Aleksi Mahlamäki

HENKILÖTURVAJÄRJESTELMÄN VERSIOPÄIVITYS

Case 2M-IT OY

Tietojenkäsittelyn koulutusohjelma

2018

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

HENKILÖTURVAJÄRJESTELMÄN VERSIOPÄIVITYS Case 2M-IT OY

Mahlamäki, Aleksi
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Joulukuu 2018
Sivumäärä: 33
Liitteitä: 1

Asiasanat: sairaala, paikannus, rfid, järjestelmä, turvallisuus

---

Hälytysjärjestelmät ovat erinomainen tapa tuottaa organisaatiossa työskentelevälle henkilöstölle lisäturvaa arkipäivän työtehtävissä. Monet organisaatiot käyttävät henkilöturvajärjestelmiä toimitiloissaan ja ne ovat räätälöitävissä asiakkaan toiveiden mukaisiksi. Yhteen hälytysjärjestelmään on integroitavissa hoitajakutsun ja henkilöturvajärjestelmän toiminnallisuuksia.

Nykyaikaisissa henkilöturvajärjestelmissä paikantaminen on tehokas ominaisuus. Paikantaminen lisää henkilöstön turvaa sekä tehostaa avun toimittamista ripeästi ja tehokkaasti. RFID -tekniikka mahdollistaa reaaliaikaisen paikantamisen.

Työn aikana tutustuttiin henkilöturvajärjestelmän arkkitehtuuriin, järjestelmäkokonaisuuteen ja toimintatapoihin. Työssä vertailtiin eri toimittajien hälytysjärjestelmien ratkaisumalleja. Syvemmin tutustuttiin Ekahaun järjestelmäratkaisuun.

Opinnäytetyön tarkoituksena oli henkilöturvajärjestelmän versiopäivityksen suorittaminen ja prosessin kirjaaminen suunnitteluvaiheesta toteutukseen. Päivitysprosessi sujui luodun työsuunnitelman mukaisesti. Projektin myötä todettiin dokumentoinnin, tiedottamisen sekä esiselvityksen tärkeys. Päivitys saatiin vietyä loppuun onnistuneesti.

PERSONNEL SECURITY SYSTEM UPDATE Case 2M-IT OY

Mahlamäki, Aleksi
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Business Information Technology
December 2018
Number of pages: 33
Appendices: 1

Keywords: hospital, positioning, rfid, system, security

Alarm safety systems are an excellent way to provide additional security for the working staff in the organization. Many organizations use personnel safety systems in their facilities and they can be tailored by the customer's wishes. An alarm system can be integrated by a nursecall-system and personal protection system functions.

Positioning in modern personnel security system is a powerful feature. Positioning will increase staff security and improve the delivery of assistance quickly and efficiently. RFID technology enables real-time positioning.

As the work progressed, the architecture, system and the working methods of the personnel security system were introduced. In the thesis, different supplier's alarm systems were compared. Deeper familiarity was introduced within the Ekahau system.

The purpose of the thesis was to record the update process from the design stage to the implementation. The updating process proceeded accordingly by the created work plan. With this project, the importance of documentation, information and preliminary study was documented. The security system update was successfully completed.

SISÄLLYS

1 JOHDANTO

Varsinais-Suomen sairaanhoitopiiri on suuri, Turun alueella sijaitseva, organisaatio, jossa liikkuu päivittäin suuret määrät sairaanhoidon henkilökuntaa ja sairaanhoitoa tarvitsevia ihmisiä. Päivittäisessä hoitotyössä syntyy väistämättömästi hankalia, toisinaan jopa vaarallisia tilanteita. Jotta henkilöstö voisi suorittaa työnsä sujuvasti turvallisessa ympäristössä, ilman väkivallan pelkoa, on henkilöturvajärjestelmän käyttöönotto ja ylläpito perusteltua. Turvajärjestelmä ei tietenkään takaa yksin henkilöstön turvallisuutta sellaisenaan, eikä se varsinkaan saa olla henkilöstön ainoa tapa tuoda turvaa hoitotyöhön, mutta tukevana turvallisuuden osa-alueena sen tuoma apu on huomattava.

2M-IT Oy on Suomen suurin terveydenhuollon ICT -palveluita tarjoava yritys. Yritys palvelee monia, eri puolella Suomea sijaitsevia, sairaanhoitopiirejä ylläpitäen tärkeitä sairaanhoidon potilasjärjestelmiä ja ohjelmistoja. 2M-IT Oy syntyi vuonna 2018, kun Länsi-Suomessa vaikuttanut Medbit ja Itä-Suomessa toiminut Medi-IT fuusioituivat yhdeksi suureksi ICT -alan yritykseksi, kattaen suurimman osan Suomen eteläisistä maakunnista. Yrityksen vaikutuspiirin kuuluvat muun muassa kaksitoista sairaanhoitopiiriä sekä yksitoista maakuntaa. (2M-IT Oy:n www-sivut 2018)

Tässä opinnäytetyössä käsitellään Turun yliopistollisessa keskussairaalassa käytössä olevaa henkilöturvajärjestelmää. Järjestelmän palvelinympäristöä ja tietoliikennettä ylläpitää 2M-IT Oy. Ohjelmisto- ja laitteistotoimittajat, kuten Fujitsu, vastaavat järjestelmän ohjelmiston ylläpidosta yhdessä Avack:in ja Ascom:in kanssa. Henkilöturvajärjestelmä koostuu kolmen eri toimittajan ratkaisukokonaisuuksien osista. Kyseinen henkilöturvajärjestelmän kokonaisuus on käytössä Varsinais-Suomen sairaanhoitopiirin T2 -sairaalassa ja A -sairaalassa.

Versiopäivitys -projektin laukaisevana tekijänä organisaatiossa oli järjestelmän tietokannan vanhentuva palvelinalusta sekä versiopäivitystä kaipaava sovellusohjelmisto. Järjestelmän päivitystä oli jo suunniteltu pidemmän aikaa, mutta varsinaisen päivityksen suorittamisen ajankohtaa ei ollut päätetty. Uudistettavat palvelimet pitivät sisäl-

lään tärkeän henkilöturvajärjestelmän tietokannan ja työasemasovelluksen. Turvajärjestelmän tietokannat haluttiin siirtää nyt uudemmalle, toimintavarmemmalle palvelinalustalle.

2 HENKILÖTURVAJÄRJESTELMÄ

Henkilöturvajärjestelmä on tekninen ratkaisu, jolla voidaan turvata työskentelevän henkilöstön työympäristö. Monet hälytysjärjestelmät toimivat lähes samoilla toimintaperiaatteilla, sekä niitä voidaan käyttää erilaisiin tarkoituksiin. Järjestelmät ovat usein joustavia, joita voidaan räätälöidä asiakkaan tarpeiden ja toiveiden mukaan. Turvajärjestelmiä voidaan käyttää myös toisenlaisissa tilanteissa, kuten esimerkiksi työhenkilöstön turvallisuuden varmistamiseen. Tällaisia tarkoitusperiä ovat vanhusten palvelutalojen turvallisuus ja erityisapua tarvitsevien henkilöiden turvallisuuden varmistaminen.

Turun yliopistollisen keskussairaalan tarve henkilöturvajärjestelmälle on henkilöstön turvaaminen päällekarkaus- ja väkivaltatilanteissa. Hälytysjärjestelmille on monia eri nimityksiä kuten päällekarkaus- tai vartijakutsujärjestelmä. Mutta hyvin usein ne ovat samanlaisia toiminnaltaan, vain niiden nimitys muuttuu tarkoitusperän mukaan. Henkilöturvajärjestelmällä pyritään lisäämään henkilökunnan turvallisuutta luomalla turvallisen tuntuinen työympäristö, mutta järjestelmää voidaan käyttää myös samanaikaisesti ennaltaehkäisemään vaarallisia tilanteita. (Forsberg & Lamponen 2014, 3)

Hälytysjärjestelmäkokonaisuuksia on monenlaisia. Useimmat niistä soveltuvat hoitajakutsuun sekä henkilökunnan turvaksi. Avunpyyntöjärjestelmiin on mahdollista integroida esimerkiksi erillinen henkilöturvajärjestelmä. Hoitotyössä automaattisesti hälyttävät järjestelmät ovat hyvin usein välttämättömiä. Avunpyyntöjärjestelmien ja henkilöturvajärjestelmien kehitys on ollut varsin nopeaa, sekä niistä on kehittynyt entistä monipuolisempia ja muunneltavampia. (Forsberg & Lamponen 2014, 3)

Nykyaikaiset tekniset ratkaisut ovat mahdollistaneet kokonaan langattomien hälytysjärjestelmien sekä reaaliaikaiseen paikantamiseen perustuvan järjestelmien kehityksen. Erilaisiin hälytysjärjestelmiin on mahdollista integroida rinnalle toimimaan muita turvaavia järjestelmiä kuten henkilöturva-, palo-, kulunvalvonta- tai potilastietojärjestelmiä. Useat toimittajat markkinoivat järjestelmiään erilaisilla nimillä ja termeillä, jotka saattavat sekoittua keskenään. Yritysten myyntihenkilöillä on usein tapana käyttää tiettyjä termejä eri asiayhteyksissä markkinoidessaan järjestelmiä asiakkailleen. (Forsberg & Lamponen 2014, 3)

