Jevgeni Iljin

Modernit talotekniikkaverkot sekä niiden turvallisuus ja tulevaisuudennäkymät

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietoliikenne

Insinöörityö

12.2.2017

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Jevgeni Iljin Modernit talotekniikkaverkot sekä niiden turvallisuus ja tulevaisuudennäkymät 37 sivua 12.2.2017
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietoliikenne
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Osaamisaluepäällikkö Janne Salonen

Insinöörityö selvittää nykypäivän kiinteistöjen nopeasti kehittyviä automaatio- ja turvallisuusjärjestelmiä kuten myös asiakaskunnan laajenevia vaatimuksia koskien turvallisuutta, helppokäyttöisyyttä ja kustannustehokkuutta. Kysyntä ei koske ainoastaan isoja rakennuskomplekseja vaan kysyntä on olemassa myös niin pientalo- kuin jopa kerrostalo asumisen tasolla.

Tämä opinnäytetyö kuitenkin keskittyy isompiin kiinteistöihin ja niiden järjestelmiin. Työ käy läpi ja arvioi erilaisia kiinteistön automaatiotekniikka- ja turvallisuustekniikka mahdollisuuksia jakautuen niin teoriaan kuten myös käytäntöön, keskittyen pääasiassa etäkäyttöhallintaan erilaisten TCP/IP-yhteysverkkojen ylitse sekä niiden suojausmenetelmiin.

Lisäksi tämä työ havainnollistaa, selittää ja arvioi kiinteistön automaatio- ja turvallisuusjärjestelmien tulevaisuutta käyttäen laajoja esimerkkejä isoista kiinteistöistä. Työ selittää, miten järjestelmän arkkitehtuuri jakautuu aina yksilö käyttäjään asti.

Lopuksi työ arvioi kehityksen tulevaisuutta sekä arvioi mahdollisia uusia riskejä, jotka tulevat tämän uuden teknologian mukana.

Avainsanat	talotekniikka, tietoliikenne, turvallisuus, verkko

Author(s) Title Number of Pages Date	Jevgeni Iljin Modern building service networks and their security and future 37 pages 12 February 2017
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data networks
Instructor(s)	Head of Department Janne Salonen

This thesis aims to explain and go through rapidly developing building automation systems and security systems as well as growing and quickly expanding customer demands for security, accessibility and efficiency. Demand is not only restricted to large business organizations but these new technologies are also in large demand among big and small housing buildings.

However this thesis focuses mainly on large organization building complexes and their building automation systems. Thesis goes through and closely inspects different building automation and security measures dividing them in theory and in practical examples while still mainly focusing on modern IoT modelled systems and TCP/IP networks and how they are protected via different security measures.

In addition this thesis goes through transition process and modernization of older building automation systems and how these system will be adapted in modern world through Internet of Things -concept. Thesis goes through few security breach examples and how these modern digital threats are being counter-measured on large and individual scale.

At the end thesis will speculate future prospects of building automation system and future threats it will be facing and how those risks will be minimized.

Keywords	building service networks, data communication, security, network

Sisällys

Lyhenteet

AC/DC	Vaihtovirta ja tasavirta. Tulee sanosita alternating current ja direct current.
BACnet	BACnet tulee sanoista Building Automation and Control. BACnet on tietoliikenneprotokolla, joka on kehitetty vastaamaan erityisesti talotekniikan tarpeisiin.
BAS	BAS tulee Building Automation System, suomennos kiinteistön automaatio järjestelmä.
DALI	Digital Addressable Lighting Interface on digitaalinen valaistuksen ohjausväylä esimerkiksi elektronisille liitäntälaitteille ja himmentimille.
GUI/UI	Graafinen käyttöliittymä ja tavallinen käyttöliittymä. Tulee sanoista graphical user interface.
I/O	Tarkoittaa input ja output eli tulo ja lähtö. Tarkoittaa yleensä ohjelmoitavan laitteen portteja.
IEEE	Institute of Electrical and Electronics Engineers on kansainvälinen tekniikan alan järjestö. Siihen kuuluu yli 400 000 jäsentä yli 160 maassa
IoT	Internet of Things, tarkoitetaan internet-verkon laajentumista laitteisiin ja koneisiin.
LTE	Long Term Evolution on edistynyt 3G-tekniikka.
LVI	LVI tulee sanoista lämpö, vesi ja ilmastointi. Esimerkkeinä LVI-laitteet, LVI-asentaja.
RFID	Radio Frequency IDentification eli radiotaajuinen etätunnistus on menetelmä tiedon etälukuun ja -tallentamiseen käyttäen RFID-tunnisteita eli tägejä.

SNMP	SNMP (lyhenne sanoista Simple Network Management Protocol) on TCP/IP-verkkojen hallinnassa käytettävä tietoliikenneprotokolla. Protokollan avulla voidaan kysellä verkossa olevan laitteen tilaa tai laite voi itsenäisesti antaa hälytyksiä.
TCP/IP	Transmission Control Protocol / Internet Protocol, on usean Internet-liikennöinnissä käytettävän tietoverkkoprotokollan yhdistelmä.
VPN	Virtual Private Network eli virtuaalinen erillisverkko on tapa, jolla kaksi tai useampia yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon.
WLAN	Wireless local area network, on langaton lähiverkkotekniikka, jolla erilaiset verkkolaitteet voidaan yhdistää ilman kaapeleita.

1 Johdanto

Tämän insinöörityön päätarkoitus on selvittää automaattisten talotekniikkajärjestelmien tulevaisuuden kehitys. Insinöörityön alussa selvitetään erilaiset talotekniikan osa-alueet niiden kehityksen alku-ajoista nykypäivään ja lopuksi niiden tulevaisuuden integraatiosta IoT -konseptiin.

Osa-alueet koostuvat erilaisista taloteknisistä alueista kuten ilmastointi, vesi, lämpö ja turvallisuus. Työ selittää, miten nämä elementit ovat käyttäjän hallittavissa, miten ne on yhdistetty isoksi kokonaisuudeksi ja miten ne ovat integroitu nykypäivän TCP/IP – verkkoon.

Työ aloittaa 1980-luvun kehityksestä ja lyhyestä historiasta selittäen, miten talotekniset laitteet ovat verkostoituneet ja mihin se on loppujen lopuksi johtanut nykypäivänä. Vaikka insinöörityö keskittyy aluksi hyvin paljon talotekniikkaan, niin työn toinen puolisko siirtyy käsittelemään enemmän tietoliikennettä.

Työn toinen puolisko keskittyy tietoliikenteeseen ja miten se on integroitunut talotekniikkaan ”Asioiden internet” -ideologian kautta ja tullut tätä kautta uudeksi kilpailevaksi kehitysratkaisuksi vanhojen järjestelmien ja menetelmien rinnalle.

Tämä moderni ratkaisu ei kuitenkaan ole täysin ongelmaton, ja työ selvittää erilaisia mahdollisia riskejä sekä niiden torjuntamahdollisuuksia.

Työn loppuosa sisältää lyhyen spekulaation kiinteistön automaatiojärjestelmien tulevaisuudesta ja mahdollisesta integraatiosta jokapäiväiseen käyttöön sekä vanhojen järjestelmien kohtalosta.

2 Talotekniikka-automaation lyhyt historia

Vuonna 1883 Warren Johnsonnin kehittämää termostaattia voidaan pitää talotekniikan ensimmäisenä keksintönä. Yksinkertainen lämpötilaa näyttävä termostaatti kertoi talonmiehelle kiinteistön lämpötilan ja oli täten myös merkki, että hiiltä oli lapioitava uuniin lämpötilan nostamiseen tai vastakohtaisesti lämpötilaa laskettiin tiloja tuulettamalla. [1.]

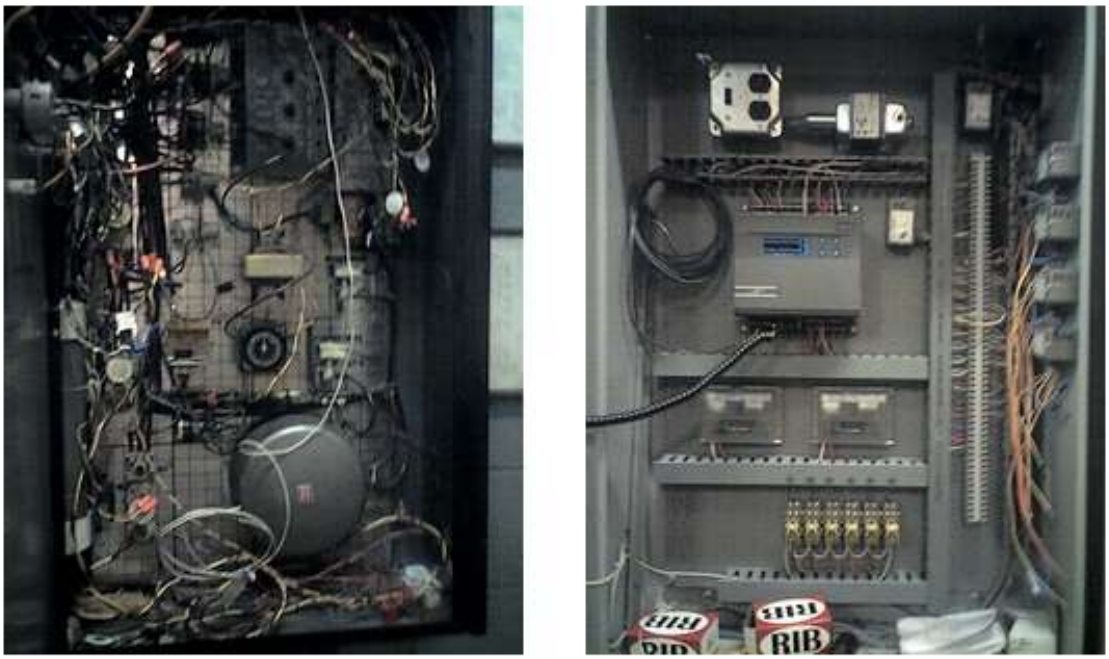
Kuvio 1. Vuonna 1925 Johnson Controlsin patentoima monikäyttöinen termostaatti.

Tästä eteenpäin talotekniikka kehittyi nopeasti toimien pneumatiikalla aina 1980-luvulle asti. Nämä järjestelmät jäivät kuitenkin pian vanhanaikaisiksi sähkömekaanisten releiden ja transistoreiden yleistyessä. 1980-luvun loppupuolella talotekniikan automaatiota aloitettiin tietokoneistaa ja pelkistä pneumatiikkapohjaisista järjestelmistä alettiin luopua. [1.]

Mutta vanhat pneumatiikkaa käyttävät järjestelmät ovat edelleen käytössä, ja niitä huolletaan sekä ylläpidetään erityisesti vanhoissa rakennuksissa.

Pneumatiikan kooste:

- Pneumatiikkaa on tapa, jolla paineistetut kaasut ohjaavat mekaanista liikettä.
- Ennen sähköisiä ja digitaalisia ohjausjärjestelmiä pneumatiikka oli yleisin tapa ohjata rakennuksen LVI-järjestelmiä.
- Hyvin ja jatkuvasti huollettu pneumaattinen järjestelmä on luotettava.
- Sisältää paljon analogisia laitteita ja voi täten olla epätarkka sekä vaikeasti hallittava.
- Epäkäytännöllinen sillä asetusten muuttaminen vie aikaa.
- Se on edelleen käytössä.



Kuvio 2. Vasemmalla vanha vahvasti pneumatiikkaa luottava ohjauspaneeli. Oikealla on sama mutta päivitetty digitaalinen paneeli. (Perri Aire Inc / Chicago)

3 Nykyaikainen automaattinen talotekniikka

Automaattisella talotekniikalla tai rakennusautomaatiolla tarkoitetaan rakennuksen lämmitys-, valaistus-, valvonta-, hälytys- ja ilmanvaihtojärjestelmien ohjaamista automaattisesti ja nykypäivänä myös etänä erilaisten TCP/IP-yhteysverkkojen ylitse. Useimmiten rakennusautomaatiojärjestelmissä pyritään yhdistämään nämä kaikki toimenpiteet yhdeksi helposti hallittavaksi järjestelmäksi. [2.]

Rakennusautomaatiolla pyritään lisäämään viihtyvyyttä ja turvallisuutta sekä vähentämään energiankulutusta. Laitteiden yhdistäminen on usein toteutettu väylätekniikalla, jolloin ne saadaan toimimaan yhtenäisesti ja älykkäästi. [2.]

