Samuli Saari

ÄLYTALON OHJELMISTORATKAISUT JA TIETOTURVA

Automaatiotekniikan koulutusohjelma

2016

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

ÄLYTALON OHJELMISTORATKAISUT JA TIETOTURVA

Saari, Samuli
Satakunnan ammattikorkeakoulu
Automaatiotekniikan koulutusohjelma
Huhtikuu 2016
Ohjaaja: Asmala, Hannu
Sivumäärä: 30
Liitteitä: 0

Asiasanat: automaatio, älytalot, rakentaminen

Opinnäytetyön tarkoituksena oli keskittyä tarkastelemaan erilaisia ohjelmistoratkaisuja joita älytaloon ja kiinteistöautomaatioon liittyy. Toinen pääasia oli tietoturva joka tulee esille älytaloa suunnitellessa. Ohjelmistoratkaisut voidaan jakaa karkeasti kahteen ryhmään: avoimiin järjestelmiin ja suljettuihin järjestelmiin.

Ohjelmistoratkaisujen lisäksi opinnäytetyössä keskityttiin myös järjestelmän elinkaareen ja sen elinkaaren aikana mahdollisesti vastaantuleviin ongelmiin. Tällaisia ongelmia voi tulla vastaan esimerkiksi laajennettaessa tai päivitettäessä järjestelmää.

Älytalon järjestelmiin liittyy läheisesti käsite esineiden internet eli Internet of Things, IoT. Jo nyt älytaloissa voidaan hyödyntää IoT-laitteita ja tulevaisuudessa niiden määrä lisääntyy arvioiden mukaan todella paljon. Tämä tarkoittaa samoja haasteita kuin muissakin IoT-järjestelmissä, esimerkiksi tietoturva-asioiden huomioon ottamista.

Yksi tärkeä asia opinnäytetyössä oli myös kustannusten vertailu. Kustannuskysymykset ovat erittäin tärkeä asia kun ollaan suunnittelemassa älytaloa. Älytaloon liitettävän automaation kustannukset riippuvat suuresti siitä, millainen järjestelmä valitaan. Kustannusten vastapainoksi odotetaan usein joko pidemmän aikavälin säästöjä, asumismukavuuden parantumista tai molempia. Suunnittelemalla juuri oikeanlainen järjestelmä on mahdollista saavuttaa molemmat. Talon jälleenmyytiarvoon kiinteistöautomaatiolla saattaa olla positiivinen vaikutus, mutta sitä on toistaiseksi vaikea arvioida.

AUTOMATION SOLUTIONS AND INFORMATION SECURITY OF SMART HOMES

Saari, Samuli
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Automation Technology
April 2016
Supervisor: Asmala, Hannu
Number of pages: 30
Appendices: 0

Keywords: automation, smart homes, building

The purpose of this thesis was to focus on the possible solutions that are needed when building a house with large amounts of home automation as well as the security of a house equipped with home automation systems. The solutions can be roughly divided into two distinctive categories: open systems and closed systems.

Along with the system comparison, part of the thesis was dedicated to the possible problems the homeowners face during the life cycle of the automated house. Such things include upgrading, updating and expanding the automation system.

One important point in the thesis was considering how cost-effective a large-scale automation system is. Home automation is a relatively new thing and the cost of the parts depends on which type of system is chosen. It is imperative that the cost is factored in to the decision when deciding whether or not to invest in such a system. When investing in home automation there are usually some expectations to be able to save money in long term or gain some sort of living condition improvements from home automation. With a carefully planned smart home system it's possible to get both. The resell price of a house might also increase from a well-conducted home automation system but currently it's too early to say this.

SISÄLLYS

1 JOHDANTO

Älytalo on talo, joka sisältää huomattavan määrän kotitalouksiin tarkoitettua kiinteistöautomaatiota. Älytalojen rakentaminen on lisääntynyt laitteistojen ja järjestelmien kehityttyä. Samalla kilpailevien järjestelmien määrä on kasvanut ja markkinoilla on useita hyvin samanlaisia järjestelmiä, joilla voidaan toteuttaa älytalon automaatio.

Kiinteistöautomaatio ja siinä käytettävät laitteet ovat hyvin pitkälti samoja kuin teollisuudessakin käytettävät laitteet. Monet teollisuusautomaatiotuotteita valmistavat yritykset valmistavat myös kiinteistöautomaatiotuotteita ja iso osa teollisuusautomaatiolaitteista voidaan suoraan hyödyntää myös kiinteistöjen asennuksia tehdessä. Tämä tekee järjestelmän valinnasta huomattavasti vaikeamman. Usein kuitenkin automaatiosuunnittelija tekee valinnan eikä rakentajan tarvitse huolehtia järjestelmän valinnasta tai asennuksesta. Erityisesti asiaan perehtyneet harrastajat saattavat kuitenkin valita ja jopa asentaa itse oman järjestelmänsä mikäli heillä on siihen tarvittavat luvat ja osaaminen. Osa järjestelmistä ei edes vaadi varsinaisia lupia, joten kynnys tehdä oma järjestelmä on suhteellisen matala. Itse tehtyjen komponenttien käyttäminen vähentää kustannuksia edelleen.

Kustannuskysymysten lisäksi älytalon rakentamiseen liittyy muitakin avoimia kysymyksiä, joita pitää ottaa huomioon suunnittelun aikana. Erityisesti turvallisuusnäkökohdat kuten virukset ja järjestelmän joutuminen hakkerien uhriksi aiheuttaa huolta omistajien keskuudessa. Tällaiset asiat on otettava huomioon ennen järjestelmän rakentamista. Mikäli talon automaatiojärjestelmä ei ole yhdistettynä internetiin, suojaus on jo kohtuullisen hyvällä tasolla. Pahimmat ongelmat tulevat esiin, jos järjestelmä on kytketty internetiin ja on näin haavoittuvainen ulkoisille uhille kuten hakkereille. Mikäli suunnitteluvaiheessa tietoturva on kokonaan laiminlyöty, on mahdollista, että hakkeri saa yhteyden järjestelmään ja näkee sekä kaikki asunnon tiedot että pystyy säätämään niitä. Pelkkä salasanasuojaus ei riitä sillä niiden murtaminen on pahimmassa tapauksessa jopa helppoa.

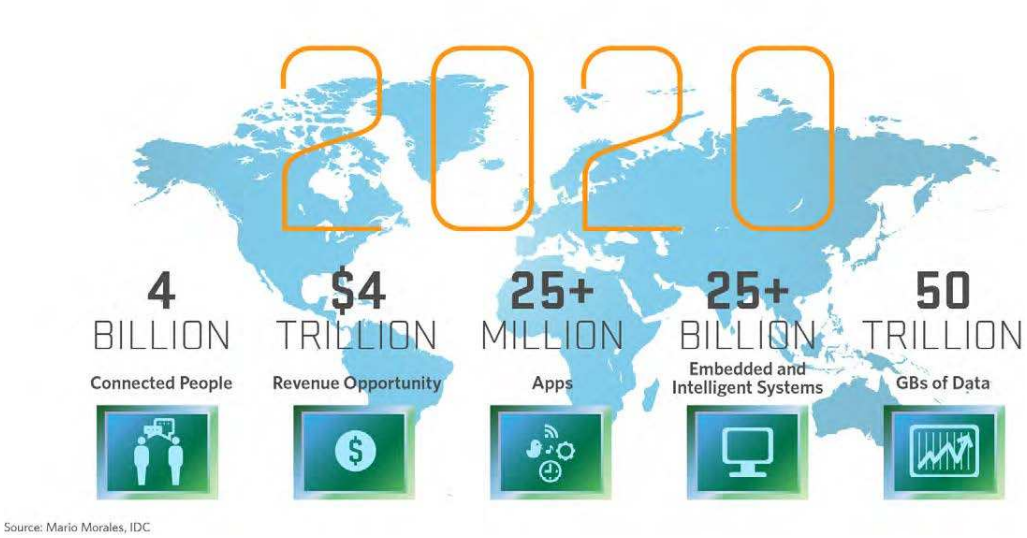
2 ÄLYTALOT YLEISESTI

2.1 Älytalon määrittely

Älytalolla tarkoitetaan taloa, johon on asennettu automaatiojärjestelmä. Vähimmäis- tai enimmäismäärää järjestelmän laajuudelle ei ole asetettu. Yleensä älytalo viittaa ensisijaisesti taloihin joissa on paljon erilaista automaatiota joka voi olla keskitetty yhteen paikkaan tai hajautettu useaan eri osaan. Keskityksen avulla asioiden monitorointi ja säätäminen tapahtuu yhdestä paikasta ja nykyisin usein myös erilaisten älylaitteiden avulla.

