvitse tehdä alussa uusiksi. Virtuaalikoneelle määritellään mallipohjan monistamisen jälkeen resurssit. Niitä ovat esimerkiksi prosessorien määrä, muistin ja kiintolevyjen koko sekä verkkosovittimet. Koneelle määritellään myös verkko, johon se liitetään. Kun kone on laitettu perusasetusten osalta valmiiksi tavallisen tietokoneen tapaan, siihen aletaan lisäämään niitä rooleja, joita se tarvitsee.

AD (Active Directory) -koneeseen asennettiin ADDS-palvelu. AD-koneen tehtävänä on tuottaa ADDS-palvelu. AD-konetta luodessa Microsoftin toimintatavasta johtuen ADDS-palvelu pitää ottaa erikseen käyttöön. AD-konetta varten voisi olla myös oma mallipohja, mutta siitä ei edellä mainitun käyttöönottotavan vuoksi saisi juurikaan ajansäästöä. ADDS-palvelun käyttöönottovaiheessa rakennetaan itse ympäristö. Kun ADDS-palvelu otetaan käyttöön, se liimautuu niin voimakkaasti siihen IP-osoitealueeseen, joka sille luontivaiheessa asetetaan. Kyseistä osoitealuetta ei pysty vaihtamaan muuten kuin tekemällä ADDS-palvelun käyttöönoton uudelleen. [16.]

Toinen tarvittava virtuaalikone oli Pyramid-palvelin. Mallipohjasta monistamisen ja resurssien asettamisen jälkeen tähän koneeseen asennettiin rakennusautomaation valvomo-ohjelma. Kone liitettiin siihen domainiin, jonka AD-kone on luonut valitulle verkkoalueelle.

Konesaliin luotu kolmas kone hyödyntää Linux-käyttöjärjestelmää. Tässä koneessa toimii HTTPS (Hypertext Transfer Protocol Secure) Proxy -palvelin. HTTPS on www-palvelinten ja selainten välisen liikenteen suojattu tiedonsiirtoprotokolla. Proxy-palvelimen tehtävänä on yhdistää ulkomaailman ja asiakkaan IP-osoitteet Pyramid-palvelimeen.

4.6 Yhteyksien luominen asiakkaan verkosta konesaliin

Seuraavaksi muodostettiin yhteys kunnan verkosta Caverionin konesaliin. Yhteyksiä voidaan rakentaa suojatusti esimerkiksi VPN- tai APN-yhteyksien avulla. Kunnan kohteiden IP-osoitealueet piti olla tiedossa, kun yhteyttä ja reitityksiä rakennettiin. Tämänlaiset yhteydet voidaan toteuttaa esimerkiksi TOSIBOX® Lukon avulla.

Asiakkaan verkkoon täytyi tehdä reititysmuutoksia, kun valitun yhteysmuodon reititin sijoitettiin eri paikkaan, missä vanha valvomo oli. Eli reititykset täytyi siirtää siihen verkkoalueeseen, johon reititin valittiin. Mikäli se olisi tullut samaan kiinteistöön, jossa vanha valvomo oli, ei näitä reititysmuutoksia olisi tarvinnut tehdä. Kyseisessä kiinteistössä oli siis jo reititykset alakeskuksiin olemassa molempiin suuntiin. Pääosin asiakkaan järjestelmässä valvomo kysyy vuoron perään alakeskuksilta esimerkiksi, onko jonkun tietyn alakeskuksen logiikalla joku tietty piste hälytyksessä. Kahden suuntaiselle liikenteelle on tarvetta, kun alakeskuksetkin voivat ilmoittaa valvomolle pisteiden hälytyksistä. Asiakkaan osa VAK:eista on liitetty asiakkaan verkkoon mobiiliyhteyksien avulla. Operaattoria

pyydettiin avaamaan yhteydet näiltä alakeskuksilta sen kiinteistöön verkkoon, johon valitun järjestelmän reititin sijoitettiin.

4.7 Varmuuskopion siirto vanhasta valvomosta

Valvomojärjestelmän varmuuskopio siirrettiin tietokoneelta konesaliin suojatun yhteyden kautta. Konesalin Windowsiin oli asennettu uusin Pyramid-ohjelman versio ja viimeisin Caverionin tuottama Pyramidin standardiprojekti, johon sisällytettiin varmuuskopiossa olleet asiakkaan kiinteistökohtaiset projektitiedostot. Niissä ovat esimerkiksi kiinteistöjen valvomografiikkakuvat, listaukset I/O-pisteistä ja tiedot IP-osoitteista.