2.1 Perustietoa järjestelmistä

Tänä päivänä erilaisia hälytysjärjestelmiä voidaan käyttää monissa erityyppisissä tarkoituksissa, kuten tässä tapauksessa henkilökunnan henkilöturvajärjestelmänä tai hoitajien avunpyyntöjärjestelminä. Tehtyyn hälytykseen voi vastata muun henkilökunnan lisäksi myös ulkoisesti hankitun turvallisuuspalvelun henkilö. Hälytysjärjestelmä käsittää terminä laajemman kokonaisuuden kuin hoitajakutsu- tai henkilöturvajärjestelmä. Henkilöturvajärjestelmä tarkoittaa kokonaisuutta, jossa tekninen laitteisto tuo mahdollisuuden hälyttää väkivaltatilanteissa apua tahoilta, joiden kanssa on sovittu ennalta avun antamisesta. (Forsberg & Lamponen 2014, 7)

2.1.1 Järjestelmän yleinen toiminta

Turvahälytyksen henkilökunta tekee hälytyspainikkeella tai tietyissä järjestelmissä hälytys voi tapahtua automaattisesti. Automaattinen hälytys vaatii kuitenkin sen, että järjestelmään määritellään ehdot, joiden täyttymistä kyseessä oleva järjestelmä tarkkailee. Hälytys välittyy palvelimelle, josta hälytyksen tiedot välitetään kansliakoneille, käytävänäytöille sekä henkilökunnan mukana oleviin langattomiin Dect-puhelimiin. Järjestelmä voi myös tukea paikannusta, jolloin henkilökunta saa avunpyytäjän tarkan sijainnin. (Forsberg & Lamponen 2014, 7)

Langattoman hälytysjärjestelmän toiminta voidaan toteuttaa käyttämällä WLAN -verkkoa, GSM -yhteyttä, Bluetooth - tai radiotaajuus-tekniikkaa. Hälytysjärjestelmät, jotka käyttävät tietoliikenneverkkoa toimiakseen kutsutaan IP-pohjaisiksi järjestelmiksi. Näistä on nykytekniikan aikana tullut entistä yleisempiä käytettyjä ratkaisuja. Internetprotokollaa käyttävä järjestelmä vaatii toimiakseen verkkoyhteyden. Langaton internetyhteys on mahdollista saavuttaa WLAN -verkolla tai mahdollisesti nettitikulla, eli mokkulalla. Käyttämällä IP -pohjaista ratkaisua, se mahdollistaa palvelun ostamisen talon ulkopuolelta. Tällöin omistajatahon ei tarvitse hankkia omaa palvelinta, kun palvelin sijaitsee toimittajan ylläpitämässä palvelinkeskuksessa. (Forsberg & Lamponen 2014, 8)

2.1.2 Järjestelmän osia yleisellä tasolla

Henkilöturvajärjestelmä koostuu tavallisesti henkilöhälyttimistä, asukaspäätteistä tai huonekojeista, palvelinympäristöstä, hallintaohjelmistosta sekä erityyppisistä hälytyksen vastaanottimista. Nykyaikaisissa ratkaisuissa hälytysilmoitukset saapuvat pääsääntöisesti henkilöstön langattomiin IP -, GSM - ja Dect -puhelimiin. Näiden laitteiden lisäksi hälytyksen on mahdollista tuoda esille käytävänäytöille, kanslian työasemille ja graafisissa pohjakuvissa työasemien näytöille. (Forsberg & Lamponen 2014, 9)

Hälytysjärjestelmä vaatii toimiakseen palvelimen, mutta joissakin toimittajien tarjoamissa ratkaisumalleissa, tällaista vaatimusta ei välttämättä enää ole. Järjestelmän palvelin voi sijaita organisaation omissa tiloissa tai esimerkiksi toimittajan omissa tiloissa, kuten konesalissa. Tänä päivänä myös pilvipalveluiden tuottamat ratkaisumallit ovat yleistyneet markkinoilla kasvavin määrin. Hallintaohjelmisto voi tällaisissa tapauksissa sijaita kokonaan toimittajan tai muun toimijan ylläpitämässä pilvipalvelussa virtuaalisena. Järjestelmään kokonaisuuteen kuuluvat hälyttimet voivat olla kytkettynä langattomasti tai langallisesti palvelimeen. Järjestelmän toimintaa tukeva ohjelmisto sijaitsee palvelimella kuten myös järjestelmän oma tapahtumaloki ja hälytysmääritelmät. Ympäristön toimintaa hallinnoidaan tavallisesti hälytysjärjestelmän omalla ohjelmistolla, joka sijaitsee järjestelmän palvelimella. (Forsberg & Lamponen 2014, 9)

Nykyaikaisiin henkilöturvajärjestelmiin on mahdollista liittää hälytyksenpaikannustoiminto. Tämän tehokkaan työkalun avulla saadaan hälytyksen tekijän tarkka sijainti selvitettyä rakennuksen sisätiloissa. Jotta paikannus toimisi tehokkaasti ja tarkasti, on rakennuksessa oltava kattava tukiasemaverkko ja henkilökunnalla paikannustunnistin mukanaan. Paikannus voi olla aluekohtainen, jolloin saadaan tieto alueesta esimerkiksi osaston ja/tai kerroksen tarkkuudella, missä hälytyksen tekijä sijaitsee. Jos paikannus on huonekohtainen, on tukiasemia sijaittava jokaisessa osaston huoneessa.
Nykyään myös reaaliaikainen paikannus on mahdollista. Henkilön sijainti voidaan selvittää tarkasti, jopa metrin tarkkuudella. Henkilöiden sijaintia voidaan tarkastella reaaliaikaisesti työasemilla toimivilla pohjakuvasovelluksilla. (Forsberg & Lamponen 2014, 14)

Hälytykset voidaan ilmaista esimerkiksi osastojen käytävänäytöillä, joissa ilmaistaan avunpyynnön sijainti osaston tai huoneen tunnuksen mukaan. Hälytykset on myös lisäksi mahdollista ilmoittaa samanaikaisesti kanslian työasemilla, vartijan työasemalla sekä hoitohenkilökunnan Dect -, GSM - tai IP -puhelimilla. (Forsberg & Lamponen 2014, 15)

3 ERILAISIA HENKILÖTURVAJÄRJESTELMIÄ

Turva-, ja hälytysjärjestelmiä on markkinoilla usealta eri toimittajalta. Esimerkiksi Ekahau RTLS (Real Time Location System), jota käytetään tähän opinnäytetyöhön pohjautuvassa projektityössä. Tässä kappaleessa esitellään 2M-IT Oy:n ylläpidossa olevia turvajärjestelmiä, joita käytetään eri sairaanhoitopiireissä. Kappaleessa tuodaan esille kolmen eri toimittajan ratkaisumallia, joita käytetään esimerkiksi Satakunnan- ja Varsinais-Suomen sairaanhoitopiireissä, Porin perusturvassa sekä Turunmaan sairaalassa.

3.1 Toimittajien ratkaisujen esittelyä

Varsinais-Suomen sekä Satakunnan sairaanhoitopiirin käytössä on Ekahaun lisäksi myös muita hälytysjärjestelmiä. Yleisen vertailun vuoksi, tässä työssä on esitelty muutama esimerkkiratkaisu, joita käytetään näissä sairaanhoitopiireissä. Ascom Miratel Innova on esimerkiksi käytössä Turunmaan sairaalassa ja Vivago Porin kaupunginsairaalassa ja Porin Perusturvassa. Ekahau on käytössä Turun yliopistollisen keskussairaalan T2 - ja A -sairaalan tiloissa.

3.1.1 Ascom Miratel Innova

Miratel Innova on toinen, IP -pohjaista ratkaisua käyttävä hälytysjärjestelmä. Se on yksi käytännöllisistä ratkaisuista palvelutaloille tai suuremmille hoito-organisaatioille. Miratel Innovan kokonaisuus koostuu hälyttimistä, lähetin -vastaanotinyksiköistä sekä kansliakoneista. Kokoonpano koostuu palvelimella sijaitsevasta järjestelmän hallinnointiohjelmistosta sekä mahdollisista tarvittavista lisälaitteista Tällaisia lisälaitteita ovat asukaspäätteet ja käytävänäytöt. Hallintaohjelmisto, jolla järjestelmää hallitaan, on nimeltään Aurora Osasto. (Forsberg & Lamponen 2014, 47)

Miratel Innovaan on mahdollista ottaa käyttöön myös puheyhteys asuntolaan asennettavien asukaspäätteiden ansiosta. Puheyhteyden avulla on mahdollista pyytää apua, kuunnella radiota tai hoitajien kuuluttaa erilaisia kuulutuksia asukkaille ja työyhteisölle. Paikantaminen onnistuu organisaation toimitiloihin asennettavien paikkalähetinyksiköiden välityksellä. Lähettimien määrä kiinteistössä määrittelee paikannuksen tarkkuuden. Hälytyksen voi järjestelmässä aktivoida langattomien hälyttimien välityksellä. Kokoonpanoon kuuluvat myös langalliset kutsulaitteet. (Forsberg & Lamponen 2014, 48)

Miratel Innova -järjestelmässä on myös mahdollista ottaa käyttöön henkilöturvaominaisuus. Hoitohenkilökunnan on mahdollista tehdä hiljainen hälytys Dect -puhelimen avulla. Tällainen hälytys tapahtuu ilman näkyvää hälytystä suoraan henkilökunnan

keskuuteen. Toinen tapa tehdä henkilöturvahälytys, on käyttää langattomia hälytyslaitteita tai huoneistoissa kalusteisiin kiinnitettävillä hälyttimillä. Järjestelmään on mahdollista integroida muita erillisiä turvajärjestelmiä. (Forsberg & Lamponen 2014, 48)