Nykypäivänä älytaloon liittyy läheisesti termi esineiden internet eli Internet of Things, lyhyesti IoT. IoT-sovellukset ovat jatkuvassa kasvussa ja vuoteen 2020 mennessä maailmassa uskotaan olevan yli 25 miljardia IoT-laitetta. (Taylot 2015) Älytaloissa voidaan hyödyntää yksittäisiä IoT-laitteita ja kerätä tieto yhteen keskusjärjestelmään. Tavallaan langattomat väyläratkaisut toimivat hieman samalla tavalla kuin IoT-laitteet, mutta yksiköitä ei ole yhdistetty internetiin vaan suojattuun lähiverkkoon, jonka kautta laitteet ottavat yhteyden keskitettyyn hallintajärjestelmään.

Esineiden internetin hyödyntäminen on mahdollista myös sellaisenaan älytaloissa. Avoin järjestelmä voidaan rakentaa IoT-laitteiden avulla niin, että keskusyksikkönä toimii esimerkiksi Raspberry Pi-tietokone ja muut komponentit ovat IoT-laitteita. Näin säästetään rahaa ja järjestelmästä tulee helposti laajennettava. Tällaisen järjestelmän rakentaminen onnistuu myös aloittejilta, joka seuraa internetistä löytyviä ohjeita.



Kuva 1. IoT-laitteiden arvioitu määrä vuonna 2020. (Taylor 2015)

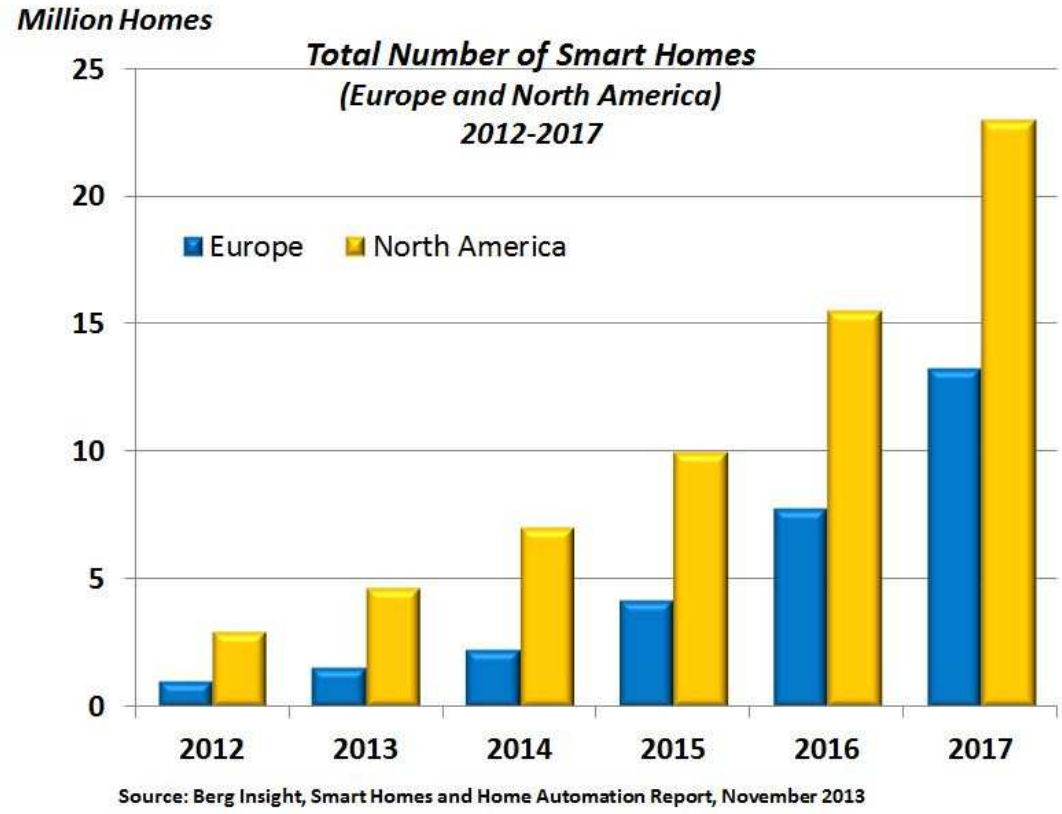
Periaatteessa pelkkä Raspberry Pi tai muu vastaava tietokone ei vielä tee talosta älytaloa. Vaikka tarkkaa määrittelyä ei ole olemassa, voidaan sanoa että älytalo vaatii ainakin jonkin verran automaatiota. Laitteet voivat olla yksittäisiä tai muodostaa isomman kokonaisuuden johon muut laitteet ottavat yhteyden. Kokonaisvaltainen järjestelmä, jonka avulla voidaan säätää ja mitata useita eri asioita toimii usein älytalon järjestelmänä mutta tällaisen rakentaminen Raspberry Pi-tietokoneen tai vastaavan laitteen avulla on harvinaista. Tämän takia vastaavat järjestelmät toimivatkin usein joko älytalojen järjestelmien apuna tai mahdollisesti niiden korvaajina tapauksissa, joissa ei vaadita kokonaista järjestelmää. Poikkeuksiakin kuitenkin on.

2.2 Älytalot meillä ja maailmalla

Erityisesti viime aikoina älytalot ovat kasvattaneet suosiotaan. Yksi syy tähän on kustannusten pieneneminen ja yleisen osaamisen lisääntyminen. Kiinnostus on ollut nousussa uusien toimijoiden lisääntyessä ja muiden älykkäiden laitteiden vallatessa markkinaosuutta myös taloihin halutaan enenevissä määrin lisää älyä. Toisaalta myös älytalojen hyödyt tunnetaan paremmin kuin ennen.

Automaation tuomat hyödyt on helpompi perustella, jos niiden kustannukset pysyvät järkevissä mitoissa. Toisaalta vallitseva taloustilanne tuo omat haasteensa

rakentamiseen. Automaation kannalta on vaikea sanoa, kuinka paljon taloudellinen tilanne vaikuttaa ihmisten suhtautumiseen lisäkustannuksia kohtaan. Yhtenä ongelmana on varmasti se, että automaatio vie rahaa muusta rakennusbudjetista. Älytaloa voidaan kuitenkin pitää myös sijoituksena, jossa osa siihen käytetystä rahasta saadaan takaisin esimerkiksi sähkönkulutukseen liittyvillä säästöillä joita älytalo voi tuoda.



Kuva 2. Älytalojen arvioitu määrä Euroopassa ja Pohjois-Amerikassa. (Infosec institute 2015)

2.2.1 Älytalot Suomessa

Suomessa älytalon asiaa on ajanut erityisesti vuosittain järjestettävät asuntomessut. Jo vuonna 1991 Varkauden asuntomessuilla nähtiin älytalo, jossa tietotekniikkaa hyödynnettiin turvallisuuteen ja asumismukavuuteen liittyvissä asioissa. (Suomen Asuntomessut) Älytalojen lisääntyessä tullaan varmasti näkemään lisää vastaavia asuntomessutaloja.

Kattavaa tutkimusta älytalojen määrästä Suomessa ei ole vielä tehty. Myös arvioiden antaminen on hankalaa. Kiinnostus älykästä tekniikkaa kohtaan on kuitenkin lisääntynyt.

