LAPPEENRANNAN TEKNILLINEN YLIOPISTO
School of Engineering Science
Tuotantotalouden koulutusohjelma
Tietojohtaminen ja informaatioverkostot

DIPLOMITYÖ

Tuomas Pylkkänen

IoT (Internet-of-Things) – teknologian hyödyntäminen rakennuksien paloturvallisuuden kehityksessä ja integroidussa älykkäässä ympäristössä

Työn tarkastajat:
Erikoistutkija Satu Pekkarinen
Professori Tuomo Uotila

TIIVISTELMÄ

Työn tekijä: Tuomas Pylkkänen **Työn nimi:** IoT (Internet-of-Things) – teknologian hyödyntäminen rakennuksien paloturvallisuuden kehityksessä ja integroidussa älykkäässä ympäristössä
Tiedekunta: Lappeenrannan teknillinen yliopisto **Koulutusohjelma:** Tuotantotalous, tietojohtaminen
Vuosi: 2018
Diplomityö: Lappeenrannan teknillinen yliopisto, 109 sivua, 9 kuvaa, 1 liite **Tarkastajat:** Erikoistutkija Satu Pekkarinen ja Professori Tuomo Uotila
Hakusanat: IoT, Internet of Things, Esineiden Internet, Paloturvallisuus, Tulipalo

Internet of Things (IoT) eli esineiden Internet on saavuttanut maailmanlaajuisesti valtavaa huomiota, koska sen avulla on mahdollista digitalisoida fyysinen maailma. IoT-teknologia on yleistymässä myös paloturvallisuutta parantavissa laitteistoissa ja järjestelmissä sekä rakennuksien talotekniikassa. Tämän työn tarkoituksena on selvittää, voidaanko IoT-teknologiaa hyödyntämällä parantaa rakennuksien paloturvallisuutta. Lähtökohtana on selvittää mitä hyötyjä ja uhkia teknologiaan liittyy sekä voidaanko teknologiaa hyödyntämällä saada aikaan kustannussäästöjä paloturvallisuustekniikasta ja sen kunnossapidosta. Lisäksi tavoitteena on selvittää IoT:n avulla tapahtuvan datan jakamisen mahdollisuuksia sekä miten IoT- ja älyteknologiaa on hyödynnetty paloturvallisuuden kehityksessä Suomen rakennuskannassa.

Tämä tutkimus on laadullinen tutkimus, jonka aineisto kerättiin teemahaastattelujen avulla. Kokonaisvaltaisen kuvan saamiseksi tutkittavasta ilmiöstä suoritettiin haastatteluja henkilöille, jotka edustivat useita eri toimialoja. Teemahaastatteluaineistoon suoritettiin aineistolähtöinen sisällönanalyysi, jonka tulokset on esitetty tutkimustulokset-osiossa. Johtopäätökset-osiossa on tuotu esille tärkeimmät tutkimustulokset sekä vastattu pää- ja alatutkimuskysymyksiin.

Keskeisimpänä tuloksena voidaan todeta, että IoT- ja älyteknologiaa hyödyntämällä voidaan parantaa rakennusten paloturvallisuutta. Paloturvallisuuden parantamiseksi esille nousivat neljä päätekijää: toimintavarmuuden parantaminen, onnettomuuksien ehkäiseminen, pelastusviranomaiselle reaaliaikaisen tiedon välittäminen sekä talotekniikan olosuhdeanturoinnin hyödyntäminen. Lisäksi IoT-teknologiaa hyödyntämällä on mahdollista saada kustannussäästöjä paloturvallisuustekniikasta ja sen kunnossapidosta erityisesti kohteissa, joissa on paljon turvallisuustekniikkaa. Tehtyjen johtopäätösten perusteella IoT-ja älyteknologian hyödyntäminen Suomen rakennuskannassa on vielä varsin vähäistä varsinkin paloturvallisuuden osa-alueella.

ABSTRACT

Writer: Tuomas Pylkkänen
Subject: Utilization of IoT (Internet-of-Things) – technology in developing fire safety in buildings and in smart environment
School: School of Engineering Science
Department: Industrial Management, Knowledge management
Year: 2018
Master's Thesis: Lappeenranta University of Technology, 109 pages, 9 figures, 1 attachment
Examiners: Special Researcher Satu Pekkarinen and Professor Tuomo Uotila
Keywords: IoT, Internet of Things, Fire safety, Fire Protection Systems, Fire

Internet of Things has reached world-wide attention because it makes digitalization of physical world possible. IoT technology is also becoming more common in fire protection devices/systems and building automation systems. The aim of this thesis is to clarify and evaluate the use of IoT technology and its possibilities in improving fire safety of buildings. The basis of this thesis is to find out the benefits and threats of the technology when it is utilized in the area of fire safety and furthermore, can it bring cost effects to fire protection systems and their maintenance operation. In addition, the aim is to find out the ability of IoT to share data and also how IoT and smart technology is utilized in development of fire safety in Finnish buildings.

This study is a qualitative one. The material for this study was collected through theme interviews. An overall picture of the phenomenon being studied was carried out by interviewing people representing several different industries. A theme-based content analysis was performed to the theme interview material and the results were presented in the research results section. The Conclusions section highlights the main findings of the study and answers to main- and sub-research questions.

The most important finding of the study is that utilization of IoT and smart technology improves fire safety of buildings. Four main factors came to prominence concerning improvement of fire safety: improving operational reliability, accident prevention, enabling transmit of real-time information to rescue departments and utilizing sensing measurement sensors of automation systems in buildings. In addition, utilization of IoT technology can save costs in fire safety technology and its maintenance, especially in buildings with a large number of fire safety technique. Based on the conclusions reached, the use of IoT and smart technology in Finnish buildings is still rather low, especially in the area of fire safety.

ALKUSANAT

Diplomityöni aihe kehittyi opintojen yhteydessä. IoT ja sen tuomat hyödyt olivat esillä usealla opintojaksolla, josta heräsi kiinnostus tutkia sen soveltuvuutta myös paloturvallisuuden osa-alueelle. Oli siis tarve löytyy diplomityölle partneri, joka kiinnostuisi aiheesta. Sellaisen sain Suomen pelastusalan keskusjärjestöstä SPEK. Ensimmäiset kiitokset kuuluvat siis Suomen pelastusalan keskusjärjestölle sekä erityisesti turvallisuusasiantuntija Lauri Lehdolle, joka toimi työni ohjaajana. Ilman teidän tukea työ olisi varmasti jäänyt tekemättä kyseisestä aiheesta. Toiset kiitokset menevät Palosuojelun edistämissäätiölle, joka uskoi diplomityöni aiheeseen ja myönsi apurahan työlleni.

Kolmanneksi haluan kiittää työni ensimmäistä tarkastajaa erikoistutkija Satu Pekkarista työn hyvästä ohjauksesta sekä kommenteista, joiden avulla työstä saatiin aikaan eheä kokonaisuus. Neljännet kiitokset menevät kaikille niille henkilöille sekä heidän edustamilleen organisaatioille, jotka osallistuivat haastateltavaksi diplomityötä varten. Ilman teidän apua työn tekeminen olisi ollut mahdotonta. Olin erityisen ilahtunut siitä, miten avuliaita te olitte auttamaan minua työni eteenpäin viemisessä.

Viidenneksi haluan kiittää omaa työnantajaani Etelä-Karjalan pelastuslaitosta joustavuudesta, että minulla oli mahdollisuus suorittaa suurin osa opinnoista työni ohessa sekä päästitte opintovapaalle viimeistelemään tämän työn. Joskus työn ja opiskelun yhteensovittaminen oli erittäin vaikeaa.

Suurimmat kiitokset kuitenkin menevät kotijoukoille. Kiitokset vaimolleni Sintulle, että minulla on ollut TAAS mahdollisuus opiskella. Ehkä opinnoista voisi pitää nyt vähän pidemmän tauon. Lisäksi erityiskiitokset kuuluvat anopilleni, jonka lastenhoitoapu oli korvaamatonta, varsinkin diplomityön tekemisen aikana. Vierailusi on ollut myös Nuutin ja Paavon mieleen.

Imatralla 20.5.2018

Tuomas Pylkkänen

Sisällysluettelo

LYHENNELUETTELO

CE	Conformité Européenne
ICT	Information and Communication Technology, tieto- ja viestintätekniikka
IoT	Internet of Things
IoE	Internet of Everything
IP	Internet protocol
LPWAN	Low Power Wide Area Network
PARK	Pelastusajoneuvoon raportoiva kiinteistö
PRONTO	Pelastustoimen resurssi- ja onnettomuustilasto
REST	Representational State Transfer
RFID	Radio Frequency Identification
SaaS	Software as a Service
SPEK	Suomen Pelastusalan Keskusjärjestö
VOC	Volatile Organic Compound, haihtuvat orgaaniset yhdisteet
VTT	Teknologian tutkimuskeskus VTT Oy
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network
WWAN	Wireless Wide Area Network

1 JOHDANTO

Tämä työ on tutkimus IoT:n mahdollisuuksista rakennuksien paloturvallisuuden kehityksessä. Tavoitteena on löytää hyötyjä ja uhkia, joita IoT-teknologiaan liittyy, kun sitä hyödynnetään paloturvallisuuden osa-alueella. Tutkimusosan tiedonkeruu suoritettiin teemahaastatteluja tekemällä. Haastattelujen avulla pyrittiin saamaan vastauksia esitettyihin tutkimuskysymyksiin sekä löytämään siten uutta tietoa tutkittavasta ilmiöstä. Tässä luvussa esitellään tutkimuksen tausta ja luonne, tuodaan esiin tutkimuksen tavoitteet sekä aiheen rajaus.

1.1 Tutkimuksen tausta ja luonne

Tulipalot muodostavat yhden merkittävimmistä riskeistä kaikille rakennustyypeille. Paloturvallisuutta on Suomessa pyritty vuosikymmenien saatossa aktiivisesti kehittämään erilaisilla lainsäädännön uudistuksilla. Lainsäädännön uudistukset ovat koskeneet etupäässä uudis- ja korjausrakentamista, mutta myös olemassa oleville rakennuksille on tullut lisävaatimuksia. Tästä hyvänä esimerkkinä on palovaroittimien pakollisuus 2000-luvun alussa, joka tuli takautuvasti velvoitteeksi rakennuksiin, joissa yövytään. Erityisesti haluttiin parantaa asuinrakennuksien paloturvallisuutta, koska niissä tapahtuvat yleisimmin kuolemaan johtaneet tulipalot. Ihmisiä menehtyy sekä loukkaantuu vakavasti rakennuspaloissa edelleen. Lisäksi tulipalot aiheuttavat vuosittain useiden miljoonien omaisuusvahingot (Pelastusopisto 2017b, s. 28-30). Näiden vahinkojen lisäksi tulipalot voivat usein lopettaa myös koko liiketoiminnan. Esimerkiksi erillisten tutkimuksien mukaan yrityksistä:

- 30% lopettaa toimintansa vuoden sisällä,
- 60% yrityksistä lopettaa toimintansa kahden vuoden sisällä,
- 70% yrityksistä lopettaa toimintansa viiden vuoden sisällä, kun kohdataan laajamittainen tulipalon. (Baird 2010, s.19).

Paloturvallisuuden parantamiseksi onkin näiden seikkojen vuoksi paljon tekemätöntä työtä, ja siksi on tehtävä aktiivisesti selvitystyötä. Yksi keino rakennuksien paloturvallisuuden parantamiseksi on hyödyntää uutta teknologiaa, jotta syttymien määrää saadaan

vähennettyä ja tapahtuneita syttymiä rajoitettua entistä tehokkaammin. Anturointia lisäämällä tulipalo saadaan aikaisemmin havaittua, mikä antaa lisää aikaa ihmisille ja viranomaisille reagoida onnettomuustilanteeseen. Uudet teknologiat, älykkäämmät laitteet sekä järjestelmien ja laitteiden yhteen liitettävyydet voivat avata uusia mahdollisuuksia kustannustehokkaalle arjen ja asumisenturvallisuuden parantamiselle. Integraatiolla, datan analysoinnilla ja sen hyötykäytöllä on mahdollista tehostaa palontorjunnan toteuttamista rakennuksissa.

Viime vuosina on käyty aktiivisesti keskustelua älykkäistä rakennuksista ja älykodeista (Intelligent Building, Smart Building, Smart Home). Rakennuksista osa pyritään tekemään nykyisin entistä älykkäämpiä. Älykkyyden lisäämisessä keskustelujen yhteydessä on noussut esille IoT ja sen hyödyntäminen rakennuksien älykkäässä ympäristössä. Markkinoilla on IoT-ratkaisuja, jotka on tarkoitettu rakennuksien talotekniikasta aina kotien automaatiojärjestelmiin. Tällä hetkellä eletäänkin varsinaista IoT-hypeä, koska kyseistä teknologiaa on ryhdytty hyödyntämään lähes kaikessa. Osaltaan tähän vaikuttaa se, että kehityksen yksittäiset tekniset esteet on saatu vähitellen korjattua. IoT:stä on kasvamassa kypsempi ja paljon tuottavampi teknologia. Voidaankin todeta, että nykyisin ainoat todelliset teknologian rajoitukset ovat niitä, jotka johtuvat mielikuvituksen puutteesta (Saarikko et al 2017, s. 3).

Erilaiset digitaaliset teknologiat yhdistyvät yhä tiiviimmin osaksi ihmisten jokapäiväistä elämää, joista tällä hetkellä kehityksen kohteena ovat erityisesti olleet tiedon, anturiteknologian ja Internetin hyödyntäminen (Palta 2016, s.9). Näin ollen myös IoT on saanut osakseen valtavaa huomiota, koska sen avulla on mahdollista digitalisoida fyysinen maailma. Vuoden 2015 aikana arvioitiin, että maailmassa oli noin yhdeksän miljardia Internetiin yhdistettyä laitetta. Tähän lukumäärään on laskettuna mukaan tietokoneet ja älypuhelimet. Laskelmien mukaan seuraavan vuosikymmenen aikana laitteiden määrä tulee kasvamaan merkittävästi. Eri arvioiden mukaan Internetiin yhdistettyjen laitteiden lukumäärä kasvaa vuoteen 2025 mennessä 25 miljardiin tai jopa 50 miljardiin laitteeseen. Näiden laskelmien perusteella IoT:ssä onkin katsottu olevan valtavaa potentiaalia, koska kasvun myötä sen taloudelliset vaikutukset voivat olla vuoteen 2025 mennessä aina 3,9 biljoonasta jopa 11,1 biljoonaan dollariin. (McKinsey Global Institute 2015, s.7, 17).

Uuden teknologian tulee olla sellaista, että siitä saadaan hyötyä. Ilman tätä ei saavuteta mitään hyötyä. Pelkästään laitteen liittäminen Internetiin tuskin tuo lisäarvoa. IoT:n yksi merkittävimmistä hyödyistä on IoT -laitteiden ja - antureiden kautta kerätty data. IoT mahdollistaakin Big Datan kertymisen, jonka avulla voidaan luoda lisäarvoa eri toiminnoille. Kerättyä tietoa voidaan hyödyntää erilaisiin tarpeisiin. Jakamalla dataa eri toimijoille voidaan esimerkiksi ennakoivasti tehdä tarvittavia ylläpitotoimenpiteitä tai dataa analysoimalla lisätä toiminnan tehokkuutta. Mahdollisuudet ovat siis valtavat. (McKinsey Global Institute 2015, s. 4).

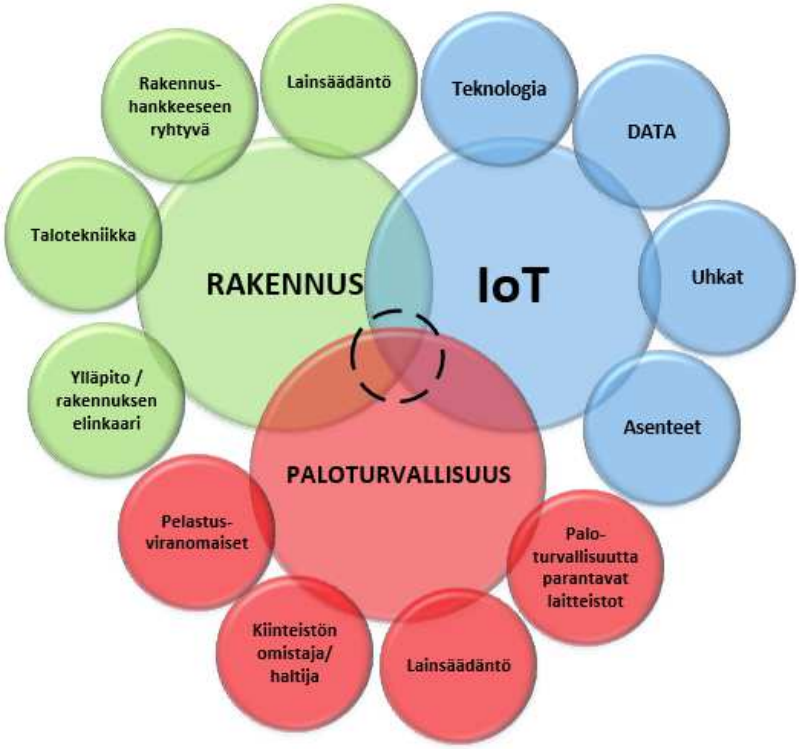
IoT:stä saatavat hyödyt perustuvat teknologian avulla saavutettavaan korkeampaan älykkyyteen ja sen suureen skaalautuvuuteen. Halutut toimenpiteet on mahdollista toteuttaa useilla eri tavoilla ja hyödyntäen useita eri tekniikoita ja menetelmiä. IoT on vielä hyvin uusi asia paloturvallisuutta parantavissa laitteistoissa ja paloturvallisuudessa yleensäkin. Sen vuoksi on tarpeellista, että sen soveltuvuutta myös paloturvallisuuden osa-alueelle tutkitaan tarkemmin.

Tämän työn ohjaajana on toiminut Suomen Pelastusalan Keskusjärjestö SPEK. SPEK kiinnostui työn aiheesta, koska IoT nähdään kiinnostavana teknologiana ja kehityssuuntana. Lisäksi tätä työtä hyödyntämällä SPEK pystyy luomaan kokonaiskuvan turvallisuusympäristön kehittymisestä sekä hyödyntämään saatua tietoa tulevaisuuden vision ja strategian edistämiseen. Tämän diplomityön tekemistä on tukenut lisäksi Palosuojelun edistämissäätiö.

1.2 Tutkimuksen tavoitteet

Tämän työn tavoitteena on selvittää miten IoT-teknologiaa hyödyntämällä voidaan parantaa rakennusten paloturvallisuutta sekä mihin suuntaan teknologiakehitys voi tulevaisuudessa edetä. Tavoitteena on tuoda esille miten IoT-teknologiaa on hyödynnetty Suomen rakennuskannan paloturvallisuutta parantavissa laitteistoissa sekä löytää hyötyjä ja uhkia, joita teknologian lisäämiseen voi kohdistua. Erityisesti hyötyjen löytämisessä keskitytään rakennuksiin asennettuihin tai asennettaviin paloturvallisuutta parantaviin laitteistoihin. Työssä on myös tarkoituksena selvittää mille eri toimijoille IoT-laitteista ja järjestelmistä kerättyä dataa on hyödyllistä jakaa sekä onko mahdollista datan jakamisella, hyödyntämisellä tai sen rikastamisella saada aikaan kustannussäästöjä itse palo-

turvallisuustekniikasta tai niiden kunnossapidosta. Lisäksi tavoitteena on selvittää laitteiden ja järjestelmien rajapintojen mahdollisuudet älykkäiden laitteiden ja järjestelmien välisissä integraatioissa.



Kuva 1. Tutkimuksen keskeiset tekijät ja tavoitteet

Työn keskeiset tekijät sekä tavoitteet on esitetty kuvassa 1. Kuvassa esitettävien kolmen ison ympyrän (rakennus, paloturvallisuus ja IoT) kautta muodostuvat työn päätekijät. Päätekijät muodostuvat pienemmistä tekijöistä. Näistä asioista muodostuu pitkälti työn teoriaosuus. Päätekijöiden ympyröiden leikkauslinjojen sisälle (merkitty katkoviivalla) muodostuu tämän työn pää- ja alatutkimuskysymykset, joihin pyritään löytämään vastauksia. Seuraavassa on esitetty tämän työn päätutkimuskysymys sekä alatutkimuskysymykset:

Työn päätutkimuskysymys on:

- Miten IoT - teknologialla voidaan parantaa rakennuksien paloturvallisuutta nyt ja tulevaisuudessa?

Alatutkimuskysymykset ovat:

- Miten IoT - teknologiaa hyödynnetään paloturvallisuuden kehityksessä Suomessa?
- Voidaanko IoT – teknologialla sekä sen avulla kerättyä dataa hyödyntämällä saada aikaan kustannussäästöjä paloturvallisuustekniikassa ja kunnossapidossa?
- Mitkä ovat rakennuksissa käytettyjen IoT - teknologioiden integraatioiden rajapintojen mahdollisuudet ja uhat datan jakamisessa eri toimijoille?

1.3 Aiheen rajaus

Työ rajataan koskemaan rakennuksia, joissa yövytään. Tällaisia rakennuksia ovat esimerkiksi asuin-, majoitus- ja hoitolaitosrakennukset. Teollisuus- ja liikerakennukset on jätetty tästä työstä tietoisesti pois, jotta työn laajuus ei kasvaisi liian suureksi. Etupäässä keskitytään rakennusten aktiivisiin palontorjuntalaitteistoihin, mutta esille on voitu tuoda ratkaisuja myös passiiviseen palontorjuntaan liittyen. Työssä käsitellään sammutus- ja pelastustoiminnassa käytettäviä (fire-fighting) IoT-ratkaisuja vain datan jakamisen ja sen hyödyntämisestä saatavien hyötyjen näkökulmasta.

Tässä työssä esitetään IoT-teknologiaa vain yleisellä tasolla, miten sitä voidaan hyödyntää sekä millä tavoin siitä saadaan hyötyä paloturvallisuuden kehityksessä. Tarkoituksena ei ole esitellä tai tutkia tarkkaa teknologian soveltuvuutta eri paloturvallisuutta parantaville laitteistoille tai tuoda esiin järjestelmäkohtaisia rajapintojen mahdollisuuksia. Tietoturvaan ja tietosuojaan liittyvät asioita käsitellään myös hyvin pintapuolisesti.

2 IoT-TEKNOLOGIA

Teknologioita yhdistämällä on mahdollista kerätä dataa erilaisissa ympäristöissä olevista toimilaitteista ja antureista. Kerättyä dataa hyödyntämällä sekä järjestelmien välisillä integraatioilla voidaan oppia tuntemaan ympäristöä paremmin ja tunnistamaan siinä tapahtuvia muutoksia. Analysoidun datan perusteella eri laitteistot ja järjestelmät voivat ohjautua automaattisesti ilman ihmisen puuttumista siihen. Tällaista ympäristöä voidaan kutsua älykkääksi ympäristöksi, jossa yhtenä merkittävänä tekijänä tällä hetkellä on IoT. (soveltaen, Raun 2016, s. 1-2).

Tässä luvussa esitellään älykkääseen ympäristöön liittyviä käsitteitä, teknologiaa ja tekniikkaa. Luvussa esitellään lisäksi IoT -teknologiaan tiivisti liittyviä asioita, kuten: tietoliikennemallit, arkkitehtuuri, toimilaitteet ja anturit, erilaiset tiedonsiirtomenetelmät, alustat, rajapinnat, data analytiikka, pilvilaskenta, tietoturvallisuus ja tietosuojaan liittyvät asiat sekä lopuksi tuodaan esille digitalisuuden haasteita ja vaikutuksia.

2.1 Älykkään ympäristön käsitteet

2.1.1 Internet of Things

Internet of Things (IoT) on määritelty useilla eri tavoilla, koska sille ei ole toistaiseksi laadittu mitään virallista määritelmää. Termin Internet of Things keksijänä voidaan pitää digitaalisten innovaatioiden asiantuntijaa Kevin Ashtonia, joka toi sen esille vuonna 1999 RFID teknologian hyödyntämisen yhteydessä. (Madakam et al 2015, s. 164-165; Wortmann & Flutcher 2015, s. 221-222). IoT:tä voidaan pitää paradigmana, jossa sensoreilla, toimilaitteilla, lähettimellä ja prosessoreilla varustetut fyysiset esineet kommunikoivat keskenään merkityksellisessä tarkoituksessa. IoT:ssä ei hyödynnetä mitään yhtä ainoaa teknologiaa, vaan se on eri teknologioiden yhdistämistä toimivaksi kokonaisuudeksi. IoT-anturit ja -toimilaitteet muodostavat yhteyden fyysiseen ympäristöön ja niitä on mahdollista eri tavoin hallita Internet-verkon yli. Näiden antureiden ja toimilaitteiden avulla on mahdollista kerätä dataa eri tavoin. Kerätty data tallennetaan ja sitä voidaan analysoida ja hyödyntää moniin tarkoituksiin. (Sethi & Sarangi 2016, s. 1). Seuraavassa on esitetty kaksi hieman erilaista määritelmää IoT:lle.

IoT on avoin ja kattava älykkäiden esineiden verkko, jolla on kyky automaattisesti organisoida, jakaa tietoa, dataa ja resursseja, reagoida ja toimia tilanteissa sekä ympäristön muutoksissa. (Madakam et al 2015, s. 165)

International Telecommunication Union on määritellyt IoT:n tietoyhteiskunnan maailmanlaajuiseksi infrastruktuuriksi, joka mahdollistaa kehittyneiden palvelujen toteuttamisen yhdistämällä fyysiset ja virtuaaliset esineet (things) olemassa olevaan sekä kehittyvään tieto- ja viestintäteknologiaan. Laajemmasta näkökulmasta katsottuna IoT:tä voidaan pitää visiona, jolla on vaikutuksia teknologiaan ja yhteiskuntaan. (International Telecommunication Union 2012, s. 2)

2.1.2 Industrial Internet

Industrial Internetillä, eli teollisella Internetillä tarkoitetaan ennen kaikkea yritysten digitalisoitumista, joka mahdollistaa teollisuuden taloudellisen kehityksen. Lisäämällä koneiden älykkyyttä, verkottamalla koneet ja laitteet sekä keräämällä ja analysoimalla tehokkaasti dataa, voidaan vaikuttaa tuotantokustannusten vähenemiseen eri tavoin, mikä tuo merkittävästi uusia tehokkuusetuja sekä nopeuttaa näin tuottavuuden ja talouden kasvua. Industrial Internet voidaan katsoa koostuvan kolmesta pääelementistä: älykkäät koneet, edistynyt analytiikka sekä ihmiset työssä. Ensimmäisessä elementissä lisäämällä tuotannossa käytettäviin koneisiin lisää anturointia, ohjauksia sekä sovelluksia ja yhdistämällä ne yhteiseen tietoverkkoon saadaan luotua älykkäitä koneita. Edistyneen analytiikan avulla on mahdollista yhdistää fysikaalisien suureiden mittaaminen sekä syvä alakohtainen osaaminen. Industrial Internet mahdollistaa eri puolella maapalloa olevien työntekijöiden yhdistämisen digitaaliseen ympäristöön, jonka kautta työntekijöillä on mahdollista vaikuttaa teollisuuden valmistusprosesseihin, laatuun, ylläpitoon ja turvallisuuteen entistä paremmin. (Juhanko & Jurvansuu 2015, s. 3-4; Evans & Annunziata 2012, s.3)

2.1.3 Internet of Everything

Teknologiaympäristömme on muutoksessa sen jatkuvan kehittymisen vuoksi. Älykkäiden esineiden määrä, datan tallennuskapasiteetti sekä viestintäteknologian kehitys ovat muuttamassa ympäristöämme kohti Internet of Everything (IoE) käsitettä. Käsitteellä

IoE (kaiken Internet) tarkoitetaan ihmisten, prosessien, datan sekä esineiden älykästä yhdistymistä. Prosessien osalta varsinkin liiketoimintaprosessit ovat keskiössä. Sosiaalisen ympäristön sekä laitteiden verkostojen yhdistymisen vaikutuksilla tulee olemaan jatkossa suuri vaikutus lähes kaikkeen toimintaan. IoE yhdistää kaiken jopa biljooniksi eri verkostoiksi, joissa näiden yhteyksien kautta syntyy valtava määrä dataa, jota ei aikaisemmin ole ollut mahdollista luoda. Tätä valtavaa datan määrää analysoimalla ja hyödyntämällä mahdollisuudet ovat rajattomat. (Yang et al. 2017, s. 1)

Kaiken verkottamisessa saadaan luotua toiminnalle myös enemmän arvoa. IoE:n avulla voi syntyä uusia liiketoimintamahdollisuuksia sekä rikkaita kokemuksia. Tästä voivat hyötyä niin yksilöt, yritykset kuin jopa kansakunnat. IoE määritelmä on hyvin lähellä Industrial Internetin määritelmää. Uutena osana määritelmässä ovat mukana yhteiskunnalliset ja ihmisten kokemukseen tulevat hyödyt. (Juhanko & Jurvansuu 2015, s. 13). Useat Internet-paradigmat kuuluvat IoE:n sateenvarjon alle kuten Internet of Things (IoT), Internet of People (IoP) ja Industrial Internet (II) (Yang et al. 2017, 1).

2.1.4 Älykkäät laitteet (Smart devices)

Älykäs laite on fyysinen elementti, joka voidaan tunnistaa koko sen käytön ajan ja se on vuorovaikutuksessa ympäristön kanssa. Lisäksi älykkäillä laiteilla on oma käyttöliittymä ja ne voivat kommunikoida keskenään tai muiden laitteiden tai järjestelmien kanssa. (Gonzales Garcia et al 2017, s. 8). Älykkäitä laitteita on nykyisin markkinoilla useita. Jotta laitetta voidaan pitää älykkäänä, tulisi sillä olla seuraavat kolme ominaisuutta:

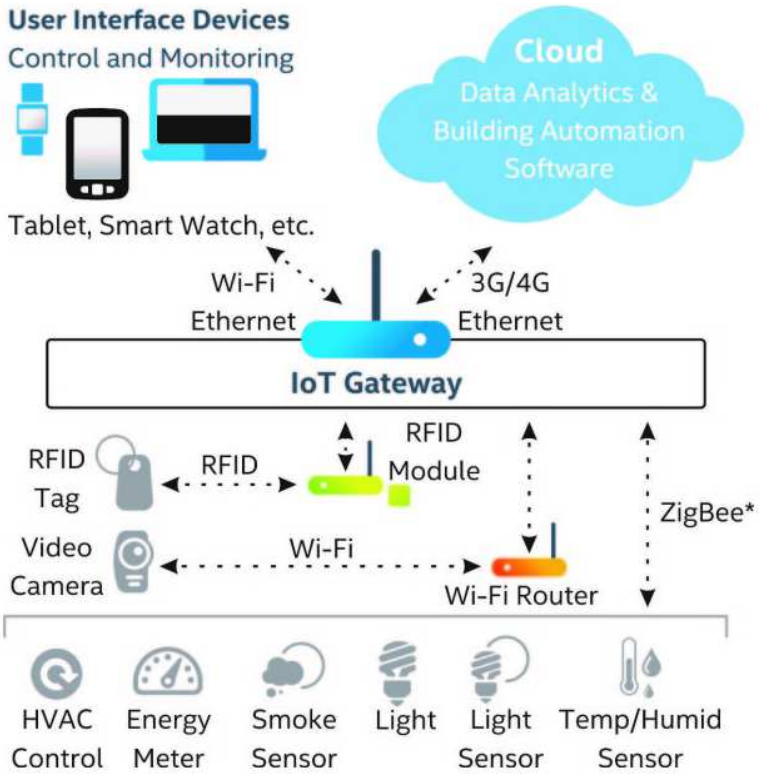
- Yhdistää ja vaihtaa dataa muiden älykkäiden tai siihen yhdistettyjen laitteiden kanssa
- Tunnistaa muutokset ympäristössä ja oppii tuntemaan mikä on normaalia, kun sitä ei ohjelmoida tiettyihin toimintoihin tietyn ajan kuluessa
- Käyttää yhtä integroitua älypuhelinsovellusta tai muuta verkkoon liitetyn laitetta kaikkien toimintojen hallitsemiseksi. (Links 2017, s. 56)

2.1.5 Big data

Big datalle ei ole olemassa tarkkaa määritelmää. Voidaan katsoa, että se käsitteenä viittaa kahteen asiaan. Datan määrä on lisääntynyt ja monipuolistunut kiihtyvällä vauhdilla viime vuosina ja sen voidaan katsoa kiihtyvän tulevaisuudessa entisestään. Toinen asia liittyy datan tallentamiseen ja sen liikuteltavuuteen liittyviin tekniikoihin sekä yleisen digitalisaation kehitykseen. Datan tallentaminen on entistä helpompaa, jota tallennetaan esimerkiksi pilvipalveluihin. Big data ilmiönä käsittelee datan määrän kasvua, datan sisällön monipuolistumista ja painetta tunnistaa oikea ja oleellinen data sekä reagoida nopeasti siitä jalostettuun informaatioon. Datasta onkin tullut tärkeä raaka-aine ja resurssi monessa toiminnassa. Tämän vuoksi ilmiö ei sinällään liity pelkästään teknologian kehitykseen, vaan sillä on ennen kaikkea taloudellisia ja yhteiskunnallisia vaikutuksia. Datan hyödyntäminen tuo aivan uusia innovaatiomahdollisuuksia. Datasta voidaan katsoa tulevan tulevaisuuden öljy. Ne, joilla on parhaimmat edellytykset hyödyntää ja rikastaa dataa, tulevat menestymään parhaiten. (Salo 2014, s.6-8)

2.2 Tietoliikennemallit

Kaksi yleisintä tietoliikennemallia ovat suora ja yhdyskäytäväpohjainen (gateway) tietoliikennemalli. Suorassa tietoliikennemallissa IoT-laite lähettää ja vastaanottaa dataa suoraan verkosta, kun taas yhdyskäytäväpohjaisessa tietoliikennemallissa IoT-laitteet ovat yhdistetty yhdyskäytävään, joka lähettää dataa tietokantaan (database), mistä tietoa tarvitsevat osapuolet hakevat sitä kun tarvitsevat sitä. (Kuusijärvi et al 2016, s 261). Kuvassa 2 on esitetty IoT-pohjainen rakennusautomaatiojärjestelmän tietoliikennemalli, jossa antureita ja toimilaitteita on yhdistetty yhdyskäytävän tai erillisen hubin kautta Internetiin.



Kuva 2. IoT-pohjaisen rakennusautomaatiojärjestelmän esimerkki (Free 2015)

Laite-pilvipalvelu (Device-to-Cloud) tietoliikennemallissa IoT-laite yhdistetään esimerkiksi suoraan sovellustarjoajan pilvipalveluun datan vaihtamiseksi tai hallitsemaan viestiliikennettä. Tässä voidaan hyödyntää erilaisia tiedonsiirtoverkkoja kuten Wi-Fi –verkkoa, jota hyödyntämällä luodaan yhteys laitteen ja Internetin välille. Tällä tavoin laite saadaan yhdistettyä pilvipalveluun. Kyseistä tietoliikennemallia käytetään varsinkin kuluttajille suunnatuissa IoT-laitteissa. (Kulkarni & Kulkarni 2017, s. 89)

Useissa tapauksissa paikallisena yhdyskäytävänä toimii älypuhelin, jolla on käytössä sovellus, joka kommunikoi laitteen kanssa ja välittää tiedot pilvipalveluun. Yksinkertaistettuna tämä tarkoittaa, että sovellusohjelmisto toimii paikallisessa yhdyskäytävälaitteessa, joka toimii välittäjänä laitteen ja pilvipalvelun välillä tarjoamalla tietoturvaa sekä muita toimintoja kuten datan tai protokollan kääntämistä. Useissa tapauksissa paikallisena yhdyskäytävänä toimii älypuhelin, jolla on käytössä sovellus, joka kommunikoi laitteen kanssa ja välittää tiedot pilvipalveluun. Toinen mahdollisuus laite-yhdyskäytävämallissa on hyödyntää keskitintä (hub), jota käytetään esimerkiksi kotiautomaatio-sovelluksissa. Keskitin on erillinen yhdyskäytävälaite, jolla on mahdollista

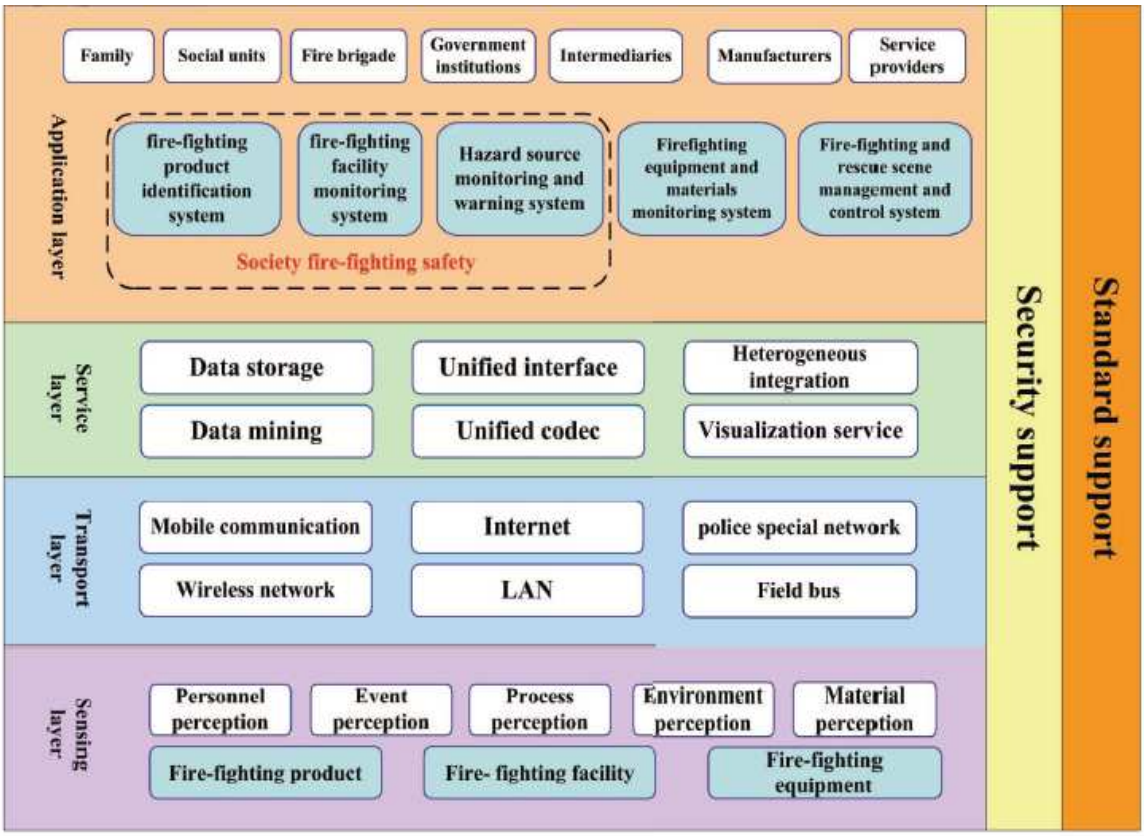
yhdistää jopa eri tuoteperheen IoT-laitteita. Siten laitteet saadaan kytketyksi pilvipalveluun, jonka kautta käyttäjällä on pääsy laitteisiin älypuhelinsovelluksella ja Internet-yhteydellä. (Kulkarni & Kulkarni 2017, s. 89-90)

Kolmas malli on back-end data-sharing malli, joka on tietoliikennearkkitehtuuri, jossa käyttäjät voivat analysoida älykkäiden laitteiden pilvipalveluun välittämää dataa. Lisäksi pilvipalvelussa on mahdollista analysoida muistakin lähteistä tullutta dataa. Kyseessä on siis laajennettu laite-pilvipalvelu tietoliikennemallista. Back-end data-sharing arkkitehtuuri mahdollistaa, että yksittäisten IoT-laitteiden datavirrat voidaan yhdistää ja analysoida. Tehokkaimmillaan arkkitehtuurin avulla voidaan yhdistää eri sovellustarjoajien pilvipalveluun tallennettu data. (Rani & Mayuri 2016, s. 4717)

IoT-teknologiassa voidaan hyödyntää erilaisia verkkotopologioita. Verkkotopologialla tarkoitetaan verkon perusrakennetta, eli miten verkon laitteet tai anturit on liitetty toisiinsa. IoT-teknologiassa käytetään yleensä tähti- tai mesh-verkkotopologioita. Tähtitopologiassa kukin toimilaite tai anturi on kytketty suoraan yhdyskäytävää (gateway), joka välittää dataa liitetyistä laitteista tai antureista eteenpäin. Mesh-topologiassa laitteet kytkeytyvät muihin alueen sisällä oleviin laitteisiin ja verkossa olevat solmut voivat toimia yksinkertaisina solmupisteinä, kuten anturisolmuina (sensor node), jotka myös reitittävät liikennettä. Mesh-verkot ovat monimutkaisempia kuin tähtitopologeilla varustetut verkot. Niiden etuna on, että ne ovat joustavampia, koska ne eivät ole riippuvaisia yhdestä yhdyskäytävästä. (Gerber 2017, s. 3-4)

2.3 IoT – Arkkitehtuuri

IoT – teknologian toimivuuden lähtökohtana on se, että laitteet ja anturit sekä tiedonsiirtoverkot saadaan yhdistettyä toisiinsa. Koko ketjun tulee olla toimiva, jotta voidaan luoda toimiva silta fyysisen ja virtuaalisien maailmojen välille. Tämä toimivuudenketju voidaan esittää IoT - järjestelmäarkkitehtuurin avulla. IoT - arkkitehtuurin suunnittelu sisältää useita tekijöitä, kuten verkottumista, viestintää, liiketoimintamalleja, prosesseja sekä tietoturvallisuutta. (Li et al 2014, s. 246)



Kuva 3. Palontorjunta IoT:n arkkitehtuurimalli (Wang et al 2014, s. 423)

IoT - arkkitehtuurille ei ole olemassa mitään yleistä mallia, josta olisi sovittu maailmanlaajuisesti. Erilaisia ja eritasoisia malleja on esitetty eri tutkijoiden toimesta (Sethi & Sarangi 2016, s. 2). Wang et al (2014) ovat esittäneet artikkelissaan paloturvallisuuslaitteistoihin liittyvän IoT – arkkitehtuurimallin, joka on esitetty kuvassa 3. Vijayalakshmi & Muruganand (2017) ovat taas kehittäneet palonvalvontajärjestelmää (fire monitoring system), jossa on päädytty samanlaiseen arkkitehtuurimalliin. Kyseessä on malli, joka on jaettu neljään kerrokseen: havainnointikerros (sensing layer), välityskerros (transporting layer), palvelukerros (service layer) sekä käyttösovelluskerros (application layer). (Wang et al 2014, s. 422; Vijayalakshmi & Muruganand 2017, s. 2142)

Havainnointikerros on arkkitehtuurin peruskerros, joka tunnistaa esineet tai toimilaitteet esimerkiksi määritellyillä yksilöllisillä IP-osoitteilla. Kerroksen tehtävänä on kerätä dataa ja tilatietoa antureista ja toimilaitteista (Sethi 2017, s. 1616). Anturit tai toimilaitteet voivat olla paloteknisiä laitteistoja tai niissä olevia antureita, joista tieto voidaan siirtää erilaisiin järjestelmiin järjestelmäintegraatioiden avulla (Wang et al 2014, s. 422).

Välityskerrosta käytetään siirrettäessä antureista tai toimilaitteista kerättyä dataa. Sen tehtävänä on ottaa vastaan digitaalisia signaaleja anturi- ja toimilaiteverkoista sekä välittää se yhdyskäytävälle erilaisen verkkojen kautta (Sethi 2017, s. 1616). Sopiva lähetys- ja kirjausmenetelmät valitaan aina tarpeen mukaan huomioiden käytössä olevat tiedonsiirtomenetelmät. Välityskerroksen tarkoituksena on välittää dataa sensoreista tai toimilaitteista eri järjestelmäalustoille. (Wang et al 2014, s. 422)

Palvelukerrosta hyödynnetään tietojen tallennukseen, heterogeenisiin integraatioihin, yhtenäisiin käyttöliittymiin, tiedonlouhintaan sekä visualisoimaan palvelut eri tietoresursseiksi (Wang et al 2014, s. 422). Palvelukerros siis tallentaa, analysoi ja prosessoi suuren määrän dataa. Se hallitsee ja tarjoaa monipuolisen joukon eri palveluita, kuten datavirran hallintaa, tietoturvallisuutta, tietokantoja, big data moduuleita, laitteiden mallinnuksen konfigurointia ja hallintaa sekä pilvilaskentaa. (Sethi 2017, s. 1616)

Käyttösovelluskerros vastaa sovelluskohtaisen palvelun tarjoamisesta eri käyttäjille (Sethi 2017, s.1616). Käyttösovelluskerrosta käytetään integrointien jakamiseen, datan älykkääseen analysointiin sekä palontorjuntaan liittyvien laitteiden prosessiohjaukseen. Sen avulla voidaan tarjota sovelluspalveluja eri toimijoille kuten asukkaille, pelastustoimelle, kiinteistön omistajille, laitevalmistajille sekä huolto- ja kunnossapitotoimijoille. (Wang et al 2014, s. 423)

2.4 Toimilaitteet ja anturit (”Things”)

Älykkäät anturit ja toimilaitteet ovat laitteita, jotka ovat yhteydessä fyysiseen ympäristöön (Sethi & Sarangi 2016, s. 1). Jokainen elektroninen laite, joka on mahdollista liittää Internetiin ja kerätä sen avulla tietoa, voidaan kutsua älykkääksi anturiksi, ja älykkääksi toimilaitteeksi, jos sen avulla voidaan suorittaa edellä mainitun lisäksi erilaisia toimintoja (Gonzales Garcia et al 2017, s 7). Älykkäät toimilaitteet ja anturit muodostavat osan älykkäästä ympäristöstä. Ne toimivat IoT-arkkitehtuurin peruskerroksessa eli havainnointikerroksessa, jossa niitä voidaan hallinnoida sekä kerätä tila- ja olosuhdetietoja. Data tallennetaan analysointia ja hyödyntämistä varten. Toimilaitteilla tai antureilla voi olla yksilöllinen IP-osoite tai ne voivat olla yhdistettyinä esimerkiksi erillisen Hubin kautta Internetiin. (Sethi 2017, s. 1616; Madakam 2015, s 250).