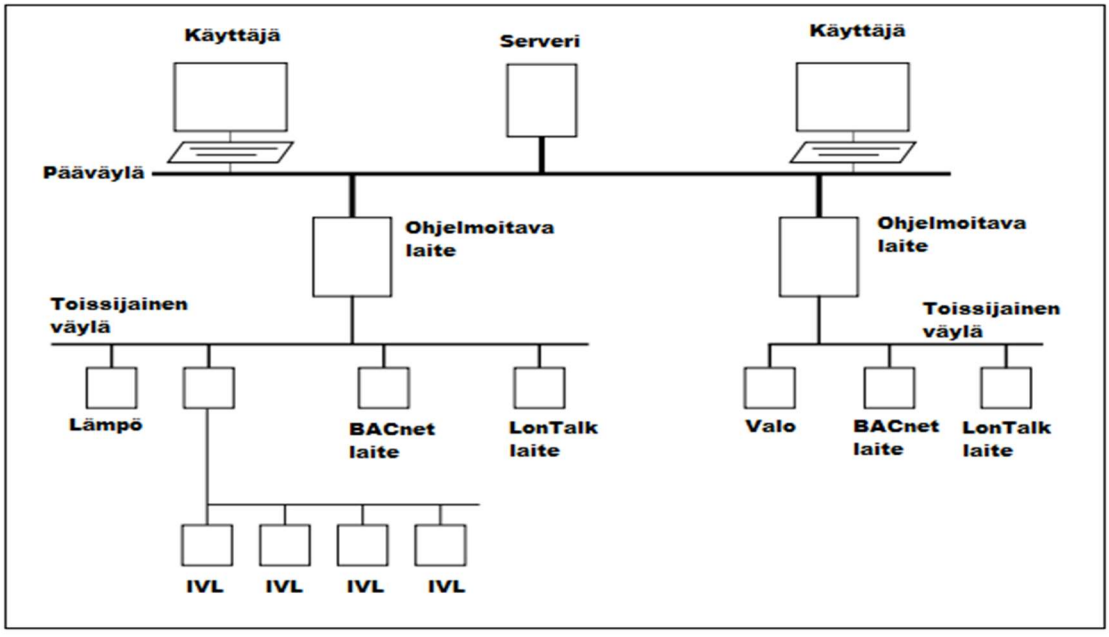
Rakennusautomaatiojärjestelmiä on markkinoilla useita, ja niiden ominaisuudet poikkeavat suuresti toisistaan. Yksinkertainenkin rakennusautomaatiojärjestelmä voidaan ohjelmoida esimerkiksi tekemään tiettyjä toimenpiteitä asunnosta poistuttaessa, kuten päälle jääneiden valojen, lieden, kahvinkeittimen ja muiden kodinkoneiden virran katkaisu.

Monipuolisemmilla järjestelmillä voidaan lisäksi hoitaa asunnon lämmönsäätö, ilmastointi ja hälytykset, kuten esimerkiksi kosteushälytys pesukoneen rikkoutuessa tai huoneiston lämpötilan putoaminen tarkoituksettomasti. [2.]

3.1 Rakennusautomaation väylätekniikka

Väylätekniikalla tarkoitetaan nykyaikaista järjestelmää, jossa yksi väylä yhdistää useita eri laitteita keskenään. Laitteet voivat olla erilaisia, mutta ne on kuitenkin liitetty saman standardoidun rajanpinnan kautta.

Useimmat rakennusautomaatioverkot koostuvat pää- ja toissijaista väylistä, väylät yhdistävät korkeantason säätimet alemman tason säätimiin, I/O-laitteisiin ja mahdollisiin käyttöliittymiin (UI, GUI). ASHRAE:n avoin protokolla BACnet tai avoin protokolla LonTalk määrittää, kuinka useimmat tällaiset laitteet ovat yhteensopivia. Nykyaikaiset järjestelmät käyttävät SNMP:tä tapahtumien seuraamiseen. [3.]



Kuvio 3. Mahdollinen esimerkki yksinkertaisesta kiinteistön laiteverkosta.

Fyysisenä yhteytenä laitteiden välillä on perinteisesti toiminut valokuitu, Ethernet, ARC-NET, RS-232, RS-485 tai WLAN. Nykyaikaiset järjestelmät luottavat standardeihin perustuviin heterogeenisiin verkkoihin, jotka on määritelty IEEE 1905,1-standardissa. Nämä verkot ovat yleensä vain IP-pohjaisia verkkoja, mutta ne voivat myös hyödyntää jo olemassa olevaa kaapelointia (Datasähkö, Power over Ethernet), käyttää suuren kaistanleveyden omaavia langattomia verkkoja, kuten LTE:tä ja IEEE 802.11n:ää ja IEEE 802.11ac:tä usein yhdistäen nämä käyttäen kiinteistön langatonta verkkoa, standardina ZigBee.

Tällä hetkellä talotekniikkamarkkinat ovat hyvin ongelmallisia, sillä eri valmistajien patentoidut laitteet ovat harvoin keskenään yhteensopivia. Täten nykyiset järjestelmät ovat yhteensopivia vain sovellustasolla, jolloin käyttäjä voi yhdistää eri valmistajien laitteita keskenään isoksi kokonaisuudeksi käyttäen SNMP-tietoliikenneprotokollaa. [3.]

3.2 Talotekniikka automaation perustoiminta

Automaattinen talotekniikkapohja perustuu tuloihin ja lähtöihin. Kiinteistön erilaiset mittauslaitteet vastaavat erilaisten ulkoisten suureiden mittauksesta ja lähettävät signaalin eteenpäin, missä ohjauslaite tulkitsee ja hoitaa jatkotoimenpiteet annetun ohjelmoinnin mukaan.

Signaalin vastaanotosta vastaa yleensä jokin analoginen sensori, mutta jos esimerkiksi otamme mukaan kulunvalvonnan, joka on nykypäivänä puhtaasti digitaalinen, on sen toiminta lähes samanlainen.

3.2.1 Talotekniikan sensorit

Sensoreiden analogisia tuloja käytetään erilaisten muuttujien mittaukseen. Esimerkkeinä ovat erilaiset lämpötila, ilmankosteus ja paineanturit, esimerkiksi termostaatti. Sähkövirtaa käyttävät sensorit 4-20 mA, 0-10 voltin ja vastuksenmittaajat.

Nykypäivän sensorit ovat tyypillisesti helppo asentaa, ja ne ovat usein langattomia.

Sensoreiden digitaalinen tulo toimii taas yleensä binäärisesti 0/1-toiminolla tai pulsseina.

Esimerkkinä 24V:n AC/DC-signaali tai jokin kosketuslaite. Jatkuvia pulsseja voidaan taas käyttää esimerkiksi toistuvan suuren mittaukseen esimerkiksi tuuliviiri ja tuulimittari.

Kuvio 4. Ventus W132 -tuulimittari (Verkkokauppa.com)

3.2.2 Talotekniikan ohjainlaitteet

Ohjainlaitteet ovat pääasiassa pieniä, integroidun tietokoneen, tulon ja lähdön omaavia talotekniikan ohjaavia laitteita. Nämä laitteet vaihtelevat suuresti, ja ne sisältävät eri kokoja ja valmiuksia ohjata erilaisia kiinteistön taloteknisiä laitteita tai suuria laiteverkkoja ja aliverkkoja.

Tyypillisesti automaattinen ohjainlaite lukee sensorista tulevan suureen, joita ovat esimerkiksi lämpötila, ilmankosteus ja paine, ja lähettää vastauksen. Lähtö on jokin ennalta ohjelmoitu ohjelma, joka lähetetään signaalina muille järjestelmissä oleville laitteille, jolloin saadaan haluttu lopputulos. Esimerkiksi sensorina toimiva valokenno kertoo, että ulkona on pimeää, jolloin ohjainlaite lähettää käskyn sytyttää ulkovalot. Tätä kutsutaan rakennusautomaatioksi. [3.]

Ohjainlaiteen ei välttämättä tarvitse olla monimutkainen, vaan se voi toimia ilman sensoreita, esimerkiksi aikaohjelmalla tai ainoastaan käyttäjän toimesta. Ohjainlaitteen tulot ja lähdöt voivat olla joko digitaalisia tai analogisia.

3.2.3 Talotekniikan suurimmat elementit

Talotekniikalla tarkoitetaan käytännössä kaikkia kiinteistön teknisiä laitteita, jotka hallinnoivat ja tuottavat rakennuksen olosuhteita.

Tärkeimmät näistä ovat olleet tyypillisesti:

- ilma
- lämpö
- valo
- vesi.

Mutta nykypäivän talotekniikka käsite on laajentunut ja käsittää sekä myös informaation, turvallisuuden ja liikkumisen. Näitä uusia osa-alueita voidaan hallita, ohjelmoida ja myös ohjata samanlaisin menetelmin.

3.2.4 Rakennuksen käyttöaste

Rakennuksen käyttöasteella tarkoitetaan rakennuksen käyttötilaa niin automaatio kuin manuaalisesti asetetussa järjestelmässä. Käyttötilat ovat yleensä esimerkiksi eri aikatauluja:

- Rakennus tyhjä
- Aamu tila, päivä tila ja yö tila.

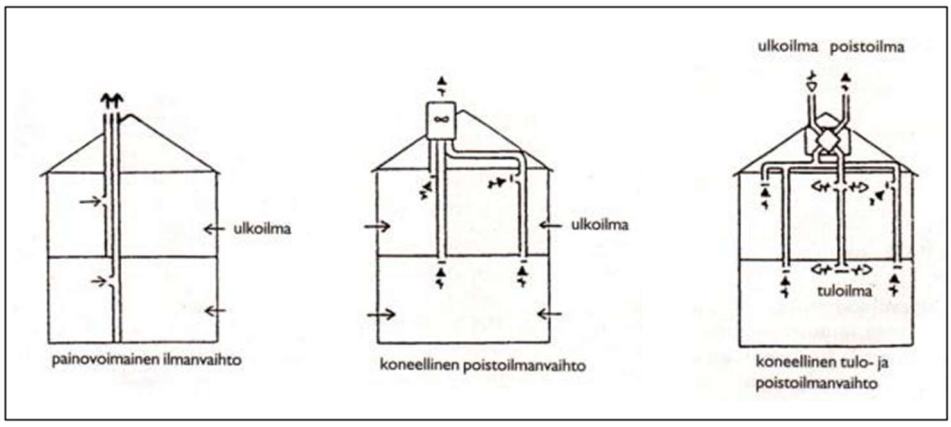
Vaikka käyttötilat perustuvat pitkälti käyttäjän asettamiin aikatauluihin ne voidaan aina muuttaa ja talotekniikkaa asettaa uudelleen. Käyttötilojen onkin tarkoitus parantaa ja helpottaa rakennuksessa olevien henkilöiden mukavuutta automaattisesti ohjaamalla talotekniikka aikaisemmin ohjelmoidun kaavan mukaan.

Käyttötilat voidaan myös jakaa pienempiin osioihin esimerkiksi osioon huone tai talonsiipi. Kehittyneissä käyttötila järjestelmissä onkin huonekohtaiset anturit ja mittarit, jotka mittaavat huoneen olosuhteita ja havaitsevat, jos tilassa oleskellaan tehtäen muutoksia sen mukaan. Huoneen kohtainen käyttötila voidaan myös usein nykypäivän laitteilla ohittaa, jos huoneessa on esimerkiksi omat talotekniikkaohjaimet, lämpö ja ilmastointi.

Käyttötilojen hyviin puoliin kuuluu energian säästö ja käyttömukavuus mutta huonosti asetut käyttötilat voivat aiheuttaa harmia, koska esimerkiksi huoneen lämmittäminen voi viedä aikaa. Mutta nykypäivän järjestelmät ovat pitkälti ohjelmoituja sisältäen esimerkiksi oppivan historian ja usein myös tarvittavan verkkoyhteyden ylitse toimivan käyttöjärjestelmän, jolla voidaan ohittaa tai muokata käyttötiloja. [3.]

3.2.5 Ilmastointi ja ilmanvaihto

Ilmastointi tarkoittaa sisäilman käsittelyä, esimerkiksi viilentämistä ja lämmittämistä koneellisesti. Toisinaan ilmastoinnilla vaikutetaan myös sisäilman kosteuteen. Arkikielessä ilmastoinnilla tarkoitetaan virheellisesti myös pelkkää ilmanvaihtoa. Kylmän lähde on usein sähköllä toimiva lämpöpumppu.



Kuvio 5. Ilmanvirtaukset rakennuksessa (Sisäilmayhdistys ry)

Huoneilman viilennystä voidaan tuottaa myös käyttämällä syvän järven viileää pohjavettä. Tällaista tekniikkaa kutsutaan myös nimellä kaukokylmä, jos viilennystä jaetaan kaukolämpöverkon tapaan.

Ilmanvaihdon tehtävänä on tuoda puhdasta ilmaa hengitykseen ja poistaa rakennuksessa syntyvät epäpuhtaudet. Ihmisen hapentarpeen tyydyttämiseksi tarvittava ilmanvaihdon määrä on murto-osa tarvittavasta kokonaisilmanvaihtomäärästä. Hapentarpeen ja keuhkoissa syntyvän hiilidioksidin poistamiseksi ihmisen keuhkojen kautta kulkee yli 15 000 litraa ilmaa vuorokaudessa. Mitä puhtaampaa tämä ilma on, sitä paremmin elimistö voi.

