Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Miika Pojanluoma

Lähtevien kuljetusyksiköiden tunnistamisen automatisointi

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Automaatiotekniikka

Insinöörityö

31.5.2020

Tekijä Otsikko Sivumäärä Aika	Miika Pojanluoma Lähtevien kuljetusyksiköiden tunnistamisen automatisointi 43 sivua + 4 liitettä 31.5.2020
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	automaatiotekniikka
Ammatillinen pääaine	kappaletavara-automaatio
Ohjaajat	jakelupäällikkö Juhani Jäppinen lehtori Reijo Leinonen

Tämän opinnäytetyön tavoitteena oli selvittää kohdeyrityksen lähtevien kuljetusyksiköiden tunnistamisen automatisoinnin mahdollisuutta ja tuottaa tekninen ratkaisu sen toteuttamiseksi. Automatisoinnilla halutaan parantaa asiakaskokemusta, vähentää virheistä johtuvaa selvitystyötä sekä lähettämössä tehtävää manuaalista työtä. Opinnäytetyö on muodoltaan selvitystyö, jonka pohjalta on tarkoitus tehdä päätös työssä esitetyn ratkaisun toteuttamisesta.

Työ aloitettiin tutustumalla tarkemmin nykyisin käytössä olevaan prosessiin. Prosessiselvityksen jälkeen listattiin toiminnallisuustarpeet ja ympäristövaatimukset, joiden pohjalta laadittiin alustava vaatimusmäärittely. Tarpeiden ollessa selvillä aloitettiin automaattisen tunnistuksen ja tiedonkeruun menetelmien ja tekniikoiden tutkiminen ja keskenään vertaileminen. Kun sovellukseen parhaiten sopiva tekniikka oli valittu, täydennettiin vaatimusmäärittelyyn tekniikan standardit, jotka määrittelevät sovellukseen sopivan järjestelmän. Järjestelmän toteuttamiseksi valittiin vaatimusmäärittelyn toteuttava laitteisto ja laadittiin kustannusarvio muutamia laitevaihtoehtoja käyttäen.

Kohdeyrityksen sovellukseen parhaiten sopivaksi vaihtoehdoksi todettiin UHF-taajuusalueen RFID-tekniikka, eli radiotaajuustunnistustekniikka. Se mahdollistaa lähtevien kuljetusyksiköiden tunnistamisen automaattisesti ja kontaktittomasti hyvällä suoristusnopeudella ja varmuudella.

Avainsanat	tunnistaminen, AIDC, viivakoodi, RFID, UHF, kuljetusyksikkö

Author Title Number of Pages Date	Miika Pojanluoma Automatization of Identification of Outbound Transportation Units 43 pages + 4 appendices 31 May 2020
Degree	Bachelor of Engineering
Degree Programme	Electrical and Automation Engineering
Professional Major	Automation Technology
Instructors	Juhani Jäppinen, Distribution Manager Reijo Leinonen, Senior Lecturer

The aim of this thesis work was to research possibilities to automatize the identification of the outbound transportation units in the target company and to produce a technical solution to accomplish it. The desirable achievements of automating the process are better customer experience, a reduction in the number of error investigation and in manual labor in the dispatch department. This thesis study is going to be used as a base for the decision to implement the proposed solution.

Thesis work was started by exploring the current process more profoundly, after which a requirements analysis was made. When the desired functionalities were clear, different techniques of AIDC, or Automatic Identification and Data Capture, were researched. Suitable technique was selected, and the requirements analysis was extended with the corresponding standards. To design the system, appropriate hardware was decided, and a cost estimate with a few different hardware options was made.

As a result, it was concluded, that the most suitable identification technique for the process is RFID, or Radio Frequency Identification, in the UHF frequency range. With the chosen technique it is possible to automatize the identification of the outbound transportation units, making it contactless with good performance and reliability.

Keywords	Identification, AIDC, Barcode, RFID, UHF, transportation unit

Sisällys

Liite 3. Lukualueiden sijainnit lastauslaitureilla

Liite 4. Laitteiston kustannuksia eri toimittajilta

Lyhenteet

AGPS	*Assisted Global Positioning System.* Matkapuhelinverkon kautta saatavilla tiedoilla avustettu satelliittipaikannusmenetelmä.
AIDC	*Automatic Identification and Data Capture.* Automaattinen tunnistus ja tiedonkeruu.
BLE	*Bluetooth Low Energy.* Bluetoothiin pohjautuva matalan energiankulutuksen langaton tiedonsiirtoteknologia.
CDMA	*Code Division Multiple Access.* Taajuushyppelyyn tai suorasekventointiin perustuva törmäyksenestomenetelmä.
CRC	*Cyclic Redundancy Check.* Tarkistussummamenetelmä tiedon oikeellisuuden tarkistamiseen.
EC-GSM-IoT	*Extended Coverage GSM IoT.* EGPRS:ään perustuva matkapuhelinverkossa toimiva LPWAN-ratkaisu.
EGPRS	*Enhanced General Packet Radio Service.* GSM-verkkojen tiedonsiirtostandardi.
EPC	*Electronic Product Code.* Sähköinen tuotekoodi.
ETSI	*European Telecommunication Standards Institute.* Eurooppalainen telealan standardisoimisjärjestö.
FDMA	*Frequency Domain Multiple Access.* Usean eri taajuuden käyttämiseen perustuva törmäyksenestomenetelmä.
GPS	*Global Positioning System.* Satelliittipaikannusmenetelmä.
HF	*High Frequency.* Radiotaajuusalue 3–30 MHz.

IEC	*International Electrotechnical Commission.* Kansainvälinen sähköalan standardointiorganisaatio.
IEEE	*Institute of Electrical and Electronics Engineers.* Kansainvälinen tekniikan alan järjestö.
IoT	*Internet of Things.* Esineiden Internet.
ISO	*International Organization for Standardization.* Kansainvälinen standardisoimisjärjestö.
LF	*Low Frequency.* Radiotaajuusalue 30–300 kHz.
LLRP	*Low Level Reader Protocol.* Radiotaajuustunnistuksen standardi, joka määrittelee tiedonsiirron tietojärjestelmän ja lukijan välillä.
LoRaWAN	*Long Range Wide Area Network.* LoRa Alliance -järjestön standardoima globaali LPWA-verkkoteknologia.
LPWAN	*Low-Power Wide Area Network.* Langaton pitkän kantaman tiedonsiirtoverkko.
LRC	*Longitudinal Redundancy Check.* Tarkistussummamenetelmä tiedon oikeellisuuden tarkistamiseen.
LTE	*Long-Term Evolution.* Langaton tiedonsiirtotekniikka.
LTE-M	*Long-Term Evolution Machine Type Communication.* LTE:hen perustuva matkapuhelinverkossa toimiva LPWAN-ratkaisu.
NB-IoT	*Narrow Band Internet of Things.* LTE:hen perustuva matkapuhelinverkossa toimiva LPWAN-ratkaisu.
NFC	*Near Field Communication.* Radiotaajuuksilla toimiva etätunnistustekniikka.

OEM	*Original Equipment Manufacturer.* Alkuperäinen laitevalmistaja.
PoE	*Power Over Ethernet.* Virransyöttötekniikka lähiverkon parikaapelin avulla.
RFID	*Radio Frequency Identification.* Radiotaajuuksilla toimiva etätunnistustekniikka.
RSSI	*Return Signal Strength Indicator.* Paluusignaalin voimakkuus.
SDMA	*Space Division Multiple Access.* Usean lukualueen käyttämiseen perustuva törmäyksenestomenetelmä.
SHF	*Super High Frequency.* Radiotaajuusalue 3–30 GHz.
SSCC	*Serial Shipping Container Code.* Standardimuotoinen tunnistenumero kuljetus- tai varastointiyksikön tunnistamiseen.
TDMA	*Time Domain Multiple Access.* Vuorottaiseen kommunikointiin perustuva törmäyksenestomenetelmä.
TDOA	*Time Difference of Arrival.* Saman signaalin eri tukiasemille saapumisten aikaero.
UHF	*Ultra High Frequency.* Radiotaajuusalue 0,3–3 GHz.

1 Johdanto

Kohdeyrityksen lähettämöstä lähtee asiakkaille keskimäärin 16000 kuljetusyksikköä päivässä. Tällä hetkellä kuljetusyksiköiden tunnistaminen lähettämössä tapahtuu manuaalisesti skannaamalla kuljetusyksiköstä viivakoodi. Manuaalinen työ pitää sisällään aina automaation verrattuna suuremman virheen riskin sekä on tehottomampaa. Lisäksi uudelleen käytettävien kuljetusyksiköiden tarkkaa varastossa olevaa määrää ei ole reaaliaikaisesti tiedossa, joka hankaloittaa kiireisten aikojen suunnittelua.

Yllä kuvatun riskin pienentämiseksi ja toiminnan tehostamiseksi halutaan lähtevien kuljetusyksiköiden tunnistaminen automatisoida. Opinnäytetyön tavoitteena on tutkia automaattisen tunnistuksen ja tiedonkeruun tekniikoita ja tuottaa malli ja tekninen ratkaisu, jolla lähtevien kuljetusyksiköiden tunnistaminen voitaisiin kohdeyrityksessä tulevaisuudessa toteuttaa. Tätä kautta parannetaan asiakaskokemusta, vähennetään virheistä johtuvaa selvitystyötä sekä lähettämössä tehtävää manuaalista työtä.

Rajauksena työhön sisällytetään lähettämöön saapuvien ja lähettämöstä lähtevien laatikoiden käsittely. Huomioon otetaan mahdollisten käyttöönotettavien tunnistustekniikoiden hyötyjen laajentaminen tulevaisuudessa myös kuljetusterminaaleihin ja edelleen asiakaspäähän.

Nykyinen prosessi

Kohdeyrityksellä on käytössä lähteville kuljetuksille uudelleen käytettävät muoviset kuljetusyksiköt, joita lähtee asiakkaille keskimäärin 15000 kpl päivässä. Uudelleen käytettävien kuljetusyksiköiden lisäksi kertakäyttöisiä pahvisia kuljetusyksiköitä, kuormalavoja ja muita kuljetusyksiköitä lähtee keskimäärin 1100 kpl päivässä.

Keräilyprosessin päätyttyä kuljetusyksiköihin liimataan osoitetarra, joka sisältää SSCC-koodin viivakoodin muodossa. Tämän jälkeen kuljetusyksiköt siirtyvät lähettämöön, jossa ne lajitellaan lähtevien kuljetusreittien mukaan. Kuljetusyksiköiden SSCC-viivakoo-

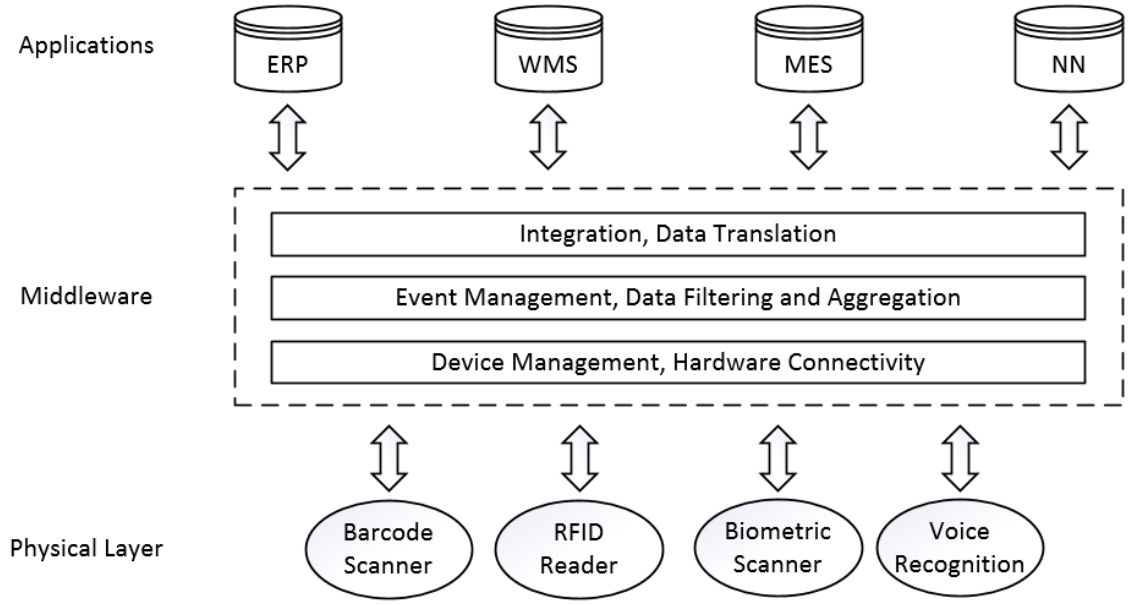
dit skannataan manuaalisesti ennen lastaamista, jolloin ne siirtyvät järjestelmässä kuljetusautoihin. Uudelleen käytettävät kuljetusyksiköt palautuvat asiakkailta ja kulkevat pesukoneen läpi ennen uutta käyttöä.

2 Automaattinen tunnistus ja tiedonkeruu

AIDC (Automatic Identification and Data Capture) eli automaattinen tunnistus ja tiedonkeruu on käsite, jolla tarkoitetaan tekniikoita objektien automaattiseen tunnistamiseen, niistä tiedon keräämiseen ja tiedon edelleen välittämiseen taustajärjestelmille. Tekniikat voidaan jakaa kahteen eri pääryhmään: annettuja ominaisuuksia tunnistaviin, kuten viivakooditunnistus ja radiotaajuustunnistus sekä luonnollisia ominaisuuksia tunnistaviin, kuten äänitunnistus, biometrinen tunnistus ja tekstintunnistus. (Bienhaus 2009, s. 1.)

AIDC:tä hyödynnetään nykypäivänä laajasti toimitusketjun eri vaiheissa. Keräämällä oikeaa tietoa oikeaan aikaan eri prosessien vaiheista saavutetaan läpinäkyvyyttä koko toimitusketjulle aina raaka-ainetoimittajilta tuotannon kautta kuluttajille. Suurimmat hyödyt ovat tehokkuuden, laadun ja asiakastyytyväisyyden kasvaminen sekä kustannusten laskeminen. (Bienhaus 2009, s. 1.)

AIDC-järjestelmä alkaa fyysiseltä tasolta, jossa sijaitsevat objekteja tunnistavat komponentit. Tunnistamisvaiheessa saattaa syntyä paljon dataa ja kaikki kerätty data ei ole välttämättä liiketoiminnan kannalta oleellista. Raaka tunnistusdata kannattaa käsitellä ns. väliohjelmistossa (engl. middleware) ennen toiminnan-, tuotannon-, varaston- yms. ohjausjärjestelmiin lähettämistä (kuva 1). Käsittelyvaiheessa voidaan tehdä mm. datan suodattamista, kontekstiin saattamista ja kokoamista. Väliohjelmistoon lasketaan kuuluvaksi myös tunnistuslaitteiston hallinta ja liityntärajapinta taustajärjestelmiin. (Bienhaus 2009, s. 2–16.)



Kuva 1. AIDC-järjestelmän arkkitehtuuri (Bienhaus 2009)

Monimutkaisemmissa prosesseissa voi olla tarpeellista useiden eri laitteistojen vuoksi luoda kullekin oma laitteistonhallinta- ja datankäsittelytaso. Kyseistä tasoa kutsutaan edgewareksi ja middleware toimii tällöin lähinnä linkkinä sen ja taustajärjestelmien välillä. (Bienhaus 2009, s. 2–16.)