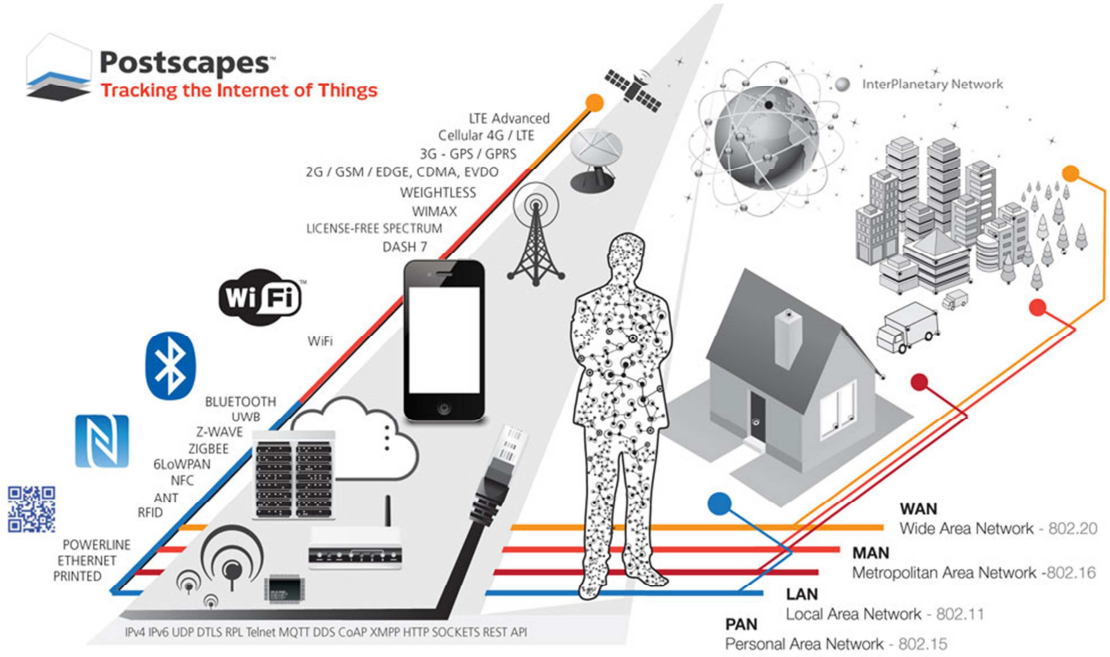
Älykkäitä toimilaitteita tai antureita voidaan kutsua myös esineiksi (things, objects). Älykkäät esineet ovat itsenäisiä fyysisiä tai digitaalisia esineitä, joihin on lisätty tunnistus, prosessointi ja verkkoon liitettävyys ominaisuuksia. Älykkäänä anturina voidaan käsittää älypalovaroitin, kun se välittää tietoa sen tilasta sekä tallentaa kerätyn datan esimerkiksi pilvipalveluun. Toimilaite on laite, jota käytetään ympäristön muutoksen aikaansaamiseksi kuten ilmastoinnin säätämiseen. Yleisimpänä toimilaitteena voidaan mainita myös älypuhelin (Sethi & Sarangi 2016, s. 1). Älykkäät anturit tai toimilaitteet voivat olla langattomia tai langallisia (Madakam 2015, s. 250). Nykyisin älykkäät anturit ovat enimmäkseen pienikokoisia, suhteellisen edullisia ja kuluttavat vähän virtaa. Rajoittavana tekijänä voidaan pitää virtalähteen kapasiteettiä, jonka vuoksi anturit eivät kommunikoi tai välitä tietoa koko aikaa. (Sethi & Sarangi 2016, s. 5, 9)

2.5 Tiedonsiirtomenetelmät

IoT ei edellytä mitään tarkkaa tiedonsiirtotekniikkaa, joten erilaisia tiedonsiirron vaihtoehtoja on useita. IoT:ssä hyödynnetään yleensä langatonta verkkoa ja tiedonsiirtoa. Kuvassa 4 on esitetty millaisia langattomia verkkoja ja tiedonsiirtoon käytettäviä standardeja IoT:ssa hyödynnetään. Langattomat verkot voidaan jakaa neljään eri kategoriaan niiden kattavuusalueen ja kantavuuden mukaan: Wireless Personal Area Network (WPAN), Wireless Local Area Network (WLAN), Wireless Metropolitan Area Network (WMAN) ja Wireless Wide Area Network (WWAN). (International Electrotechnical Comission, 2014, s. 22)

WPAN – verkossa tiedonsiirron kantama on vain kymmeniä metrejä, jonka vuoksi laitteet saadaan kommunikoimaan vain lähietäisyydeltä. PAN - laitteella on yleensä pieni lähetysteho ja ne käyttävät varaukseltaan pieniä virtalähteitä. Tunnetuin PAN- verkon standardi on Bluetooth, joka on yleisesti käytetty toiminto esimerkiksi yhdistämällä laitteita älypuhelimeen. (Lethaby 2017, s.5). Bluetooth standardin lisäksi yleisiä kodin automaatiojärjestelmissä käytettävistä standardeja ja protokollia ovat ZigBee, Z-Wave ja Thread. Z-Wave ja Zigbee ovat yhdet yleisimmin käytetyistä kodin automaatiojärjestelmien langattomista standardeista. Niiden etuna on laaja valikoima erilaisia standardia tukevia langattomia laitteita, jotka on helppo liittää järjestelmiin. Heikkoutena voidaan pitää niiden varsin alhaista tiedonsiirtonopeutta, joka Z-Wave:lla on ZigBee:tä huo-

nompi. Thread on taas avoin langaton protokolla, joka hyödyntää vain IPv6 uuden sukupolven Internet protokollaa. Se on suunniteltu ennen kaikkea tulevaisuuden IoT:n tarpeisiin. (Parrish 2017).



Kuva 4. Verkkojen kattavuusalueet ja käytettävät standardit (Postcapes 2018)

WLAN – verkoissa kantama voi olla nykyisin yli 100 metriä. WLAN – verkoista käytetään usein nimitystä Wi-Fi - verkko, joka on yleisesti käytetty verkko asuinrakennuksissa ja julkisissa tiloissa. Wi-Fi - verkon etuna on sen hyvä tiedonsiirtonopeus, kun taas sen heikkoutena on korkea virrankulutus. Suuren suosion vaikutuksesta Wi-Fi on hyvin yhteensopiva eri laitteiden kanssa ja siksi sen avulla on mahdollista muodostaa Internet-yhteys kustannusedullisesti. (Lethaby 2017, s.5-8)

WMAN - verkolla voidaan saavuttaa jopa yli 25 km kantavuus, jonka vuoksi sillä on mahdollista muodostaa kaupungin laajuinen peittoalue. Etuna WMAN - verkossa on suuri lähetysteho, mutta sillä on suhteellisen alhainen tiedonsiirtokapasiteetti. Esimerkkeinä WMAN - verkoista voidaan mainita WiMAX ja LTE (Lethaby 2017, s.5)

Laajimman kantavuusalueen verkon muodostaa WWAN - verkko, joka voi kattaa vaikka koko maapallon. WAN - verkko on muodostunut monimutkaisista langallisista ja langattomista yhteyksistä. Internetiä voidaan pitää yhtenä WAN-verkkona. (Lethaby

2017, s.5). WWAN- verkoista yksi käytetyimmistä on 3G/4G matkapuhelinverkot, jotka ovat avaintekijöitä tämän päivän IoT-teknologiassa. Matkapuhelinverkon globaalin käytettävyyden ja hyvän tiedonsiirtonopeuden vuoksi 3G/4G matkapuhelinverkkojen hyödyntäminen IoT:ssä on hyvinkin yleistä. (AT&T 2016, s. 3-5). Lähitulevaisuudessa IoT:ssä voidaan hyödyntää uuden sukupolven 5G-verkkoa. Sen etuina on nykyistä 4G LTE – matkapuhelinverkkoa nopeampi tiedonsiirto, tiedonsiirto on luotettavampaa sekä tiedonsiirtoviive tulee pienenemään. Tämä mahdollistaa esimerkiksi reaaliaikaisen videokuvan siirtämisen langattomassa verkossa paljon tehokkaammin. Lisäksi 5G-verkkoon on mahdollista kytkeä entistä enemmän laitteita. (Brake 2016, s.4-6).

Tulevaisuudessa matkapuhelinverkot tulevat kehittymään entisestään. Puhutaan jo 6G- ja 7G-verkoista, vaikka 5G-verkko ei ole vielä edes käytössä. Esimerkiksi 6G-verkon teoreettinen tiedonsiirtonopeus on arvioitu kasvavan 5G-verkkoon verrattuna kymmenkertaiseksi. Se on arvioitu kattavan koko maailmanlaajuisen alueen, jonka yhteydessä tullaan hyödyntämään myös satelliittiteknologiaa. Siten saadaan parannettua suorituskykyä, tehokkuutta ja luotettavuutta. 6G-verkosta seuraavan sukupolven 7G-verkko tulee olemaan paranneltu versio edeltäjästään, jossa kehitetään entisestään tietoturvallisuutta ja satelliittiviestintää. Tavoitteena 7G-verkossa on pystyä tarjoamaan langattomia HD- tason videolähetyksiä ilman minkäänlaista viivettä. (Karki & Garia 2016, s. 16).

LPWAN (Low Power Wide Area Network) - verkot edustavat uutta tiedonsiirron mahdollisuutta, jotka täydentävät perinteisiä matkapuhelinverkkoja. LPWAN- teknologiat tarjoavat uusia ominaisuuksia, kuten laaja peittoalue, hyvä rakenteen läpäisykyky sekä matala virrankulutus. Ennen kaikkea LPWAN- verkot on rakennettu IoT:n kasvaviin tarpeisiin. Etuna perinteisiin langattomiin teknologioihin nähden LPWAN-verkkoja hyödyntämällä ei tarvitse rakentaa rakennuksen sisälle kallista tiedonsiirto infrastruktuuria, vaan laitteita voidaan liittää helposti suoraan LPWAN-verkkoon. Anturin tai laitteen liittämisestä verkkoon suoritetaan maksu palvelua tarjoavalle operaattorille. Tunnetuimmat LPWAN-verkoista ovat LoRa ja Sigfox verkot, joista kummatkin ovat käytössä myös Suomessa. (Raza et al 2017, s. 855-856; Collin & Saarelainen 2016, s. 178-179)

2.6 Alustat ja rajapinnat

IoT-arkkitehtuurin yksi tärkeimmistä ja kriittisimmistä osista on alusta (platform), jossa virtuaalinen ja aineellinen maailma yhdistyvät. Alusta mahdollistaa eri datalähteistä tulevan informaation kokoamisen yhteen. Sen tehtävänä on yhdistää toiminnallisten järjestelmien datavirrat ja tietojärjestelmät toisiinsa sekä kytkeä sovelluskehityksen, tietovarastot ja analytiikan toisiinsa kattaen myös suurimman osan myös tietoturvan toteutumisesta. (Zdravković et al 2016, s. 216; Collin & Saarelainen 2016, s.228)

Merkittävää on myös se, että alusta voi itse sisältää suuren osan teknologisesta infrastruktuurista ja sen eri toiminnallisuuksista. Näin se helpottaa IoT-ympäristön rakentumista. Alustan avulla voidaan esimerkiksi avata näkymä sensoriverkkoon ja sitä kautta auttaa antureiden tai toimilaitteiden löytämisessä. Ei ole nimittäin itsestäänselvyys, että verkkoon liitettävät anturit tai toimilaitteet alkavat lähettää ja vastaanottaa dataa heti niiden päälle kytkeytyessä. Alustat osaavat huolehtia laitteiden löydettävyydestä, voivat ohjata tietoliikennettä halutulla tavalla, tunnistavat päätepisteiden viestintäprotokollat, sekä varmistavat, että järjestelmä on riittävän tietoturvallinen vaatimalla esimerkiksi tunnistautumista ja salaamalla siten liikenteen. (Collin & Saarelainen 2016, s. 228)

Alustojen ominaisuuksissa on eroja. Yksinkertaisimmillaan alusta mahdollistaa vain antureiden liitettävyyden ja hallinnan. Laajempi alusta voi sisältää jonkinlaisen kehitysalustan, tietoturvan ja integroinnin perusominaisuudet sekä tukea vähäisiä määriä protokollia. Kehittynyt alusta sisältää monipuoliset, lukemattomien erilaisten sensorien, datavirtojen, verkkojen, analytiikan ja sovellusten hallinnan ja integroinnin ominaisuudet, samoin kuin tehokkaan kehitysalustan sekä visualisoinnin, analytiikan ja käyttöliittymän työkalut niin loppukäyttäjille kuin ylläpitäjille. Erittäin kehittynyt alusta skaalautuu käytännössä loputtomasti, vaikka antureiden määrä nousee miljooniin kappaleisiin. (Collin & Saarelainen 2016, 229.)

Ohjelmointirajapinta (Application programming interface, API) määrittelee, miten ohjelmisto tarjoaa palveluita tai tietoja sovelluksille tai muille tietojärjestelmille. Rajapinta voi olla pelkkä datarajapinta, jonka kautta saadaan luettua palvelun sisältämä data toisiin järjestelmiin. Rajapinta voi olla myös toiminnallinen rajapinta, joka tarjoaa myös laskenta-algoritmeja tai mahdollisuuden muuttaa järjestelmän tietoja rajapinnan kautta.

Ohjelmointirajapinta voi olla avoin tai suljettu. Avoimessa ohjelmointirajapinnassa sen kaikki ominaisuudet ovat julkisia ja niitä voi käyttää ilman rajoittavia ehtoja. Rajapintakuvaus ja sen dokumentaatio tulee olla avoimesti saatavilla jotta rajapintaa voi vapaasti käyttää. (Avoin rajapinta 2014)

IoT-teknologian kehityksen vuoksi olisi tarpeellista, että järjestelmien väliset integraatiot olisivat helpompia toteuttaa. Esimerkiksi talotekniikassa järjestelmät ovat olleet aikaisemmin suljettuja järjestelmiä, jonka vuoksi järjestelmäintegraatiot ovat olleet räätälöityjä ratkaisuja ja siten kalliita ja työläitä toteuttaa. Avoimuutta lisäämällä pystytään lisäämään rajapinnan yhteensopivuutta sekä sen skaalautuvuutta. Sen avulla saavutetaan luotettavuutta sekä kustannusten pienenemisiä. Yksi ratkaisu tähän olisi standardisoinnin lisääminen, joka mahdollistaisi luotettavan ja yhteensopivan rajapinnan. Standardisoinnin avulla pystyttäisiin vaikuttamaan myös tietoturvaan. Talotekniikassa ohjelmointirajapintojen toteuttamiseksi REST-arkkitehtuuri olisi hyvä vaihtoehto, koska sen avulla saataisiin parannettua yhteensopivuutta sekä helpotettua integrointien toteuttamista. (Ihasalo et al 2017, s 4)

2.7 Pilvilaskenta ja data analytiikka

Pilvilaskenta tai pilvipalvelu (cloud computing) on joukko Internetin kautta tarjolla olevia resursseja ja palveluita. Sen tavoitteena on jakaa käyttäjien kesken käyttöjärjestelmät, eri sovellukset, tallennettu data sekä prosessointikapasiteetti. Pilvilaskenta käyttää tehokkaasti hajautettuja resursseja ja siten ratkaista laaja-alaisia laskennallisia ongelmia. Resursseja on mahdollista jakaa suuren käyttäjämäärän kesken, jotka pystyvät käyttämään sovelluksia ja tietoa mistä tahansa ja milloin tahansa. Pilvilaskenta on avainteknologia IoT:ssa ja resurssien jakamiseksi Internet-verkon yli. (Sadiku et al 2014, s. 34-35)

Pilvilaskenta on laajenemassa IoT:n kehityksen ja yleistyminen vuoksi kohti sumulaskentaa (fog computing). Sumulaskennassa palvelut tuodaan verkon reunalle, lähemmäksi loppukäyttäjiä ja laitteita. Samoin kuin pilvilaskenta sumulaskenta tarjoaa datan tallennus-, laskenta- ja sovelluspalveluja loppukäyttäjälle. Sumulaskennassa toimintoja hajautetaan ja paikallinen verkko voi ottaa hoitaakseen osan pilvilaskennan tehtävistä. Näin esimerkiksi sovellukset toimivat lähempänä toiminta ympäristöä, joka nopeuttaa siten toimintoja ja antaa näin lisäarvoa. (Stojmenovic & Wen 2014, s.1-2)

Data analytiikka on raakadatan jalostamista siten, että siitä saadaan kiinnostavaa ja hyödyllistä informaatiota. Nykyisin on hyvin yleistä, että data tallennetaan erilaisiin pilvipalveluihin, jossa data analysoidaan eri tavoin. Informaatiota voidaan käsitellä visuaaliseen tai muuhun tarpeelliseen muotoon. Visualisoinnin avuksi on useita tekniikoita, joiden avulla informaatiosta voidaan tehdä kiinnostavampaa. Datan analysoinnin yksi tärkeimmistä tekijöistä on muuttaa data tiedoksi, jolloin se antaa päätöksentekijöille mahdollisuuden käyttää tietoa esimerkiksi päätöksenteon tukena. (Gubbi et al 2013, s.1648). Big data analytiikka onkin kasvava trendi. Datan analysoinnilla voidaan luoda uutta tietoa, jota hyödyntämällä voi syntyä taas uutta ymmärrystä. Tätä ymmärrystä voidaan hyödyntää esimerkiksi liiketoiminnan kehittämiseen. (Salo 2014, s.68).

Tallennettua ja analysoitua dataa on mahdollista käyttää älykkäästi esimerkiksi älykkäiden laitteiden hallintaan ja käyttöön. On erittäin tärkeää kehittää tekoälyä koskevia algoritmeja, jotka voivat olla keskitetty tai hajautettu tarpeen mukaan. Hermoverkkojen muodostumiset, koneoppiminen ja muiden keinotekoisten älykkäiden tekniikoiden kehitys on tulevaisuudessa tarpeen automaattisen päätöksenteon tehostamisen saavuttamiseksi. Data analytiikasta saatavan tehokkuuden varmistamiseksi, järjestelmien tulee olla yhteensopivia ja niiden on kyettävä keskustelemaan keskenään. (Gubbi et al 2013, s.1648).

2.8 Tietoturvallisuus

IoT:n tunnistetuimmat uhkat ovat tieto- ja kyberturvallisuuteen liittyvät uhkatekijät. Nämä uhkatekijät tulee huomioida kaikkien niiden toimijoiden toimesta, jotka ovat osana IoT-järjestelmän kokonaisuutta. Järjestelmään tai laitteeseen voi kohdistua merkittävä riski, ellei kiinnitetä riittävästi huomiota laitteiden ja antureiden tietoturvaan. (Lindqvist & Neumann 2017, s. 26-30). Tietoturvallisuuden haasteet voivat pahimmassa tapauksessa muodostaa jopa esteen IoT:n hyödyntämiselle (Kuusijärvi et al 2016, s. 260). Sen vuoksi on tarpeellista arvioida, mitkä laitteet kannattaa riskiperusteisesti liittää Internetiin. Tietoturva ei rajoitu pelkästään laitteiden käyttäjiin tai omistajiin vaan tietoturvallisuuteen liittyvät asiat on huomioitava myös esimerkiksi laitevalmistajien, laitteistojen myyjien sekä palveluntarjoajien toimesta. Puutteet tietoturvallisuudessa voivat edesauttaa järjestelmiin kohdistuvia hyökkäyksiä, jotka voivat vaikuttaa aina jopa ih-

misten turvallisuuteen. Kyberhyökkäykset voivat pahimmassa tapauksessa aiheuttaa omaisuuden tuhoutumista tai ihmishenkien menetyksiä suoraan tai välillisesti. (Lindqvist & Neumann 2017, s. 26-30)

Tietoturvan näkökulmasta lähes jokaista laitetta tai anturia voidaan pitää tietynlaisena tietoturvariskinä. Internetiin liitettyjen antureiden ja laitteiden sekä langattomien verkkojen määrä on jatkuvassa kasvussa, jonka myötä tietoturvallisuuteen liittyvät riskit lisääntyvät. Tästä esimerkkinä viime vuosina sattuneet tapaukset, joissa IoT-teknologiaa hyödyntävät kiinteistöautomaatio-ratkaisut ovat joutuneet kyberhyökkäyksien kohteeksi. Kyberhyökkäykset ovat kohdistuneet kiinteistöautomaation eri osiin. Sen vuoksi onkin tärkeää, että tieto- ja kyberturvallisuudesta huolehditaan IoT-arkkitehtuurin kaikissa kerroksissa (layers), jotta varmistutaan riittävästä tieto- ja kyberturvallisuudesta. (Rathinavel et al 2017, s. 1-2). Kyberhyökkäyksissä hyödynnetään laitteiden tai järjestelmien haavoittuvuuksia, joita IoT-laitteissa voidaan nykyisin pitää ennemmin ominaisuutena kuin puutteena. Kyberhyökkäyksien avulla on mahdollista tietyissä tapauksissa aiheuttaa jopa fyysistä vahinkoa, jopa tulipaloja. IoT-laitteita on vuosien saatossa hyödynnetty myös palvelunestohyökkäyksissä, joissa parhaimmillaan on voinut olla osallisena jopa kymmeniä miljoonia laitteita. Palveluestohyökkäyksien tutkinta on osoittanut, että laitteiden tietoturva on saatettu järjestää hyvinkin puutteellisesti. Myöskään laitteiden omistajat eivät ole olleet tietoisia, että heidän IoT-laitteita on käytetty palvelunestohyökkäyksissä. (Lindqvist & Neumann 2017, s. 26-27)

IoT-teknologiassa laitteiden tai koko järjestelmien etähallinta on tätä päivää. Etähallinta on katsottu yhdeksi isoksi tietoturvallisuuteen liittyväksi uhkaksi, koska se mahdollistaa erilaiset hyökkäykset järjestelmiä kohtaan (Miorandi et al 2012, s. 1507). Tietoturvallisuuteen ei liity pelkkä ICT-teknologian, vaan siihen esimerkiksi järjestelmien manageroinnin liittyviä ongelmia. IoT-laitteiden manageroinnin ja hallinta ei ole välttämättä yhtä hyvin tunnistettu kuin normaali tietokoneisiin liittyvä tietohallinto. (Lindqvist & Neumann 2017, s. 28).

Tieto- ja kyberturvallisuuteen liittyvät oleellisena osana ihmiset sekä heidän asenteensa ja suhtautumisensa niihin. Ihminen voi toimia turvallisuuden mahdollistaja, mutta tahattomalla tai tahallisella käytöksellä se voi muodostaa merkittävän riskin. Tämän vuoksi

ihmisen toiminta tuleekin aina huomioida tieto- ja kyberturvallisuuden hallinnassa. On kuitenkin huomioitava, että ihmisien hallinta ja käsittely eivät ole helppoa, koska ihmisillä on erilaisia asenteita, odotuksia sekä heidän tietoteknisessä osaamisessa on eroja. Ihmiset on saatava tietoiseksi ja ymmärtämään, kuinka tärkeää riittävän tieto- ja kyberturvallisuuden tason saavuttaminen on, ja sitouttaa heidät näihin turvallisuusvaatimuksiin. Tämä toiminta varmistetaan esimerkiksi seuraavilla toimenpiteillä:

- Kehittämällä tehokas turvallisuusdokumentaatio kuten turvallisuuskäytännöt ja –säännöt
- Turvallisuuskäytäntöjen ja -sääntöjen tehokkuuden tarkastelu mukaan lukien henkilöstö, dokumentointi ja teknisen valvonnan menettelyt
- Tieto- ja kyberturvallisuuden käytäntöjen toiminnan käyttöönotto, kuten koulutus ja perehdytys. (Riahi et al 2014, s.3)

IoT-teknologiaan liittyvät riskit tulee tulevaisuudessa huomioida tehokkaammin, jotta luotettavuus teknologiaan lisääntyy. Näihin liittyy tiiviisti järjestelmien luotettavuus, kestävyys ja joustavuus, järjestelmien toiminnallinen yhteentoimivuus, laitteiden helppo asennettavuus ja käyttö, nopea automatisoitu vakavien puutteiden korjaaminen, ohjelmistojen päivittäminen sekä yksityisyyden suoja. Ennen kaikkea nämä asiat tulee ottaa huomioon, jotta varmistutaan tai varmistetaan riittävä tietoturvallisuus. Viime aikoina suurin osa tietoturvallisuuteen liittyvistä riskeistä on johtunut kilpailun aiheuttamasta kiireestä tuotemarkkinoilla. Laitteiden tietoturvallisuuspuutteet eivät ole olleet laitevalmistajien huolenaiheena. (Lindqvist & Neumann 2017, s. 27). Liikenne ja viestintävaliokunta on EU:n tietosuoja-asetuksen lausunnossaan todennut saman. IoT-laitteissa keskeinen ongelma on tällä hetkellä se, että laitevalmistajat ja niitä hyödyntävä käyttäjätahot eivät ole riittävästi tietoisia tietoturvaan liittyvistä vaatimuksista (Liikenne- ja viestintävaliokunta 2017, s.6). Toinen riski on se, että monille käyttäjille ei ole enää selvää, mitkä laitteet kommunikoivat ja millä tavoin. Tämän vuoksi viestinnän suojaaminen saattaa näiden laitteiden välillä saattaa jäädä vaillinaiseksi. Tulevaisuudessa IoT-laitteiden viestinnän salausmenetelmiä tulisi kehittää sekä saada markkinoille uudenlaisia tuotteita. On valitettavaa, että kehitystä salaus- ja suojausmenetelmissä tapahtuu usein vasta silloin, kun käytössä olevissa laitteissa havaitaan heikkouksia. (Liikenne- ja viestintäministeriö 2018, s.58)

Laitteiden valmistajien tulee panostaa tietoisuuden lisäämiseen. Laitteistojen standardien kehittämiseen tulee kiinnittää erityistä huomioita, jotta verkkojen turvallisuutta saadaan parannettua. Tietoturva tulee muistaa jo laitteita valmistaessa. (Liikenne- ja viestintävaliokunta 2017, s.1-7). Tietoturvallisuuden parantamiseksi tarvitaan yhtenäisiä standardeja, jotka ratkaisevat osaltaan myös eri laitevalmistajien laitteiden yhteensopivuusongelmia. Yhteysprotokollien tietoturvaa tulee parantaa, jotta ne eivät aiheuta niin suurta tietoturvariskiä kuin nykyään. (Lindqvist & Neumann 2017, s. 29)

Tietoturvallisuus on huomioitava myös turvalaitteistojen, kuten paloilmoitinlaitteistojen ilmoituksensiirtojärjestelmissä. Esimerkiksi ilmoituksensiirtojärjestelmässä on oltava riittävä suojaus siirtoverkosta tulevilta palvelunestohyökkäyksiltä. Järjestelmä- ja laitetietoturvan suojaustasoa koskevien vaatimusten lisäksi tulisi korostaa toiminnallista tietoturvaa. Ilmoituksensiirtopalvelun tarjoajalla ja muilla osapuolilla, jotka ylläpitävät ja käyttävät yhtä tai useampaa ilmoituksensiirtojärjestelmää, olisi oltava täysin dokumentoitu tietoturvapolitiikka. (SFS-CLC/TS 50136-7 2017, s.6; SFS-EN 50136-1 2012, s. 22)

2.9 Tietosuoja

Hyödynnettäessä IoT-teknologiaa on tietosuojaan liittyvät asiat aina muistettava ja huomioitava. Tietosuoja käsitteeseen liittyy tiiviisti yksityisyyden suoja. IoT-teknologian laajenemisen myötä ihmisiin liittyvää dataa kerätään tulevaisuudessa entistä tehokkaammin erilaisien antureiden ja laitteiden avulla. Jopa siten, etteivät ihmiset edes välttämättä tiedä tai tiedosta sitä (Mäkinen 2015, s.262). IoT-teknologia mahdollistaa myös entistä arkaluontoisemman datan keräämisen ihmisistä ja heidän toimistaan, koska IoT:n avulla on mahdollista luoda tehokas pääsy fyysiseen ympäristöön. Juuri sinne, missä ihmiset elävät ja asuvat (Weinberg et al 2015, s. 621). Tietosuojaan liittyvien asioiden käsittely eri IoT-teknologioitten osa-alueilla ei ole kuitenkaan mikään uusi asia. Esimerkiksi Chan & Perrig (2003) julkaisemassa artikkelissa lähes 15 vuotta sitten, on kuvattu langattomien sensoriverkkojen tietoturvaan ja tietosuojaan liittyviä asioita, jotka ovat edelleenkin ajankohtaisia. Langattomien sensoriverkkojen tiedonsiirrossa on mahdollista päästä esimerkiksi talon ulkopuolelta käsiksi verkossa liikkuvaan tietoon. Näiden tietojen avulla on mahdollista saada selville ihmisten henkilökohtaisia tietoja tai

tietoa heidän arkirutiineistaan. Tätä ei kuitenkaan pidetty sensoriverkkojen suurimpana uhkana, vaan suurempi uhka liittyi laitteiden etäyhteyksiin ja -hallintaan, joiden avulla päästään hallinnoimaan sensoriverkoihin kytkettyjä laitteita sekä päästään käsiksi kerättyyn dataan. Väärinkäytökset etäyhteyttä hyödyntämällä aiheuttavat väärinkäyttäjälle pienemmän riskin eikä tekijän tarvitse olla edes fyysisesti läsnä. Etäkäyttö mahdollistaa myös monien järjestelmien samanaikaisen tarkkailun. (Chan & Perrig 2003, s.103-104). Tietosuojan pettäessä on mahdollista, että henkilöistä saatua tietoa voidaan hyödyntää rikollisiin tarkoituksiin, joka voi näin muodostaa merkittävän turvallisuusuhkan (Lindqvist & Neumann 2017, s. 26).

IoT:n yksi keskeisimpiä asioita on data ja sen kerääminen. Dataan liittyy useita eri prosesseja, joissa jokaisessa tietosuojaan liittyvät asiat tulee huomioida. Näitä ovat esimerkiksi datan kerääminen, tiedonsiirto, analysointi ja sen hyödyntäminen. Voidaankin sanoa, että ilman dataa IoT:tä ei ole olemassa. (Weinberg et al. 2015, s. 620). Datan keräämiselle tulisi aina olla perusteet, eikä dataa tulisi kerätä vain tulevia tarpeita varten. Näin ollen keräystarve tulee aina etukäteen miettiä, miksi dataa kerätään ja mihin tarkoitukseen. Henkilötietoja ei tule kerätä tai analysoida siten, että yksilön voi tunnistaa kerätystä aineistosta (Mäkinen 2015, s.273). Viime vuosina huolenaiheeksi on noussut kerätyn datan omistajuussuhteet, eli kuka omistaa datan. Omistajuussuhteet ovat äärimmäisen hankalia tilanteissa, jossa kerättyä dataa jalostetaan eri vaiheissa kolmansien osapuolien toimesta. Omistajuussuhteet voivat aiheuttaa ongelmia etenkin, kun dataan liittyy liiketoiminnallisia hyötyjä tai data sisältää liian henkilökohtaista tietoa. (Weinberg et al 2015, s. 620).

Euroopan parlamentin ja neuvoston tietosuoja-asetusta 2016/679 sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn. Tähän liittyy myös IoT-teknologian avulla kerätty data. Osa IoT-teknologiassa hyödynnettävien antureiden tai laitteiden tiedonsiirrosta voi sisältää henkilötietoja, jotka voivat liittyä yleisen tietosuoja-asetuksen soveltamisen piiriin. Henkilötietojen keräämisessä tulee siis huomioida uusi EU:n tietosuoja-asetuksen vaatimukset. Suomessa liikenne- ja viestintävaliokunta on esittänyt lausunnossaan uudesta EU:n tietosuoja-asetuksesta, että sääntelyssä on tarpeen huomioida myös IoT-teknologian tarpeet. Sääntely ei saa olla liian rajoittavaa, jotta säilytetään Euroopan kilpailukyky globaaleilla markkinoilla, eikä näin rajoiteta alan innovaatioita ja

palvelukehitystä. Sääntelyn avulla on myös mahdollista ehkäistä erityisesti tietoturvaan ja yksityisyyden suojaan liittyviä ongelmia. (Liikenne- ja viestintävaliokunta 2017, s.1-7)

2.10 Digitalisaation haasteet ja vaikutukset

Digitalisaation vaikutukset näkyvät koko yhteiskunnassa sekä erityisesti yritysten ja organisaatioiden toimintaympäristöissä. Vaikutukset kohdistuvat kaikkeen liiketoimintaan ja sen merkitys tulee tulevaisuudessa kasvamaan entisestään. On huomioitava, että digitalisaatiossa nykyiset toimintamallit eivät vain muutu digitaaliseksi, vaan se mahdollistaa myös kokonaan uudenlaisen lähestymistavan tarkastella yritysten liiketoimintakenttää. Organisaatioiden ja yritysten tuleekin ottaa digitalisaatioon enemmin ennakoiva lähestymistapa, kuin jäädä odottamaan mitä tulee tapahtumaan. Digitalisaatio onkin avainasemassa organisaation sisäisen tehokkuuden toteutuksessa sekä uusien palveluiden kehittämisessä asiakkaille. (Parviainen et al 2017, s.74)

Digitalisaatiolla on voimakas vaikutus työskentelytapoihin, joka vauhdittaa siten myös organisaatioissa tapahtuvaa muutosta. Muutoksen hallittavuuteen vaikuttaa pitkälti se, miten ihmisten ja organisaatioon liittyviä näkökohtia johdetaan. Tämä edellyttää organisaatiossa uutta osaamista, uudenlaista johtamista sekä ketteryyttä, jotta organisaatiossa päästään kohti digitaalisempaa ajattelutapaa. Digitaalisuuden lisäämisen yhteydessä on tärkeää huomioida myös työntekijöiden osaamisen taso, jolloin varmistutaan, että kaikki osaavat käyttää uutta teknologiaa. Erityisesti on keskityttävä sellaisiin työntekijöihin, jotka eivät ole niin teknologiaorientoituneita. Heille on tarjottava riittävää käytännön koulutusta, jossa tuodaan esiin, miten teknologia uudistus vaikuttaa juuri heidän työskentelytapoihinsa. Näin varmistutaan siitä, että digitalisaatiolla saadaan tahdottu vaikutus esimerkiksi liiketoiminnan edistämiseen. (Kohnke 2016, s.85, 89)

Teknologian kehityksessä on siis tarpeen huomioida teknologian loppukäyttäjät ja heidän tarpeensa. Loppukäyttäjät voivat yritysmaailman lisäksi olla yksityisiä ihmisiä. Yleisesti teknologian lisääntyminen saattaa aiheuttaa ihmisissä pelkoa, muutosvastarintaa sekä muita psykologisia esteitä, jos he katsovat olevansa osaamattomia ja tottumattomia teknologian käyttöön ja sen hyödyntämiseen. Näin ollen kohderyhmän ajattelumallit, kokemattomuus ja motivaatio ovat tärkeitä huomioon otettavia asioita. Esimer-

kiksi ikääntyneet ja lähitulevaisuudessa tähän ikäryhmään laskettavat henkilöt eivät ole yleensä tottuneita teknologian ostajia. Tämän vuoksi yleisen ajattelumallin muutos teknologiamyönteisempään suuntaan on suuri tekijä teknologioitten käyttöönotossa. On huomioitava, että teknologian lisääntymisen yhteydessä on tarpeen lisätä motivaatiota, jalkauttaa toimintamalleja sekä varmistaa palveluiden ja laitteiden helppo käytettävyys. (Ympäristöministeriö 2017, s. 140)

Uuden teknologian hankintaan ja sen käyttöön voivat vaikuttaa useat eri asiat. Esimerkiksi kodin automaatiojärjestelmien haasteisiin ja mahdollisuuksiin liittyvässä tutkimuksessa esille nousi seuraavia tekijöitä, jotka rajoittavat uuteen teknologiaan investoimista: teknologian hankintahinta ja sen aiheuttamat ylläpitokustannukset, teknologian käytettävyyden helppous, järjestelmän yhteensopivuus ja joustavuus sekä riittävän turvallisuuden ja yksityisyyden takaaminen. Kustannukset ovat yksi merkittävimmistä tekijöistä, jotka vaikuttavat uuden teknologian hankintaan. Ihmiset eivät ole aina valmiita maksamaan uudesta teknologiasta. Tähän liittyy pitkälti se, kuinka paljon uusille ominaisuuksille ja mahdollisuuksille annetaan arvoa. Järjestelmien tulee lisäksi olla hyvin yhteensopivia sekä tarvittaessa muokattavissa, jotta uusien laitteiden lisääminen järjestelmään on helppoa. Loppukäyttäjän näkökulmasta järjestelmissä yksi oleellinen asia on niiden helppokäyttöisyys, joka korostuu ennen kaikkea käyttöliittymässä. Esimerkiksi kodin automaatiojärjestelmässä vaikeasti käytettävä tai ymmärrettävä käyttöliittymä voi aiheuttaa jopa esteen laitteiston tai järjestelmän käytölle, jos käyttäjä tuntee epävarmuutta laitteiston käyttöön. Turvallisuuteen ja yksityisyyteen liittyen ihmisiä huolestuttivat järjestelmän etäkäytön aiheuttamat riskit varsinkin lukitusten ja kameravalvonnan osalta. (Brush et al 2011, s. 2119-2122)

Liiketoiminnan ja toimintaympäristön erityispiirteet määrittävät, minkälaisin painopistein ja kuinka nopeasti digitalisaatio vaikuttaa yrityksen liiketoimintaan. Esimerkiksi huolto- ja kunnossapitopalveluissa etäteknologian kehittyminen avaa uusia mahdollisuuksia. Palveluntuotantoa on mahdollista johtaa ja optimoida reaaliaikaisesti sekä tehostaa työnohjausta mobiiliteknologiaa hyödyntämällä. Ongelmana kuitenkin on se, että huolto ja kunnossapitopalvelut ovat keskimäärin heikommin standardoituina palveluina huomattavasti hitaampia automatisoida, koska monet kohteet vaativat edelleen fyysistä läsnäoloa (Palta 2016, s 22-28).

Rakennusteollisuudessa digitalisaation kehityksessä yhtenä merkittävänä haasteena on ollut yllättävän hidas reagointi uuden teknologian tarjoamiin mahdollisuuksiin. Yhtenä syynä tähän on katsottu vaikuttavan sen, että rakennusteollisuuden eri toimijat toimivat liikaa omissa siiloissa, mikä on muodostanut esteitä sekä rajoitteita uuden teknologian yleistymisessä ja talotekniikan järjestelmien yhteen integroitumisessa. (Virtanen 2015, s. 603-604). Tämän lisäksi digitaalisuutta ei myöskään nähdä kilpailuetuna. Tampereen teknillisen yliopiston tekemän tutkimuksen mukaan kiinteistö- ja rakennusalalla digitaalisuuden mahdollisuuksia ei nähdä niin merkittävänä kilpailuetuna kuin muissa toimialoissa. Haasteiksi digitaalisuuden kehittämisessä olivat yleensä organisaation riittämätön teknologian osaaminen sekä ketteryyden puute teknologian käyttöönotossa. Yhtenä syynä digitalisaation vähäisen hyödyntämien syyksi katsottiin tuotteen, eli rakennuksen pitkä elinkaari, jonka vuoksi teknologiatrendeihin ei haluta liian harkitsemattomasti panostaa. Valittujen teknologia ratkaisujen tulisi kestää vuosia sekä olla helposti päivitettävissä (Puhto et al 2016, s. 32). IoT-teknologian yhdeksi tulevaisuuden ongelmaksi voi muodostua nykyisin käytettävien standardien moninaisuus. Esimerkiksi tiedonsiirtoon liittyviä standardeja on useita. Väärin valittu standardi voi aiheuttaa merkittävän riskin erityisesti laitevalmistajille, jos valittu standardi ei tulekaan yleistymään (Links 2017, s.59).

3 PALOTURVALLISUUTTA PARANTAVAT LAITTEISTOT

Tässä luvussa tuodaan esiin rakennuksien yleisiä paloturvallisuusvaatimuksia Suomessa sekä paloturvallisuutta parantavien laitteistojen vaatimustasoja niin lainsäädännön kuin standardien tasolla. Esille tuodaan myös mitä paloturvallisuutta parantavien laitteistojen järjestelmäintegraatiossa tulee ottaa huomioon, millaisia nykyaikaisia älykkäitä paloturvallisuutta parantavia laitteistoja ja järjestelmiä markkinoilla on sekä millä tavoin IoT- ja älyteknologiasta saadaan erilaisia hyötyjä.
Luvussa esitellään paloturvallisuutta parantavien laitteiden valmistajien tuotteiden nimiä ja niiden ominaisuuksia. On huomioitava, että markkinoilla voi olla myös muiden valmistajien tuotteita tai järjestelmiä, joilla voi olla samanlaisia ominaisuuksia tai toimintoja, mitä tässä luvussa on tuotu esille.

3.1 Rakennuksien paloturvallisuusvaatimukset Suomessa

Suomessa uudis- ja korjausrakentamisen yhteydessä rakennuksien tai niiden tilojen suojaaminen paloturvallisuutta parantavilla laitteistoilla perustuu pitkälti maankäyttö- ja rakennuslainsäädäntöön, kun taas olemassa olevia rakennuksia takautuvasti koskevat ja kunnossapitoon liittyvät vaatimukset perustuvat yleensä pelastuslainsäädäntöön.

3.1.1 Rakentamiseen liittyvät paloturvallisuusvaatimukset

Suomessa uudis- ja korjausrakentamisessa rakennushankkeeseen ryhtyvän on huolehdittava, että rakennus suunnitellaan ja rakennetaan sen käyttötarkoituksen edellyttämällä tavalla paloturvalliseksi. Palon syttymisen vaaran rajoittamisen lisäksi on huomioitava, että kantavien rakenteiden on oltava sellaiset, että ne palon sattuessa kestävät vähimmäisajan ottaen huomioon rakennusten sortuminen, poistumisen turvaaminen pelastustoiminta sekä palon hallintaan saaminen. Palon ja savun kehittymistä sekä niiden leviämistä rakennuksessa on pystyttävä rajoittamaan. Lisäksi rakennuksessa on käytettävä paloturvallisuuden kannalta soveltuvia teknisiä laitteistoja. (Maankäyttö- ja rakennuslaki 132/1999, 117 b §)

Uudis- ja korjausrakentamisen tarkemmat paloturvallisuusvaatimukset on esitetty ympäristöministeriön asetus rakennusten paloturvallisuudesta (848/2017). Rakennuksen paloturvallisuudelle asetetut olennaiset tekniset vaatimukset täyttyvät, jos rakennus tullaan suunnittelemaan ja rakentamaan noudattaen asetuksessa esitettyjä luokkia ja lukuarvoja. Paloturvallisuusvaatimusten voidaan katsoa täyttyvän myös siinä tapauksessa, jos rakennus suunnitellaan ja rakennetaan perustetuen oletettuun palonkehitykseen. (Ympäristöministeriön asetus rakennusten paloturvallisuudesta 848/2017, 3§). Käytettäessä asetuksessa esitettyjä luokkia ja lukuarvoja tulee niiden mukaisesti rakennus suojata tapauksesta riippuen erilaisilla paloturvallisuutta parantavilla laitteilla.