2.2.2 Älytalot muualla

Maailmalla älytaloja on rakennettu jo kymmeniä vuosia. Jo 1980-luvulla Amerikassa rakennettiin älytaloja, joihin asennettiin esimerkiksi keskusjärjestelmä josta voitiin säätää lämmitystä ja jäähdytystä. Osa näistä järjestelmistä on edelleen käytössä ja huolimatta varaosien heikosta saatavuudesta ne toimivat edelleen varsin hyvin. Kuitenkin nämä ovat suhteellisen yksinkertaisia laitteistoja, jotka voitaisiin toteuttaa hyvin edullisesti nykyaikana. On kuitenkin selvää, että vuosikymmeniä vanhat mutta edelleen toiminnassa olevat järjestelmät ovat hyvää mainosta älytaloille.

Myös Amerikan ulkopuolella älytaloja on rakennettu jo vuosia. Eurooppalainen KNX-väylä on alan suurimpia standardeja ja laajalti käytössä erityisesti Euroopassa. (KNX Association 2016) Vuoden 2013 arvion mukaan älytalojen määrä vuonna 2017 Euroopassa ja Pohjois-Amerikassa voi olla jopa 35 miljoonaa. (Infosec institute 2015) Joka tapauksessa niiden määrä on ollut kasvussa jo vuosia ja lisää rakennetaan jatkuvasti.

2.3 Älytalon hankinnan perusteet

Älytalon rakentamiseen on useita syitä. Koska älytalojen automaatio nostaa talon rakennuskustannuksia, kannattaa keskittyä siihen kuinka rahaa voidaan säästää myöhemmin ja mitä hyötyjä älytalosta saadaan. Energian säästäminen on yksi hyvä esimerkki rahan säästämisestä älytalojen avulla. Älytalon lämmitysjärjestelmä voi tutkia sähkön pörssihintaa ja näin määritellä paras mahdollinen aika talon lämmitykselle. Tällä tavalla järjestelmä säästää sähköä ja maksaa osan kuluista takaisin vuosien kuluessa. Myös muut kustannussäästöt saattavat houkutella älytalon rakentajaa.

2.3.1 Älytalon hyödyt

Energiansäästö on ollut yleinen puheenaihe jo vuosien ajan ja talojen energiankulutuksessa on yritetty päästä niin alas kuin mahdollista. Tämä on osaksi mahdollista automaation avulla, joka valvoo energiankulutusta ja jopa energian tuottamista mikäli sellainen on mahdollista. Aurinkopaneelit ja muut vastaavat energiaa tuottavat laitteet voidaan lisätä talon sähköverkkoon niin, että ne tuottavat osan talon kuluttamasta sähköstä.

Asumismukavuuden parantuminen on tärkeä osa automaatiota. Asumisturvallisuuteen liittyvät seikat kuten automaattinen kulunvalvonta ja turvakamerajärjestelmä voidaan liittää osaksi älytaloa. Näiden avulla taloa voidaan valvoa myös silloin, kun asukkaat eivät ole itse kotona. Muita asumismukavuuteen liittyviä asioita kuten automaattisesti säätyvä lämmitysjärjestelmä, palo- ja häkävaroittimet sekä auringonvalon mukaan säätyvä valaistus- ja sälekaihdinjärjestelmä voidaan myös lisätä samaan järjestelmään.

2.3.2 Älytalon ongelmat

Kustannusten lisäksi älytaloilla on myös muita ongelmia. Ne voidaan jakaa muutamaan eri kategoriaan sen mukaan, millaisista ongelmista on kyse. Osa ongelmista tulee vastaan suunnittelu- ja rakennusvaiheessa, osa asumisvaiheessa ja osa päivitettäessä järjestelmää uudempaan. Suunnittelu- ja rakennusvaiheessa suurin ongelma muodostuu kustannuksista. Määrittämällä tarkka budjetti, sekään ei ole kovin suuri asia.

Asumisvaiheessa eteen tulevat mahdolliset ongelmat, joita älytalon järjestelmien käyttäminen voi aiheuttaa. Huono käyttöliittymä, järjestelmän epävakaus ja muut käyttöön liittyvät ongelmat täytyy saada poistettua ennen järjestelmän luovutusta asiakkaalle. Pahimmassa tapauksessa ongelmat voivat olla jopa niin suuret, että asukas haluaa jättää osan ominaisuuksista käyttämättä niiden vaivalloisuuden tai epävakauden takia. Tällainen järjestelmä ei palvele käyttäjän etuja eikä sellaista tilannetta saisi päästä syntymään.

Elinkaaren loppupuolella järjestelmän päivitys tai vaihtaminen uuteen saattaa olla huomattavasti vaikeampaa, jos sitä ei ole otettu huomioon jo suunnitteluvaiheessa. Automaatiojärjestelmiä rakennettaessa tällainen otetaan kuitenkin aina huomioon. Teollisuusautomaatiojärjestelmissä hyvänä puolena on laitteiden ja ohjelmistojen parempi tuntemus, jolloin voidaan tehdä suunnitelma kuinka kauan varaosia voidaan toimittaa ja kuinka kauan laitteiston voidaan olettaa olevan olemassa nykymuodossaan. Älytalojärjestelmät muuttuvat jatkuvasti ja tämän takia on vaikeampi arvioida kuinka kauan järjestelmää tai sen osia tuetaan.

3 OHJELMISTORATKAISUT

3.1 Ohjelmistoratkaisujen luokittelu

Ohjelmistoratkaisut voidaan jakaa kahteen pääryhmään, avoimiin ja suljettuihin ohjelmistoihin. Avoimet järjestelmät ovat yleensä avoimia sekä ohjelmistoltaan että laitteistoltaan kun taas suljettuihin järjestelmiin voidaan yleensä liittää vain yhden valmistajan hyväksymiä komponentteja, Viimeisen kymmenen vuoden aikana on kuitenkin siirrytty kohti yhteisiä väyläratkaisuja joita voidaan hyödyntää sekä kiinteistö- että teollisuusautomaatiossa.

Vaikka nykyään logiikat ja muut keskusyksiköt ovat usein avoimia järjestelmiä, myös suljettuja järjestelmiä on edelleen olemassa. Yksittäiset IoT-laitteet voivat olla suljettuja järjestelmiä mikäli niistä ei ole mahdollista muodostaa yhteyttä muihin IoT-laitteisiin tai laitteisiin, joiden tarkoitus on kerätä tietoa.

3.2 Suljetut järjestelmät

Suljetut järjestelmät ovat usein IoT-laitteita. Monet edulliset IoT-laitteet sisältävät vain älypuhelinyhteyden internetin tai lähiverkon yli eikä niistä ole mahdollista siirtää dataa laitteisiin johon se voitaisiin kerätä analysointia varten. Avoimiin

järjestelmiin sen sijaan voidaan liittää muitakin laitteita. Suljetut järjestelmät ovat yksinkertaisia ja toimivat erityisen hyvin silloin, kun halutaan ohjata yhtä kohdetta kerrallaan. Huono puoli on keskitetyn ohjausjärjestelmän puute. Siitä on haittaa erityisesti silloin, kun halutaan kytkeä kaksi tai useampi laite yhteen.

Suljetuilla älytaloratkaisuilla on harvoin helppo rakentaa kokonaisvaltainen järjestelmä. Suljettuihin järjestelmiin ei voi lisätä muita kuin laitevalmistajan omia komponentteja. Mikäli yksi laitevalmistaja valmistaa kaikkia tarvittavia komponentteja, järjestelmä voidaan rakentaa yhden toimittajan osista. Tulevaisuudessa järjestelmä on kuitenkin riippuvainen yhden toimittajan osista joiden hinta ja saatavuus saattavat muuttua ratkaisevasti vuosien aikana.

3.3 Avoimet järjestelmät

Avoimet järjestelmät ovat määritelmän mukaisesti järjestelmiä, johon voidaan liittää muidenkin kuin keskusyksikön valmistajan komponentteja. Nykyään iso osa logiikoista tukee avoimia automaatioväyliä. Näin järjestelmään voidaan liittää usean eri komponenttivalmistajan komponentteja. Koska useat yritykset valmistavat samanlaisia komponentteja, loppukäyttäjä voi kilpailuttaa tuotteet ja valita sen, jossa on sopivat ominaisuudet ja alhaisin hinta. Suljetuissa järjestelmissä tämä ei yleensä ole mahdollista.