2.1 Viivakoodit

Viivakoodit ovat visuaalisia tunnuksia, jotka sisältävät informaatiota. Niiden sisältö on luettavissa elektronisesti käyttäen laseria tai kameroita. Viivakoodeja käytetään yleisesti tuotteiden tunnistamiseen, jolloin niihin sisällytetty tieto koostuu muun muassa tuotenumeroista, sarjanumeroista ja eränumeroista. Parhaimmillaan tietoa mahtuu viivakoodeihin tuhansia merkkejä. (GS1 barcodes)

Viivakoodien käyttö mahdollistaa nopean ja luotettavan tiedonkeruun, jonka johdosta toimintoja saadaan tehostettua ja kustannuksia alennettua. Viivakoodien yhteyteen on yleensä myös lisätty sen sisältämä tieto ihmisluettavassa muodossa, jolloin lukemisen epäonnistuessa tunnistus voidaan yhä suorittaa. (SFS-käsikirja 301-1 2010, s. 20.)

Viivakoodien huonoja puolia ovat lukemisen vaativa suora näköyhteys lukijan ja luettavan viivakoodin välillä sekä lyhyet lukuetäisyydet. Ympäristön olosuhteiden aiheuttamat likaantumiset ja haalistumiset voivat muuttaa viivakoodin lukukelvottomiksi ja ympäristössä oleva kosteus voi johtaa lasersäteiden heijastumiseen ja sitä kautta lukuvarmuuden heikentymiseen. (SFS-käsikirja 301-1 2010, s. 20.)

Yksiulotteiset viivakoodit

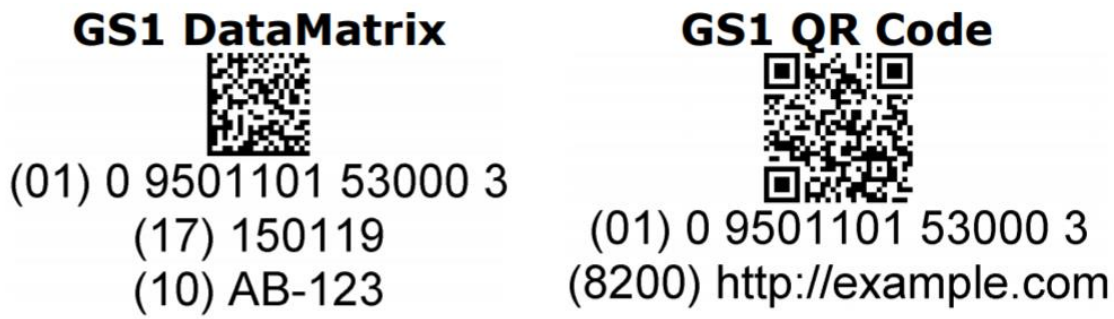
Yksiulotteiset eli lineaariset viivakoodit ovat perinteisin ja yhä yleisin käytössä oleva viivakoodiluokka. Yksiulotteiset viivakoodit koostuvat mustista pystysuorista viivoista ja niiden väliin jäävistä tyhjistä alueista (kuva 2). Ne yhdessä muodostavat tietyntyyppisen kuvion, joka luetaan lukijalaitteella. (Introduction Into Barcodes 2014, s. 3.)

Kuva 2. GS1 EAN/UPC 1D-viivakoodit (GS1 barcodes).

Yksiulotteiset viivakoodit ovat yksinkertaisia luoda ja lukea, sekä niiden käyttökustannukset ovat pieniä. Niihin mahtuva tiedon määrä on pieni, sitä rajoittaa tiedon tallentaminen yhdensuuntaisesti, joten suuren tietomäärän tallentaminen venyttää viivakoodia vertikaalisesti. (Introduction Into Barcodes 2014, s. 3.)

Kaksiulotteiset viivakoodit

Kaksiulotteisissa viivakoodeissa tieto on tallennettuna matriisimuotoon tai päällekkäisiin yksiulotteisiin viivakoodeihin. Matriisimuotoisissa viivakoodeissa tieto voi olla tallennettuna sekä pystysuuntaisesti että vaakasuuntaisesti (kuva 3). Niissä tieto voi olla jaettuna lukuisiin erimuotoisissa soluihin, kuten neliöihin, ympyröihin sekä kuusikulmioihin. (Introduction Into Barcodes 2014, s. 3.)



Kuva 3. GS1 2D-viivakoodit (GS1 barcodes).

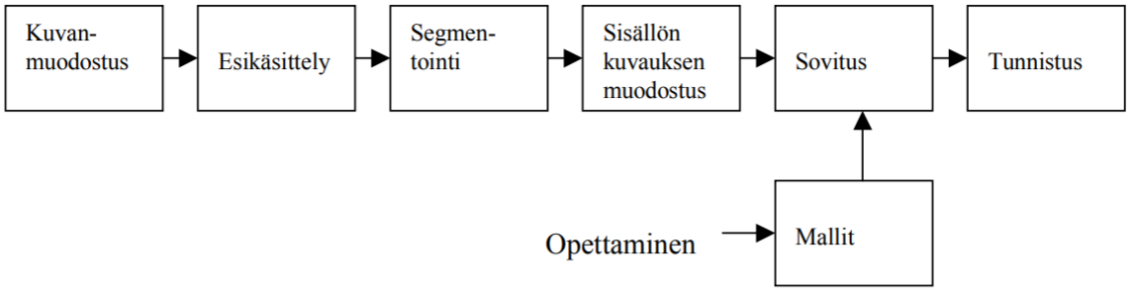
2D-viivakoodit ovat kapasiteetiltaan huomattavasti suurempia kuin 1D-viivakoodit, parhaimmillaan niihin voidaan tallentaa tuhansia alfanumeerisia merkkejä. Samaan 2D-viivakoodiin on mahdollista tallentaa tietoa useaa eri datatyyppiä käyttäen, kuten numeerista, binaarista sekä tekstiä. 2D-viivakoodit tarjoavat myös mahdollisuuden käyttää virheenkorjaustekniikoita. Viivakoodin sisältämä tieto kokonaisuudessaan voidaan saada luettua, vaikka viivakoodista olisi vaurioitunut jopa 20 %. 2D-viivakoodien luominen ja lukeminen vaatii 1D-viivakoodeihin nähden monimutkaisempia menetelmiä ja laitteita, joten käyttökustannukset voivat olla myös korkeampia. (Introduction Into Barcodes 2014, s. 3.)

2.2 Konenäkö

Konenäöllä tarkoitetaan kameran tai muun sensorin tuottaman kuvan sisällön analysointia koneellisesti. Koneen tehtävänä voi olla tunnistaa kuvista kohteita ja määrittää niiden sijainnit ja asennot sekä niissä tapahtuneet muutokset. Kaksiulotteisten kuvien analysointi on huomattavasti yksinkertaisempaa kuin kolmiulotteisten näkymien, joissa kohteet näyttävät erilaisilta eri suunnista tarkasteltaessa. Haasteita luovat lisäksi toisensa osittain peittävät kohteet, valaistuksen muutokset sekä kameran tai kohteen liikkeessä olo. (Pietikäinen & Silven, s. 1.)

Konenäön keskeisimpiä sovelluksia ovat visuaalinen laadunvalvonta ja lajittelu, joilla päästään parempaan tuotteen laatuun ja pienempiin tuotantokustannuksiin. Robotiikan sovelluksia ovat erilaiset materiaalinkäsittely-, lajittelu- ja kokoonpanotehtävät, joissa konenäöllä roboteista saadaan sopeutuvampia, joustavampia ja itsenäisempiä. Konenäköä

käytetään lisäksi liikkuvien koneiden, robottien ja autojen navigoinnissa. (Pietikäinen & Silven, s. 1.)



Kuva 4. Yksinkertaistettu kuva-analyysiprosessi (Pietikäinen & Silven, s. 5.).

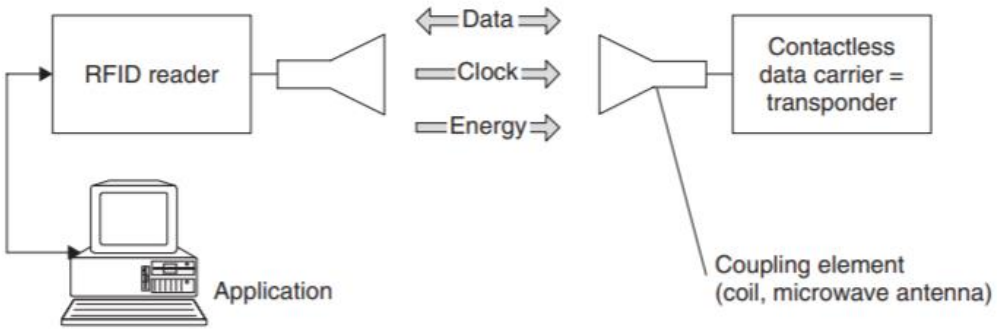
Kuva-analyysi (kuva 4) alkaa kuvan muodostamisella kameralla tai muulla sensorilla, jonka jälkeen kuvaa esikäsitellään analyysin kannalta edullisempaan muotoon digitaalisen kuvankäsittelyn menetelmillä. Näihin kuuluvat esimerkiksi valaistuksessa tapahtuneiden muutosten normalisointi, kohinan suodatus tai mielenkiinnon kohteina olevien piirteiden korostaminen.

Seuraavan vaiheena on kuvan segmentointi, jossa erotetaan kohteet ja kohteiden osat toisistaan ja taustastaan. Menetelminä käytetään yleisesti kuvien jakamista sävyiltään, väreiltään tms. ominaisuuksiltaan homogeenisiin alueisiin sekä reunanilmaisua, jossa kuvasta ilmaistaan edellä mainittujen alueiden reunakohtia.

Tämän jälkeen sisällöstä muodostetaan kuvaus laskemalla segmentoitujen alueiden tai reunojen ominaisuuksia kuvaavia piirteitä, joita ovat mm. muoti, väri ja tekstuuri. Jos kohde muodostuu useasta alueesta tai reunasta, tarvitaan lisäksi tietoa niiden keskinäisistä relaatioista. Muodostettuja kuvauksia ja systeemille etukäteen opetettuja malleja vertaamalla voidaan kuvasta tunnistaa kohteita tai ilmaista poikkeamia malleista. (Pietikäinen & Silven, s. 5-6.)

2.3 Radiotaajuustunnistus

RFID, eli radiotaajuustunnistus on tekniikka tiedon lukemiseen ja tallentamiseen kontaktittomasti. Elektroniselle tunnisteelle on tallennettu tietoa muodossa, jonka lukijalaite pystyy langattomasti lukemaan, sekä tarvittaessa myös muuttamaan, lukitsemaan tai tuhoamaan (kuva 5). Lukijalaite voi välittää lukemansa tiedon edelleen tietojärjestelmiin, jotka sovelluksesta riippuen voivat tarvittaessa lähettää takaisin luettuun tietoon liitettävää informaatiota. Tunniste itsessään on liitettynä johonkin esineeseen joko suoraan valmistusvaiheessa tai jälkikäteen esim. tarrana liimattuna. (SFS-käsikirja 301-1 2010, s. 9.)



Kuva 5. Yksinkertaisen RFID-järjestelmän komponentit (Finkenzeller 2010, s. 8.).

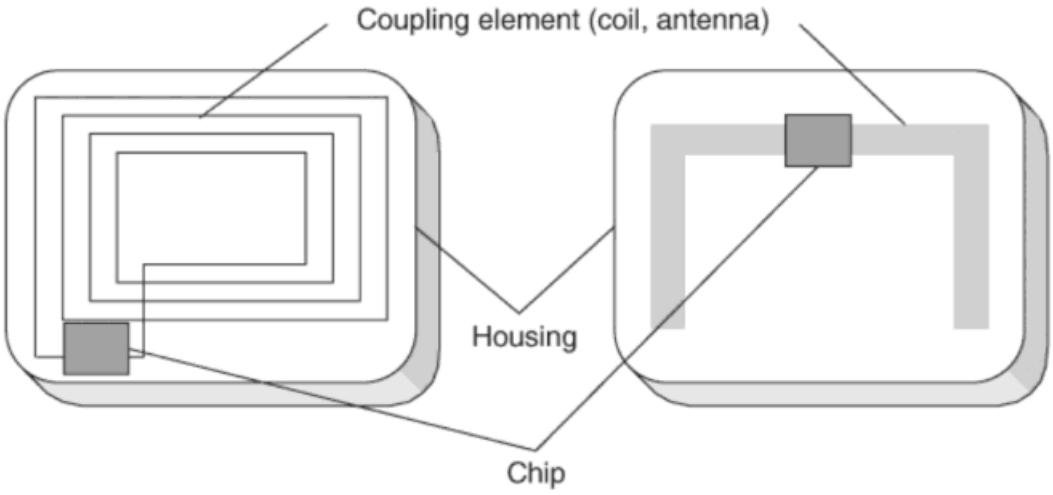
Yksi suurimmista RFID-tekniikan sovellusaloista on toimitusketjut ja tuotteiden seuranta. Toimitusketjun eri vaiheissa voidaan suorittaa automaattista tiedonkeruuta, jonka johdosta manuaalisen työn määrä vähenee, läpinäkyvyys tuotannossa sekä toimitusketjussa paranee ja tiedon oikeellisuus tehostuu. (SFS-käsikirja 301-1 2010, s. 122.)

Toinen suuri sovellusala on kulunvalvonta. RFID-tunnisteella varustettuja kulkulupia voidaan käyttää korvaamaan fyysisiä avaimia, jolloin suurilla joukoilla kustannukset pienentyvät ja esimerkiksi avaimen katoamisen vuoksi lukkojen uusiminen ei ole tarpeellista. Ajallinen rajoitus kulkuluvan voimassaololle ja mahdollinen sallittujen kulkualueiden muokkaaminen on yksinkertaisempaa. Käyttökohteita ovat yritysten lisäksi mm. joukkoliikenne, hotellit, kuntosalit, huvipuistot, laskettelukeskukset jne. (SFS-käsikirja 301-1 2010, s. 145.)

Muita sovellusalueita ovat mm. maksuvälineet, ympäristön ja olosuhteiden tarkkailu, ajanotto urheilukilpailuissa, kirjojen käsittely kirjastoissa, karjaeläinten tunnistaminen, potilaiden sekä potilastietojen tunnistaminen terveydenhuollossa ja vanhustenhoito. (SFS-käsikirja 301-1 2010, s. 122–152.)

2.3.1 Tunnisteet

RFID-tunniste on RFID-järjestelmässä se osa, jolla tunnistamisessa käytettävä data kuljetetaan. Tunniste koostuu tavallisesti antennista, mikrosirusta sekä jonkinlaisesta kotelointista (kuva 6). Aktiivisissa ja semipassiivisissa tunnisteissa on lisäksi jonkinnäköinen virtalähde, yleensä paristo. (Finkenzeller 2010, s. 9.)