3.1.2 Rakennuksien kunnossapidon paloturvallisuusvaatimukset

Kiinteistön omistaja, haltija ja toiminnanharjoittajan on osaltaan huolehdittava, että rakennuksiin lainsäädännön tai viranomaisen vaatimuksin vaaditut varusteet ja laitteet pidetään toimintakunnossa ja huollettava ja tarkastettava asianmukaisesti:

- *sammutus-, pelastus- ja torjuntakalusto;*
- *sammutus- ja pelastustyötä helpottavat laitteet;*
- *palonilmaisu-, hälytys- ja muut onnettomuuden vaaraa ilmaisevat laitteet;*
- *poistumisreittien opasteet ja valaistus*. (pelastuslaki 379/2011, 12 §)

Kunnossapidon huolehtimisen lisäksi rakennuksen omistajan ja haltijan sekä toiminnanharjoittajan on osaltaan varauduttava henkilöiden, omaisuuden ja ympäristön suojaamiseen vaaratilanteissa. Tarpeen mukaan on myös ryhdyttävä toimenpiteisiin poistumisen turvaamiseksi tulipaloissa ja muissa vaaratilanteissa sekä toimenpiteisiin pelastustoiminnan helpottamiseksi. (pelastuslaki 379/2011, 14 §)

3.2 Paloturvallisuutta parantavien laitteistojen vaatimustasot

Paloturvallisuutta parantavien laitteiden tulee olla käyttötarkoitukseen sopivia ja toimintavarmoja (laki pelastustoimen laitteista 10/2007, 5 §). Rakennukseen kiinteästi asennettavat palonilmaisulaitteistot ja vastaavat järjestelmät, jotka lainsäädännön taikka viranomaisen päätöksen mukaan on asennettava taikka jotka liitetään tiedonsiirtoyhteydellä

hätäkeskukseen, sekä automaattiset sammutuslaitteistot on suunniteltava ja asennettava niin, että ne toimivat asianmukaisesti ja luotettavasti, eivätkä aiheuta vaaraa ihmisille, omaisuudelle tai ympäristölle. Laitteiston suunnittelussa ja asennuksessa tulee ottaa huomioon laitteiston ja asennuskohteen käyttötarkoitus sekä niiden yhteensopivuus laitteiston toimintaan mahdollisesti vaikuttavien muiden järjestelmien kanssa. (Laki pelastustoimen laitteista 10/2007, 7 §)

Standardeissa on yleensä esitetty paloturvallisuutta parantavien laitteistojen yksityiskohtaiset tekniset vaatimukset. Standardien käyttäminen on vapaaehtoista, toisin kuin lakien ja asetusten soveltaminen. Viranomaisilla ja lainsäätäjillä on mahdollista kuitenkin määräyksillään ja organisaatiot toimivaltansa rajoissa tehdä standardien käytöstä pakollista. Suomessa standardeja on käytetty tietyllä tavalla lainsäädännön apuvälineenä. Monien maiden viranomaiset ja lainsäätäjät myös Suomi mukaan lukien, käyttävät standardeja, jotta säädöksiin ei tarvitsisi sisällyttää yksityiskohtaisia vaatimusten kuvauksia. (Suomen Standardisoimisliitto SFS ry 2018, s. 9-12). Suomessa esimerkiksi lainsäätäjä on tehnyt paloturvallisuutta parantavissa laitteissa standardien käytöstä tietyissä tapauksissa pakollista viittaamalla niihin eri lainsäädännöissä.

Paloturvallisuutta parantavat laitteet kuuluvat yleensä harmonisoidun tuotestandardin piiriin, jonka vuoksi tuotteet on varustettava CE-merkillä. Tämä perustuu EU:n rakennustuoteasetukseen. CE-merkinnän etuna on, että se parantaa rakennustuotteiden liikkuvuutta Euroopan talousalueella sekä mahdollistaa yhdenmukaisen tavan vertailla eri valmistajien tuotteiden soveltuvuutta suunnitteilla olevaan rakennuskohteeseen. (Tukes 2014). Harmonisoidut tuotestandardit mahdollistavat toimivien ja laadukkaiden tuotteiden suunnittelun, valmistamisen ja asentamisen. Tuotteet ovat turvallisia käyttää sekä niiden yhteentoimivuus esimerkiksi vanhojen ja uusien tuotteiden kanssa on yleensä huomioitu. (Euroopan komissio 2018)

Toimintakunnon takaamiseksi paloturvallisuutta parantaville laitteistoille on järjestettävä riittävä huolto- ja kunnossapitotoiminta koko laitteiston käyttöiän ajaksi. Näin varmistutaan siitä, että laitteistot pysyvät toimintakunnossa koko sen elinkaaren ajan. Yleensä jokaisella paloturvallisuutta parantavalle laitteistolle tulee laatia oma kunnossapito-ohjelma, jossa otetaan huomioon laitteiston valmistajan antamat ohjeistukset. Vi-

ranomaismääräyksenä oleville laitteistoille voi lisäksi olla velvoitteen tehdä kolmannen osapuolen tarkastuksia tietyin väliajoin. Paloturvallisuutta parantavien laitteiston kunnossapitoon liittyvät velvoitteet ja vaatimukset voivat perustua lainsäädäntöön tai standardien tuomiin velvoitteisiin (Pelastuslaki 379/2011, 12§; N:o SM-1999-967/Tu-33, 10§, 19§, 20§; Hakkarainen 2007, s.43)

3.2.1 Palovaroittimet

Palovaroitin on laite, joka sisältää yhdessä kotelossa kaikki komponentit, mahdollisesti poissulkien virtalähteen, jotka ovat tarpeellisia savun ilmaisemiseen ja akustisen hälytyksen antamiseen (SFS EN 14604 2006, s. 10). Palovaroittimet tulivat pakolliseksi alkaen 1.9.2000 (Pelastustoimilaki 561/1999, 92 §). Pelastustoimilaki 561/1999 31 § edellytti takautuvasti varustamaan asunnot, majoitus- sekä hoitolaitostilat vähintään paristokäyttöisillä palovaroittimilla tai suojaustasoltaan vähintään vastaavanlaisilla laitteilla. Voimassa oleva pelastuslaki edellyttää varustamaan asunnot ja majoitus- sekä hoitolaitostilat edelleen palovaroittimilla (pelastuslaki 379/2011, 17 §). Esimerkiksi asuinhuoneisto tulee varustaa riittävällä määrällä palovaroittimia huomioiden asunnon muoto ja syttymisvaaraa aiheuttavat toiminnot. Vähimmäisvaatimuksena on kuitenkin, että asunnon jokainen kerros sekä niihin yhteydessä olevat kellarikerrokset ja ullakkotilat tulee varustaa vähintään yhdellä palovaroittimella tason alkavaa 60 m² kohden. (Sisäministeriön asetus palovaroittimen sijoittamisesta ja kunnossapidosta 239/2009, 3§).

Ympäristöministeriön asetus rakennuksien paloturvallisuudesta (848/2017) 38 § edellyttää esimerkiksi asuinhuoneistojen suojaamisen sähköverkkoon kytketyillä palovaroittimilla. Lisäksi enintään 50 majoituspaikan majoitustilat sekä enintään 25 vuodepaikan hoitolaitokset tulee varustaa sähköverkkoon kytketyillä palovaroittimilla. Sähköverkkoon kytketyn palovaroittimen sähkövirran saanti tulee olla varmistettu esimerkiksi paristolla tai akulla. Edellä mainitut vaatimustaso on ollut voimassa niissä rakennuksissa, joissa rakennuslupa on haettu 1.2.2009 jälkeen (Ympäristöministeriön asetus rakennusten paloturvallisuudesta annetun ympäristöministeriön asetuksen muuttamisesta 2009).

Palovaroittimien osalta huoneiston haltija, eli asukas on velvollinen huolehtimaan siitä, että asunto varustetaan riittävällä määrällä palovaroittimia tai muita laitteilla, jotka mahdollisimman aikaisessa vaiheessa havaitsevat tulipalon ja varoittavat asunnossa olevia (pelastuslaki 379/2011, 17 §). Lisäksi palovaroittimen toimintakunto tulee varmistaa säännöllisellä testauksella, joka kuuluu yleensä asukkaan vastuulle (Sisäministeriön asetus palovaroittimen sijoittamisesta ja kunnossapidosta 239/2009, 5 §). Sähköverkkoon kytketyissä palovaroittimissa, joissa sähkövirran syöttö on varmistettu paristolla, on pariston vaihtaminen sekä palovaroittimen kunnossapito katsottu olevan kiinteistön omistajan vastuulla. Asukkaan vastuulla on palovaroittimen toimintakunnon säännöllinen testaaminen. (SPEK 2018). Sähköverkkoon kytkettyjen palovaroittimet katsotaan kiinteiksi sähköasennuksiksi, jonka vuoksi niiden asentaminen ja vaihtaminen on sallittu vain asianmukaiset oikeudet omaavalla sähköalan ammattilaisella (Sähköturvallisuuslaki 1135/2016, 4§, 73§)

Palovaroittimien on täytettävä palovaroitinstandardin SFS EN 14604 Palovaroittimet vaatimustaso sekä merkittävä CE-merkinnällä (Valtioneuvoston asetus palovaroittimien teknisistä ominaisuuksista 291/2009, 3§, 5§). Turvallisuus ja kemikaaliviraston sekä standardien kanta on, että palovaroittimessa voi olla standardien vaatimuksien mukaisuuden lisäksi ylimääräisiä toimintoja, mutta ne eivät saa häiritä palovaroittimen normaalia toimintaa (Meurman 2017). Palovaroittimia on esimerkiksi mahdollista kytkeä yhteen muiden palovaroittimien kanssa sekä varustaa ne hälytyksen hiljennystoiminnoilla (SFS EN 14604 2006, s. 18, 50).

3.2.2 Paloilmoitinlaitteistot

Paloilmoittimella tarkoitetaan laitteistoa, joka havaitsee ja automaattisesti ja välittömästi ilmoittaa alkavasta palosta sekä laitteiston toimintavalmiutta vaarantavista vioista. (Ympäristöministeriön asetus rakennusten paloturvallisuudesta 848/2017, 1 §). Palohälytys tulee kuulua paikallisesti sekä palotiedon tulee ohjautua yleensä suoraan hätäkeskukseen. Paloilmoitinlaitteistossa voi olla sekä palonilmaisu- että palohälytystoiminto, ja se koostuu yleensä toisiinsa kytketyistä komponenteista, kuten paloilmaisimista, paloilmoituspainikkeista ja hälyttimistä. Nämä komponentit on yhdistetty ilmoitinkeskuk-

seen yhdellä tai useammalla siirtotiellä. Kaikki laitteiston komponentit, myös ilmoituskeskus, ovat yleensä myös yhdistetty suoraan tai välillisesti tehonlähteeseen. (SFS-EN 54-13 2017, s.5-10)

Paloilmoitinlaitteiston päätoiminnon, eli palonilmaisun lisäksi järjestelmän signaaleita voidaan käyttää suoraan tai epäsuoraan muiden paloturvallisuutta parantavien laitteiden tai oheislaitteiden ohjauksiin. Tällaisia laitteita voivat olla esimerkiksi: sammutuslaitteistot, palo-ovet, savunhallintalaitteistot, ilmastoinnin eri toiminnot, hissien ohjaukset sekä lukitusten avaaminen. On huomioitava ettei paloturvallisuutta parantavia laitteistoja tai oheislaitteiden vikaantuminen saa häiritä paloilmoitinjärjestelmän oikeaa toimintaa, tai estää viestintää muille laitteistoille (SFS-CEN/TS 54-14 2004, s 27, 36). Lähtökohta on siis se, että paloilmoittimen tulee olla itsenäinen järjestelmä. Sen avulla voidaan ohjata muita järjestelmiä, mutta muilla järjestelmillä ei saa ohjata paloilmoitinta. Paloilmoittimeen liitettävät ohjaukset eivät saa vaarantaa paloilmoittimen toimintaa. (Hakkarainen 2007, s.31)

Rakennuksien tai tilojen suojaaminen paloilmoitinlaitteistolla perustuu yleensä rakennuslainsäädäntöön. Paloilmoitinlaitteisto voi olla liitetty hätäkeskukseen tai hälyttää vain paikallisesti. Paloilmoitinlaitteistolla on tietyissä tapauksissa mahdollista saada pidennettyä poistumismatkan pituutta tai suurennettua palo-osaston kokoa. Lisäksi paloilmoitinlaitteisto tulee asentaa yli 50 majoituspaikan majoitustiloihin sekä yli 25 vuodepaikan hoitolaitoksiin. (Ympäristöministeriön asetus rakennusten paloturvallisuudesta 848/2017 15§, 32§, 38§)

3.2.3 Automaattiset sammutuslaitteistot

Automaattisella sammutuslaitteistolla tarkoitetaan laitteistoa, joka havaitsee tulipalon ja sammuttaa sen alkuvaiheessaan, tai pitää palon hallinnassa, kunnes lopullinen sammutus saadaan suoritetuksi muilla keinoin (Ympäristöministeriön asetus rakennusten paloturvallisuudesta 848/2017 1 §; SFS EN 12845+A2 2015, s.6). Automaattiset sammutuslaitteistot voidaan jakaa ryhmiin niiden sammutteen mukaan. Sammutteita ovat yleensä: vesi, vaahto, jauhe tai erilaiset kaasut. Lisäksi sammutuslaitteistot, joiden sammutteena

toimii vesi, voidaan jakaa perinteiseen sprinkleri-, matalapaine vesisumu-, korkeapaine vesisumu- sekä vesivalelulaitteistoihin. (LVI 65-10512 2012, s. 3-6). Yleisin sammutuslaitteistoista on sprinklerilaitteisto, joka koostuu vesilähteestä/vesilähteistä ja yhdestä tai useammasta sprinkleriasennuksesta. Lisäksi sprinklerilaitteistoon on voitu liittää sähköllä tai polttomoottorilla toimiva paineenkorotuspumppu tai – pumppuja. Jokainen sprinkleriasennus koostuu asennusventtiilistä laitteineen sekä putkistosta ja sprinklereistä. Sprinklereiden toiminta perustuu lämpötilaan, jotka laukeavat määrätyssä lämpötilassa ja levittävät sammutusvettä niiden vaikutusalueelle. (SFS EN 12845+A2 2015, s.6)

Rakennuksien suojaaminen automaattisella sammutuslaitteistolla voi perustua rakennuslainsäädäntöön tai pelastuslainsäädäntöön tuomiin velvoitteisiin. Ympäristöministeriön asetuksessa rakennusten paloturvallisuudessa on esitettyjä luokkia ja lukuarvoja, joiden perusteella rakennus tai sen osa tulee suojata automaattisella sammutuslaitteistolla. Esimerkiksi yli kaksikerroksiset P2- paloluokan puurakenteiset asuinkerrostalot tulee suojata automaattisella sammutuslaitteistolla. Suojatessa rakennus tai sen osa automaattisella sammutuslaitteistolla voidaan esimerkiksi kasvattaa rakennuksen kerrosalaa, kerroslukua, korkeutta, palo-osaston kokoa sekä saada lievennyksiä kantaviin rakenteisiin, pintaluokkiin sekä uloskäytävien lukumäärään liittyen. Lisäksi automaattinen sammutuslaitteisto voidaan joutua asentamaan takautuvasti pelastuslain nojalla hoitolaitoksiin tai tuki- ja palveluasuntoihin, jos niiden poistumisturvallisuusselvityksen perusteella rakennuksen tai osan poistumisturvallisuus ei ole riittävä. (Ympäristöministeriön asetus rakennusten paloturvallisuudesta 848/2017; pelastuslaki 379/2011 18§-21§, 82§)

3.2.4 Savunhallintalaitteistot

Savunpoiston tai savunhallinnan tarkoituksena on poistaa tilasta savua, jolloin tilan olosuhteita saadaan parannettua. Tämä mahdollistaa turvallisen poistumisen, omaisuuden suojaamisen sekä sammutus- ja pelastustoiminnan nopeuttamisen. Savunpoisto on siis tulipalossa syntyvän savun ja lämmön poistamista tilasta, joka voidaan toteuttaa painovoimaisesti taikka koneellisesti. Savunpoistossa on huomioitava korvausilman saanti, jotta tilaan saadaan syötettyä riittävästi viileää ilmaa poistettujen kuumien savukaasujen tilalle. Lisäksi savunhallinnassa tilassa voi olla kiinteitä tai automaattisia savusulkuja,

jotka rajoittava savun leviämistä. (CEN/TR 12101-5. 2005, s 8-82). Savunhallintaan kuuluu myös ylipaineistus, jolla tarkoitetaan tilan esimerkiksi uloskäytävän paineistamista ylipaineella, jolloin palotilanteessa savu ei pääse tunkeutumaan paineistettuun tilaan (EN 12101-6 2005, s. 9).

Voimassa oleva rakentamiseen liittyvä lainsäädäntö edellyttää, että rakennukseen on suunniteltava ja rakennettava sen eri tiloihin soveltuva mahdollisuus poistaa tilasta savua sammutus- ja pelastustoiminnan tehostamiseksi. Tietyissä tapauksissa savunpoisto on järjestettävä erityistoimenpitein, jossa savunpoisto voidaan toteuttaa erillisten savunpoistoluukkujen, -ikkunoiden, tai -puhaltimien tai niiden yhdistelmien avulla. (Ympäristöministeriön asetus rakennusten paloturvallisuudesta 848/2017 1§, 42§).

3.2.5 Poistumisvalaistusjärjestelmät

Poistumisreittivalaistuksen tarkoituksena on avustaa tilassa olevien henkilöiden turvallista poistumista luomalla sopivat näkyvyysolot ja osoittamalla suuntaa opastein poistumisreiteillä. Poistumisvalaistuksen tulee mahdollistaa turvallisen poistuminen myös silloin, kun valaistuksen normaali sähkönsyöttö häiriintyy. (SFS-EN 1838 2015, s.6). Lisäksi poistumisvalaistuksen avulla voidaan varmistaa esimerkiksi paloilmoituspainikkeiden ja alkusammutuskaluston riittävä näkyvyys normaalin sähkönsyötön häiriinnyttyä (SFS-EN 50172 2004, s.10). Suomessa uloskäytävät ja niille johtavat poistumisreitit tulee merkitä poistumisopasteilla. Vaatimus koskee esimerkiksi majoitustiloja ja hoitolaitoksia, mutta ei asuinrakennuksia. Poistumisopasteiden tulee olla jatkuvasti valaistuja. Poistumisvalaistuksen virransyöttö tulee olla varmennettu siten, että toimivat vähintään yhden tunnin ajan normaalin virransyötön katketessa. (Sisäasiainministeriön asetus rakennusten poistumisreittien merkitsemisestä ja valaisemisesta 805/2005, 3 - 5§)

3.3 Paloturvallisuutta parantavien laitteiden järjestelmäintegraatiot

Paloturvallisuutta parantavia laitteistojen erilaisia integraatioita on toteutettu jo vuosikymmenien ajan. Esimerkiksi Bushby (2001, s.6-7) esitteli artikkelissaan jo 2000-luvun alussa paloilmoitinjärjestelmän integroimista IP-pohjaiseen rakennusautomaatio- ja oh-

jausjärjestelmään. Yleisin tapa järjestelmäintegraatioissa on kuitenkin ollut käyttää paloilmoittimen signaaleja suoraan tai epäsuoraan muiden paloturvallisuutta parantavien laitteiden tai oheislaitteiden ohjauksiin, kuten paloilmoitinlaitteistot kappaleessa 3.2.2 tuotiin esille. Paloilmoittimen ollessa osa järjestelmäintegraatiota on erityisesti varmistuttava siitä, että paloilmoitinjärjestelmän toimintaa ei häiritse tai sen toiminta ei häiriinny laukaistavasta järjestelmästä. Toisen palontorjuntajärjestelmän toiminta tai vikaantuminen ei myöskään saa häiritä paloilmoitinjärjestelmän oikeata toimintaa, tai estää antamasta viestiä mihinkään muuhun järjestelmään. (SFS-CEN/TS 54-14 2004, s. 27-36). Lisäksi toimintavarmuuden takaamiseksi esimerkiksi tiedonsiirron katkeaminen minkä tahansa muun järjestelmän ja paloilmoittimen välisessä siirtotiessä, ei saa haitata paloilmoittimen toimintaa (SFS-EN 54-13 2017, s.10).

Paloilmoitinlaitteisto voidaan myös yhdistää kauempana sijaitsevaan hälytyskeskukseen tai vikavalvomoon sekä rakennusautomaatio- tai palontorjuntajärjestelmään. Näitä järjestelmiä ei pidetä kuitenkaan paloilmoittimen osina (SFS-EN 54-13 2017, s. 5). Paloturvallisuutta parantavien laitteiden osalta integroidun hälytysjärjestelmän sisällä on mahdollista siirtää komentosignaaleja toiseen tai ohjauskeskukselta muihin osiin. Esimerkiksi paloilmaisin voidaan poistaa käytöstä etäkomennolla ohjauskeskuksesta. Lisäksi integraatiolla on mahdollista parantaa henkilöturvallisuutta, kuten kulunvalvontajärjestelmän ohjauksella estää CO^2-sammutuslaitteiston toiminta, kun henkilö astuu suojattuun tilaan. (SFS-CLC/TS 50398 2009, s.24)

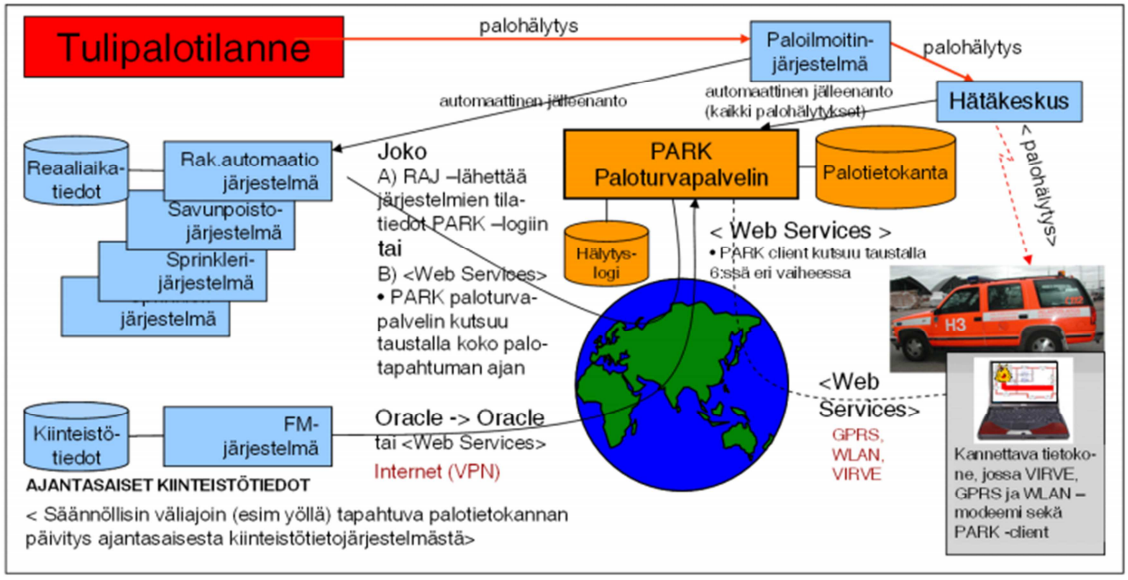
Integroimalla paloilmoitin- ja kiinteistöautomaatiojärjestelmä yhteen voidaan saavuttaa niin toiminnallisia kuin taloudellisia etuja. Näitä etuja ovat esimerkiksi keskitetty pääsy rakennusinformaatioon, antureista saatavan tiedon jakaminen, helpompi kunnossapito, tieto ihmisten paikantamiseksi, savunpoiston hallinta ja edellytysten luominen uudelle toimivalle ja turvallisuutta parantavalle teknologialle (Hakkarainen 2007, s. 31; Bushby 2001, s.9). Paloturvallisuutta parantavien laitteiden kuten paloilmoitin-, savunpoisto ja sammutuslaitteistojen integraatiolla saadaan pienennettyä omaisuusvahinkoja, parannettua henkilöturvallisuutta, mahdollistettua alkusammutuksen suorittaminen sekä taattua pelastustoimelle onnistumisen mahdollisuudet tulipalon sammutus- ja pelastustoiminnassa (Hakkarainen 2007, s.32).

Suomen markkinoilla on ollut turvajärjestelmiä, joiden avulla on mahdollista monitoroida ja hallita esimerkiksi paloilmoittimen, sammutuslaitteistoja, kamera-, murto- ja kulunvalvontaa. Näistä esimerkkinä ovat Schneider Electricin Esgraf-turvajärjestelmä sekä Siemens MM8000 valvontajärjestelmä. Erillisen tietokoneelta käytettävän käyttöliittymän avulla on ollut mahdollista seurata eri järjestelmien tilatietoja ja hälytyksiä sekä ohjata niitä. Visualisoinnin helpottamiseksi eri järjestelmissä olevia laitteita on voitu sijoittaa rakennuksien pohjakuviin, jolloin laitteiden paikantaminen käyttöliittymässä on helppoa esimerkiksi eri järjestelmien hälytyksien yhteydessä. (Schneider Electric 2016; Siemens 2011). Hedengren Security valmistaa Prodex FIREscape paloturvavalojärjestelmää, jossa yhdistyy kaksi rakennuksen keskeistä turvallisuusjärjestelmää: paloilmoitin- ja poistumisvalaistusjärjestelmä. Nämä on integroitu yhdeksi kokonaisuudeksi. Järjestelmän etuna on se, että yhdellä keskuksella sekä yhdellä kaapeloinnilla saadaan hallittua kahta eri järjestelmää. Järjestelmään on lisätty älykkyyttä, joka ohjaa palotilanteessa rakennuksessa olevat henkilöt turvallista reittiä ulos poistumisreiteillä olevien muuttuvin symbolein varustettujen opasvalaisimien avulla. (Hedegren Security 2017)

Suomessa kokeiltiin kehittää vuosien 2003 - 2007 välillä järjestelmää, jolla pystytään välittämään kiinteistöistä reaaliaikaista tilannetietoa alueen pelastusviranomaiselle jopa Internet-verkon yli. Toteutusorganisaationa toimivat Ramboll Finland Oy ja VTT. Ramboll Oy:n vastuulla oli hankkeen kokonaisvastuu ja VTT vastasi hankkeen tutkimusosuudesta. Mukana kehitystyössä oli useita eri viranomaisia, kiinteistön omistajia sekä palo- ja viestintäalan yrityksiä. Pilottihankkeita oli pääkaupunkiseudulta ja Oulusta. PARK-hankkeen tavoitteena oli hyödyntää uusinta ICT-teknologiaa, jotta tietoa saadaan siirrettyä pelastuslaitoksien johtoyksiköihin. Tarkoituksena oli tehostaa kiinteistössä tapahtuvaa pelastustoimintaa varsikin palohälytyksen alkutilanteessa.

PARK- järjestelmä koostuu paloturvapalvelimesta, palotietokannasta, hälytyslokitietokannasta sekä johtoauton kannettavassa tietokoneessa olevasta PARK- käyttöliittymästä. Järjestelmä yhdistää tallennetut ajantasaiset kiinteistötiedot, paloilmoituksesta tulevat tiedot ja paloteknisien laitteistojen keskeiset tiedot tilanteeseen liittyväksi täsmäraportiksi. Järjestelmän avulla voitiin lukea paloilmoittimelta tulleita tapahtumia, mutta ei voinut hallita järjestelmää esimerkiksi kuittaamalla palohälytyksiä. Pelastusviranomai-

sella oli palohälytyksen sattuessa mahdollista PARK-paloturvasovelluksen kautta monitoroida paloilmoitinlaitteistoa sekä hyödyntää järjestelmään tallennettuja kiinteistökohtaisia tietoja. Järjestelmää testattiin ja demonstroitiin GPRS, WLAN ja kiinteillä internet yhteyksillä. Kuvassa 5 on esitetty PARK-järjestelmän tiedonsiirron toteuttaminen. (Piira 2007, s. 1-4)



Kuva 5. PARK -tiedonsiirto. (Piira. 2005, s. 3)

3.4 Nykyaikaiset älykkäät paloturvallisuutta parantavat laitteistot

3.4.1 Palovaroittimet

Euroopan ja Suomen markkinoille on tullut älykkäitä palovaroittimia, joita voidaan hallita Internet-verkon yli sekä kerätä jopa dataa niiden toiminnasta. Näin ollen useita älykkäitä palovaroittimia voidaan pitää IoT-laitteina. Markkinoilla olevat älykkäät palovaroittimet hyödyntävät eri tiedonsiirtomenetelmiä. Palovaroittimien yhdistäminen Internetiin voi tapahtua esimerkiksi liittämällä palovaroitin tilan Wi-Fi-verkkoon, yhdistämällä se osaksi kodinautomaatiojärjestelmää tai hyödyntämällä suoraan LPWAN radioteknologian verkkoa. Seuraavassa on esitetty neljä erilaista älykästä palovaroitinratkaisua, jotka täyttävät Suomen lainsäädännön edellytyksenä olevan yhdenmukaistetun tuotestandardin SFS-EN 14604 vaatimukset.

Älykkäistä palovaroittimista ensimmäisenä esittelyssä on Google Nest Protect palovaroitin. Palovaroitin voidaan yhdistää esimerkiksi huoneiston Wi-Fi-verkkoon sekä ohjata toimintoja älypuhelinsovelluksella. Tavalliseen palovaroittimeen verrattuna kyseisessä palovaroittimessa on useita eri antureita kuten: valo-, kosteus-, liike-, lämpötila-, hiilimonoksidi- sekä savuanturit. Useiden antureiden vuoksi palovaroittimessa on useita eri toimintoja. Palovaroitin voidaan hiljentää älypuhelinsovelluksen kautta tai heiluttamalla kättä palovaroittimen alla, jolloin liikesensori lopettaa hälytyksen. Palovaroittimessa on ääniohjaus, joka hälyttää paikallisesti. Tieto alkaneesta palosta välittyy myös haluttuihin älypuhelimiin, joihin on luotu Nest-tilit. Nest Protect testaa patterin tilan, antureiden toimivuuden sekä ääni- ja hälytysäänet automaattisesti. Palovaroitin on varustettu pienitehoisella mikroprosessorilla, jonka vuoksi palovaroitin pysyy toimintakunnossa useita vuosia. Nest Protect -palovaroittimia on kahdenlaisia, paristokäyttöisiä sekä sähköverkkoon kytkettäviä. Nest Protect -palovaroitin toimii yhteen muiden Nest tuoteperheen älylaitteiden kanssa kuten Nest Thermostat kanssa. Palovaroittimen liikeanturin avulla voidaan kerätä tietoa siitä, onko esimerkiksi asukas kotona ja ohjata sisälämpötilaa sen mukaan. (Nest Protect 2018)

Kodinautomaatiojärjestelmään kytkettävistä älykkäistä palovaroittimista voidaan mainita Fibaro Groupin valmistama palovaroitin. Palovaroitin hyödyntää tiedonsiirtomenetelmänä Z-Wave standardia, jonka kautta se on liitettävissä standardia tukeviin kodinautomaatiojärjestelmiin. Fibaro Groupin älykkäässä palovaroittimessa on perinteisen savuanturin lisäksi lämpötila-anturi. Palovaroitinta voidaan hallinnoida älypuhelinsovelluksella sekä sen toiminnasta voidaan kerätä dataa. Integroimalla palovaroitin kodinautomaatiojärjestelmään voidaan sen avulla tehdä erilaisia ohjauksia kodin muihin järjestelmiin tai laitteisiin. (Fibaro 2018)

Kappaleessa 2.5 tiedonsiirtomenetelmät mainittiin, että Suomessa on hyödynnettävissä kaksi erillistä LPWAN radioteknologian verkkoa. Älykkäitä palovaroittimia on mahdollista yhdistää suoraan näihin verkkoihin, eikä sen vuoksi rakennuksen sisällä tarvitse välttämättä olla rakennettuna erillistä infrastruktuuria tiedonsiirtoa varten. Alueella toki tulee olla kyseisen verkon riittävä verkkopeitto. Smockeo on yksi älykkäistä palovaroittimista, jonka tiedonsiirrossa hyödynnetään Sigfox-verkkoa. Sigfox-verkkoon liittämisen jälkeen älykästä palovaroitinta voidaan hallita älypuhelinsovelluksella, kuten muita-

kin älykkäitä palovaroittimia. Sigfox-verkkoon liittämisestä verkko-operaattori perii vuosittain maksun verkkoon liitetyistä laitteista. (Smockeo 2018)

Uusien älykkäiden palovaroittimien lisäksi on nykyisin mahdollista yhdistää olemassa olevat palovaroittimet tai hiilimonoksidivaroittimet Internetiin. Tämä on mahdollista Roost Wi-Fi Batteryn avulla. Kyseessä on Wi-Fi toiminnolla varustettu 9V "älyparisto", jota voidaan ohjata älypuhelinsovelluksella. 9V paristo sopii paristokäyttöisten palo- tai hiilimonoksidivaroittimien paristokoteloon. Patteri on soveltuva myös sähköverkkoon kytkettyihin varoittimiin, jos sen virransyöttö on varmennettu 9V pariston avulla. Kuitenkaan tässä tapauksessa ei saada aikaan kaikkia hyötyjä, kuten palohälytyksen hiljentäminen älypuhelinsovelluksella. Roost Batteryssä on muutamia etuja. Se ilmoittaa älypuhelimeen hyvissä ajoin patterin vanhenemisesta. Tämä tieto palohälytyksestä saadaan ohjattua haluttuihin älypuhelimiin. Älykäspatteri voidaan nimetä suojatun tilan mukaan, jolloin palohälyttävän kohteen sijainnista saadaan tarkempi tieto. Lisäksi älykäspatteri kerää automaattisesti dataa esimerkiksi viimeisimmistä hälytyksistä ja testauksista. (Roost Inc. 2018)

3.4.2 Kodin automaatiojärjestelmät ja turvajärjestelmät

Kodin automaatiojärjestelmät ovat älykkäitä järjestelmiä, joihin on mahdollista liittää erilaisia toimilaitteita ja antureita kuten kuvassa 6 on esitetty. Näitä voivat olla esimerkiksi valaistuksen ohjaukset, lämpötilan mittaus tai palovaroitin. Automaatiojärjestelmissä yleinen malli on se, että toimilaitteet tai anturit liitetään suoraan yhdyskäytävään (gateway) tai niiden yhdistäminen tapahtuu erillisen hubin kautta (Ivanovic et al 2017, s.65-66).

Toimilaitteita ja antureita voidaan ohjata tai monitoroida esimerkiksi älypuhelin Internet-verkon yli. Järjestelmään liitettävät toimilaitteet ja anturit tukevat yleensä vain yhtä tiedonsiirtoon liittyvää standardia kuten Wi-Fi, Z-Wave tai ZigBee standardeja. Automaatiojärjestelmään liitetyistä toimilaitteista ja antureista voidaan kerätä dataa sekä niiden välille voidaan tehdä erilaisia integraatiota. (Ivanovic et al 2017, s.65-66). Esimerkiksi palovaroittimen toimiessa on mahdollista vilkuttaa asuinhuoneiston valoja, jotka on yhdistetty samaan kodin automaatiojärjestelmään (Fibaro 2018). Analysoimalla ke-

rättyä dataa automaatiojärjestelmä voi oppia asukkaan tottumuksista sekä havaita jopa hätätilanteita (Ivanovic et al 2017, s.65).

Kuva 6. Esimerkki Z-Wave kodin automaatiojärjestelmästä (Z-Wave 2018)

Cozify on valmistanut kodin automaatiojärjestelmän, jossa hubin avulla on mahdollista yhdistää eri laitevalmistajien toimilaitteita ja antureita samaan järjestelmään. Kyseiseen kodin automaatiojärjestelmään voi yhdistää, tai siinä on valmius yhdistää eri standardien ja protokollien toimilaitteita ja antureita. Tämä mahdollistaa useiden eri laitevalmistajien antureiden ja toimilaitteiden yhdistämisen ja integroimisen yhteen. (Cozify 2018)
Kodin turvajärjestelmät ovat etupäässä tarkoitettu turvallisuuden parantamiseen, eivätkä ole yhtä monipuolisia ratkaisuja kuten kodin automaatiojärjestelmät. Järjestelmään voidaan yhdistää useita toimilaitteita ja antureita kuten palovaroittimia tai murtosuojauslaitteistoja. Kodin turvajärjestelmissä palveluun kuuluu yleensä vartiointi sekä hälytyskeskus palvelut. Hälytyksen yhteydessä tieto välittyy palveluntarjoajan hälytyskeskukseen, jonka tiedonsiirrossa hyödynnetään GSM- ja Internetyhteyttä. Esimerkiksi paloilmoituksen yhteydessä hälytyskeskuspäivystäjän on mahdollista monitoroida asuintiloja kamerailmaisimien ottamien kuvilla. Erillisien mobiilisovelluksen avulla asukkaalla on myös mahdollisuus hallinnoida asunnon eri toimilaitteita. (Verisure 2018; Sector Alarm 2018)

3.4.3 Automaattiset paloilmoitinlaitteistot

Paloilmoitinjärjestelmät ovat olleet paloturvallisuustekniikan edelläkävijöitä älytekniikan saralla jo useita vuosia. Nyt järjestelmiä on ollut mahdollista liittää Internetiin siten, että niitä voidaan hallita, kerätä dataa sekä valvoa Internet-verkon yli, jopa mobiilisti.

Siemens on kehittänyt Desigo CC:n, avoimen kiinteistönhallintajärjestelmän, jonka avulla käyttäjän on mahdollista hallita kaikkia kiinteistössä olevia järjestelmiä ja optimoida ne haluamallaan tavalla. Decigo CC:n valvomoalustaan on mahdollista integroida myös turvallisuuteen liittyviä järjestelmiä, kuten paloilmoitintoteutuksia. Valvomoalusta mahdollistaa myös erilaisten järjestelmien välisten integraatioiden tekemisen esimerkiksi paloilmoitinlaitteiston, äänievakuoinnin, rakennusautomaation sekä kameravalvonnan kanssa. Tämä mahdollistaa erilaisten järjestelmien alaisten toimintojen toteuttamisen paloilmoituksen sattuessa. Järjestelmäintegraatioiden tekeminen Decigo CC:ssä on helpotettu käyttämällä avoimen tiedonsiirron standardeja ja protokollia. Decigo CC:n yhteyteen on saatavissa eritasoisia Sinteso-elinkaaripalvelun moduuleja, joka mahdollistaa erilaiset lisäpalvelut. Näitä ovat esimerkiksi etäyhteyden muodostaminen paloilmoitinjärjestelmään tietokoneelta tai mobiilisti. Etäyhteyden avulla voidaan monitoroida ja hallita paloilmoitinta tarkastamalla laitteiston valmiustila tai tekemällä ilmaisimien ja paloryhmien irtikytkentöjä. Koko kiinteistön eri rakennusautomaatio- ja turvallisuusjärjestelmiä voidaan hallita yhden käyttöliittymän kautta. Sinteso-elinkaaripalvelu taas antaa mahdollisuuden kerätä haluttua dataa eri järjestelmistä analysointia varten. Laajimmillaan Siemens voi tarjota Sinteso-elinkaaripalvelun avulla erilaisia tuki- ja päivityspalveluita Internet-verkon yli. (Siemens 2017)

Schneider Electricin kehittämä EcoStructure on esineiden internetiä (IoT) tukeva avoin, yhteensopiva arkkitehtuuri ja alusta. Paloilmoitinjärjestelmien tehokkuuden hallintaan on kehitetty EcoStructure Fire Expert online-sovellus, joka toimii Saas-pilvipalveluratkaisuna. Sitä voidaan hyödyntää Schneider Electricin valmistamissa paloilmoitinjärjestelmissä. Käyttöliittymä on selainpohjainen ja sitä voidaan käyttää tietokoneella sekä mobiililaitteilla kuten älypuhelimella tai tabletilla. Fire Expertin perusnäkymä sisältää paneelin sekä silmukka- ja osoiteviat. Lisäksi käyttäjät voivat nähdä myös kaikki irtikytkennät ja huoltoilmoitukset. Erillisen reitittimen tai yrityksen ver-

kon avulla voidaan paloilmoitinjärjestelmän pääkeskus liittää helposti online-sovellukseen. Reititin on valmiiksi konfiguroitu ja testattu, joten yhteydenluonti paloilmoitinjärjestelmästä Fire Expertiin on vaivatonta ja turvallista. (Schneider Electric 2017)

3.4.4 Automaattiset sammutuslaitteistot

IoT-ratkaisuja on tarjolla myös automaattisien sammutuslaitteistojen puolelle. Sprinklerilaitteistoihin on mahdollista lisätä anturointia, joiden avulla voidaan monitoroida järjestelmää reaaliaikaisesti. Monitoroinnin kohteena voi olla esimerkiksi putkiston paineen tai pumppujen toiminnan seuranta. (FireTweet 2016). Monitoroinnin lisäksi sprinklerilaitteistojen älykkyyttä voidaan lisätä asentamalla ohjaus- ja valvontakeskus. Parhaiten järjestelmä soveltuu vesisumujärjestelmiin. Ohjaus- ja valvontakeskus voi kerätä ja tallentaa kaiken sen datan kaikista laitteistoon tehtävistä testauksista, huoltotoimenpiteistä sekä sattuneista hälytyksistä. Laitteiston tilan seuranta tai sen hallinta voidaan toteuttaa langallisella kosketusnäytöllä, tekstiviestillä tai Internet-pohjaisella käyttöliittymällä. Ohjaus- ja valvontakeskus on myös mahdollista liittää olemassa oleviin kiinteistövalvontalaitteisiin. (Probemen 2017). Myös perinteiseen sprinklerilaitteiston hälytysventtiilin yhteyteen on mahdollista liittää erillinen testauslaitteisto, jonka avulla sammutuslaitteiston toimintavarmuutta voidaan testata automaattisesti (ProjectFire 2018)

3.4.5 Poistumisvalaistusjärjestelmät

Primex Wireless' on kehittänyt Wi-Fi pohjaisen poistumisvalaistusjärjestelmän hallintajärjestelmän. Kyseinen järjestelmä hyödyntää rakennuksen olemassa olevaa Wi-Fi verkkoa. Primex Wireless' SNS ohjelma ottaa vastaan dataa Wi-Fi vastaanottimella ja sensoreilla varustetuista turvavalojen ja opasvalaisimien polttimoiden ja akkujen tilasta. Hallintajärjestelmää käytetään selainpohjaisella sovelluksella, josta pystyy näkemään järjestelmän tilan. Vikojen ilmaantuessa järjestelmä ilmoittaa huoltohenkilöstölle tarpeen mukaan. Valmistajan mukaan olemassa olevia turvavalaisimia tai opasvalaisimia voidaan päivittää Wi-Fi valmiuteen. Hallintajärjestelmän avulla voidaan keskittää huol-

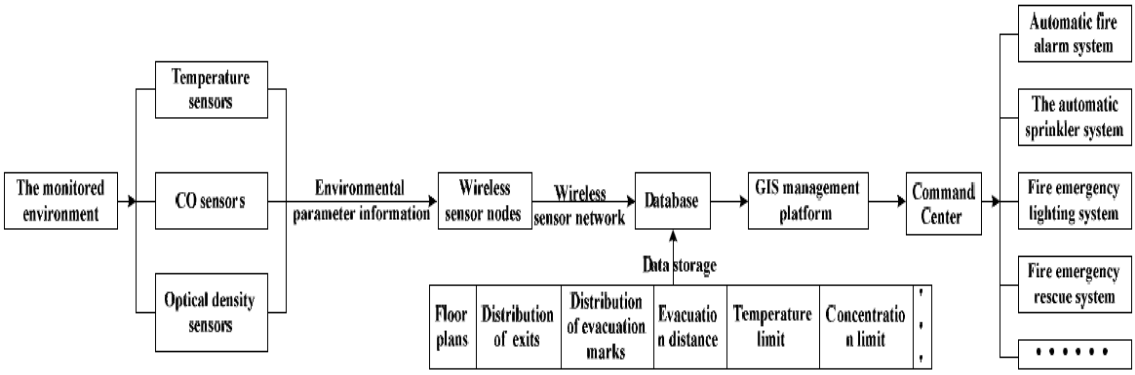
totoimenpiteet paljon ennakoivemmiksi sekä vikaantumisien korjaaminen voidaan keskittää tehokkaammin. Tuote on tarkoitettu Yhdysvaltojen markkinoille, koska sillä ole EN-standardin mukaisia turvavalaisimia tai opasvalaisimia. (Swedeberg 2012)

Normaluxilla on markkinoilla älykäs poistumisvalaistusjärjestelmä, jota on mahdollista hallita älypuhelimella tai tabletilla Internet-verkon yli. Lisäksi poistumisvalaistusjärjestelmän asennuksissa on mahdollista hyödyntää esimerkiksi DALI -valaistuksen digitaalista ohjasväylää, KNX hajautettua väyläpohjaista kiinteistöohjausjärjestelmää tai BACnet tiedonsiirtoprotokollaa. Järjestelmään on lisäksi mahdollista asentaa langattomia poistumisopasteita. Poistumisopasteet ja turvavalaisimet diagnosoivat toimintaa itsenäisesti. Jos järjestelmän komponenttiin, kuten valaisimen akkuun tai valonlähteeseen tulee vika, välittää järjestelmä automaattisesti tiedon haluttuun paikkaan. Tarvittavat huoltotoimenpiteet voidaan toteuttaa näin nopeasti ja tehokkaasti. (Normalux 2018, s. 23-31)

3.4.6 Evakuointijärjestelmä

Myös evakuointiin sekä väestönvaroittamiseen liittyvät järjestelmät ovat kehittymässä entistä älykkäämmiksi. Järjestelmien kehittämiseen on ollut selkeää kiinnostusta, mikä on havaittavissa useista tieteellisistä artikkeleista ja esityksistä. Tutkimus- ja kehitystyö ovat keskittyneet ennen kaikkea tarkan onnettomuustiedon ja toimintaohjeiden välittämiseen älypuhelimiin sekä erilaisten sisäpaikannusjärjestelmien hyödyntämiseen ihmisten paikantamiseen. IoT:n hyödyntäminen on katsottu olevan mahdollista myös evakuointijärjestelmien kehityksessä, koska langattomia verkkoja, rakennuksien talotekniikanjärjestelmiä, valvontakameroita, turva- ja sisäpaikannusjärjestelmistä sekä näiden järjestelmäintegraatioilla avulla saadaan tehokkaasti aikaan jopa reaaliaikainen tilannekuva onnettomuus- tai vaaratilanteesta. Tilannekuvan avulla voidaan selvittää mitä ja missä on tapahtunut, seurata onnettomuuden kehitystä, saada tietoa rakennuksessa tai alueella olevien ihmisten sijainnista ja tehokkaasti tiedottaa ihmisiä vaaratilanteesta sekä ohjata heidät turvallisinta reittiä pois vaara-alueelta. Lisäksi tätä samaa tietoa on mahdollista välittää viranomaisille. (Gokceli et al 2017; Ryu 2015; Bhavani & Uthra 2017; Mohan et al 2016)

Henkilöiden paikantamiseen voidaan käyttää useita eri teknologioita, kuten WLAN kolmiomittausta ns. sormenjälkipaikannusta (fingerprint), henkilökohtaisien paikannustunnistimien kautta tai nykyaikaisen kameratekniikan avulla (Gokceli et al 2017, s. 7; Mohan et al, s. 684). Tutkituissa järjestelmissä toiminta perustuu pitkälti älypuhelinsovelluksen kautta välitettäviin tietoihin, jonka kautta pystytään visuaalisesti osoittamaan esimerkiksi rakennuksen pohjakuvaan esitettynä henkilön ja vaara-alueen sijainti sekä osoittaa turvallisin reitti poistumaan rakennuksesta tai vaara-alueelta. Vaara-alueen tunnistaminen voi perustua esimerkiksi osoitteellisen paloilmoitinjärjestelmän välittämään tietoon. Paikantamisen ja opastuksen lisäksi ihmisille on mahdollista kertoa oikeat toimintaohjeet miten toimia kyseisessä vaara- tai hätätilanteessa. Tilanteen kehittymistä on mahdollista monitoroida esimerkiksi hallinnointikeskuksesta. (Ruy 2015, s.165-167; Bhavani & Uthra 2017, s. 494-496)



Kuva 7. Evakuointijärjestelmän rakennemalli (Liu & Zhu 2014, s. 579)

Kuvassa 7 on esitetty evakuointijärjestelmän rakennemalli. Esitettyyn evakuointijärjestelmään kuuluu kolme vaihetta: 1) Sensoreiden avulla kerätään valvottavasta ympäristöstä parametritietoa, kuten lämpötilasta, hiilimonoksidin tiheydestä, valon taajuudesta jne. 2) Välitetään informaatiota, joka on saatu sensoreilta komentokeskukseen langatonta verkkoa hyödyntäen ja prosessoidaan dataa käyttäen paikkatietojärjestelmän toimintoja sekä hyödyntäen datavaraston tietoja. 3) Tietoja käsitellään tulosten mukaan: kerran kun palo tapahtuu rakennuksessa, aloittavat tarkoituksen mukaiset palontorjuntajärjestelmät toimintansa, jotta voidaan luoda hyvät mahdollisuudet evakuoinnille ja ohjaamiseksi ihmiset nopeasti ulos. (Liu & Zhu 2014, s. 579)

Tämän työn tekemisen yhteydessä ei löytynyt markkinoilta vielä edellä mainittuja älykkäitä ratkaisuja, jotka olisi pitkälti toteutettuna IoT-ratkaisuna. Kuitenkin älykkäimmistä evakuointi- ja tiedotusjärjestelmistä voidaan mainita Siemens Desigo CC valvomoalustalle tehdyn Desigo Mass Notification järjestelmän. Mass Notificatio järjestelmällä on mahdollista varoittaa erilaisissa hätätilanteissa rakennuksessa tai kiinteistön alueella oleskelevia ihmisiä. Desigo CC valvomoalustan hyödynnettävyyden vuoksi siihen on helppo integroida myös muita talotekniikkaan tai turvallisuuteen liittyviä järjestelmiä. Järjestelmän käytön ja hallinnoinnin yhtenä vaihtoehtona on selainpohjainen käyttöliittymä, johon on mahdollista luoda ennalta määriteltyjä skenaarioita sekä niihin liittyviä varoitusviestejä. Järjestelmän hallinnoijalla on mahdollista nopeasti valita sopiva hätätilanne ja välittää se ihmiselle eri tavoin. Varoitusviestien välittämiseksi on useita mahdollisuuksia kuten tekstiviesti, sähköposti, näyttötaulut, sosiaalisen median Facebook ja Twitter sekä ilmoitukset tietokoneiden kuvaruutujen kautta. Lisäksi varoittaminen on mahdollista toteuttaa perinteisesti kaiuttimien kautta puheena live-ilmoituksena tai nauhoitteena. Mass Notification järjestelmään on mahdollista integroida rakennuksien asema- ja pohjapiirustuksia tai seurata valvontakameroiden avulla tapahtumien kulkua. Lisäksi järjestelmää voidaan käyttää päivittäisiin tiedottamistarpeisiin asioihin, jotka on tarpeellista välittää alueen tai rakennuksen ihmisille. (Siemens 2016)

3.5 IoT-teknologian kautta saatava hyöty

IoT:n yksi suurimmista hyödyistä on laitteiden monitorointi Internet-verkon yli, eli mahdollisuus seurata laitteiden toimintaa etäyhteydellä lähes reaaliaikaisesti. Tämä tuo valtavia mahdollisuuksia esimerkiksi huolto- ja ylläpitotoimintaan. IoT-laitteiden älykkyyden kasvaessa on etäyhteyttä hyödyntäen mahdollistaa toteuttaa ennakoivaa huoltoa siten, että omistajat eivät välttämättä edes huomaa laitteen huollon toteuttamista. Laitteiden huollosta vastaava taho voi lisäksi selvittää suoraan, mikä laitteessa on vikana ja analysoida vikaa jo ennen kuin saapuu fyysisesti paikalle. Yksilöidyn tunnistamisen avulla vikaantuneen laitteen löytäminen on myös helppoa. (Saarikko et al 2017, s. 5-6; Deloitte 2016, s.40). Esimerkiksi FireTweet yritys tarjoaa palontorjuntalaitteisiin liittyen IoT-ratkaisuun perustuvaa reaaliaikaista monitorointia. Sprinklerilaitteistossa on mahdollista seurata jatkuvasti putkiston painetta tai sprinkleripumppujen tehoa, kun taas

reaaliaikaisella monitoroinnilla voidaan seurata, että käsisammuttimet ovat paikallaan ja toimintakuntoisia. (FireTweet 2016).