Automaatiojärjestelmän versioiden päivittäminen aiheuttaa hyvin usein asioita, joita pitää käydä läpi ja muuttaa. Tämän tyylisten päivitysten yhteydessä on erinomainen mahdollisuus parantaa järjestelmän toimintaa entisestään. Varmuuskopion siirtämisen jälkeen alkoi vertailu, mitkä asiat toimivat nykystandardin kanssa ja mitkä vaativat muutoksia. Pyramid-ohjelman päivityksessä oli jonkun verran tekemistä, kun paikallinen vanhempi ohjelma asiakaskohtaisine toimintoineen päivitettiin uudempaan versioon. Yksi muutoksista oli valvomon grafiikkakuvien tiedostomuodon muuttaminen ”pro standardi” -muodoksi. Vanhaan versioon oli myös jäänyt historiatietoja. Mikäli niitä ei olisi siivottu pois, jotkut niistä eivät olisi haitanneet mitään, jotkut olisivat hidastaneet järjestelmää ja osasta olisi voinut tulla jopa suoranaista haittaa. Osa muutoksista tehtiin asetuksia muuttamalla ja osaan tarvitsi tehdä muutoksia Cicode-ohjelmointikielellä.

4.8 Konesalin ja julkisen internetin rajalla tunnistautuminen

Raja-aluetta konesalin ja julkisen internetin välillä voidaan kutsua DMZ (Demilitary Zone) -alueeksi. DMZ:n avulla pystytään tietty palvelin ja palvelu laittamaan sellaiseksi, ettei se ole suoraan internetissä eikä sisäverkossa. [16.]

Konesaliin on tehty käyttäjän pääsyjä varten HTTPS Proxy -palvelin. Se on Linux-pohjainen ohjelmisto, joka tekee itse kyseisen palvelimen. [16.]

Caverionilla on käytössään palvelu, jota käytetään konesalin ja julkisen internetin rajalla tunnistautumiseen. Sitä käytetään kirjautumisten määrän vähentämiseksi SSO (Single Sign On) -tyylisten palveluiden yhteydessä. Palvelun palvelin keskustelee konesalissa

olevan Proxyn kanssa ja sallii liikenteen avauksen kyseiselle palvelimelle. Tähän palveluun luotiin asiakaskohtainen nimiavaruus. Palvelun nimiavaruuden avulla määritellään mihin julkisella osoitteella kuljettaessa ohjaudutaan. Kuntaa varten tuli oma nimiavaruus, joka nimettiin asiakkaan yksilöivällä tavalla. Nimiavaruuden alle luotiin käyttäjät, jotka palvelua jatkossa käyttävät. Kyseinen nimiavaruus on linkitetty Pyramid-koneeseen.

4.9 Etäkäyttö ja CAL-lisenssit

Käytettäessä Anywhere-ohjelmaa kaikki istunnot ja sen lisäksi myös tarvittava ohjelmisto pyörivät yhdessä koneessa. Ohjelman etäkäytöllä käyttäjällä on siis pelkästään näkymä omalla koneellaan. Taustalla tehdyt muutokset tulevat edellistä valvomoa paremmin käyttöön, sillä ohjelma käyttää ja lukee jatkuvasti esimerkiksi kuvia sisältäviä tiedostoja. Nykyisessäkin järjestelmässä on asioita, jotka eivät päivity ilman, että järjestelmää joutuu käynnistämään uudelleen. Kaikesta huolimatta jatkossa on paljon enemmän asioita, jotka pystytään tekemään taustalla. Myös uudempi Citect-versio käsittelee edellistä versiotaan paremmin asioita, joita voi päivittää ilman käytettävyyden katkeamista.

Jokaiselle etäkäyttäjällä täytyy olla käytössään CAL (Client Accesses Licenses) -lisenssi, joiden määrä määrittelee, kuinka monta käyttää voi olla yhtä aikaa. Microsoft RDS -palvelun lisensointi vaatii CAL-lisenssien käytön. Serveriohjelmistot sisältävät RDP- (Remote Desktop Protocol) ja RDS-käyttöön kaksi lisenssiä itsessään. Lisenssejä tarvitaan lisää, kun käyttäjiä on enemmän kuin kaksi. Niitä voidaan ostaa esimerkiksi viiden lisenssin paketeissa. Kyseinen palvelu on käyttäjäpohjainen (engl. User). On olemassa myös laitepohjainen (engl. Device) lisenssi, jolloin jokainen lisenssi on sidottu yhteen tiettyyn koneeseen. Tietokoneen vaihtuessa lisenssiin täytyy päivittää uuden koneen tiedot. [16.]