Ilmanvaihdon toiminta perustuu paine-eroihin. Ilma virtaa suuremmasta paineesta pienempään. Paine-ero voidaan saada aikaan joko puhaltimilla (koneellinen ilmanvaihto) tai lämpötilaeron ja tuulen yhteisvaikutuksella (painovoimainen ilmanvaihto). Mikäli tuloilma puhalletaan koneellisesti tilaan, on kyseessä tulo- ja poistoilmanvaihto, muussa tapauksessa vain poistoilmanvaihto. Jos tuloilmaa kostutetaan tai jäähdytetään, puhutaan ilmastoinnista.

Poistoilmanvaihdon toteutuksessa on tärkeää järjestää hallittu korvausilman sisäänotto, esimerkiksi ulkoilmaventtiilien avulla. Koneellisen tulo- ja poistoilmanvaihdon etuna on mahdollisuus tuloilman suodatukseen ja lämmöntalteenottoon poistoilmasta. Huonosti hoidettuun tuloilmakanavistoon kertyvä lika voi kuitenkin ajan kuluessa alkaa haista ja pilata sisäilmaa. Painovoimaisen poistoilmanvaihdon suosio erityisesti asuinrakennuksissa perustuu alhaisiin investointikustannuksiin. Painovoimainen ilmanvaihto ei itse aiheuta melua, mutta meluisalla paikalla ikkunatuuletus voi olla ongelmallista.

Nykypäivän ilmastointi ja ilmanvaihto on pitkälti automatisoitu ja on liitetty verkkoon esimerkiksi BACnet, TCP/IP. Ohjelmoinnin avulla laitteet toimivat erilaisten aikataulujen mukaan sekä voivat esimerkiksi sammua pois päältä automaattisesti tulipalotilanteessa.

Suomessa asuntojen yleisin ilmanvaihtotapa on painovoimainen ilmanvaihto. Se oli 1960-luvulle saakka lähes yksinomainen ilmanvaihtotapa. Nykyään uusien asuinrakennusten ilmanvaihtoa ei enää yleensä järjestetä painovoimaisena, koska sen ei katsota enää riittävän kaikkiin huonetiloihin. Osittain tämä johtuu uusiin järjestelmiin usein liitetyistä lämmön talteenottojärjestelmistä, jotka edellyttävät koneellista ilmanvaihtoa. [4.]

Sisäministeriön julkaiseman rakentamismääräyskokoelman osassa D2 on määritelty tyypillisimpien tilojen vähimmäisilmamaarät pinta-alaa kohden. [4.]

3.2.6 Lämmitys

Rakennuksen lämmityksen tavoitteena on ylläpitää hyviä lämpöoloja sekä viihtyisyyden sekä terveyden kannalta. Lämmitystarpeeseen vaikuttavat rakennus- ja ilmanvaihtotekniikka, sääolot ja tavoitelämpötilat. Lämmöntarve mitoitetaan yleensä huone sekä rakennuskohtaiseksi. Lämmityslaitteilla lämmitetään rakennuksen tilojen lisäksi myös käyttövesi ja ilmanvaihdon tuloilma. Lämmitysjärjestelmää valittaessa on hyvä ottaa huomioon rakennuksen koko, käyttötarkoitus, sijainti ja energiatarve.

Tavallisimmat lämmöntuotantotavat rakennuksissa ovat kauko-, öljy- ja sähkölämmitys sekä kotimaisten kiinteiden polttoaineiden käyttö. Lisäksi käytetään maakaasulämmitystä, ulkomaisia kiinteitä polttoaineita, erilaisia lämpöpumppuja sekä aurinkolämmitystä.

Lämmöntuotantotavoista selkeästi yleisin on kaukolämmitys, jota käytetään lähes puolessa rakennuskannasta. Vesikiertoiset järjestelmät on lämmönjakelussa yleisimmät. Suuret kiinteistöt lämmitetään lähes aina vesikiertoisesti

Vesikiertoisesta kaukolämmitysjärjestelmässä lämpö siirretään kuumana vetenä suljetussa kaksiputkisessa kaukolämpöverkossa. Kuuma vesi johdetaan kiinteistön lämpöjakokeskukseen, jossa se luovuttaa lämpöä asiakkaiden lämmitysverkkoon ja lämpimän käyttöveden valmistukseen lämmönsiirtimen avulla. Talot käyttävät lämpöä huoneiden ja käyttöveden lämmittämiseen sekä ilmanvaihtoon. Kaukolämpöverkon vesi palaa jäähtyneenä paluujohdossa takaisin tuotantolaitokseen uudelleen lämmitettäväksi. Kaukolämpövesi ei kierrä talojen lämmitysverkossa. [5.]

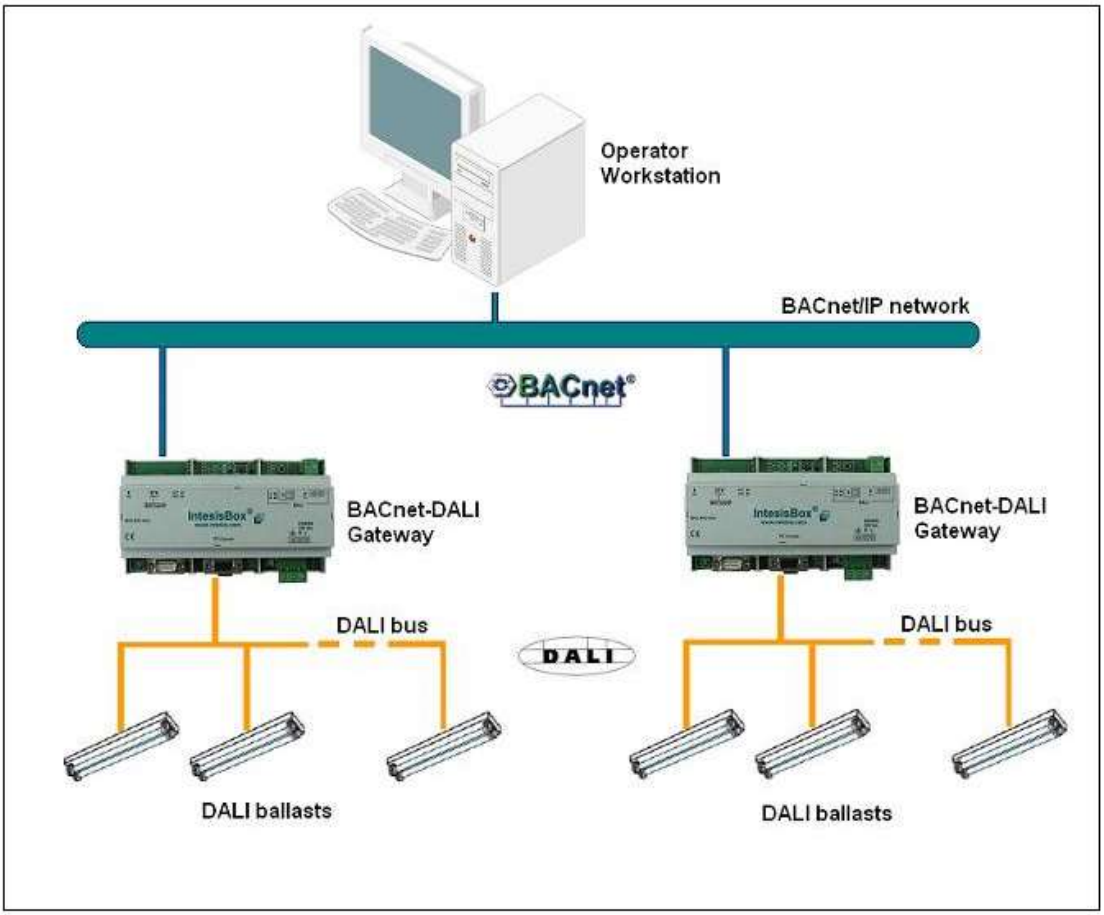
3.2.7 Valaistus

Kiinteistön valaistus voidaan kytkeä päälle, pois päältä tai himmentää riippuen rakennuksen automaatiosta ja valojärjestelmästä. Automaatiinen valaistus perustuu erilaisiin käyttötiloihin, aikataulukoihin tai nykypäivänä läsnäolotunnistimiin. Yksi tyypillinen esimerkki on, jos liiketunnistin ei tunnista liikettä tilassa puolessa tunnissa, niin valot sammuvat automaattisesti. Toinen esimerkki on ulos asennettu valokenno, joka voi ohjata sekä sisätilojen että liiketilojen valaistusta.

Nykypäivän valaistus on pyritty tekemään mahdollisimman energia tehokkaaksi käyttäen automaatiota ja energiansäästövalaisimia. Uusien rakennusten valaistus on nykypäivänä kytketty väylään (DALI). DALI-valaisimet ovat täysin himmennettäviä ja havaitsevat sekä ilmoittavat, jos järjestelmässä on esimerkiksi palanneita lamppuja tai signaalivikoja.

3.2.8 DALI lyhyesti

DALI (Digital Addressable Lighting Interface) on digitaalinen valaistuksen ohjausväylä elektronisille liitäntälaitteille ja himmentimille.



Kuvio 6. Dali integroituna BACnet-verkkoon

DALI on digitaaliseen väylätekniikkaan perustuva osoitteellinen ja kaksisuuntainen valaistuksenohjausjärjestelmä, joka soveltuu niin kaupallisiin, arkkitehtonisiin kuin yksityisasuntojen valaistussovelluksiin. Järjestelmät voivat olla pieniä ja kevyitä tai massiivisia ja muihin järjestelmiin yhdistettyjä esimerkiksi BACnet- tai TCP/IP-verkkoon.

DALI-protokollalla saadaan yksinkertaisilla johdotuksilla ja ohjelmoinnilla aikaa, energiansäästäviä, säädettäviä ja helposti muunneltavia valaistusratkaisuja. Lisäksi kaksisuuntaisen toiminnan ansiosta järjestelmän vikatietojen ja kulutuksen seuranta onnistuu keskitetysti. [6.]

3.2.9 Vesi

Vesijohtoverkosto koostuu vesijohdoista laitteineen, paineenkorotus pumppaamoista ja vesitorneista. Vesi pumpataan verkostoon yhdestä tai useammasta vesilaitoksesta. Vesijohtoverkosto sijaitsee maan alla, jossa se on suojassa jäätymiseltä ja vesi säilyy viileänä. Vesijohtoverkosto on vedenjakelun ylivoimaisesti kallein osa, ja se tarvitsee jatkuvaa uusimista. Suomen vesilaitoksilla on yhteensä noin 100 000 km vesijohtoa. Vesijohtoverkostosta vesi johdetaan kiinteistöjen sisäisiin putkiin. Vanhimmat näistä ovat terästä. Uudemmat ovat joko muovia tai kuparia. [7.]

Kuvio 7. Viisaiden vesihallintojärjestelmien kasvavat markkinat (Navigant Research 2016)

Veden käyttö kiinteistöissä on ollut hyvin yksinkertaista kuitenkin kestävän kehityksen myötä myös veden kulutukseen on alettu kiinnittää enemmän huomiota ja sen myötä lisätä hallintaa. Nykypäivän järjestelmät ovat myös ottaneet tämän huomioon.

Uusissa järjestelmissä on tarkoitus helpottaa veden kulutuksen seuraamista ja toimia sen mukaisesti. Esimerkiksi erilaisten vuotojen nopea sulku, epätavallisten käyttöaikojen seuranta. [7.]

3.2.10 Kiinteistöhälytykset

Nykypäivänä kaikki automaattiset taloteknisetjärjestelmät sisältävät hälytys mahdollisuuden. Kuitenkin niistä ei ole hyötyä, jos tiedonkulun järjestely on laiminlyöty, joten on hyvä varmistaa ja ottaa käyttöön kaikki mahdollisesti käytössä olevat tiedonkulkukanavat ja että tiedonvälitys kaikille osallisille esimerkiksi, isännöitsijälle, kiinteistöhoitajalle, huoltomiehelle tai asukkaalle on järjestetty asianmukaisesti. Talotekniset hälytysviestit voidaan lähettää sähköpostilla, tekstiviestillä, puhelulla ja äänimerkillä. Vakuutussyistä järjestelmät ovatkin hyvin standardisoituja ja usein vaativat tarkat asetukset, sisältäen lokikirjan hälytyksestä ja tarkan tapahtuman raportin.

Asetukset voivat määrittää, jos hälytyviesti lähetetään välittömästi vai vasta tietyn rajan ylittyessä. Usein hälytysviestit onkin jaettu eri tärkeys- ja kiireellisyysluokkiin kuten esimerkiksi ennakkovaroitukseen ja vikahälytykseen.