Automaattisen paloilmoitinlaitteiston reaaliaikainen etäyhteys Internetin välityksellä mahdollistaa tehokkaamman järjestelmän monitoroinnin ja ohjaamisen. Etäyhteyden avulla voidaan valvoa järjestelmien tilaa mistä tahansa, milloin tahansa. Yleensä paloteknisiä laitteistoja käytetään ja hallinnoidaan rakennuskohtaisista käyttökeskuksista käsin. Etäyhteyden avulla voidaan lisätä tehokkuutta ja vähentää ylläpitokuluja. Ennen kaikkea voidaan tehokkaammin erottaa erheelliset palohälytykset oikeista tulipaloista ja parantaa omaisuuden ja henkilöiden turvallisuutta. (Shinde et al 2017, s. 1080)

Älytekniikan avulla voidaan vähentää erheellisiä palohälytyksiä. Erilaisten antureiden ja järjestelmäintegraatioiden avulla saadaan laitteistojen toiminta ohjautumaan automaattisesti halutulla tavalla. Antureista kerätyn tiedon perusteella sekä ennalta määriteltyjen algoritmien avulla voidaan tunnistaa tulipalo entistä luotettavammin. Yhden anturin sijaan on mahdollista käyttää useita antureita tulipalon tunnistamiseen. Ennakkoon määriteltyjen kynnysarvojen ylittyessä palontorjuntalaitteet aloittavat vasta toimintansa. Palontorjuntalaitteistojen toimiessa paloilmoitus voidaan ohjata halutulle alueelle sekä välittää laitteiston toiminnasta tarpeellisille toimijoille. Esimerkiksi tulipalon sattuessa savu- ja hiilimonoksidi-ilmaisimien toiminnat voivat ohjata sammutuslaitteiston toimintaa, esimerkiksi havaitessa tilassa savua ja hiilimonoksidin nousua. Tämä indikaatio käynnistää sammutuslaitteiston pumpun sekä avaa laitteiston pääsulkuventtiilin. (Oh et al 2013, s. 2-3)

Tuomisaari (2017) on diplomityössään tuonut esiin hyötyjä, joita voidaan saada, kun IoT-teknologiaa sovelletaan sammutuslaitteistoon (fire protection system). Asiaa lähestytään etupäässä laitevalmistajan näkökulmasta. IoT-teknologiaa hyödyntämällä voidaan sammutuslaitteiston tilaa monitoroida aiempaa huomattavasti tarkemmin. Tarkan monitoroinnin avulla sammutuslaitteistoon tulevat vikaantumiset saadaan nopeasti selville. Tämän myötä esimerkiksi laitevalmistajan on mahdollista aloittaa nopeasti toimenpiteet ilmi tulleiden vikojen korjaamiseksi. Näin ollen on mahdollista kehittää ja tehostaa huolto- ja kunnossapitopalvelujen tarjontaa. Keräämällä dataa sammutuslaitteistosta, sen komponenteista tai sammutuslaitteiston ympäristöstä, laitevalmistajan on

mahdollista hyödyntää saatua tietoa tuote- ja palvelukehityksessään. Toisena mainittavana asiana on, että kerättyä dataa voidaan käyttää kohdentamaan määräaikaishuoltotoimenpiteitä tai muuttaa tiettyjä huoltotoimenpiteitä vain tarpeen mukaan suoritettavaksi. Lisäksi kerätystä datasta voivat olla kiinnostuneita eri osapuolet, ja osapuolien komponentteja on esimerkiksi asennettu osaksi sammutuslaitteistoa. IoT-teknologia mahdollistaa datan jakamisen eri osapuolille. (Tuomisaari 2017, s. 46)

Älykkäässä evakuointijärjestelmässä eri laitteiden järjestelmäintegraatioiden avulla on mahdollista havaita alkaneen tulipalon sijainti sekä osoittaa rakennuksessa tai alueella oleskeleville ihmisille missä tulipalo on syttynyt sekä ohjata heidät turvallisinta reittiä ulos. Näin estetään henkilövahinkojen syntyminen sekä mahdollistetaan saman tiedon välittämisen esimerkiksi pelastusviranomaiselle. (Ryu 2018, s. 166-167). Evakuointijärjestelmän ollessa integroituna rakennuksen sisäpaikannusjärjestelmään, voidaan rakennuksessa oleskeleville ihmisille välittää heidän sijainneistaan tietoa langatonta verkkoa hyödyntäen esimerkiksi älypuhelinsovellukseen, jossa tieto on esitetty visuaalisesti rakennuksen pohjakuvaan. Tämä mahdollistaa nopean poistumisen rakennuksesta ja lisää näin turvallisuutta. Lisäksi rakennukseen loukkuun jääneet ihmiset voidaan löytää helpommin. (Mohan et al 2016, s. 685)

4 TUTKIMUKSEN TOTEUTUS JA TUTKIMUSMENETELMÄT

Tässä luvussa kuvataan tutkimuksessa käytetyt tutkimusmenetelmät, esitellään tutkimuksen toteutus, sisällön analyysin suorittaminen ja lopuksi arvioidaan tutkimuksen luotettavuutta. Tämä tutkimus on laadullinen tutkimus.

4.1 Tutkimusmenetelmät

Tutkimusmenetelmäksi valittiin kvalitatiivinen eli laadullinen tutkimus, koska lähtökohtana on pyrkiä saamaan mahdollisimman syvällinen näkemys tutkittavasta ilmiöstä (Kananen 2017, s. 33). Laadullisessa tutkimuksessa pyritään myös tutkimaan valittua kohdetta mahdollisimman kokonaisvaltaisesti (Hirsjärvi et al 2010, s.161). Tutkimuksen tavoitteena oli haastattelujen avulla kerätä tietoa ja näkemyksiään siitä, miten IoT-teknologiaa voidaan hyödyntää paloturvallisuuden kehityksessä. Haastattelutapahtuma on systemaattinen tiedonkeruun muoto, jossa on tavoitteena saada aikaan mahdollisimman luotettavia ja päteviä tietoja. (Hirsjärvi et al 2010, s. 207). Haastatteluun päädyttiin, koska se on hyvin joustava menetelmä laadullisen tutkimuksen tarpeisiin. Sen avulla voidaan hakea vastauksia erilaisiin ongelmiin tai tutkia erilaisia ilmiöitä. Haastattelun yhteydessä on mahdollista toistaa kysymys, oikaista väärinkäsityksiä sekä selventää ilmaisujen sanamuotoja sekä käydä myös vapaampaa keskustelua haastateltavien kanssa. (Tuomi & Sarajärvi 2009, s. 73-74). Samoin on mahdollista saada esiin vastausten taustalla olevia motiiveja, haastatteluaiheiden järjestystä on mahdollista säädellä sekä mahdollisuus syventää annettuja vastauksia (Hirsjärvi et al 2010, s.205).

Aineiston kerääminen päätettiin toteuttaa teemahaastatteluja suorittamalla. Kaikki haastattelut olivat yksilöhaastatteluja. Teemahaastattelu on avoimen haastattelun ja lomakehaastattelun välimuoto ja sitä voidaankin kutsua myös puolistrukturoiduksi haastatteluksi. Teemahaastattelussa haastattelu etenee ennalta valittujen teemojen mukaisesti. Tyypillistä on, että teemahaastattelussa aihepiirit, eli teemat ovat ennalta tiedossa. Teemahaastattelussa kysymysten tarkka muoto ja järjestys voi puuttua, jonka vuoksi kaikille haastateltaville ei välttämättä esitetä samoja kysymyksiä. Puolistrukturoidusta haastattelussa vastauksia ei ole sidottu mihinkään vastausvaihtoehtoihin, vaan haastateltavat voivat vastata omin sanoin. Teemahaastattelussa otetaankin huomioon ihmisten tulkin-

nat asioista. Haastateltavien antamat merkitykset heidän esittämilleen asioille ovat keskeisiä. (Hirsjärvi & Hurme 2014, s. 46-48). Teemahaastatteluun päädyttiin myös sen vuoksi, että haastatteluaineiston pilkkominen analyysivaiheessa on suhteellisen helppoa, koska haastattelun teemat muodostavat itsessään jo jäsennellyn ja ryhmitellyn aineiston (Tuomi & Sarajärvi 2009, s.93).

Teemahaastattelun runko perustuu neljään yläteemaan, joiden alla on kahdesta neljään kysymystä. Yhteensä kysymyksiä on 14. Kolmen ensimmäisen teeman kysymykset esitettiin kaikille haastateltaville. Viimeisen teeman kysymykset esitettiin haastateltaville, joilla mahdollisesti oli osaamista paloteknisistä laitteistoista ja niiden integraatioista. Teemahaastattelun runko ja kysymykset on esitetty liitteessä 1. Alla on esitetty teemahaastattelun rungon pääteemat sekä suluissa niihin liittyvien kysymysten lukumäärä.

- IoT – teknologian ja älytekniikan hyödyntäminen rakennuksissa (4)
- Datan kerääminen, jakaminen ja sen rikastamisesta saatava hyöty (2)
- IoT – teknologian rajapinnat sekä uhat ja mahdollisuudet (4)
- Paloteknisiä laitteistoja ja toimintavarmuutta koskevat lisäkysymykset (4)

Teemahaastattelun kysymykset voidaan jakaa mielipidekysymyksiin sekä tosiasiakysymyksiin (Hirsjärvi & Hurme 2014, s. 106). Haastattelun rungon kysymykset edustivat kumpiakin kysymyksiä. Kysymyksistä on selkeästi havaittavissa mitkä ovat tosiasiakysymyksiä ja mitkä mielipidekysymyksiä. Lisäksi tähän vaikutti erityisesti haastateltavan tietopohja vastata kyseiseen kysymykseen.

Tiedonkeruun järjestäminen haastattelujen avulla antoi myös tutkijalle mahdollisuuden keskustella haastattelun lopuksi tutkimusaiheeseen liittyvistä asioista. Haastateltava sekä haastattelija vaihtoivat usein tietojaan aihealueeseen liittyen. Tämä tiedonvaihto on kokonaisuutena ollut hedelmällistä ja sillä on ollut todella paljon merkitystä tutkittavan ilmiön syvällisemmässä ymmärtämisessä. IoT:n kehitys ja teknologian hyödyntäminen on ollut nopeaa. Tämän vuoksi tiedonvaihtaminen on ollut tärkeää ja se on mahdollistanut uusimpien tietojen tuomisen esiin tässä työssä myös kirjallisuuskatsauksen näkökulmasta.

4.2 Tutkimuksen toteutus

Tutkimusta varten tehtiin kaksi eri selvitystä. Teemahaastattelujen avulla pyrittiin selvittämään Suomen tilannetta IoT:n ja älytekniikan hyödyntämisestä rakennusten paloturvallisuuden kehityksessä, kuten edellisessä kappaleessa tuotiin esille. Toisessa selvityksessä tavoitteena oli lomakehaastattelun avulla selvittää IoT-teknologian hyödyntämistä paloturvallisuuden kehityksessä muissa Pohjoismaissa. Lomakehaastattelu toteutettiin strukturoidulla lomakkeella, jossa oli lisäksi kaksi avointa kysymystä. Lomakehaastattelu toteutettiin hyödyntäen Webropol - sähköistä kyselylomaketta. Lähete sekä linkki kyselylomakkeeseen toimitettiin sähköpostilla CTIF-organisaation Pohjoismaiden yhteyshenkilöille. Vastauksia saatiin vain kaksi, joten tiedonkeruu epäonnistui useista muistutuksista huolimatta. Näin ollen Pohjoismaiden tilanne jäi tässä työssä selvittämättä.

Tutkimuksen yksi haasteellisimmista tehtävistä oli haastateltavien valitseminen. Tutkimussuunnitelman teon yhteydessä kävi jo selväksi, että aiheeseen liittyvää substanssiosaamista ei Suomessa toistaiseksi vielä juuri ole. Tämän vuoksi päädyttiinkin haastattelemaan useita eri alojen henkilöitä. Haastattelujen perusteella on tarkoituksena saada aina pieni osa ymmärrystä tutkittavasta aiheesta, jotka kokoamalla pyritään saamaan käsitys tutkittavasta aiheesta (Kananen 2017, s.90). Haastateltavien valinnassa tuli tarkkaan arvioida, minkä eri osa-alueen henkilöitä tutkimusta varten on syytä valita. Valinnan jälkeen tuli suorittaa toinen arviointi, jossa arvioitiin haastateltavan tietopohjaa vastata teemahaastattelussa esitettyihin kysymyksiin.

Henkilöiden valintaan saatiin apua diplomityön ohjaajalta, joka ehdotti muutamia henkilöitä haastateltavaksi. Osa näistä henkilöistä tuli valittua, kun heidän soveltuvuus haastateltavaksi oli arvioitu. Haastateltavaksi sopivan henkilön valitseminen tapahtui yleensä tutkijan oman selvitystyön tuloksena. Haastateltavia valittiin osin myös lumipallo-otantaa käyttäen, jossa haastateltava henkilö suositteli haastattelemaan kyseistä henkilöä tämän aiheeseen liittyvän osaamisen vuoksi (Hirsjärvi & Hurme 2014, s. 59). Haastateltavista kolme valittiin lumipallo-otannalla. Tämä oli toisaalta tutkimuksen kannalta välttämätöntä, koska moni haastateltavaksi alustavasti suostunut ei loppujen lopuksi suostunutkaan tehtävään. Laitevalmistajista osa ei suostunut haastateltavaksi, koska yrityksen IoT- ja älyteknologiaan liittyvä tuotekehitys oli siinä vaiheessa, ettei

niiden tuomista hyödyistä haluttu vielä kertoa. Loppujen lopuksi haastateltavia valikoitui yhteensä 14 henkilöä, joista jokaista haastateltiin vain yhden kerran. Haastateltaviksi soveltuvia henkilöitä lähestyttiin sähköpostilla tai soittamalla. Teemahaastattelun runko toimitettiin haastateltaville sähköpostilla yleensä noin viikkoa ennen sovittua haastattelua. Näin annettiin haastateltavalle mahdollisuus tutustua ja valmistautua haastatteluun etukäteen.

Haastateltavat edustivat seuraavia toimialoja:

Pelastusviranomaiset	2 henkilöä
Talotekniikan osaajat	2 henkilöä
Paloteknisten laitteistojen valmistajat	2 henkilöä
Paloturvallisuussuunnittelijat	1 henkilö
Paloteknisten laitteistojen suunnittelijat	1 henkilö
Kiinteistön omistajien edustajat	2 henkilöä
Tietoturva-asiantuntijat	1 henkilö
Verkkoliikenneasiantuntijat	1 henkilö
Tutkimus- ja kehityshenkilöstö	2 henkilöä

Tarkoituksena oli suorittaa haastattelutilanteet mahdollisimman usein kasvotusten, jotta voitaisiin olla mahdollisimman hyvässä vuorovaikutuksessa haastateltavan kanssa (Kananen 2017, s. 91). Teemahaastattelujen avulla on haastateltavan ja haastattelijan välille mahdollista saada aikaan syvä dialogi, jonka vuoksi kertynyt materiaali voi olla rikkaampaan moneen muuhun tiedonkeruu menetelmään nähden (Hirsjärvi & Hurme 2014, s. 135). Kasvokkain haastattelujen suorittaminen ei kuitenkaan tullut kaikissa tapauksissa mahdolliseksi matkustamiseen liittyvien rajoitteiden tai aikataulullisten syiden vuoksi. Haastattelutilanteista viisi suoritettiin kasvotusten, kolme Skypen välityksellä ja kuusi puhelinhaastatteluna. Haastattelutilanne oli kestoltaan yleensä noin tunnin mittainen suoritus. Kaikki haastattelut nauhoitettiin digitaalisella sanelimella sekä haastattelujen yhteydessä haastattelija teki omia muistiinpanoja.

Nauhoitettu laadullinen aineisto kirjoitettiin puhtaaksi sanasanaisesti eli aineisto litteroitiin. Litterointi toteutettiin etupäässä sanatarkasti, koska se antaa aineiston analyysille monipuolisia mahdollisuuksia (Hirsjärvi & Hurme 2014, s. 140 - 141). Tekstiä pyrittiin litteroinnin yhteydessä kirjoittamaan luettavampaan muotoon poistamalla sanojen toistamisia tai muuttamalla puhekieltä kirjakieleksi. Litteroinnin tuloksena syntyi tekstiä

noin 100 sivua A4 arkkia. Haastattelujen litteroinnin yhteydessä jätettiin litteroimatta keskustelut, jotka eivät liittyneet itse aiheeseen. Poistetuista kohdista on maininta litterointiaineistoissa.

4.3 Sisällönanalyysi

Laadullisessa tutkimuksessa aineiston analysointi alkaa jo haastattelutilanteessa. Tutkijan tehdessä haastattelut hänellä on mahdollisuus tehdä sen yhteydessä havaintoja ilmiöstä ja sen jakautumisesta. (Hirsjärvi & Hurme 2014, s. 136). Litteroidulle aineistolle suoritettiin sisällönanalyysi. Sisällönanalyysi on laadullisessa tutkimuksessa hyvin usein käytetty perusanalyysimenetelmä, jonka avulla voidaan tehdä monenlaista tutkimusta. Hyvänä puolena sisällönanalyysissä voidaan pitää sitä, että sitä voidaan pitää väljänä teoreettisena viitekehyksenä tutkittavaan aiheeseen. Samalla tutkittavasta aiheesta yritetään saada kuvaus tiivistetyssä ja yleisessä muodossa. (Tuomi & Sarajärvi 2009, s. 91)

Sisällönanalyysissä etsitään tekstin merkityksiä, joiden avulla pyritään luomaan tutkimusaineistosta teoreettinen kokonaisuus (Tuomi & Sarajärvi 2009, s. 104). Sisällönanalyysin analysointitapa tarkentui aineistolähtöiseksi analyysiksi. Aineistolähtöisessä analyysissä analyysiyksiköt valitaan litteroidun aineiston tarkoituksen ja tehtävän asettelun mukaisesti. Tärkein ajatus tässä on, että analyysiyksiköt eivät ole etukäteen harkittuja tai sovittuja. Aikaisemmin suoritetuilla teorioilla, havainnoilla ja tiedoilla tutkittavasta ilmiöstä ei tulisi olla vaikutusta lopputuloksen kanssa, koska analyysi on aineistolähtöistä. Tutkimukseen liittyvä teoria perustuu näin vain analyysin suorittamiseen. Analyysin suorittajan on sen vuoksi huomioitava, että haastateltavien lausumat ohjaavat analyysiä sekä tutkijan tehtävänä on pyrkiä ymmärtämään tutkittavien vastauksia heidän omasta näkökulmastaan analyysin kaikissa vaiheissa. (Tuomi & Sarajärvi 2009, s. 95, 113)

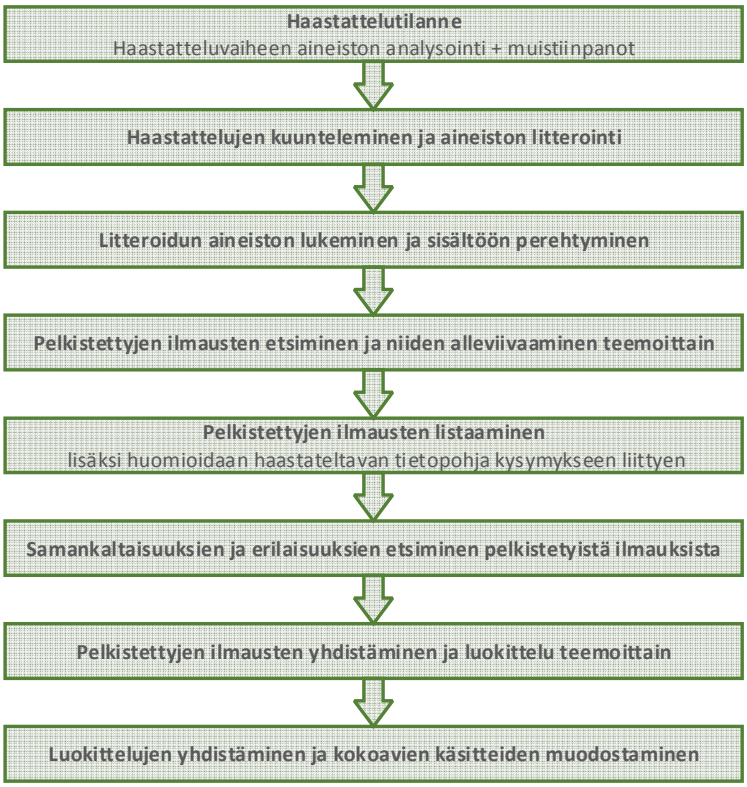
Aineistolähtöisessä sisällönanalyysissä teksti luokitellaan sen mukaan, mitä tutkimusaineistosta löydetään (Kananen 2017, s.141). Litteroidulle aineistolle suoritettiin aineistolähtöinen sisällönanalyysi, joka perustuu Tuomi & Sarajärvi (2009, s. 108 – 109) kirjassa esitettyyn menetelmään. Aineistolähtöinen analyysi voidaan heidän mukaansa jakaa kolmeen karkeaan kategoriaan; pelkistämiseen, ryhmittelyyn ja teoreettisen käsitteen luomiseen. (Tuomi & Sarajärvi 2009, s. 108)

Aineistolähtöisen sisällönanalyysin toteutettiin soveltaen Tuomi & Sarajärven (2009, s. 108 - 112) kirjassaan esittämän kolmen karkean kategorian mukaisesti:

Pelkistäminen: aineiston pelkistämisen yhteydessä litteroidusta aineistosta karsittiin tutkimuksen kannalta epäolennaiset tekstit pois ja tärkeimmät kohdat merkittiin värikoodein. Värikoodeilla merkityt ilmaukset listattiin ylös.

Ryhmittely: aineiston ryhmittelyssä tuotiin esille tutkimuksen kannalta merkittävät tiedot, joiden avulla muodostettiin tutkimuksen teoreettiset käsitteet. Pelkistämisen yhteydessä merkityt ilmaukset käytiin tarkasti läpi, jonka yhteydessä listauksista etsittiin samankaltaisuuksia ja eroavaisuuksia. Samalla tehtiin määrällistä sisällönanalyysiä, jotta voitiin arvioida oliko haastateltavien vastauksissa yhteneväisyyksiä tai eroja. Tärkeimmät käsitteet luokiteltiin siten, että löydettiin vastauksia esitettyihin teemoihin.

Teoreettisen käsitteen luominen: tehtyjen yläkäsitteiden avulla muodostettiin kuvaus tutkittavasta aiheesta. Ryhmitellystä aineistosta tehtiin tulkintoja ja päättelyitä, joiden yhteydessä saatiin näkemys tutkittavasta ilmiöstä.



Kuva 8. Aineistolähtöisen analyysin toteutus (Soveltaen Tuomi & Sarajärvi 2009, s. 108)

Kuvassa 8 on esitetty tarkempi aineistolähtöisen sisällönanalyysin eteneminen sekä sen eri vaiheet. Sisällönanalyysivaiheessa yhdistetään käsitteitä, jolloin saadaan vastaus tutkittavaan aiheeseen. Empiiristä aineistoa analysoimalla edetään siis kohti käsitteellisempää näkemystä tutkittavasta aiheesta ja ilmiöstä (Tuomi & Sarajärvi 2009, s.112). Sisällönanalyysin ryhmittelyvaiheessa tehtiin myös määrillistä sisällönanalyysiä, jotta voitiin arvioida miten yleisiä haastateltavien vastaukset olivat muiden haastateltavien vastauksien kanssa. Ilmiön tutkimisen kannalta ei ollut merkityksellistä tuoda esille kaikkien haastateltavien vastauksia, vaan pyrkiä yhdistelemään tärkeimmät käsitteet, jotka haastatteluissa tulivat esille.

4.4 Tutkimusten luotettavuus

Tutkimusta voidaan suorittaa monella eri tavalla. Tämän vuoksi on tärkeää arvioida tehdyn tutkimuksen luotettavuutta. Yleisesti tutkimuksen luotettavuutta arvioidessa puhutaan termeistä reliaabelius sekä validius. Reliaabelius tarkoittaa tutkimuksen mittaustulosten luotettavuutta, eli tutkimuksen tuloksena ei tule sattumanvaraisia tuloksia. Validius taas tarkoittaa tutkimusmenetelmän tai mittarin kykyä mitata juuri kyseistä asiaa. (Hirsjärvi et al 2010, s.231). Laadullisessa tutkimuksessa ei reliaabeliuden ja validiuden määritelmä välttämättä ole kovin relevantti, koska tutkijan on vaikeampaa päästä käsiksi objektiiviseen todellisuuteen ja totuuteen (Hirsjärvi & Hurme 2014, s.185).

Tässä työssä tutkimuksen luotettavuustarkastelu perustuu vahvistettavuuteen, arvioitavuuteen sekä saturatioon. Luotettavuustarkastelussa vahvistettavuudella tarkoitetaan aineistotriangulaatiota luotettavuuden lisääjänä. Eri lähteistä kerätyn tiedon avulla saadaan vahvistusta esitetyille väitteille (Kananen 2017, s.177 - 178). Tämän työn kirjallisuuskatsauksen avulla voidaan esittää vahvistusta tutkittavasta ilmiöstä. Samoja asioita on tullut esille myös suoritetun tutkimuksen tuloksissa. Toisena luotettavuustarkastelun perustana on arvioituvuus. Arvioituvuuden perustana on se, että tutkimuksen kaikissa vaiheissa aineiston keräämisestä aina johtopäätöksiin asti on pidetty tehdyistä toimenpiteistä riittävää dokumentaatiota. Hyvän dokumentaation avulla on mahdollista jäljittää tutkimusaineistosta tehdyt havainnot sekä niistä tehdyt arvioinnit. (Kananen 2017, s.178) Suurin osa tutkimusaineistosta ja aineiston analyysivaiheen ratkaisuista on sähköisessä muodossa ja ne on toteutettu loogisessa järjestyksessä. Kolmantena asiana,

jolla tutkimuksen luotettavuutta voidaan arvioida, on saturaatio eli kyllästäminen. Riittävän saturaation saavuttamiseksi tulee eri lähteistä kerättyjen tulosten toistua (Kananen 2017, s.179). Saturaatio voidaankin katsoa toteutuneen selkeästi tiettyjen kysymysten osalta. Haastateltavat antoivat samanlaisia vastauksia, vaikka he edustivat aivan eri toimialoja.

Tutkimuksen luotettavuuden arvioinnissa teemahaastatteluissa on kuitenkin huomioitava muutama asia, jotka voivat vaikuttaa tutkimustulosten luotettavuuteen. Ensinnäkin laadullisessa tutkimuksessa käytetyt käsitteet, tutkimusasetelmat sekä -menetelmät ovat tutkijan itsensä asettamia ja näin vaikuttavat aina tuloksiin. Tämän vuoksi onkin erityisen tärkeää muistaa, että analyysin suorittamisen tulee tapahtua aineiston haastateltavien ehdoilla eikä tutkijan ennakkoluulojen asettelemana. (Tuomi & Hirsjärvi 2009, s. 96). Toisena voidaan pitää sitä, onko haastattelija osannut vastata oikein esitettyihin kysymyksiin (Hirsjärvi et al 2010, s.232). Teemahaastattelu antoi kuitenkin hyvän mahdollisuuden tarkentaa kysymystä, jos haastateltava ymmärsi kysymyksen väärin tai vastasi ohi kysyttävän aiheen. Kolmantena luotettavuustekijänä on oikeiden haastateltavien valinta. On hyvin vaikeaa osoittaa varmasti, että juuri valitulla 14 henkilöllä on paras osaaminen ja tietopohja tutkittavan aiheeseen liittyen. Tätä luotettavuutta on parannettu lumipallo-otannalla sekä työn ohjaajan edustaman organisaation verkostoilla.

Tutkimuksessa käytetyn otoksen suuruus on 14 henkilöä, jota voidaan pitää pienehkönä otoksena. Laadullisessa tutkimuksessa tämä kuitenkin voidaan katsoa olevan riittävä määrä, koska tilastollisten yleistyksien sijasta on tarkoituksena tutkia ilmiötä tai löytää siitä uutta merkittävää tietoa (Hirsjärvi & Hurme 2014, s. 59). Haastateltavat edustivat useita eri toimialoja, jonka avulla saatiin riittävä kokonaiskuva tutkittavasta ilmiöstä. Kuten aikaisemmassa kappaleessa tuli esille, näiden seikkojen vuoksi voidaankin pitää kerättyä aineistoa riittävän laajana. Kokonaisuudessaan tutkimus on toteutettu laadullisen tutkimuksen ohjeistuksia noudattaen.

5 TUTKIMUSTULOKSET

Tässä luvussa esitetty tutkimusaineisto kerättiin teemahaastattelujen avulla, kuten edellisessä luvussa todettiin. Tutkimustuloksia ei esitetä täysin teemahaastattelun rungon mukaisessa järjestyksessä eikä kysymyskohtaisesti. Tämä johtuu siitä, että vastauksia esitettyihin teemoihin ja kysymyksiin pystyttiin sisällönanalyysin yhteydessä yhdistelemään. Suuremmaksi osaksi tutkimustulokset on esitetty kysymyskohtaisessa järjestyksessä. Kappaleiden sisällä voi olla alaotsikointia luettavuuden ja asian hahmottamisen parantamiseksi.

5.1 IoT – teknologian hyödyntäminen Suomen rakennuskannassa

Haastattelujen perusteella voidaan todeta, että IoT- teknologiaa on hyödynnetty Suomen rakennuskannassa. Kuitenkaan mitään vakiintunutta IoT:n hyödyntäminen ei vielä ole, vaikka teknologian puolesta esteitä sen käyttöön ei haastatteluissa tullut esille. Haastattelujen yhteydessä tuli esille paljon erilaisia järjestelmäintegraatioita ja anturitekniikkaa, joiden osalta ei voida puhua oikeastaan IoT-teknologiasta. Laitteen tai toimilaitteen langattomuus tai Internet-yhteys ei voida katsoa täyttävän vielä IoT:n lähtökohtia. Monessa tapauksessa voidaankin puhua älykkäistä järjestelmistä tai älykkäistä laitteista.

IoT:tä on hyödynnetty niin olemassa olevissa rakennuksissa kuin uudisrakentamisen yhteydessä. Hyödyntämistä on tapahtunut ennen kaikkea talotekniikan puolella. IoT mahdollistaa helpon tavan ohjata ja hallita talotekniikan eri osa-alueita etäyhteydellä internetin verkon yli. Yleensä tietoa kerätään langattomien antureiden avulla, jotka ovat yhdistetty erillisen gatewayn tai hubin kautta pilvipalveluun. Haastatteluissa tulivat esille rakennuksien etäluettavat sähkömittarit, jotka löytyvät jo melkein jokaisesta suomalaisesta rakennuksesta tai asuinhuoneistosta. Etäluettavat sähkömittarit voidaan katsoa IoT-laitteiksi, joten jokaisesta sähköverkkoon kytketystä rakennuksesta löytyy ainakin yksi IoT-ratkaisu.

IoT:tä hyödynnetään myös erilaisissa olosuhdemittauksissa, joista yleisimmät ovat lämpötilan, kosteuden, VOC ja CO^2 mittaukset. IoT:n hyödyntäminen on tullut osaksi myös veden virtauksen mittaamisessa sekä valaistuksen säätämisessä ja hallinnoinnissa. Lisäksi anturitekniikasta on tarpeen mainita liiketunnistimet sekä läsnäoloanturit, jotka

ovat tietyissä tapauksissa merkittävässä roolissa eri ohjauksien toteutuksessa. Eri antureista saatuja mittaustietoja hyödynnetään erilaisten ohjauksien toteutuksessa, joista yleisimpiä ovat ilmanvaihdon ja lämpötilan säädöt. Antureista kerättyä dataa hyödyntämällä ja järjestelmäintegraatioiden avulla saadaan rakennusten energiantehokkuutta parannettua sekä siten myös rakennuksen elinkaarikustannuksia pienennettyä.

Rakennustyypeistä yleisimmin IoT:tä hyödynnetään erilaisissa liike- ja toimistorakennuksissa. Asuinrakennuksissa IoT:n hyödyntäminen on paljon liike- ja toimistorakennuksia vähäisempää, mutta siitä saatavat hyödyt on tunnistettu varsinkin isoimpien vuokra-asuntoja omistavien kiinteistön omistajien toimesta. Toimistorakennuksien puolella on tällä hetkellä menossa pilottihankkeita, joissa IoT-teknologiaa hyödynnetään työntekijöiden sisätilapaikannuksessa sekä toimitilojen hallinnassa. Näiden tietojen perusteella saadaan tehostettua toimistotilojen käyttöä sekä kerättyä dataa voidaan hyödyntää tilojen suunnitteluun.

IoT:n käyttö paloturvallisuuden osa-alueella on vielä varsin vähäistä, huomattavasti vähäisempää kuin esimerkiksi muussa talotekniikassa. Suomessa IoT:tä on hyödynnetty automaattisissa paloilmoitinlaitteistoissa, kodin automaatiojärjestelmissä ja kodin turvajärjestelmissä. Automaattisien paloilmoitinlaitteistojen osalta on olemassa olevia järjestelmiä päivitetty IoT -aikaan. Määrät ovat laitevalmistajien mukaan vielä yksittäistapauksia. Kodin automaatio- tai turvajärjestelmissä IoT:n hyödyntäminen on paloilmoitinlaitteistoja huomattavasti yleisempää. Tosin haastattelujen perusteella ei saatu selvyyttä siitä, miten yleisiä nämä järjestelmät ovat. Kuitenkin markkinoilla on useita eri valmistajan laitteistoja, jotka on toteutettu IoT-ratkaisuna ja niitä löytyy jo suomalaiskodeistakin. Kodin automaatio- ja turvajärjestelmissä paloturvallisuus on vain yksi osa-alue. Esimerkiksi murtohälytysjärjestelmien liiketunnistimet, valvontakamerat ja muut anturit ovat paljon yleisempiä vastaavissa järjestelmissä.

5.2 Syyt IoT – ja älyteknologian vähäiselle hyödyntämiselle

Haastateltavilta kysyttiin onko IoT:n tuomat hyödyt riittävästi tiedostettu sekä miksi IoT- tai älyteknologiaa ei hyödynnetä jo laajasti uudis- ja korjausrakentamisessa. Vastaukset menivät paljolti ristiin näiden kahden kysymysten osalta. Näin ollen näitä kahta kysymystä käsitellään kokonaisuutena. Mainitsemisen arvoinen asia on, ettei kukaan

haastateltavista oikeastaan puhunut siitä, että uusi älyteknologia olisi kehityksen rajoitteena, vaan syyt löytyivät ihan muista asioista.

IoT- ja älyteknologian tuomien hyötyjen tunnistaminen ja tiedostaminen jakoi vastaajia. Kokonaisuutta ajatellen uuden teknologian tuomia hyötyjä ei ole riittävästi tunnistettu ja tiedostettu. Tämä koskee oikeastaan koko kenttää ja siihen liittyviä eri toimijoita. Kuitenkin Suomessa aiheeseen liittyen osaamista löytyy, joten siitä teknologian hyödyntäminen ei jää kiinni. Pitää vain löytää siihen perehtyneet osaajat. Rakennushankkeeseen ryhtyvien ja kiinteistön omistajien joukossa on myös asiantuntemusta aiheeseen liittyen. Nämä toimijat ovatkin hyödyntäneet uutta teknologiaa ja osaavat vaatia älykkäitä ratkaisuja jo esimerkiksi suunnitteluvaiheessa.

Haastattelujen yhteydessä korostui rakennusalan vanhakantaisuus. Osaltaan tämän vuoksi uuden teknologian tuominen rakennuksiin on hidasta. Rakennusalaa pidetään vanhakantaisena ja asioita halutaan tehdä edelleen perinteisillä tavoilla. Tämä ei koske jotain tiettyjä tahoja vaan koko rakennushankkeessa mukana olevia toimijoita aina tarvesuunnittelusta rakennuksen kunnossapitoon asti. Suunnittelutyötä saatetaan tehdä hyvässäkin hengessä, mutta viimeistään älylaitteiston tai -järjestelmän hankintavaiheessa vaihdetaan näkökantaa ja laitteisto tai järjestelmä jää hankkimatta. Yksi haastateltavista kiteytti asian seuraavasti.

”Rakentaminen ylipäätään perustuu vanhoihin, vanhakantaisiin menetelmiin ja siellä voin kerta kaikkiaan sanoa, että suurimalle osalle kaikki uudet asiat ovat myrkkyä.”

Haastattelujen perusteella esille nousi yhdeksän erilaista syytä siihen, miksi IoT- ja älyteknologiaa ei vielä hyödynnetä kovin laajasti olemassa olevissa rakennuksissa tai uudis- ja korjausrakentamisen yhteydessä. Nämä on esitelty alapuolella olevassa taulukossa. Lisäksi näitä syitä on avattu enemmän omissa kohdissaan.

- Rakennushankkeeseen ryhtyvän ja kiinteistön omistajien tietämättömyys
- Tarjotulla teknologiavaihtoehdolla ei ole referenssikohteita
- Laitevalmistajat eivät osaa esittää teknologialla saatavia hyötyjä riittävästi
- Uuteen teknologiaan liittyvä riskinotto
- Teknologiakustannukset
- Standardoinnin puute järjestelmien yhteensopivuudessa ja rajapinnoissa

- Voimassa oleva lainsäädäntö ei velvoita
- Suunnittelijoiden osaamisen taso
- Uuden teknologian käyttämisen pelko

Rakennushankkeeseen ryhtyvän ja kiinteistön omistajien tietämättömyys

Haastateltavista seitsemän mainitsi, että uuden teknologian hyödyntäminen johtuu paljolti rakennushankkeeseen ryhtyvien ja kiinteistön omistajien tietämättömyydestä. Tässäkin tosin pitää huomioida, että jotkut alan toimijat tietävät paljon uuden teknologian tuomista hyödyistä. Eniten tietämättömyyttä katsottiin kahden haastateltavan osalta olevan yksityisomistuksessa olevissa asunto-osakeyhtiöissä, jotka muodostavat Suomessa valtavan suuren kiinteistömassan. Useat suurten kiinteistömassojen omistajat, kuten vuokra-asuntoja omistavat tahot sekä kunnalliset ja valtiolliset toimijat, ovat sen sijaan huomanneet jo älyteknologiasta saatavat hyödyt esimerkiksi energiatehokkuuden näkökulmasta. Yleisenä katsauksena voidaankin todeta, että uuden teknologian hyödyntäminen rakennuksissa on paranemaan päin, kuten yksi haastateltava totesi.

"…varsinkin asiakkaiden puolelta tulee, että halutaan tehdä asioita eri tavalla ja paremmin kuin ennen. Se ei ole enää sillee, että tehkää meille se, minkä teitte aikaisemminkin."