3.1.2 Vivagon ratkaisumalli

Vivagon tarjoamat ratkaisut mahdollistavat reaaliaikaisen turva- ja hyvinvointi -järjestelmien käyttöönoton. Järjestelmä täyttää perinteiset hoitajakutsujärjestelmän vaatimukset, joiden lisäksi Vivago kykenee tekemään automaattisen hälytyksen esimerkiksi tilanteissa, joissa henkilö ei kykene itse apua kutsumaan kuten potilaan ollessa tajuttomana. Vivagon tukijärjestelmä on joustava ja se on sopiva sekä pienille palveluyksiköille että suuremmille terveysalan organisaatioille. Järjestelmän kokonaisuuden perustana toimivat Vivago -tuoteperheen tuotteet: CARE -kellot, Vista -sovellus sekä organisaation toimitiloihin asennetut Viva POINT -tukiasemat. Lisäksi järjestelmään on mahdollista liittää Room POINT -huonekojeita, langattomia AddOn -painikkeita sekä muun muassa langallisia hälytyspainikkeita ja vetonaruhälyttimiä. (Forsberg & Lamponen 2014, 64-65)

Henkilökunnan turvahälytykset on mahdollista toteuttaa, joko käyttämällä AddOn -painiketta tai CARE -kelloa. Kyseinen laite on langaton, kolikon kokoinen laite. Sitä on mahdollista henkilöstön kuljettaa mukanaan taskussa, kaulalla tai esimerkiksi vyöllä. CARE -kello voi hälyttää myös tilanteissa, joissa hoitaja ei itse kykene tekemään hälytystä. Tällaisia tilanteita on esimerkiksi hoitajan tajunnan menetys. Turvahälytykset on mahdollista ohjata tietyille eri tahoille eri vuorokauden aikoina. Tällaisia tahoja ovat esimerkiksi ulkoisesti hankittu turvallisuuspalvelu tai toinen hoito-osasto. (Forsberg & Lamponen 2014, 66)

Hälytyksen yhteydessä on mahdollista toteuttaa automaattisesti avautuva kaksisuuntainen puheyhteys hoitajan ja asiakkaan välillä. Järjestelmän paikannus perustuu Vivagon sovellukseen, joka on nimeltään Viva POINT. Sovelluksen ja Room POINT -

huonekojeiden liittäminen organisaation tukiasemakokonaisuuteen, mahdollistaa hälytystilanteessa hälyttäjän tiedon välittämisen hoitohenkilökunnalle tukiaseman tarkkuudella. Hälytysviesti välitetään hoitohenkilökunnan puhelimiin ääni- ja tekstiviesteinä. Hälytysviesti sisältää tarkempia tietoja hälytyksen tekijästä, kuten mistä se on tullut, mikä hälytys on kyseessä ja tiedon siitä, miltä osastolta tai rakennuksen osasta hälytys on tullut. (Forsberg & Lamponen 2014, 66)

3.1.3 Ekahau Real Time Location System

Tässä opinnäytetyössä on käsitelty Ekahauta sen vanhalla nimellä. Tämän työn lähteissä ja Turun yliopistollisessa keskussairaalassa on vielä käytössä järjestelmän vanha nimi, Ekahau. Vuonna 2016 Ekahau RTLS:n osti Airista Flow niminen yritys. Fujitsu, joka ylläpitää palvelua TYKS:in ympäristössä, kutsuu järjestelmää Ekahau -nimellä. (Prnewswire 2016)

Ekahau on IP -pohjaista ratkaisua käyttävä henkilöturvajärjestelmä. Järjestelmä käyttää reaaliaikaista paikannusta hälytyksien sijainnin kohdentamiseen. Ekahau toimii organisaation tiloissa langattomasti, organisaation omaa WIFI -tukiasemaverkkoa hyväksikäyttäen. Kyseinen järjestelmä toimii samassa tietoliikenneverkossa muun tietoliikenteen rinnalla, eikä tarvitse omaa erillistä kaapelointia tai verkkoa toimiakseen. Järjestelmää käytetään ensisijaisesti erilaisten hoitolaitosten sekä sairaaloiden hoitajakutsu- ja henkilökunnan turvajärjestelmänä. Ekahauta käyttävät osiot on mahdollista integroida kohdeorganisaatiossa yhdeksi toimivaksi järjestelmäkokonaisuudeksi. Tämä tarkoittaa konkreettisesti sitä, että järjestelmään on integroitavissa muitakin turvallisuuden toimintoja erillisinä ohjelmiston moduuleina. (Forsberg & Lamponen 2014, 35)

Hälytysjärjestelmän kokonaisuus sisältää langattomat henkilöhälyttimet, joita henkilöstö kantaa mukanaan. Osastoilla huoneissa sijaitsevat kiinteät langattomat hälytyspainikkeet, sekä järjestelmän oman palvelinohjelmiston. Palvelimella toimii myös käytettävä työasemasovellus, josta hälytysten sijainnit ovat tarkasteltavissa. Tiloissa,

joissa paikannusta käytetään, on käytössä WLAN -pohjaiset RFID -tunnisteet. Kyseiset tunnisteet on mahdollista paikantaa käytettävän tukiasemaverkon sisällä muutaman metrin tarkkuudella. Organisaatiossa olevan verkon on oltava kattavammin ja tiheämmin rakennettu, kuin tavanomaiseen tiedonsiirtoon tarkoitettu tukiasemaverkko on yleisesti toteutettu. (Forsberg & Lamponen 2014, 36)

Ekahaun paikannus perustuu paikannettavan kohteen liikkeiden koottuihin historiatietoihin sekä tunnisteen signaalin vahvuuden mittaamiseen, organisaation tukiasemaverkoston avulla. RFID -tunnisteiden sijainti on mahdollista havainnoida työasemasovelluksesta rakennuksen pohjapiirustukseen perustuen reaaliaikaisesti. Järjestelmällä on mahdollista myös paikantaa tukiasemaverkon sisällä toimiva laite, jos vain laitteeseen on asennettu paikannusta toteuttava sovellus tai tunnistin. (Forsberg & Lamponen 2014, 36)

Tagi - eli RFID (Radio Frequency Identification) on pieni, langaton tunnistin. Kyseisiä tunnistimia käytetään Ekahaun paikannus- sekä kulunvalvontajärjestelmän kannettavissa sekä kiinteissä hälytinlaitteissa. Tunnistimen sisällä sijaitsevaan pieneen mikrosiruun voidaan tallentaa yksilöityä tietoa. Siruun tallennettua dataa on mahdollista välittää radioaaltotekniikan avulla, kattavan tukiasemaverkon välityksellä. (Forsberg & Lamponen 2014, 10)

Hälytykset tehdään painamalla hälytyspainiketta, jolloin hälytykset välittyvät järjestelmässä kuuluviin työasemiin ja tukiasemaverkossa toimiviin hälytyslaitteisiin sekä GSM -, Virve -, että Dect -puhelimiin tekstiviestinä. Tämän lisäksi hälytykset voivat näkyä kanslian työasemien näytöillä sekä osastojen omilla käytävänäytöillä. Hälyttimissä on myös kaksivärinen led-valo -ominaisuus sekä värinätoiminto. Nämä ominaisuudet viestittävät käyttäjälle laitteen erilaisista toiminnoista. Hälytykset on mahdollista kuitata samoilla laitteilla, kuin millä hälytykset on otettu vastaan. (Forsberg & Lamponen 2014, 36)

Lisäavunpyyntö, jossa on sekä sijaintitieto että hätäkutsu, on mahdollista toteuttaa järjestelmään kuuluvalla laitteella, jota henkilöstö kantaa mukanaan kaulanauhassa tai taskussa. Kyseinen kannettava laite, on yleensä muodoltaan henkilökorttimainen. Lait-

teessa on pieni led-näyttö, viestin lukemista varten. Laitteessa on myös kolme ohjelmoitavaa painiketta sekä akku, jota voidaan ladata. Hälytykset on mahdollista osoittaa useampaan haluttuun kohteeseen. (Forsberg & Lamponen 2014, 36)

3.2 Turvajärjestelmien käyttö hoitotyössä

Henkilöturvajärjestelmällä pyritään lisäämään henkilökunnan turvallisuutta luomalla turvallisen tuntuinen työympäristö, mutta kyseistä järjestelmää voidaan käyttää myös samanaikaisesti ennalta ehkäisemään vaarallisia tilanteita. Monilla aloilla ja tehtävissä ovat väkivalta sekä väkivallan uhka nousseet huomattavaksi työnsuojeluongelmaksi. Esimerkiksi tutkimusten mukaan, juuri terveydenhuoltoalan potilastyössä kohdataan lisääntyvissä määrin väkivaltaan yhdistettyjä työtapaturmia. Tällaisia tapauksia voivat olla esimerkiksi väkivaltaisten tai päihtyneiden potilaiden tai heidän perheidensä kohtaaminen ensiapu- tai ensihoitotilanteissa. (Siiki 2010, 92)

27 § Väkivallan uhka

”Työssä, johon liittyy ilmeinen väkivallan uhka, työ ja työolosuhteet on järjestettävä siten, että väkivallan uhka ja väkivaltatilanteet ehkäistään mahdollisuuksien mukaan ennakolta. Tällöin työpaikalla on oltava väkivallan torjumiseen tai rajoittamiseen tarvittavat asianmukaiset turvallisuusjärjestelyt tai -laitteet sekä mahdollisuus avun hälyttämiseen.

Edellä 1. momentissa tarkoitettua työtä ja työpaikkaa varten työnantajan on laadittava menettelyohjeet, joilla ennakolta kiinnitetään huomiota uhkaavien tilanteiden hallintaan ja toimintatapoihin, joilla väkivaltatilanteen vaikutukset työntekijän turvallisuuteen ja terveyteen voidaan torjua tai rajoittaa. Tarvittaessa on tarkistettava turvallisuusjärjestelyjen ja -laitteiden toimivuus.