Hälytykset voivat olla yksinkertaisesti tai hyvinkin pitkälle ohjelmoituja sisältäen erilaisia arvoja ja komentoja. Esimerkiksi suuret kiinteistöt aiheuttavat jatkuvasti erinäisiä ennakkovaroituksia eri talotekniikkalaitteista, mutta vasta tietyn raja-arvon ylittyessä hälytyksen kiireellisyysaste nousee.

Hälytykset voidaan automatisoida ohjaamaan kiinteistön muita laitteita. Esimerkiksi palohälytys voi sulkea ilmastoinnin ja palo-ovet. Kriittiset hälytykset voidaan taas ohjelmoida hälyttämään käyttäjää jatkuvasti esimerkiksi viiden minuutin välein tekstiviestillä. Jotkin hälytyksistä kuten palohälytys ovat myös käyttäjien laukaistavissa, esimerkiksi palopainike. [3.]

3.2.11 Turvajärjestelmät

Nykypäivän kiinteistöt pitävät sisällään myös usein turvatekniikkaa ja ovat usein myös osa talon automaatiojärjestelmää. Turvajärjestelmät ovat pitkälle automatisoituja, ja niiden tarkoitus on parantaa kiinteistön turvallisuutta ja informoida käyttäjää.

Tyypillisimmät turvalaitteet ovat kamerat, anturit, erilaiset tunnistimet kuten esimerkiksi liike ja ääni. Laitteet voidaan asentaa niin sisälle kuin ulos suojaamaan kiinteistöä erilaisilta uhilta. Laitevalikoima ja tarjonta on hyvin laaja, mutta toimintaperiaate on yleensä samanlainen ja turvajärjestelmät ovat myös siirtymässä puhtaasti IP-pohjaiseen järjestelmään.

Laitteet on usein kytketty akkuvirtaan, ja ne ovat hyvin ohjelmoituja. Koska valikoima on laaja, turvajärjestelmämenetelmät vaihtelevat suuresti yksinkertaisesta murtohälyttimestä isoon verkkoon, joka voi jopa sisältää satoja kameroita ja ilmaisimia. [3.]

Nykypäivänä turvallisuusratkaisut on kuitenkin usein ulkoistettu erillisen turvallisuusyrityksen hoidettavaksi.

3.2.12 Kulunvalvonta

Kulunvalvonta eli kulunseuranta on tietyllä alueella tai tietyssä rakennuksessa liikkuviin henkilöihin kohdistuvaa, vartioinnilla tai teknisillä laitteilla toteutettua valvontaa. Tietotekniikan liiton ATK-sanakirjan mukaan kulunvalvonnalla tarkoitetaan oviin ja kulkuväyliin kohdistuvaa valvontaa ja tarkkailua. Valvonnan yleinen syy on asiattomien henkilöiden kulun estäminen.

Kulunvalvonnalla voidaan lisätä valvottavan alueen turvallisuutta ja ehkäistä ilkivaltaa. Sen osana voidaan käyttää kulunvalvontajärjestelmiä, joihin on liitetty esimerkiksi RFID-lukijoita ja valvontakameroita. [8.]

Turvallisuuden lisäksi kulunvalvonnan tavoite on myös tarjota vaihtoehto niin sanotuille vanhoille mekaanisille avaimille korvaamalla ne sähköisillä tunnisteilla. Sähköinen järjestelmä on halvempi, sillä lukot itsessään voivat olla yksinkertaisia, eikä uusintasarjoituksen tarvetta ole, jos avain esimerkiksi katoaa.

Kuvio 8. Sähköinen lukko ja avaintunniste (Jevgeni Iljin, 2017)

Suurin hyötyihin kuuluu myös tarkasti määritelty kulkuoikeusohjelma, jolla voidaan rajata henkilöiden kulkuoikeuksia erittäin tarkasti käyttäen aikaohjelmia, sääntöjä ja poikkeuksia. Sähköiset avaimet ovat myös halpoja.

Kulunvalvonta usein perustuu käyttäjärekisteriin, joka on helposti muokattavissa sisältäen henkilöiden tiedot ja tiedot heille luovutetusta kortista. Nykypäivän sähköiset avainjärjestelmät pohjautuvat lähes täysin IP-järjestelmiin sisältäen omat palvelimet, missä tietokanta kulunvalvonnasta säilytetään.

Kuten turvajärjestelmät myös kulunvalvonta usein ulkoistetaan saman turvallisuusyrityksen hoidettavaksi. Suomen markkinajohtaja on Stanley Security Oy.

4 Rakennusautomaation yhteysprotokollat

Henkilökohtaisten tietokoneiden (eng. Personal Computer, PC) aikakaudella ei ollut vielä tietoa mahdollisuudesta, että tietokoneet voisivat kommunikoida keskenään. Vasta

1980-luvulla, kun DOS-käyttöjärjestelmä julkaistiin IBM-tietokoneille, siitä tuli standardi, joka hallitsi markkinoita noin 90%:n osuudella. Käyttäjien ei enää tarvinnut huolehtia, josko erilaiset järjestelmät olivat enää yhteensopivia.

Valitettavasti rakennusautomaationjärjestelmissä tilanne oli toinen. Eri valmistajat kehittivät omia järjestelmiään. Tämä aiheutti lähes aina yhteensopivuusongelmia, sillä eri valmistajien talotekniikkalaitteet eivät sopineet keskenään.

Järjestelmien kehittyessä yhä monimutkaisemmiksi sekä joustavimmiksi laitteiden yhteensopivuusongelmat aiheuttivat edelleen ongelmia. Koska taloautomaatiojärjestelmät kasvoivat isoksi, oli lähes mahdotonta integroida koko laiteverkko yhteen ainoaan järjestelmään.

Ensimmäiset yritykset korjata tämä ongelma olivat eri valmistajien kokeilut kehittää oma järjestelmät hallitsemaan koko talotekniikkaverkkoa. Vaikka yritykset olivatkin onnistuneita, ne aiheuttivat suurta harmia käyttäjille, joiden valinta laitehankinoissa supistui rajusti. He olivat pakotettuja yhden valmistajan käyttäjäksi ja olivat erittäin riippuvaisia yhdestä valmistajasta niin varaosissa kuin järjestelmän päivityksissä.

Toinen keino ratkaista yhteensopivuusongelmat oli yhteensopivien protokollien kehittäminen ja julkaisu. Protokolla pyrki yhdistämään eri talotekniikkalaitteita niin, että niiden välinen kommunikointi olisi mahdollista. Yhteisistä protokollista tulikin nopeasti standardi eri valmistajien kesken.

Rakennusautomaation protokollat voidaan jakaa kahteen ryhmään. Yksi vaihtoehto on, että koko talotekniikkalaite käyttää julkista protokollaa antaen laitevalmistajalle täyden vapauden. Toiset protokollat taas ovat rajattuja, jotka kuitenkin käyttävät standardoitua yhteysrajapintaa yhteensopivuuden luomiseksi. [9.]

Kolme suosituinta taloautomaation yhteensopivuusprotokollaa ovat nykypäivänä BACnet, LonMark ja Modbus. Vaikka kolme järjestelmää hallitsevatkin markkinoita ja koska talotekniikan päivittäminen on hidasta, TCP/IP-protokolla on vahvasti mukana varsinkin nykypäivän rakennusprojekteissa usein integroiden nämä keskenään.

4.1 BACnet

BACnet tulee sanoista Building Automation and Control Network. BACnet on ASHRAE:n ja erilaisten rakennusautomaation organisaatioiden yhdessä kehittämä rakennustekniikka standardi. Vuosien kehityksen jälkeen se otettiin käyttöön virallisesti vuonna 1995 standardi oli nimeltään ASHRAE 135-1995. Standardi hyväksyttiin ANSI:n toimesta samana vuonna, ja sen nimeksi tuli ANSI/ASHRAE 135-1995.

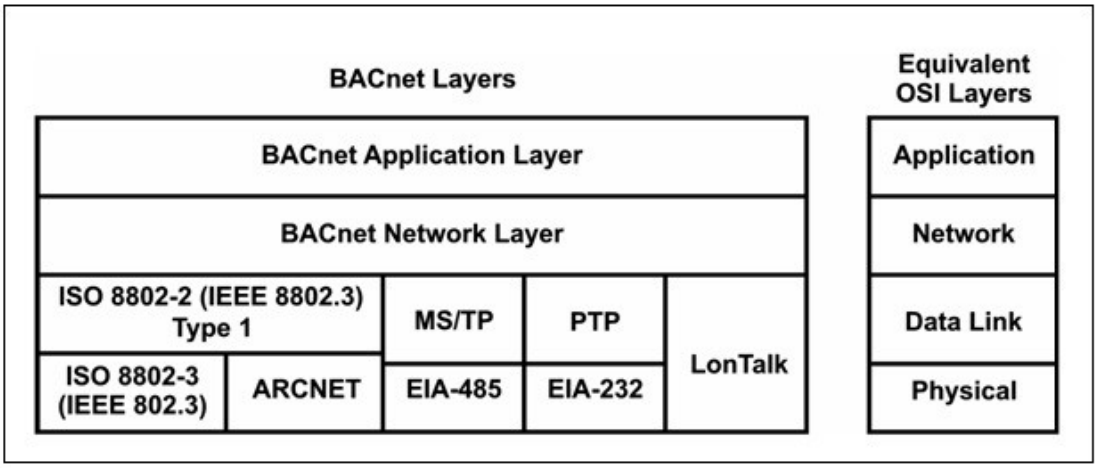
Seuraavien kuuden vuoden aikana standardi kehittyi jatkuvasti, ja sitä päivitettiin usein. Vuonna 2001 ASHRAE julkaisi päivitetyn standardin ASHRAE/ANSI 135-2001. Vuonna 2003 BACnetistä tuli kansainvälinen standardi ISO-16484-5.

BACnet on vapaa, avoin kommunikaatioprotokolla. Sitä voidaan käyttää lähes kaikissa talotekniikkalaitteissa. Niitä ovat lämpö-, vesi-, ilmastointi-, valaistus-, turvallisuus- ja kulunvalvontalaitteet. Oletusarvoisesti ne voivat hyödyntää monia erilaisia verkkoja kommunikointiin. BACnet-ohjeistus pitää sisällään tarkat ohjeet kaapeloinnista ja sen asennusmahdollisuuksista. BACnet-protokolla on suunniteltu tarkasti rakennusautomaatiota ja eri talotekniikkalaitteita varten. Se sisältää tarkat ohjauskomennot eri tarkoituksiin kuten esimerkiksi lukemien tulkitseminen sekä ohjauskäskyjen lähettäminen eteenpäin.

BACnetin kehittäjien lähestymistapa oli ottaa hyvin huomioon kaksi taloautomaation tärkeää osa-aluetta. Yhteensopivuus eri laitteiden kesken sekä toimiva mahdollisimman yksinkertainen ja yhtenäinen hallintajärjestelmä. Tämä saavutettiin olio-lähestymistavalla muuttujien seuraamiseen, hallintaan, muokkaamiseen ja yhteyksien muodostamiseen. BACnetin oliopohjainen lähestyminen sisältää kaksi osa-aluetta: objektit ja palvelut.

BACnet-oliolähestymistavassa, objektit ovat kokoelmia ominaisuuksia, joissa kukin edustaa osaa tietoa. Standardoitujen tietosuureiden lisäksi objekti voi myös olla valmistajan itse määrittelemä tieto, kunhan se on standardin mukainen, sillä BACnet-protokolla myös sisältää ennakkotiedot oletetuista tietuteista. BACnet on toimiva protokolla, koska jokainen objekti ja tietue käsitellään aina samalla tavalla.

BACnet-palveluilla tarkoitetaan arvojen lukemista ja kirjoittamista eli muuttamista. Palvelut ovat BACnetin keinoja välittää tieto taloteknisten laitteiden kesken. Tämä tarkoittaa eri hallinta-asetusten muuttamista, lähettämistä tai käskyn antamista. [10.]



Kuvio 9. BACnet-kerrokset ja supistettu OSI-malli.

4.2 LonMark, LonTalk ja LonWorks

LonMark-standardi tarjoaa erityyppisen ratkaisun yhteensopivuusongelmien ratkaisuun. Toisin kuin BACnet, LonMark on yksityisomistuksellinen Echelon Corporationin ja Motorolan yhteistyössä kehittämä 1990-luvulla kehittämä protokolla. LonMark-standardi pohjautuu yksityisomistukselliseen LonTalk-protokollaan se määrittää verkkosäännöt, joiden mukaan eri laitteet kommunikoivat keskenään.

Jotta yksityisomistuksellisen protokollan integrointi olisi helppoa, Echelon ja Motorola kehittivät mikroprosessorin nimeltä the Neutron. Tämän mikroprosessorin ja sen sisältämän ohjelmiston ansiosta protokolla määrittää informaation käsittelyn. Koska suurin osa protokollasta oli itse mikrosirussa, se antoi valmistajalle mahdollisuuden keskittyä paremmin laitekehitykseen.