Yksi haastateltavista totesi, etteivät tilaajat osaa tai uskalla vaatia uusinta teknologiaa. Osaajia Suomessa löytyy ja on olemassa valmiita ratkaisuja, joilla on jo useita referenssikohteita. Kuitenkaan ei ymmärretä miten teknologialla voidaan tehostaa toimintaa pitkällä tähtäimellä. Tietämättömyys koskee näin ollen myös IoT-laitteista kerätyn datan hyödyntämistä sekä sitä, mitä hyötyjä siitä voidaan saada tulevaisuudessa. Pitäisi olla etukäteen visio ja näkemys siitä miten tietoa kerätään eri laitteista ja antureista sekä miten kerätty dataa voidaan käyttää hyödyksi. Toisaalta kaikkea ei voi perustella tietämättömyydellä. Esimerkiksi rakennushankkeeseen ryhtyvän ollessa perustajaurakoitsija ei tällä välttämättä ole intressejä investoida teknologiaan, joka parantaisi rakennuksen paloturvallisuutta tai vähentäisi rakennuksen elinkaarikustannuksia.

"…osaamisen puute on ennen kaikkea siellä tilaajan päässä. Kyllä jos tilaajat lähtisivät rohkeasti vaatimaan, niin niitä aivan varmasti tulisi. Ei se jää siitä kiinni, etteikö niitä osattaisi tehdä"

"Tilaajalta pitäisi tulla se tahto, että tilaaja sanoo, että tässä huoneessa tarvitaan tällaista ja tällaista sensoria ja tätä ja tätä sen pitää tehdä. Niin silloin ne sinne laitetaan."

"Monet tahot kyllä tänä päivänä puhuvat paljon digitaalisuudesta ja sen käyttöönotosta, mutta hyvin harva ymmärtää mitä se tuo mukanaan ja missä sitä voidaan hyödyntää sekä kuka sitä hyödyntää."

"Sit varsinkin sellaisille ammattimaisille omistajille ja kiinteistösijoittajille, sinne pitäisi saada sitä tietoisuutta. Se on aika pieni investointi, millä voidaan saada sitä käytön mukavuutta ja käytön parantuvuutta ja toisaalta niin ku turvallisuustekijöitä ihan eri tasolle."

"...rakennusurakoitsija ei ole kiinnostunut elinkaaren aikaisista kustannuksista, muuta kuin pakon edessä."

Tarjotulla teknologiavaihtoehdolla ei ole referenssikohteita

Seitsemän haastateltavaa sanoi yhdeksi oleelliseksi syyksi IoT-teknologiaa hyödyntävien referenssikohteiden puuttumisen. Niiden kautta esimerkiksi laitevalmistajat voisivat markkinoida tuotteittaan paremmin. Ongelmana on kuitenkin saada uudelle teknologialle referenssikohteita, kuten yksi haastateltavista totesi.

"Isoissa hankkeissa ensimmäinen viesti yleensä on, että mitään uutta ei haluta kokeilla. Tää pitää olla olemassa olevaa tekniikkaa ja siitä pitää olla referenssi, se on melkein aina noin....se on tosi vaikeaa mitään uutta tuomaan….pitää olla jossain testattu ja sen jälkeen sen markkinoille voi saada."

Harva rakennushankkeeseen ryhtyvä tai kiinteistön omistaja on siis valmis olemaan kohde, jonne uutta teknologiaa asennetaan ensimmäistä kertaa. Tällä on myös vaikutusta siihen, etteivät laitevalmistajat ole kovin innokkaita kehittämään omia tuotteita, jos olemassa oleva laitekanta käy kaupaksi. Haastateltavien mukaan on merkittävää, että laitteistoja tai järjestelmiä hankkivat pääsevät katsomaan laitteiston toimintaa käytännössä sekä kuulemaan käyttökokemuksia uuden teknologian tuomista hyödyistä.

Laitevalmistajat eivät osaa esittää teknologialla saatavia hyötyjä riittävästi

Neljä haastateltavaa totesi, etteivät laitevalmistajat osaa tuoda esille riittävän tehokkaasti tuotteista saatuja hyötyjä. Helpoin tapa motivoida ostajaa on esittää uudesta teknologiasta saatu hyöty muuttamalla se euroiksi ja ennen kaikkea suhteuttaa se ostajan rakennukseen tai kiinteistömassaan. Kahden haastateltavan osalta tämäkään ei ole aina riittävä tapa ostajien motivoitiin vaan uudella teknologialla saatuja hyötyjä tulisi tuoda vieläkin tehokkaammin esille. Esimerkiksi viihtyvyyden paraneminen asunnossa tai työpaikalla voi saada aikaan paljon enemmän kiinnostusta uuteen teknologiaan kuin vain pelkkä suora euroiksi muutettu hyöty. Kuten yksi haastateltavista totesi, että työpaikalla 1 % viihtyvyyden lisäämisen parantavan tutkitusti työntekijöiden työntehokkuutta 4 %. Riittävien hyötyjen esittämättä jättäminen aiheuttaa sen, etteivät rakennushankkeeseen ryhtyvät tai kiinteistön omistajat kiinnostu valmistajan tarjoamista tuotteista. Tämä osaltaan heikentää uuden IoT- teknologian ja älytekniikan lisääntymistä rakennuskannassa. Seuraavassa yhden laitevalmistajan kommentti myynnin näkökulmasta:

”Kyllä siinä myyntimiehetkin voivat mennä itseensä. Jos sinä menet sinne ja myyt, et tiedätkö sä, tää on tosi hieno, tää on ehdottomasti paras. Ei se oikein mene läpi. Kyllä se täytyy pystyä osoittamaan se säästö…laittaa euroiksi se. ”

Uuteen teknologiaan liittyvä riskinotto

Haastateltavista viisi toi esille, että uuteen teknologiaan liittyy selkeä riskinotto, jota rakennushankkeeseen ryhtyvä tai kiinteistön omistaja ei halua ottaa panostamalla uusimpaan teknologiaan. Älyteknologian alalle on tullut paljon toimijoita, joista osa on uusia. Uskalletaanko hankkia teknologiaa uudelta yritykseltä, jonka kautta ei välttämättä muutaman vuoden päästä enää saada tukea hankitulle IoT- laitteelle, koska on olemassa jo uusi tuote tai yritys on mennyt konkurssiin? Voidaan pelätä myös, että jäädään yhden toimittajan loukkuun. Laitteistojen saatavuus, tuki ja huolto tulisi olla saatavilla riittävän pitkään, vaikka teknologia kehittyykin nopeasti. Alla yhden haastateltavan kommentti aiheeseen liittyen.

”Varmasti tuo riskin ottaminen, rakennuksen elinkaari 100 vuotta ja IoT- teknologian ehkä viisi vuotta. Miten sä sovitat sen siihen elinkaariajatteluun?”

Teknologiakustannukset

Haastateltavista viisi katsoi, että uuden teknologian käyttöönotto aiheuttaa liikaa kustannuksia tai siihen voi liittyä harmittavia lisäkustannuksia esimerkiksi ylläpitovaiheessa. Uudisrakentamisen yhteydessä uudet teknologiakustannukset ovat erityisessä tarkkailussa, vaikka perinteinen rakennusautomaatio ja talotekniikka maksavat myös. Ei pitäisi katsoa liikaa uuden älyteknologian aiheuttamiin hankintainvestointeihin, vaan katsoa siitä saatavia hyötyjä rakennuksen elinkaaren mukaan. Kun hyödynnetään uutta teknologiaa, voidaan miettiä tuoko investointi siihen meneviä kustannuksia koskaan takaisin. Teknologiassa takaisinmaksuaika on se, mikä yleensä ratkaisee. Seuraavassa yhden haastateltavan näkemys kustannusvaikutuksista.

"...juhlapuheissa ollaan käytön aikaisten kustannusten ystäviä, mutta kun tullaan rakennuspaikalle, niin mistä halvimmalla saadaan, niin sieltä otetaan. Ja siis voisi sanoa, että paloturvallisuus tulee valitettavasti jälkijunassa."

Jotta uusi älyteknologia lisääntyy, pitää löytyä riittävän edullisia ratkaisuja. Esimerkiksi asuinhuoneistoihin paloturvallisuutta parantavien äly- tai IoT-teknologiaa hyödyntävien laitteistojen hinta ei saa olla liian korkea, koska se tuo ensimmäisen rajoitteen niiden hankintaan ja hyödyntämiseen. Turvallisuustekniikan investoinnissa tulee miettiä muutakin kuin kustannuksia. Esimerkiksi turvallisuustekniikan etuna on se, että se toteuttaa turvallisuutta jatkuvasti, joka takaa ennakoivan toiminnan ja jatkuvuuden hallinnan. Yksi haastateltavista antoi yhden esimerkin miten paloturvallisuuteen investointiin voidaan pahimmassa tapauksessa suhtautua.

"…jos puhutaan turvallisuustekniikasta, niin voi olla, ettei sitä koskaan tarvita. Jos turvallisuuskulttuuri on hyvällä tasolla, niin sitten alat miettimään, miksi tähän on laitettu, miksi olen ostanut kalliit laitteet, jos täällä ei ole tulipaloa."

Voimassa oleva lainsäädäntö ei velvoita

Kaksi haastateltavaa nosti esiin lainsäädännöllisen näkökulman. Voimassa oleva lainsäädäntö ei edellytä tai ohjaa uuden älyteknologian hyödyntämistä, jonka vuoksi uusi teknologiakaan ei yleisty. Rakennushankkeeseen ryhtyvät kiinteistön omistajat tai niiden haltijat eivät katso tarpeelliseksi tehdä asioita enemmän kuin lainsäädäntö edellyt-

tää. On siis turhauttavaa tuoda markkinoille uutta teknologiaa, jos se ei kuitenkaan aiheuta kiinnostusta kuin yksittäisissä tapauksissa.

"Sehän se just on, että jos ne vaatimukset alkaa jollain tavalla muuttumaan, niin sitten se tuo kehitykselleki enemmän painetta muuttua."

Kyseiset haastateltavat arvioivat, että esimerkiksi pelastuslain vastuujaon muutoksilla voitaisiin tietyissä tapauksissa rakennuksien paloturvallisuutta parantaa, mikä kysynnän kasvaessa mahdollisesti toisi myös uuden älyteknologian markkinoille.

"Ei ole mitään lakia sen takana. Siinähän se on, että voidaan täällä Suomessa tehdä vaikka mitenkä hienoa…,mutta jos sille ei saada mitään laajempaa hyväksyntää, että me otettaisiin niitä tekniikoita käyttöön, mitkä ovat tietyllä tavalla lainsäädännön vaatimia."

Standardoinnin puute järjestelmien yhteensopivuudessa ja rajapinnoissa

Neljä haastateltavaa toi esille, että yksi syy varsinkin IoT:n hyödyntämiseen johtuu puuttuvista standardeista, joiden mukaan järjestelmäintegraatiot tulisi toteuttaa. Laitteiden välinen yhteentoimivuus katsottiin hyvin yleiseksi ongelmaksi, joka osaltaan vaikuttaa IoT:n hyödyntämisen esimerkiksi integroidessa vanhoja järjestelmiä uusiin. Tehdessä varsinkin vaativimpia yhteensovittamisprojekteja voivat teknologiasta saadut kustannushyödyt lopulta kadota. Lisäksi esille nousi, että IoT-antureiden osalta Suomessa markkinat ovat pitkälti pienten yritysten, varsinkin Start-up yritysten temmellyskenttää. Pienemmät yritykset tarjoavat edullisia antureita, jotka ovat käyttäjäystävällisiä, kun taas isoimmat talotekniikan laitevalmistajat valmistavat monesti kalliita IoT- antureita jotka toimivat vain heidän omassa ympäristössään. Tämä tuo omat rajoitteensa.

"Mitä enemmän joudutaan tekemään erillisiä räätälöintejä kuhunkin väleihin, se niin ku poistaa sitä ajatusta, että kuinka paljon lisähyötyä siitä voi saada."

"...tuntuu, että kaikki haluaa puuhastella sen analysoinnin ja sen visuaalisen esittämisen parissa, tai jonkin uuden ratkaisun sen tiedon pohjalta parissa, mutta harva haluaa pohdiskella ja työskennellä sen parissa, miten harmonisoitaisiin rajapintoja ja tietoa ja sen välittymistä."

Suunnittelijoiden osaamisen taso

Haastateltavista kuusi henkilöä katsoi suunnittelijoiden osaamisessa olevan puutteita uuden teknologian hyödyntämisessä, kun asiaa katsotaan kokonaisuutena. Suunnittelijoiden osaamisen tasoa tuotiin vahvasti esille. Osaltaan syynä pidettiin suunnittelu puolen vanhakantaisuutta. Yhtenä syynä arvioitiin, etteivät suunnittelijat perehdy riittävästi uuden teknologian tuomiin mahdollisuuksiin. Esille tuli, että suunnittelijat eivät ole riittävän oma-aloitteisia tai uskaliaita tarjoamalla uusinta teknologiaa, vaan tarjotaan tilaajalle perinteisiä ja omasta näkökulmasta turvallisia ratkaisuja. Teknologiasta saatuja hyötyjä ei esitetä tilaajalle yleensä tarpeeksi selvästi. Lisäksi yhden näkökulman mukaan uuden teknologian tarjoamisen rajoitteena pidettiin alalla olevaa kovaa kilpailua. Seuraavassa on esitetty haastateltavan näkökulmia aiheeseen liittyen.

”Sanoisin, että siellä suunnittelupuolella suurin haaste tulee olemaan, jos kenttä tulee muuttumaan.”

Uuden teknologian käyttämisen pelko

Kolme haastateltavaa toi esille, että uuden teknologian käyttöön liittyy ennakkoluuloja ja pelkoja. Voidaan luulla, ettei uutta laitteistoa tai järjestelmää hyödynnetä tarpeeksi. Haastatteluissa tuli esille varsinkin rakennuksen ylläpidon aikainen toiminta. Kiinteistönhuollon henkilöstö tai isännöitsijät eivät ole välttämättä tottuneet käyttämään teknisiä laitteistoja. Tämän vuoksi pidettiinkin laitteistojen ja järjestelmien käyttäjälähtöisyyttä hyvin tärkeänä asiana. Käyttöliittymien tulisi olla hyvin helppokäyttöisiä ja selkeitä. Lisäksi järjestelmien tulee olla varmatoimisia, etteivät ne työllistä ylläpitovaiheessa.

”…ja mitenkä ylläpidon näkökulmasta sille huoltomiehelle, jos sille on vaikeuksia hallita olemassa olevaa tekniikkaa niin ku ylläpitää ja käyttää, niin sitten tulee nämä IoT-laitteet, onko se vielä enemmän sekaisin. ”

”Et paljon on puhutaan siitä, että ei niitä voi pystyä käyttää, kukaan ei pysty hyödyntämään niitä tekniikoita, et siis vikaherkkyys ja käyttäjälähtöisyys, ne on ne asiat joihin pitäisi panostaa. ”

5.3 IoT-teknologian lisääntyminen palo- ja henkilöturvallisuuslaitteistoissa

Haasteltavilta kysyttiin tuleeko IoT- ja älyteknologia lisääntymään merkittävästi henkilö- ja paloturvallisuuslaitteistoissa. Mielipiteitä pyydettiin siihen, miten tilanne muuttuu vuoteen 2025 mennessä. Kaikkien haastateltavien mielestä IoT- ja älyteknologia tulee lisääntymään henkilö- ja paloturvallisuuslaitteistoissa tulevaisuudessa tavalla tai toisella. Miten paljon teknologia tulee lisääntymään ja missä laitteistoissa, ei juuri osattu sanoa. IoT-teknologian lisääntymisen osalta tuotiin haastattelujen yhteydessä esiin markkinatutkimuslaitosten ja muiden tekemiä visioita sekä näkemyksiä teknologian kasvusta. Nähtiinkin, että lisääntymistä tulee tapahtumaan jokaisella toimialalla, jopa paloturvallisuuden osa-alueella. Kehityksen katsottiin olevan selkeää jatkuvuutta talotekniikan ja kiinteistöautomaation IoT- ja älyteknologian lisääntymiseen sekä sen todettiin olevan yleisesti hyvin positiivista. Lisääntymisen edellytyksenä haastateltavista neljän mielestä tilaajien ja rakennushankkeeseen ryhtyvien tulisi nähdä konkreettisia esimerkkejä uuden teknologian asennuksista ja niiden tuomista hyödyistä, jotta teknologian lisääntymistä varsinkin merkittävästi tulisi tapahtumaan. Kuitenkin henkilö- ja paloturvallisuuslaitteistojen osalta katsottiin, etteivät ne ole sellaisia, joissa teknologia tulee merkittävästi lisääntymään, koska siihen liittyy esimerkiksi laitteiden standardointiin ja lainsäädännön tuomia velvoitteita. Lisäksi tietoturvan ja tietosuojan tuomat seikat olivat haasteltavien mielestä haasteellisia. Seuraavassa neljän haastateltavan näkemyksiä IoT- ja älyteknologian lisääntymiseen henkilö- ja paloturvallisuuslaitteistoissa.

"…säädeltävyyden takia paljon hitaampaa se kehitys muuten kuin muulla sellaisella, jossa voi tuoda vapaammin noita IoT-laitteita ja antureita ja siihen liittyviä kaikenlaisia applikaatioita."

"...kyllä minä uskon, että se lisääntyy, mutta siinä on nämä lainsäädännön ja standardien pullonkaulat, että se ei ole ehkä kovin nopeaa ja voimakasta."

"Tulee, jos meidän viranomaisten vaatimustaso nousee ainakin niin ku paloturvallisuuslaitteistojen puolella. ...jos ei nouse, niin mennään paristovehkeillä vielä 2025."

"..ku jollain lailla ratkaistaan tietoturva ja tietosuoja, niin varmasti tulee lisääntymään, kaikkiin näihin ongelmiin liittyen."

5.4 Palo- ja henkilöturvallisuuden parantaminen IoT-teknologiaa hyödyntämällä

Haastateltavista 11 henkilön mielestä IoT- teknologian integraatioilla voidaan parantaa rakennuksien henkilö- ja paloturvallisuutta. Loput kolme haastateltavaa eivät osanneet sanoa suoraa kantaa kysymykseen, mutta totesivat sen olevan mahdollista. Kukaan haastateltavista ei pitänyt IoT- teknologiaa turhana tai sopimattomana parantamaan rakennuksien palo- ja henkilöturvallisuutta. Yhden haastateltavan mukaan IoT:n hyödyntäminen paloturvallisuudessa on haasteellista, koska esimerkiksi paloturvallisuutta parantavat laitteistot ovat niin vahvasti standardoitu.

Haastateltavat kertoivat haastattelujen yhteydessä omia näkemyksiään siitä, millä tavalla IoT:llä voidaan parantaa rakennuksien henkilö- ja paloturvallisuutta. Seuraavassa yhteenveto näkemyksistä sekä lisäksi tarkempia näkemyksiä mitkä ovat IoT- teknologian mahdolliset vahvuudet:

- Toimintavarmuuden parantaminen
- Talotekniikan olosuhdeanturoinnin hyödyntäminen
- Onnettomuuksien ehkäiseminen
- Pelastusviranomaiselle reaaliaikaisen tilannekuvan välittäminen

Toimintavarmuuden parantaminen

Toimintavarmuuden paraneminen tuli haastatteluissa esille kahden kysymyksen kohdalla. Ensimmäinen liittyi siihen, voidaanko IoT-teknologialla parantaa rakennuksien palo- ja henkilöturvallisuutta sekä toinen kysymys millä tavoin uudella älytekniikalla saadaan paloturvallisuuslaitteistoihin lisää toimintavarmuutta. Ensimmäinen kysymys esitettiin kaikille haastateltaville ja jälkimmäinen kysymys kymmenelle haastateltavalle.

Haastateltavista viisi toi esille, että IoT- teknologiasta voidaan saada ennen kaikkea hyötyä paloturvallisuutta parantavien laitteistojen toimintavarmuuden paranemisessa. IoT- ja älyteknologiaa hyödyntämällä voidaan toimintavarmuutta saada parannettua, kun järjestelmiä voidaan monitoroida paljon paremmin ja tehokkaammin kuin ennen. Laitteistojen etävalvonta alkaa yleistyä entisestään, minkä vuoksi laitteistojen tilaa voidaan seurata tehokkaammin etäyhteydellä Internet-verkon yli. Järjestelmän tila saadaan näin helposti tarkastettua. Paloturvallisuutta parantavien laitteistojen toimintavarmuus

voi parantua myös kun lisätään älykästä anturointia tai tuodaan laitteistoihin enemmän älyä, jolloin antureista saadaan helpommin erilaista tietoa. Tämän tiedon avulla voidaan kohdentaa huoltoon ja kunnossapitoon liittyviä asioita. Laitteistoja voidaan näin ollen huoltaa etukäteen, eikä yllättäviä vikaantumisia turvalaitteisiin pääse syntymään. Toisin sanoen turvalaitteistoja voidaan huoltaa asianmukaisemmin jatkossa sekä suoritetuista huoltotöistä jää selkeät merkinnät järjestelmiin.

Älykkyyttä lisäämällä laitteistot voivat tunnistaa niihin tulevat vikaantumiset nykyistä tehokkaammin, kun laitteistot ja järjestelmät osaavat valvoa itseään huomattavasti paremmin. Turvalaite tai koko järjestelmä voidaan ohjelmoida siten, että se testaa itsensä tietyn väliajoin, mikä taas lisää laitteiston toimintavarmuutta. Älykkyyden ansioista voidaan myös esimerkiksi paloturvallisuutta parantavien laitteistojen kohdistuvan inhimillisen tekijän mahdollisuutta pienentää. Anturointia lisäämällä on mahdollista huomata tehokkaammin ihmisen tekemät unohdukset tai virheelliset toiminnot. Haastateltavista kolme henkilöä toi esille huolenaiheensa paloturvallisuutta parantavien laitteistojen huollon ja kunnossapidon laadusta. Paloturvallisuutta parantavien laitteistojen kunnossapito on hyvinkin vaihtelevaa, mihin tulisi erityisesti kiinnittää huomioita. Riittävällä kunnossapidolla saadaan varmistettua laitteiston toimintavarmuus sen elinkaaren aikana. Uudella teknologialla voidaan parantaa rakennuksen ylläpidon aikaista toimintaa, kuten yksi haastateltavista totesi.

“IoT- ratkaisuilla pystyä käytönaikainen kunnossapito toteuttaa sillä tavoin, että kaikki nämä turvajärjestelmät liittyvät laitteet ovat toimintakuntoisia. Nyt ei välttämättä ole ja ennen kaikkea tähän toimintavarmuuteen pitäisi kiinnittää enemmän huomioita.”

Toimintavarmuuden parantamiseen liittyen kaksi haastateltavaa toi esiin sen, että lisäämällä älytekniikkaa paloturvallisuutta parantaviin laitteistoihin, saadaan hallittua järjestelmiä paljon kokonaisvaltaisemmin. Tämä edellyttää, että tiettyjä toimenpiteitä tulee ryhtyä tekemään yhä enemmän tiettyjen prosessien mukaisesti. Tämä tulee lisäämään toimintavarmuutta niin käyttöönoton kuin ylläpidon aikana. Lisäksi laitteistoihin ja järjestelmiin suoritetut toimenpiteet/korjaukset kirjautuvat yhteiseen järjestelmään. Kokonaisuuden hallinta korostuu ennen kaikkea suurissa järjestelmäintegraatioissa. Seuraavassa yhden haastateltavan näkemys asiaan.

"Kokonaisuuden hallitseminen, että ne osa-alueet toimivat sen ajatuksen mukaisesti, se on tuossa teknologiassa mahdollista toteuttaa ja sitten visualisoida se."

Talotekniikan olosuhdeanturoinnin ja muun anturoinnin hyödyntäminen

IoT- anturointia on lisätty rakennusten eri tilojen olosuhteiden mittaamiseen. Näistä antureista voidaan saada monenlaista dataa, jota pystyttäisiin hyödyntämään myös palon havaitsemiseen. Kerätyn informaation avulla voitaisiin saada paremmin tietoa, mitä rakennuksessa oikein tapahtuu myös henkilö- ja paloturvallisuuden näkökulmasta. Haastateltavista kuusi henkilöä toi jollain tavalla esille sen, että talotekniikkaan liitettyä anturointia tai muuta anturointia olisi hyödyllistä käyttää myös palon havaitsemiseen tai henkilöturvallisuuden parantamiseen. Varsinkin lämpötilan ja CO^2- mittauksien tuloksia voisi hyödyntää palon havaitsemisessa. Mittaustulosten avulla voitaisiin varmentaa esimerkiksi olemassa olevaa paloilmoitinlaitteiston toimintaa. Sisäpaikannusjärjestelmistä saatavien tietojen avulla olisi mahdollista varmistua siitä, että rakennuksessa oleskelevat ihmiset ovat poistuneet rakennuksesta tai ohjata heitä poistumaan turvallisinta reittiä ulos. Mielipiteitä oli myös toisin päin eli paloturvallisuutta parantavien laitteistojen olosuhteisiin liitettyä tietoa voisi hyödyntää myös muussa talotekniikassa.

Automaattisista paloilmoitinlaitteistoista ja sammutuslaitteistoista tulevat erheelliset palohälytykset ovat suuri ongelma niin Suomessa kuin muissakin Pohjoismaissa. Lisäämällä anturointia voidaan erheellinen palohälytys tunnistaa helpommin, joka taas luonnollisesti vähentää niiden määrää. Olosuhteiden tunnistamisessa voidaan hyödyntää antureiden lisäksi esimerkiksi kameravalvontaa, jonka avulla varmuus palohälytyksen oikeellisuudesta voidaan varmistaa.

Haastattelujen yhteydessä haastateltavista kaksi nosti esille, että anturoinnin lisääminen olisi tarpeen esimerkiksi automaattisen paloilmoitinlaitteiston paloilmaisimiin. Vaihtoehtoisesti olemassa olevista paloilmaisimista kerättyä dataa olisi hyvä hyödyntää kiinteistöautomaatiossa ja sen ohjauksissa. Tästä hyötynä olisi se, ettei tilaan tarvitsisi tuoda useaa eri anturia, vaan kaikki tarvittava anturointi olisi yhdessä samassa laitteessa. Anturoinnin ja laitteistojen integraatioista on puhuttu jo yli kymmenen vuoden ajan.

Kolmen haastateltavan näkemyksen mukaan laajempaa anturointia voidaan tuoda myös passiivisiin palontorjuntalaitteisiin kuten palo-oviin. Olemassa on jo langattomia antureita, joista voidaan saada tilatietoa onko ovi kiinni vai auki. Tulipalotilanteessa saataisiin helposti varmuus siitä, että palo-ovet ovet sulkeutuneet. Palo-oviin asennettavan anturoinnin avulla voitaisiin seurata ihmisten käyttäytymistä siitä, miten usein palo-ovet on esimerkiksi kiilattu auki, kuten yksi haasteltavista totesi.

"Yhtä lailla tässä paloturvallisuudessa, tarkempaa ja laajempaa sensorointia, siitä että palo-ovet menevätkö ne oikeasti kiinni, aina jos joku blokkaa ne auki….siitä kertyisi lokia. Pystytään pääsemään niin ku inhimillisen toiminnan jäljille siitä, että pitäisikö kouluttaa vähän paremmin ja muuttaa asenteita niiden henkilöiden."

Onnettomuuksien ehkäiseminen

Haastateltavista kolme katsoi IoT-teknologian integraatioiden mahdollisuuden olevan onnettomuuksien ehkäisemisessä. Rakennuksen tiloissa olosuhteiden muuttumisen perusteella järjestelmien integraatioilla voidaan tehdä erilaisia toimintoja. Yhtenä esimerkkinä tuotiin esille sähkövirran pois kytkeminen sähkölaitteista palohälytyksen yhteydessä. Etäkäytön avulla on mahdollisuus tarkastaa tiettyjen laitteistojen tilatietoja sekä sulkea ne etähallinnalla Internet-verkon yli, jos on jäänyt askarruttamaan, onko jokin sähkölaite jäänyt päälle. Yksi haastateltavista toi esille myös muut asumisturvallisuuteen liittyvät onnettomuudet. Anturi- ja kameravalvonnan avulla on mahdollista esimekiksi arvioida piha-alueen liukkautta sekä tarvittaessa tehdä automaattisia varoituksia siitä asukkaille sekä kiinteistönhuoltoon liukkauden torjumiseksi.

Järjestelmäintegraatioiden avulla voidaan rakennuksen asukkaille tai siellä oleskeleville välittää helpommin tietoa alkaneesta tulipalosta tai muusta vaaratilanteesta. Tietoa tapahtumista on mahdollista välittää henkilön älypuhelimeen tai näyttötauluihin. Järjestelmien integraatioiden avulla voidaan helposti näyttää parhaimmat poistumisreitit ja lähimmät uloskäytävät rakennuksen tai pohjakuvan 3D-kuvassa, joka lisää evakuoinnin nopeutta.

Haastattelujen yhteydessä neljä haastateltavaa toi esiin, että IoT- ja älyteknologialla voidaan parantaa kotona asumisen turvallisuutta. Turvallisuus ei aina parane pelkästään paloturvallisuuden näkökulmasta, vaan uudella teknologialla voidaan saada aikaan lisää

turvallisuuden tuntua esimerkiksi ikääntyneille tai liikuntarajoitteisille ihmisille. Kotona tapahtuneita onnettomuuksia voidaan rajoittaa tai mahdolliset onnettomuudet voidaan havaita mahdollisimman aikaisessa vaiheessa siten, että tieto onnettomuudesta tai sen uhasta saadaan asukkaan ja muiden tarvittavien tahojen tietoon nopeammin.

Pelastusviranomaiselle reaaliaikaisen tilannekuvan välittäminen

Viiden haastateltavan näkemyksen mukaan rakennuksien IoT- teknologian integraatioista hyötyvät myös pelastusviranomaiset. Rakennuksien älykkäistä järjestelmistä on mahdollista IoT- teknologian avulla välittää reaaliaikaista tilannekuvaa alueen pelastusviranomaiselle. Eri antureista saatavan tiedon perusteella saadaan selville mitä rakennuksessa tapahtuu. Reaaliaikainen tilannekuva helpottaa pelastustoiminnan johtamista, koska sitä voisi hyödyntää heti alusta lähtien päätöksenteon tukena. Pelastusviranomainen voisi saada tietoja esimerkiksi; onko rakennuksen sisällä liikettä, ovatko rakennuksessa oleskelleet ihmiset poistuneet rakennuksesta, ovatko palo-ovet sulkeutuneet sekä miten tulipalo kehittyy. Järjestelmien integraatioiden helpottuessa useista eri toiminnoista voitaisiin saada hyödyllistä tietoa. Tämä tieto voitaisiin esittää esimerkiksi rakennuksen 3D-kuvassa tai digitaalisessa kaksosessa. Haastateltavista kaksi toi esiin muutamia ongelmia, jotka tulisi ehdottomasti ratkaista. Toinen on järjestelmien helppokäyttöisyys. Pelastusviranomaisen käyttämien sovellusten ja käyttöliittymien tulee olla helppokäyttöisiä ja niihin tuleva tieto olla helposti hyödynnettävissä ja ymmärrettävissä. Toinen asia koskee sovellusten standardointia. Pelastusviranomaisen käytössä olevien sovellusten tulisi olla standardoituja, koska jokaiselle eri järjestelmälle ei voi olla omaa sovellusta tai erilaista käyttöliittymää, kuten yksi haastateltavista totesi.

“Tämä ala vaatisi jonkun verran standardointia, koska nythän kaikki jossain määrin kehittelee omia juttujaan. Ei pelastusviranomaisella voi olla lopulta 25 eri laitevalmistajan tablettisovellusta paloautossa mukana...sen pitäisi jollain tasolla standardoitu.”

5.5 IoT – laitteista kerättävän datan hyödyntäminen

5.5.1 Datan kerääminen ja jakaminen

IoT-laitteista tai -antureista kerätyn datan jakaminen oli haastateltavien mielestä pitkälti sopimustekninen asia. Datan jakaminen useille eri toimijoille on mahdollista, mutta sen tarve tulee aina tarkkaan miettiä ja määritellä. Toimijoiden tiedon tarvekin vaihtelee. Jotkut voivat tarvita vain lyhyen yhteenvedon kerätystä datasta, kun taas toinen voi edellyttää reaaliaikaisen datan saamista. Kolmasosa haastateltavista piti erityisen tärkeänä huomioida datan keräämisessä tietosuojaan liittyvät asiat. Dataa kerättäessä varsinkin asumisympäristöstä on kiinnitettävä huomioita yksityisyyden suojaan. Toiminnan pitää ehdottomasti olla voimassa olevan lainsäädännön mukaista. Kerättyä dataa tulee hyödyntää vain niiden toimijoiden, jotka tietoa todella tarvitsevat. Tällä tavoin pystytään ennakoimaan/ennaltaehkäisemään dataan liittyviä väärinkäytöksiä. Kerättävän datan osalta on siis tarvetta etukäteen miettiä, mitä dataa on tarvetta kerätä, kenelle sitä jaetaan sekä kenen sitä tarvitsee hyödyntää. On kuitenkin muistettava, että datan keräämisestä ja jakamisesta saadaan hyötyä vain siinä tapauksessa, että eri toimijoilla on käytössä heidän tarpeitaan vastaavat/heille sopivat sovellukset tai käyttöliittymät.

Tällä hetkellä dataa kerätään talotekniikan eri osa-alueilta, etupäässä ylläpito-organisaatiolle ja sen johtamisen tueksi. Rakennuksien talotekniikkaa on jo useita vuosia voitu etäkäyttää sekä suorittaa laitteistojen etäseurantaa. Etäseurantapalveluiden avulla on voitu varmistua, että rakennusta käytetään asiallisesti. Etäseurantaa on ollut mahdollista tehdä myös paloilmoitinlaitteistoissa, joissa irtikytkentöjä on voitu tehdä Internet-verkon yli. Kuitenkin datan kerääminen on haastateltavien mukaan vielä aika alkutekijöissään, mutta kovaa vauhtia kasvussa. Talotekniikasta ja rakennusautomaatioista kerätty data kerätään/tallennetaan/kootaan pilvipalveluihin, josta se on hyödynnettävissä tarpeen mukaan. IoT-ratkaisut ovat olleet suurelta osin tila-olosuhteiden hallintaa, jossa eri tilojen olosuhteita seurataan sekä jonkin verran on toteutettuna myös laitteistojen ohjauksia.

Datan jakamisen osalta haastateltavista yhtä lukuun ottamatta kaikki toivat esille, että kiinteistön turvallisuuteen liittyvistä IoT-laitteista ja -antureista olisi tarpeellista jakaa

dataa varsinkin kiinteistön ylläpidosta vastaaville henkilöille, kuten isännöitsijöille ja kiinteistönhuollosta vastaaville. Toisen suuren osa-alueen muodostavat huoltoliikkeet. Erityisesti olisi tarpeen jakaa tietoa varsinkin paloturvallisuutta parantavista laitteistoista vastaaville huoltoliikkeille, joiden kanssa kiinteistöllä on sopimukset kunnossapidon toteutuksesta. Datan jakaminen toimijoiden välillä parantaa heidän välistään kommunikointia. Uusissa IoT- ratkaisuissa tähän on pyritty varsinkin automaattisten paloilmoitinlaitteistojen huoltoliikkeiden ja kiinteistön omistajien edustajien välillä.

Pientalokiinteistöjen omistajilla ja asuinhuoneistojen asukkailla on myös luonnollisesti tarve ja oikeus saada itselleen dataa, joka on kerätty IoT- laitteista. Usein suurin hyöty datan keräämisestä ja jakamisesta tulee juuri heille. Asukkailla on myös tietyissä tapauksissa oikeus kieltää datan kerääminen asuintiloistaan. Tämän vuoksi onkin erityisen tärkeää sopia eri asukkaiden kanssa, mitä dataa kerätään, ketkä sitä hyödyntävät ja mihin tarkoitukseen sitä ylipäätään kerätään.

Haastateltavista kahdeksan mainitsi, että dataa henkilö- ja paloturvallisuuslaitteistoista olisi tarpeen jakaa myös alueen pelastusviranomaiselle erityisesti niissä tapauksissa, joissa pelastuslaitos on hälytettynä kohteeseen. Tietyissä tapauksissa datan jakaminen olisi myös tarpeellista onnettomuuksien ehkäisytoimintaa, jota voitaisiin hyödyntää niin valvontatoiminnassa kuin pelastuslaitoksen riittävän valmiuden määrittelyssä.

Haastateltavista kuusi mainitsi haastattelujen yhteydessä, että IoT-laitteistojen valmistajat keräävät dataa omista laitteistaan tai että heidän olisi syytä kerätä dataa esimerkiksi tuote- ja palvelukehitystä varten. Kuitenkin usea haasteltava ihmetteli käytännössä, miten vähän valmistajat keräävät dataa, vaikka heillä olisi siihen mahdollisuus. Yksi haastateltavista totesi seuraavasti.

“Laitevalmistajat keräävät mielestäni aika vähän dataa, en tiedä yhtään laitevalmistajaa, joka niin ku määrätietoisesti keräisi dataa omista laitteistaan.”

5.5.2 Datan jalostamisessa ja rikastamisesta saatavat hyödyt

Datan keräämisessä ja sen hyödyntämisessä nähtiin olevan merkityksellistä potentiaalia. Kaikki haastateltavat antoivat jonkinlaisia näkemyksiä datan keräämiseen ja sen hyödyntämiseen liittyen. Esille nousi, että talotekniikasta ja paloturvallisuutta parantavissa

laitteistoissa olisi tarve alkaa keräämään dataa mahdollisimman nopealla aikataululla, vaikka perimmäistä syytä sen tarpeelle ei olisikaan olemassa/vielä tiedossa. Tulevaisuudessa kehittyneellä analytiikalla voidaan datasta saada rikastettua tärkeääkin informaatiota, joka voisi tarjota aivan uutta tietoa, osaamista tai aivan uusia liiketoimintamahdollisuuksia. Seuraavassa on esitetty haastateltavien kommentteja aiheeseen liittyen.

"Mitä enemmän me saadaan tietoa, että meillä on kaikkia uusia algoritmeja, ja tekoäly tulee, niin sitä enemmän me pystytään ihan uusi korrelaatioita löytämään, mitä aikaisemmin me ei ole pystytty tekemään, kun me ei olla yhdistetty niitä tietoja."

"…me ei voida tietää, että mitä tietoa me voitaisiin kaivata viiden vuoden päästä."

"…jos yhdistetään tietoa eri laitteista, niin sehän voi tuoda uutta osaamista siihen, miten niin ku kannattaa optimoida."

"Kyllä siis, ja siihen olen ihan niin ku sitä mieltä, että kaikkea dataa mitä kerätään pitäisi käyttää hyödyksi. Ja nimenomaan vastuullisuuden ja turvallisuuden parantamiseksi."

Haastatellut kiinteistöjen omistajien edustajat toivat esiin yhteistyön merkityksen kiinteistön omistajien ja tilojen käyttäjien välillä kerätyn datan hyödyntämisessä. Kerättyä dataa tulee jakaa eri toimijoiden kesken. Rakennuksissa olevien tietojärjestelmien alustojen tulisi olla sellaisia, että niistä voisi hyötyä mahdollisimman moni rakennuksen toimija ja ne taipuisivat tarvittaessa myös käyttäjän tarpeiden mukaan. Tämä mahdollistaisi paremman palvelun tarjoamisen tilojen käyttäjille, eikä rakennuksessa olisi monia IoT-alustoille rakennettuja järjestelmiä. Lisäksi tarvittavan kerätyn datan siirtäminen kiinteistöjen sähköiseen huoltokirjaan nähtiin tarpeelliseksi. Sähköisessä huoltokirjassa data saataisiin koottua helposti yhteen paikkaan sekä hyödynnettyä tehokkaammin.

Datan jalostamisen ja rikastamisen osalta saatavista hyödyistä nousi yleisimmin esille palo- ja henkilöturvallisuuteen liittyvien laitteistojen ennakoiva huolto. Haastateltavista seitsemän näki ennakoivan huoltotoiminnan olevan sellaista, jossa IoT- teknologialla kerättyä dataa voidaan erityisesti hyödyntää. Ennakoivan huollon avulla varmistetaan, etteivät laitteistot pääse vikaantumaan yllättäen. Älykkäiden järjestelmien avulla saadaan laitteiston vikaantuminen nopeasti tarvittavien toimijoiden tietoon hyvissä ajoin. Tämä toki lisää rakennuksien turvallisuutta, mutta ennen kaikkea voi tuoda kustannus-

säästöjä huoltotoimintaan. Paloturvallisuutta parantavien laitteistojen etähallinnointi mahdollistaa, ettei järjestelmiä tarvitse huoltaa enää perinteisellä tavalla, jolloin kiireelliset korjaustoimenpiteet vähentyvät. Kiinteistön omistajan ja huoltoliikkeen välinen kommunikaatio paranee, joten varsinkin paloturvallisuutta parantavia laitteistoja huoltavat sopimusliikkeet voivat tahdittaa ja suunnitella tarvittavia huoltotoimenpiteitä paljon tehokkaammin. Lisäksi kustannuksia saadaan vähennettyä, kun huoltokohteessa tarvitsee käydä vain tarpeen mukaan ja näin turha ajaminen kiinteistöjen välillä jää vähemmälle. Näin on mahdollista tarjota myös nopeampaa ja parempaa palvelua. Alla kahden haastateltavan toteamuksia aiheeseen liittyen.

"Sen pitäisi parantaa sen huoltoliikkeen bisnestä, tuota ne pystyy paremmin suunnittelemaan oman työnsä, kun ei tule äkkilähtöjä samalla tavalla. Voi vaikka viikon työt ohjelmoida sen mukaan, mitä nää älykkäät järjestelmät ovat ilmoitelleet. Ei tarvitse odotella, että vika pamahtaa päälle."

"Turvallisuus syntyy nimenomaan, ennakoivan huollon, ennakoivan toiminnan, huollon ja kunnossapidon kautta."

Laitteiden valmistajien intressi hyödyntää kerättyä dataa tuli esille kuuden haastattelun yhteydessä. Kuten haastatteluissa tuli ilmi, ei datan kerääminen laitevalmistajien toimesta ole kovin yleistä. Näin ollen sen hyödyntäminenkin on melko vähäistä. Kuitenkin laitevalmistajat voisivat hyödyntää ja rikastaa kerättyä dataa omassa tuote- ja palvelukehityksessään. Datan rikastamisen avulla voitaisiin esimerkiksi kehittää olemassa olevia tuotteita ympäristöihin sopivimmiksi tai laadukkaamman palvelun kehittämiseksi. Haastateltujen laitevalmistajien edustajien mukaan he hyödyntävät keräämäänsä dataa etupäässä palvelutoiminnan kehittämiseen, ei niinkään tuotekehityksen tarpeisiin. Tavoitteena on järkiperäistää toimintoja siten, että ne palvelevat itse yritystä, asiakkaita ja partnereita. Palvelua on rakennettu olemassa olevien tekniikoiden ja ratkaisujen päälle. Paloturvallisuutta parantavista laitteistoista datan kerääminen ja sen hyödyntäminen olisi tarpeen huomioida erityisesti myös toimintavarmuuden näkökulmasta. Tarkastellessa paloturvallisuuden kannalta hyvin kriittisiä kohteita, tulee myös paloturvallisuutta parantavien laitteiden toimintavarmuuden ja jatkuvuuden todennäköisyydet ottaa huomioon kohteen riskiarvioissa. Yhden haastateltavan mukaan näistä ei ole olemassa kun-

nolla tietoa. Datan kerääminen olisi yksi vaihtoehto asian ratkaisemiseksi, kuten yksi haastateltavista toi asian esille.

”...ensinnäkin laitevalmistajilla pitäisi olla vikaantumiskriteerit, frekvenssit tiedossa, että missä ajassa joku osa vikaantuu. Meillä ei rakentamisessa ole mitään tällaista todennäköisyyteen pohjautuvaa tarkastelua, me ollaan se unohdettu aktiivisesti.”

Haastateltavista seitsemän toi haastattelujen yhteydessä esille sen, että pelastusviranomaiset voisivat hyödyntää paloilmoituskohteen IoT-antureista ja -laitteista kerättyä dataa paremman tilannekuvan aikaansaamiseksi. Tämä nopeuttaisi ja helpottaisi pelastuslaitoksen toimenpiteitä onnettomuustilanteessa. Esille nousi 2000-luvulla käynnissä ollut PARK-hanke, jonka tarkoituksena oli tehostaa ja nopeuttaa pelastustoimelle rakennuksista saatavan reaaliaikaisen tiedon välittämistä. Toisin sanoen tarkoituksena oli parantaa onnettomuuden tilannekuvan hahmottamista. Samantyyppiselle järjestelmälle olisi haastattelujen perusteella edelleen tarve. Haastateltavat esittivät näkemyksiä, joiden mukaan tulisi olla järjestelmä, jonka tiedot perustuisivat etukäteen tallennettuihin tietoihin, kuten esimerkiksi rakennusten pohjakuviin ja kiinteistön muihin tietoihin sekä reaaliaikaiseen informaatioon, jotka saataisiin välitettyä helposti alueen pelastusviranomaiselle. Kahden haastateltavan osalta esille nousi tarvittavien tietojen jakaminen nykyaikaisessa rakennuksen tietomallissa tai digitaalisessa kaksosessa. Sen avulla voitaisiin helposti esittää esimerkiksi uloskäytävät, hyökkäysreitit sekä olosuhteet hälyttävässä tilassa. Tällöin pelastuslaitoksen hyödyntämää tietoa jäisi talteen ja se olisi helposti hyödynnettävissä onnettomuuden jälkikäsittelyssä.