Valtioneuvoston asetuksella voidaan antaa tarkempia säännöksiä työntekijän turvallisuuteen ja terveyteen liittyvistä järjestelyistä eri toimialoilla ja tehtävissä, joissa esiintyy ilmeistä väkivallan uhkaa.” (Työturvallisuuslaki 738/2002, 5 § 27)

Työpaikalla, jossa on todettu tavallista suurempi väkivallan vaara, tulee olla sen torjumiseen tai rajoittamiseen tarvittavat asianmukaiset turvallisuusjärjestelyt tai turvallisuuslaiteet olemassa. Työntekijällä tulee myös olla mahdollisuus avun hälyttämiseen tarvittaessa. (Siiki 2010, 94)

Työnantajan on huolehdittava, että työpaikan turvallisuus- sekä hälytyslaitteet ovat aina toimintakuntoisia. Työnantajan vastuulla on tarvittaessa myös tarkistuttaa säännöllisin väliajoin turvajärjestelmien ja -laitteiden toimintakyky. Työnantajan on osattava arvioida, milloin ja miten laitteiden sekä miten järjestelmien toimintakyvyn tarkistus suoritetaan. Tekniset hälytyslaitteet eivät saa kuitenkaan olla yrityksen ensisijainen väkivallan torjumiseen tarkoitettu väline, eivätkä missään tapauksessa ainoa keino väkivallan uhan torjunnassa. (Siiki 2010, 94)

Organisaatio voi varautua uhka- ja vaaratilanteisiin ja ennalta ehkäistä niitä myös monin erilaisin teknisin ratkaisuin. Nykyaikaiset tekniset turvaratkaisut ovat edistyneitä ja monipuolisia sekä niiden kustannukset ovat jatkuvasti laskeneet. Tekniikan tuomat mahdollisuudet työn turvallisuuden lisäämisessä, ovat hyvä ja välttämätön osa turvallisen työpaikan luomisessa. (Rantaeskola, Hyyti, Kauppila & Koskelainen 2015, 64)

Työnantajan on mahdollista hankkia työntekijöilleen mukana pidettäviä, henkilökohtaisia hälyttimiä, joiden avulla henkilökunta kykenee tehdä hälytyksen mistä sijainnista tahansa. Organisaatiossa voidaan turvautua myös kiinteään järjestelmään, joka on rakennettu osaksi työpisteisteisiin. Hälytyslaitteet ja -painikkeet on asennettava siten, että ne eivät häiritse hoitohenkilökunnan työntekoa, mutta ovat helposti käytettävissä hälytystilanteissa. (Rantaeskola ym 2015, 65)

4 PAIKANTAMINEN

Ulkotiloissa tapahtuva paikantaminen onnistuu satelliittien avustuksella. Nykyään toteutettava paikannus on hyvin tarkkaa, tyypillisesti muutaman metrin tarkkuudella. Kaupunkialueilla, satelliittien signaaleja häiritsevät korkeat talot. Sisätiloihin signaali ei näin ollen usein esteettä pääse. Jotta sisätilapaikannus toimisi saumattomasti satelliittipaikannuksen kanssa, tarvitaan uudenlaisia paikannustekniikoita. Tällaisia ovat esimerkiksi inertianavigointitekniikka sekä langattomat paikannusjärjestelmät. (Kuusniemi 2018)

Langattomia paikannustekniikoita ovat:

- Matkapuhelintukiasemien signaaliin perustuva paikantaminen
- Langattoman lähiverkon signaalivoimakkuuksien mittaamiseen perustuva paikannus
- Bluetooth-tekniikkaan perustuva paikannus
- RFID -tunnisteisiin perustuva paikantaminen
- Ultraääni- sekä infrapuna-tekniikkaan perustuva paikannus
- UWB -signaaleihin perustuva paikantaminen (Kuusniemi 2018)

4.1 WIFI -Paikantaminen

RFID -tunnisteita voidaan käyttää organisaation sisällä reaaliaikaiseen paikantamiseen WIFI -verkon avulla. WLAN -tukiasemien muodostamalla kattavalla verkolla, tunnisteet voidaan paikantaa kolmesta viiteen metrin tarkkuudella. Paikantaminen on mahdollista integroida karttapohjaisen sovelluksen kanssa, jolloin tunnisteet näkyvät esimerkiksi rakennuksen pohjapiirustuksen mukaisen kartan perusteella. Tunnisteen tarkka sijainti määritellään tukiasemien ja tunnistimien välillä kulkevien signaalien avulla. Tukiasemat mittaavat aikaa, jonka signaalin kulku tunnisteesta tukiasemaan ottaa. Vaaditaan vähintään kolme toisiaan lähellä sijaitsevaa tukiasemaa, jotta tarkka mittaustulos voidaan tehdä. Tukiasemat on sijoitettava tarkasti ja suunnitellusti organisaation sisätiloissa. (excitingIP 2009)

Aktiiviset RFID -tunnisteet käyttävät 802.11 WLAN -protokollaa toimintaansa. Tunnisteet voidaan yksilöidä ja paikantaa käyttäen organisaation omia WLAN -tukiasemia. Aktiiviset tunnisteet käyttävät WLAN -protokollaa lähettääkseen sijaintitietoja tietyin väliajoin tukiasemille. Tukiasemat taas välittävät signaaleista saadut tiedot RTLS -järjestelmälle, joka havainnollistaa käyttäjälle tunnisteiden fyysisen sijainnin organisaation tiloissa. (excitingIP 2009)

4.2 RFID -tekniikka yleisellä tasolla

Yleisnimitys radiotaajuuksia hyväksikäyttävälle paikannustekniikalle on RFID. Kyseistä tekniikkaa käytetään yleisesti asioiden ja esineiden tai henkilöiden tunnistamiseen, havainnointiin tai yksilöintiin. Radiotaajuus -tekniikka toimintaperiaate perustuu RFID -tunnisteeseen, joka on kooltaan pieni mikrosiru. Siruun voidaan tallentaa tietoja. RFID -lukija tulkitsee tunnisteeseen tallennetun tiedon radioaaltotekniikan avulla. (RFIDLab Finland Oy 2016)

RFID -tunnisteet ovat yksinkertaisia langattomia muistilaitteita. Tunnisteessa olevalle mikrosirulle voidaan tallentaa tuotetta yksilöiviä tietoja. Tuotetietojen syöttämisen jälkeen tunniste voidaan kiinnittää haluttuihin kohteisiin. Tämä tunnisteeseen tallennettu tieto luetaan RFID -lukijalla, joka välittää sirun sisältämän tiedon järjestelmään. Tunnistus on mahdollista tehdä ilman, että luettavaan kohteeseen ei ole suoraa katsekontaktia. Lukijan avulla on myös mahdollista muokata tunnisteen sisältämiä tietoja. RFID -tekniikkaa käytetään usein paikoissa, joissa käytetään viivakoodeja RFID:n rinnalla. (RFIDLab Finland Oy 2016)

RFID -tekniikka on ollut käyttökelpoista jo vuosikymmeniä ja sen käyttö onkin kasvanut monille aloille. Tällaisia aloja ovat esimerkiksi teollisuus ja logistiikka. Termin alle kuuluukin monta erilaista tekniikkaa. Lukuetäisyydet ja tunnistamisnopeudet vaihtelevat eri standardien väleillä. RFID -tekniikkaa on käytetty hyväksi muun muassa kulkuavaimissa ja matkakorteissa. (RFIDLab Finland Oy 2016)

Tunnisteiden valmistuskustannukset ovat ajan saatossa pienentyneet alkuperäisestä, samalla kun tunnisteiden fyysinen koko on pienentynyt. Vaikka tunnisteiden fyysinen koko on pienentynyt, on taas vastaavasti niiden tallennuskapasiteetti suhteessa kasvanut. Tämä on mahdollistanut RFID -tunnisteiden käytön useammilla sovelluskohteilla. Tunnisteiden käyttötapa sekä kohde vaikuttavat tunnisteiden tehoon, fyysiseen kokoon, lähetystaajuuteen, tallennuskapasiteettiin ja sen antennimalliin. (Suomen Standardisoimisliitto 2010, 9)

4.2.1 Aktiivinen tunniste

Aktiivisia tunnisteita käytetään yleisesti reaaliaikaista paikannusta vaativissa tilanteissa, kuten suljetuissa järjestelmissä. Suljettu järjestelmä tarkoittaa sitä, että tunniste ei poistu järjestelmän ”alueelta”. Hyvin suuri osa reaaliaikaista paikannusta käyttävistä järjestelmistä käyttää toimiakseen aktiivisia RFID -tunnisteita. (Cisco 2014) Aktiivinen tunniste sisältää oman virtalähteen, mikä parantaa tunnistimen lukuetäisyyttä. Tunnisteen tavanomaisena virtalähteenä on yleensä litiumparisto tai akku. Aktiivisella tunnisteella on suurempi muistikapasiteetti kuin virtalähteettömällä passiivisella tunnisteella. Aktiivinen tunniste kykenee tallentamaan sekä lähettämään tunnisteen tietojen lisäksi muita lisätietoja. Tunnisteen virtalähde voi olla hyvinkin pitkäikäinen jopa useita vuosia. Lukuetäisyys voi myös vaihdella useista kymmenistä metreistä jopa satoihin metreihin. (Suomen Standardisoimisliitto 2010, 39.)