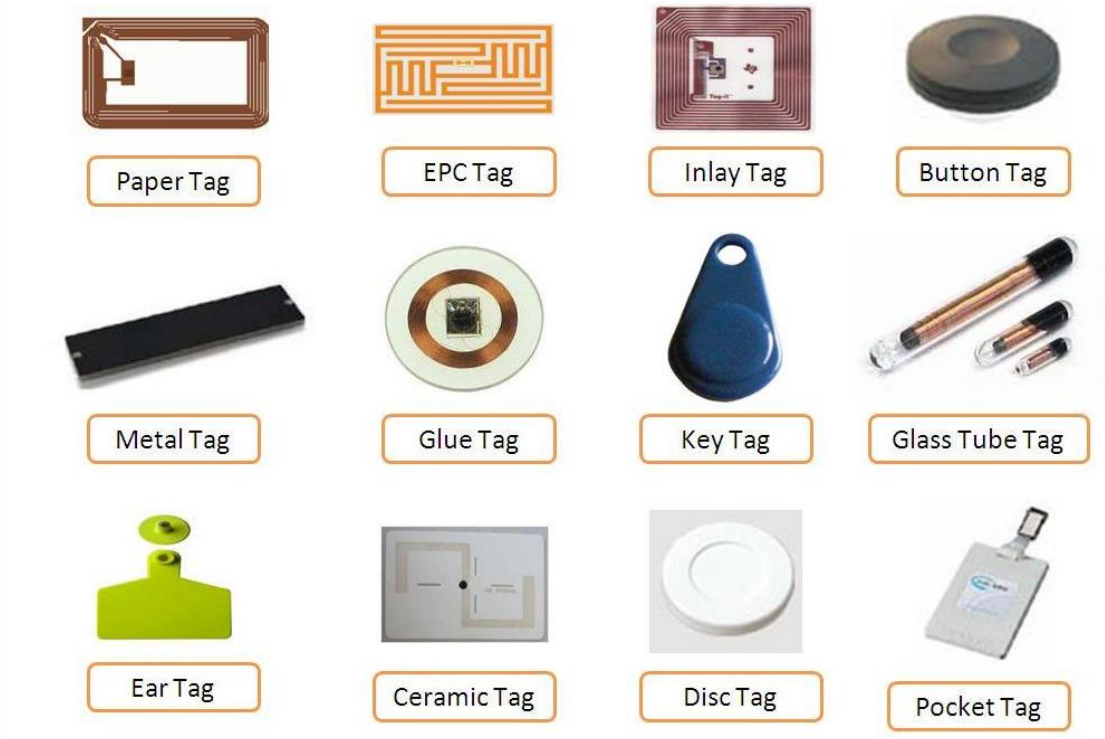
Kuva 6. RFID-tunnisteen perusrakenne, vasemmalla silmukka-antennilla ja oikealla dipoliantennilla (Finkenzeller 2010, s. 8.).

Tunnisteessa olevan muistin määrä riippuu tunnisteen tyypistä ja tavallisesti se vaihtelee muutamasta tavusta satoihin kilotavuihin. Yksinkertaisimmissa järjestelmissä tunnisteet ovat kirjoitussuojattuja ja niiden muistiin on tallennettu pysyvästi yleensä vain muutamien tavujen pituinen sarjanumero. (Finkenzeller 2010, s. 24.)

Tunnisteita on kaiken kokoisia ja muotoisia riippuen käyttökohteesta (kuva 7). Pienimmät tunnisteet ovat esimerkiksi paperimassaan sisällytettäviä ns. pulverityyppisiä tunnisteita, jotka ovat kooltaan 0,05 mm x 0,05 mm x 5 µm. Suurimmat ovat koko luokaltaan useita

senttimetrejä suuntaansa, joiden käyttökohteita on esimerkiksi autoteollisuudessa. Tunnisteen muodolla voidaan vaikuttaa sen näkyvyyteen objektissa, johon se kiinnitetään. Esimerkiksi kulunvalvontakorteissa ja muissa älykorteissa käytetään ohuita tunnisteita kortin litteän muodon säilyttämiseksi. (SFS-käsikirja 301-1 2010, s. 25–26.)

Tunnisteiden kotelointiin käytetään tavallisesti muovia, epoksia, lasia tai paperia. Valintaan vaikuttavat kohteen ominaisuudet sekä siihen kohdistuvat ulkoiset vaikutukset, kuten ympäristön olosuhteet. Näitä voivat olla lämpötila, ilmankosteus, erilaiset nesteet, pöly jne., joita silmällä pitäen tunnisteet ovat yleensä IP-luokiteltuja. Tunnisteiden kiinnitystapoja kohteeseen ovat mm. liimaaminen, injektoiminen, ruuvaaminen. (Finkenzeller 2010, s. 13–21.)



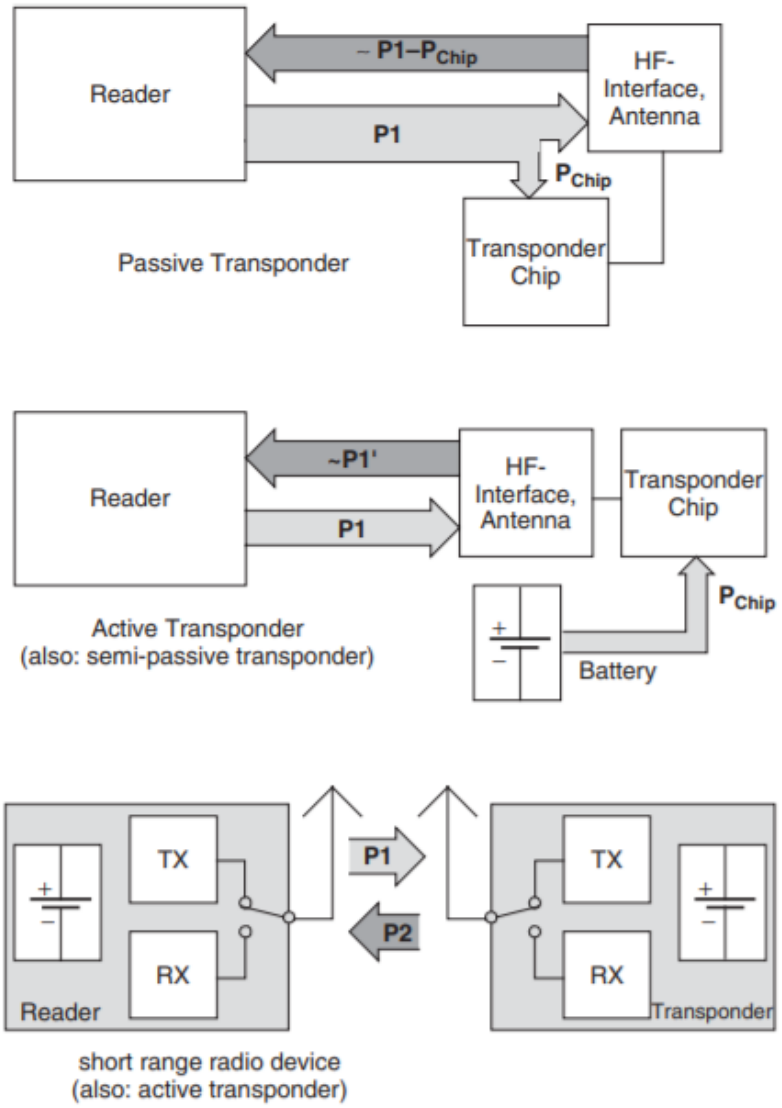
Kuva 7. Erilaisia RFID-tunnisteita (RDIF Tags 2014).

Passiiviset tunnisteet eivät nimensä mukaisesti sisällä omaa virtalähdettä, vaan ne saavat energiansa lukijan lähettämistä radioaalloista (kuva 8). Tunnisteen antenniin indusoituvan sähkövirran avulla se pystyy lähettämään tietoa lukijalle sekä suorittamaan sen lähettämät käskyt. Passiivisten tunnisteiden lukuetäisyys on kohtalaisen pieni, 10 milli-

metristä noin viiteen metriin. Passiiviset tunnisteet ovat halpoja valmistaa, joten niitä voidaan käyttää kohteissa, joissa tunnisteita tarvitaan suuri määrä. Lisäksi yksinkertainen rakenne mahdollistaa hyvin pienen koon, mikä lisää sen sovellusmahdollisuuksia. (SFS-käsikirja 301-1 2010, s. 38.)

Semipassiiviset tunnisteet sisältävät virtalähteen, jonka tuottamalla energialla se vahvistaa lukijan lähettämän signaalin takaisinsirontaprosessia (kuva 8). Semipassiivinen tunniste ei siis sisällä omaa lähetintä, vaan kommunikointi lukijan kanssa tapahtuu muuten samalla tavalla kuin täysin passiivisilla tunnisteilla. Lukuetäisyys on suurempi kuin vastaavalla passiivisella tunnisteella sekä siirrettävät tietomäärät voivat olla suurempia. Toisaalta oma virtalähde lisää tunnisteen hintaa sekä kokoa, jotka rajaavat sen käyttökohteita. (SFS-käsikirja 301-1 2010, s. 38–39.)

Aktiiviset tunnisteet sisältävät virtalähteen lisäksi myös lähettimen (kuva 8). Tämä lisää lukuetäisyyttä huomattavasti, jopa satoihin metreihin asti. Virtalähteen käyttö mahdollistaa suuremman muistimäärän sekä erilaisten antureiden käytön, joiden keräämää dataa tunniste voi tallentaa sekä lähettää. Aktiiviset tunnisteet ovat virtalähteensä sekä lähettimensä vuoksi kalliimpia sekä suurempia kuin passiiviset tunnisteet. Aktiivinen tunniste ei pysty myöskään toimimaan ilman virtalähdettä sekä virtalähteen alettua kuoleentumaan saattaa tunniste lähettää puutteellista tai väärää tietoa. (SFS-käsikirja 301-1 2010, s. 39.)



Kuva 8. Vertailua passiivisen, semipassiivisen sekä aktiivisen tunnisteen välillä (Finkenzeller 2010, s. 23.)

2.3.2 Lukijat

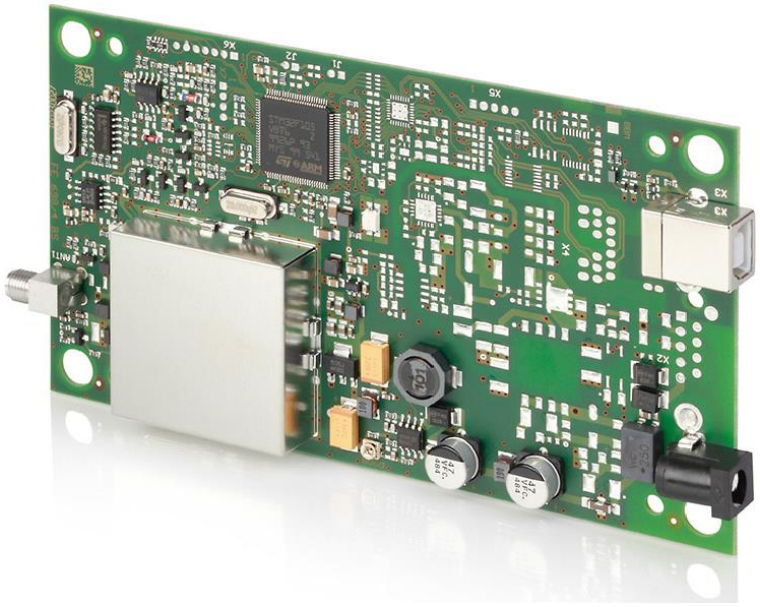
Jotta tietojärjestelmä pystyy lukemaan tunnisteella olevaa tietoa tai kirjoittamaan tunnisteelle, tarvitaan tietojärjestelmän ja tunnisteen väliin lukija (kuva 9). Kommunikointi tapahtuu tavallisesti master-slave periaatteella. Lukija saa taustajärjestelmältä käskyn suorittaa komentoja tunnisteen kanssa, jolloin taustajärjestelmä toimii siis master-roolissa ja lukija slave-roolissa. Jotta lukija voi suorittaa taustajärjestelmän komennot, täytyy sen ensin ottaa yhteys tunnisteeseen. Lukijan ja tunnisteen välisessä kommunikaatiossa

lukija toimii master-roolissa ja tunniste slave-roolissa, jossa lukija hoitaa mm. yhteyden luomisen ja törmäyksenesto- sekä tunnistautumisprosessit. (Finkenzeller 2010, s. 317.)

Kuva 9. Erilaisia RFID-lukijoita (RFID Readers).

Lukijat voidaan luokitella karkealla tasolla kolmeen eri luokkaan. OEM-lukijat on tarkoitettu integroitavaksi tilaajan omiin järjestelmiin, tietojenkeruuterminaaleihin, robotteihin yms. ja ne toimitetaan yleensä häiriösuojattuna tai koteloimattomina piirilevyinä. Valmiiksi koteloidut teollisuuskäyttöön tarkoitetut lukijat ovat usein standardisoiduilla liitännöillä varustettuja, jolloin ne on helppo liittää järjestelmiin. Langattomat lukijat sisältävät usein oman näytön ja käyttöliittymän datansyöttöä varten. Esimerkkejä käyttökohteista ovat mm. eläinten tunnistus, maksupäätteet ja matkalippujen tarkastus. (Finkenzeller 2010, s. 338–339.)

Lukijat rakentuvat pääosin kahdesta eri moduulista: ohjausjärjestelmästä sekä radiorajapinnasta (kuva 10). Radiorajapinta koostuu sekä lähettimestä, että vastaanottimesta ja tarvitsee toimiakseen antennin. Lähetin sekä vastaanotin on yleensä koteloitu häiriösuojapeltiin, jotta systeemiin kuulumattomat radiosignaalit eivät pääse aiheuttamaan häiriöitä. Ohjausjärjestelmä koostuu tavallisesti erilaisista muistipiireistä, mikroprosessorista sekä erillisistä sovelluskohtaisista mikropiireistä. Ohjausjärjestelmä kommunikoi taustajärjestelmän kanssa sekä suorittaa sen komennot radiorajapinnan avulla. Lisäksi sen sovelluskohtaiset mikropiirit yleensä hoitavat laskentatehoa vaativat kryptausalgoritmit. (Finkenzeller 2010, s. 317–324.)



Kuva 10. FEIG Electronicin valmistama HF-taajuusalueen lukija. Radiorajapinta nähtävissä kote-loituna vasemmalla alhaalla (FEIG Electronic Products).

Kannettavat lukijat käyttävät yleensä kiinteitä antenneja, mutta esimerkiksi varastosovel-luksissa antennit voivat olla erillisiä ja niitä voi olla useampia per lukija. Antennin koko ja tyyppi vaikuttavat saavutettavaan lukuetäisyyteen. Antennivalinnalla voidaan myös vai-kuttaa lukukulman suuruuteen, joissakin sovelluksissa voi olla vaatimuksena esimerkiksi hyvin kapea lukualue. (SFS-käsikirja 301-1 2010, s. 30–32.)

Lukijan ja tunnisteen välinen kytkeytyminen voi tapahtua joko magneettisesti tai sähkö-magneettisesti. Magneettisessa kytkeytymisessä lukija luo magneettisen kentän, jota kutsutaan lähikentäksi. Tunnisteissa käytetään tällöin silmukkamuotoisia antenneja, joissa lukijan luoma kenttä indusoi sähkövirtaa tunnisteille. Induktion tehokkuuteen vai-kuttaa silmukoiden sisäänsä sulkema pinta-ala. Sähkömagneettisessa kytkeytymisessä lukijan luomaa kenttää kutsutaan kaukokentäksi. Siinä kytkeytyminen perustuu sähkö-magneettisen säteilyn eli radioaaltojen absorptioon ja tunnisteissa käytetty antennityyppi on yleensä dipoliantenni. (SFS-käsikirja 301-1 2010, s. 31–35.)

2.3.3 Taajuusalueet

RDIF-tekniikka toimii radiotaajuuksilla, joten on tärkeää, ettei se häiritse muita radiosovelluksia tai ota häiriötä muista radiosovelluksista. Jotta vältyttäisiin päällekkäisten taajuuksien käytöstä muiden radiosovellusten kanssa, on RFID-tekniikalle määritelty omat taajuusalueensa. Taajuusalueet vaihtelevat jonkin verran maiden ja maanosien välillä, mutta ne voidaan jakaa karkeasti neljään eri luokkaan. Eri taajuusalueiden käyttö vaikuttaa ratkaisuissa mm. lukuetäisyyksiin sekä häiriönsietoon, joten taajuusalue tulee valita sovelluskohteen mukaisesti (taulukko 1). (Finkenzeller 2010, s. 155–156.)