Avoimiin järjestelmiin sisältyvät myös avoimen lähdekoodin järjestelmät. Avoin lähdekoodi tarkoittaa tässä tapauksessa sitä, että jokin laitteiden osa on avointa lähdekoodia. Joissakin tapauksissa se voi viitata esimerkiksi siihen, että laitteesta voi valmistaa itse muunneltuja kopioita. Raspberry Pi-tietokoneen kohdalla se tarkoittaa sekä avoimia laiteajureita että avointa käyttöjärjestelmää jota voi itse muokata tarpeisiinsa sopivaksi.

Kuva 3. Yksinkertainen Raspberry Pi-järjestelmä. (Upton 2015)

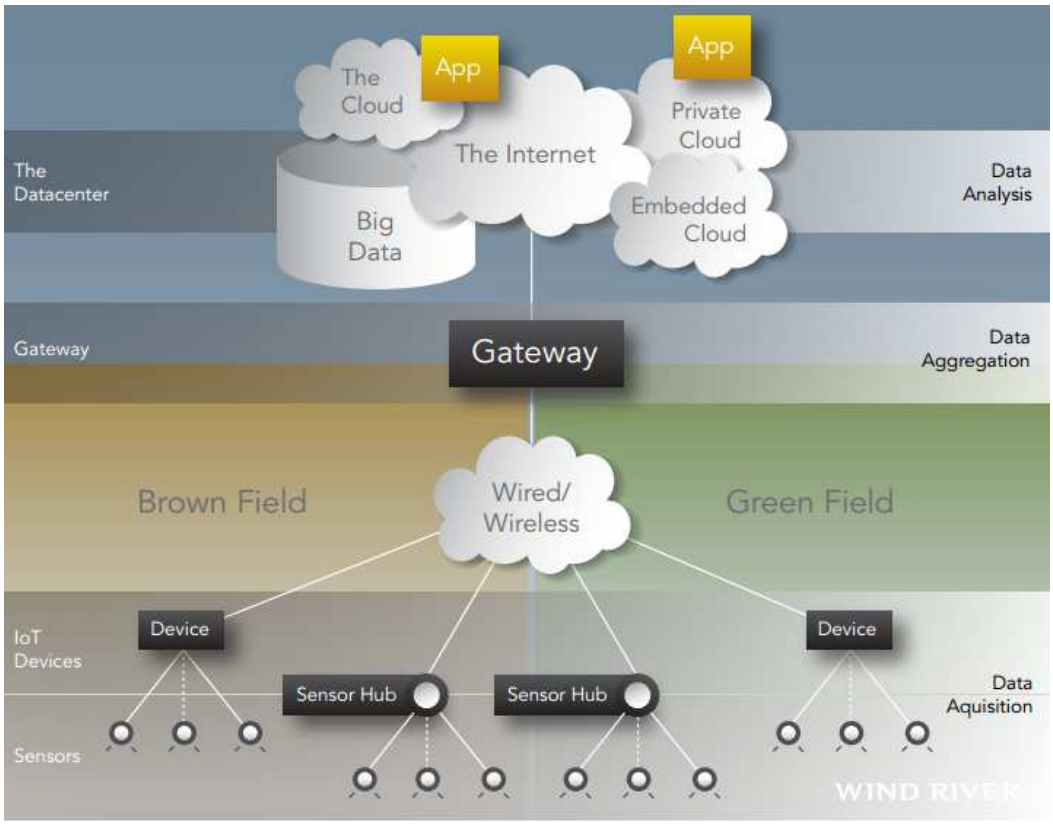
Avoimen lähdekoodin järjestelmien hyväksi puoleksi voi mainita myös matalan aloituskynnyksen. Internetistä löytyy paljon materiaalia ja komponenttien hinnat ovat paljon matalampia kuin kaupallisissa järjestelmissä. Myös alan ammattilaiset kuten automaatioinsinöörit voivat helposti toteuttaa pieniä projekteja. Monet automaatiolaitteissa käytettävät ohjelmointikielet kuten IEC-standardiin 61131-3 kuuluvat standardit ohjelmointikielet ovat tuettuina. Osa ohjelmointiympäristöistä kuten Codesys tukevat tämän lisäksi myös korkeamman tason ohjelmointikieliä. Näin myös PC-puolen ohjelmoijat voivat ohjelmoida automaatiojärjestelmiä jo osaamiensa ohjelmointikielien avulla.

Avoimen lähdekoodin järjestelmien hyvät puolet ovat lisänneet älytaloista ja taloautomaatiosta kiinnostuneiden harrastajien määrää. Usein harrastajat ovat keskittyneet yhteen älytalon ominaisuuteen kerrallaan. Näitä voivat olla esimerkiksi valoautomatiikka, kulunvalvonta tai lämmitysjärjestelmän automatisointi. Myös esineiden internet eli IoT on suosittua koska sen avulla voidaan etäohjata laitteita jotka on kytketty internetiin. Tähän tarkoitukseen avoimen lähdekoodin järjestelmät

sopivat erityisen hyvin. Internetissä on paljon ohjeita projekteja varten ja niissä on hyvät ohjeet etäohjauksen toteuttamiseen.

IoT-laitteet voivat olla osa joko avointa tai suljettua järjestelmää. Avoimen lähdekoodin IoT-laitteet ovat erityisesti elektroniikan harrastajien suosiossa. Komponentit ovat halvempia kuin muissa järjestelmissä ja ohjeita löytyy kaikkiin yleisimpiin asioihin.

Yhteisön tuottama ohjesisältö kuuluu erottamattomasti avoimen lähdekoodin projekteihin. Ohjeiden avulla on helppo päästä alkuun ja niitä voi soveltaa myös sellaisissa projekteissa, joihin ei ole suoraan oikeita ohjeita. Muissa järjestelmissä tälläinen ei yleensä ole mahdollista. Näinollen hyvä dokumentaatio pienentää entisestään aloituskynnystä erityisesti niiden kohdalla, joilla ei ole automaatioon liittyvää koulutusta tai jotka ovat kiinnostuneet elektroniikasta yleisesti.

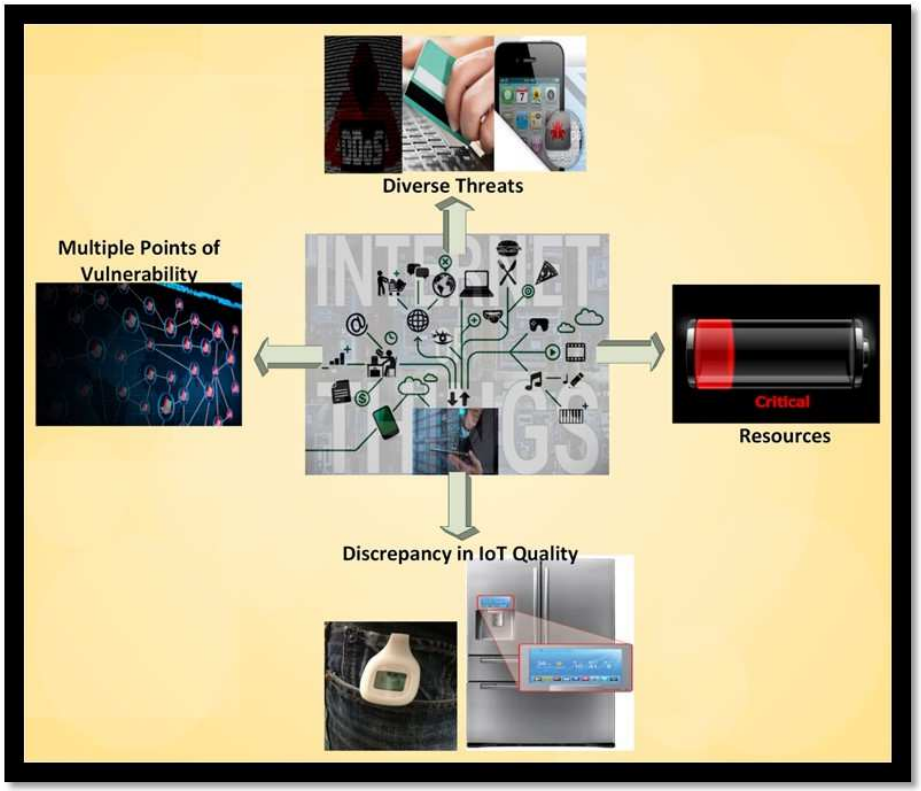


Kuva 4. Esimerkki IoT-topologiasta. (Wind River 2015)

4 TIETOTURVA

Tietoturva on merkittävä asia kun tehdään älytalon automaatiosuunnittelua. Mikäli älytalon automaatiojärjestelmään on yhteys talon WLAN-verkon tai jopa internetin kautta, pitää varmistaa, että ulkopuoliset henkilöt eivät pääse ottamaan yhteyttä taloon. Suojaus on huomattavasti helpompi järjestää, mikäli yhteys toimii vain talon sisällä olevan verkon kautta, joka ei ole yhteydessä internetiin. Jos kuitenkin halutaan jonkinlainen yhteys myös talon ulkopuolelle, on varmistuttava siitä että tarpeellisesta suojauksesta on huolehdittu.