Kuva 1 Aktiivisia tunnisteita (Cisco 2014)

4.2.2 Puolipassiivinen tunniste

Puolipassiiviset tunnisteet erottavat passiivisista tunnisteista siten, että ne käyttävät sisäänrakennettua virtalähdettä viestintä- sekä liitännäispiireille. On kuitenkin huomattava, että vaikka tunnisteet käyttäisivätkin sisäistä virtalähdettä, puolipassiiviset RFID -tunnisteet eivät käytä virtalähdettä radioaaltojen tuottamiseen. (Cisco 2014) Puolipassiivisella ei ole omaa lähetintä, vaikka se omaisikin oman virtalähteen. Tunniste pystyy vahvistamaan signaalinsa takaisinsirontaprosessia, jonka ansiosta sen lukuetäisyys on passiivista tunnistetta suurempi. Puolipassiiviset tunnisteet kykenevät varmemmin välittämään suurempia tietomääriä, kuin passiiviset tunnisteet. Vaikka tunnisteen virtalähteestä loppuisi voima, kykenee se toimimaan myös passiivisena. (Suomen Standardisoimisliitto 2010, 38-39.)

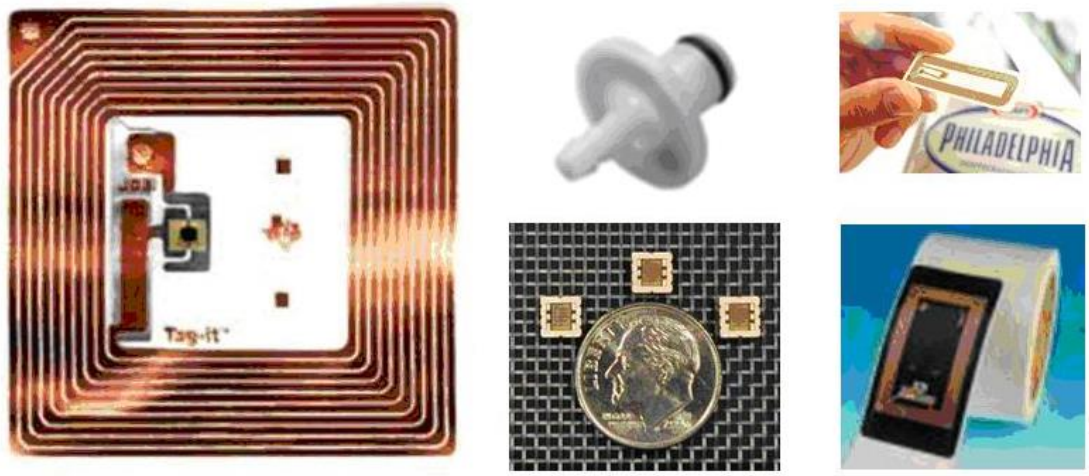
Kuva 2 Puoli-passiivinen tunniste (Cisco 2014)

4.2.3 Passiivinen tunniste

Passiivisilla RFID -tunnisteilla ei yleensä ole omaa sisäänrakennettua virranlähdettä, kuten litiumparistoja tai akkua. Passiivinen tunniste sen sijaan saa energiansa antenninsa avulla, RFID -lukijan energisoivalta sähkömagneettikentältä. Sähkömagneettisesta kentästä kytketty energia suoritetaan oikaisulla ja jännitteen moninkertaistuk-

sella. Tällöin tunniste saa tarvitsemansa energiamäärän toimiakseen. Tyypillisesti passiivinen tunniste ei kykene viestimään isäntäsovelluksen kanssa, ellei tunnistetta käsitellä RFID -lukijalla. (Cisco 2014)

Passiivisen tunnisteen lyhyen kantaman aiheuttaa sen virtalähteettömyys. Tämä vaatii sen, että RFID -lukijan on oltava tunnisteen lähellä. Tunnisteen lyhyt lukuetäisyys heikentää sen käytettävyyttä, mutta se voi olla käyttötavasta riippuen, jopa toivottu ominaisuus. Passiivinen tunniste on tässä tapauksessa hyvä vaihtoehto, jos tunnisteen lukeminen pidemmiltä etäisyyksiltä halutaan estää. Passiivinen tunniste voi säilyttää toimintakykynsä jopa kymmeniä vuosia. Tiedot on tuhottava tunnisteelta käsin, jos niitä ei enää haluta säilyttää tarpeellisuuden loppumisen jälkeen. (Suomen Standardisoimisliitto 2010, 38.)



Kuva 3 Passiivisia tunnisteita (Cisco 2014)

4.2.4 RFID:n käyttämät taajuudet

RFID -tekniikkaa käyttäviä tunnisteita ja lukijalaitteita on kehitetty useammalle eri taajuusalueille, jotta niiden soveltuvuutta erilaisiin käyttötarkoituksiin voitaisiin mahdollistaa. Näitä taajuusalueita on olemassa neljä erilaista. On todettu, että mitä korkeampi käytetty taajuus on, sitä pidemmälle sekä nopeammin tietoa voidaan siirtää.

Suurten taajuuksien heikkoutena on niiden suurempi herkkyys toimintahäiriöille nesteiden ja metallien läheisyydessä. Nopeimmin kehittyvä taajuusalue on nykyisin UHF -taajuuden käyttämä radiotaajuus. (Suomen Standardisoimisliitto 2010, 40)

RFID -tekniikan käyttämät taajuusalueet jaetaan neljään luokkaan:

- LF (Low Frequency) Taajuus alle 135kHz
- HF (High Frequency) Taajuus 13,56 MHz
- UHF (Ultra High Frequency) Taajuudet 869MHz – 928 MHz ja 433 MHz
- Mikroaallot 2,45 GHz tai 5.8 GHz (Suomen Standardisoimisliitto 2010, 40.)

Kun tunnisteiden lukuetäisyyttä halutaan kasvattaa, pitää ottaa käyttöön suuremmat taajuudet. Matalampien taajuuksien tunnisteet toimivat 125 KHz:n tai 134 KHz:n taajuusalueilla. Tällöin sovellukset käyttävät tavanomaisesti passiivisia tunnisteita. Matalilla taajuuksilla tiedonsiirron nopeus on hyvin alhainen. Matalien taajuuksien eli LF -taajuuksien tunnisteet, kykenevät toimimaan tilanteissa, joissa tunnisteet joutuvat kosketuksiin nesteiden, lumen tai metallien kanssa. Tällaiset olosuhteet ovat taas hyvin epäsuotuisia UHF -taajuuksien käytölle. Alhaisia taajuuksia käyttävät tunnisteet ovat edullisia, ne tarvitsevat vain vähän energiaa toimiakseen, eivätkä ole herkkiä suuntaukselle. (Suomen Standardisoimisliitto 2010, 40-41)

Sovellukset, jotka käyttävät korkeita RFID -taajuuksia, eli HF -taajuuksia, toimivat 13,56 MHz:n taajuudella. Tiedonsiirto HF -taajuudella toimii hieman nopeammin ja paremmin metallien ja nesteiden vaikutusalueella, kuin LF -taajuudella. Parempi toimintakyky nostaa HF -tunnisteiden hintaa suhteessa matalamman taajuuden tunnisteihin. HF -taajuuden tunnisteet ovat hieman herkempiä suuntaamiselle, kuin LF -tunnisteet, mutta ovat kohinalle vastustuskykyisempiä. HF -tunnisteita käytetään esimerkiksi sairaaloissa, joissa niiden käyttämä taajuus ei sotke muiden sairaalassa toimivien laitteiden toimintaa. (Shepard 2005, 63)

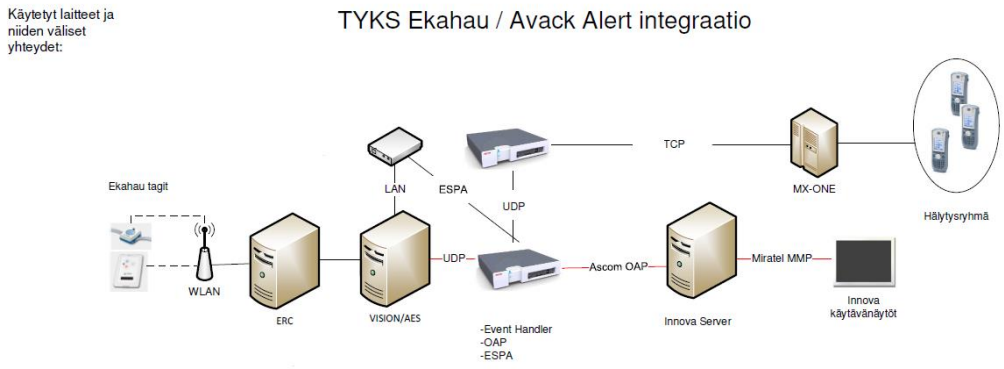
UHF -taajuudet, eli erittäin korkeiden taajuuksien passiiviset toiminnot, toimivat yleisesti taajuuksilla 868 MHz / 915 MHz. Aktiiviset toiminnot taas toimivat taajuuksilla 315 MHz / 433MHz. UHF -taajuuksia käyttävien tunnisteiden tiedonsiirto on hyvin nopeaa, mutta sen suorituskyky metallien ja kosteuden lähettyvillä on huono. (Suomen Standardisoimisliitto 2010, 42)

RFID -sovellukset, jotka käyttävät toimiakseen mikroaaltoja, kykenevät suuriin lukuetäisyyksiin ja tehokkaaseen tiedonsiirtoon lukijalta tunnisteelle. Tunnisteet toimivat valitettavan huonosti nesteiden ja metallien välittömässä läheisyydessä. Mikroaallot käyttävät toimintaansa 2,45 GHz tai 5,8 GHz:n taajuuksia. (Lahiri 2005, 1-48)

5 JÄRJESTELMÄARKKITEHTUURI

Turun yliopistollisessa keskussairaalassa käytössä oleva hälytysjärjestelmä ei koostu vain yhden toimittajan tuottamasta ratkaisusta, vaan kolmen eri toimittajan yhteen integroidusta kokonaisuudesta. Ascom:in osuus hälytysjärjestelmästä oli jo olemassa osana vanhaa potilaskutsujärjestelmää. Ekahau:sta puuttui rajapinta välittämään hälytykset käytävänäytöille sekä Dect -puhelimiin. Avack:in osuus kokonaisuudesta oli toimia viestin välittäjänä Ascom:in päätelaitteille ja henkilökunnan Dect -puhelimille.