Taulukko 1. Taajuusalueiden ominaisuuksia (SFS-käsikirja 301-1 2010, s. 41).

Taajuuskaista	**LF (Low Frequency)**	**HF (High Frequency)**	**UHF (Ultra High Frequency)**	**Mikroaallot**
Taajuudet	30–300 kHz	3–30 MHz	0,3–3 GHz	2–30 GHz
Kytkeytyminen	Magneettinen	Magneettinen	Sähkömagneettinen	Sähkömagneettinen
Tyypilliset RFID-taajudet	125–134 kHz	13,56 MHz	433 MHz tai 865–956 MHz	2,45 GHz
Arvioitu lukuetäisyys	< 0,5 m	< 1,5 m	433 MHz: <100 m 865–956 MHz: 0,5–5 m	< 10 m
Tyypillinen tiedonsiirtonopeus	n. 1 kbit/s	n. 100 kbit/s	433–956 MHz: 640 kbit/s	n. 100 kbit/s
Ominaispiirteet	Lyhyet etäisyydet, pieni tiedonsiirtonopeus, läpäisee veden, muttei metallia.	Suuremmat etäisyydet, melko hyvä tiedonsiirtonopeus, läpäisee veden, muttei metallia.	Pitkät etäisyydet, suuri tiedonsiirtonopeus, alle sadan objektin yhtäaikainen luku, ei läpäise vettä eikä metallia.	Pitkät etäisyydet, suuri tiedonsiirtonopeus, ei läpäise vettä eikä metallia.
Tyypillinen käyttökohde	Älykortit, eläinten tunnistus	Kulunvalvonta ja turvallisuus	Logistiikka	Liikkuvien autojen tietullit

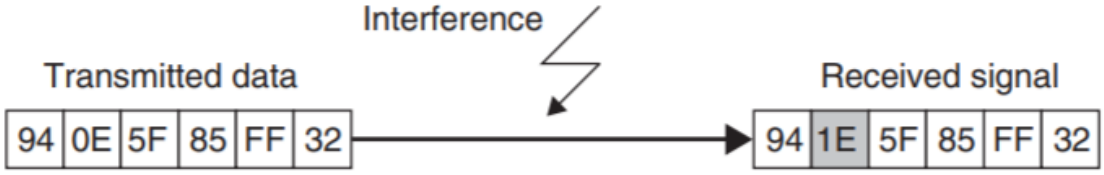
Magneettisesti kytkeytyvät ratkaisut operoivat tyypillisesti LF-taajuusalueella (Low Frequency) taajuuksilla 125–134 kHz ja HF-taajuusalueella (High Frequency) taajuuksilla 6,78 MHz ja 13,56 MHz. Näillä taajuusalueilla käytetään yleensä halpoja passiivisia tunnisteita ja lukuetäisyys on verrattain pieni. LF-taajuuksilla toimivat tunnisteet eivät ole herkkiä suuntaukselle, energiankulutus on pientä, ne toimivat hyvin nesteiden ja muiden

ei-metallisten esineiden läpi, mutta tiedonsiirtonopeus on suhteellisen hidas. HF-taajuuksilla edellä mainitut ominaisuudet ovat hieman huonommat, lukuun ottamatta tiedonsiirtonopeutta, joka kasvaa. (Finkenzeller 2010, s. 162–164; SFS-käsikirja 301-1 2010, s. 40–42.)

Sähkömagneettisesti kytkeytyvät ratkaisut operoivat yleensä UHF-taajuusalueella (Ultra High Frequency) taajuuksilla 433 MHz sekä 865–956 MHz ja SHF-taajuusalueella (Super High Frequemcy) taajuuksilla 2,45 GHz sekä 5,8 GHz. Kyseisillä taajuusalueilla käytetään sekä passiivisia, että aktiivisia tunnisteita. Ratkaisut tukevat suuria lukuetäisyyksiä sekä tiedonsiirtonopeuksia, mutta toimivat huonosti nesteiden ja metallien läheisyydessä. (Finkenzeller 2010, s. 160–161; SFS-käsikirja 301-1 2010, s. 40–42.)

2.3.4 Tiedon eheys

Erilaiset häiriöt tiedonsiirron aikana voivat aiheuttaa muutoksia siirrettävään tietoon (kuva 11). Siirretyn tiedon oikeellisuuden tarkistamiseen voidaan käyttää erilaisia menetelmiä, joista tarkistussummamenetelmät ovat kaikkein yleisimpiä. Pariteettibitti on näistä yksinkertaisin ja tavanomaisin menetelmä, muita menetelmiä ovat mm. CRC (Cyclic Redundancy Check) ja LRC (Longitudinal Redundancy Check). Myös erilaisia törmäyksenestomenetelmiä käytetään mahdollistamaan useiden tunnisteiden samanaikaista tunnistamista. (Finkenzeller 2010, s. 189–194.)



Kuva 11. Tiedonsiirron aikana tuleva häiriö voi aiheuttaa muutoksia siirrettävään tietoon (Finkenzeller 2010, s. 190).

Pariteettibitti lisätään jokaiseen tavuun siten, että tavussa olevien ykkösten määrä määrittää pariteettibitin arvon. Paritonta pariteettibittiä käytettäessä tulee ykkösten määrän olla pariton ja parillista käytettäessä parillinen, pariteettibitin arvo valitaan siten kyseisen ehdon täyttämiseksi. Pariteettibittitarkistus on yksinkertainen ja helppo toteuttaa, mutta

se ei huomaa virhettä, jossa parillinen määrä bittejä kääntyy väärinpäin. Tämän vuoksi sitä ei suositella käytettävän järjestelmissä, joissa tiedon eheys on erityisen tärkeää. (SFS-käsikirja 301-1 2010, s. 93.)

CRC-menetelmä sekä LRC-menetelmä perustuvat kumpikin lähetettävästä sisällöstä lasketun arvon käsittelyyn. Laskettu arvo lisätään lähetykseen ja vastaanottopäässä lasketaan uusi arvo koko lähetyksestä, sisältäen mukaan aiemmin liitetyn arvon. Mikäli lähetys on tullut perille oikein, uudesta arvosta tulee aina nolla, joten tiedon oikeellisuus on helppo todeta. LRC-menetelmä on näistä yksinkertaisempi ja nopeampi, mutta mahdollistaa useiden virheiden esiintyessä niiden kumoutumisen tarkistusvaiheessa. CRC-menetelmässä käytetään monimutkaisempaa laskentatapaa, jolla tiedon oikeellisuuden toteaminen on erittäin varmaa. (Finkenzeller 2010, s. 190–193; SFS-käsikirja 301-1 2010, s. 93–94.)

Useiden tunnisteiden yhtäaikaista tunnistamista varten on kehitetty useita erilaisia törmäyksenestomenetelmiä, jotka voidaan jakaa karkeasti neljään eri luokkaan.

- SDMA (Space Division Multiple Access) perustuu useiden lukualueiden luomiseen lukijoita ja/tai antenneja lisäämällä. Lisää järjestelmän käyttöönottokuluja.
- FDMA (Frequency Domain Multiple Access) perustuu useiden eri taajuuksien yhtäaikaiseen käyttämiseen. Lisää järjestelmän käyttöönottokuluja.
- TDMA (Time Domain Multiple Access) perustuu tunnisteiden lukemiseen samalla taajuudella ja lukualueella vuorotellen. Suosituin menetelmä, jonka käyttäminen muiden menetelmien kanssa on helppoa ja myös suositeltavaa menetelmän hitauden takia.
- CDMA (Code Division Multiple Access) voidaan jakaa kahteen eri menetelmää. Suorasekventointiin perustuvassa DS-CDMA -menetelmässä tunnisteiden signaalit pystytään erottamaan toisistaan käyttämällä varmenteena sekventoinnin tulosta. Taajuushyppelyyn perustuvaan FH-CDMA-menetelmässä tieto lähetetään palasina eri taajuuksilla, jotka valittu algoritmi määrittää.

Yksi tunnetuimmista ja yksinkertaisimmista törmäyksenestoratkaisuista on TDMA menetelmään perustuva ALOHA. Menetelmää käytetään ainoastaan pienen datamäärän sisältävien passiivisten tunnisteiden kanssa, jolloin lähetyksen pituus on lyhyt. Yhden tunnisteen lähetyksien välissä pidettävät tauot ovat pitkiä ja ne vaihtelevat tunnisteiden välillä. Tällä tavalla saadaan usean eri tunnisteen paketit perille tietyin todennäköisyyksin

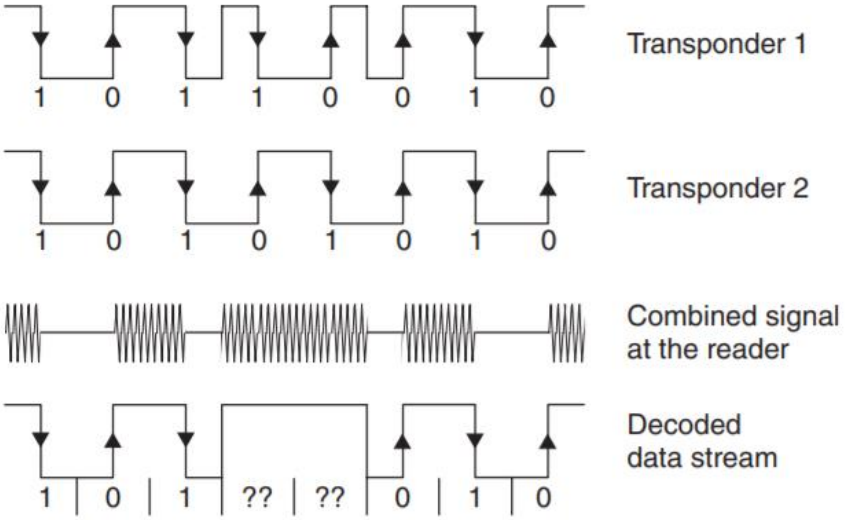
ilman yhteentörmäystä (taulukko 2). (Finkenzeller 2010, s. 194–201; Hsin-Chin 2010, s. 51–55.)

Taulukko 2. Esimerkki yhtä aikaa lukualueella olevien tunnisteiden lukuajoista ALOHA-menetelmää käyttäen (Finkenzeller 2010, s. 200).

Tunnisteiden lukumäärä lukualueella	**Keskiarvo (ms)**	**90 % luottamusväli (ms)**	**99,9 % luottamusväli (ms)**
2	150	350	500
3	250	550	800
4	300	750	1000
5	400	900	1250
6	500	1200	1600
7	650	1500	2000
8	800	1800	2700

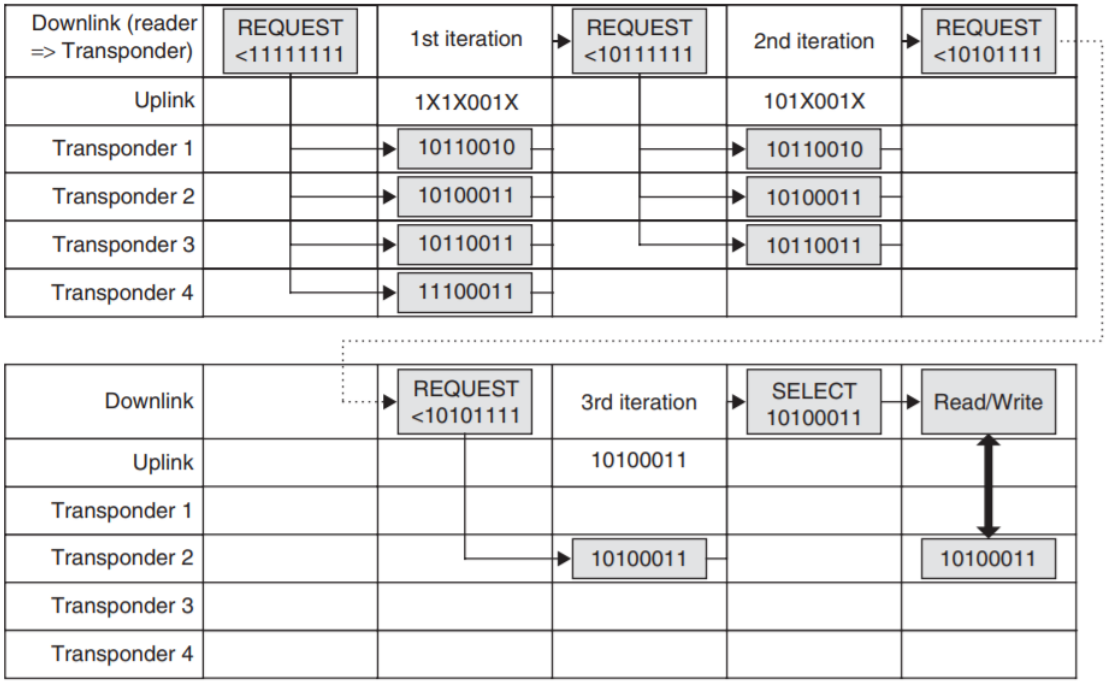
ALOHA-menetelmän heikon suorituskyvyn vuoksi siitä on kehitetty paranneltuja versioita. S-ALOHA (Slotted ALOHA) -menetelmässä tunnisteille on määritelty lähetysaikaikkunat, joita lukija hallinnoi. Dynaamisessa S-ALOHA -menetelmässä lähetysaikaikkunoiden määrää vaihdellaan tarpeen mukaan, jolloin sekä suorituskyky, että luettavien tunnisteiden määrä pysyvät hyvinä. (Finkenzeller 2010, s. 199–211.)

Binäärihaku (tai binäärinen puuhaku) perustuu lukualueella yhtä aikaa olevien tunnisteiden bittimuotoisten sarjanumeroiden yksittäisten bittien arvojen vertailuun. Lukija pyytää ensin kaikkia sovelluksen sarjanumeroavaruudessa olevia tunnisteita lähettämään sarjanumeronsa yhtäaikaisesti ja analysoi vastaanottamansa signaalin bitti kerrallaan. Lukija havaitsee törmäyskohdat esimerkiksi nousevan ja laskevan reunan avulla (kuva 12). (Finkenzeller 2010, s. 204–208.)



Kuva 12. Törmäyksen tunnistaminen 8-bittisessä Manchester-koodauksessa (Finkenzeller 2010, s. 205).

Jos lukija havaitsee törmäyksen, lukualueella on useampi tunniste. Lukija määrittää eniten määräävän bitin, jossa törmäys on tapahtunut, ja lähettää pyynnön kaikille törmäyskohtaa pienempien sarjanumeroiden omaaville tunnisteille. Kaavaa toistetaan, kunnes kaikki lukualueella olevat tunnisteet on saatu yksilöityä (kuva 13). (Finkenzeller 2010, s. 206–208.)