Perinteisesti tietoturva on tarkoittanut tietoteknisten laitteiden, kuten tietokoneiden ja älypuhelimien suojausta. Myös automaatiojärjestelmät täytyy suojata ja toistaiseksi niiden tietoturva on usein varsin huono. Tulevaisuudessa tullaan näkemään järjestelmien ja niiden suojauksen kehitystä. Myös esineiden internetin suojaus tulee näkymään jatkossa entistä selkeämmin. Tämä voi vaikuttaa myös taloautomaation laitteistojen tietoturvaan positiivisesti. Esineiden internet tuo kuitenkin lisää haasteita tietoturvan kannalta.



Kuva 5. IoT-laitteiden tietoturvaan liittyviä haasteita (Infosec institute 2015)

4.1 Tietoturvauhat

Vääriin käsiin joutuessaan älytalon tiedot saattavat aiheuttaa huomattavan vaaratilanteen. Sähkönkulutuksen ja valaistuksen tietojen perusteella voidaan päätellä ollaanko talossa kotona vai ei. Mikäli ulkopuoliset tahot saavat yhteyden myös turvakameroihin ja kulunvalvontaan, he voivat pahimmassa tapauksessa päästä jopa taloon sisälle. Yleensä tästä kuitenkin huolehditaan niin, että elintärkeisiin ominaisuuksiin ei päästä talon ulkopuolelta lainkaan käsiksi.

Hakkeroinnin uhriksi joutuminen on mahdollista, jos yhteys internetiin ei ole täysin suojattu. Hyväkään suojaus ei kuitenkaan poista uhkaa kokonaan. Tämän takia onkin tärkeää minimoida asiat, joihin hakkeri voi saada yhteyden. Samalla on hyvä estää järjestelmän etäsammutus, jotta hakkeri ei voi sulkea koko järjestelmää pois päältä asukkaiden tietämättä.

Yleensä tällaiset uhat otetaan hyvin huomioon. On kuitenkin poikkeuksia ja joskus logiikat saattavat olla lähes suoraan yhteydessä internetiin. Jopa teollisuuslaitosten logiikoita voi löytää internetistä niin, että ne vastaavat ping-kutsuun ja niihin saa suoran yhteyden. Suurin osa niistä on kuitenkin salasanasuojattuja mutta jos niiden ohjelmistosta löytyy jokin haavoittuvuus, yhteyden saaminen voi olla hyvinkin yksinkertaista. Ennakkotapauksia on, esimerkiksi amerikkalaisen vedenpuhdistamon automaatiojärjestelmän kaataminen internetin välityksellä. (Smith 2011)

Muutaman vuoden takainen Stuxnet-mato tehtiin häiritsemään Iranin ydinaseohjelman uraaninrikastamista ja se saastutti tietokoneita, joissa havaittiin Siemensin Step 7-ohjelmisto. Näin mato pystyi muuttamaan logiikoiden ohjausparametreja ja häiritsemään tehtaan prosesseja. Älytalojen järjestelmät eivät toistaiseksi ole saavuttaneet niin suurta levinneisyyttä että laajamittainen hyökkäys olisi kovin todennäköinen, mutta jos yksi järjestelmä yleistyy selkeästi muita yleisemmäksi on vastaava hyökkäys sekä mahdollinen että myös todennäköinen. (Zetter, K 2014)

4.2 Suojaustavat

Yksinkertaisin tapa suojautua ulkopuolisilta tahoilta on estää järjestelmään pääsy internetin välityksellä. Joissakin tapauksissa internet-yhteyttä halutaan kuitenkin hyödyntää, syystä tai toisesta. Tällöin on oltava varma että hakkerit eivät voi kaapata järjestelmää. Palomuurin avulla voidaan estää suora yhteys logiikkaan. Samalla voidaan piilottaa suurin osa porteista niin että vain muutama portti on avoin internetiin. Salasanasuojauksen käyttäminen on myös suositeltavaa sen helppouden takia.

Salasanojen murtaminen on mahdollista, erityisesti jos salasana on tarpeeksi lyhyt. Edellämainittu amerikkalainen vesilaitos oli suojattu lyhyellä, vain kolme merkkiä sisältävällä salasanalla. Hakkerit keksivät salasanan luultavasti brute force-hyökkäyksen avulla eli kokeilemalla mahdollisimman paljon satunnaisia salasanoja ennen kuin löysivät oikean ja saivat yhteyden laitoksen järjestelmään. Oikeaoppinen tapa käyttää salasanoja on estää niiden käyttö ennen kuin palvelin on vastaanottanut esimerkiksi ssh-yhteyden läpi annetun private/public key-parin. Sen pituus voi olla esimerkiksi 256 bittiä ja se on erittäin turvallinen tapa ottaa yhteys toiseen laitteeseen. Joissakin tapauksissa voidaan käyttää myös pidempiä suojausavamia kuten 1024 bittiä pitkiä avaimia.

Suojausavainten huono puoli on kuitenkin se, että ne pitää säilyttää laitteen mukana. Näin ollen on erittäin tärkeää, että suojausavainten sisältämät laitteet kuten kännykät ja kannettavat tietokoneet pidetään hyvässä tallessa etteivät avaimet päädy vääriin käsiin. Toisaalta yhteyden muodostamiseen tarvitaan edelleen myös salasana, jonka pituus voisi olla esimerkiksi 10 merkkiä tai enemmän. Näin yhteyden muodostus olisi lähes mahdotonta ilman salausavainta ja vaikeaa vaikka hakkerit olisivat onnistuneet saamaan salausavaimen. Toinen huono puoli tässä ratkaisussa on sen vähäinen tuki. Nykypäivän logiikat eivät toistaiseksi tue kovin edistyneitä salaustekniikoita kuten RSA-avaimia. Myös ssh-yhteys on vielä harvinaisuus. Kun tietoturvaan kiinnitetään lisää huomiota, paremmat suojaustavat luultavasti tulevat yleistymään.

IoT- ja älytalojärjestelmiä suojattaessa voidaan käyttää muissa IT-sovelluksissa käytettyjä suojaustapoja. Parhaassa tapauksessa nämä ratkaisut toimivat aivan yhtä hyvin kuin IoT-järjestelmille tarkoitetut tietoturvaratkaisut. Mikäli valitaan tietoturvajärjestelmä jota ei ole suoraan tarkoitettu älytaloihin tai IoT-järjestelmiin, täytyy laitteiston tarpeet ottaa huomioon. (Wind River 2016)

4.3 Suojaukseen liittyvät ongelmat

Hyvä tietoturvaratkaisu ei häiritse käyttäjää, mutta suojaa laitteistoa ulkopuolisilta hyökkääjiltä. Hyvään tietoturvaan kuuluu läpinäkyvyys, hyvä suojaustaso ja helppokäyttöisyys. Parhaassa tapauksessa käyttäjä ei päivittäisessä käytössä juuri huomaa eroa suojaamattomaan järjestelmään paitsi syöttäessään salasanaa. Tietysti myös suojaustason täytyy olla hyvällä tasolla. Mahdollisten virheiden sattuessa myös helppokäyttöisyys pitää olla kunnossa eli asetuksia pitää pystyä säätämään helposti, joko asukkaan tai huoltomiehen toimesta.