Pelastusviranomaisia edustavat tahot toivat esille, että IoT-antureista ja -laitteista kerättyä dataa voitaisiin hyödyntää onnettomuuksien tutkinnassa sekä onnettomuuksien ehkäisyssä kehittämällä kansallista riskinarviointia sekä hyödyntämällä dataa valvontatoiminnan näkökulmasta. Pelastusviranomaiset, poliisi, vakuutusyhtiöt sekä muut onnettomuustutkintaa tekevät tahot hyödyntävät tulipalojen yhteydessä etäluettavista sähkömittareista kerättyä dataa. Sähkömittareista kerätty data saadaan siltä sähköyhtiöltä, joka vastaa alueen sähkönjakelusta. Etäluettavista sähkömittareista kerättyä tietoa voidaan hyödyntää esimerkiksi tulipalojen tutkinnan yhteydessä: mikä on ollut asuinhuoneiston tai rakennuksen sähkönkulutus ennen tulipaloa tai milloin sähköt ovat tilasta katkenneet.

Kerättyä dataa voitaisiin hyödyntää myös ihmisten toiminnan seuraamiseen, minkä seikan toi esille kaksi haastateltavista. Toiminnan seuraamisessa voisi tarkastella esimerkiksi, miten ihmiset poistuvat rakennuksesta palohälytysten sattuessa. Tästä kerättyä tietoa voitaisiin hyödyntää tutkiessa esimerkiksi ihmisten käyttäytymistä palohälytyksien yhteydessä sekä uloskäytäviä suunniteltaessa. Arviointiin tulisi ulottaa tieto, miten usein tapahtuu läheltä piti tilanteita tai paloturvallisuutta heikentävää toimintaa, kuten palo-ovien kiilaamista auki asentoon.

5.6 IoT-teknologian hyödyntämiseen liittyvät uhkakuvat

Haastattelujen aikana haastateltaville esitettiin kaksi kysymystä, jotka liittyivät IoT-teknologiaa hyödyntämiseen liittyviin uhkiin ja toimintavarmuuden riskeihin. Ensimmäinen liittyi siihen, mitä uhkatekijöitä IoT:n hyödyntämiseen liittyy sekä toinen aiheuttaako IoT riskitekijöitä paloturvallisuuslaitteistojen toimintavarmuudelle. Ensimmäinen kysymys esitettiin kaikille haastateltaville ja jälkimmäinen kysymys kymmenelle haastateltavalle.

Haastateltavien mukaan IoT:n hyödyntämiseen liittyy erilaisia uhkatekijöitä. Esille nousivat perinteiset IoT-teknologiaan liittyvät uhkatekijät kuten tietoturvaan ja tietosuojaan liittyvät asiat. Kaikki haastateltavat mainitsivat yleisimmäksi uhkatekijäksi tietoturvan sekä sen rinnalla kyberturvallisuuteen liittyvät uhat. Tietoturva tulee haastateltavien mukaan aina huomioida puhuttaessa IoT-teknologian hyödyntämisestä. Palo- ja henkilöturvallisuuteen liittyvät IoT-laitteet ja niiden tietoverkot eivät tee tässä poikkeusta. Tietoturva tulee huomioida aina, kun tietoa siirretään langattomasti. Lisäksi IoT-antureiden ja -laitteiden salasanoihin tulee kiinnittää huomiota. Uuden teknologian lisääntyminen järjestelmissä muodostaa myös tietynlaisen uhkan laitteistojen toimintavarmuudelle. IoT-teknologian osalta sitä ei kuitenkaan pidetty uhkana, koska sen nähtiin lisäävän laitteistoihin toimintavarmuutta enemmän kuin heikentävän sitä. Uhkatekijöiden ei katsottu olevan ylitsepääsemättömiä, vaan IoT-teknologian hyödyntämisestä katsottiin olevan enemmän hyötyä kuin haittaa, kuten kaksi haastateltavista asian kiteytti.

“Ei sitä voi mikään pysäyttää, et niin paljon meillä siihen tulee hyvää, meillä tulee paljon enemmän hyvää ku pahaa.”

"...muutenkin Internetin osalta jatkuvaa kilpajuoksua sen kanssa. Aina joku löytää jonkun aukon ja se paikataan tai, mut kyllähän näihin liittyvät hyödyt on varmasti moninkertaisia, kyllähän näihin kaikkiin aina ratkaisu löydetään."

Haastatteluissa nousi esille useita esimerkkejä siitä, miten tieto- ja kyberturvallisuus voivat olla uhattuina ja miten näitä uhkia voidaan estää. Haastateltavat toivat esiin ajankohtaisia tietoturvallisuuteen liittyviä tapauksia, kuten haittaohjelmistoja, tietoverkkojen tietoturvapuutteita sekä palvelunestohyökkäyksiä. Järjestelmien sisälle ei saa päästä helposti hakkeroimalla ja laitteistojen tietoturva tulee järjestää siten, ettei laitteistoja voida valjastaa esimerkiksi palvelunestohyökkäyksiin. Tietoturvallisuuteen liittyvät uhat on otettava huomioon toiminnan koko ketjussa aina fyysisistä laitteista järjestelmien rajapintoihin, tietoverkkoon ja niiden sovelluksiin. Suomessa on jo tapahtunut rakennuksiin ja niiden rakennusautomaatioon kohdistuneita hyökkäyksiä, joiden vuoksi esimerkiksi kahdesta asuinkerrostalosta saatiin katkaistua lämmöt pois järjestelmää vastaan kohdistuneen palvelunestohyökkäyksen avulla. Kyberuhka on erityisen tärkeä muistaa, koska sen avulla voidaan saada aikaan paljon vahinkoa. Kuten yksi haastateltavista totesi, että laittamalla palomuurit ja salasanat kuntoon, on tehty jo paljon tietoturvallisuuden parantamiseksi.

Yhden haastateltavan mukaan erityisesti valmistajien tulisi kiinnittää huomioita IoT-antureiden ja -laitteiden tietoturvaan, vaikka laitteiden käyttö onkin käyttäjän tai omistajan vastuulla. Tämä johtuu siitä, ettei laitteiston ostaja tai käyttäjä välttämättä ole perehtynyt tietoturvaan liittyviin asioihin. Toki kaikkea vastuuta ei voi vierittää valmistajan vastuulle, mutta olisi tarpeen, että se käyttäisi esimerkiksi eri laitteissa vähän erilaisia oletussalasanoja. Ohjelmistopäivityksiä tulisi tarjota laitteistoille mahdollisimman pitkään sekä reagoida tehokkaasti tilanteisiin, joissa laitteen tietoturvauhka on tullut esille. Vastaavanlaiset tietoturvauhkat ovat yleisiä erityisesti kuluttajille tarkoitetuissa IoT-antureissa ja -laitteissa. IoT-markkinat ovat tällä hetkellä erittäin kovat, minkä vuoksi tuotteiden tietoturvassa voi olla puutteita pyrkiessä saamaan niitä markkinoilla nopealla tahdilla, kuten haastateltava totesi.

"...no nyt on kultaryntäys käymässä, kaikki haluaa tehdä jotain, äkkiä markkinoille välittämättä mistään muusta, saadaan bitti kulkemaan, ja tuo tietoturva tulee joskus myöhemmin, jos on tullakseen"

Haastattelujen perusteella tietosuojan liittyvät asiat olivat toiseksi yleisin uhkakuva. Tietosuojaan liittyy myös yksityisyyden suoja. Datan keräämisen osalta on huomioitava, ettei yksilöä voida tunnistaa sen joukosta. Sen vuoksi hyödynnettävä data pitää muuttaa tai käsitellä siten, että yksittäistä ihmistä ei voida jäljittää. Lisäksi tietosuojaan liittyen kolme haastateltavaa toi esille Suomen ja Euroopan unionin alueella olevan tietosuoja-asetuksen muutokset ja sen tuomat velvoitteet. Jatkossa rekisterinpitäjän tulee huolehtia, että tietosuoja-asetuksessa esille tuotuja tietosuoja-periaatteita tullaan noudattamaan henkilötietojen käsittelyvaiheissa.

Uhkakuvana pidettiin myös liian suljettuja järjestelmiä ja niiden rajapintoja sekä dataformaatin soveltuvuutta. Järjestelmien välillä liikkuvien dataformaattien tulee olla sellaisia, että tieto siirtyy helposti järjestelmien välillä ja järjestelmät osaavat tunnistaa ja lukea tämän tiedon. Järjestelmäintegraatioissa Suomessa on ollut tapauksia, joissa järjestelmien välinen kieli on jäänyt määrittelemättä. Ongelma on tullut esiin laitteistoja testattaessa. Suljettujen ekosysteemien taas katsottiin aiheuttavan sen, etteivät järjestelmät ole helposti yhteensopivia. Tästä syystä uutta teknologiaa ei voida hyödyntää riittävän kustannustehokkaasti ja helposti. Rajapintojen osalta toivottiin avoimempia rajapintoja, jotta järjestelmäintegraatiot olisivat mahdollisimmin helposti toteutettavissa. Lisäksi katsottiin, että avoimien rajapintojen avulla voidaan parantaa jopa tietoturvaa, kuten yksi haastateltavista totesi.

"Sanoisin, että kannatan itse noita rajapinta-kehitysyhteistyötä, jossa nämä isot yritykset ovat mukana. Siinä me saadaan tuo tietoturva-taso paranemaan."

IoT-teknologiassa hyödynnetään laajalti langatonta tiedonsiirtoa sekä paristolla tai akulla toimivia IoT-laitteita ja -antureita. Haastateltavilta kysyttiin, voiko IoT-teknologian hyödyntäminen aiheuttaa riskitekijän paloturvallisuuslaitteiden toimintavarmuudelle. Kokonaisuutena langatonta ja paristolla toimivaa IoT-teknologiaa ei pidetty merkittävänä uhkana toimintavarmuudelle, varsinkaan, jos järjestelmässä on riittävästi älykkyyttä ilmoittaa hyvissä ajoin virtalähteen loppumisesta tai siitä, että langaton yhteys IoT-

laitteeseen on poikki. Paloturvallisuutta parantaville langattomille laitteistoille tulisi tehdä iso määrä testejä, jotta saataisiin selvyys laitteistojen virrankulutuksesta. Kokonaiset langattomat järjestelmät on syytä suunnitella siten, ettei signaalin häviäminen järjestelmässä aiheuta mitään suurempaa katastrofia. Haastateltavat korostivat näissä tapauksissa huollon roolia. Järjestelmän huoltaminen tulee olla selkeästi järjestetty, jotta järjestelmä saadaan luotettavasti toimivaksi. Seuraavassa kahden haastateltavan näkemyksiä huollon tarpeellisuudesta:

"…pitää olla se organisaatio, joka käy siitä huolehtimassa."

"…tällainen langattomuus ja patteripohjainen järjestelmä vaatii enemmän huoltoa ja sillä tavalla, että se edellyttää siten, että huolto toimii ja ne pysyy kunnossa."

Langatonta tiedonsiirtoakaan ei pidetty merkittävänä uhkana toimintavarmuudelle, varsinkin, jos langattoman verkon toimivuuden osalta tehdään mittaukset ammattilaisen toimesta. Näin varmistetaan ennakkoon kuuluvuuden taso, eikä yllätyksiä ylläpitovaiheessa pääse tulemaan. Haastateltavista kolme oli sitä mieltä, että tällä hetkellä parhaimpaan tulokseen päästään, kun esimerkiksi IoT-antureiden tai -laitteiden asennuksessa hyödynnetään kaapelointia langattomuuden sijaan. Näin saadaan toimintavarmempi järjestelmä. Tämä ratkaisee niin turvallisen tiedonsiirron kuin virransaannin. Langattomaan tiedonsiirtoon liittyy muutamia riskejä. Niitä on kuitenkin mahdollisuus pienentää. Käytettäessä esimerkiksi 4G-yhteyttä voidaan toimivuutta/toimivuus varmistaa kahden eri operaattorin hyödyntämisellä. Yhden operaattorin kuuluvuudessa ollessa ongelmia toiminta-alueella toinen toimii, joten se ei aiheuta tiedonsiirrossa ongelmia. Paristoihin liittyvää riskiä voidaan tulevaisuudessa pienentää energiaomavaraisilla antureilla. Nämä anturit saavat käyttöenergiansa esimerkiksi valosta tai lämpötilaeroista.

5.7 Asuinrakennuksien riittävä paloturvallisuustaso

Haastateltavilta kysyttiin saadaanko nykylainsäädännön mukaisilla paloturvallisuuslaitteistojen vähimmäisvaatimuksilla asuinrakennuksissa aikaan riittävä paloturvallisuuden taso. Monella haastateltavalla oli vaikeuksia vastata esitettyyn kysymykseen. Kaksi haastateltavista ei osannut tai halunnut vastata kysymykseen juuri mitään. Kysymysasettelua jouduttiin tarkentamaan ja usein esitettiin lisäkysymys siitä, voiko älytekno-

logiaa hyödyntämällä parantaa asuinrakennuksien paloturvallisuutta. Vastaukset vaihtelivat paljon. Tärkeimpänä havaintona vastauksista voidaan todeta, että älykkyyden lisääminen paloturvallisuuslaitteistoihin koettiin tarpeelliseksi. Lisäksi pidettiin tarpeellisena palovaroittimien sijoittamista jokaiseen huonetilaan sekä niiden yhteen kytkemistä, jotta hälytys saataisiin kuuluvammaksi.

Palovaroittimen kunnossapito oli kolmasosalla haastateltavista yleinen huolenaihe. Useimmin esille tullut seikka/asia oli se, että vastuu palovaroittimien kunnossapidon osalta esimerkiksi kerros- ja rivitaloissa tulisi olla enemmin omistajan kuin haltijan vastuulla niin paristokäyttöisissä kuin sähköverkkoon kytketyissä palovaroittimissa. Vastuuta siis olisi parempi näissä tapauksissa siirtää omistavalle taholle. Palovaroittimen toimintakuntoon liittyen esille nousi erilaisia syitä asukkaan unohduksesta aina tahallisuuteen saakka. Haastattelijat kertoivat omia kokemuksiaan liittyen palovaroittimien kunnossapitoon sekä viimeaikaisiin kuolemaan johtaneisiin tulipaloihin, joissa asuinrakennuksessa ei ollut lainkaan palovaroitinta tai palovaroitin ei ollut toimintakuntoinen. Yksi haastateltavista totesi seuraavasti.

”Siinä mielessä, jos katsotaan, että se on aidosti pakollinen laite, niin kyllä se vastuu pitäisi olla sen rakennuksen omistajalla, eikä haltijalla.”

Haastateltavista kolme oli sitä mieltä, että palovaroittimiin liittyy epävarmuutta, koska niiden laatuvaatimuksiin ei kiinnitetä riittävästi huomioita. On tapauksia, joissa palovaroitin ei toimikaan tulipalossa riittävän nopeasti tai palovaroitin ei reagoi ollenkaan. Palovaroittimien laatua tulisi tarkkailla enemmän, koska kyseessä on pakollinen turvalaite, kuten yksi haastateltavista totesi.

“Vaatimukset tulisi olla tiukemmat, mitä Suomessa saa noita laitteita myydä. ...kun puhutaan pakollisesta turvalaitteesta.”

Pelastusviranomaiset toivat esiin palovaroittimien osalta kaksi parannusehdotusta tai kehityksen kohdetta, joissa IoT-teknologiaa voitaisiin hyödyntää. Uusilla älypalovaroittimilla voitaisiin parantaa varsinkin kerros- ja rivitalojen paloturvallisuutta. Asumisturvallisuutta saataisiin parannettua, kun pystyttäisiin seuraamaan palovaroittimen toimintakuntoa. Palovaroittimista voitaisiin välittää tietoa esimerkiksi huoneiston haltijalle, kiinteistönhuollolle ja isännöitsijälle, mikäli palovaroittimen paristo loppuu tai palova-

roitin poistetaan. Näin varmistuttaisiin, että jokaisessa asuinhuoneistoissa olisi riittävä määrä palovaroittimia ja ne myös pysyisivät toimintakunnossa. Palovaroittimien toimintaa valvoisi haltijan lisäksi myös kiinteistön omistajan edustaja. Lisäksi IoT-teknologian avulla olisi mahdollista ilmoittaa alkaneesta palosta helposti myös muiden asukkaiden älypuhelimiin ja ketjuttaa asuinrakennuksessa olevia palovaroittimia varmistamaan palohälytyksen kuuluvuus.

Toisessa tapauksessa ehdotettiin, että älypalovaroittimiin voitaisiin liittää uusissa henkilöautoissa pakollisena oleva eCall-hätäviestipalvelu. eCall-hätäviestipalvelussa auto soittaa automaattisesti hätäkeskukseen ja avaa samalla puheyhteyden hätäkeskuksen ja auton välille, kun henkilöauto on joutunut onnettomuuteen. Ehdotuksessa esimerkiksi asuinrakennuksessa olevat älykkäät palovaroittimet olisi varustettu samanlaisella eCall-hätäviestipalvelulla. Älykkäät palovaroittimet varustettaisiin useilla antureilla ja ne näin ollen tunnistaisivat onko kyseessä oikea vaaratilanne vai erheellinen hälytys. Hätäviesti lähtisi hätäkeskukseen vain ennalta määriteltyjen algoritmien perusteella, jotta erheellisiä hälytyksiä ei välittyisi hätäkeskukseen. Puheyhteyden avulla asukas voisi keskustella hätäkeskuspäivystäjän kanssa ja kertoa lisätietoja tapahtuneesta.

Kaksi haastateltavista oli sitä mieltä, että uudisrakentamisessa riittävä paloturvallisuus saavutettaisiin varustamalla rakennukset automaattisilla sammutuslaitteistoilla. Heidän mielestään se olisi oikea ratkaisu, jos asuinrakennusten paloturvallisuutta haluttaisiin parantaa siten, että sillä olisi vaikutusta henkilö- ja omaisuusvahinkojen määrään.

Haastattelujen yhteydessä nousi esille se, ettei paloturvallisuutta voida jättää pelkkien paloturvallisuutta parantavien laitteiden varaan, vaikka uusi teknologia toisikin niihin parannuksia. Kolme haastateltavista toikin esille, että riittävän paloturvallisuuden takaamiseksi tarvitaan myös turvallisuuskasvatusta ja –koulutusta sekä sosiaalista tukea. Lisäksi haastatteluissa puhuttiin väestön ikääntymisen tuomista riskeistä sekä siitä, että erittäin huonokuntoisia ihmisiä hoidetaan kotona. Juuri tällaisiin riskikohteisiin älytekniikan lisääminen asuinrakennuksissa olisi tarpeen.

5.8 Osaamisen tarpeen lisääminen tulevaisuuden kehitystä varten

Haastateltavilta haluttiin näkemyksiä siitä, millaista osaamista tai minkä eri toimijoiden mukana oloa alan kehittyminen tulevaisuudessa vaatii, että IoT- ja älyteknologiaa hyödynnettäisiin rakennuksissa entistä tehokkaammin. Vastaukset olivat hyvin erilaisia, muutamia poikkeuksia lukuun ottamatta. Esille nousi, että laitteistojen, järjestelmien ja sovellusten tulee olla helppokäyttöisiä. Käyttäjälähtöisyys ylläpidon ja loppukäyttäjän tarpeiden näkökulmasta tulee muistaa. Tämä asia tulisi huomioida jo järjestelmien ja sovellusten kehittämisen yhteydessä, jotta ongelmia ei esiintyisi rakennuksen ylläpitovaiheen alkuvaiheilla. Järjestelmiä ja sovelluksia hyödyntävien henkilöiden tulee voida helposti omaksua niiden käyttö. Seuraavassa lainauksia haastatteluista aiheeseen liittyen:

"Opeteltaisiin ensin tällaisia käyttäjälähtöisen kehittämisen menetelmiä ja miettikää sen yksilön näkökulmasta, mitä siitä on hyötyä ja sellaista osaamista."

"...järjestelmien pitää olla sillä tasolla, että ne tukisi sitä käyttämistä, että se pystyisi siihen, pystyttäisiin hoitamaan ilman niin ku kolmea erityistä asiantuntijaa."

Toisena merkittävänä seikkana voidaan mainita digitalisaatioon liittyvän tietoisuuden lisääminen koko rakentamisen ketjussa aina lainsäädännön valmistelusta rakennuksen ylläpitoon saakka. Tarvetta tietoisuuden lisäämiseen on niin olemassa olevan teknologian vaihtoehdoista, tietoturvasta kuin aiheeseen liittyvästä termistöstä ja perusasioista lähtien. Ratkaisuvaihtoehtoina tähän haastateltavat toivat näkemyksiä digitalisaatioon liittyvän tietämyksen ja osaamisen lisäämiseen niin ammatilliseen koulutukseen kuin täydennyskoulutukseen. Esille tuli esimerkiksi erilaisia täydennyskoulutusvaihtoehtoja eri osa-alueille, joissa kerrottaisiin digitalisaation mahdollisuuksista, hyödyistä ja niihin kohdistuvista uhkista. Erityisesti ylläpidon roolia tietämyksen lisäämisessä tuotiin useimmin esille.

Pelastusviranomaisten edustajat toivat esille näkemyksen, että pelastustoimen olisi jo syytä herättää keskustelua siitä, minkälaisia toiveita pelastustoimella on digitalisuuteen ja älyteknologian lisääntymiseen liittyen. Tulisi miettiä, mitkä ovat tulevaisuudessa pelastustoimen valmiudet ottaa vastaan rakennuksista tulevaa dataa, jota voitaisiin hyödyntää esimerkiksi pelastustoiminnan johtamisessa. Pelastusviranomaisten ja tarvittaes-

sa muidenkin turvallisuusviranomaisten tulisi olla mukana digitalisaation kehityksessä puhuttaessa henkilö- ja paloturvallisuuslaitteistoista. Rakennuskohteetkin muuttuvat koko ajan vaativammiksi. Rakennetaan yhä korkeammalle ja syvemmälle sekä rakennuksien leveyskin on vuosien saatossa kasvanut. Tämä tuo tarpeen uuden teknologian asentamiselle rakennuksiin sekä niistä saatavan datan hyödyntämisen pelastustoimen tarpeisiin. Seuraavassa yhden haastateltavan näkemys pelastustoimen mukana olosta teknologian kehittymiseen liittyen.

”Se keneltä osaaminen ja resurssit puuttuu, olla ohjaamassa ja viemässä kehitystä eteenpäin on viranomaiset. Mitä me halutaan, mitä ne laitteet on, mitä ne järjestelmät on, mitkä on ne rajapinnat, mitkä ovat ne tietoturvavaatimukset. Mitkä ovat meidän odotukset niille?”

Haastatteluissa mainittiin, että erilliselle digiasiantuntijalle olisi tarvetta rakennushankkeiden yhteydessä. Tästä on ollut valtakunnallisesti puhetta eri yhteyksissä ja Suomessa ovatkin valmisteilla ensimmäiset rakennushankkeet, joissa on digitalisaation vastuualueelle nimetty digikonsultti. Digikonsultin tehtävä olisi esimerkiksi määritellä se, mikä kyseisen rakennuksen digitalisaation hyödyntämisen taso on. Henkilö toimisi tilaajan tai rakennushankkeeseen ryhtyvän asiantuntijana. Haastatteluissa nousi myös poikkeavia mielipiteitä. Välttämättä ei ole oikein lisätä uutta roolia, vaan olisi ehkä tarpeen lisätä rakennushankkeessa mukana olevien suunnittelijoiden osaamisen tasoa.

5.9 Turvalaitteistojen standardien vaikutus älytekniikan lisääntymiseen

Haastateltavilta haluttiin näkemyksiä siitä mikä on turvalaitteistojen standardien ja suunnitteluohjeiden vaikutus älytekniikan hyödyntämiseen ja kehitykseen. Kysymys esitettiin kymmenelle haastateltavalle. Näistä kymmenestä vain noin puolella oli kokemusta turvalaitteistojen standardien tai suunnitteluohjeiden vaatimustasoista. Kaikki kuitenkin antoivat oman mielipiteensä. Tuloksien perusteella voidaan todeta, että voimassa olevat standardit tai suunnitteluohjeet eivät estä uuden teknologian hyödyntämistä esimerkiksi paloteknisissä laitteistoissa. Standardien osalta 7/10 oli sitä mieltä, että voimassa olevat standardit vaikeuttavat älytekniikan lisääntymistä. Yleisin peruste oli se, että standardit kehittyvät hyvin hitaasti, jonka vuoksi teknologian kehitys voi mennä standardien edelle. Näin ollen standardit voivat perustua jopa vähän vanhentuneeseen

ajatusmalliin, joka ei kannusta uusien hyväksikin havaittujen tapojen tai teknologian käyttöä. Seuraavassa yhden haastateltavan näkemys standardien vaikutuksesta älytekniikan hyödyntämiseen liittyen:

"Sanotaan tuota, että ne vaikeuttavat joka tapauksessa, koska ne elää hitaasti. Jos meillä ei ole mitään tehty, niin standardia ei voi etukäteen kirjoittaa."

Kuitenkin yleinen näkemys oli, että standardit tulee olla ennen kaikkea turvalaitteistoja varten ja ne tulee tehdä niiden mukaan. Siten varmistetaan riittävä turvallisuustaso. Turvallisuuden katsottiin siis olevan tärkeä asia, joka voidaan saavuttaa ajantasaisilla standardeilla maksimaalisen hyödyn saavuttamiseksi.

5.10 IoT-teknologia järjestelmäintegraatioissa

Haastateltaville esitettiin kysymys, onko mahdollista yhdistää olemassa olevia suljettuja turvallisuusjärjestelmiä ja IoT-teknologiaa yhteen. Kysymys esitettiin kymmenelle haastateltavalle. Kukaan haastateltavista ei pitänyt integrointien tekemistä mahdottomana. Kokonaisuutena voidaan todeta, että järjestelmien integroitiin sisältyy paljon kysymyksiä, jotka tulee ratkoa aina tapauskohtaisesti. Suomessa paloturvallisuutta parantavia laitteistoja on integroitu yhteen rakennuksien rakennusautomaation kanssa jo vuosia. Se ei sinällään ole uutta. Lisäksi paloturvallisuutta parantavia laitteistoja on yhdistetty erilaisiin kiinteistöjen hallintajärjestelmiin, joista laitteistoa tai koko rakennusta voidaan monitoroida. Suurimpana ongelmana järjestelmien integroinnissa nousivat esiin rajapintojen puutteet tai niiden avoimuuden puute. Haastateltavista yli puolet (6/10) olivat tätä mieltä. Turvallisuusjärjestelmät ovat yleensä aikaisemmin rakennettu hyvin suljetuiksi järjestelmiksi, jonka vuoksi niiden yhdistäminen muihin järjestelmiin on ollut haastavaa. Järjestelmien yhteensovittaminen on ollut haasteellista. Olemassa olevien järjestelmien ja uuden teknologian konfigurointiin voi sisältyä niin paljon manuaalista työtä, että sen kustannukset voivat nousta korkeiksi. Näin ollen järjestelmäintegraatiosta tuleekin saada merkittävää hyötyä, jotta se kannattaa toteuttaa. Seuraavassa kaksi kommenttia aiheeseen liittyen:

"Ja sitten tää kustannustehokkuus on niin ku, siitä pitäisi olla hyötyjä, joista moni olisi valmis maksamaan. Se vaatii niitä applikaatioita, jotka oikeesti hyödyntää sitä integrointia."

”…että sellaista manuaalista työtä siinä järjestelmän virittämisessä. Järjestelmäkonfiguraatio menee sen verran aikaa, että helposti ei löydy maksajaa sille työlle.”

Paloturvallisuuslaitteistojen sekä –järjestelmien integrointien helpottamiseksi rajapintojen tulisi haastateltavien mukaan olla entistä avoimempia. Tämä mahdollistaisi kustannustehokkaamman ja helpomman järjestelmäintegraatioiden toteutuksen ja tiedonsiirron onnistumisen. Lisäksi uudenaikaisten väyläliitäntöjen kautta saadaan data siirtymään tehokkaasti laitteiden ja järjestelmien välillä. Laitevalmistajien edustajat kertoivat haastattelujen yhteydessä, että heidän uusimmissa järjestelmissään laitteisto- tai järjestelmäintegraatioissa toiminta on jo huomattavasti helpompaa, koska järjestelmät tukevat laajasti eri protokollia. Heidän järjestelmiinsä voidaan yhdistää muita kolmannen osapuolen järjestelmiä sekä heidän turvallisuuslaitteistojaan voidaan liittää esimerkiksi muiden valmistajien kiinteistönhallintajärjestelmiin.

Laajoihin räätälöityihin järjestelmäintegraatioihin sinällään kuuluu ohjelmistojen päivittämiseen liittyvä riski. Päivitettäessä yksi järjestelmän osa ei voida tietää, miten se vaikuttaa muihin järjestelmiin. Haastateltavista kaksi toi haastattelujen yhteydessä tämän näkemyksen esille. Rakennusautomaatioon liittyy useita standardeja, joiden mukaan esimerkiksi järjestelmien yhdistämisiä voidaan toteuttaa. Vaatii vain aikaa, että rakennusalalla aletaan käyttää entistä vakioituneimpia standardeja. Standardeja pidetään tärkeänä tekijänä järjestelmäintegraatioissa, koska niiden avulla tietoturvallisuuskin saadaan varmistettua. Yleisesti tulevaisuuden visiona haastatteluissa oli, että järjestelmäintegraatiot tulevat olemaan entistä laajempia. Turvajärjestelmiä ja kiinteistöautomaatioon liittyviä laitteita ja järjestelmiä integroimalla yhteen voidaan saada aikaan parannusta nykyiseen turvallisuustasoon. Seuraavassa kolme kommenttia haastateltavilta aiheeseen liittyen:

”…kun järjestelmät alkavat jutella keskenään ja sitten tehdään yhteen päivitys, niin vaikuttaako se päivitys niihin kymmeneen muuhun järjestelmään?”

“Sitten kun ne on standardin mukaisia, niin sitten sä tiedät, että ne on turvallisia käyttää ja turvallisuusaspektit on huomioitu.”

“Mitä paremmin se saadaan integroitua eri järjestelmiin yhteen sitä parempi turvallisuustasohan me saavutetaan.”

6 JOHTOPÄÄTÖKSET

Tässä luvussa esitetään työn johtopäätökset sekä tuodaan vastauksia niin päätutkimuskysymykseen kuin sen alatutkimuskysymyksiin. Saadut johtopäätökset perustuvat tutkimustuloksiin, kirjallisuuskatsauksessa esille tuotuihin asioihin sekä muihin aihetta sivuaviin tutkimuksiin. Johtopäätöksissä on pyritty käytännönläheisesti tuomaan esille ratkaisuja joiden avulla IoT-teknologiaa hyödyntämällä on mahdollista parantaa paloturvallisuutta sekä saada sen avulla erilaisia hyötyjä. Luvun lopussa tuodaan esiin jatkotutkimusehdotuksia.

6.1 Tutkimustulosten päätelmät

Yleisenä johtopäätöksenä voidaan todeta, että IoT-teknologian hyödyntäminen on mahdollista myös paloturvallisuuden osa-alueella. Se tuo hyvän lisän olemassa olevien laitteistojen kehittämiseen sekä antaa mahdollisuuden kehittää entistä kiinnostavampia paloturvallisuutta parantavia laitteistoja ja niihin liittyviä palveluita. IoT myönteisyys näkyikin tutkimustuloksissa selvästi. Tähän varmasti vaikuttaa se, että kaikki haastateltavat olivat hyvin uuteen teknologiaan sekä digitaalisuuteen orientoituneita henkilöitä. Teknologian ei katsottu olevan rajoittava tekijä, vaan sen nähtiin mahdollistavan monia asioita, joista on hyötyä niin kustannustehokkuuden, viihtyvyyden kuin turvallisuudenkin parantamisessa.

Haastateltavat edustivat yhdeksän eri toimialan osaajaa. Tämä johtui siitä, että tarkoituksena oli saada kokonaisvaltainen kuva IoT-ilmiöstä rakennusten paloturvallisuuden kehityksessä. Aiempaa tutkimusta tästä ilmiöstä ei juuri ole tehty. Haastateltavien vastauksissa ei löytynyt selkeitä eroja eri toimialojen väliltä, mikä sinällään oli jopa yllättävää. Toki haasteltavien tarkentavissa vastauksissa oli hyvinkin paljon eroja, johon vaikutti pitkälti haastateltavan osaamisen taso tutkittavaan aiheeseen liittyen, eikä niinkään haastateltavan edustama toimiala. Tutkimustuloksissa tuli esimerkiksi esille, että uuden teknologian hyödyntäminen rakennusteollisuudessa on haasteellista, koska sitä pidetään hyvin vanhakantaisena toimijana. Näissä mielipiteissä korostuivat haastateltavien työkokemus rakennushankkeissa mukana olosta, eikä niinkään heidän edustamansa toimiala.

Haastateltavat olivat hyvinkin innovatiivisia ja pystyivät kertomaan omia ideoita siitä, miten IoT-teknologiaa hyödyntämällä voitaisiin saada parannusta paloturvallisuuteen. Hyvä esimerkiksi tällaisesta on eCall-hätäviestipalvelun hyödyntäminen myös asuinrakennusten paloturvallisuusratkaisuissa. Kyseinen hätäviestipalvelu tulee pakolliseksi maaliskuun 2018 jälkeen tyyppihyväksyttyihin henkilö- ja pakettiautoihin (Hätäkeskuslaitos 2018). Kuitenkin eCall-hätäviestipalvelun käyttö voisi tulevaisuudessa olla myös rakennuksissa mahdollista, koska se on teknologisesti mahdollista toteuttaa. Se olisi varteen otettava vaihtoehto asuinrakennusten paloturvallisuuden parantamiseksi erityistapauksissa. Ehdotus kuitenkin edellyttäisi vielä paljon kehitystyötä, jotta palovaroittimiin saataisiin nykyistä enemmän älykkyyttä erheellisten hälytysten estämiseksi.

Tutkimustuloksissa korostuivat ennen kaikkea palon havaitsemiseen tarkoitetut paloturvallisuutta parantavat laitteistot, kuten palovaroittimet ja automaattiset paloilmoitinlaitteistot. Tähän todennäköisesti vaikuttivat jo markkinoilla olevat IoT-ratkaisut. Henkilö- ja paloturvallisuuslaitteistojen osalta esimerkiksi savunpoistolaitteistot, poistumisvalaistusjärjestelmät sekä evakuointijärjestelmät jäivät tutkimustuloksissa hyvin vähäiselle huomioinnille, vaikka IoT:tä voitaisiin hyödyntää myös niissä, kuten kirjallisuuskatsauksessa on tuotu esille.

6.2 IoT-teknologian hyödyntäminen Suomen rakennuskannassa

Tutkimustuloksien perusteella voidaan todeta, että IoT- ja älyteknologian hyödyntäminen Suomen rakennuskannassa on kokonaisuudessaan varsin vähäistä ja paloturvallisuuden kehityksessä vieläkin vähäisempää. Haastatteluissa IoT-ratkaisuista esille nousivat etupäässä kiinteistöautomaation toteutukset, eivätkä niinkään paloturvallisuuteen liittyvät ratkaisut. Haastateltavien esille tuomat paloturvallisuuden IoT-ratkaisut perustuivat pitkälti kirjallisuuskatsauksessa esille tuotuihin laitteisiin tai järjestelmiin. Esille ei oikeastaan noussut käytännön esimerkkejä erilaisista paloturvallisuuden IoT-ratkaisuista, mikä oli yksi tämän tutkimuksen tavoitteista. Syy tähän on varmasti se, ettei IoT-teknologiaa hyödyntäviä paloturvallisuusratkaisuja vielä juurikaan ole.

IoT-teknologian hyödyntämisen kehityssuuntaa voidaan pitää positiivisena, mikä tuloksistakin on havaittavissa. Haastateltavien näkemysten mukaan IoT:n avulla ja sitä hyödyntämällä on mahdollista parantaa rakennusten paloturvallisuutta. Kokonaisuutta kat-

soessa IoT:n yleistymiseen löytyy tukea myös markkinatutkimuslaitoksen ennusteesta. Esimerkiksi Mckinsey Global Institute on ennustanut, että Internetiin liitettävien laitteiden määrä tulee seuraavan kymmenen vuoden aikana lisääntymään vähintään kolminkertaiseksi nykyisestä määrästä (Mckinsey Global Institute 2015 s.7, 17). Lisäksi Dooley et al (2017) ovat tehneet kiinteistöjen IoT-markkinakatsauksen, jonka mukaan IoT nähdään yhdeksi tärkeimmistä kiinteistö- ja rakennusalan kehityssuunnista ja investointikohteista lähitulevaisuudessa (Dooley et al 2017, s. 8). Tämän työn tekemisen yhteydessä Suomen markkinoille on tullut uusia toimijoita, jotka tarjoavat IoT-ratkaisuja myös paloturvallisuuden puolelle. Näistä esimerkkinä voidaan mainita älykkäät palovaroittimet.

Tutkimustuloksissa tuli vahvasti esille erilaisia syitä, joiden vuoksi IoT- ja älyteknologiaa hyödynnetään toistaiseksi varsin vähän Suomen rakennuskannassa. IoT:n hyödyntämisen vähäisyyden syynä ei ollutkaan itse teknologia tai sen rajoitteet, vaan selkeämmin asennoituminen uuteen teknologiaan ja sen tuomiin haasteisiin. Näiden seikkojen voidaankin katsoa muodostavan merkittävimmät haasteet IoT- ja älyteknologian lisääntymiseksi. Osaltaan esille tulleet syyt ovat hyvinkin ymmärrettäviä, koska uusien asioiden sisäistäminen vie aina oman aikansa. Teknologian kehitys on saattanut vaikuttaa siihen, ettei rakennusalalle ole syntynyt riittävän nopeasti vakiintuneita malleja siitä, millä tavalla älykkyyttä rakennuksiin lisättäisiin. Markkinoille on tullut osaamista, valmiita sovelluksia, komponentteja ja tiedonsiirtoratkaisuja, joiden avulla toteutukset on mahdollista tehdä helposti ja suhteellisen kustannustehokkaasti. Lisäksi tietämys teknologian avulla saatavista hyödyistä on lisääntynyt, vaikka itse tietämyksen puute oli tämän työn tutkimustulosten perusteella yksi yleisimmin tunnistetuimmista ongelmista, miksi IoT- ja älyteknologiaa ei hyödynnetä laajasti jo Suomen rakennuskannassa.

Kappaleessa 5.2 esitettiin yhdeksän syytä siihen, miksi IoT- ja älyteknologiaa hyödynnetään toistaiseksi Suomessa rakennuksissa melko vähän. Osa esille nostetuista yhdeksästä syystä linkittyy tavalla tai toisella toisiinsa. Esille nostetuista syistä esimerkiksi referenssikohteiden puute, teknologiaan liittyvä riskinotto sekä teknologiakustannukset liittyvät tietyllä tavalla toisiinsa ja muodostuvat myös esteen teknologioiden kehitykselle. Merkittävänä yhdistävän tekijänä voidaan pitää rakennushankkeeseen ryhtyvälle tai kiinteistön omistajalle muodostuvat normaalia suuremmat teknologian hankintakustan-

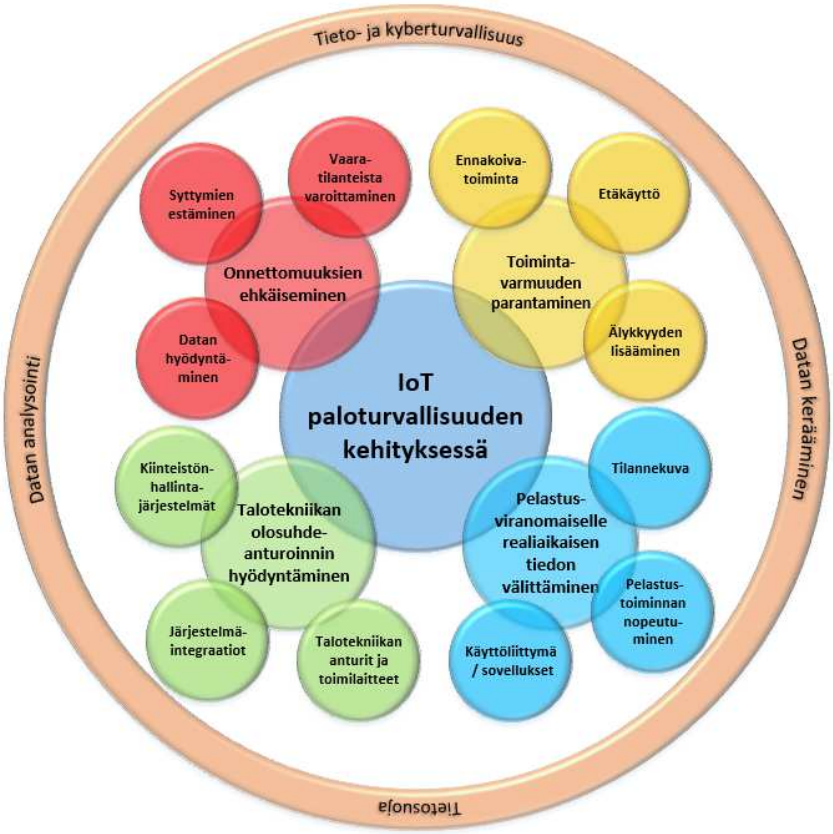
nukset ja tietynlainen pelko kustannusten kasvusta ylläpitovaiheen aikana. Pilottikohteessa uuden teknologian hyödyntäminen voi aiheuttaa haittaa niin kustannusten kuin toiminnan kannalta. Rakennushankkeeseen ryhtyvä tai kiinteistön omistaja ei välttämättä halua ottaa riskiä ja satsata uusimpaan teknologiaan. Tämä voi johtaa siihen, ettei laitevalmistajilla ole kiinnostusta kehittää laitteistojen teknologiaa entistä älykkäämmiksi. Laitevalmistaja voi katsoa tarpeettomaksi kehittää tuotteitaan tai palveluitaan, jos ne eivät aiheuta markkinoilla riittävästi kiinnostusta. Olisikin tarpeellista, että rakennushankkeen eri osapuolet ymmärtäisivät järjestelmäintegraatioiden tuottamat tehokkuusedut huomioiden rakennuksen koko elinkaaren.

Paloturvallisuustekniikka kuten muukin talotekniikka tulisi ottaa paremmin huomioon rakennusten suunnittelun yhteydessä sekä rakennuksen elinkaariajattelussa. Esimerkiksi paloturvallisuutta parantavien laitteistojen suunnittelussa lainsäädännön ja standardien vaatimustason lisäksi olisi syytä kiinnittää huomiota entistä enemmän rakennuksen käyttötarkoituksen tuomiin vaatimuksiin, muuntojoustavuuteen, ylläpidon toteutukseen sekä ennen kaikkea sen loppukäyttäjien tarpeisiin. Näin varmistettaisiin, että paloturvallisuustekniikka on juuri kohteeseen soveltuva. Pelkkien valmiiden perinteisten mallien valinta kohteeseen ei aina tuo toivottua tulosta elinkaariajattelun näkökulmasta, jos uusinta teknologiaa ei oteta riittävästi huomioon. Sen vuoksi tietoisuuden lisääminen uusista teknologioista ja niiden mahdollisuuksista tulisi tuoda esille entistä tehokkaammin rakennushankkeen eri osapuolille sekä loppukäyttäjille.

Uuden teknologian hankinta riippuu paljon siitä miten paljon sille annetaan arvoa. Tulevaisuus näyttää miten uudet älykkäät ratkaisut tulevat yleistymään. Luottoa älykkyyden lisäämiseen asumisen turvallisuuden lisäämiseksi on havaittavissa. Esimerkiksi vakuutusyhtiöt ovat alkaneet markkinoimaan älykotipaketteja kotivakuutuksen lisäksi eräänlaisena älykotivakuutuksena. LähiTapiola tarjoaa nykyisin Cozifyn älykotilaitteistoa asiakkailleen. Tässä yhteydessä vakuutusyhtiö maksaa suurimman osan vakuutuksenottajan laitteiston hankintakustannuksista. Kyseiseen älykotilaitteistoon on mahdollista liittää esimerkiksi älykkäitä palovaroittimia. (LähiTapiola 2018). Tulevaisuudessa älykkäitä ratkaisuja voisi markkinoida tehokkaammin esimerkiksi iäkkäille ihmisille kodinhoidon lisäpalveluna ja siten parantaa asukkaan turvallisuutta ja turvallisuuden tunnetta.