LonTalk määrittää ainoastaan informaation väylän eikä puutu itse tietosisältöön. Protokolla LonWorks määrittää taas sekä sisällön että itse tietorakenteen, jonka laitteet vaihtavat keskenään. LonWorks on hajautettu ohjausjärjestelmäprotokolla, joka toimii vertaisverkkoperiaatteella, mikä tarkoittaa, että mikä tahansa laite voi kommunikoida muiden verkossa olevien laitteiden kanssa tai käyttää isäntää yhteyden muodostamiseen. LonWorks tukee suuren valikoiman viestintäväyliä.

LonWorksin kanssa yhteensopivia laitteiden välisiä muuttuvia arvoja kutsutaan Standard Network Variable Typeksi tai SNVT:ksi. Vaikka SNVT-verkossa talotekniikkalaitteiden arvoja määritetäänkin objekteina kuten BACnet-protkollassa LonWorksin toimintatapa on silti erilainen. Jotta SNVT toimisi, on lähettävillä ja vastaanottavilla laitteilla oltava tieto SNVT-verkon tarkasta rakenteesta.

Alunperin tämä aiheutti ongelmia, sillä LonWorks ei asettanut ohjeita tai standardia, mitä kukin koodi tarkoitti, ja tämä aiheutti yhteensopivuusongelmia eri valmistajien kesken. Tämän vuoksi pian vuonna 1994 SNVT-koodit standardoitiin.

Yhteensopivuuden takaamiseksi kaikki LonMarks-merkinnän saaneet laitteet testataan LonMarksin protokollalla.

Kuten BACnet LonWorks on myös kansainvälisten standardiorganisaatioiden hyväksymä (ANSI / CEA 709,1 ja IEEE 1473-l). [9.]

4.3 Modbus

Modbus on kolmas ja vanhin rakennusautomaatioyhteensopivuusprotokolla. Sen kehitti 1970-luvulla Modicon Incorporated. Protokolla oli tarkoitettu lähinnä teollisuuskäyttöön ohjaamaan automatisoituja järjestelmiä ja pienempiä ohjelmoitavia laitteita. Nykyään se on yksi eniten käytetyimmistä protokollista teollisuudessa. Mutta sen yksikertaisuus on myös hyödynnetty onnistuneesti rakennusautomaatiossa ratkaisemaan talotekniikan yhteensopivuusongelmat.

Modbus mahdollistaa monien samaan verkkoon kytkettyjen laitteiden välisen kommunikoinnin, esimerkiksi järjestelmän, joka mittaa lämpötilaa sekä kosteutta, ja toimittaa tulokset tietokoneelle. [9.]

Modbus-protokollaa käytetään usein yhdistämään valvontatietokone kenttälaitteeseen (RTU) keskitetyn hallinnan järjestelmissä. Modbus-protokollasta on olemassa sarjaportti- ja ethernet-versiot.

Sarjamuotoiselle liikenteelle on olemassa kaksi muunnelmaa erilaisilla numeerisen datan esitysmuodolla ja hiukan erilaisilla protokollan yksityiskohdilla. Modbus RTU on kompakti binaarinen datanesitysmuoto. Modbus ASCII on tekstipohjainen ja ihmisen ymmärrettävässä muodossa. Molemmat muunnelmat käyttävät sarjaliikennettä. RTU-formaatissa käytetään tiedon eheyden tarkistukseen CRC-tarkistussummaa, kun taas ASCII-formaatti käyttää longitudinal redundancy check -tarkistussummaa. Solmut, jotka on määritetty käyttämään RTU-muunnelmaa, eivät kommunikoi ASCII-muunnelmaa käyttävien solmujen kanssa, ja päinvastoin.

TCP/IP-yhteyksille (esimerkiksi ethernet) on olemassa uudempi muunnelma, Modbus/TCP. Se on helpompi toteuttaa kuin Modbus/ASCII tai Modbus/RTU, koska se ei tarvitse tarkistussumman laskentaa.

Tietomalli ja toimintokutsut ovat samanlaisia kaikille kolmelle yhteysprotokollalle; vain kapselointi on erilainen.

On olemassa myös laajennettu versio, Modbus Plus (Modbus+ or MB+), mutta se on käytössä pääasiassa Modiconissa. Se tarvitsee dedikoidun prosessorin käsittelemään nopeaa HDLC-tyyppistä token-kiertoa. Se käyttää kierrettyä parikaapelia 1 Mbps nopeudella, ja sisältää muuntajaeristyksen jokaisessa kenttälaitteessa, joka tekee siitä muutos/reuna-liipaistavan jännite/taso-liipaisun sijasta. Modbus Plus:n liittäminen tietokoneeseen vaatii erityisliitännän, tyypillisesti laajennuskortin (PCI tai PC-Card).

Jokaiselle Modbus-väylään liitettävälle laitteelle annetaan yksilöllinen osoite. Jokainen laite voi lähettää Modbus-komennon, vaikkakin yleensä vain yksi master-laite tekee sitä. Modbus-komento sisältää sen laitteen modbus-osoitteen, jolle komento on tarkoitettu. Vain tämä laite suorittaa komennon, vaikka kaikki laitteet voivat vastaanottaa komennon. Kaikki Modbus-komennot sisältävät tarkisteen, jolla varmistetaan komennon kulkeminen virheettömänä. Perus Modbus-komennot voivat käskeä kenttälaitetta vaihtamaan jonkin rekisterin arvoa, tai yhtä hyvin komentaa laite lähettämään takaisin yhden tai useamman arvon sen rekistereistä.

Monet modeemit tukevat Modbusia, ja jotkut niistä on erityisesti suunniteltu tälle protokollalle. Yhteys voi olla langallinen tai langaton (esimerkiksi SMS tai GPRS). Tyypillisimmät haasteet järjestelmän suunnittelussa ovat pitkät viiveet ja ajastukseen liittyvät ongelmat. [11.]

4.4 Rakennusautomaatio ja TCP/IP-protokolla

Vuonna 2007 Frost & Sullivan konsulttiyrityksen tekemän selvityksen mukaan, IP-pohjaisten rakennusautomaatiojärjestelmien käyttöönotto kasvu on kiihtynyt. Halvempien laitteiden ansiosta se on nykypäivänä varteenotettava vaihtoehto. Informaatioteknologia on vahva työkalu ja monet yrityksen pystyvät integroimaan jo olemassa olevaan IP-verkkoon rakennusautomaatioverkon luoden näin yhden ison verkkokokonaisuuden. Tämä mahdollistaa yhtenäisen helposti hallittava järjestelmän.

Uuden sukupolven IP-teknologia IP.v6 mahdollistaa lähes rajoittamattoman osoiteavaruuden. Varatut IP-osoitteet kasvavat eksponentiaalisesti, siksi on myös tärkeää että vapaiden IP-osoitteidenavaruus kasvaa.

IP-yhteysprotokollan joustavuus, helppous takaa kiinteistöille ja yrityksille mahdollisuuden luoda yhteensopiva ja helposti hallittava rakennusautomaatiojärjestelmä. IP-teknologian suurista valteista huolimatta, huono suunnittelu ja toteutus voi pilata lähes koko kiinteistön verkkoinfrastruktuurin ja aiheuttaa pahimmissa tapauksissa suurta aineellista vahinkoa. Siksi onkin tärkeää rakentaa tasapainoinen järjestelmä joka on niin kustannustehokas kuin sekä myös turvallinen. On havaittu että käyttäjien aiheuttavat ongelmat ovat suurin vahinkoriski ja tämä pitää ottaa huomioon järjestelmän suunnittelussa. [12.]

5 Esineiden internet

Esineiden internetillä (Internet of Things, lyhyemmin IoT) tarkoitetaan internetverkon laajentumista laitteisiin ja koneisiin, joita voidaan ohjata, mitata ja sensoroida internet-verkon yli. IoT:n käsite on ollut käytössä ensimmäisen kerran jo 1990-luvulla; englanninkielistä termiä ehdotti Kevin Ashton vuonna 1999.

Tiedon teollinen internet start-up-liiketoimintayksikön johtaja Taneli Tikka selitti kesällä 2015 ilmiötä näin: "IOT liittyy digitalisaatioon, ja se tapahtuu monella eri tavalla."

Digitalisaatio ei tarkoita palveluiden sähköistämistä, vaan sitä, että kun yksi asia digitalisoituu, koko ekosysteemi ja arvoverkosto sen ympärillä muuttuu. Näin on käynyt esimer-

kiksi kirjojen, musiikin, kuvien, karttojen ja matkustamisen digitalisoitumisen myötä. Television puolelta Tikka mainitsi pelkästään netissä toimivan Machinima-kanavan, jolla on 450 miljoonaa katsojaa.

Kun IOT:hen liittää sanat teollisuuden internet, se tarkoittaa, että seuraavaksi digitalisaatioon siirtyy perusvalmistava teollisuus. Jotta valmistava teollisuus pysyy elinkelpoisena, on kehitettävä jotain uutta ja innovatiivista. Tieto on jakanut teollisuuden toimintatavat kolmivaiheiseen horisonttimalliin. Ensimmäisessä vaiheessa teollisuusyritykset keskittyvät ydintoimintaansa ja rakentavat uutta vanhan päälle. Seuraavaksi yritykset tekevät kokonaan uusia tuotteita ja palveluita ja kolmannessa vaiheessa yritykset tekevät todella radikaaleja asioita. Esimerkki kolmannen vaiheen toiminnasta voisi olla se, että isot nosturit korvataan pienten robottien armeijalla.

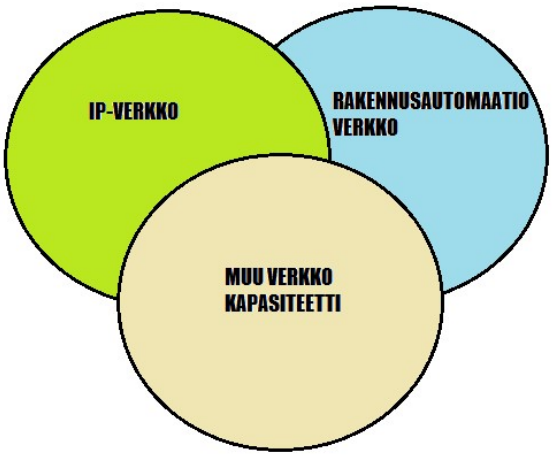
Kuvio 10. Esineiden internet -esimerkki

Teollisen internetin on ennustettu tavoittavan globaalisti 1,9 biljoonan dollarin markkinat vuonna 2020. On myös ennustettu, että mikäli suomalaiset yritykset lähtevät aktiivisesti rakentamaan roolia teollisen internetin alustojen ja ekosysteemien avaintoimijoina, voidaan Suomeen saavuttaa jopa 12 miljardin euron suuruiset investointien ja 48 000 työpaikan kasvunäkymät.

Gartnerin mukaan vuonna 2015 noin 4,9 miljardia laitetta on liitettynä verkkoon, kun vuonna 2020 vastaava lukumäärä on jopa 25 miljardia laitetta. Se tarkoittaa yli kolmea laitetta maapallon jokaista asukasta kohden. [13.]

Tulevaisuuden vision mukaan miljardit eri laitteet liitetään yhteen vuorovaikutukseen keskenään ja isompiin verkkoihin, mikä hämärtää fyysisen ja virtuaalisen maailman. Elämme edelleen murrosvaihetta, mutta hyvin pian kuluttajat eivät ole ainoastaan yhteydessä kanssaihmisiin, mutta he myös pystyvät vaikuttamaan helposti sekä mahdollisesti langattomasti omaan fyysiseen ympäristöön kuten kiinteistöön, autoon ja erilaisiin laitteisiin. Internet Protokollalla on ollut jo keskeinen rooli eri medioiden yhteensovittamisessa, ja sen odotetaan kasvavan entistä suuremmaksi esineiden internet -teorian mukaan.

Siirtymät ja suunnitelmat koskien täysin IP-pohjaisia kiinteistöjä ja talotekniikkajärjestelmiä ovat jo käynnissä monien valmistajien toimesta, sillä kustannussäästöt vanhoihin järjestelmiin verrattuna ovat kasvamassa entistä suuremmiksi.



Kuvio 11. Esimerkki yhteensovitetuista rinnakkaisverkoista

Esineiden internetin potentiaali tulee esille vahvasti esimerkiksi yritysrakennusrakentamisessa, mutta sama konsepti voidaan integroida kaikkiin kiinteistöihin. Kun käyttäjät tai asiakkaat astuvat toimistorakennukseen, hotelliin, sairaalaan, vähittäiskauppaan tai teatteriin, he harvoin miettivät, miten rakennustekniikka toimii. Oletus on aina, että kaikki toimii odotusten mukaisesti ja turvallisesti.