4.10 Jatkohälytykset valvomosta

Aikaisemmin käytössä olleessa tietokoneessa oli sarjaporttiin kytkettynä GSM-moduuli. Tämän avulla järjestelmään tulleet hälytykset lähtivät tekstiviesteillä huoltohenkilöille. Myös sähköpostipalvelimen kautta on ollut ennenkin mahdollista lähettää hälytyksiä, jos valvomokone on ollut verkossa.

Konesaliympäristöistä on mahdollista lähettää hälytykset fyysisten koneiden tapaan sarjaporttiin kytkettyä GSM-moduulia hyödyntämällä. Konesaleissa ei suoranaisesti ole fyysisiä sarjaportteja, joten silloin tarvitsee käyttää Ethernetissä olevaa Ethernet-sarjaporttimuunninta. Tämä linkitetään haluttuun koneeseen ja muuntimeen laitetaan moduuli. Tämä ei ole järkevä ratkaisu isommissa konesaleissa, koska yhden koneen sarjaporttiliitäntä hallitsee vain yhden laitteen.

Jatkossa asiakkaan palvelu toimii niin, että valvomokoneen olemassa olevan palvelun avulla hälytyksiä sisältävät sähköpostit lähetetään erilliseen palveluun. Sieltä ne päätyvät tekstiviestien kautta huoltohenkilöille. Sähköpostissa on mukana hälytyksen vastaanottajan puhelinnumero. Palvelu on ulkoisen palveluntarjoajan softaa.

4.11 Käyttöönotto

Ennen lopullista käyttöönottoa ohjelman käytöstä ja siihen kirjautumisesta tehtiin kirjautumisopas. Materiaali jaettiin asiakkaan edustajille sekä huoltohenkilöille. Opasta käytettiin avuksi järjestetyissä koulutustilaisuuksissa, joissa käytiin läpi valvomon kirjautumistunnusten käyttöönotto sekä turvallinen ja sujuva käyttö. Järjestelmän tietoturvalliseen käyttöön sisältyy riittävän vahvan henkilökohtaisen salasanan lisäksi kaksivaiheinen tunnistautuminen. Tämä tarkoittaa sitä, että tunnuksen ja salasanan lisäksi käyttäjä tunnistetaan jollakin toisellakin tavalla. Sitä hyödynnetään yleisesti esimerkiksi pankkien verkkopalveluihin kirjauduttaessa.

Käyttöönoton yhteydessä paikallisen fyysisen valvomon toiminta lopetettiin ja Pyramid-järjestelmää siirryttiin käyttämään konesalin kautta. Tässä yhteydessä kaikki kohteista tuleva muuttuva data, hälytys- ja trendilokit siirrettiin vanhasta valvomosta palvelinkoneelle.

5 Loppupohdinta

Tämän opinnäytetyön tarkoituksena oli päivittää pöytäkoneella ollut rakennusautomaatiojärjestelmän versio ja siirtää se konesalin serverikoneelle. Tämä oli samalla työn päätavoite. Päivitystyö saatiin valmiiksi aikataulun mukaisesti ja pöytäkoneen ikääntymisen tuoma rikkoutumisen uhka onnistuttiin välttämään. Tämän tyyliset järjestelmien päivitystyöt on hyvä tehdä hyvissä ajoin ennen laitteiden käyttöiän loppumista.

Projektin aikataulu oli asiakkaan kanssa yhdessä sovittu, mutta sitä päivitettiin kolmansien osapuolien vuoksi. Välillä projekteissa syntyy aikatauluissa viivästyksiä, kun toimijoiden määrä on suuri. Aikataulun päivittäminen ei kuitenkaan tuonut merkittävää haittaa, sillä käytössä ollut valvomojärjestelmä toimi uuden järjestelmän käyttöönottoon saakka.

Työn yhteydessä automaatiojärjestelmä päivitettiin uudempaan versioon. Päivityksessä järjestelmästä tehtiin Caverionin standardin mukainen. Tämä helpottaa tulevaisuudessa tehtäviä järjestelmäversioiden päivitystä, kun asiakkaan järjestelmässä ei ole standardista poikkeavia ratkaisuja.

Konesaliin luotiin ympäristö järjestelmää ja etäkäyttöä varten. Tulevaisuudessa etäkäyttöominaisuuksien kysyntä tulee todennäköisesti kasvamaan ja varmasti automaatiojärjestelmiä toimittavat yritykset niihin panostavat. Asiakkaan verkon ja konesalin välille muodostettiin turvallinen VPN-yhteys. Tietoturvalliset yhteydet ovat elintärkeät, jotta asiakkaiden kiinteistöjen turvallisuus tai liikesalaisuudet eivät vaarannu.