6.3 Rakennuksien paloturvallisuuden parantaminen IoT-teknologialla

Tämän työn pääkysymys on: Voidaanko IoT-teknologialla parantaa rakennuksien paloturvallisuutta nyt ja tulevaisuudessa? Tuloksien perusteella IoT-teknologialla voidaan parantaa paloturvallisuutta ja se on jo nyt mahdollista. Tulevaisuudessa IoT-ratkaisut tulevat suurella todennäköisyydellä lisääntymään, mikä tulee parantamaan entisestään paloturvallisuutta. Samanlaisia tuloksia tuli esille myös kirjallisuuskatsauksen yhteydessä. Kuvassa 9 on kuvattu, miten IoT-teknologiaa hyödyntämällä saadaan kehitystä paloturvallisuuteen liittyen. Tutkimuksessa nousi esille neljä päätekijää, joista jokaista on avattu tarkemmin omissa kappaleissaan. Päätekijät koostuvat pienemmistä tekijöistä, joiden kautta voidaan katsoa syntyvän paloturvallisuuden kehitystä sekä sitä kautta myös parannusta. Jokaisen erillisen tekijän kohdalla on huomioitava erityisesti tieto- ja kyberturvallisuuteen sekä tietosuojaan liittyvät asiat. Lisäksi IoT mahdollistaa laajan datan keräämisen sekä sen analysoinnin.



Kuva 9. IoT paloturvallisuuden kehityksessä

Tutkimustuloksista on huomioitava, että esille tuodut hyödyt tai ratkaisut ovat tietyissä tapauksissa mahdollista toteuttaa muutenkin kuin IoT-ratkaisuina. Laitteita ja järjestelmiä ei ole aina välttämätöntä kytkeä Internetiin tai kerätä dataa joka toiminnoista, jotta paloturvallisuutta saadaan parannettua. IoT eikä mikään muukaan teknologia yksin varmista rakennuksien riittävää paloturvallisuutta, vaan paloturvallisuus muodostuu useista eri tekijöistä. Ihmisen rooli on edelleen tärkeässä osassa riittävän paloturvallisuuden varmistamiseksi. Teknologia tuo kuitenkin paloturvallisuuden parantamiseen uusia mahdollisuuksia, joista IoT on tällä hetkellä yksi kiinnostavimmista ja monet asiat mahdollistava.

Tutkimustuloksissa ei tullut esille juuri data-analytiikkaan tai datan laajempaan hyödyntäminen liittyviä mahdollisuuksia, vaikka nämä asiat ovat hyvin olennainen osa IoT:n kautta saaduista hyödyistä ja mahdollisuuksista. Tähän osa syynä on varmasti se, että IoT on varsin uusi asia paloturvallisuuden osa-alueella. Samanlaisiin tuloksiin on päädytty kiinteistöjen IoT-markkinakatsauksessa 2017, jonka perusteella markkinoilla olevat IoT-tuotteet ja -palvelut keskittyvät pääsääntöisesti yksittäisen asian optimointiin, ei prosessien kehittämiseen tai uuden asiakasarvon tai liiketoiminnan kehittämiseen (Dooley et al 2017, s 4). Tulevaisuudessa IoT-teknologian yleistymisen myötä tulee varmasti ilmi uusia hyötyjä, joita tässä työssä ei ole tuotu esille.

6.3.1 Toimintavarmuuden parantaminen

Haastatteluissa yksi esille nostetuimmista asioista oli toimintavarmuuden parantaminen IoT:n avulla. Tämä korostuu ennen kaikkea paloturvallisuutta parantavissa laitteistoissa. Toimintavarmuuden katsottiin paranevan, kun laitteita ja järjestelmiä voidaan monitoroida etäyhteyden avulla. Etäyhteys ei paloturvallisuutta parantavissa laitteistoissa ole mikään uusi asia. Kuitenkin Internet-yhteyttä hyödyntämällä monitorointi ja hallinnointi voidaan toteuttaa entistä tehokkaammin mobiilisti älypuhelimella tai tabletilla. Shinde et al (2017, s.1080) ovat esittäneet artikkelissaan, että IoT-teknologiaa hyödyntämällä voidaan luoda etäyhteys paloilmoitinlaitteistoon, jonka kautta järjestelmän tehokas monitorointi ja ohjaus on mahdollista. Tuomisaari (2017, s 46) on tuonut diplomityössään esille saman asian sammutuslaitteistojen osalta. Internetiin kytkettyjen antureiden ja laitteiden tilaa on mahdollista tarkkailla reaaliaikaisesti, saada nopeasti selville laitteis-

toa tai järjestelmää koskevat viat/vikailmoitukset sekä hallinnoida järjestelmiä tekemällä esimerkiksi paloilmoitinlaitteistolle irtikytkentöjä. IoT-ratkaisuna toteutettuna on mahdollista välittää dataa useille eri toimijoille aina kiinteistön omistajalta laitevalmistajalle asti. Näin ollen yhä useammat toimijat pääsevät tarkastelemaan järjestelmää ja siihen kytkettyjä laitteita. Tämä mahdollistaa myös paloturvallisuutta parantavien laitteistojen ennakoivan huoltotoiminnan suorittamisen. Laitteistoja ja järjestelmiä voidaan huoltaa ennen kuin laitteistot ennättävät vikaantumaan, mikä lisää laitteistojen toimintavarmuutta.

Toimintavarmuuden voidaan katsoa myös paranevan teknologian kehityksen vuoksi. Paloturvallisuutta parantavat laitteistot ja järjestelmät ovat muuttuneet koko ajan älykkäämmiksi. Älykkyyden lisääminen mahdollistaa tehokkaamman diagnostiikan suorittamisen. Järjestelmä huomaa laitteistoon tulevat viat ennakkoon sekä virheelliset toiminnot, jotka johtuvat esimerkiksi ihmisen väärästä toiminnasta. Parhaimmassa tapauksessa laitteisto osaa korjata puutteet itse niin, ettei ihmisen toimintaa välissä juuri tarvita. Paloturvallisuutta parantavien laitteistojen toimiessa yhteen muiden järjestelmien kanssa, mahdollistetaan myös erheellisten palohälytysten tunnistaminen entistä paremmin. Lisäämällä laitteistoihin anturointia ja älykkyyttä on mahdollista ennalta määriteltyjen algoritmien avulla entistä paremmin tunnistaa alkanut tulipalo.

Suomen nykyinen automaattinen paloilmoitinlaitteistokannan voidaan katsoa olevan tärkeä osa henkilöturvallisuuden parantamista ja omaisuuden suojaamista. Esimerkiksi varhaisen tulipalojen havaitsemisen vuoksi pystyttiin ehkäisemään arviolta 16 miljoonan euron vahingot vuonna 2016 (Pelastusopisto 2017a). Laitteisto on hyvin luotettava, mutta tämän lisäksi on huomioitava, että Suomessa erheellisten palohälytysten ilmoitusten määrä on jopa 96 % (Pelastusopisto 2017b, s. 27). Tämän vuoksi onkin tarpeellista kehittää järjestelmiä, jotta erheellisten paloilmoitusten määrää saadaan vähennettyä, vaikka laitteisto on merkittävä ja luotettava paloturvallisuuden parantaja.

Toimintavarmuuden säilyttäminen on erittäin tärkeää tulipaloa rajoittavissa laitteistoissa, kuten sprinklerilaitteistoissa, joissa huollon laiminlyönti saattaa aiheuttaa ihmisten joutumisen hengenvaaraan sekä tuottaa huomattavia taloudellisia menetyksiä (SFS EN 12845+A2 2015, s.7) Nieminen (2018) on diplomityössään tutkinut rakennusten sprink-

lerilaitteistojen luotettavuutta. Sprinklerilaitteistoa voidaan pitää luotettavana laitteistona, koska luotettavuuden vaihteluväli oli yleisesti 99 % tasolla. Tutkimuksessa esille tulleet laitteistojen toimimattomuudet johtuivat suurimmaksi osaksi puutteellisesta ylläpidosta. Laitteiston ylläpidosta on huolehdittava, jotta sprinklerilaitteiston luotettavuus säilyy korkeana koko laitteiston elinkaaren ajan. (Nieminen 2018, s.73-74). IoT tarjoaa vaihtoehtoisen ratkaisun sammutuslaitteistojen monitorointiin, jotta voidaan varmistua laitteiston toimivuudesta.

Palovaroitin tuli Suomessa pakolliseksi asuinrakennuksiin vuoden 2000 aikana. Suomalaisten näkemys palovaroittimen tarpeellisuudesta turvallisuuden kannalta on vuosien saatossa lisääntynyt. Pelastusopisto on tehnyt suomalaisten pelastusasenteisiin liittyvän tutkimuksen vuonna 2017, jonka perusteella 94 % suomalaisista pitää palovaroitinta erittäin tärkeänä laitteena (Kokki 2017a, s 8). Kuitenkin palovaroittimen puuttumista asuinrakennuksista ja niihin kohdistuvaa puutteellista ylläpitoa voidaan pitää isona ongelmana, vaikka suurin osa pitää palovaroitinta tärkeänä turvallisuuden parantajana. Safetum Oy:n tekemien pelastustarkastuksien perusteella vuonna 2017 noin 61 %:ssa taloyhtiössä oli puutteita palovaroittimien kunnossapidossa (Safetum 2017). Pelastustoimen resurssi- ja onnettomuustilaston PRONTO tietojen perusteella Suomessa vuosina 2012 – 2016 asuinrakennuksissa sattuneissa rakennuspaloissa ja rakennuspalovaaroissa palovaroitin puuttui noin 28 %:ssa pientaloista, 33 %:ssa rivitaloista ja noin 39 %:ssa kerrostaloista. Lisäksi palovaroitin ei ollut sattuneissa tulipaloissa toimintakuntoinen noin 2 %:ssa pientaloista, noin 4 %:ssa rivitaloista sekä noin 6 %:ssa kerrostaloista. Palovaroittimen toimimattomuuteen saattoi vaikuttaa pariston epäkunto, pariston puuttuminen tai palovaroitin oli rikkonainen (Kokki 2017b).

Rivi- ja kerrostaloissa palovaroittimen puuttuminen ja sen toimimattomuus on yleisempää kuin pientaloissa. Palovaroitin on asuinrakennuksissa pakollinen turvalaite ja sen toimintakunnon säännöllinen testaaminen on haltijan eli asukkaan vastuulla. Lisäksi asukkaan velvollisuutena on huolehtia myös, että asunto varustetaan riittävällä määrällä palovaroittimia. Osa palovaroittimien kunnossapitovastuusta voi olla taloyhtiöllä, jos asuinhuoneistoihin on asennettu sähköverkkoon kytketyt palovaroittimet (pelastuslaki 379/2011 17 §; SPEK 2018). Asukkaan laiminlyödessä palovaroittimen asentamisen tai sen kunnossapidon, aiheuttaa se paloturvallisuusriskin. Paloturvallisuusriski ei muodos-

tu välttämättä vain huoneiston asukkaalle, asukkaille tai sen omaisuudelle, vaan myös koko asuinrakennuksen asukkaille ja omaisuudelle. Esimerkiksi rivi- ja kerrostaloissa asuinhuoneistojen palovaroittimet ja niiden toimintakunnossa pitäminen voi kiinnostaa myös asuinrakennuksen muita asukkaita tai kiinteistön omistajatahoa. IoT-teknologian hyödyntämällä on mahdollista tuoda parannusta palovaroittimien toimintavarmuudelle.

Esimerkiksi älykkäiden palovaroittimien avulla taloyhtiöissä kiinteistön ylläpidon henkilöstöllä tai omistajataholla on mahdollista monitoroida tehokkaasti rakennuksien palovaroittimien toimintakuntoa sekä niiden olemassaoloa. Etuna on, että asukkaan poistaessa palovaroittimen paikaltaan, sen pariston loppuessa tai palovaroittimen muuten vikaantuessa tulisi se myös muiden kuin asukkaan tietoon. Lisäksi palovaroitin tulisi uusia viimeistään 10 vuoden iässä, ellei valmistaja ole osoittanut lyhyempää käyttöikää (Meurman 2018, s. 22). Myös tätä olisi mahdollista monitoroida IoT:n avulla. Kiinteistön omistajalla voidaankin katsoa olevan oikeus palovaroittimien toimintakunnon seurantaan liittyen, jos se pelastuslain (379/2011) 14 §:n omatoimiseen varautumiseen liittyvään riskianalyysin perusteella katsoo sen tarpeelliseksi. Kiinteistön omistajalla kuten haltijallakin on velvollisuus ehkäistä vaaratilanteiden syntymistä. Esitetty ratkaisu luonnollisesti toisi parannusta paloturvallisuuden tasoon. Erityisesti älykkäiden palovaroittimen hyödyt tulisivat esiin vuokrakerros- ja rivitaloissa, joissa kiinteistön omistaja vastaa rakennuksesta kokonaisuutena. Tutkimustuloksissa tuli esille, että palovaroitin tulisi velvoittaa sijoittamaan asunnon jokaiseen tilaan, jotta tulipalo havaittaisiin nopeasti. Nykyinen vaatimustaso palovaroittimien määrästä asuinhuoneistoissa ei katsottu riittäväksi.

Kiinteistön omistaja pystyisi helposti edellyttämään palovaroittimen saattamista toimintakuntoon, jos vikaantumisia tulisi esiin. Monitoroinnin tuoman hyödyn lisäksi IoT-teknologiaa hyödyntämällä voidaan tehokkaasti varoittaa muita talon asukkaita alkaneesta palosta. Palohälytys voisi ohjautua muiden asuinhuoneistojen palovaroittimiin, porrashuoneen palovaroittimiin tai talon asukkaiden älypuhelimiin. Vastaavanlainen esimerkki tuli esille teemahaastattelujen yhteydessä. Lisäksi laitevalmistajat ovat osoittaneet kiinnostusta älykkäiden palovaroittimien tuomiin mahdollisuuksiin taloyhtiöiden ympäristössä.

6.3.2 Pelastusviranomaiselle reaaliaikaisen tilannekuvan välittäminen

Tuloksissa tuli esille, että kiinteistön kiinteistöautomaatiosta ja paloturvallisuustekniikasta saatua tietoa olisi tarpeellista jakaa langattomasti alueen pelastusviranomaiselle paloilmoituksien yhteydessä paremman tilannekuvan aikaansaamiseksi. IoT-teknologiaa pidettiin tiedon välitykseen hyvin soveltuvana, koska se mahdollistaa reaaliaikaisenkin tiedon välittämisen. Suomessa pelastusviranomaiset saavat paloilmoituksen tai tulipalon sattuessa tietoa ensisijaisesti hätäkeskuksen kautta. Hätäkeskus hälyttää paikalle pelastuslaitoksen yksiköitä ennakkoon määriteltyjen vasteiden mukaisesti.

Rakennuksen ollessa suojattu automaattisella paloilmoitinlaitteistolla tai sammutuslaitteistoilla välittyy tieto paloilmoituksesta luotettavalla yhteydellä hätäkeskukseen. Yhtenä ongelmana on se, että paloilmoituksen yhteydessä saatava tieto on hyvin vähäistä, johon sisältyy yleensä vain paloilmoituskohteen nimi ja osoite. Lisätietoina voi tietyissä tapauksissa olla mainittuna tarkennuksena rakennuksen numero, nimi tai rakennuksen osa. Tämä on yleistynyt varsinkin isoissa kiinteistöissä, joissa on useita rakennuksia. Lisäksi pelastusviranomainen voi saada lisätietoja hätäkeskuksesta, jos paloilmoituskohteesta soitetaan hätäkeskukseen tai hätäkeskus saa kiinni paloilmoitinlaitteiston hoitajan tai sen vastuuhenkilön. Tiedon saaminen perustuu siis pitkälti hätäkeskuksen kautta saatavaan informaatioon, jonka vuoksi pelastusviranomaisella on usein hyvin rajalliset tiedot paloilmoituksesta syystä ja mahdollisesta tulipalon kehittymisestä. Jos lisätietoja ei ole saatavilla, saadaan tilanne selville vasta pelastuslaitoksen suoritettua tiedustelua alueelle, josta palohälytys on tullut. Pelastusviranomaiset ovat laatineet tiettyihin kohteisiin johtamisen tueksi erillisiä kohdekortteja, joissa on esitetty tärkeimpiä tietoja kiinteistöistä (Päijät-Hämeen pelastuslaitos 2018). Juuri muuta tietoa pelastusviranomainen ei voi ennen kohteeseen tuloa hyödyntää, vaikka se nopeuttaisi sammutus- ja pelastustoimenpiteitä.

Pelastusviranomaisen tilannekuvan parantamiseksi Suomessa toteutettiin 2000-luvulla PARK-hanke, jonka lähtökohtana oli tehostaa tiedon välittämistä alueen pelastusviranomaiselle. PARK hankkeesta on kerrottu tarkemmin kappaleessa 3.3. Hanketta voidaan IoT-teknologian näkökulmasta pitää pioneerihankkeena, koska tiedonsiirto tapahtui Internet-verkon yli sekä siinä yhdistettiin useista eri laitteista ja lähteistä kerättyä tietoa.

Kehitetty PARK-järjestelmä ei aiheuttanut kiinnostusta eikä se siten valmistunut kaupalliseksi tuotteeksi, vaikka järjestelmällä saatiin selkeää hyötyä paloturvallisuuden parantamiseksi. Mitään vastaavaa järjestelmää ei ole tullut sen jälkeen Suomen markkinoille. PARK-järjestelmää vastaavalle sovellukselle voidaankin katsoa olevan entistä enemmän tarvetta. Suomessa on viime vuosina alettu rakentaa entistä korkeampia ja kooltaan suurempia rakennuksia. Suurissa kiinteistömassoissa esimerkiksi paloturvallisuutta parantavilla laitteistoilla tehty paloturvallisuuden parannus on toteutettu siihen pisteeseen, ettei kustannustehokkaita keinoja paloturvallisuuden parantamiseksi juuri enempää ole. Voimassa oleva rakentamiseen liittyvä lainsäädäntö sekä paloturvallisuutta parantavia laitteistoja koskevat standardit edellyttävät niiltä vain palotiedon välittämistä hätäkeskukseen. Mitään muuta tietoa ei ole tarvetta toimittaa.

Pelastuslain (379/2011) 14 §:n 1 momentin kohdan 4 mukaan esimerkiksi kiinteistön omistajan on tulipalossa tai vaaratilanteen aikana ryhdyttävä toimenpiteisiin pelastustoiminnan helpottamiseksi. Pelastustoimintaa helpottaviksi toimenpiteiksi voidaan katsoa esimerkiksi reaaliaikaisen informaation välittäminen alueen pelastusviranomaiselle muunkin kuin hätäkeskuksen kautta. Välitetyn reaaliaikaisen informaation avulla voidaan helpottaa pelastustoimenpiteitä. Tämän vuoksi olisikin tarpeellista kehittää uutta sovelluspohjaa, jossa kiinteistön eri turva- ja kiinteistöautomaatiojärjestelmät sekä tietokannat voidaan integroida yhteen ja välittää niistä saatavaa tietoa tehokkaasti täsmäraporttina alueen pelastusviranomaiselle. Tätä informaatiota voitaisiin alkaa analysoida sekä hyödyntää heti paloilmoituksen alusta alkaen pelastustoiminnan johtamisen tueksi, millä saataisiin nopeutettua sammutus- ja pelastustoimenpiteitä kohteessa. IoT-teknologian avulla datan välittäminen ja hyödyntäminen voidaan toteuttaa tehokkaasti. Digitalisaation yleistymisen myötä tarvittavaa informaatiota on mahdollista tuottaa visuaaliseen muotoon esimerkiksi rakennuksen 3D-kuvissa tai digitaalisessa kaksosessa.

Tutkimustuloksissa tuli myös esille, että pelastusviranomaisten tulisi lähitulevaisuudessa olla aktiivisesti tuomassa esiin omaa kantansa siitä, miten rakennuksista välitettyä dataa otetaan vastaan. Esille tuotavia asioita olisivat esimerkiksi miten dataa olisi heille helpointa siirtää, mitkä ovat tietoturvallisuuden vaatimustasot sekä millä sovelluspohjalla datan hyödyntäminen tapahtuisi. Lisäksi tutkimustuloksissa korostui vahvasti se asia, että pelastusviranomaiselle suunnatun käyttöliittymän tulisi olla helppokäyttöinen. Väli-

tetyn tiedon tulisi olla helposti ja tehokkaasti hyödynnettävissä onnettomuustilanteen johtamisen tukemiseen sekä onnettomuuden jälkiselvittelyn yhteydessä.

6.3.3 Talotekniikan olosuhdeanturoinnin hyödyntäminen

Tulevaisuudessa on mahdollista hyödyntää rakennuksien talotekniikan anturointia, laitteita ja järjestelmiä myös tulipalojen havaitsemisessa tai tulipalojen leviämisen arvioinnissa ja ennustamisessa. Markkinoilla on olemassa kiinteistönhallintajärjestelmiä, joiden kautta eri järjestelmiä voidaan integroida yhteen sekä hallita kaikkia eri järjestelmiä yhdestä käyttöliittymästä. Rakennuksesta saatua tietoa voidaan ohjata yhteen paikkaan sekä saada siten monenlaista tietoa rakennuksen olosuhteista sekä niissä tapahtuvissa muutoksista. Tätä tietoa olisi mahdollista hyödyntää paloturvallisuutta parantavien laitteistoista tulevan tiedon rinnalla. Kiinteistöautomaatiojärjestelmän tarjotessa avoimia rajapintoja sekä sen ollessa hyvin skaalautuva, voi se mahdollistaa talotekniikan anturiteknologian hyödyntämisen jälkikäteenkin paloturvallisuuden parantamiseksi. Tulevaisuudessa IoT-pohjaisten kiinteistöautomaatiojärjestelmien positiiviset käyttökokemukset voivat vauhdittaa järjestelmäintegraatiota sekä hyödyntää eri järjestelmiä yhteen.

Rakennuksen tai kiinteistön kameravalvonnan hyödyntäminen on yksi parhaimmista keinoista selvittää tilannetta palohälyttävällä alueella. Paloilmoitinjärjestelmän sekä kameravalvonnan integrointeja yhteiseen käyttöliittymään on jo toteutettu. Palohälytyksen sattuessa hälyttävää aluetta on mahdollista tarkkailla kameravalvontaa hyödyntäen tietokoneelta käsin. Tulevaisuudessa tämä on mahdollista tehdä mobiilisovelluksen kautta sekä hyödyntäen enenevässä määrin langatonta tiedonsiirtoa. Vastaavat järjestelmät tulevat todennäköisesti yleistymään myös asuinrakennusten kodinturvajärjestelmissä sekä kodin automaatiojärjestelmissä.

Tulipalon havaitsemiseen olisi mahdollista hyödyntää kiinteistöautomaation osana olevia lämpötilan, CO^2 ja ilmanpaineen mittaukseen liittyviä anturointeja sekä muita pelkkää tilatietoa välittäviä antureita. Tietoa hyödyntämällä voitaisiin saada varmuutta tulipalon syttymisestä, sen kehittymisestä sekä palo-osastoinnin varmistumisesta. Tähän vaikuttaa oleellisesti se, että miten usein näistä antureissa mittaustietoa välitetään esimerkiksi pilvipalveluun. Mittaustiedon tulee olla lähes reaaliaikaista, jotta sitä kannattaa hyödyntää tulipalojen havaitsemiseen.

Tulipalon havaitsemisessa ei ole esimerkiksi juuri hyödynnetty ilmanpaineen vaihteluun perustuvaa mittausta. Vuosina 2015-2016 tehtiin Suomessa huoneistopalon paineenhallintaan liittyvää tutkimusta. Tutkimuksen perusteella voitiin todeta, että tiiviissä huoneistossa tulipalon alkuvaiheessa asuinhuoneistoon voi muodostua suuri ylipaine hyvinkin nopeasti. Palon kehittyessä ylipaine alkaa tasoittua. (Hostikka & Janardhan 2017, s. 13-14). Jos rakennuksen sisätiloissa tehdään ilmanpaineeseen perustuvaa mittausta, voitaisiin tätä tietoa hyödyntää tulipalon havaitsemiseen sekä tulipalon kehittymisen arviointiin ja ennustamiseen. Rakennuksien anturointia hyödyntämällä on mahdollista varmistua myös passiivisten palontorjuntalaitteiden toimivuudesta. Esimerkiksi oviantureiden avulla on mahdollista saada selvyys ovatko palo-ovet sulkeutuneet. Samalla mahdollistetaan palo-ovien käytön aikainen seuranta siitä, miten usein niitä pidetään auki.

6.3.4 Onnettomuuksien ehkäisy

IoT-teknologiaa hyödyntämällä on mahdollista estää onnettomuuksien syntymistä. IoT-antureista ja –laitteista kerättyä dataa voidaan hyödyntää onnettomuuksien ehkäisemiseksi suoraan tai välillisesti. Suomessa rakennuksien etäluettavista sähkömittareista kerättyä dataa hyödynnetään pelastuslaitosten toimesta palontutkinnan yhteydessä. Palontutkinnan yhtenä tavoitteena on vastaavien onnettomuuksien ehkäiseminen ja vahinkojen rajoittaminen (pelastuslaki 379/2011 41§). Sähkönkulutukseen liittyvä tieto voi olla tietyissä tapauksissa merkittävässä roolissa selvitettäessä tulipalon syttymissyytä. Syttymissyyn selviämisen perusteella on mahdollista estää vastaavien onnettomuuksien syntyminen. Tulevaisuudessa IoT-antureiden ja -laitteiden yleistyessä voidaan kerättyä dataa hyödyntää entistä tehokkaammin onnettomuuksien ehkäisyyn liittyvässä toiminnassa.

Rakennuksen eri olosuhteista, ihmisten sijainnista, laitteiden ja järjestelmien tilatiedoista kerätään yhä enemmissä määrin tietoa. Tämän datan hyödyntäminen mahdollistaa yhä tarkemman tulipalon tai onnettomuuden kehittymisen analysoinnin. Esimerkiksi jotkut IoT-palovaroittimet tallentavat dataa pilvipalveluun havaitessaan alkaneen tulipalon. Tämä data voi olla arvokasta tietoa palontutkinnalle. Tällaista dataa ei ole ollut mahdollista saada aikaisemmin. Tuloksissa tuli esille, että IoT-laitteista kerättyä dataa voitaisiin palon- ja onnettomuustutkinnan lisäksi hyödyntää myös muussa onnetto-

muuksien ehkäisytyössä kuten pelastuslaitoksen valvontatoiminnassa sekä kansallisen riskienhallinnan kehittämisessä.

Onnettomuuksia voidaan ennalta ehkäistä IoT:n avulla myös suoraan. Tulipalon alkuvaiheessa laite- ja järjestelmäintegraatioilla on mahdollista estää tulipalon kehittyminen. Esimerkiksi palovaroittimen tai automaattisen paloilmoittimen havaitessa alkanut tulipalo voidaan järjestelmäintegraatiota hyödyntämällä katkaista sähkövirta tietyistä laitteista. Vastaavia kiinteisiin asennuksiin perustuvia järjestelmiä on ollut olemassa jo vuosia, mutta tulevaisuudessa tähän todennäköisesti hyödynnetään IoT:tä yhä useammin. Lisäämällä rakennusten älykkyyttä ja anturointia on mahdollista, että ympäristössä tapahtuvat muutokset tunnistetaan entistä tarkemmin ja tehokkaammin. Näin voidaan luoda entistä älykkäämpiä ympäristöjä, joissa ihmisten tekemät virheet ja unohdukset havaitaan jo ennen kuin onnettomuus tai tulipalo saa alkunsa. Suurin osa rakennuksissa syttyneistä tulipaloista aiheutuu juuri ihmisen toiminnasta (Pelastusopisto 2017b, s.14). Älykkäässä ympäristössä myös datan kerääminen ja sen analysointi on entistä helpompaa, mikä mahdollistaa uuden tiedon jalostamisen. Yhtenä esimerkkinä älykkäistä ratkaisuista voidaan ottaa esille toimistorakennusten sisäpaikannukseen liittyvät pilottihankkeet. Niissä on mahdollista paikantaa työntekijöiden sijainti. Tätä tietoa hyödyntämällä olisi tulipalotilanteessa mahdollista varmistaa, että kaikki työntekijät ovat poistuneet rakennuksesta sekä saada selville miten nopeasti ihmiset toimivat ja poistuvat rakennuksesta tulipalon tai palohälytyksen sattuessa.

Onnettomuuksien ehkäisyn näkökulmasta IoT-ratkaisuilla voidaan viestiä ja varoittaa rakennuksessa tai naapurirakennuksessa oleskeleville henkilöille alkaneesta tulipalosta tai muusta onnettomuudesta. Esimerkiksi asuinkerrostalossa olisi mahdollista varoittaa älypuhelinsovelluksen kautta asukkaille alkaneesta tulipalosta tai muusta vaarasta.

6.4 IoT-teknologian avulla saatavat kustannussäästöt

Talotekniikan IoT-ratkaisuilla voidaan todistetustii saada säästöjä rakennusten elinkaarikustannuksista. Sama voidaan katsoa pätevän osin myös paloturvallisuutta parantavien laitteistojen elinkaarikustannuksiin. Tämä korostuu ennen kaikkea suurissa kohteissa tai niissä, joissa on paljon paloturvallisuustekniikkaa. Kustannussäästöjen ei kuitenkaan voida katsoa olevan niin merkittäviä kuin mitä saadaan muussa talotekniikassa. Säästöjä

voidaan saada erityisesti automaattisista paloilmoitinlaitteistoista tai sammutuslaitteistoista, koska niiden huoltoon ja kunnossapitoon liittyy muita paloturvallisuutta parantavia laitteistoja kovempi vaatimustaso. Automaattisissa paloilmoitinjärjestelmissä etävalvonta tai -hallinta on ollut mahdollista jo useiden vuosien ajan esimerkiksi client server – arkkitehtuurimalliin toteutettuna, joten siltä osin kustannussäästöjä on ollut mahdollista saada jo ilman IoT-ratkaisujakin.

Pienemmissä kiinteistöissä, kuten asuinrakennuksissa, ei saada kustannussäästöjä uutta teknologiaa lisäämällä, koska esimerkiksi asuinrakennuksissa palovaroittimien kunnossapidon ja huollon voi suorittaa yleensä asukas itse. Älyteknologia on perinteistä teknologiaa kalliimpaa. Esimerkiksi perinteisten paristokäyttöisten palovaroittimien korvaaminen älypalovaroittimilla lisää kustannuksia huomattavasti, koska älypalovaroittimen hinta on yli kymmenkertainen perinteiseen palovaroittimeen verrattuna. Lisäksi tiedonsiirtoon tai ohjaukseen rakennettava tiedonsiirtoinfrastruktuuri voi lisätä kustannuksia entisestään. Tähän voi olla ratkaisuna LPWAN-verkojen hyödyntäminen. LPWAN-verkon käyttö tiedonsiirrossa voi tuoda kustannussäästöjä, vaikka niihin liitetyistä laitteista peritäänkin vuosimaksuja. Verkkojen etuna perinteisiin langattomiin teknologioihin nähden on se, ettei rakennuksen sisälle tarvitse rakentaa kallista tiedonsiirtoinfrastruktuuria (Raza et al 2017, s. 855-856). Yksittäisten IoT-anturin, kuten älypalovaroittimen, asentaminen rakennukseen on helppoa ja edullista, jos rakennuksessa ei ole käytössä muuta tiedonsiirtoinfrastruktuuria.

Kehitystä on ollut myös automaattisten paloilmoitinlaitteistojen kohdalla, jotka ovat siirtyneet IoT-aikaan. Tästä esimerkkinä ovat Siemensin kiinteistönhallintajärjestelmä Desigo CC ja Schneider Electric EcoStructure Fire Expert online-sovellus. Kummankin valmistajan järjestelmissä paloilmoitinlaitteistoa on mahdollista monitoroida ja hallita mobiilisti etäyhteydellä. Etäyhteyden avulla paloilmoitinlaitteistojen huolto- ja kunnossapitotoiminnassa on mahdollista saada kustannussäästöjä esimerkiksi tekemällä irtikytkentöjä etäyhteydellä mistä tahansa. Näin ollen ei ole tarvetta mennä tekemään irtikytkentöjä perinteisesti rakennuskohtaiselta paloilmoitinkeskukselta. Tämä vähentää paloilmoitinlaitteiston hoitajan käyntejä kohteessa ja näin tietyissä tapauksissa vähentää myös kustannuksia (Siemens 2017; Schneider Electric 2017).

Paloilmoitinlaitteistojen IoT-ratkaisuista hyötyvät myös laitteistojen valmistajat, laitevalmistajien partnerit sekä paloilmoitinhuoltoliikkeet. Kustannussäästöt näille toimijoille syntyvät etupäässä operatiivisen työn tehostamisesta. Paloilmoitinlaitteiston asentamisen yhteydessä järjestelmän oikeaoppinen asennus on mahdollista tarkastaa sekä suorittaa paloilmoitinkeskuksen konfigurointi etäyhteyttä hyödyntäen. Perinteisesti nämä toimenpiteet on tehty fyysisesti paloilmoitinkeskukselta. Pilvipalvelun etuna on taas se, että viimeisin konfigurointi jää pilvipalveluun talteen tulevia muutoksia tai uudelleen ohjauksia silmällä pitäen.

Kun kiinteistön omistajalla ja laitevalmistajien partnereilla tai paloilmoitinhuoltoliikkeillä on huoltosopimukset paloilmoitinlaitteiston huolto- ja kunnossapidosta, on näillä toimijoilla mahdollista suorittaa järjestelmään ennakoivaa ja keskitettyä huoltotoimintaa siten, ettei kiinteistön omistajan tarvitse puuttua sen suorittamiseen. Tämän saman hyödyn Tuomisaari (2017, s.46) on havainnut sammutuslaitteistojen IoT-ratkaisuja käsittävässä diplomityössään. Mobiilisovelluksella partnerit ja huoltoliikkeet voivat monitoroida järjestelmiä hyvin helposti sekä näkevät heidän huoltosopimuksensa alaiset kohteet jopa yhdessä käyttöliittymänäkymässä. Tämän avulla huollosta ja kunnossapidosta vastaavat voivat suunnitella töiden suorittamista ennakkoon. Kiinteistön omistajalle tästä voi tulla pitkällä aikavälillä kustannussäästöjä, koska laitteiston huoltaminen voi tulevaisuudessa muuttua siten, että järjestelmää huolletaan vain silloin, kun on tarve.

Paloilmoitinlaitteistosta on vuosikymmenien aikana otettu ulos ohjaukseen liittyvää tietoa. Tämän toiminnan paloilmoitinlaitteistoa koskevat standardit ovat mahdollistaneet. Tutkimustuloksissa nousi esille tahto hyödyntää paloilmoitinlaitteistoon liitettyjen ilmaisimien anturointia myös kiinteistöautomaation ohjauksissa ja datan keräämisessä entistä tehokkaammin. Paloilmaisimissa anturointi on lisääntynyt monikriteeri-ilmaisimien yleistymisen myötä. Paloilmoitinjärjestelmän etuna on, että se kattaa yleensä kaikki rakennuksen tilat, joten järjestelmän kautta on mahdollista kerätä laajasti dataa rakennuksen eri tilojen olosuhteista, esimerkiksi lämpötilasta. Näin ollen rakennukseen ei tarvitsisi tehdä erillistä anturointia ja näin saataisiin aikaan kustannussäästöjä kiinteistön rakennusautomaatiosta.

IoT-teknologiaa käyttämällä voidaan saada kustannussäästöjä laitteiden asennusten yhteydessä, koska laitteet toimivat yleensä omalla virtalähteellä eikä kaapelointia näin tarvitse tehdä. Tästä johtuen asennukset ovat halvempia ja nopeampia suorittaa. Näin ollen rakenteisiin ei tarvitse tehdä aukkoja tai miettiä kaapeleiden näkyviin jäämistä. Edut tulevat kysymykseen varsinkin olemassa olevissa kohteissa. (Oh et al 2013, s. 2). On kuitenkin huomioitava, että kaapeloinnin puuttuminen tuo lisäkustannuksia huolto- ja kunnossapitotoiminnalle, joten pitkällä aikavälillä laitteiden paristojen vaihtamiskustannukset voivat tulla kalliiksi.

6.5 IoT-teknologiaan liittyvät uhkatekijät

IoT:n suurimmiksi uhkatekijöiksi voidaan katsoa puutteet tieto- ja kyberturvallisuudessa sekä tietosuojaan liittyvissä asioissa. Puutteet näissä uhkatekijöissä tulivat vahvasti esille niin tutkimustuloksissa kuin kirjallisuudessa. Kyseiset uhkat ja riskit katsottiin olevan kuitenkin hallittavissa, eikä niistä näin ollen muodostu estettä IoT:n hyödyntämiselle. Uhkiin tulee suhtautua vakavasti, mikä edellyttää huolellista ennakkoon varautumista, kun henkilö- ja paloturvallisuuteen liittyviä laitteita tai järjestelmiä yhdistetään Internetiin tai tiedonsiirto tapahtuu langattomasti. Tietoturvallisuudessa ollessa puutteita on henkilö- ja paloturvallisuuslaitteistoihin mahdollista kohdistaa vastaavanlaisia kyberhyökkäyksiä, kuten kiinteistönautomaatiojärjestelmiin on vuosien saatossa toteutettu. Pahimmillaan kyberhyökkäykset voivat aiheuttaa omaisuuden tuhoutumista tai välillisesti jopa ihmishenkien menetyksiä (Lindqvist & Neumann 2017, s 26-28).

On siis erityisen tärkeää, että tietoturvallisuus huomioidaan kaikkien eri järjestelmäkokonaisuuteen kuuluvien toimijoiden toimesta. Turvallisuuden varmistamisessa tulee erityisesti ottaa huomioon ihmisten toiminta, koska ihmisen tahaton tai tahallinen käytös muodostaa merkittävimmän riskin tieto- ja kyberturvallisuuden toteutumiselle. Rathinavel et al (2017, s. 1-2) artikkelissa on mainittu, että tietoturvallisuus on varmistettava IoT-arkkitehtuurin kaikissa kerroksissa, joka siten kattaa laajalti suurimman osan kokonaisuudesta. Erityisesti laitevalmistajien rooli ja vastuu tietoturvallisuuteen liittyen tuli eri lähteissä vahvasti esille. Riittävä tietoturva tulee huomioida laitteiden valmistuksen yhteydessä sekä tarjoamalla aktiivisesti ohjelmistopäivityksiä tietoturvapuutteita havaittaessa. Laitteistoihin liittyvät tietoturvallisuuspuutteet eivät ole olleet aina laite-

valmistajien huolenaiheena (Lindqvist & Neumann 2017, s 27; Liikenne- ja viestintävaliokunta 2017, s.1-7).

Laitteiden ja sovelluksien hallinta etäyhteydellä on yksi IoT:n tärkeimmistä ominaisuuksista. Puutteet etähallinnassa ja siihen liittyvän ohjeistuksen toteutuksessa, mahdollistavat erilaiset väärinkäytökset, mikä aiheuttaa taas riskin niin tietoturvallisuuteen kuin tietosuojaankin liittyen. Etähallinnan tietoturvapuutteet mahdollistavat hyökkäykset järjestelmää kohtaan, kun taas ohjeistukset datan käsittelyssä aiheuttavat tietosuojariskin (Miorandi et al 2012, s. 1507; Chan & Perrig 2003, s.103-104). Tietosuojaan liittyvät asiat ovat olleet vahvasti esillä viime vuoden ajan, koska EU:n tietosuoja-asetus astuu voimaan vuoden 2018 toukokuussa. Tietosuoja-asetus antaa perusteet kaikkeen henkilötietojen käsittelyyn. Hyödynnettäessä IoT-teknologiaa paloturvallisuutta parantavissa laitteistoissa, on niiden kautta mahdollista kerätä dataa asumisympäristöstä ja sitä kautta myös ihmisten tottumuksista jopa siten, etteivät asukkaat edes välttämättä tiedä tai tiedosta sitä (Mäkinen 2015, s.262).

Älykkäissä palovaroittimissa erilaisten antureiden määrä on selvästi lisääntymään päin, minkä vuoksi niiden avulla on mahdollista kerätä dataa paljon tehokkaammin ja hyödyntää dataa myös muissa kodin automaatiojärjestelmissä tai niiden integraatioissa. Kyseisen datan väärinkäytön perusteella on mahdollista saada selville ihmisten tottumuksia, jotka liittyvät vahvasti yksityisyyden suojan piiriin. Tutkimustuloksissa tuli esille, että on tärkeää etukäteen miettiä, onko dataa tarvetta kerätä, kenelle sitä jaetaan ja kenen sitä tarvitsee hyödyntää. Mäkinen (2015) on tuonut artikkelissaan esille samoja asioita, kuten sen, että on tarpeen etukäteen miettiä miksi dataa kerätään ja mihin tarkoitukseen (Mäkinen 2015, s.273).

6.6 Paloturvallisuutta parantavien laitteistojen standardit ja rajapinnat

Paloturvallisuutta parantavat laitteistot ovat yleisesti olleet näihin päiviin asti suljettuja järjestelmiä. Tähän on vaikuttanut vahvasti niitä koskeva tarkka standardointi. Paloturvallisuutta parantavien laitteistojen standardit muodostavat minivaatimustason siitä, mitä vaatimuksia järjestelmään asennetuilla komponenteilla tulee olla sekä miten järjestelmät tulee suunnitella ja asentaa. Tutkimustulosten ja kirjallisuuskatsauksen perusteella voidaan todeta, että vaikka vaatimustason ollessa näissä laitteistoissa korkea, eivät

standardit kuitenkaan estä uuden teknologian hyödyntämistä paloturvallisuutta parantavissa laitteistoissa tai järjestelmissä. Standardien katsottiin tosin kehittyvän hyvin hitaasti, minkä vuoksi teknologian kehitys voi mennä standardien edelle. Tämä toisaalta hidastaa uuden teknologian hyödyntämistä, myös IoT:n. Markkinoille tulleet uudet ratkaisut ovat hyvä osoitus siitä, miten älykkyyttä on paloturvallisuutta parantaviin laitteistoihin lisätty. Älykkyydellä ei ole korvattu mitään standardien vaatimusten mukaista, vaan älykkyyttä on tuotu standardien vaatimustason lisäksi. Samalla laitteesta on voitu tehdä entistä hyödyllisempi tai kiinnostavampi, koska yhtä laitetta voidaan hyödyntää myös muuhunkin kuin pelkkään paloturvallisuuden varmentamiseen. Tästä hyvänä esimerkkinä on Nest Protect älypalovaroitin, joka kykenee keskustelemaan Nest-tuoteperheen muiden laitteiden kanssa ja näin sitä on mahdollista hyödyntää kiinteistön muuhunkin toimintaan tai ohjauksiin (Nest Protect 2018).

Älykkyyden ja teknologian lisäämiseen yleensäkin on huomioitava se, ettei lisäominaisuuksilla vaaranneta laitteen päätoimintoa kuten palovaroittimessa tulipalon havaitsemista ja riittävän tehokkaan varoitusäänen antamista. On selvää, etteivät standardit tule lähitulevaisuudessakaan mahdollistamaan kaikkien paloturvallisuutta parantavien laitteistojen toteuttamista kokonaisuudessaan IoT-ratkaisuna. Toisaalta se ei ole myöskään tarkoituksenmukaista tai välttämätöntä. On muistettava, että paloturvallisuutta parantavien laitteistojen tärkein ominaisuus on toimivuus ja toimintavarmuus niiden havaitessa tai rajoittaessa tulipalo, varoitettaessa ihmisiä, estäessä lisävahinkojen syntymistä sekä tehostaessa sammutus- ja pelastustoiminnassa onnistumista.

IoT-teknologian hyödyntäminen muodostaa henkilö- ja paloturvallisuuslaitteistoille uuden uhkan, puutteet tietoturvassa ja tietosuojaan liittyvissä asioissa. Kuten on todettu, älykkyys tulee lisääntymään myös näissä laitteissa ja järjestelmissä. Onkin tarpeellista, että nämä tekijät huomioidaan henkilö- ja paloturvallisuuteen liittyvien laitteiden standardien päivityksien yhteydessä. Standardeissa tultaisiin mainitsemaan etenkin tietoturvallisuuteen liittyvät asiat, koska ne muodostavat tulevaisuudessa laitteistolle selvän riskitekijän. Standardien myötä tietoturvallisuuden vaatimukset tulisivat laitevalmistajien huomioitavaksi jo laitteistoja ja järjestelmiä kehittäessä.

Tutkimustulosten perusteella paloturvallisuutta parantavien laitteistojen rajapintojen tulisi olla entistä avoimempia, jotta erilaiset järjestelmäintegraatiot olisivat helpompia ja kustannustehokkaampia toteuttaa. Lisäksi dataformaattien tulisi olla sellaisia, että tiedonsiirto järjestelmien välillä onnistuu mutkattomasti. Liian suljetut järjestelmät voidaan katsoa muodostavan yhden IoT-teknologiaan liittyvän uhkakuvan, jos järjestelmiä ei voida integroida tulevaisuudessa helpommin yhteen. Rajapintoihin ja tiedonsiirtoon liittyvä standardointi olisi tarpeen, koska sen katsottiin ratkaisevan myös tietoturvallisuuteen liittyvät ongelmat. Laajoissa järjestelmäintegraatioissa järjestelmien yhteentoimivuus tulee huomioida jo suunnitteluvaiheessa, jotta varmistetaan järjestelmän toimivuus. Lisäksi on arvioitava miten ylläpidon aikana tehtävät järjestelmäpäivitykset tulevat vaikuttamaan koko järjestelmän toimivuuteen. Suomessa on sattunut tapauksia, joissa kiinteistön ohjausjärjestelmät eivät ole toimineet toivotulla tavalla, kun yhteentoimivuuteen ei ole kiinnitetty riittävästi huomiota suunnittelu- ja toteutusvaiheessa.