Uusien trendien tavoite on tuoda niin sanottu SmartBuild-infrastruktuuri, jonka tarkoitus olisi vastata paremmin tarpeisiin ja olla vuorovaikutuksessa reaaliajassa käyttäjän kanssa. Nopeasti muokattavissa käyttäjän mieltymysten mukaa. Päätavoite on supistaa verkkoja ja luoda helpompi järjestelmä.

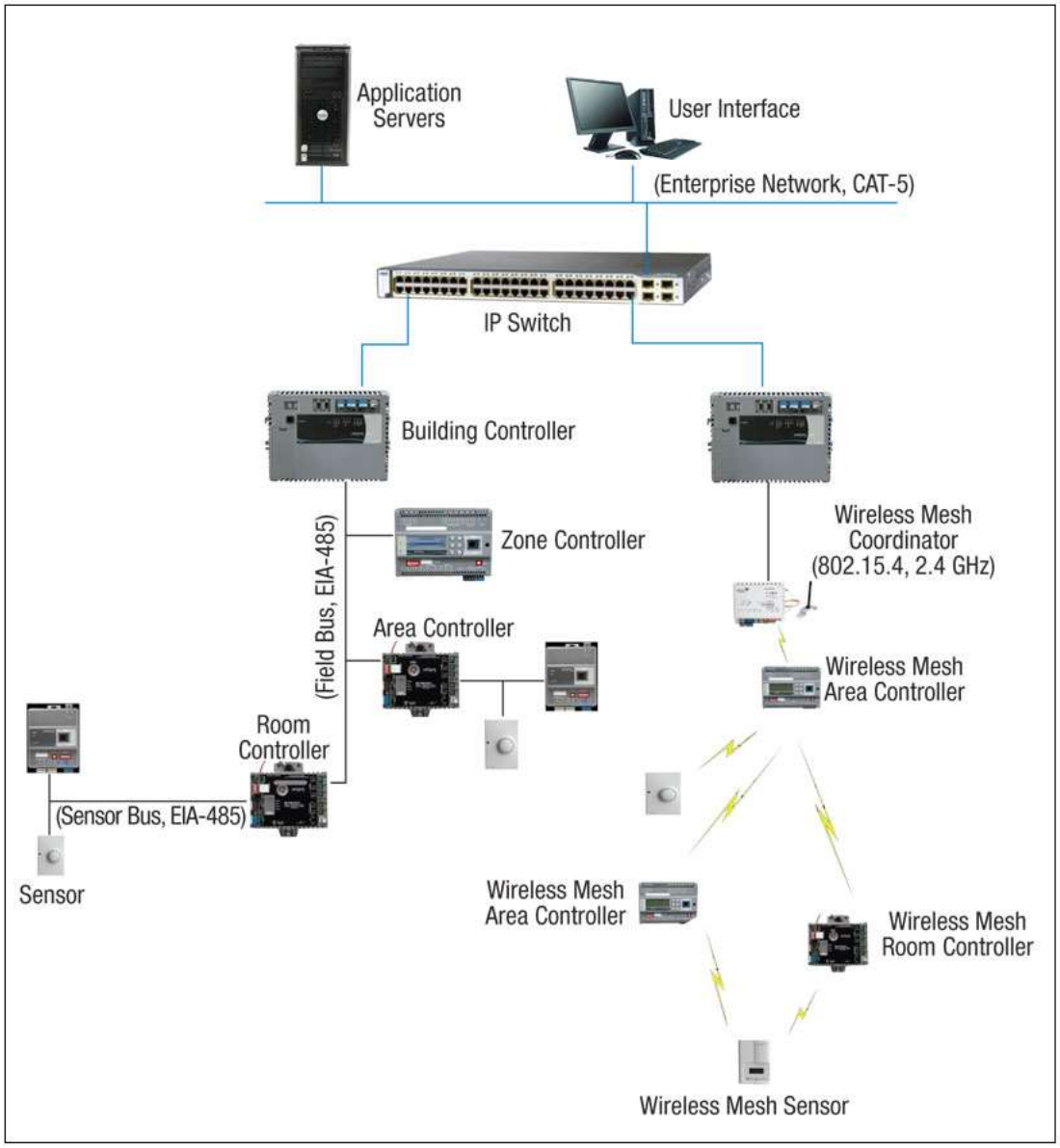
Nykypäivän kiinteistöjen verkot koostuvat yleensä kolmesta eri elementistä. IP-verkko pitää sisällään kaikki IT-laitteet kuten reitittimet, kytkimen sekä kaikki sovellukset ja käytössä olevat järjestelmät, jotka ovat kytköksissä ulkomaailmaan. Uudet paljon kaistaa varaavat järjestelmät, jotka vaativat luotettavaa reaaliaikaista turvallista väylää, on jaettu usein omaan varattuun verkkoon, jota käyttävät myös talotekniset ja rakennusautomaatiojärjestelmät.

Tällä hetkellä suurin osa rakennusautomaatioverkoista oli olemassa ennen IP-verkkoa, ja ne oli asennettu vuosikymmeniä sitten, nämä niin sanotut vanhat järjestelmät ovat laajalti edelleen käytössä

Vasta 2000-luvun alussa rakennusautomaatiojärjestelmät alkoivat tukea verkkokerrosta sekä ylläpitämään palveluita kuten HTML ja tukemaan muita web-teknologioita kuten Obixia ja BACnet Web Servicea. Tämä kehitys on edesauttanut suurten yhteensopivien laitemarkkinoiden kasvua.

Nyt on käyttäjällä mahdollisuus valita isosta eri laitevalmistajien valikoimasta, sillä laitevalmistajat tarjoavat rakennustekniikkalaitteissaan IP-rajapohjan yhteyden muodostamiseksi. Suosituimmat rakennusautomaatiojärjestelmät kuten BACnet/IP tai LON/IP ovat nykypäivää ja ne toimivat parikaapeleilla koko arkkitehtuurin läpi.

Uuden halvemman langattoman teknologian avulla IP mitä luultavammin saavuttaa vielä entistä isomman markkinaosuuden yhteysprotokollana esimerkkeinä 6LoWPAN- ja ROLL-teknologiat. Nykypäivän lähes kaikki rakennusautomaatiotekniikat käyttävät IP-teknologiaa ja ovat tämän vuoksi yhteensopivia eri laitteiden kesken.



Kuvio 12. Tyypillinen esimerkki nykypäivän talotekniikkaverkosta

IP-teknologia on samalla avannut aivan uudentyyppiset markkinat talotekniikkalaitevalmistajille, kun yhteensopivuus ei ole enää ongelma. Tällöin laitteita voidaan kytkeä yhteen IoT-teorian mukaan. Esimerkkinä ovat terveydenhuollon markkinat. Sairaalat sisältävät lukemattomia pitkälle tilaustyönä tehtyjä laitteita ja sovelluksia, joiden tarkoitus on olla helposti saatavilla henkilökunnalle ja asiakkaille.

Tutkimusten mukaan verkkojen yhdistäminen yhdeksi isoksi järjestelmäksi lisää selviä säästöjä. Eräät tutkimukset ovat osoittaneet, että talotekniikan ja IP-verkon yhdistäminen säästää:

- 50 % vähemmän yksittäisiä käytäviä (gateway)
- 20 % vähemmän asennus ja integrointi kustannuksia
- 20 % vähemmän energiakustannuksia
- 30 % vähemmän kunnossapito kustannuksia.

Näiden säästöjen lisäksi esimerkiksi äänidata ja video-data voidaan yhdistää IP-verkkoon kustannusten vähentämiseksi. Järjestelmät helppous ja etäkäyttö mahdollistavat henkilökunta vähennykset, ja reaaliaikainen etävalvonta on suuri etu ennenkin kunnossapitoa ajatellen.

Luotettavuus ja reaaliaikaisuus ovat tärkeitä elementtejä etenkin talotekniikkalaitteille ja niitä hallinoivia järjestelmiä ajatellen. Nykypäivänä käyttäjäkeskeisessä ja digitaalisesti muodostettujen verkkojen maailmassa tarvitaan nopeita reaaliaikaista tietoa käsitteleviä yhteyksiä, ja IP-pohjainen järjestelmä täyttää nämä vaatimukset edullisesti ja helposti erilaisilla joustavilla ratkaisulla.

Esineiden internet koostuu erilaisista älykkäistä IP-objekteista, jotka yleensä koostuvat pienistä mikroelektronisista laitteista, jotka taas koostuvat viestintälaitteesta, joka on tyypillisesti pienitehoinen radio pienestä mikroprosessorista, anturista tai aktuaattorista.

Uudet IP-protokollat ja teknologiat suunnitellaan kehitetään erityisesti älykkäille IP-objekteille erityisesti antureille ja aktuaattoreille eli toimilaitteille, esimerkiksi sähkömoottori- tai hydrauliikkalaitteille, joka toimii osana talotekniikkaa, tehdasta ja älykkäissä rakennuksissa. Näiden uusien teknologien käyttö mahdollistaa entistä tehokkaamman verkonresurssien käytön ja tarjoaa uusia mahdollisuuksia, mikä ei ollut ennen mahdollista.

Kehittyneempien pakkausmenetelmien ansiosta tietoa pystytään siirtämään isommissa määrin käyttäen vähemmän kaistaa. Tarkasti asetettu reititys osaa ottaa huomioon ainutlaatuiset ominaisuudet koskien talotekniikkalaitteita. Näin IP-protokolla pääsee laitetasolle asti, jolloin itse verkon reunalaitteet ovat pullonkaula.

Verkkojen yhdistäminen käyttäen IP-protokollaa nojautuu olennaisesti yhteensopivuuteen. IP-verkko tukee monenlaisia sovelluksia ja palveluita. Tämä ei ainoastaan edesauta uusien innovatiivisten ratkaisujen kehitystä, mutta johtaa voimakkaasi kokonaiskustannuksien ja monimutkaisuuksien vähennykseen yhdistäen erilaiset verkot keskenään yhteisellä standardilla.

Historia puhuu puolestaan jo reilut 30 vuotta sitten kehitetty IP-protokolla, joka tuki alussa hidasta tiedonsiirtoa, on kehittynyt huimasti ja pystyy toimimaan väylänä valtaville tietomäärille. Jatkuvan kehityksen ansiosta IP-teknologia tulee säilyttämään kilpailukykynsä myös tulevaisuuden talotekniikkamarkkinoilla. [14.]

Alla on joitakin esimerkkejä IP-verkon ominaisuuksista, joita voidaan hyödyntää talotekniikassa:

Ryhmälähetys (multicast) tarkoittaa tietoliikenteessä joukko-, moni- tai ryhmälähetystä. Siinä multicast-kehys lähetetään yhdeltä monelle. Kohdejoukko on tietty erikseen määritelty ryhmä, johon vastaanottajat voivat halutessaan liittyä.

VPN (Virtual Private Network) eli virtuaalinen erillisverkko on tapa, jolla kaksi tai useampia yrityksen verkkoja voidaan yhdistää julkisen verkon yli muodostaen näennäisesti yksityisen verkon. Nykyisin VPN-määritelmä on laajennettu koskemaan myös yksittäisten etätyöasemien liittämistä yrityksen verkkoon. [15.]

VPN-verkon yksityisyys ja tietoturva voidaan hoitaa joko fyysisesti tai salauksella. Asiakkaan verkkoja yhdistävä VPN voi siis perustua jommallekummalle seuraavista:

- perinteiset suljetut verkot, kuten operaattoriverkot fyysisellä suojauksella
- julkiset ja avoimet verkot, kuten salattu Internet.

QoS (engl. Quality of Service) on termi, jolla tarkoitetaan tietoliikenteen luokittelua ja priorisointia. Priorisoinnin perusteella osaa liikenteestä voidaan hidastaa tai jopa pudottaa kokonaan pois, mikäli linjojen välityskyky ei riitä. Liikennettä voidaan priorisoida sovellusten, käyttäjien tai käytettyjen tietokoneiden perusteella.