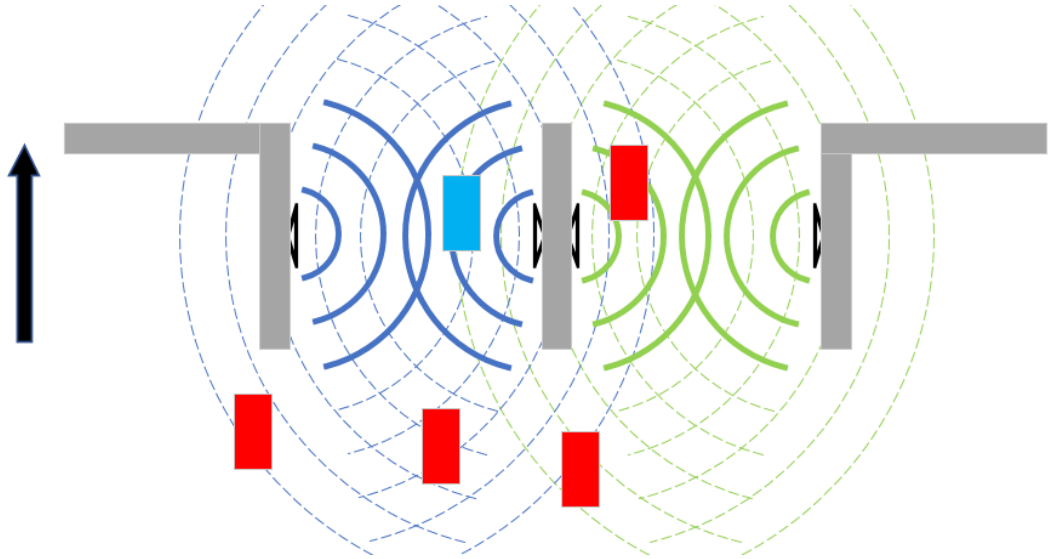


Kuva 13. Binäärihaulla tunnisteiden identifiointi (Finkenzeller 2010, s. 207).

Tarvittavien kyselykierrosten määrä riippuu lukualueella olevien tunnisteiden määrästä ja se kasvaa nopeasti. Sovelluksissa, joissa sarjanumerot ovat pitkiä, kasvaa kyselykierrosten datamäärät suuriksi. Tällöin lukija voi pyytää lähettämään kullakin kyselykierroksella sarjanumeroista vain ne tietyt bitit, joissa törmäys on enää mahdollista. (Finkenzeller 2010, s. 209–211)

2.3.5 Harhaluku, ristivaikutus sekä ylikuuluminen

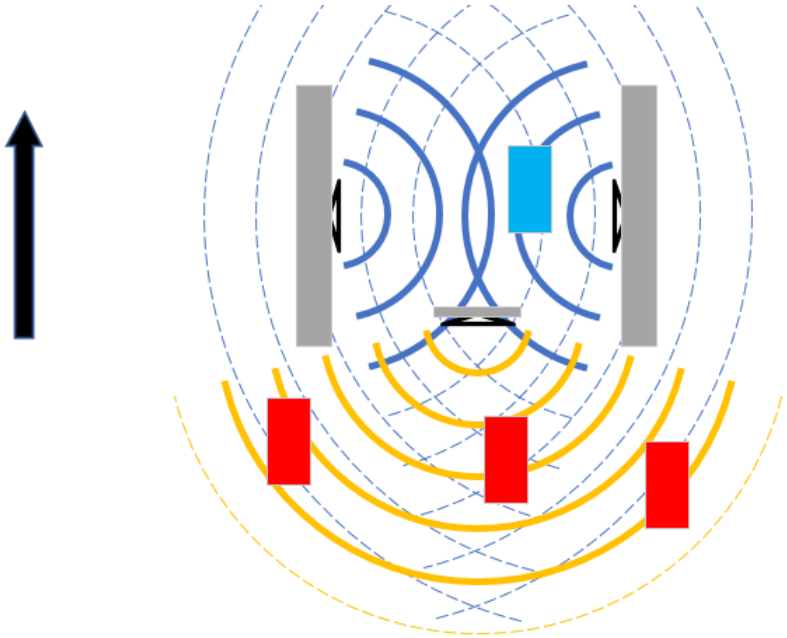
Joissakin sovelluksissa on tarpeellista käyttää useita lähekkäisiä lukualueita, joiden kunkin läpi kulkevat tunnisteet halutaan tunnistaa lukualuekohtaisesti (kuva 14). Lähekkäin toisiaan olevat lukualueet luovat mahdollisuuden ristivaikutukselle tunnisteiden lukemisessa. Lukija saattaa virroittaa viereisen lukualueen läpi kulkevan tunnisteen ja kommunikoida sen kanssa (englanniksi cross reading) tai tunniste voi saada virran oman lukualueensa lukijasta, mutta vastaa viereisen lukualueen lukijan komentoihin (englanniksi cross talk). (Toivonen 2012, s. 24–26.)



Kuva 14. Kaksi vierekkäistä porteilla luotua lukualuetta. Vasemmanpuoleisen portin läpi kulkeva, ja sen tunnistamaksi haluttava objekti kuvattu sinisenä suorakulmiona.

Lukualueen rajoittamisella pyritään minimoimaan mahdollisuus ristivaikutukselle. Lukualueesta on mahdotonta tehdä täysin teräväreunaista, mutta siihen voidaan vaikuttaa mm. lähetysteholla ja antennivalinnoilla. Yksinkertainen mekaaninen keino lukualueen rajoittamiseksi on asentaa lukualueen reunoille suojalevyjä, jotka heijastavat radioaaltoja. (Toivonen 2012, s. 29–30.)

Ylimääräisten antennien käyttö uusien poissulkevien lukualueiden luomiseksi on myös mahdollinen keino lukualueen rajoittamiseksi. Tällöin ne suunnataan pois suljettavaan suuntaan, jolloin niiden lukemat tunnisteet voidaan suodattaa varsinaiselta lukualueelta pois. Kuvassa 15 on luotu portti kahdella toisiaan vastaan osoittavalla antennilla, lukualue havainnollistettu sinisellä. Kolmas antenni on lisätty osoittamaan poispäin varsinaisesta lukualueesta, lisätty lukualue havainnollistettu oranssilla. Tunnisteet, jotka ovat oranssilla lukualueella, jätetään huomioimatta varsinaisella lukualueella. (Toivonen 2012, s. 29–30.)



Kuva 15. Kolmannen antennin käyttäminen lukuportin kanssa.

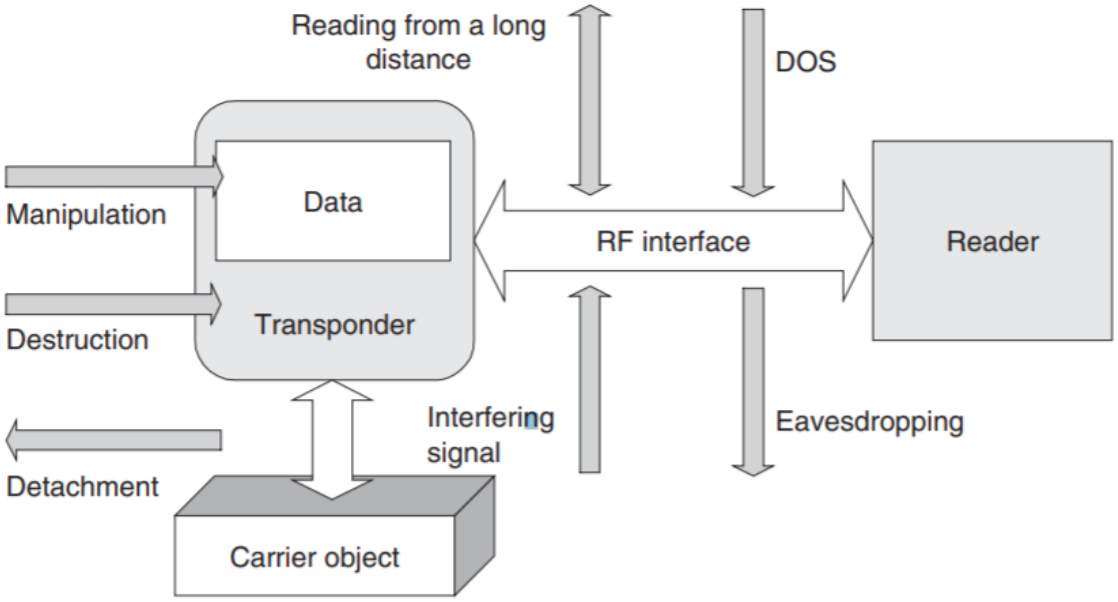
Yksi tapa vähentää ristilukemisten mahdollisuutta on käyttää lukemisen käynnistämiseen erillistä anturia, esimerkiksi optisia antureita. RFID-lukeminen käynnistetään vasta kun lukualueella tapahtuu liikettä. (Toivonen 2012, s. 30–31.)

Lukutapahtumien takaisinsirontasignaalien ominaisuuksia analysoimalla voidaan ristilukemisia sulkea pois lukijatasolla sekä havaita tunnisteiden liike. Lukutapahtumien RSSI, eli tunnisteelta takaisin lukijalle tulevan signaalin voimakkuus, on ylikuulumistapauksissa huomattavasti pienempi, kuin tarkoitetulla lukualueella tehdyillä lukemisilla. Asettamalla alarajat RSSI:lle, voidaan ei-halutut lukemiset jättää huomiotta. Tunnisteen liikkuessa suhteessa lukijaan, sen takaisinsirontasignaalin aallonpituus muuttuu jatkuvasti. Tätä kutsutaan Doppler-ilmiöksi ja sen avulla voidaan havaita tunnisteen liike, sen suunta sekä nopeus. Tunnisteen liike on mahdollista todeta myös lähtevän ja takaisinsirontasignaalin vaihekulman avulla. (Toivonen 2012, s. 31–34.)

Ylemmällä tasolla voidaan ristilukemisia sulkea pois valitsemalla ensimmäinen lukija, joka tunnisteen lukee, ja määrittää se oikeaksi. Kyseessä on hyvin suoraviivainen tapa, mutta se vaatii päätöksentekoa ylemmältä kuin lukijatasolta. Tällöin käytettävissä on useamman lukijan keräämä data ja tiedetään lukualueiden väliset suhteet fyysisessä maailmassa. (Toivonen 2012, s. 26–27.)

2.3.6 Tietoturva

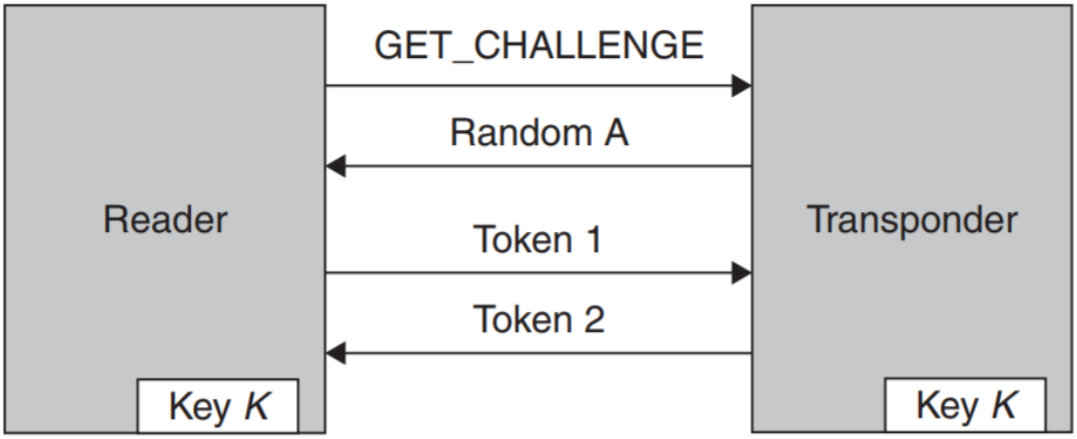
RFID-järjestelmät, siinä missä muutkin tiedonsiirtojärjestelmät, sisältävät riskin mahdollisille väärinkäytöille. Informaatiota voidaan yrittää varastaa, väärää informaatiota voidaan yrittää syöttää järjestelmälle, järjestelmän toimintavarmuutta voidaan yrittää heikentää tai sen toiminta voidaan yrittää estää kokonaan. RFID-järjestelmässä mahdollisia reittejä väärinkäytölle ovat tunnisteet, lukijat sekä niiden välinen radioliikenne (kuva 16). (Finkenzeller 2010, s. 213–214.)



Kuva 16. RFID-järjestelmään kohdistuvia hyökkäystapoja (Finkenzeller 2010, s. 214).

Tietoturvan tarve riippuu oleellisesti sovelluskohteesta. Tietoturvan vahventuessa sen toteuttamisen kustannukset kasvavat, joten tarve on syytä määritellä huolella. Yksinkertaistettuna sovelluksissa, joihin ei liity arvoelementtiä, ei ole tarvetta kovinkaan vahvalle tietoturvalle. Tällaiseksi voidaan luokitella esimerkiksi esineiden tunnistaminen suojatussa tilassa ja tuotantoautomaation sovellukset. Tiukempaa tietoturvaa vaativat sovellukset, joihin liittyy rahallista toimintaa joko suoraan, tai välillisesti esimerkiksi kulunvalvonnan sovelluksissa. Keskeisimmät tietoturvan menetelmät RFID-järjestelmissä ovat todentamismenetelmät sekä siirrettävän tiedon suojaaminen. (SFS-käsikirja 301-1 2010, s. 95–96.)

Todentamismenetelmillä voidaan varmistaa tunnisteen ja lukijan oikeellisuus kommunikaation alkaessa. Symmetrisessä todentamisessa (kuva 17) kaikki RFID-järjestelmän tunnisteet ja lukijat käyttävät samaa salausavainta. Tunniste ja lukija käyttävät salausalgoritmia ja salausavainta luomiensa satunnaislukujen salaamiseen. Ne lähetetään ja puretaan tietyssä järjestyksessä puolin ja toisin, jolloin vastapuolen oikeellisuus voidaan varmentaa vertaamalla purettuja lukuja. Symmetrinen todentamisen huonona puolena on koko järjestelmän yhteinen avain, jonka joutuessa vääriin käsiin on koko järjestelmä vaarassa. Turvallisemmat todentamismenetelmät käyttävät johdettuja avaimia, jolloin jokaiselle tunnisteelle on luotu oma uniikki avaimensa yhteistä isäntäavainta käyttäen. Lukija varmistaa tunnisteen oikeellisuuden kommunikaation alkaessa purkamalla salauksen isäntäavaimella. (Finkenzeller 2010, s. 227–228.)



Kuva 17. Symmetrisen todentamisen vaiheet (Finkenzeller 2010, s. 227).

Siirrettävän tiedon suojaamisella voidaan estää vääriin käsiin joutuneen tiedon hyödyntäminen tai lähetetyn tiedon muuttaminen. Yleisimmät suojausmenetelmät ovat satunnaislukujen generointiin pohjautuvat menetelmät, hajautusalgoritmit sekä kryptausalgoritmit. Kryptausalgoritmit vaativat paljon laskentatehoa, joten niitä käytetään yleensä vain parhainta mahdollista tietoturvaa vaativissa sovelluksissa. Kevyeksi salaukseksi voidaan laskea toteutukset, joissa käytetään satunnaislukugeneraattoria ja yksinkertaisia tarkistussummatoimintoja. Kaikista kevyimmissä toteutuksissa on käytössä ainoastaan loogiset bittioperaattorit. (SFS-käsikirja 301-1 2010, s. 101–102.)

2.3.7 Standardit

RFID-tekniikalle on luotu eri tahojen toimesta useita standardeja, mutta yleisesti hyväksytty globaali standardi puuttuu edelleen. Tärkeimpiä toimijoita RFID-standardien osalta ovat:

- ETSI (European Telecommunication Standards Institute), joka ylläpitää EN-standardeja
- ISO (International Organization for Standardization), joka ylläpitää ISO-standardeja
- ISO/IEC JTC 1 (International Organization for Standardization ja International Electrotechnical Commission yhdistymä), joka ylläpitää ISO/IEC-standardeja
- GS1/EPCglobal, joka ylläpitää EPC-standardeja.

RFID-tekniikkaa varten laadittujen standardien lisäksi alalla voidaan soveltaa myös yleisesti radiotaajuusalueilla toimivia laitteita määritteleviä standardeja. (Regulatory Constraints On The Use Of RFID; Finkenzeller 2010, s. 233.)