Talotekniikan osalta Ihasalo et al (2017) ovat päätyneet raportissaan samanlaisiin tuloksiin. Heidän talotekniikan avoimiin rajapintoihin ja tiedonkuvauksiin liittyvän raportin mukaan avoimuudella on mahdollista lisätä rajapinnan yhteensopivuutta sekä skaalautuvuutta. Avoimuuden avulla saavutetaan parempi luotettavuus sekä mahdollisesti jopa kustannusten pienenemistä. Standardointi parantaisi myös tietoturvallisuuden toteutumista. Raportissa tuli lisäksi esille, että tulevaisuudessa rajapintaprotokollille ja tiedonkuvausmenetelmille vaatimuksia tulevat asettamaan myös rakennusten liittäminen muiden alojen laitteisiin. (Ihasalo et al. 2017, s. 4-6). Paloturvallisuutta parantavat laitteistot voisivat olla esimerkiksi tällaisia laitteistoja. Olisikin tarpeellista, että järjestelmien avoimuus otettaisiin paremmin huomioon suunnittelu- ja hankintavaiheessa.

6.7 Jatkotutkimusehdotukset

Suoritetun tutkimuksen perusteella esille nousi kolme jatkotutkimusehdotusta. Tämän diplomityön yksi tavoitteista oli tutkia, miten IoT-teknologiaa on hyödynnetty paloturvallisuuden kehityksessä eri Pohjoismaissa. Kyseinen tutkimus ei onnistunut, koska vastausprosentti jäi lomakehaastattelussa hyvin alhaiseksi. Ensimmäinen jatkotutkimusehdotus on suorittaa vastaavanlainen tutkimus uudestaan. Tutkimusta olisi tosin syytä laajentaa, jos se suoritetaan pro gradun tai diplomityön ainoana tutkimuksena.

Pohjoismaihin kohdistetun tutkimuksen perusteella olisi mahdollista selvittää ovatko äly- ja IoT-ratkaisut yleistyneet eri maissa samaan tahtiin vai löytyykö niissä erityisiä poikkeuksia. Tutkimuksen avulla voisi löytyä jo hyväksi havaittuja ratkaisuja tai kiinnostavia pilottikohteita muista Pohjoismaista.

Toisena jatkotutkimusehdotuksena olisi suorittaa tutkimusta varsinkin kuluttajille suunnattuihin paloturvallisuuteen liittyviin IoT-laitteisiin, kuten palovaroittimiin. Ennen kaikkea tutkimusta olisi syytä keskittää esimerkiksi laitteiden käyttöönotettavuuteen, toimintaominaisuuksiin, hallittavuuteen, datan keräämiseen sekä tietoturvallisuuteen liittyen. Palovaroitin on asuinrakennuksissa pakollinen turvalaite, minkä vuoksi voidaan olettaa, että tulevaisuudessa älykkäiden palovaroittimien määrä tulee asuinrakennuksissa lisääntymään. Ihmisiä olisi tarpeen valistaa uuden teknologian mahdollisuuksiin, jotta he osaisivat vaatia sitä esimerkiksi rakentamisen yhteydessä. Markkinoilla onkin jo useita erimallisia älykkäitä palovaroittimia, jotka poikkeavat toisistaan esimerkiksi palovaroittimessa olevien antureiden määrän tai siinä käytettävän tiedonsiirtomenetelmän perusteella. Uudet älykkäät palovaroittimet sisältävät siis toimintoja, joihin kuluttajat eivät ole perinteisissä paristokäyttöisissä tai sähköverkkoon kytketyissä palovaroittimissa tottuneet. Suoritetun tutkimuksen perusteella voitaisiin laatia valistusmateriaalia, jossa tuotaisiin esiin perusteita älykkäistä palovaroittimista, niiden tuomista mahdollisuuksista sekä ennen kaikkea muistuttaa huomioimaan tietoturvaan ja tietosuojaan liittyvät asiat palovaroittimien käytössä ja niiden hallinnoinnissa.

Kolmas jatkotutkimusehdotus liittyy hieman toiseen jatkotutkimusehdotukseen. IoT-teknologiassa on hyvin yleistä, että IoT-laitteet tai –anturit ovat paristokäyttöisiä. Paloturvallisuutta parantavien IoT-laitteiden virrankulutusta tulisi tutkia tarkemmin. Tällä tavoin voitaisiin saada selvyyttä siitä, pitävätkö valmistajien antamat paristojen tai akkujen kestävyys paikkaansa. Tutkimus olisi tarpeen, jotta voitaisiin arvioida tarkemmin järjestelmien toimintavarmuutta sekä niihin liittyvää manuaalista huoltotarvetta. Paristojen tai akkujen vaihtovälin perusteella olisi mahdollista arvioida esimerkiksi huoltotoimintaan meneviä kustannuksia pitkällä aikavälillä.

7 YHTEENVETO

Suomessa tulipaloissa menehtyy vuosittain noin 70-80 ihmistä sekä loukkaantuu useita satoja ihmisiä. Suurin osa kuolemaan johtaneista tulipaloista tapahtuu asuinrakennuksissa. Lisäksi rakennuspaloista aiheutuu vuosittain noin 120 miljoonan omaisuusvahingot (Pelastusopisto 2017b, s. 29-30). Tulipalojen vaikutukset huomioiden, ei asuinrakennusten paloturvallisuutta parantavissa laitteistoissa ole viimeisen kymmenen vuoden aikana tapahtunut merkittävää kehitystä, jolla tulipalojen vaikutuksia saataisiin vähennettyä. Tämän tutkimuksen lähtökohtana oli selvittää voidaanko paloturvallisuuden osa-aluetta digitalisoimalla parantaa rakennusten paloturvallisuutta. Työssä selvitettiin IoT-teknologian tuomia mahdollisuuksia paloturvallisuuden kehityksessä. Työn yhteydessä selvitettiin lisäksi, mitä hyötyjä ja uhkia IoT- ja älyteknologian hyödyntämiseen liittyy sekä tuotiin esille IoT:n hyödyntämisen tuomia kustannusvaikutuksia paloturvallisuustekniikkaan ja sen kunnossapitoon. Tutkimuksessa tuotiin myös esille IoT:n avulla tapahtuvan datan jakamisen mahdollisuudet sekä selvitettiin, miten IoT-teknologiaa on hyödynnetty paloturvallisuuden kehityksessä Suomen rakennuskannassa.

Tämä tutkimus toteutettiin laadullisena tutkimuksena. Tutkimusaineisto kerättiin teemahaastattelun avulla, jonka yhteydessä jokaista haastateltavaa haastateltiin yhden kerran. Haastateltavat henkilöt edustivat yhdeksää eri toimialaa, jotta tutkittavasta ilmiöstä voitiin saada mahdollisimman kokonaisvaltainen kuva. Kerättyyn tutkimusaineistoon suoritettiin aineistolähtöinen sisällönanalyysi teoreettisen kokonaiskuvan saamiseksi.

Johtopäätöksenä voidaan todeta, että IoT- ja älyteknologiaa hyödyntämällä on mahdollista parantaa rakennusten paloturvallisuutta. Näiden teknologioiden hyödyntäminen Suomen rakennuskannassa on kuitenkin vielä varsin vähäistä, vaikka älykkäitä paloturvallisuusratkaisuja on jo tullut Suomen markkinoille. Tutkimustulosten perusteella syyt IoT- ja älyteknologian vähäiseen hyödyntämiseen eivät liittyneet niinkään itse teknologiaan, vaan asenteisiin uutta teknologiaa kohtaan. Tämän lisäksi IoT- ja älyteknologian tuomia hyötyjä ei ole osattu tunnistaa riittävän hyvin.

Lisäämällä paloturvallisuutta parantavien laitteistojen älykkyyttä tai hyödyntämällä niissä IoT:tä, voi rakennuksien paloturvallisuus parantua nykytilanteeseen verrattuna. Tutkimustuloksissa esille nousi neljä päätekijää, joilla on vaikutusta paloturvallisuuden kehitykseen hyödyntäessä IoT- ja älyteknologiaa:

- Toimintavarmuuden parantaminen
- Onnettomuuksien ehkäisy
- Pelastusviranomaiselle reaaliaikaisen tiedon välittäminen
- Talotekniikan olosuhdeanturoinnin hyödyntäminen

Toimintavarmuuden parantamisessa yksi oleellisimmista tekijöistä on laitteiden tai järjestelmien etäkäytön tehostuminen. Etäkäytön avulla mahdollistetaan laitteiden ja järjestelmien monitorointi mobiilisti mistä tahansa, jolloin laitteiston tilaa voidaan tarkkailla nykyistä paremmin. Etäkäytön mahdollisuuden lisäksi paloturvallisuutta parantavat laitteistot muuttuvat tulevaisuudessa entistä älykkäämmiksi. Niihin lisättävä anturointi mahdollistaa ympäristössä tapahtuvien olosuhteiden muutoksien tunnistamisen entistä tehokkaammin, jonka avulla voidaan vähentää siten esimerkiksi erheellisien palohälytyksen syntymistä. Myös laitteiden diagnostiikka kehittyy, jolloin laitteisiin tulleet viat pystytään tunnistamaan ja korjaamaan nopeasti. Näin ollen laitteiden huolto- ja kunnossapitotoiminta voidaan toteuttaa ennakoivasti.

IoT:tä hyödyntämällä voidaan estää onnettomuuksien syntymistä tai rajoittaa niiden vaikutuksia. Tehokkain keino ehkäistä tulipaloja on estää niiden syttyminen. IoT:n ja järjestelmäintegraatioiden avulla mahdollistetaan esimerkiksi sähkövirran katkaiseminen laitteista, kun anturit havaitsevat tulipalon riskin. IoT tarjoaa myös tehokkaan ratkaisun välittää tietoa älypuhelinsovelluksiin ihmisten varoittamiseksi alkaneesta vaaratilanteesta sekä ohjeistamiseksi toimimaan oikein eri onnettomuustilanteissa. Lisäksi antureista ja laitteista kerättyä dataa voidaan hyödyntää tulipalojen ehkäisemiseen välillisesti esimerkiksi onnettomuuksien tutkinnan yhteydessä tai tutkiessa työntekijöiden turvallisuuskäyttäytymistä.

IoT-ratkaisuna toteutettujen talotekniikan tai paloturvallisuutta parantavien laitteistojen kautta saatua tietoa voidaan välittää esimerkiksi alueen pelastusviranomaiselle. Reaaliaikaisen tiedon avulla tulipalon kehitystä on mahdollista seurata jo hälytysajon aikana, mikä mahdollistaa entistä nopeamman ja tehokkaamman sammutus- ja pelastustoiminnan.

Tulevaisuudessa paloturvallisuutta parantavan laitteiston lisäksi talotekniikan olosuhdeanturointia on mahdollista hyödyntää paloturvallisuuden kehityksessä. Olosuhdeanturointia voidaan hyödyntää tulipalojen havaitsemiseen, tulipalon kehityksen ennustami-

seen sekä ihmisten paikantamiseen ja käyttäytymisen seuraamiseen. Rakennusten IoT-pohjaisten kiinteistönautomaatiojärjestelmien yleistyessä talotekniikan eri järjestelmät voidaan integroida helpommin ja kustannustehokkaammin yhteen, jolloin rakennuksessa olevista antureista kerättyä tietoa voidaan käyttää useissa eri toiminnoissa ja ohjauksissa. Tämä lisää rakennusten turvallisuutta, koska järjestelmiä voidaan hallita yhdestä käyttöliittymästä, mikä taas helpottaa eri antureista ja toimilaitteista kerätyn tiedon yhdistämistä.

IoT:n hyödyntämisen suurimmiksi uhkiksi muodostuivat puutteet tieto- ja kyberturvallisuudessa sekä tietosuojaan liittyvissä asioissa. Nämä uhkatekijät ja riskit katsottiin kuitenkin olevan hallittavissa, jonka vuoksi niiden ei katsottu muodostavan estettä IoT:n hyödyntämiselle paloturvallisuudessa. Viime vuosina kiinteistöautomaatiojärjestelmiä kohtaan tapahtuneet kyberhyökkäysten todettiin olevan mahdollisia myös paloturvallisuustekniikkaa kohtaan. Sen vuoksi onkin erityisen tärkeää, että riittävästä tietoturvasta huolehditaan IoT-arkkitehtuurin kaikissa kerroksissa sekä kaikkien järjestelmäkokonaisuuteen kuuluvien toimijoiden ja henkilöiden toimesta. Tieto- ja kyberturvallisuuden lisäksi on huomioitava tietosuojaan liittyvät asiat, joista ajankohtaisimpana esille nousivat EU:n tietosuoja-asetuksen tuomat velvoitteet.

Paloturvallisuutta parantavia laitteistoja koskevat standardit mahdollistavat IoT-teknologian hyödyntämisen niissä. Markkinoilla olevissa laitteissa IoT-teknologialla ei ole korvattu mitään standardien vaatimusten mukaisuutta, vaan älykkyyttä on tuotu standardien vaatimustason lisäksi. Samalla laitteesta on voitu tehdä entistä hyödyllisempi ja kiinnostavampi. Tulevaisuudessa tulisi kiinnittää huomioita paloturvallisuutta parantavien laitteistojen yhteensopivuuteen muiden talotekniikanjärjestelmien kanssa. Erityisesti huomio tulisi kohdistua rajapintojen avoimuuteen, tiedonsiirrossa käytettäviin dataformaatteihin sekä niiden standardien kehittämiseen. Tämä mahdollistaisi entistä helpommat järjestelmäintegraatiot, jotka toisivat myös kustannussäästöjä. Kustannussäästöjä syntyy myös paloturvallisuutta parantavien laitteistojen ylläpidosta kohteissa, joissa on paljon paloturvallisuustekniikkaa. IoT- ja älyteknologian hyödyntämisestä kustannussäästöt tulisivat laitteiden etäkäytöstä, huolto- ja kunnossapidon ennakoivammasta toiminnasta sekä langattomien antureiden käytöstä.

LÄHTEET

AT&T. 2016. What you need to know about IoT wide area networks. [Verkkojulkaisu]. [Viitattu 14.2.2018]. Saatavilla: https://www.business.att.com/content/whitepaper/what_need_know_iot_networks.pdf

Avoin rajapinta. 2014. Avoimen rajapinnan määritelmä. [Verkkojulkaisu]. [Viitattu 1.3.2018]. Saatavilla: http://avoinrajapinta.fi/

Baird, M. 2010. Background Paper. The Recovery Phase of Emergency Management. University of Memphis. [Verkkojulkaisu]. [Viitattu 22.3.2018]. Saatavilla: http://www.memphis.edu/ifti/pdfs/cait_recovery_phase.pdf

Bhavani, D. & Uthra, R. 2017. Deployment of emergency navigation system in IoT based smart buildings using wireless sensor network. International Journal of Pure and Applied Mathematics. Vol. 115, 6, pp. 491-498.

Brake, D. 2016. 5G and Next Generation Wireless: Implications for Policy and Competition. [Verkkojulkaisu]. [Viitattu 15.2.2018]. Saatavilla: http://www2.itif.org/2016-5g-next-generation.pdf

Brush, A., Lee, B., Mahajan, R., Agarwal, S. & Saroiu, S. 2011. Home Automation in the Wild: Challenges and Opportunities. Session: Home Automation 7.5.2011, Vancouver, BC, Canada. pp 2115-2124.

Bushby, S. 2001. Integrating Fire Alarm Systems with Building Automation and Control Systems. Fire Protection Engineering, Summer 2001, pp. 5-7.

Chan, H. & Perrig, A. 2003. Security and Privacy in Sensor Networks. Computer. Vol. 36, 10, pp. 103-105.

Deloitte. 2016. REflexions magazine issue 4, pp. 1-46. [Verkkojulkaisu]. [Viitattu 2.2.2018]. Saatavilla: file:///C:/Users/oem/Downloads/gx-real-estate-reflexions-issue-4.pdf

Dooley, K., Ihasalo, H., Jylhä, T. & Sairanen, S. 2017. Kiinteistöjen IoT-markkinakatsaus. Granlund Oy. [Verkkojulkaisu]. [Viitattu 2.3.2018]. Saatavilla: https://issuu.com/granlundoy/docs/granlund_iot-raportti_2017_issuu

Collin, J. & Saarelainen, A. 2016. Teollinen Internet. Talentum: Helsinki.

Cozify. 2018. Cozify. [viitattu 22.3.2018] Saatavilla: https://www.cozify.fi/

Evans, P. & Annunzianta, M. 2012. Industrial Internet: Pushing the Boundaries of Minds and Machines. General Electric. [Verkkojulkaisu]. [Viitattu 2.10.2017]. Saatavilla: http://www.ge.com/docs/chapters/Industrial_Internet.pdf

Euroopan komissio. 2018. Benefits of standards. [Verkkojulkaisu]. [Viitattu 20.4.2018]. Saatavilla: https://ec.europa.eu/growth/single-market/european-standards_en

Fibaro. 2018. Smoke Sensor. [viitattu 22.3.2018] Saatavilla: https://www.fibaro.com/en/products/smoke-sensor/

FireTweet. 2018. Service. [viitattu 30.3.2018] Saatavilla: http://www.firetweet.in/services.html

Free, E. 2015. Intel IoT unlocks doors to robust Building Management systems. [Verkkojulkaisu]. [Viitattu 12.11.2017]. Saatavilla: https://blogs.intel.com/iot/2015/04/15/how-the-internet-of-things-can-unlock-the-door-to-a-more-robust-bms/

Gerber, A. 2017. Connecting all the things in the Internet of Things. IBM Corportion. pp. 1-10. [Verkkojulkaisu]. [Viitattu 10.10.2017]. Saatavilla: https://www.ibm.com/developerwor ks/library/iot-lp101-connectivity-network-protocols/index.html

Gokceli, S., Zhmurov, N., Kurt, G. & Ors, B. IoT in Action: Design and implementation of a building evacuation service. Journal of Computer Networks and Communications. Hindawi. Volume 2017, pp.1-14.

Gonzales Garcia, C., Meana-Llorian, D., Garcia-Bustelo, B., & Lovelle J. 2017. A review about Smart Objects, Sensors, and Actuators. Department of Computer Science, O. International Journal of Interactive Multimedia and Artificial Intelligence, January 2017, pp. 7-10.

Gubbi, J., Buyya, R., Marusic, S. & Palaniswawi, M. 2013. Internet of Things: A vision, architectural elements, and future directions. Future generation computer systems. Elsevier. Vol 29, 7, pp. 1645-1660.

Hakkarainen, T. 2007. Talo- ja turvatekniikka tulipalotilanteessa. Nykytilanne ja tarvekartoitus. VTT Tiedotteita. [Verkkojulkaisu]. [Viitattu 11.12.2007]. Saatavilla: http://www.vtt.fi/inf/pdf/tiedotteet/2007/T2383.pdf

Hedegren Security. 2017. Prodex FIREscape suunnitteluopas. [Verkkodokumenti]. [Viitattu 8.12.2017]. Saatavilla: https://hedengrensecurity.fi/wpcontent/uploads/2017/05/Suunnitteluopas _2017_web-1.pdf

Hirsjärvi, S. & Hurme, H. Tutkimushaastattelu – Teemahaastattelun teoria ja käytäntö. Tallinna Raamatutrukikoda: Gaudeamus Oy.

Hirsjärvi, S., Remes, P., Sajavaara, P. 2010. Tutki ja kirjoita. Helsinki: Tammi.

Hostikka, S. & Janardhan R. 2017. Pressure management in compartment fires. Aalto yliopisto. Science + technology 1/2017. Research Report. Unigrafia Oy: Helsinki.

Hätäkeskuslaitos. 2018. eCall. [Verkkojulkaisu]. [Viitattu 30.3.2018]. Saatavilla: https://www.112.fi/hatanumero_112/soittajan_paikantaminen/ecall

Ihasalo, H., Jantunen, P. & Salo, E. 2017. Raportti: Talotekniikan avoimet rajapinnat ja tiedonkuvaukset. Aalto yliopisto, Sähkötekniikan korkeakoulu. [Verkkojulkaisu]. [Viitattu 25.3.2018]. Saatavilla: http://eea.aalto.fi/fi/midcom-serveattachmentguid-1e796b70497eb5096 b711e7aaacdb2ccee264166416/loppuraportti-7_fi.9.2017.pdf

International Electrotechnical Comission. 2014. Internet of Things: Wireless Sensor Networks. White paper, pp. 1-78. [Verkkodokumentti]. [Viitattu 1.12.2017]. Saatavissa: http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf

Internal Telecommunication Union. 2012. ITU-T Y.2060, Series Y: Global Information Infrastructure, Internet protocol aspects. Next generation networks-Frameworks and functional architecture models. Overview of the Internet of things. 6/2012. Sveitsi, Geneve.

Ivanovic, S., Milivojsa, S., Eric, T. & Vidakovic, M. 2017. Collection and analysis of system usage data in smart home automation systems. 2017 IEEE 7th International Conference on Consumer Electronics – Berlin (ICCE-Berlin). pp. 65-66.

Juhanko, J. & Jurvansuu, M. (toim.). 2015. Suomalainen teollinen internet-haasteesta mahdollisuudeksi. Etla raportti, No 43. [Verkkojulkaisu]. [viitattu 7.2.2018]. Saatavissa: https://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-42.pdf

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylä: Suomen Yliopistopaino Oy.

Karki, R. & Garia, V. 2016. Next Generations of Mobile Networks. International Journal of Computer Applications (0975 – 8887) International Conference on Advances in Information Technology and Management ICAIM – 2016, pp. 13-17.

Kohnke, O. 2016. It's Not Just About Technology: The People Side of Digitalization. Shaping the Digital Enterprise. Springer International Publishing, Switzerland. pp.69-91.

Kokki, E. 2017a. Suomalaiset pelastusasenteet 2017. Pelastusopisto, D-sarja: Muut julkaisut 1/2018. [Verkkojulkaisu]. [Viitattu 30.3.2018]. Saatavilla: http://info.smedu.fi/kirjasto/Sarja_D/D1_2018.pdf

Kokki, E. 2017b. Tietoa rakennustyypeittäin palovaroittimien olemassa olosta ja sen toimivuudesta rakennuspaloissa ja rakennuspalovaaroissa 2012-2016, tilastotieto. Sähköpostiviesti, 19.9.2017. Vastaanottaja Tuomas Pylkkänen [Viitattu 8.2.2018].

Kulkarni, S. & Kulkarni S. 2017. Communication Models in Internet of Things: A Survey. International Journal of Science Technology & Engineering. Vol. 3, 3, pp. 87-91.

Kuusijärvi, J., Savola, R., Savolainen, P. & Eversti A. 2016. Mitigating loT Security Threats with a Trusted Network Element. The 11th International Conference for Internet Technology and Secured Transactions (ICITST-2016). IEEE, pp 260-265.

Lethaby, N. 2017. Wireless connectivity for the Internet of Things: One size does not fit all. Texas Instruments. [Verkkodokumentti]. [Viitattu 10.12.2017]. Saatavilla: http://www.ti.com/lit/wp/swry010a/swry010a.pdf

Li, S., Xu, L D. & Zhao, S. 2014. The Internet of Things: a survey. Information Systems Frontiers. April 2015. Vol. 17, 2, pp. 243-259.

Liikenne- ja viestintäministeriö. 2018. Sähköisen viestinnän salaus- ja suojausmenetelmät. Liikenne- ja viestintäministeriön julkaisuja 2/2018. Helsinki. [Verkkojulkaisu]. [Viitattu 10.3.2018]. Saatavilla: http://urn.fi/URN:ISBN:978-952-243-546-0

Liikenne- ja viestintävaliokunta. 2017. Valiokunnan lausunto LiVL 6/2017 vp─ U 19/2017 vp. [Verkkojulkaisu]. [Viitattu 20.11.2017]. Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/LiVL_6+2017.pdf

Lindqvist, U & Neumann, P. 2017. Inside risks, The future of Internet of Things. Communications of the ACM. February 2017, Vol. 60, 2, pp. 26-30.

Links, C. 2017. Evolution of The IoT as a Service. Microwave Journal, Vol. 60, Issue 5, pp. 52-60.

Liu, S-J. & Zhu, G-q. 2014. The Application of GIS and IoT Technology on Building Fire Evacuation. Elsevier Ltd, pp. 577-582.

Lähitapiola. 2018. Älykotivakuutus. [Verkkojulkaisu]. [Viitattu 30.3.2018]. Saatavilla: https://www.cozify.fi/products/lahitapiola-alykotipaketti

Madakam, S. 2015. Internet of Things: Smart Things. International Journal of Future Computer and Communication, Vol. 4, No. 4, pp. 250-253.

Madakam, S., Ramaswawy, R & Tripathi, S. 2015. Internet of Things (IoT): A Literature Review. Journal of Computer and Communications. Vol 3, pp. 164-173.

Mckinsey Global Institute. 2015. Mapping the value beyond the hype. 6/2015. [Verkkojulkaisu]. [Viitattu 1.12.2017] Saatavilla: https://www.mckinsey.com/business-functions /digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

Meurman, K. 2018. Palovaroittimien ikääntymisselvitys loppuraportti. Turvallisuus- ja kemikaalivirasto. [Verkkojulkaisu]. [Viitattu 18.3.2018]. Saatavissa: http://www.tukes.fi/Tiedostot/pelastustoimen_laitteet/Loppuraportti_ikaantymisselvitys.pdf

Meurman, K. 2017. IoT-palovaroittimet. Sähköpostiviesti 24.8.2017. Vastaanottaja Tuomas Pylkkänen. [Viitattu 9.2.2018].

Miorandi, D., Sicari, S., De Pellegrini, F. & Chlamtac, I. 2012. Internet of things: Vision, applications and research challenges ScienceDirect, Elsevier B.V. Vol. 10, 7, pp. 1497-1516.

Mohan, M., Sridhar, P. & Srinath, S. 2016. SMART Evacuation System. International Journal for Research in Applied Science & Engineering Technology (IJRASET). Vol. 4, III, pp. 682-685.

Mäkinen, J. 2015. Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things. Information & Communications Technology Law. Vol. 24, 3, pp. 262 -277.

Nest Protect. 2018. Nest Protect. [viitattu 22.3.2018]. Saatavilla: https://nest.com/smoke-co-alarm/overview/

Nieminen, M. 2018. Rakennusten automaattisten sprinklerilaitteistojen luotettavuus. Diplomityö. Tampereen teknillinen yliopisto.

Normalux 2018. Intelligent system. [Verkkodokumentti]. [Viitattu 22.3.2018] Saatavilla: http://www.ecolight.eu/intranet/uploads/descargas/Intelligent%20System.pdf

Oh, J., Jiang, Z. & Panganiban, H. 2013. Development of a Smart Residential Fire Protection System. Advances in Mechanical Engineering. Volume 2013, pp. 1-6.

Palta. 2016. Digitalisaatio palvelualoilla – Pysyykö Suomi mukana digikehityksessä? Palvelualojen työnantajat PALTA ry. Helsinki. [Verkkojulkaisu]. [Viitattu 20.4.2018] Saatavilla: https://www.palta.fi/wp-content/uploads/2016/11/Digitalisaatio-palvelualoilla-Pysyyk%C3%B6-Suomi-mukana-digikehityksess%C3%A4_FINAL.pdf

Parrish, K. 2017. Zigbee, Z-Wave, Thread and Wemo: What's the Difference? [Verkkodokumentti]. [Viitattu 1.2.2018]. Saatavilla: https://www.tomsguide.com/us/smart-home-wireless-network-primer,news-21085.html

Parviainen, P., Kääriäinen, J., Tihinen, M. & Teppola, S. 2017. Tackling the digitalization challenge: how to benefit from digitalization in practice. International Journal of Information Systems and Project Management, Vol. 5, 1, pp. 63-77.

Pelastusopisto. 2017a. Automaattiset paloilmoitukset säästivät 16 miljoonan euron palovahingoilta. Uutinen, 9.2.2017. [Verkkojulkaisu]. [Viitattu 16.4.2017]. Saatavilla: https://www.pelastusopisto.fi/automaattiset-paloilmoitukset-saastivat-16-miljoonan-euron-palovahingoilta/

Pelastusopisto. 2017b. Pelastustoimen taskutilasto 2012-2016. D-sarja: Muut 1/2017. [Verkkodokumentti]. [Viitattu 15.3.2018]. Saatavilla: http://info.smedu.fi/kirjasto/Sarja_D/D1_ 2017.pdf

Piira, K. 2005. Pelastusautoon raportoiva kiinteistö - PARK. VTT Rakennus- ja yhdyskuntatekniikka, pp. 1-6. [Verkkojulkaisu]. [Viitattu 11.12.2017]. Saatavilla: http://www.spek.fi/loader.aspx?id=3c053b80-6812-4bda-9f0e-ecef3fa33ff9

Päijät-Hämeen pelastuslaitos. 2018. Kohdepiirros. [viitattu 10.4.2018]. Saatavilla: https://www.phpela.fi/.../ohjeet_20130527092440_kohdepiirrosohje_phpela.doc

Postcapes. 2018. IoT Technology Guidebook. [Verkkojulkaisu]. [Viitattu 1.2.2018]. Saatavilla: https://www.postscapes.com/internet-of-things-technologies/

Probemen Oy. 2017. Sammutusjärjestelmä - uusi aika. Mainoslehti.

ProtectFire. 2018. Bellcheck. [viitattu 20.4.2018] Saatavilla: http://www.projectfireproducts.co.uk/products/bellcheck/

Puhto, J., Snellman, S., Gussander, J-E., Kärkkäinen, H. & Pekkanen, J. 2016. Digiselvitys 2016, Digitaalisuuden nykytila ja kehityssuunnat kiinteistö- ja rakennusalalla. Tampereen teknillinen yliopisto, Rakennustekniikan laitos, raportti 19. [Verkkojulkaisu]. [Viitattu 16.4.2018]. Saatavilla: https://tutcris.tut.fi/portal/files/7869519/ Digiselvitys_2016.pdf

Rani, K. & Mayuri, A. 2016. Paper on Basics of Internet of Things. International Journal of Emerging Trends in Science and Technology Impact Factor. Vol 03, 06, pp. 4144-4149.

Rathinavel, K., Pipattanasomporn, M.,Kuzlu, M. & Rahman, S. 2017. Security Concerns and Countermeasures in IoT-Integrated Smart Buildings. IEEE Power & Energy Society Innovative Smart Grid Technologies Conference, 4/2017, pp.1-5.

Raun, N. 2016. Smart environment using internet of things (IOTS) - a review. IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference. 10/2016, pp.1-6.

Raza, U., Kulkarni, P. & Sooriyabandara, M. 2017. Low Power Wide Area Network: An Overview. IEEE Communications Surveys & Tutorials. Vol. 19, 2, pp. 855-873.

Riahi, A., Natalizio, E., Challal, Y., Mitton, N. & Iera, A. 2014. A systemic and cognitive approach for IoT security. International Conference on Computing. Networking and Communications (ICNC). 10.1.2014. Honolulu, United States. 2014. pp. 1-6.

Roost Inc. 2018. [Viitattu 22.3.2018]. Saatavilla: https://www.getroost.com/product-battery

Ryu, C-S. 2015. IoT-based Intelligent for Fire Emergency Response Systems. International Journal of Smart Home. Vol. 9, 3, pp. 161-168.

Saarikko, T., Westergren, U. & Blomquist, T. 2017. The Internet of Things: Are you ready what's coming? BUSHOR-1398, Elsevier Inc. pp. 1-10.

Sadiku, M., Musa, S. & Momoh, O. 2014. Cloud computing: opportunities and challenges. Potentials IEEE. Vol 33, 1, pp. 34-35.

Salo, I. 2014. Big Data & pilvipalvelut. Docendo. Saarijärven Offset Oy: Saarijärvi.

Sethi, N. 2017. IoT-Architecture and its Technical Issues. International Journal of Advanced Research in Computer Science. Vol. 8, 5, pp. 1616-1617.

Sethi, P. & Sarangi, S. 2016. Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering. Vol. 2017, pp. 1-25.

Shinde, R., Pardeshi, R., Vishawakarna, A. & Barhate, N. 2017. Need for Wireless Fire Detection Systems using IoT. International Research Journal of Engineering and Technology (IRJET). Volume 04, 01, pp. 1078-1081.

Schneider Electric. 2016. Esgraf tuote-esite.

Schneider Electric. 2017. EcoStructure Fire Expert tuote-esite

Sector Alarm. 2018. Sector Alarm [viitattu 18.3.2018] Saatavilla: https://www.sectoralarm.fi/

Siemens. 2017. Desigo CC ja Sinteso paloilmoitusjärjestelmä myyntiesite.

Siemens. 2016. Desigo Mass Notification. [Verkkojulkaisu]. [Viitattu 25.3.2018]. Saatavilla: https://www.downloads.siemens.com/downloadcenter/Download.aspx?pos=download&fct=getasset&id1=A6V10444884

Siemens. 2011. Tuote-esite MM 8000 Valvomo-ohjelmisto. [Viitattu 2.1.2018] Saatavilla: http://www.siemens.fi/pool/products/industry/talotekniikka/paloturvallisuus/valvomojarjestelmat/mm8000_tuote-esite_mp4_40.pdf

Smockeo. 2018. Introduction. [viitattu 22.3.2018] Saatavilla: https://www.smockeo.com/en/

SPEK. 2018. Jokaisessa asunnossa on oltava toimivat palovaroittimet. [Verkkojulkaisu]. [Viitattu 15.4.2018] Saatavilla: http://www.spek.fi/Suomeksi/Turvatietoa/ Paloturvallisuus/Kerrostaloasujalle/Toimivat-palovaroittimet

Stojmenovic, I. & Wen, S. 2014. The Fog Computing Paradigm: Scenarios and Security Issues. Proceedings of the 2014 Federated Conference on Computer Science and Information Systems. Vol. 2, pp. 1–8.

Suomen Standardisoimisliitto SFS ry. 2018. Avain standardien maailmaan, SFS-käsikirja 1. [Verkkojulkaisu]. [Viitattu 20.3.2018]. Saatavilla: https://www.sfs.fi/files/83/kk1_avain_standardien_maailmaan_web.pdf

Swedeberg, C. 2012. At Hospita, Wi-Fi sensors can monitor emergency lights, code blue situations. RFID Journal. 7.5.2012, pp. 1-2. [Verkkojulkaisu]. [Viitattu 30.11.2017]. Saatavilla: http://www.rfidjournal.com/articles/view?9289

Tukes. 2014. Mitä EU:n rakennustuoteasetus tarkoittaa tuotteen valmistajan kannalta? [Verkkojulkaisu]. [Viitattu 10.5.2018]. Saatavilla: http://www.tukes.fi/fi/Toimialat/ Rakennustuotteet1/Rakennustuotteet/Mita-rakennustuoteasetus-tarkoittaa-tuotteen-valmistajan-kannalta/

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. Jyväskylä: Gummerus Kirjapaino Oy.

Tuomisaari, V. 2017. Utilizing Internet of Things in fire protection systems. Diplomityö. Aalto-yliopisto.

Verisure. 2018. Verisure Smart alarms. [Viitattu 1.4.2018] Saatavilla: https://www.verisure.fi/palo.html#1

Vijayalakshmi, S. & Muruganand, S. 2017. Internet of Things technology for fire monitoring system. International Research Journal of Engineering and Technology (IRJET). Vol. 4, 6, pp. 2141-2147.

Virtanen, A. 2015. Digitalization Enables User-centric People Flow Planning in Smart Buildings. Council on tall building and Urban Habitat (CTBUH). New York Conference, pp. 603-608. [Verkkojulkaisu]. [Viitattu 16.4.2018]. Saatavilla: http://global.ctbuh.org/resources/papers/download/2514-digitalization-enables-user-centric-people-flow-planning-in-smart-buildings.pdf

Wang, J., Zhang, D., Liu, M., Xu, F., Sui, H-I & Yang, S-F. 2014.Discussion of Society Fire-fighting Safety Management Internet of Things Technology System. Fifth International Conference on Intelligent Systems Design and Engineering Applications. IEEE. pp. 422-425.

Weinberg, B. 2015. Internet of Things: Convenience vs. privacy and secrecy. Business horizons. Vol. 58, 6, pp. 615 -624.

Wortmann, F. & Flutcher, K. 2015. Internet of Things Technology and Value Added. Business & Information Systems Engineering. Vol 57, 3, pp. 221-224.

Yang, L., Martino, B. & Zhang. Q. 2017. Internet of Everything. Mobile Information Systems. Vol. 2017, pp. 1-3.

Ympäristöministeriö. 2017. Älyteknologiaratkaisut ikääntyneiden kotona asumisen tukena. Ympäristöministeriön raportteja 7/2017. Helsinki. [Verkkojulkaisu]. [Viitattu 13.4.2018]. Saatavilla : http://urn.fi/URN:ISBN:978-952-11-4730-2

Zdravković, M., Trajanovi, M., Sarraipa, J., Jarmid-Goncalves, R., Lezoche, M.,Aubry, A. & Panetto, H. 2016. 6th International Conference on Information Society and Techology, ICIST 2016, Feb 2016, pp. 216-220.

Z-Wave. 2018. Z-Wave for consumers. [viitattu 1.2.2018] Saatavilla: https://z-wavealliance.org/z-wave_for_consumers/

LAINSÄÄDÄNTÖ

Laki pelastustoimen laitteista 10/2007

Maankäyttö- ja rakennuslaki 132/1999

Pelastuslaki 379/2011

Pelastustoimilaki 561/1999 (kumoutunut)

Sisäasianministeriön asetus automaattisista sammutuslaitteistoista A:65 SM-1999-967/Tu-33

Sisäministeriön asetus palovaroittimen sijoittamisesta ja kunnossapidosta 239/2009

Sisäasiainministeriön asetus rakennusten poistumisreittien merkitsemisestä ja valaisemisesta 805/2005

Sähköturvallisuuslaki 1135/2016

Ympäristöministeriön asetus rakennusten paloturvallisuudesta 848/2017

Ympäristöministeriön asetus rakennusten paloturvallisuudesta annetun ympäristöministeriön asetuksen muuttamisesta 2009

Valtioneuvoston asetus palovaroittimien teknisistä ominaisuuksista 291/2009

STANDARDIT JA SUUNNITTELUOHJEET

LVI 65-10512. 2012. Sammutuslaitteistot. Rakennustieto Oy.

SFS-CEN/TR 12101-5. 2005. Savunhallintajärjestelmät. Osa 5: Savunpoistolaitteistojen suunnittelu ja mitoitus. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

SFS-CEN/TS 54-14. 2004. Paloilmoittimet. Osa 14: Suunnittelu-, mitoitus-, asennus-, käyttöönotto-, käyttö- ja huolto-ohjeet. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

SFS-CLT/TS 50136-7. 2017. Hälytysjärjestelmät. Ilmoituksensiirtojärjestelmät ja -laitteet. Osa 7: Soveltamisohjeet. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

SFS-CLC/TS 50398. 2009. Hälytysjärjestelmät. Yhdistetyt ja integroidut hälytysjärjestelmät. Yleiset vaatimukset. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

SFS-EN 54-13. 2017. Paloilmoittimet. Osa 13: Laitteiston osien yhteensopivuuden ja yhdistettävyyden arviointi. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

SFS-EN 54-16. 2009. Paloilmoittimet. Osa 16: Äänihälytyksen hallinta- ja osoituslaitteet. Suomen Standardisoimisliitto SFS ry. Helsinki, SFS.

SFS-EN 1838. 2014. Valaistussovellukset. Turvavalaistus. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

SFS-EN 12101-6 + AC. 2005. Savunhallintajärjestelmät. Osa 6: Paineistus. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

SFS-EN 12845+A2. 2015. Kiinteät palosammutusjärjestelmät. Automaattiset sprinklerilaitteistot. Suunnittelu, asennus ja huolto. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

SFS-EN 14604. 2006. Palovaroittimet. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

SFS-EN 50136-1. 2012. Hälytysjärjestelmät. Ilmoituksensiirtojärjestelmät ja laitteet. Osa 1. Yleiset vaatimukset ilmoituksensiirtojärjestelmille. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

SFS-EN 50172. 2004. Poistumisvalaistusjärjestelmät. Suomen Standardisoimisliitto SFS ry. Helsinki: SFS.

Diplomityö: *Internet of Things teknologian hyödyntäminen paloturvallisuuden kehityksessä ja integroidussa älykkäässä ympäristössä*

Haastateltava vastaavat kysymyksiin vapaasti oman toimialansa ja näkemyksensä mukaisesti. Haastateltavat tulevat edustamaan pelastusviranomaisia, talotekniikan edustajia, laitevalmistajia, kiinteistön omistajien edustajia, tietoturva-asiantuntijoita sekä muita älytekniikan tai -hankkeiden kanssa tekemisissä olevia henkilöitä.

Teemahaastattelun teemat ja kysymykset – tutkija haastattelee. Haastattelu tullaan nauhoittamaan. Kysymysten alapuolella on esitetty joitain sanoja tai lauseita kysymysten tarkentamiseksi, vastaamiseen helpottamiseksi sekä haastattelijan tueksi.

Internet of Things – teknologian ja älytekniikan hyödyntäminen rakennuksissa

- Onko IoT - teknologiaa hyödynnetty Suomen rakennuskannassa?
  - ✓ Esimerkkejä kohteista (mainintoja)
  - ✓ Yleisimmät teknologian käyttökohteet
  - ✓ Paloturvallisuus

- Onko IoT – teknologian ja älytekniikan tuomat hyödyt riittävästi tiedossa ja tunnistettu?
  - ✓ Tutkimus
  - ✓ Rakennushankkeeseen ryhtyvät tai kiinteistöjen omistajat
  - ✓ Laitevalmistajat
  - ✓ Talotekniikan ja sähköalan suunnittelijat/urakoitsijat

- Mitkä ovat suurimmat tekijät siihen, ettei IoT – teknologiaa tai älytekniikkaa hyödynnetä jo laajasti uudis- ja korjausrakentamisessa?
  - ✓ Kustannukset, riskinotto
  - ✓ Tietämättömyys
  - ✓ Ei valmiiksi räätälöityjä malleja, ei referenssikohteita

- Voidaanko IoT – teknologian integraatioilla parantaa rakennuksien palo- ja henkilöturvallisuutta?
  - ✓ Olemassa olevien paloturvallisuuslaitteiden parantaminen
  - ✓ Toimintavarmuuden parantaminen
  - ✓ Syttymisien vähentäminen/estäminen
  - ✓ Ihmisen toimintaan liittyvät unohdus ja erehdys

Datan kerääminen, jakaminen ja sen rikastamisesta saatava hyöty

- Mille eri toimijoille IoT – turvallisuuslaitteista ja -sensoreista kerättyä dataa voidaan jakaa?
  - ✓ Isännöitsijä, kiinteistömanageri, kiinteistönhuolto
  - ✓ Omistaja, osakkeen omistaja
  - ✓ Laitevalmistaja, huolto
  - ✓ Viranomaiset

- Millä tavoin eri toimijat hyötyvät IoT – turvallisuuslaitteista ja -sensoreista kerätyn datan rikastamisesta ja hyödyntämisestä?
    - ✓ Tuote- ja palvelukehitys
    - ✓ Turvallisuuden varmistaminen
    - ✓ Ennakoiva toiminta, huolto ja kunnossapito
    - ✓ Kustannussäästöt

IoT rajapinnat sekä uhat ja mahdollisuudet

- Mitä uhkatekijöitä IoT - teknologian hyödyntämiseen liittyy?
    - ✓ Tietoturva, tietosuoja, yksityisyyden
    - ✓ Rajapinnat

- Saadaanko nykylainsäädännön mukaisilla paloturvallisuuslaitteiden vähimmäisvaatimuksilla aikaan asuinrakennuksissa riittävä paloturvallisuustaso?
    - ✓ Palovaroitin
    - ✓ Väestön ikääntyminen, liikuntarajoitteisuus

- Tuleeko IoT – ja älyteknologian lisääntymään merkittävästi henkilö- ja paloturvallisuuslaitteistoissa?
    - ✓ Tulevaisuuden näkymä vuonna 2025
    - ✓ Missä laitteissa tai järjestelmissä
    - ✓ Rajapinnat

- Millaista osaamista / minkä eri toimijoiden mukanaoloa alan kehittyminen tulevaisuudessa vaatii?
    - ✓ Puuttuuko erityistä osaamista
    - ✓ Koulutustarpeet

Pelastusviranomaisille, laitevalmistajille sekä talotekniikan osaajille esitettävät lisäkysymykset

- Vaikeuttavatko tai mahdollistavatko voimassa olevat turvalaitteistoja koskevat standardit ja suunnitteluohjeet älytekniikan hyödyntämistä/kehitystä?

- Aiheuttaako IoT - teknologia riskitekijöitä paloturvallisuuslaitteiden toimintavarmuudelle?
    - o Langaton tiedonsiirto
    - o Sensoreiden ja laitteiden verkkovirtaan kuulumattomuus

- Millä tavoin uudella älytekniikalla saadaan paloturvallisuuslaitteisiin lisää toimintavarmuutta?

- Onko mahdollista yhdistää olemassa olevia suljettuja turvallisuusjärjestelmiä uuteen IoT- tietoverkkoon?
    - o Kustannustehokkaasti
    - o Helposti, turvallisesti