Yksinkertainen mutta tehokas turvajärjestelmä estää suurimman osan ulkopuolisista hyökkäyksistä. Uhat ovat huomattavasti suuremmat, jos hyökkäys kohdistuu nimenomaan tiettyyn järjestelmään. Jos kodin WLAN-verkkoa ei ole suojattu, hyökkääjä voi päästä siihen käsiksi myös talon ulkopuolelta. Tällaista hyökkäystä vastaan on tärkeää suojata sekä automaatiojärjestelmä että WLAN-verkko salasanalla. Kohdistetut hyökkäykset ovat kuitenkin älytalon harvinaisuuden takia toistaiseksi harvinaisia mutta tulevaisuudessa siihen on hyvä varautua. WLAN-verkon suojaaminen on myös muista tietoturvaan liittyvistä syistä tärkeää.

Käyttäjäkokemuksen heikkeneminen liian tiukasta suojauksesta johtuen pitää pystyä estämään mikäli se on mahdollista. Älytalon yhtenä tarkoituksena on parantaa asumiseen liittyviä seikkoja kuten asumismukavuutta. Asumismukavuus kärsii mikäli käyttäjää rasitetaan ongelmilla, kuten suojauksesta johtuvilla yhteysongelmilla tai pitkien salasanojen kirjoittamisella. Tämän takia on erityisen tärkeää suunnitella älytalon järjestelmä niin, että käyttäjä pitää järjestelmän käyttämisestä.

4.4 Tietoturvan haasteet tulevaisuudessa

Amerikkalainen tietoturvayhtiö PWC teki tutkimuksen tietoturvasta vuonna 2014. Tutkimus keskittyi yleisen tietoturvan uhkiin mutta mukana oli myös asiaa esineiden internetistä. Sen mukaan hyökkäykset IoT-laitteisiin ovat yleistyneet. Kohteina ovat olleet mm. televisiot, termostaatit ja muut vastaavat laitteet. Tutkimuksen mukaan IoT-laitteiden puutteelliset suojausjärjestelmät tekevät niistä helppoja kohteita hakkereille. (PWC 2014)

Automaation kannalta tämä tarkoittaa samoja haasteita. IoT-järjestelmien liittäminen älytalon automaation osaksi tai jopa korvaamalla älytalon ohjausjärjestelmä kokonaan IoT-laitteilla tutkimuksen toteamat uhat pitää ottaa huomioon sellaisenaan. Tulevaisuudessa IoT-laitteiden määrä kasvaa ja niitä tullaan varmasti näkemään myös älytalon ohjausjärjestelmien apuna. Uhkien lisääntyessä tietoturva muuttuu yhä tärkeämmäksi asiaksi ja tulevaisuudessa myös tietoturvayhtiöt kiinnostuvat tästä kehittyvästä osa-alueesta.

5 LAITTEISTOT JA KOMPONENTIT

5.1 Väylät yleisesti

Väylät kuuluvat olennaisena osana automaatiojärjestelmään. Sekä teollisuus- että kiinteistöautomaation liittyvät väylät ovat yleisesti käytössä automaatiossa ja varsinkin viime vuosien aikana tapahtuneen hintojen laskun takia ne ovat yhä suositumpia. Kiinteistöautomaatiossa KNX-väylä on tällä hetkellä johtava väyläratkaisu sen kustannustehokkuuden, laajennettavuuden ja suuren komponenttimäärän takia. Myös muita kilpailevia väyliä on käytössä, mutta Euroopassa ne ovat KNX-väylää harvinaisempia.

Käytettyjä väyliä yhdistää niiden standardisointi. Nykyään on tärkeää että automaatioon liittyvät asiat on standardisoitu. Erilaisia standardeja on useita ja niitä

mainostetaan erityisesti väylien yhteydessä. Standardit väylät helpottavat komponenttivalmistajien työtä ja lisäävät näin väyliin liitettävien komponenttien lukumäärää. Suuresta komponenttimäärästä on erityisesti hyötyä kun useat valmistajat voivat kilpailla keskenään sekä hinnalla että ominaisuuksilla. Pelkkä standardointi ei kuitenkaan riitä. Jotta kaikki laitteet toimivat keskenään ilman ongelmia, tarvitaan standardia valvova taho joka varmistaa että laitteet toimivat keskenään saumattomasti.

5.2 KNX-väylä

KNX-väylä on tällä hetkellä suosituin kiinteistöautomaatioväylä Euroopassa. Isossa osassa Suomessa rakennetuissa älytaloissa käytetään nimenomaan KNX-väylää. Amerikassa sen käyttö on hieman vähäisempää. KNX-väylän etuihin kuuluvat mm. hyvä laitteistotuki, komponenttien yleisyys ja edullinen kustannustaso verrattuna muihin kiinteisiin väyliin.

KNX-standardia ylläpitää KNX Association, joka varmistaa että jokainen laite on yhteensopiva väylän kanssa ja antaa hyväksynnän laitteelle. Näin varmistutaan väylän toiminnasta eri laitteiden yhteydessä. Sekä suljetut että avoimet järjestelmät tukevat KNX-väylää.

Väylässä voi olla enintään 65536 laitetta 16-bittisen muistiavaruuden mukaan. Väylä käyttää kierrettyä paria tiedonsiirtoon ja sen maksiminopeus on 9600 bit/s. Nopeus ei ole kovin suuri verrattuna esimerkiksi Ethernet-tiedonsiirtoon mutta nopeus on riittävä taloautomaatiossa käytettäville laitteille. Kaapelin maksimipituus yhtä segmenttiä kohden on 1000 m ja yhdessä segmentissä voi olla enintään 64 laitetta. Neljä segmenttiä voidaan liittää toisiinsa toistimien avulla jolloin kaapelin pituus voi olla enintään 4000 m ja laitteiden maksimimäärä on 256.

KNX-väylä voi olla myös langaton. Langaton KNX-väylä muistuttaa Z-Wavea toiminnallisuudeltaan joka on KNX-väylän kilpailija. Langattoman järjestelmän avulla vältytään kaapelien vetämiseltä ja järjestelmä on helppo asentaa. Mikäli

halutaan poistaa kaikki kaapeloinnit, etälaitteissa voidaan käyttää myös akkuja. Tämä toimii erityisesti niiden laitteiden kanssa, jotka eivät kuluta kovin paljon sähköä. Luotettavuus kuitenkin kärsii mikäli laitteet toimivat akuilla. Langaton verkko voi myös ottaa häiriötä sähkölaitteista joka myös heikentää langattomien verkkojen luotettavuutta. (Reinisch 2006)

5.3 Muut väylät

Taloautomaatiossa voidaan käyttää perinteisten johdotettavien väylien lisäksi myös langattomia väyliä. Amerikassa erityisen suosittu Z-Wave on langaton väylätyyppi. Se on varsin yksinkertainen väylä joka käyttää noin 900 MHz taajuutta. Myös Z-Waveen voidaan liittää avoimia järjestelmiä. Väylän hyviin puoliin kuuluvat mm. pieni virrankulutus ja langattomuus. Langattomien järjestelmien luotettavuus ei ole samalla tasolla kaapelointia käyttävien väylien kanssa, mutta älytaloissa luotettavuus on kuitenkin riittävällä tasolla. Langattomien väylien hyvä puoli on myös laajennettavuus koska taloon ei tarvitse vetää uusia kaapeleita mikäli järjestelmää halutaan laajentaa. Tämä mahdollistaa myös helpon asennuksen ja käyttöönoton jo olemassa oleviin taloihin. (Z-Wave 2016)

Z-Wave ja muut langattomat järjestelmät muistuttavat IoT-järjestelmiä suuresti. Erona on kuitenkin se, että IoT-laitteet on yleensä kytketty internetiin tai ainakin suojattuun sisäverkkoon josta saattaa olla yhteys internetiin mutta Z-Wave käyttää omaa langatonta taajuuttaan joten siihen ei pääse käsiksi WLAN-laitteilla. Näin saavutetaan myös pienempi interferenssi langattomien verkkojen välillä koska WLAN käyttää 2,4GHz taajuutta ja Z-Wave pienempää kuin tämä. WLAN-verkkojen keskinäinen interferenssi on suuri ongelma erityisesti kerrostaloissa. Sen välttäminen vähentää mahdollisia yhteysongelmia.