ISO/IEC 18000-standardisarja on kehitetty tavaroiden ja esineiden käsittelyyn tarkoitetuille RFID-sovelluksille. Se on jaettu seitsemään osaan:

- ISO/IEC 18000-1 Part 1 - Reference architecture and definition of parameters
- ISO/IEC 18000-2 Part 2 - Parameters for Air Interface Communications below 135 kHz
- ISO/IEC 18000-3 Part 3 - Parameters for Air Interface Communications at 13.56 MHz
- ISO/IEC 18000-4 Part 4 - Parameters for Air Interface Communications at 2.45 GHz
- ISO/IEC 18000-5 Part 5 - Parameters for Air Interface Communications at 5.8 GHz - abandoned project.
- ISO/IEC 18000-6 Part 6 - Parameters for Air Interface Communications at 860 to 930MHz
- ISO/IEC 18000-7 Part 7 - Parameters for Air Interface Communications at 433 MHz

Standardisarjassa määritellään muun muassa tunnisteiden ominaisuuksia, tunnisteiden ja lukijan välisen tiedonsiirron rakenne sekä törmäyksenestotapoja. Lisäksi saman organisaation standardit ISO/IEC 15961 ja ISO/IE 15962 määrittelevät sovelluksen ja lukijan

välisen tiedonsiirtoprotokollan. (Regulatory Constraints On The Use Of RFID; SFS-käsikirja 301-1, s. 66–86.)

ISO/IEC 18000-6 on nykyään saatavilla myös osiin jaettuna, ISO/IEC 18000-61, ISO/IEC 18000-62, ISO/IEC 18000-63 ja ISO/IEC 18000-64. Näistä ISO/IEC 18000-63 on yhteensopiva EPC UHF Gen2 Air Interface Protocol standardin kanssa. (ISO/IEC 18000-6 2013.)

GS1/EPCglobal kehittämiä standardeja ovat seuraavat:

- EPC Tag Data Standard määrittelee elektronisen tuotekoodin (EPC, Electric Product Code) sekä informaation, joka kuljetetaan Gen 2 RFID-tunnisteilla
- EPC Tag Data Translation määrittelee edellisen konekielisesti
- EPC UHF Gen2 Air Interface Protocol määrittelee RFID-järjestelmän fyysiset ja loogiset vaatimukset UHF-taajuusalueella 860 MHz - 960 MHz
- EPC Class-1 HF RFID Air Interface Protocol määrittelee RFID-järjestelmän fyysiset ja loogiset vaatimukset HF-taajuudella 13,56 MHz
- LLRP (Low Level Reader Protocol) määrittelee tiedonsiirron tietojärjestelmän ja lukijan välillä

GS1 tarjoaa lisäksi suosituksia oppaiden muodossa standardien soveltamiseen kaupallisissa sovelluksissa. (EPC/RFID Standards.)

2.4 NFC-tekniikka

NFC (Near Field Communication) on radiotaajuuksilla toimiva etätunnistustekniikka, joka pohjautuu osin RFID-tekniikkaan. Tekniikassa käytetään myös lukijoita sekä tunnisteita, joita on olemassa sekä passiivisia että aktiivisia. NFC-lukijat voivat myös toimia itse tunnisteina, esimerkiksi matkapuhelimessa oleva lukija voi jäljitellä maksukorttia tai matkalippua. NFC käyttää HF-taajuutta 13,56 MHz ja tiedonsiirtonopeudessa päästään 424 kbit:iin asti. (NFC Technology.)

NFC on suunniteltu toimimaan alle 10 cm:n lukuetäisyydeltä, jonka vuoksi sen turvallisuustaso on parempi kuin muilla langattomilla tunnistusmenetelmillä. Sitä käytetäänkin

tämän ansiosta erilaisissa maksutapasovelluksissa, kuten lähimaksu. (NFC Technology.)

2.5 Bluetooth ja Wi-Fi

Bluetooth ja Wi-Fi ovat lyhyen kantaman langattomia tiedonsiirtoteknologioita. Kyseisiä teknologioita on mahdollista käyttää objektien automaattiseen tunnistamiseen ja tiedonkeruuseen. Kummankin teknologian käyttäminen vaatii tunnisteelta aktiivista radiota, eli virtalähteen käyttäminen on pakollista. (Learn About Bluetooth; Discover Wi-Fi.)

Bluetooth operoi UHF-taajuusalueella taajuuksilla 2,402–2,480 GHz. Bluetooth on jaettu kahteen eri luokkaan: Bluetooth Classic ja Bluetooth Low Energy (BLE). BLE on kehitetty erityisesti alhaisempien kustannuksien sovelluksille, jotka vaativat pientä energiankulutusta ja joissa tiedonsiirto voidaan hoitaa yksinkertaisemmin sekä hitaammin. Tiedonsiirtonopeuksissa Bluetooth Classicilla päästään 3 Mbit/s asti ja BLE:llä 2 Mbit/s asti. Lukuetäisyydet vaihtelevat alle metristä 1 kilometriin riippuen muiden radiotaajuuksilla toimivien teknologioiden tapaan mm. antennin koosta ja käytetystä lähetystehosta. (Bluetooth Core Specification v. 5.2, s. 187–188; Learn About Bluetooth.)

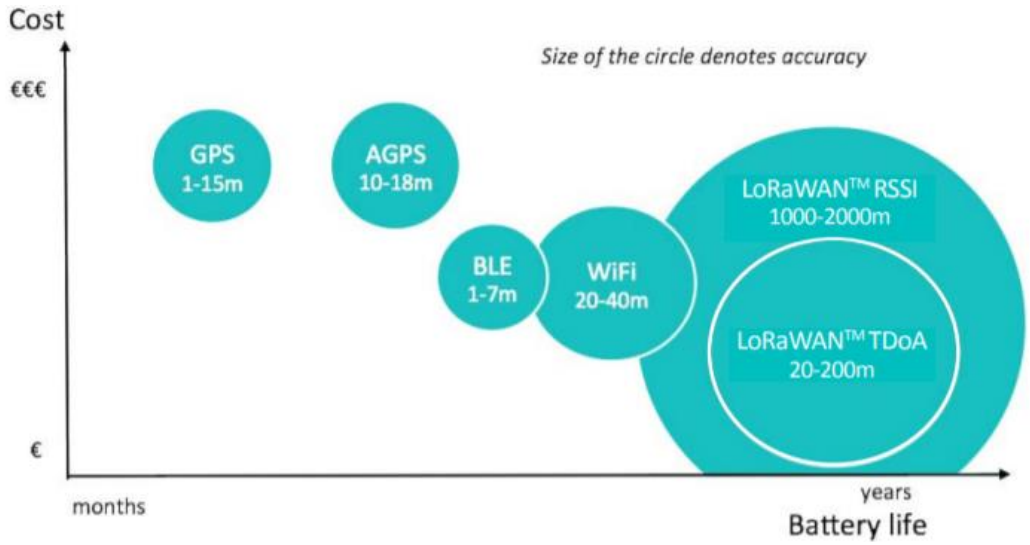
Wi-Fi perustuu IEEEn langattoman tiedonsiirron standardiin 802.11. Se käyttää UHF-taajuutta 2,4 HGz sekä SHF-taajuutta 5 GHz. Teoreettiset tiedonsiirtonopeudet vaihtelevat Wi-Fi sukupolvesta riippuen 54–1300 Mbit/s. (Discover Wi-Fi.)

2.6 LPWAN-tiedonsiirtoverkot

Low Power Wide Area Network (LPWAN) on yleisnimitys langattomista pitkän kantaman tiedonsiirtoverkoista, jotka on suunnattu matalan energian- ja datansiirtomäärän toteutuksille. LPWAN-verkon yhden tukiaseman kantavuudet vaihtelevat käytetyn tekniikan mukaan muutamasta kilometristä jopa useisiin kymmeniin kilometreihin. LPWAN-verkon laitteet vaativat käytännössä aina virtalähteen, joka on tavallisesti paristo tai akku. LPWAN-verkkojen sovelluskohteita ovat mm. älykkäät kaupunki-infrastruktuurit, kotiautomaatio ja muu henkilökohtainen IoT, maanviljelys ja karjankasvatus, logistiikka sekä monitorointi teollisuudessa. Halvimpien laitteiden hinnat ovat $1–$5 ja laitteiden käytöstä

verkossa peritään tavallisesti kuukausi- tai vuosimaksua. (Low Power Wide Area Networks: An Overview, s. 1–5.)

LPWAN-ratkaisut mahdollistavat objektien tunnistamisen laajoilla alueilla, jolloin ns. perinteisten lukupisteiden väliltä voidaan kerätä objektien paikkatietoa. Paikkatietoa voidaan käyttää esimerkiksi logistiikassa lähetysten saapumisaikojen arvioimiseen ja mahdollisten kuljetusongelmien havaitsemiseen. LPWAN-ratkaisun paikannuksen tarkkuus riippuu siinä käytetystä paikannusmenetelmästä (kuva 18). Ulkotiloissa päästään hyviin tarkkuuksiin ja paikannuksen osalta käytännössä joka paikan kattavaan toiminta-alueeseen käyttämällä GPS- tai AGPS-menetelmää. Kyseiset menetelmät ovat kalliita ja kuluttavat paljon energiaa. RSSI:n (Received Signal Strength Indication), eli paluusignaalin voimakkuuden perusteella saadaan tarkkuudeksi 1000–2000 m ja TDOA:n (Time Difference Of Arrival), eli signaalien tukiasemille saapumisten aikaerojen perusteella 20–200 m. Kyseiset tekniikat ovat huomattavasti vähemmän energiaa kuluttavia ja kustannuksiltaan halvempia. (LoRaWAN Geolocation Whitepaper 2018, s. 2–3.)



Kuva 18. LPWAN-ratkaisuissa käytettyjen paikannusmenetelmien tarkkuus, kustannukset ja pariston elinikä. (LoRaWAN Geolocation Whitepaper 2018, s. 2).

Sisätiloissa tarkkuutta vaativissa sovelluksissa voidaan käyttää BLE- tai Wi-Fi-menetelmiin perustuvia ratkaisuja. Näissä tukiasemien tiheydellä voidaan vaikuttaa saavutettavaan tarkkuuteen, mutta yhden tukiaseman toimintamatkat ovat suhteellisen lyhyitä. Menetelmiä voidaan myös yhdistellä, jolloin saadaan sekä sisätiloissa tarkasti toimiva, että

pitkällä toimintamatkalla toimiva ratkaisu. (LoRaWAN Geolocation Whitepaper 2018, s. 2–3.)

LPWA-verkot voidaan jakaa lisensoituja matkapuhelinverkkotaajuuksia käyttäviin tekniikoihin sekä lisensoimattomia taajuuksia käyttäviin tekniikoihin. LPWAN-tekniikalle itselleen ei ole olemassa standardia, tosin useat kaupalliset allianssit ovat luoneet standardeja yksittäisistä lisensoimattomia taajuuksia käyttävistä LPWAN-ratkaisuista, kuten LoRaWAN ja SigFox. Matkapuhelinoperaattorit tarjoavat matkapuhelinverkoissa toimivia LPWAN-ratkaisuja. EC-GSM-IoT perustuu EGPRS:ään, NB-IoT osittain LTE:hen rajoitetulla kaistalla ja LTE-M nimensä mukaisesti LTE:hen (kuva 19). (Low Power Wide Area Networks: An Overview, s. 1–2; LPWA network technologies and standards: LPWAN wireless IoT guide.)

Technologies	LTE-Evolution	Narrowband			Non-3GPP	
	LTE-M	NB-IoT		EC-GSM	LoRa	SigFox
		NB-LTE	NB-CIoT			
Coverage	< 11 km	< 15 km	< 15 km	< 15 km	< 20 km	< 13 km
Spectrum	Licensed (7-900 MHz)	Licensed (7-900 MHz)	Licensed (8-900 MHz)	Licensed (7-900 MHz)	Unlicensed (867-869 MHz or 902-928 MHz)	Unlicensed (900 MHz)
Bandwidth	1.4 MHz	200 kHz	200 kHz	2.4 MHz	125 kHz, 250 kHz, 500 kHz	100 kHz
Date Rate	< 1 Mbps	< 150 kbps	< 400 kbps	10 kbps	< 50 kbps	< 100 bps
Battery Life	> 10 years	> 10 years	< 10 years	> 10 years	< 10 years	> 10 years

Kuva 19. LPWAN-tekniikoiden vertailua. (Min, Yiming, Xin, Xiaofei, Iztok 2018).

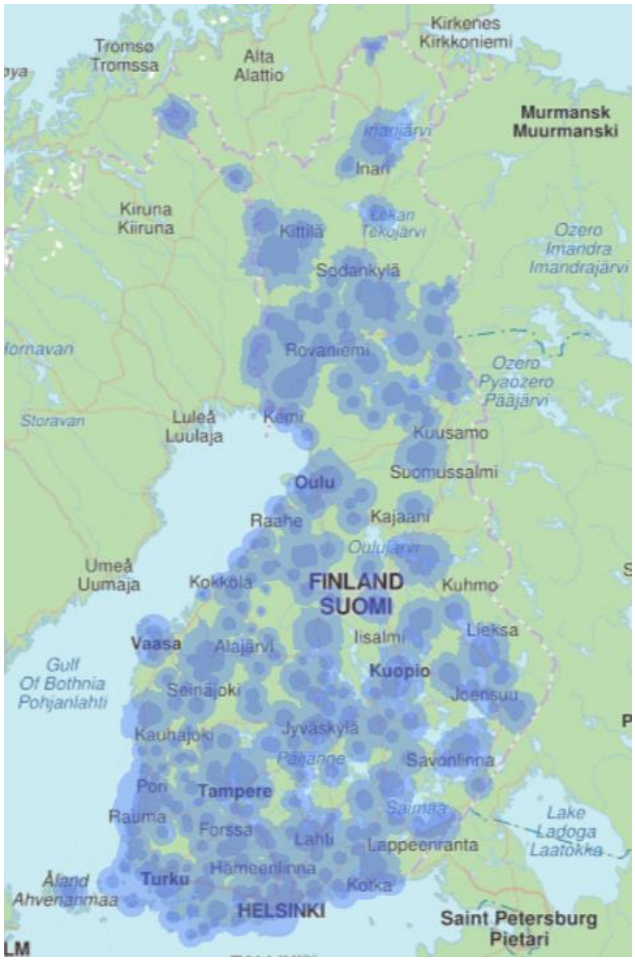
LPWA-verkoissa käytetään osittain samankaltaisia törmäyksenestomenetelmiä kuin RFID-tekniikassa. Esimerkiksi NB-IoT käyttää ja IEEE-standardi määrittelee käytettäväksi FDMA:ta ja Weightless-W sekä Weightless-P käyttävät sekä FDMA:ta että TDMA:ta. (Low Power Wide Area Networks: An Overview, s. 9–11.)

Suurin osa LPWA-tekniikoista käyttää todentamismenetelmänään symmetristä todentamista, joissa periaate on sama kuin alaluvussa 2.3.6 esitellyssä menetelmässä. (Low Power Wide Area Networks: An Overview, s. 15.)

Suomessa matkapuhelinoperaattori DNA tarjoaa sekä NB-IoT- että LTE-M -teknologioita tällä hetkellä 4G-verkossa ja on laajentamassa niitä myös 5G-verkkoon. Matkapuhelinoperaattorit Elisa ja Telia tarjoavat kumpikin ainoastaan NB-IoT -teknologiaa 4G-verkossa. (IoT-Teknologiat; IoT - Teollinen internet; NB-IOT.)