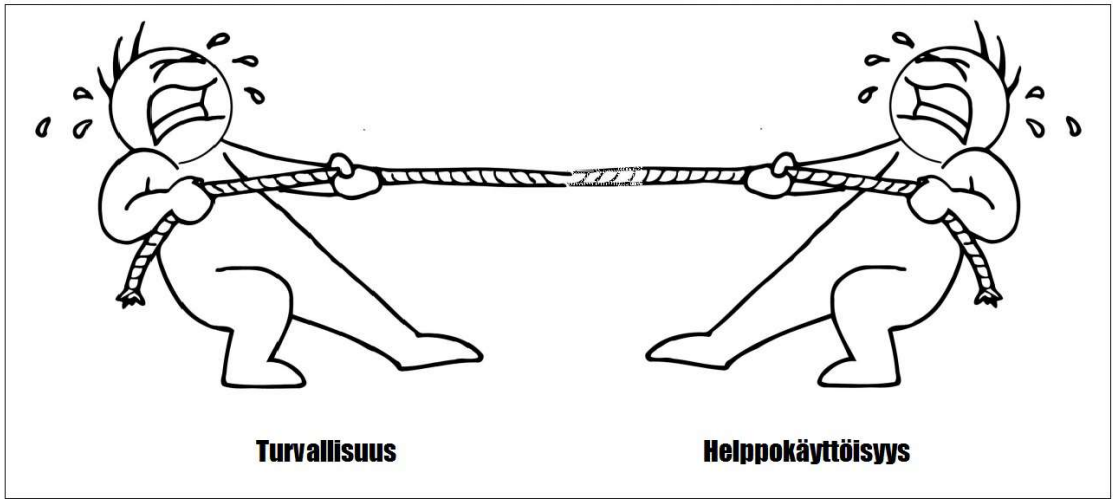
QoS-tekniikoita on kahdenlaisia. Luokittelutekniikat keskittyvät QoS-tiedon jakamiseen ja liikenteen luokitteluun, kun taas suodintekniikat ovat erilaisia algoritmeja itse reitittimissä, jotka toteuttavat itse suodatusta ja priorisointia. [16.]

Luotettavuuden säilyttämiseen on kehitetty useita tekniikoita tarjoamaan luotettavan kaistan tiedonsiirtoa varten käyttäen esimerkiksi redundanssia. Tapa laskee uuden reitin millisekunneissa säilyttäen verkon torjuen näin mahdolliset viat tai hidastavat haitat. Toisin sanoen verkko voi älykkäästi automatisoituna etsiä vaihtoehtoisia reittejä, jos alkuperäinen kaista on poikki.

Turvallisuus on talotekniikassa tärkeä osa-alue, ja hyvin suunniteltu IP-verkko on erittäin turvallinen, kun taas vastakohtana huonosti suunniteltu tulee aiheuttamaan harmia esimerkiksi mahdollisten hyökkäysten johdosta.

6 Talotekniikka ja turvallisuus

Hyvin suunniteltu SmartBuilding-turvallisuusjärjestelmä vähentää riskien määrää huomattavasti. Suunnitelmassa otetaan huomioon niin itse suunnittelu, asennus sekä käyttö. Käsitteenä tämä on vielä uusi mutta etenkin yritysmaailmassa on asiaan alettu kiinnittämään entistä enemmän huomiota. Tarve luoda turvallinen ympäristö ja torjua siihen kohdistuvat uudet uhat on nykypäivää uusissa moderneissa rakennuksissa.



Kuvio 13. Turvallisuuden ja helppokäyttöisyyden tasapaino

IoT ideologia tuo helppokäyttöisyyden lisäksi aivan uudet ongelmat talotekniikkaan kuten esimerkiksi cyber-hyökkäykset ja erilaiset haittavaikutukset, jotka tapahtuvat IP-verkon ylitse ja voivat yltää aina verkossa oleviin talotekniikkalaitteisiin.

Vuonna 2016 eräs SmartBuilding-rakennus kävi läpi kokeellisen testin IBM:n X-Force hakkeritutkijaryhmän toimesta. Päämääränä oli löytää ja alleviivata potentiaaliset riskit koskien IoT-ideologiaa.

IBM-tutkijat osoittivat, että rakennuksen niin sanotut älykkäät kiinteistön automaatiojärjestelmät ovat tällä hetkellä turvallisuusriski yrityksille. Tutkimusinstituutti Gartnerin mukaan älykkäät kodin laitteet ja yritysten älykkäät laitteet ovat 45 prosenttia koko maailmanlaajuisen verkon kapasiteetista.

IBM X-Force -raportin mukaan kaikki laitteet, jotka on yhdistetty verkkoon, niin kodin laitteet kuten myös talotekniikkajärjestelmät ovat nykypäivänä samojen uhkien alaisia. Rakennuksen ilmastointi, valaistus ja lämpö ovat kaikki mahdollisia kohteita nykypäivänä.

IBM:n tietoturva-asiantuntijat osana penetraatiotestiä valitsivat suorittivat testin omasta aloitteesta ja valitsivat satunaisen rakennuksen, joka on niin sanottu moderni SmartBuilding ja IoT-ratkaisuja käyttävä kiinteistö. He hakkeroivat kiinteistön verkkoinfrastruktuuriin osoittaakseen nämä ongelmat. He todistivat, että nykypäivän SmartBuilding-suojausmenetelmät ovat heikkoja.

Useimmat nykyiset talotekniikan automaatioratkaisut (BAS, Building Automation Systems) toimivat samalla tavalla. Kukin rakennus pitää sisällä oman BAS-ohjaimen, joka on vastuussa rakennuksin älykkäistä ratkaisuista kuten tiedonkeräys ja ohjauskäskyjen antamisesta. Sensorit ja anturit on esimerkiksi kytketty ilmastointiin ja erilaisiin ilmankosteusmittareihin. Tämä BAS-ohjain on taas kytketty internetverkkoon WiFi:n ja rakennuksen oman reitittimen kautta, josta se osissa tapauksissa lähettää tiedot eteenpäin laitevalmistajalle, huoltoyritykselle tai esimerkiksi yrityksen pääkonttoriin, jotka keräävät tiedon pääpalvelimiin ympäri maata.

IBM:n X-Force tutkija Paul Ionescu kirjoitti omassa blogissaan, kuinka näille älykäs toimisto teknologia laitteille on annettu vähän huomiota tietoturvariskejä ajatellen koska nämä uudet älykkäät ratkaisut eivät ole vielä osa perinteistä IT-infrastruktuuria. Itseasiassa, viimeisimmän tutkimuksen mukaan koskien BAS-järjestelmiä osoittaa että vain 29

prosenttia toimijoista on ryhtynyt parannustoimiin tai aikovansa ryhtyvän toimiin parantaakseen BAS-verkkojen turvallisuuta IoT-ideologia ajatellen.

Osoittaakseen nämä haavoittuvuudet Paul Ionescu ja ryhmä X-Force tutkijoita laittoivat omat kyvyt koetukselle ja suorittivat eettiset hakkerointi harjoituksen murtautumalla nimettömään SmartBuild-toimistorakennuksen verkkoon Pohjois-Amerikassa. Testi suoritettiin tarkoituksena murtaa pääseuranta- ja valvontapalvelin, joka ohjaa paitsi kyseistä rakennusta sekä on myös yhteyksissä muihin Pohjois-Amerikassa oleviin toimistoihin.

Tutkijat olivat yllättyneitä perustietoturva virheiden määrästä, jotka mahdollistivat murtautumisen järjestelmään. Toimenpiteet kuten jaetut salasanat ja suojaamaton data, joka säilytettiin lukumuotoisena tekstinä, mahdollistivat heille mahdollisuuden murtautua loppujen lopuksi pääpalvelimelle. Haavoittuvan palvelimen lisäksi he pystyivät myös paikallistamaan reitittimen sekä itse BAS-hallintalaitteen.

Ohjelmistovirhe rakennusautomaation järjestelmän diagnostiikkasivulla mahdollisti X-Force-tutkijoille pääsyn laitteen asetuksiin ja sitä kautta myös sen sisältämiin salasanoihin. Sieltä he pystyivät purkamaan salasanat ja löysivät salasan pääpalvelimelle, joka ohjaa useita eri asemia ympäri Pohjois-Amerikkaa sijaitsevia rakennuksia.

Tutkijat ajoivat itse laitoksen viereen, jossa ohjelmistoa käytettiin ja pystyivät pääsemään päähallintapalvelimelle käyttämällä aikaisemmin saatua salasanaa ja kiinteistön omaa WiFi-verkkoa.

Tämän lisäksi IBM:n X-Force-tutkijat pystyivät muuttamaan rakennuksen perusolosuhteita kaikissa yrityksen rakennuksissa. He myös onnistuivat saamaan pääsyn rakennuksen sähköisiin ovilukkoihin, palohälyttimiin, turvajärjestelmiin ja jopa kylmäkalusteisiin jättäen koko rakennuksen auki mahdolliselle fyysiselle murrolle.

IBM ilmoitti, että heikko tietoturvallisuus, avoin internetyhteys ja haavoittuva hallintajärjestelmä on yleinen tietoturvariskiyhdistelmä joka tekee yrityksistä haavoittuvaisia tai jopa yrityksistä, jotka toimivat vain kiinteistövuokraajina. Tämä jättää rakennuksen alttiiksi tietoturvahyökkäyksille, sanoi Diana Kelly, IBM:n turvallisuusneuvonantaja.

Kuvio 14. IBM, Building Operating Management survey 2015

IBM on työskennellyt yhteistyössä mainitun yrityksen kanssa ja on ollut myös yhteydessä kiinteistöautomaatiovalmistajan kanssa ilmoittaen heille heidän havaitsemat haavoittuvuudet.

X-Forcen suorittama penetraatiotesti toi esille paljon näkökantoja, jotka koskevat BAS-järjestelmien tietoturvaa. Heidän koetulokset tullaan esittämään vuonna 2016 InterConnect-tieturvakonferenssissa.

SmartBuilding-konseptin turvallisuus on suhteellisen uusi huolenaihe. Ennen talotekniikka ja automaatio oli kytketty omaan verkkoon ja järjestelmään, mutta nykypäivänä helppokäyttöisyyden vuoksi kaikki kytketään samaan IP-verkkoon ja samoihin palvelimiin.

Monista vanhoista standardeista on luovuttu ja siirrytty käyttämään uusia ratkaisuja. Vaikka nämä järjestelmät saattavatkin olla taloudellisesti ja käyttömukavuudeltaan parempia, niin turvallisuus joudutaan usein miettimään uudelleen välttääkseen uudet riskit. [17.]

6.1 Turvallisuuden suunnittelu

Turvallisuuden pääpaino suunnittelussa on luoda raja kiinteistön verkon ympäri ja tarjota useita tapoja seurata, hallita ja valvoa verkkoon pääsyä. Päätöksen suunnittelun aikana vaikuttavat suuresti tulevaisuuden mahdollisuuksiin. Siksi onkin tärkeää, että kaikki sidosryhmät kuten valvojat, käyttäjät kommunikoivat keskenään, ja turvallisuuden tarve selvitetään jo etukäteen. Fyysinen turvallisuus, verkon infrastruktuuri ja laitevalinta ovat suunnittelun tärkeitä elementtejä.

Fyysisellä turvallisuudella tarkoitetaan yleensä kiinteistön omia turvallisuutta edistäviä rajoja kuten ovet, sijainti ja mahdollinen fyysinen valvonta. Vasta kun fyysinen turvallisuus on ratkaistu, on järkevää siirtyä itse verkon suojaukseen.

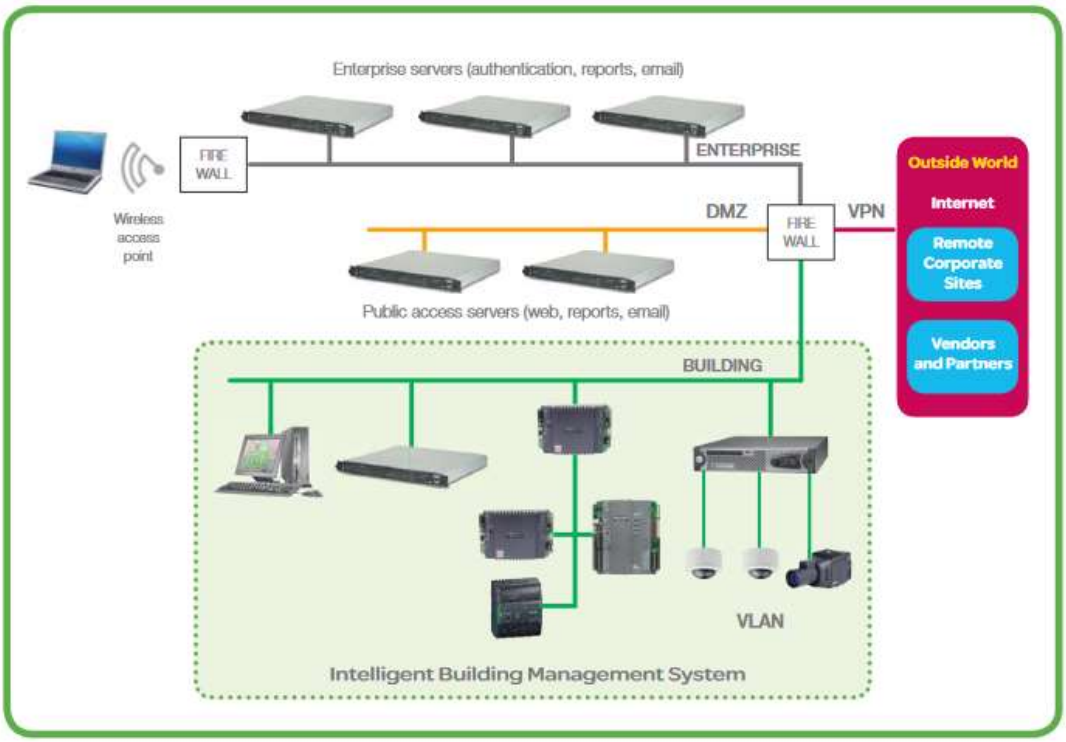
Asioita, jotka kannattaa ottaa huomioon esimerkiksi palvelinhuoneen suunnittelussa:

- mahdolliset fyysiset esteet kuten ovet, serverikaapit ja kulunvalvonta
- asiattomien pääsyn estäminen
- kaistakaapelien suojaus.