5.4 Väyliin liitettävät komponentit

Älytaloissa käytetään usein väyläratkaisua, jolloin kaikki komponentit liitetään väylän kautta. Kaikkiin yleisiin väyliin on saatavilla tuhansia komponentteja jolloin

väylän valinta ei perustu siihen, mitä komponentteja siihen voidaan valita. Käytännössä aina löytyy sopiva komponentti huolimatta siitä, mitä väylää käytetään.

Komponentit valitaan suunnitteluvaiheessa tehtyjen päätösten mukaan. Koska komponenttien on tarkoitus on toimia saumattomasti yhdessä, täytyy komponentteja valittaessa miettiä niiden sopimista järjestelmän yleiskuvaan muun yhteensopivuuden lisäksi. Tämä on kuitenkin enemmänkin suunnitteluun liittyvä kysymys kuin suoraan väylistä riippuvainen asia.

Mikäli suunnitteluvaiheessa päädytään IoT-pohjaiseen järjestelmään, komponentit ovat yleensä täysin erilaisia kuin väyliin liitettävät komponentit. IoT-komponentit eivät tarvitse kalliita väyläliityntöjä joten komponenttihinnat ovat edullisempia väylään liitettäviin komponentteihin verrattuna. Toisaalta komponentit tehdään usein halvemmalla jonka takia niiden luotettavuus saattaa olla heikompi.

6 ÄLYTALON SUUNNITTELU

Älytalon määritelmän mukaisesti älytalon automaatio voi olla joko keskitetty, yleensä huomattavan suuri järjestelmä tai hajautettu, pienempiin paloihin jaettu kokonaisuus joka voidaan kytkeä yhteen keskusjärjestelmään tai pitää täysin erillään toisistaan. Tässä opinnäytetyössä keskitytään lähinnä ensimmäiseen tapaukseen mutta myös jälkimmäiseen liittyvistä asioista voidaan mainita.

Keskitettyjä järjestelmiä suunnitellessa pitää ottaa huomioon erityisesti se, mitä tietoa halutaan näyttää loppukäyttäjälle. Joissakin tapauksissa kaikkea tietoa ei tarvitse eikä kannatakaan esittää talon käyttäjille. Siitä huolimatta tietoa voi kerätä jos siitä saadaan jotakin hyötyä myöhemmin. Tällaista tietoa on vaikkapa lämpötila vähemmän käytetyissä huoneissa. Tiedon ei tarvitse olla jatkuvasti näkyvillä mutta sitä voidaan myöhemmin analysoida, jolloin nähdään onko lämpötila ollut tasainen eri puolilla taloa.

Ominaisuudet kannattaa jakaa sen mukaan kuinka tärkeitä ne ovat järjestelmän ja käyttäjän kannalta. Automaatiolaitteet ovat suhteellisen halpoja, mutta turhien laitteiden asennusta kannattaa kuitenkin välttää. Ylimääräiset laitteet myös lisäävät ylläpitokustannuksia ja ne kannattaa jättää pois tai korvata laitteilla, joista saadaan jotain konkreettista hyötyä.

6.1 Suunnittelun aloittaminen

Aloitettaessa älytalon suunnittelua kannattaa ensimmäiseksi selvittää, mitä käyttäjä talolta haluaa. Yksinkertaisuus on tärkeää, joten kannattaa pyrkiä varmistamaan ettei käyttäjää rasiteta liialla informaatiolla. Toisaalta on tärkeää että järjestelmästä ei tule puolivalmista, jolloin sen hyödyt jäävät pieniksi.

Suunnittelun tärkein asia on saada aikaan toimiva kokonaisuus, jossa ei ole mitään liikaa eikä mitään myöskään puutu. Käymällä läpi mahdollisia valintoja voidaan saavuttaa tavoite ja löytää tarvittavat asiatm joita käyttäjä kaipaa. Suunnitelman osat muodostavat kokonaisuuden, joka vaikuttaa sekä laitteiden että ohjelmiston valintaan.
Tällä hetkellä suosituksi noussut älytaloratkaisu on KNX-väylää hyödyntävä kokonaisuus, joka sisältää KNX-organisaation hyväksymiä komponentteja. Mikäli KNX-väylä valitaan, voidaan käyttää useissa asennuksissa käytettyjä jo hyväksi havaittuja komponentteja ja varmistua osien yhteensopivuudesta jo ennen järjestelmän asennusta.

6.2 Suunnittelun eteneminen

Käyttäjän vaatimusten perusteella voidaan valita väyläratkaisu ja tarvittavat komponentit. Mikäli päädytään pienempään ja edullisempaan ratkaisuun myös avoin järjestelmä voi tulla kysymykseen. Tarkemmat komponenttivalinnat tehdään tämän jälkeen.

Myös komponenttivalinta tehdään asiakkaan vaatimusten mukaan. Annettu budjetti vaikuttaa suuresti järjestelmän laajuuteen ja samalla valittaviin osiin. Tämän takia

budjetti on hyvä selvittää heti alussa, jolloin suunnitelma voidaan tehdä mahdollisimman valmiiksi heti alussa.

Alkusuunnittelun jälkeen tutkitaan millainen järjestelmä rakennettavaan taloon voidaan tehdä. Tässä vaiheessa on hyvä suunnitella myös HMI eli käyttöliittymä. Käyttöliittymän vaatimuksiin kuuluu yksinkertaisuus ja helppokäyttöisyys. Hyvä käyttöliittymä sisältää kuitenkin tarpeeksi paljon tietoa järjestelmästä ja sen toiminnasta. Tämän saavuttaminen ei aina ole helppoa mutta se on äärimmäisen tärkeää käyttäjän kannalta.

Käyttöliittymiin on olemassa useita valmiita järjestelmiä. Parhaassa tapauksessa on olemassa valmis käyttöliittymä, johon on helppo tehdä tarvittavat muokkaukset jotta se mukautuu asiakkaan tarpeisiin sopivaksi. Usein asukas näkee järjestelmästä ainoastaan käyttöliittymän, jonka takia käyttöliittymä on olennainen osa älytalossa asumista. Hyvä käyttöliittymä tarkoittaa yleensä parempaa asumismukavuutta ja tyytyväisyyttä valittuun järjestelmään.

Kuva 6. Esimerkki kännykällä käytettävästä käyttöliittymästä. (Blair Construction 2014)

6.3 Suunnittelun viimeistely

Komponenttivalinnan ja käyttöliittymän suunnittelun jälkeen vuorossa on suunnittelun viimeistely. Viimeistelyvaiheessa käydään läpi tavoitteet ja budjetti jonka rajoissa toimitaan.

Suunnittelun viimeistelyyn kuuluu komponenttien yhteensopivuuden varmistaminen. Näin vältytään ikäviltä yllätyksiltä asennusvaiheessa. Myös järjestelmään tulevien anturien ja toimilaitteiden sopivuus valittuun käyttötarkoitukseen täytyy varmistaa. Esimerkkinä tästä voidaan mainita esimerkiksi lämpötilan mittaamiseen käytettyjen anturien sopiva lämpötila-asteikko.

Mikäli suunnittelu on onnistunut, rakennusvaiheessa ei pitäisi enää tulla yllätyksiä komponenttien suhteen. Muutoksia on mahdollista tehdä myös suunnittelun jälkeen, mutta yleensä pyritään siihen että järjestelmä tulee kerralla kuntoon. Pienet muutokset vaikuttavat niin vähän että ne voidaan tehdä myös viimeistelyn jälkeen.

Älytaloja rakennettaessa automaatiojärjestelmän suunnittelu voi olla yksi osa talosuunnittelua. Tässä tapauksessa suunnittelusta huolehtiva yritys suunnittelee sekä talon että sen automaatiojärjestelmän. Tällä tavalla voidaan rakentaa älytalo jossa automaatojärjestelmä sopii täydellisesti yhteen talon muiden ominaisuuksien kanssa. Joissakin tilanteissa se saattaa olla erittäin hyödyllinen asia, erityisesti myytäessä taloja jotka rakennetaan ensin ja myydään vasta niiden valmistumisen jälkeen.