LoRaWAN-verkkoteknologia

LoRaWan on LoRa Alliance -järjestön standardoima globaali LPWA-verkkoteknologia. Järjestöön kuuluu yli 500 yritystä ja verkkoja oli vuoden 2018 lopussa yli 100 maassa. Suomessa LoRaWan-verkkoa ylläpitää ja kehittää Digita (kuva 20). (What is the LoRaWAN Specification? 2019.)



Kuva 20. Digitan ylläpitämän LoRaWan verkon peitto Suomessa (IoT:n kartta).

LoRaWan-verkot ovat tähtimuotoisia, joissa tiedonsiirto tapahtuu radiotaajuuksilla yksihyppyisenä, eli suoraan ilman välipisteitä päätelaitteilta yhdyskäytäville, joista edelleen IP-protokollaa käyttäen palvelimille. Verkkoratkaisusta löytyy myös tuki multicast-toiminnolle, jossa useille päätelaitteille voidaan lähettää samanaikaisesti viestejä hyödyntäen koko kaistan. LoRaWan käyttää päätelaitteiden ja yhdyskäytävien välillä muuttuvaa tie-

donsiirtonopeutta, jota palvelimet hallinnoivat radiolähetyksen tehon ohella päätelaitekohtaisesti. Täten saadaan maksimoitua verkon kapasiteetti ja minimoitua päätelaitteiden energiankulutus. Tiedonsiirtonopeus tekniikassa vaihtelee 0,3 kbps:n ja 50 kbps:n välillä. LoRaWan käyttää kahta eri salaustasoa, 128-bittisiä avaimia sekä verkkoliikenteeseen sekä sisällön salaamiseen. (What is the LoRaWAN Specification? 2019.)

LoRaWan päätelaitteet voidaan jakaa kolmeen eri luokkaan.

- A-luokan päätelaite on vähiten energiaa kuluttava, jonka kanssa kommunikointi tapahtuu asynkronisesti aina päätelaitteen tarpeesta. Päätelaitteen lähettämää viestiä seuraa kaksi vastaanottoikkunaa, jotka mahdollistavat palvelimen viestien vastaanottamisen.
- B-luokan päätelaitteen kanssa kommunikointi on A-luokan ominaisuuksien lisäksi mahdollista myös ennalta ajastettujen vastaanottoikkunoiden puitteissa. Tämä kasvattaa jonkin verran energiankulutusta, pitäen sen kuitenkin edelleen tarpeeksi maltillisena paristo- ja akkukäyttöisiä sovelluksia ajatellen.
- C-luokan päätelaite on vastaanottovalmiudessa jatkuvasti, mikä nostaa energiankulutusta huomattavasti. C-luokan päätelaitteet eivät ole ideaalisia sovelluksiin, joissa jatkuvaa virtaa ei ole saatavilla.

Päätelaitteiden tilaa voidaan tarvittaessa vaihtaa väliaikaisesti C-luokkaa vastaavaksi esimerkiksi laiteohjelmiston asennusta varten. (What is the LoRaWAN Specification? 2019.)

3 Menetelmän ja järjestelmän valinta

3.1 Valittu tekniikka

Kohdeyrityksen sovellukseen parhaiten sopivaksi automaattisen tunnistamisen tekniikaksi todetaan olevan RFID. Se mahdollistaa lähtevien kuljetusyksiköiden kontaktittoman ja nopean tunnistamisen turvallisesti ja hyvällä lukuvarmuudella. Käytettäväksi taajuusalueeksi valitaan UHF, joka mahdollistaa passiivisten tunnisteiden käyttämisen. Ne ovat tunnistusominaisuuksiltaan tarkoitukseen sopivia, fyysisiltä mitoiltaan pienikokoisia sekä niiden virtalähteettömyyden ansiosta kustannukset pysyvät maltillisina ja ne ovat käytännössä huoltovapaita. Valintaa puoltavat lähtevien kuljetusyksiköiden suuri volyymi, kuljetusyksiköiden fyysiset ominaisuudet, tarvittavat lukuetäisyydet sekä tilojen

ahtaus. Järjestelmän laitteiston valinnassa käytettäväksi standardinksi valitaan EPC UHF Gen2 Air Interface Protocol. Standardi on yhteensopiva ISO/IEC 18000-63 standardin kanssa ja markkinoilta löytyy paljon vaihtoehtoja tunnisteille sekä lukijoille. Standardissa määritellyt tunnisteiden muistiominaisuudet ovat riittävät sovelluksessa vaadittujen tietojen tallentamiseen. Standardi mahdollistaa sovellukselle riittävän tasoisen tietoturvan sekä tiedon eheyden tarkistamisen.

Konenäön käyttämistä viivakoodien lukemiseen lastauslaiturilla olisi hankala toteuttaa johtuen sen vaatimasta näköyhteydestä viivakoodin ja sen lukijan välillä. BLE-, Wi-Fi- ja LPWAN-ratkaisut vaatisivat aktiivisten tunnisteiden käyttämistä, jolloin tunnisteen koko ja hinta nousevat huomattavasti virtalähteen myötä. LPWAN-verkot avaisivat mahdollisuuden seurata kuljetusyksiköitä myös kuljetusmatkojen ajan lähettämön, terminaalien ja asiakkaiden välillä. Tämä vaatisi tosin usean eri paikannusmenetelmän käyttöä, jotta saataisiin riittävä tarkkuus sisätiloissa lähettämössä sekä riittävän pitkä toimintamatka kuljetusmatkoja ajatellen. LPWAN-tunnisteiden hinnat ovat kuitenkin tällä hetkellä korkeat, joten kohdeyrityksen suurten volyymien vuoksi kustannukset nousevat moninkertaisiksi RFID-tekniikkaan verrattuna.

EPC UHF Gen2 Air Interface Protocol

EPC UHF Gen2 Air Interface Protocol -standardi määrittelee fyysiset ja loogiset vaatimukset passiivisia tunnisteita käyttävälle, lukijan kontrolloiman kommunikaation RFID järjestelmälle UHF-taajuusalueella 860–960 MHz. (EPC UHF Gen2 Air Interface Protocol, s. 7.)

Standardi määrittelee tiedon eheyden tarkastukseen kaksi eri tarkistussummamenetelmää, CRC-16 ja CRC-5. Tarkistussummamenetelmät toimivat myös osana tietoturvaa. Toisena tietoturvamenetelmänä käytetään satunnaislukugeneraattoria, joka tuottaa 16-bittisen avaimen. Kyseistä avainta voidaan käyttää kahvana tai cover-koodina salasananvaihdoksissa. (EPC UHF Gen2 Air Interface Protocol, s. 33–57.)

Standardissa tunnisteen muisti on jaettu neljään eri loogiseen osioon.

- Reserved memory sisältää kirjautumis- sekä tuhoamissalasanat, jos sellaiset on käytössä

- EPC memory sisältää StoredCRC -koodin, StoredPC -koodin sekä EPC-koodin, jolla tunnisteen sisältämä objekti identifioidaan
- TID memory sisältää ISO/IEC 15963 standardin mukaisen tunnisteen luokituksen, joka kertoo lukijalle tunnisteen kanssa käytettävissä olevat komennot ja menetelmät.
- User memory on valinnainen, vapaassa käytössä oleva muisti.

Muistin fyysinen rakenne on tunnisteen valmistajan määriteltävissä. (EPC UHF Gen2 Air Interface Protocol, s. 41.)

Standardi määrittelee tunnisteiden hallinnalle kolme eri operaatiota. Select -operaatiolla voidaan valita tietty tunnistepopulaatio. Inventory -operaatiolla hoidetaan tunnisteiden tunnistaminen sekä yksilöinti. Access-operaatiolla voidaan olla vuorovaikutuksessa yksittäisen tunnisteen kanssa esimerkiksi tietojen lukemista tai uudelleenkirjoittamista varten. (EPC UHF Gen2 Air Interface Protocol, s. 57.)

Laajennettavuus tulevaisuudessa

Lähtevien kuljetusyksiköiden automaattista tunnistamista tulevaisuudessa on pohdittu myös terminaali- ja asiakaspäähän, jolloin sama varmuus ja läpinäkyvyys saataisiin läpi koko toimitusketjun. Terminaali- ja asiakaspään ratkaisut on rajattu pois opinnäytetyöstä, mutta järjestelmän mahdollinen laajentaminen on otettu huomioon. Valittua UHF-taajuusalueella toimivaa RFID-tunnistusta on mahdollista käyttää myös kuljetuksen eri vaiheissa joko luomalla pysyviä lukualueita terminaali- ja asiakaspäähän tai käyttämällä langattomia käsilukijoita.

3.2 Järjestelmän osat

Vaatimusmäärittelyssä asetettujen vaatimusten lisäksi järjestelmän komponenteiksi valitaan standardin EPC UHF Gen2 Air Interface Protocol toteuttavat komponentit. Valinnoissa on kiinnitetty erityistä huomiota tilojen ahtauden luomiin haasteisiin. (Liite 1: Vaatimusmäärittely.)

Tunnisteet

Uudelleen käytettäviin kuljetusyksiköihin pysyviksi tunnisteiksi valittiin vaihtoehdoiksi Confidex Carrier PRO sekä Omni-ID IQ 800P (taulukko 3). Kummatkin ovat EPC Class1 Gen2 standardin mukaisia ja ne ovat myös luokiteltu pesunkestäviksi. Tunnisteiden sijainniksi uudelleen käytettävässä kuljetusyksikössä valitaan paikka, joka on mahdollisimman hyvin suojassa mekaaniselta kuormitukselta. Parhaiten paikaksi soveltuvat liitteessä 2 merkityt kohdat 1 ja 2.

Tunnisteiden pesunkestävyys tulee testata huolellisesti. Reaalimaailma voi poiketa testiympäristöstä merkittävästi, vaikka luvattujen ominaisuuksien ja valmistajan testien perusteella tunnisteet ovatkin sovellukseen sopivia.

Taulukko 3. Pysyvien tunnisteiden vaihtojen vertailua (Product Datasheet Confidex Carrier Pro 2013; Product Datasheet Omni-ID® IQ 800P 2017).

Tunniste	**Confidex Carrier PRO**	**Omni-ID IQ 800P**
Protokolla	EPC Class1 Gen2	EPC Class1 Gen2
Taajuusalue	860-960 MHz	860-960 MHz
Lukuetäisyys	<12,5 m	<10,0 m
Muisti	EPC 128 bit, User 512 bit, TID 96 bit	EPC 96 bit, User 512 bit, TID 64 bit
Alusta-materiaali	Muovi ja muut ei metalliset pinnat	Muovi ja muut ei metalliset pinnat
Koko	92 x 24 x 0,2 mm	95 x 21 x 0,24 mm
Lämmönkesto	-35°C…+90°C	-35°C…+85°C
IP-luokitus	IP68	IP68
Pesunkesto	Kyllä	Kyllä
Pesusyklejä	Min. 800	Ei ilmoitettu

Muihin kuljetusyksiköihin valitaan kertakäyttöiset tulostettavat tunnisteet, joihin on mahdollista tulostaa myös nykyisen osoitetarran mukaiset näkyvät tiedot pintaan. Vaihtoehdoiksi on valittu Confidex Crosswave Classic ja Zebra Z-Perform 1500T ZBR4000 (taulukko 4). Kummatkin ovat standardin EPC Class1 Gen2 mukaisia, nykyisen osoitetarran kokoisia sekä yhteensopivia valitun tulostimen kanssa.

Taulukko 4. Kertakäyttöiset tulostettavien tunnisteiden vaihtoehtojen vertailua (Product Datasheet Confidex Crosswave Classic 2019; Materials Spec Sheet Z-Perform 1500T 2016; Materials Spec Sheet Zebra ZBR4000 Inlay 2019).

Tunniste	**Confidex Crosswave Classic**	**Zebra Z-Perform 1500T ZBR4000**
Protokolla	EPC Class1 Gen2	EPC Class1 Gen2
Taajuusalue	860-960 MHz	860-960 MHz
Lukuetäisyys	<10 m	<20 m
Muisti	EPC 496 bit, User 128 bit, TID 64 bit	EPC 128 bit, User N/A, TID 96 bit
Alusta-materiaali	Ei-metalliset pinnat	Ei-metalliset pinnat
Koko	101,6 x 155,4 x 0,2 mm (4” x 6”)	101,6 x 152,4 x 0,2 mm (4” x 6”)
Lämmönkesto	-35°C…+70°C	-40°C…+85°C
IP-luokitus	IP68	Ei ilmoitettu

Kertakäyttöiset tunnisteet tulostetaan ja liimataan kuljetusyksiköiden päätyihin pakkauspisteillä, joten jokainen pakkauspiste tulee varustaa omalla tunnistetulostimella.

Lukijat

Lastauslaitureille valittiin Impinj Speedway Revolution R420 -lukija. Asiakkailta palautuvien uudelleen käytettävien kuljetusyksiköiden tunnistukseen, lähettämöön saapuvien uudelleen käytettävien kuljetusyksiköiden tunnistukseen ja keräilyyn lähtevien uudelleen käytettävien kuljetusyksiköiden kirjoituspisteen yhteyteen valittiin Impinj Speedway Revolution R120 -lukija (taulukko 5). Lukijat ovat suorituskyvyltään erinomaisia ja ne sisältävät tarpeellisen määrän antenniportteja kunkin lukualueen luomiseksi.

Taulukko 5. Lukijoiden vertailua (Product Datasheet Speedway Reader Family 2019).

Lukija	**Speedway Revolution R420**	**Speedway Revolution R120**
Protokolla	EPC Class1 Gen2	EPC Class1 Gen2
Taajuusalue	EU1: 865-868 MHz EU2: 915-921 MHz	EU1: 865-868 MHz
Lähetysteho	EU1: 31.5 dBm AC/30.0 dBm PoE EU2: 33.0 dBm AC/33.0 dBm PoE+	EU1: 30.0 dBm AC/30.0 dBm PoE
Antenniportit	4	1
Lukunopeus	1100 tunnistetta/s	200 tunnistetta/s
Jännitelähde	AC-DC power supply/PoE	AC-DC power supply/PoE
Op-erointilämpötila	-20°C…+50°C	-20°C…+50°C
IP-luokitus	IP52	IP52

Lukijat sijoitetaan suojaisaan paikkaan lukualueiden läheisyyteen, jotta antennikaapeloinnista saadaan mahdollisimman yksinkertaista. Lukualueiden sijainnit on merkitty liitteessä 3.

Antennit

Lastauslaiturien lukualueiden antennivaihtoehdoiksi valittiin Kathrein WRA 7070 ja Advantenna-SP12 (taulukko 6). Tunnisteet voivat olla missä tahansa päin lukualuetta, joten ympyrämuotoisella polarisaatiolla olevilla antenneilla saavutetaan paras lukuvarmuus sovelluksen lukualueilla. Lukualueet ovat lastauslaiturilla hyvin lähekkäin toisiaan, joten ristilukujen tunnistamiseksi ja eliminoimiseksi on perusteltua käyttää useaa antennia per lukualue. Lukualueiden sijainnit ja mitat on merkitty liitteessä 3.

Taulukko 6. Lastauslaitureiden antennivaihtoehtojen vertailua (Product Datasheet WRA 7070 2019; Product Datasheet Advantenna-SP12 2019).