Hälytys tapahtuu henkilöstön mukana kulkevilla henkilöhälyttimillä tai kiinteillä huonehälyttimillä. Hälytysviesti välitetään WIFI -tukiasemille, joista edelleen WLAN -verkon kautta Ekahaun ERC -palvelimelle (Kuva 4.). Tällä ERC -palvelimella on järjestelmän tietokanta, jossa on määriteltynä hälytysalueet ja osastot. ERC -palvelin lähettää tiedon Ekahau Vision -palvelimelle, joka esittää hälytyksen sijainnin organisaation pohjakartassa. Vision -palvelin välittää hälytyksen tiedot eteenpäin Avack:in AES -sovellukselle, joka taas muuntaa hälytyksen tiedot oikeaan muotoonsa. Viestintäpalvelin lähettää muunnetun hälytystiedon Ascom:in käytävänäytöille. Samalla hälytysviesti välittyy hoitohenkilöstön Dect -puhelimiin. Viestintäpalvelin lähettää hälytystä toistuvasti kahdeksan sekunnin välein, kunnes hälytys on käyty vahtimestarin tai vartijan toimesta kuittaamassa. Osastojen käytävänäytöillä hälytys toistuu 10 sekunnin välein. (Ascom 2017)



Kuva 4 Järjestelmän rakenne (Ascom 2017)

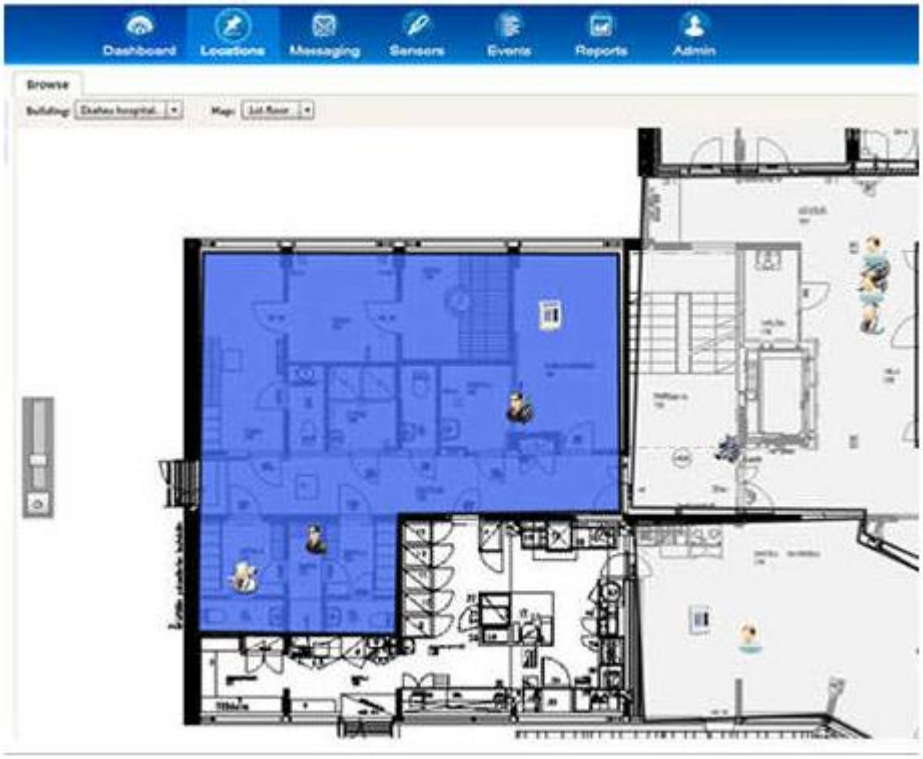
5.1 Järjestelmä Ekahaun näkökulmasta

Henkilöturvajärjestelmä on langattomasti toimiva hälytysjärjestelmä. Ekahau käyttää Turun yliopistollisen sairaalan T2 - sekä A -sairaalan langatonta WIFI -verkkoa toimintaympäristönään. Järjestelmä ei käytä yleistä tietoliikenneverkkoa, vaan toimii omana suljettuna verkkonaan sairaalan tietoliikenneverkon rinnalla. Kyseinen järjestelmä käyttää siis vain samaa infrastruktuuria. Turvapaikantimien, eli tagien, tarkka sijainti saadaan määriteltyä WLAN -tukiasemien välityksellä. Jotta henkilön tekemän hälytyksen sijainti saataisiin tarkasti selville, on rakennuksessa käytettävä tiheää tukiasemaverkostoa. Turvapaikantimet käyttävät paikantamiseen kolmea, sijainniltaan lähintä, tukiasemaa sijaintinsa määrittelemiseen. Turvapaikannin kytkeytyy langattomaan verkkoon lähimmän tukiaseman avulla. Tukiaseman, johon paikannin on kytkeytynyt ja kahden muun lähimmän tukiaseman avulla, paikantimen tarkka fyysinen sijainti voidaan saada selville. Tätä tapahtumaa kutsutaan kolmiomittaukseksi. (Fujitsu 2015)

5.1.1 Ekahau Vision -Pohjakuvasovellus

Vision on työasemasovellus, joka mahdollistaa hälytyksen paikantamisen organisaation pohjakuvan perusteella (kuva 5.). Vision mahdollistaa hälytyslaitteiden, ihmisten, tuotteiden tai laitteiden reaaliaikaisen paikantamisen organisaation toimitiloissa. Esi-

merkiksi turvallisuushenkilökunta voi havaita hälytyksen tarkan fyysisen sijainnin Vision:in avulla, omilta työasemiltaan. Sovellus ilmoittaa fyysisen sijainnin lisäksi esimerkiksi määritellyn osaston nimen sekä koodin. (Airistan Flown www-sivut 2018)



Kuva 5 Pohjakuvasovellus Vision (Airistan Flown www-sivut 2018)

5.1.2 Airista Flow B4 -henkilöhälytin

B4 -henkilöhälytin (kuva 6.) on langaton henkilökortin kokoinen, tietoliikenteellisesti kaksisuuntainen hälytin, jota hoitohenkilöstö kantaa mukanaan. Henkilöhälyttimen avulla henkilöstö kykenee vaaratilanteessa hälyttämään paikalle vartijan tai lisää hoitohenkilökuntaa. Henkilöhälyttimessä on myös sisäänrakennettu liiketunnistin, joka tunnistaa, jos käyttäjä on pidemmän aikaa liikkumatta, esimerkiksi tajuttomana. Pitkään paikallaan ollut hälytin havaitsee liikkumattomuuden ja laukaisee hälytyksen automaattisesti. Henkilöhälyttimessä on myös riistokytkin, jolloin laite hälyttää myös automaattisesti, koska laite on riuhtaistu nopeasti irti kaulanauhasta, tai rintataskusta. Henkilöhälyttimessä on myös pieni led-näyttö viestien välittämistä varten. (Airistan Flown www-sivut 2017)

Henkilöhälyttimessä on ladattava akku, joka voi toimia viikkoja ilman latausta. Akun käyttöikä riippuu tosin siitä, kuinka usein hälytin lähettää signaaleja tukiasemille. Mitä useammin signaalia lähetetään tukiasemille, sitä tarkempi on paikannustarkkuus. (Airistan Flown www-sivut 2017)

Kuva 6 Henkilöhälytin B4 (Airistan Flown www-sivut 2017)

5.1.3 Airista Flow A4 -huonehälytin

A4 -Huonehälytin (kuva 7.) on kiinnitettävissä erityyppisiin sairaanhoidon laitteisiin, huonekaluihin sekä osastojen hoitohuoneisiin. Huonehälytin on pölyn ja roiskeenkestävä. Laitteessa on litiumparistot, jotka ovat vaihdettavissa. Niiden kesto on yleensä viitisen vuotta. Huonehälyttimessä on kaksi painiketta, hälytyspainike vaaratilanteita varten sekä painike mahdollisten laiterikkojen varalle. Painike voi esimerkiksi välittää tiedon laiterikoista tekniselle toimistolle. TYKS:in tapauksessa, teknistä hälytystä ei laitteesta voi lähettää. Molemmista painikkeista tehdään henkilöturvahälytys. (Airistan Flown www-sivut 2017)

Kuva 7 Airista A4 huonehälytin. (Airistan Flown www-sivut 2017)

5.2 Hälytyksen teko vaaratilanteissa

Uhkaavan hätätilanteen sattuessa, henkilö painaa henkilöhälyttimessä tai huonehälyttimessä sijaitsevaa hälytyspainiketta, jolloin tieto hälytyksestä välitetään sairaalan langatonta verkkoa hyväksikäyttäen toisille hoitajille, vahtimestarille sekä vartijoille. Turvajärjestelmä välittää vastaanottajille osaston ja huoneen tarkkuudella hälytyksen sijainnin. Vartijoilla on käytössään työasemasovellus, joissa hälytyksen sijainti esitetään pohjakuvassa. Täten vartijan on helppo siirtyä kohteeseen, josta hälytys on aktivoitu.

Hälytyksen saatuaan vahtimestari, hoitohenkilökunta tai vartija siirtyy hälytyksen mukaiseen sijaintiin ja käy tarkistamassa tilanteen. Jokainen hälytystilanne on käytävä tarkistamassa paikan päällä. Tehtyä hälytystä ei saa kuitata pois, ilman että kohteessa on fyysisesti käyty tarkistamassa tilanne. Hälytykset on kuitattava hoidetuiksi työasemalla toimivalla järjestelmän sovelluksella, muuten hälytykset jäävät voimaan.