Päivitystyön päätteeksi järjestelmän toimivuus testattiin ja asiakkaan henkilökunnalle järjestettiin koulutustilaisuudet ohjelman käyttöönottoon ja käyttöön liittyen. Järjestelmien huolellinen testaaminen ja asiakkaan perehdyttäminen ovat tärkeä osa työtä. Testaaminen varmistaa järjestelmien toimivuuden ja kouluttaminen sujuvan käytön.

Opinnäytetyön toisena tavoitteena oli oppia hahmottamaan, mitä päivitystyö sisältää ja mitä työn onnistuminen vaatii. Päivitystyöprosessi oli ajallisesti suhteellisen pitkä. Järjestelmään liitettyjä kohteita on huomattavan paljon, mikä vaikutti työmäärään. Oman aikansa veivät sopimusneuvottelut, koneympäristön perustaminen sekä järjestelmän testaaminen.

Työ on opettanut valvontajärjestelmän päivittämisestä, VPN-yhteyksien muodostamisesta sekä konesaliympäristöstä. Myös sopimusneuvotteluiden eteneminen ja kunnan päätöksiin vaikuttavat sopimukselliset tekijät ovat arvokkaita tietoja tämän työn tekijälle, mitä voidaan hyödyntää tulevissa projekteissa.

Lähteet

1 Härkönen, Pentti & Liedes, Riikka. 2018. Rakennusautomaatiojärjestelmät, ST-käsikirja 17. E-kirja. Sähkötieto Ry.

2 Piikkilä, Veijo & Sahlstén, Toivo. 2017. Kiinteistöjen tiedonsiirtoväylät, ST-käsikirja 21. E-kirja. Sähkötieto Ry.

3 Metasys® Building Automation System. 2021. Verkkoaineisto. Johnson Controls International PLC. <https://www.johnsoncontrols.com/building-automation-and-controls/building-management/building-automation-systems-bas>. Luettu 26.4.2021.

4 Härkönen, Pentti & Liedes, Riikka. 2018. Kiinteistöjen valvomojärjestelmät, ST-käsikirja 22. E-kirja. Sähkötieto Ry.

5 Understanding Modbus Protocol - RTU vs TCP vs ASCII. 2021. Verkkoaineisto. DPS Telecom. <https://www.dpstele.com/modbus/index.php>. Luettu 26.4.2021.

6 M-Bus -järjestelmän suunnitteluohjeet 2009. 2009. Verkkoaineisto. Saint-Gobain Pipe Systems Oy. <https://docplayer.fi/19168901-Suunnit-teluohjeet-2009.html>. Luettu 23.4.2021.

7 Kansainvälinen KNX-standardi. 2021 Verkkoaineisto. KNX Finland ry. <https://www.knx.fi/index.php?k=224571>. Luettu 24.4.2021.

8 Heikkilä, Teemu. 2008. BACnet Foorum Helsinki - Avoimen rakennusautomaatiojärjestelmän suunnittelu. Verkkoaineisto. <https://docplayer.fi/2259742-Bacnet-foorum-helsinki.html>. Luettu 25.4.2021.

9 The Basics of LonWorks. 2004. Verkkoaineisto. EC&M, Endeavor Business Media, LLC. <https://www.ecmweb.com/content/article/20892561/the-basics-of-lonworks>. Luettu 26.4.2021.

10 Lightning know-how Dali Manual. 2020. Verkkoaineisto. Tridonic GmbH & Co KG. <https://www.tridonic.it/it/download/technical/DALI-manual_en.pdf>. Luettu 26.4.2021.

11 DI-16. 2021. Verkkoaineisto. Fidelix Oy. <https://www.fidelix.com/bms/di-16/>. Luettu 28.4.2021.

12 Yrityksen sisäinen dokumentti. 2021. Caverion Suomi Oy.

13 TOSIBOX®-tuotteet. 2021. Verkkoaineisto. Tosibox Oy. <https://www.tosibox.com/fi/tuotteet/>. Luettu 26.3.2021.

14 Tilaajan edustaja 1. 2021. Vantaa. Puhelinkeskustelu 12.3.2021.

15 Tilaajan edustaja 2. 2021. Vantaa. Puhelinkeskustelu 15.3.2021.

16 Nio, Aki. 2021. Tuotekehityssuunnittelija, Caverion Suomi Oy, Kouvola. Puhelinkeskustelu 17.3.2021.

17 Konesalipalvelut, Pyramid järjestelmäkaavio. 2021. Yrityksen sisäinen materiaali. Caverion Suomi Oy.