7 OHJELMISTORATKAISUJEN NYKYTILA JA TULEVAISUUS

7.1 Älytalojen nykytila

Tällä hetkellä älytalot ovat edelleen voimakkaasti kasvava automaation osa-alue. Suurin osa taloista perustuu johonkin väyläratkaisuun kuten KNX-väylään. Pohjois-Amerikassa langaton Z-Wave on yleinen väylä ja myös muutamalla muulla

langattomalla väylätyypillä on kohtuullinen markkinaosuus. KNX-väylän leviämistä Amerikkaan on saattanut hidastanut sertifikoitujen KNX-urakoitsijoiden puute. Myös komponenttien hankkiminen Euroopasta on yleensä kallista.

Suomessa kehitys jatkuu kuten muuallakin. Eurooppalaiseen tyyliin kiinteät väylät ovat täälläkin yleisiä. Avoimia kiinteistöautomaatiojärjestelmiä tukevat Suomessa esimerkiksi Avoin automaatio ry. (Avoin automaatio ry 2016) Raspberry Pi- ja Arduino-harrastajia löytyy Suomesta jonkin verran ja Suomen ammattikorkeakouluissa on niihin liittyvää opetusta. Kummallakaan järjestelmällä ei kuitenkaan ole varsinaista yhtenäistä foorumia suomeksi, toisin kuin esimerkiksi avoimen lähdekoodin Linux-järjestelmällä.

Ulkomaiset internet-foorumit kuten Arduinon oma foorumi sisältävät paljon dokumentaatiota erilaisten laitteiden ja komponenttien käyttämisestä Arduinon kanssa. Kiinteistöautomaatiosta kertovaa dokumentaatiota on tosin edelleen suhteellisen vähän. Suurin osa siihen liittyvästä dokumentaatiosta keskittyy yhteen kohteeseen kerrallaan.

7.2 Älytalojärjestelmien tulevaisuus

Älytalojen yleistyessä voimakkaasti on toistaiseksi hankala arvioida järjestelmien tulevaisuutta. Tällä hetkellä perinteiset kiinteistöautomaatiojärjestelmät ovat edelleen suosittuja, mutta tulevaisuudessa IoT-laitteiden määrän ennustetaan lisääntyvän suuresti. Näin voidaan olettaa että IoT-laitteita hyödyntäviä laitteistoja tullaan näkemään myös älytaloissa. Varsinkin Pohjois-Amerikassa kehitys on jo pitkään vaikuttanut tältä.

Langattomat väylät kuten Z-Wave helpottavat automaation lisäämistä taloihin joissa ei vielä ole automaatiojärjestelmää koska uusia kaapeleita ei tarvita. On mahdollista että Z-Wave yleistyy myös Euroopassa, erityisesti vanhemmissa taloissa. Toistaiseksi sillä ei ole kovinkaan suurta markkinaosuutta täällä. Tilanne voi kuitenkin muuttua, mikäli langattomia väyliä halutaan ottaa käyttöön. Uusien väylien

laajamittainen käyttöönotto on usein hankalaa, jonka takia on hyvä valita jo valmiiksi tunnettu ja testattu väylä.

Järjestelmien kehittyessä myös tietoturvan pitää kehittyä. Tällä hetkellä älytalojen tietoturvasta puhutaan yleisellä tasolla eikä älytaloihin vielä ole olemassa montaakaan tietoturvaratkaisua joka olisi keskittynyt pelkästään älytalojen suojaamiseen. Yleisimmät palomuurit ja muut vastaavat järjestelmät on tarkoitettu tietokoneiden suojaamiseen mutta ne toimivat samalla myös älytalojärjestelmien kanssa.

8 YHTEENVETO

Älytalot ovat toistaiseksi harvinaisia, mutta järjestelmien kehittyessä tilanne varmasti muuttuu. Jo nyt uusia älytaloja rakennetaan selvästi enemmän kuin ennen ja esineiden internet eli IoT tuo varmasti lisää uusia älytaloja maailmaan. Erilaiset älyä sisältävät laitteet, kuten älykkäät lämmitystermostaatit ja muut vastaavat ovat lisääntyneet jatkuvasti ja liittämällä niitä toisiinsa voidaan muodostaa yksinkertainen mutta toimiva älytalojärjestelmä. Tämä helpottaa älytalon rakentamista ja madaltaa aloituskustannuksia selkeästi.

Jo nyt erilaiset älytaloihin asennettavat järjestelmät ja niiden suojausjärjestelmät ovat tarpeeksi kehittyneitä päivittäiseen käyttöön. Kehityksen edetessä hinnat laskevat ja älytalojen määrä jatkaa kasvuaan. Sekä suljetut että avoimet järjestelmät kehittyvät koko ajan. Molemmissa tullaan näkemään uudistuksia vaikka pääasiat pysyvätkin luultavasti samoina. Avoimen lähdekoodin tietokoneet ja mikrokontrollerit pysyvät luultavasti suosittuina komponentteina, mutta myös uusia laitteita voi tulla markkinoille.

Tietoturvan haasteet korostuvat älytalojen yleistyessä. Tietokoneiden suojaamiseen käytettävä tietoturva on sopiva myös älytaloihin, mutta sen käytössä pitää ottaa huomioon mahdolliset muutokset joita voidaan tarvita älytalojen suojaamisessa.

Tällä hetkellä älytalojen suojausjärjestelmät ovat vielä suhteellisen kehittymättömiä, mutta laajamittaiset hyökkäykset hyökkäykset älytalojen logiikoita ja muita laitteita vastaan ovat vielä harvinaisia. Tulevaisuudessa hyökkäykset todennäköisesti lisääntyvät ja tietoturvasta tulee entistä ajankohtaisempi.

LÄHTEET

Avoin automaatio ry. 2016. Viitattu 16.4.2016. http://www.avoinautomaatio.fi/

Blair Construction. 2014. Viitattu 12.4.2016. http://www.blairconstructionbr.com/automation/

Infosec institute. 2015. Security Challenges in the Internet of Things (IoT). Viitattu 13.4.2016. http://resources.infosecinstitute.com/security-challenges-in-the-internet-of-things-iot/

KNX Association. 2016. Viitattu 22.4.2016. https://www.knx.org/knx-en/knx/association/what-is-knx/

Livingston, V. 2014. Home Sweet (Smart) Home: Keep the Fire Burning. Viitattu 15.4.2016. https://iotworldnews.com/2014/01/home-sweet-smart-home-keep-the-fire-burning/

Upton, L. 2015. Viitattu 20.4.2016. https://www.raspberrypi.org/blog/diy-home-alert-system/

PWC. 2014. Managing cyber risks in an interconnected world – Key findings from The Global State of information Security Survey 2015. Viitattu 4.4.2016. http://www.pwc.ch/user_content/editor/files/publ_ass/pwc_managing_cyber_risks_in_an_interconnected_world_the_global_state_of_information_security_survey_2015.pdf

Reinisch, Granzer, Neugschwandtner, Praus, Kastner. 2016. Wireless Communication in KNX/EIB. Viitattu 28.4.2016. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.154.8488&rep=rep1&type=pdf

Smith, G. 2011. 'Russian' hackers seize control of U.S. public water system by remotely destroying pump. Viitattu 16.4.2016. http://www.dailymail.co.uk/sciencetech/article-2064283/Hackers-control-U-S-public-water-treatment-facilities.html

Suomen Asuntomessut. 2015. Viitattu 24.3.2016. http://asuntomessut.fi/organisaatio/messuhistoria/varkaus-1991/

Taylor, R. 2015. Behind The Numbers: Growth In The Internet Of Things. Viitattu 22.3.2016. http://www.seediscover.com/behind-the-numbers-growth-in-the-internet-of-things/

Wind River. 2015. Viitattu 22.4.2016. http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

Zetter, K. 2014. An unprecedented look at Stuxnet, the world's first digital weapon. Viitattu 12.4.2016. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Z-Wave. 2016. Viitattu 25.4.2016. http://www.z-wave.com/faq