Hälytysjärjestelmän hankkija voi halutessaan laatia määritelmät, missä ja miten tehdyn hälytykset näkyvät ja kuuluvat. Järjestelmän omalla ohjelmistolla voidaan muokata osastojen hälytystekstit sopiviksi ja henkilökunnalle selkeiksi tulkita.

5.3 Järjestelmään kuuluvien laitteiden mahdollisia vikatilanteita

Arkipäiväisessä käytössä vikatilanteita esiintyy kaikista yrityksistä huolimatta. Organisaation pitää osata varautua mahdollisiin laitteiston häiriö- tai vikatilanteisiin, koska mikään järjestelmä ei ole täysin toimintavarma. Seuraavaksi on esitelty mahdollisia vikatilanteita, joita organisaatio voi kohdata.

- Sairaalan verkossa on toimintahäiriöitä, tai se on kokonaan alhaalla, eli poissa käytöstä.
- Langattomien tukiasemien verkko on alhaalla, jonka seurauksena hälyttimet eivät pysty ilmoittamaan paikannustietoja tukiasemille.
- Käytävänäytöissä voi olla häiriötä tai ne ovat rikki, jolloin hälytysten tiedot eivät näy oikein henkilöstölle.
- Dect -puhelinjärjestelmässä on vikaa, jolloin hälytykset eivät välity henkilöstön työpuhelimiin.
- Paikantimet eivät toimi, mikä tarkoittaa, että henkilökunta ei pahimmassa tapauksessa pysty edes tekemään hälytystä. (Fujitsu 2015)

Hälytysalueita suunnitellessa, asianomaisen organisaation on otettava huomioon järjestelmän mahdolliset rajoitteet. Koska kyseinen järjestelmä käyttää sairaalan langatonta verkkoa toimiakseen, on yleiset katvealueet, kuten portaikko tai hissi otettava huomioon. Tekniset työtilat kuten pannuhuoneet, saattavat myös heikentää paikantimien toimintaa. (Fujitsu 2015)

6 VERSIOPÄIVITYSPROJEKTI

Projektin alkuvaiheessa, selvitettiin mikä on projektin ja versiopäivityksen tavoite. Miksi tiettyjä suunniteltuja toimenpiteitä täytyy tehdä ja mihin osa-alueisiin kakki tarvittavat toimenpiteet tulevat projektin edetessä vaikuttamaan. Järjestelmien versiopäivityksiä ei voi tehdä suunnittelematta nopealla tahdilla, vaan ne on suunniteltava perusteellisesti alusta loppuun. Prosessiin kuului riskien kartoittaminen sekä toimenpiteiden huolellinen suunnittelu. Oli otettava huomioon tulevan versiopäivityksen vaikutukset muihin sivullisiin järjestelmiin. Esimerkiksi, jos päivitettävän järjestelmän ympäristössä on toiminnassa muita sen toimintaa tukevia järjestelmiä, on tehdyt muutokset muokattava niihin yhteensopiviksi. Tällöin vuorovaikutus järjestelmien välillä jatkuu ongelmitta.

On otettava myös huomioon prosessin aiheuttamat katkot järjestelmien toiminnassa ja tietoliikenteessä. Päivityksen aiheuttamat katkotilanteet tulee suunnitella etukäteen sekä tehdä riskiarvio sen vaikutuksista muihin järjestelmiin. Pitkä suunnittelematon katko voi vaikuttaa järjestelmien toimintaan negatiivisesti. Samoin myös viestintä prosessin eri osapuolien kanssa on pidettävä mielessä. On erityisen tärkeää, että henkilökunta, jotka käyttävät päivitettävää järjestelmää, ovat tietoisia tehtävistä muutoksista ja katkoista. Tällöin vältytään turhilta yhteydenotoilta ja vikailmoituksilta.

6.1 Päivityksen suunnitteluvaihe

Projektin aloituspalaverissa kartoitettiin työryhmän kanssa päivitysprosessin alkutilannetta. Alkutilanteessa todettiin, että järjestelmä sijaitsee vanhenevalla palvelinalustalla. Uudet korvaavat palvelinalustat oli jo suunniteltu ja valmiiksi pystytetty. Turvajärjestelmä oli jo asennettuna uusilla tuotantopalvelimilla, mutta järjestelmän palvelut olivat poiskytkettyinä. Alkuperäiseen suunnitelmaan kuului vanhan verkon jatkaminen toiseen konesaliin, jossa uudet tuotantopalvelimet sijaitsivat. Vanhat palvelimet olivat verkossa, jonka jatkamista alun perin suunniteltiin.

Projektin aloituspalaveri pidettiin 2M-IT:n, Fujitsun, Ascomin, Avackin ja TYKS:in teknisen toimiston kesken. Kokouksessa käytiin läpi tarvittavat verkkomuutokset, mitä uuden turvajärjestelmän päivitys vaatisi. Samalla käsiteltiin IP -osoitteiden tarve pysyä muuttumattomana palveluiden käytön siirtyessä vanhoilta palvelimilta uusille.

Kyseessä olevaa verkkomuutosta varten oli tehtävä verkon jatkamisen vaikutusanalyysi. Analyysissä arvioitiin verkon jatkamisen aiheuttaman katkoksen vaikutus muihin verkossa toimiviin järjestelmiin, sovelluksiin ja palveluihin. Samassa verkossa sijaitsi useita tärkeiden järjestelmien palvelimia, joihin katko saattoi vaikuttaa. Tämän vuoksi oli hyvin tarpeellista selvittää toimenpiteen aiheuttaman katkon suuruus. Vaikutusanalyysin perusteella, voitiin varautua mahdollisiin ongelmatilanteisiin oikealla tavalla. Pidempi suunnittelematon katko verkossa sijaitsevissa tietokanta-palvelimissa voisi osoittautua ongelmalliseksi. Versiopäivityksen yhteydessä, Ekahaun tietokannat siirtyisivät uudelle palvelimelle. Järjestelmän työasemien ohjelmaan ei tule muutoksia, vain palvelimen sovelluksen versio muuttuu.

Seuraava työryhmän tekninen kokous pidettiin Turussa kesäkuun kahdeskymmenesensimmäinen päivä. Kokouksessa käytiin läpi Ekahaun toimintatapaa. Hälytysjärjestelmä käyttää sairaalan omaa tukiasemaverkkoa toimintaansa. Tehtäväksi tuli selvittää, onko lähivuosina tehty sairaalan osastoilla tukiasemamuutoksia tai vaihdoksia. Jos laitevaihdoksia oli osastoilla tehty, tuli vaihdettujen laitteiden MAC -osoitteet selvittää, sekä välittää tieto siitä Fujitsun yhteyshenkilölle. Tukiasemat ajettiin järjestelmään MAC- osoitteen perusteella, joten oli tärkeää selvittää, oliko muutoksia tapahtunut.

Kokouksessa päätettiin myös käydä läpi järjestelmän työasemat, joissa turvajärjestelmän pohjakuvasovellusta käytetään. Tällä selvitettiin, ovatko työasemien osoitteet oikein järjestelmän tietokannassa, jotta hälytykset tulevat oikeisiin työasemiin. Työasemien nimellä ei ollut asiassa tärkeyttä, vain IP -osoitteella. Toimittaja korosti IP -osoitteen muuttumattomuuden tärkeyttä, jotta vältettäisiin paljolta määrittelytöiltä. Kaikkien järjestelmässä käytettävien laitteiden IP -osoitteiden on oltava kiinteitä.

Tiistaina syyskuun kahdentenakymmenentenäyhdeksäntenä päivänä, suoritettiin suunniteltu vanhan verkon laajennus uuteen konesaliin, joka oli edellytyksenä versiopäivityksen aloittamiseen. Suunniteltua verkon laajennusta ei kuitenkaan kyetty suorittamaan loppuun asti. Syy tähän oli se, että verkossa sijaitsi fyysisiä palvelimia, joiden liittymät menisivät poikki, jos laajennus suoritettaisiin sellaisenaan. Alun perin tietona oli, että verkossa olisi ollut vain virtuaalisia palvelimia. Täten verkon laajennusta ei suoritettu, mutta uutta vaihtoehtoista suunnitelmaa aloitettiin heti kehitellä. Uutena ratkaisumallina oli uusien virtuaalisten palvelimien siirto konesaliin yksinään. Vanhassa suunnitelmassa kaikki verkon palvelimet olisivat siirtyneet, mutta nyt päätettiin siirtää vain Ekahaun palvelimet. Tämän vuoksi epäonnistunut verkon jatkaminen, ei haitannut varsinaista versiopäivityksen suunnittelua sekä toteutuksen etenemistä. Kun uudet palvelimet olivat siirretty konesaliin onnistuneesti, alkoi Fujitsu päivittämään turvajärjestelmän versiota uuteen.

Perjantaina lokakuun kahdentenatoista päivänä, työryhmän palaverissa todettiin Fujitsun saaneen järjestelmän päivityksen valmiiksi. Tämä merkitsi työn olevan siinä vaiheessa, että uusien tuotantopalvelimien käyttöönottoa ja testaamista voitaisiin alkaa suorittamaan. Palaverissa suunniteltiin ”workflow”, eli työjärjestys, jota työryhmä noudattaisi varsinaisen päivityksen aikana ja jokaiselle työryhmän jäsenelle määriteltiin oma rooli päivitysprosessin aikana. Palvelimien vaihto ja testaus päätetiin suorittaa marraskuun kuudentena päivänä. Turvajärjestelmän katkosta ilmoitettiin sairaalan henkilöstölle, jotta turhilta sekaannuksilta vältyttäisiin.