Verkon turvallisuudella taas tarkoitetaan tiedonsiirron suojausmenetelmiä kiinteistön älykkäiden laitteiden välillä sekä rajapintaa ulkomaailmaan, jonka kautta asiattomat henkilöt voivat mahdollisesti tunkeutua.

Verkon turvallisuuden parantamiseksi voidaan tehdä lukuisia muutoksia kuten esimerkiksi verkon rajoittaminen segmentointi ja päätepisteiden rajoittaminen, käyttäjien tarkka

lajittelu ja oikeuksien jakaminen sekä lukuisat järjestelmät kuten aikaisemmin mainittu VPN ja palomuuri. [18.]



Kuvio 15. Esimerkki tyypillisestä verkon infrastruktuurista.

6.2 Palomuuri

Tietoverkoissa palomuuri (Firewall) on eristävä moniosainen järjestelmä, joka suodattaa suojattavan verkon ja vaarallisemman verkon välisiä yhteyksiä.

Useimmiten palomuuria tarvitaan avoimesta internetyhteydestä tulevilta hyökkäyksiltä suojautumista varten. Palomuurilaitteilla on sääntöjä, joilla sisään tulevista yhteyksistä suodatetaan pois kaikki muu, paitsi tarvittava minimi. Nykyisin on myös yleistä, että vastuuntuntoisesti suodatetaan myös ulkomaailmaan lähtevää liikennettä, jotta oman verkon asiakkaat eivät voi häiriköidä muiden verkkoihin (esimerkiksi väärennetyillä lähdeosoitteilla). Useiden yritysten sisällä suositaan työntekijöiden koneilta ulospäin lähtevän liikenteen kontrollointia palomuurin avulla muun muassa tietosuojan turvaamiseksi.

Kokonaisvaltainen palomuurijärjestelmä koostuu useimmiten kahdenlaisista komponenteista:

- pakettisuodatin
- yhdyskäytävä.

Palomuuri saattaa vastaanottaa ohjeita tunkeilijan havaitsemisjärjestelmältä estettävästä liikenteestä.

Useimmiten palomuureja on isommissa yritysverkoissa useampia. Palomuurien perusongelma on, että niiden läpi hyökännyttä murtautujaa ei voida enää estää tekemästä tuhojaan. Niinpä yrityksillä on eteisverkko eli demilitarisoitu alue (demilitarized zone, DMZ), joka sijaitsee luotetun sisäverkon ja Internetin välissä. Internetin ja eteisverkon sekä eteisverkon ja sisäverkon välissä ovat palomuurit. Eteisverkkoon sijoitetaan kaikki julkiset palvelimet. Vaikka tunkeutuja pääsisi murtautumaan kyseisille palvelimille, olisi hänellä vielä toinen palomuuri edessään ennen sisäverkkoa.

Tosiasiassa nykyiset palomuurilaitteet osaavat toteuttaa jopa useita erilaisia eteisverkkoja sisältävän konfiguraation yhdellä laitteella. Palomuurilaitteeseen vain lisätään verkkoliittymiä, ja sille määritetään, onko liittymän takana luotettu verkko, täysin turvaton verkko vai jotain siltä väliltä. [19.]

6.3 Käyttäjien hallinta

Verkon suojattu käyttö voidaan saavuttaa käyttäjien todentamisella ja heille myönnettyjen oikeuksien tarkoilla hallintakeinoilla kuten esimerkiksi autentikoinnilla, jolloin käyttäjä saa hänen käyttöön myönnetyt oikeudet organisaation sisälle. Tätä käytäntöä kutsutaan rooliksi.

Käytäntöä voidaan edelleen parantaa salasanoilla, määritetyillä kulkuoikeuksilla verkon sisällä kuten pääsyllä tietyille palvelimille ja reitittimille.

Käyttäjien todentamista voidaan parantaa myös entisestää erilaisilla fyysisillä tunnisteilla kuten esimerkiksi ID-korteilla, USB-tikuilla ja biometrisillä tunnisteilla. Nämä menetelmät voidaan yhdistää edellä mainittuihin.

6.3.1 Active Directory

Active Directory (AD) on Microsoftin Windows -toimialueen käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. Se mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja sovelluksille sekä tarjoaa tavan nimetä, kuvata, paikallistaa, hallita ja suojata käytössä olevia verkon resursseja.

Active Directory -hakemistopalvelu on sisälletty Microsoft Windows Server 2012-, Microsoft Windows Server 2008-, Microsoft Windows Server 2003 - ja Microsoft Windows Server 2000 -käyttöjärjestelmiin. [20.]

6.3.2 Kerberos

Kerberos on todennusprotokolla. Kerberoksen avulla käyttäjät voivat todistaa henkilöllisyytensä toisilleen verkon yli, ja se on suunniteltu käytettäväksi internetin kaltaisissa verkoissa, joissa ei suoraan ole salausmenetelmää käytössä. Kerberos perustuu Needhamin ja Schroederin avaintenjakomalliin. Käyttäjien todennuksen lisäksi Kerberos estää salakuuntelun ja tunnistaa, jos viestiä on muokattu matkalla. [21.]

7 Loppupäätelmä

Työn loppupäätelmä on, että talotekniikka kehittyy kovaa tahtia juuri IoT-konseptia noudattaen ja että tarve integroida talotekniset laitteet helpoksi hallittavaksi kokonaisuudeksi käyttäjille on suuri.

Helppokäyttöisyyden lisäksi TCP/IP-protokollalla toimiva talotekninen järjestelmä on kustannustehokas ja energiaa säästävä etenkin kestävää kehitystä ajatellen. Jatkuvasti kehittyvät teknologiat tarjoavat useita joustavia ratkaisuja ja vaihtoehtoja käyttäjille.

Automaation lisäksi etäkäyttö mahdollistaa nopeat muutokset järjestelmään, jolloin mahdollisilta henkilökuluilta voidaan säästyä, sillä erilaisten muutosten tekeminen esimerkiksi ilmanvaihtoon tai kiinteistön lämmitykseen ei välttämättä enää vaadi huoltomiehen käyntiä.

Erilaiset langattomat ratkaisut ovatkin nykypäivää uusissa kiinteistössä samalla, kun vanhoja kiinteistöjä uudistetaan näillä teknologioilla. On kuitenkin vaikea sanoa, luovutaanko vanhoista verkkomenetelmistä joskus tai jos ollenkaan, sillä järjestelmän modernisoitin kustannus, joka on koko ajan muuttumassa edullisemmaksi, voi olla silti edelleen esteenä. Monet käyttäjät eivät myöskään näe tarvetta modernisoida kiinteistön vanhoja järjestelmiä omien tottumuksiensa vuoksi.

On kuitenkin todennäköistä, että nämäkin järjestelmät uudistuvat ennen pitkää ja Smart-Building ja kestävä kehitys -konsepti saavan enemmän jalansijaa.

Uudisrakennuksissa tilanne on kuitenkin avain toisenlainen, sillä moderni käyttäjäystävällinen kiinteistö on monille imagokysymys etenkin yritysmaailmassa.

Uusi teknologia tuo kuitenkin mukanaan omat ongelmat ja riskinsä. Jatkuva kamppailu turvallisuuden ja käyttömukavuuden välillä korostuu etenkin tässä, sillä TCP/IP-verkot sisältävät omat riskinsä, mitä ei ennen ole talotekniikassa nähty.

Kuten useiden uutisotsikoiden ja IBM X-Force-tutkimuksen mukaan fiktiosta voi tulla totta, ja tietomurto rakennuksen taloteknisiin laitteisiin voi aiheuttaa todellisia vaurioita niin laitteille kuin itse fyysisesti rakennukselle ja jopa ihmisille. Ongelmana on myös, että konsepti on edelleen tuore ja hankkijoilta sekä jopa valmistajilta puuttuu kyky sekä tieto tietoliikenteen turvallisuuden takaamisesta.

On kuitenkin selvää, että kuten sähköautot, esineiden internet niin myös talotekniikka tulee kehittymään samanlaiseen suuntaan ja täten verkostoitumaan osaksi isompaa jokapäiväistä kokonaisuutta.

Lähteet

1 Harcourt Brown & Carey. 2015. A Brief History Of Building Automation and Controls. .<http://www.harcourtbrown.com/a-brief-history-of-building-automation-and-controls> 2015 Luettu 1.3.2017

2 Wikipedia. 2017. Verkkodokumentti. <https://fi.wikipedia.org/wiki/Rakennusautomaatio>. Luettu 1.3.2017.

3 Wikipedia. 2017. Verkkodokumentti. <https://en.wikipedia.org/wiki/Building_automation>. Luettu 1.3.2017.

4 Sisäilmayhdistys Ry, perustietoa sisäilmasta. 2017. Verkkodokumentti. <http://www.sisailmayhdistys.fi/Perustietoa-sisailmasta/Ilmanvaihdon-perusteet>. Luettu 15.3.2017.

5 Liedes, Riikka. 2013. Rakennuksen lämpökuormat sekä lämmityksen ennakoiva ja sääennustepohjainen säätö. Diplomityö. Aalto-yliopisto.

6 Wikipedia. 2017. Verkkodokumentti. <https://fi.wikipedia.org/wiki/Digital_Addressable_Lighting_Interface>. Luettu 17.3.2017.

7 Wikipedia. 2017. Verkkodokumentti. <https://fi.wikipedia.org/wiki/Vesihuolto>. Luettu 20.3.2017.

8 Wikipedia. 2017. Verkkodokumentti. <https://fi.wikipedia.org/wiki/Kulunvalvonta>. Luettu 21.3.2017.

9 Piper, James 2007. BACnet, LonMark and Modbus: How and Why They Work. Verkkodokumentti. <http://www.facilitiesnet.com/buildingautomation/article/BACnet-LonMark-and-Modbus-How-and-Why-They-Work-Facilities-Management-Building-Automation-Feature--7712>. Luettu 22.3.2017.

10 Wikipedia. 2017. Verkkodokumentti. <https://en.wikipedia.org/wiki/BACnet>. Luettu 24.3.2017.

11 Wikipedia. 2017. Verkkodokumentti. <https://en.wikipedia.org/wiki/Modbus>. Luettu 25.3.2017.

12 Cisco. 2008. Building Automation System over IP (BAS/IP) Design and Implementation Guide. Verkkodokumentti. <http://www.cisco.com/c/dam/en_us/solutions/industries/docs/trec/jControls_DIG.pdf>. Luettu 28.3.2017.

13 Wikipedia. 2017. Verkkodokumentti. <https://fi.wikipedia.org/wiki/Esineiden_internet>. Luettu 1.4.2017http://rtcmagazine.com/articles/view/101879

14 RTC Magazine. 2010. The Internet of Things and the Convergence of Networks. Verkkodokumentti. <http://rtcmagazine.com/articles/view/101879>. Luettu 1.4.2017.

15 Wikipedia. 2017. Verkkodokumentti. <https://fi.wikipedia.org/wiki/VPN>. Luettu 2.4.2017.

16 Wikipedia. 2017. Verkkodokumentti. <https://fi.wikipedia.org/wiki/QoS>. Luettu 4.4.2017.

17 CSO Online. 2016. Verkkodokumentti. <http://www.csoonline.com/article/3031649/security/ibms-x-force-team-hacks-into-smart-building.html>. Luettu 5.4.2017.

18 Schneider Electric. 2011. Best Practices for Securing an Intelligent Building Management System. Verkkodokumentti. <http://www.schneider-electric.com/solutions/ww/...facility-intelligent...system/med/4664764/application/pdf/1222_wp_bestprac_us_final.pdf>. Luettu 7.4.2017.

19 Wikipedia. 2017. Verkkodokumentti. <https://fi.wikipedia.org/wiki/Palomuuri>. Luettu 8.4.2017.

20 Wikipedia. 2017. Verkkodokumentti. <https://en.wikipedia.org/wiki/Active_Directory>. Luettu 9.4.2017.

21 Wikipedia. 2017. Verkkodokumentti. <https://en.wikipedia.org/wiki/Kerberos_(protocol)>. Luettu 13.4.2017.