6.2 Versiopäivityksen suoritus

Työ aloitettiin aamulla, marraskuun kuudentena päivänä 2018. Työn ensimmäinen etappi oli varmistaa työryhmän läsnäolo ja valmius tehtävän aloitukseen. Työryhmän kesken pidettiin yllä keskusteluohjelma skype:ssä keskustelukanavaa auki koko prosessin ajan. Kanavalla tiedotettiin päivityksen edistymisestä sekä ratkottiin yhdessä ongelmatilanteita tehokkaasti. Samalla kaikki työryhmän henkilöt pysyivät koko päivitysprosessin myötä ajantasalla.

Varsinainen päivitysprosessi aloitettiin sammuttamalla vanhat turvajärjestelmän tuotantopalvelimet. Palvelimien sammutus tapahtui 2M-IT:n toimesta. Vanhat palvelimet sammutettiin ja turvajärjestelmän palvelut muutettiin, varmuuden vuoksi, manuaalisesti disabled -tilaan. Samoin virtuaalipalvelimien verkkokortit asetettiin disabled -tilaan, jotta samanaikaista vanhojen ja uusien tuotantopalvelinten päällä oloa ei pääsisi tapahtumaan. Uusiin tuotantopalvelimiin asetettiin vanhojen palvelimien IP -osoitteet ja DNS -viittaukset, joita vanhoissa palvelimissa käytettiin. Tämän toimenpiteen lopuksi, uudet palvelimet varmuuden vuoksi käynnistettiin uudelleen. Palveluiden käynnistyminen varmistettiin, sekä ne asetettiin käynnistymään automaattisesti aina palvelimen käynnistyksen yhteydessä.

Sairaalalla työryhmän testihenkilöstö vahvisti Ekahaun paikannuksen toimivan normaalisti. Seuraavana askeleena oli suorittaa turvajärjestelmässä muutama testihälytys, jotta järjestelmän toiminta saataisiin todettua toimivaksi. Testauksen edetessä tuli ilmi, että hälytyksien ilmoitukset näkyivät normaalisti osastojen käytävänäytöillä, mutta henkilökunnan Dect -puhelimiin viestit eivät tulleet perille. Testaushenkilöt alkoivat selvitellä tilannetta.

Tilanteen arviona oli, että uudelta tuotantopalvelimelta puuttuisi oikein määritelty COM-portti, joka välittää hälytykset oikeaan paikkaan. Uuteen palvelimeen asennettiin hallintasovellus, jolla kykenee määrittelemään COM -porttien määritelmiä. Palvelimelle määriteltiin portti ja viestintäpalvelimen IP -osoite. Mallia määritelmiin katsottiin vanhoilta palvelimilta, missä yhteydet toimivat vanhassa kokoonpanossa oikein. Toimenpiteen jälkeen työryhmä piti pienen tauon, jonka jälkeen uudet määritelmät testattiin.

Uuden testauksen jälkeen todettiin, että nyt hälytyksen viestit välittyivät Dect -puhelimille. Mutta samalla huomattiin, että hälytyksen paikannuksessa oli joitain ongelmia. Hälytykset saattoivat mennä nyt väärälle osastolle. Ongelmaa alettiin tutkia ja varauduttiin järjestelmän palauttamiseen vanhaan kokoonpanoonsa. Tässä tapauksessa vanhat turvajärjestelmän palvelimet palautettaisiin tuotantoon, ja uudet palvelimet sammutettaisiin.

Useamman testihälytyksen jälkeen kuitenkin todettiin paikannus toimivaksi. Ekahau toimi testien mukaan moitteettomasti. Hälytyksien tiedoissa oli virheitä vain yhden hoitoyksikön kohdalla. Oletettavasti vikaa oli Avack:in paikannustiedoissa, asiaa tosin päätettiin selvittää erillisenä ongelmana. Työryhmän päätös oli jäädä käyttämään uusia tuotantopalvelimia. Vanhat turvajärjestelmän palvelimet päätettiin jättää talteen varmuuden vuoksi, jos jotain tarvetta palauttamiselle ilmestyisi. Näin ollen todettiin työryhmän kesken versiopäivitysprosessi onnistuneeksi.

6.3 Projektin tulosten läpikäynti

Useamman tehdyn testihälytyksen jälkeen todettiin, että järjestelmä toimi vakaasti ja oikein uusilla palvelinalustoilla. Paikan päällä ollut testihenkilöstö totesi ja vahvisti, että järjestelmän versiopäivitys oli suoritettu päätökseen onnistuneesti. Tehdyt testihälytykset näkyivät ja paikantuivat oikein. Hälytysten sijaintitiedot välittyivät myös oikeille tahoille ja laitteille.

Vaikka versiopäivitys sujui melko hyvin ja onnistuneesti, päivityksen aikana havaittiin ongelmatilanteita. Havaitut ongelmatilanteet oli hyvä raportoida jatkoa ajatellen, jotta niiltä vältyttäisiin seuraavissa päivityksissä. Päivitysprosessin aikana, havaittiin, että uusilta tuotantopalvelimilta puuttui järjestelmää tukevia sovelluskomponentteja. Hälytykset eivät välittyneet henkilöstön Dect -puhelimiin oikein. Ongelmaa ratkottiin työryhmän kanssa ja puuttuva sovellus asennettiin tuotantopalvelimelle. Sovellus, jolla hallinnoitiin palvelimen portteja, puuttui kyseiseltä palvelimelta. Onneksi projektitiimillä oli valmis keskusteluyhteys, jolloin havaittu puute saatiin nopeasti ratkaistua. Tapaus opettaa, miksi hyvin tehty taustatyö on aina tarpeellista tehdä huolella ennen asennusten aloittamista.

Toinen tärkeä, usein unohtunut ja toisinaan aliarvostettu kunnollinen dokumentointi, jää monesti tekemättä. Suoritetun päivityksen jälkeen, järjestelmän kokonaisuuteen tuli muutoksia. Järjestelmän alusta muuttui, joten on tarpeellista korjata tiedot kaikissa järjestelmää koskevissa dokumenteissa. Samoin dokumentteihin on hyvä kirjata päivityksen aikana havaitut puutteet, jolloin tulevissa tapauksissa vältetään samat virheet.

LÄHTEET

Ascom 2017. TYKS Ekahau / Avack intergraatio.

Airista Flow 2018. Airista flow universal visibility software. Yrityksen kotisivut. Viitattu 22.11.2018. https://www.airistaflow.com/software/

Airista Flow. 2017. Yrityksen kotisivut. Viitattu 22.11. 2018. https://www.airistaflow.com/wp-content/uploads/2016/09/AiRISTAFlow_B4.pdf

Airista Flow. 2017. Yrityksen kotisivut. Viitattu 22.11.2018- https://www.airistaflow.com/wp-content/uploads/2016/07/AiRISTAFlow_RTLS_A4_DS.pdf

Cisco, WiFi Location-Based Services 4.1 Design Guide. Viitattu 22.10.2018. https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/WiFiLBS-DG/wifich6.html

excitingIP 2009. Location Tracking using Wi-Fi based RFID Tags Viitattu 22.10.2018. http://www.excitingip.com/335/location-tracking-using-wi-fi-based-rfid-tags/

Forsberg, K., Lamponen, M. 2014. Apua paikalle – Kooste avunpyyntöjärjestelmistä. Helsinki: Kopio Niini Oy.

Fujitsu 2015. VSSHP A- ja T-sairaalan henkilöturvajärjestelmä.

Kuusniemi, H. 2018. Maanmittauslaitos. Viitattu: 13.11.2018. https://www.maanmittauslaitos.fi/tutkimus/teematietoa/sisatilanavigointi

Lahiri, S. 2005. RFID Sourcebook. IBM Press ISBN 0131851373

PR Newswire. 2016. Viitattu 13.11.2018. https://www.prnewswire.com/news-releases/airista-announces-acquisition-of-ekahau-rtls-300230238

Rantaeskola, S., Hyyti, J., Kauppila, J., Koskelainen, M. 2015. Haastavat asiakastilanteet – väkivalta työssä. Viro: Print Best.

RFID Lab Finland Oy. 2016. Mitä on RFID? Viitattu 16.10.2018. http://www.rfid-lab.fi/rfid-teknologia-teknologia/mita-on-rfid/

SFS. 2010. RFID. Osa 1: Opas. Johdatus Tekniikkaan. Helsinki: SFS.

Shepard, S. 2005. RFID Radio Frequency Identification. The McGraw-Hill Companies ISBN 0-07-144299-5

Siiki, P. 2010. Työturvallisuuslaki. Helsinki: Edita Prima Oy.

Työturvallisuuslaki 23.8.2002/738. Viitattu 1.8.2018. http://www.finlex.fi/fi/laki/ajantasa/2002/20020738

2M-IT Oy. 2018. Yrityksen kotisivut. Viitattu 22.11.2018. https://2m-it.fi/yritys/

LIITE 1

VARSINAIS-SUOMEN
SAIRAANHOITOPIIRI

Aleksi Mahlamäki

Varsinais-Suomen sairaanhoitopiirin ky
Risto Pajunen
PL 52
20521 TURKU

Opinnäytetyö: Henkilöturvajärjestelmän päivitys / VSSHP ky Tyks

Varsinais-Suomen sairaanhoitopiirin ky myöntää luvan Aleksi Mahlamäelle käyttää Tyks:n Ekahau-henkilöturvajärjestelmän päivityksen kuvaamista opinnäytetyössään.

Lisäksi opinnäytetyössä voidaan käyttää asiaan liittyviä laitetoimittajilta saatuja tietoja, jotka toimivat työn lähdeaineistona.

Vsshp ky myöntää opinnäytetyölle omalta osaltaan julkaisuluvan.

Turussa 7.12.2018

Risto Pajunen
sähkön käytön johtaja
sähkötöiden johtaja
VSSHP ky:n sähköyksikön päällikkö