Antenni	**Kathrein WRA 7070**	**Advantenna-SP12**
Taajuusalue	865–868 MHz	865 - 868 MHz
Polarisaatio	Ympyrä	Ympyrä
Keilanleveys	65°/65°	40°/70°
Vahvistus	8,5 dBi	9,5 dBi
Lukuetäisyys	<12 m	<10 m
Impedanssi	50 Ω	50 Ω
Operointilämpötila	-40°C…+70°C	-20°C…+70°C
IP-luokitus	IP67	IP62

Asiakkailta palautuvien uudelleen käytettävien kuljetusyksiköiden tunnistukseen, lähettämöön saapuvien uudelleen käytettävien kuljetusyksiköiden tunnistukseen ja keräilyyn lähtevien uudelleen käytettävien kuljetusyksiköiden kirjoituspisteen antennivaihtoehdoiksi valittiin Impinj Mini-Guardrail, Kathrein MIRA-100 ja Kathrein WRA 6060 (taulukko 7). Kuljetusyksiköt kulkevat kyseessä oleviin pisteisiin kuljetinhihnaa pitkin, joten tarvittavat lukuetäisyydet ovat pieniä.

Taulukko 7. Kuljetinhihnojen antennivaihtoehtojen vertailua (Product Datasheet Mini-Guardrail Antenna 2018; Product Datasheet WRA 6060 2019; Product Datasheet MIRA-100 2019)

Antenni	**Impinj Mini-Guardrail**	**Kathrein MIRA-100**	**Kathrein WRA 6060**
Taajuusalue	860-960 MHz	865–868 MHz	865–868 MHz
Polarisaatio	Lineaarinen	Ympyrä	Ympyrä
Keilanleveys	-	100°/100°	60°/60°
Vahvistus	Far-Field: -20 dBi	2,5 dBi	5,5 dBi
Lukuetäisyys	<7,5 cm	<2 m	<5 m
Impedanssi	50 Ω	50	50
Operointilämpötila	0°C…+40°C	-20°C…+55°C	-40°C…+70°C
IP-luokitus	IP41	IP67	IP67

Tunnistetulostimet ja päätelaitteet

Tunnistetulostimeksi valittiin Zebra ZT410. Tulostimella voi tulostaa EPC Class1 Gen2 standardin mukaisia tunnisteita nykyisen kokoiselle osoitetarrapohjalle. Yrityksellä on ennestään käytössä samanmallisia tulostimia, joskin RFID-tulostusominaisuutta ei ole vielä hyödynnetty.

Jokaisen lastauslaiturin yhteyteen sijoitetaan väliohjelmistoon yhteydessä oleva kiinteästi asennettu kosketusnäytöllinen päätelaite. Esimerkiksi Apple/Android tablettitietokone + seinäteline soveltuu tarkoitukseen.

Väliohjelmisto

Väliohjelmiston käyttö on perusteltua järjestelmän laajuuden vuoksi. Lukijoilta tulee paljon dataa, joka on käsiteltävä ennen tuotannonohjausjärjestelmään lähettämistä. Erillistä väliohjelmistoa käyttämällä voidaan luoda myös mahdollisuus kuljetusyksiköiden lastaamiselle riippumattomana tuotannonohjausjärjestelmän tilasta. Sopivia väliohjelmistoja ovat esimerkiksi Aspire Middleware, Microsoftin Biztalk ja SAPin Auto-ID Infrastructure. Jotkin RFID-järjestelmätoimittajat tarjoavat lisäksi myös itse kehittämiään väliohjelmistoja.

4 Järjestelmätoiminnot

Kuljetusyksiköiden yhdistäminen SSCC-koodiin

Uudelleen käytettävän kuljetusyksikön tunnisteeseen kirjoitetaan SSCC-koodi keräilyyn lähdön yhteydessä. Kuljetusyksikön sijainniksi kirjataan järjestelmässä ”keräilyssä”. Kertakäyttöisiin kuljetusyksiköihin tulostetaan ja liimataan tunniste, johon kirjoitetaan tulostamisen yhteydessä SSCC-koodi.

Lähtevien kuljetusyksiköiden tunnistaminen

Kuljettaja valitsee lastauslaiturin päätelaitteelta lastattavan kuljetusreitin. Lastauslaiturin kautta lastatut kuljetusyksiköt tunnistetaan ja jos ne kuuluvat laituriin yhdistettyyn kuljetusreittiin, ne kirjataan lastatuiksi. Lastauslaiturin päätelaite hälyttää, jos lastauslaiturin kautta lastataan väärän kuljetusreitin kuljetusyksiköitä. Kun kaikki kuljetusreitin kuljetusyksiköt on lastattu, kuljetusreitti kirjataan kuljetusvalmiiksi ja tieto lähetetään varastonhallintajärjestelmälle sekä ilmoitetaan lastauslaiturin päätelaitteella. Kun reitti on kuljetettu varastonhallintajärjestelmässä, kuljetusyksiköt kirjataan lähetetyiksi ja kuljetusreitti irrotetaan lastauslaiturista.

Tunnisteettomat ja vialliset uudelleen käytettävät kuljetusyksiköt

Tunnisteettomat uudelleen käytettävät kuljetusyksiköt voidaan poistaa kierrosta lisäämällä RFID-lukija nykyisen laatikkopesukoneen jälkeen olevan viivakooditarkistuspisteen yhteyteen. Nykyisellään mekaaninen manipulaattori poistaa kuljetushihnalta kuljetusyksiköt, joista puuttuu viivakoodi tai se on viallinen. Tunnisteettomien sekä fyysisesti viallisten uudelleen käytettävien kuljetusyksiköiden tunnisteet kirjataan poistetuiksi järjestelmässä.

Kuljetusyksiköiden sijaintitieto

Uudelleen käytettävien kuljetusyksiköiden sijainti asiakkaille lähteneiden kuljetusyksiköiden lisäksi saadaan selville tunnistamalla myös asiakkailta palautuvat kuljetusyksiköt,

keräykseen lähtevät kuljetusyksiköt sekä lähettämöön saapuvat kuljetusyksiköt. Kuljetusyksikön sijaintitietona voisi siis olla esimerkiksi ”varastossa”, ”keräyksessä”, ”lähettämössä”, ”lastattu”, ”lähetetty” tai ”poistettu kierrosta”. Palautuvien kuljetusyksiköiden tunnistamiseen käytetään samaa lukijaa, kun tunnisteettomien kuljetusyksiköiden poistamiseen.

5 Kustannusarvio

Työssä luotiin kaksi eri kustannusarviota. Toisessa on otettu huomioon kaikkien yrityksestä lähtevien kuljetusyksiköiden tunnistaminen ja toisessa ainoastaan uudelleen käytettävien kuljetusyksiköiden tunnistaminen. Kertakäyttöisiä kuljetusyksiköitä lähtee päivittäin 1100 kpl ja keräily- sekä pakkaustoiminnot tapahtuvat monessa eri yksikössä, jonka vuoksi tunnistetulostimia tarvitaan suuri määrä. Tunnistetulostimien ja kertakäyttöisten tunnisteiden hintojen vuoksi kustannukset nousevat huomattavasti.

Kertaluontoisia kustannuksia kaikkien kuljetusyksiköiden tunnistuksesta yhteensä 130000–240000 € ja vuosittaisia kustannuksia n. 60000 €. Kertaluontoisia kustannuksia pelkästään uudelleen käytettävien kuljetusyksiköiden tunnistuksesta yhteensä 100000–200000 € ja vuosittaisia kustannuksia n. 3000–5000 €.

Laitteisto

Laitteiston osalta uudelleen käytettävien kuljetusyksiköiden tunnistamisesta muodostuu kustannusarvioksi n. 70000 €–130000 € (taulukko 8). Laitteiston hinnat ovat listahintoja suoraan niitä tarjoavien yritysten verkkokaupoista.

Kuljetusyksiköiden pesutiheyden ja tunnisteille luvatun pesusyklien keston perusteella tunnisteiden käyttöikä on 16,7 vuotta. Tunnisteiden uusimisesta koituvat kustannukset voidaan jakaa vuositasolle, jolloin saadaan vuosittaisiksi kustannuksiksi n. 3000–5000 €.

Taulukko 8. Laitteiston kustannusarvio uudelleen käytettävien kuljetusyksiköiden tunnistamisessa

	Lukumäärä	Yksikköhinta	Yhteensä
Pysyvät tunnisteet	100000	0,36–0,76 €	36000,00–76000,00 €
Lastauslaiturin lukijat	14	1075,00–1821,30 €	15050,00–25498,20 €
Lastauslaiturin antennit	56	120,00–202,00 €	6720,00–11312,00 €
Muut lukijat	2	680,00–966,70 €	1360,00–1933,40 €
Muut antennit	2	126,00–287,46 €	252,00–574,92 €
Antennikaapelit	58	43,45–111,69 €	2520,10–6478,02 €
Lastauslaiturin päätelaitteet	14	362,90 €–508,00 €	5080,60 €–7112,00 €
Yhteensä			**66982,70 €–128908,54 €**

Lisäkustannuksia laitteistolle kertakäyttöisten kuljetusyksiköiden tunnistamisesta muodostuu kertakäyttöisistä tunnisteista n. 55000 €/v sekä tunnistetulostimista n. 32000–42000 € (taulukko 9). Tunnistetulostimien lukumäärässä otettu huomioon yrityksellä tällä hetkellä käytössä olevat yhteensopivat tulostimet.

Taulukko 9. Laitteiston lisäkustannukset kertakäyttöisten kuljetusyksiköiden tunnistamisessa.

	Lukumäärä	Yksikköhinta	Yhteensä
Kertakäyttöiset tunnisteet	276100 kpl/v	0,20 €	55220,00 €/v
Tunnistetulostimet	10	3235,00–4165,00 €	32350,0–41650,0 €

Ohjelmisto, järjestelmäintegraatio sekä tunnisteiden lisääminen

Väliohjelmiston hinnaksi arvioidaan 5000–20000 € ja taustajärjestelmään integraation hinnaksi arvioidaan 15000–40000 €. (Nummela 2014; Nurminen 2006.)

Tunnisteiden lisääminen tuotteisiin ja niiden vieminen järjestelmään käy kahdelta henkilöltä nopeudella 350–400 tunnistetta tunnissa. (Bowen Ayre 2012 s. 19) Tunnisteiden lisääminen 100000:een uudelleen käytettävään kuljetusyksikköön ja niiden vieminen järjestelmään veisi siis n. 500–570 henkilötyötuntia, josta saadaan 24 € tuntiveloituksella n. 12000–14000 €.

6 Yhteenveto

Opinnäytetyön tavoitteena oli tutkia kohdeyrityksen lähtevien kuljetusyksiköiden tunnistamisen automatisoinnin mahdollisuutta. Selvitystyön pohjalta on tarkoitus luoda päätös työssä esitetyn ratkaisun toteuttamisesta.

Selvitystyö aloitettiin kuvaamalla nykyprosessi ja laatimalla vaatimusmäärittely sovelluksen tarkempien tarpeiden ja rajoitteiden selville saamiseksi. Tämän jälkeen aloitettiin olemassa oleviin automaattiseen tunnistukseen ja tiedonkeruuseen, sekä sen tekniikoihin ja menetelmiin tutustuminen. Eri tekniikoiden ominaisuuksia läpikäymällä voitiin hahmottaa kohdesovellukseen ylipäätään käyvät vaihtoehdot ja valita niistä parhaiten tarkoitukseen sopiva tekniikka. Kun toiminnallisuustarpeet oli kartoitettu ja käytettävä tekniikka selvillä, valittiin sopivat laitteistovaihtoehdot järjestelmän toteuttamiseksi.

Automaattisella tunnistuksella ja tiedonkeruulla tarkoitetaan tekniikoita objektien automaattiseen tunnistamiseen, niistä tiedon keräämiseen ja tiedon edelleen välittämiseen taustajärjestelmille. Kohdeyrityksen sovellukseen parhaiten sopivaksi vaihtoehdoksi todettiin UHF-taajuusalueen RFID-tekniikka. RFID on radiotaajuustunnistustekniikka, joka mahdollistaa lähtevien kuljetusyksiköiden tunnistamisen automaattisesti ja kontaktittomasti. UHF-taajuusalueella saavutetaan riittävä lukuetäisyys ja kuljetusyksiköissä voidaan käyttää passiivisia tunnisteita, jotka eivät vaadi virtalähdettä. Ne ovat fyysisesti pienikokoisia, niiden elinikä on pitkä ja ne ovat alhaisen hintansa puolesta yrityksen suuriin volyymeihin sopivia.

Työssä päästiin tavoitteisiin ja työn perusteella yrityksellä on hyvät edellytykset lähteä toteuttamaan järjestelmää. Ajanmukaisen lähdemateriaalin löytäminen oli paikoitellen haasteellista sillä automaattinen tunnistaminen ja tiedonkeruu on nopeasti kehittyvä ala. Työhön olisi ollut mahdollisesti hyödyllistä ottaa vielä mukaan tarjouksia sovelluksia tarjoavilta yrityksiltä, jolloin laitteiden vertailuun olisi saatu luultavasti enemmän vaihtoehtoja. Nyt tarjousten pyytäminen päätettiin jättää vasta järjestelmän toteuttamisvaiheeseen.

Lähteet

Bienhaus, Diethelm. 2009. Patterns for Managing Data in Complex Automatic Identification and Data Capturing Environments. Saksa: Institute of Nanostructure Technologies and Analytics / Technological Electronics, University of Kassel & Department of Systems Engineering, University of Cooperative Education Nordhessen.

Bluetooth Core Specification v. 5.2. 2019. Bluetooth SIG.

Bowen Ayre, Lori. 2012. RFID in Libraries: A Step toward Interoperability. Yhdysvallat: American Library Association.

Discover Wi-Fi. Verkkoaineisto. Wi-Fi Alliance 2020. <https://www.wi-fi.org/discover-wi-fi>. Luettu 4.4.2020.

EPC/RFID Standards. Verkkoaineisto. GS1. <https://www.gs1.org/standards/epc-rfid>. Luettu 21.10.2019.

FEIG Electronics Products. Verkkoaineisto. FEIG Electronics. <https://www.feig.de/en/products/identification/product/id-iscmrm102/>. Luettu 9.11.2019.

Finkenzeller, Klaus. 2010. RFID Handbook. Iso-Britannia: John Wiley & Sons Ltd.

GS1 barcodes. Verkkoaineisto. GS1. <https://www.gs1.org/standards/barcodes>. Luettu 10.9.2019.

Hsin-Chin, Liu. 2010. The Approaches in Solving Passive RFID Tag Collision Problems, Radio Frequency Identification Fundamentals and Applications Bringing Research to Practice. Romania: InTech.

Introduction Into Barcodes. 2014. Verkkoaineisto. ByteScout. <https://bytescout.com/books/introduction-into-barcodes-book.html>. Luettu 10.9.2019.

IoT:n kartta. Verkkoaineisto. Digita. <https://www.digita.fi/iotn-kartta/>. Luettu 1.10.2019.

IoT-Teknologiat. Verkkoaineisto. DNA Oyj. <https://www.dna.fi/yrityksille/iot/iot-teknologiat>. Luettu 25.11.2019.

IoT - Teollinen internet. Verkkoaineisto. Elisa Oyj. <https://yrityksille.elisa.fi/iot-teollinen-internet>. Luettu 25.11.2019.

ISO/IEC 18000-6. Information technology — Radio frequency identification for item management — Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General. 2013. International Organization for Standardization.

Learn About Bluetooth. 2020. Verkkoaineisto. Bluetooth SIG. <https://www.bluetooth.com/learn-about-bluetooth/>. Luettu 4.4.2020.

LoRaWAN Geolocation Whitepaper. 2018. Toimintokuvaus. LoRa Alliance.

LPWA network technologies and standards: LPWAN wireless IoT guide. Verkkoaineisto. i-SCOOP. <https://www.i-scoop.eu/internet-of-things-guide/lpwan/>. Luettu 30.9.2019.

Materials Spec Sheet Z-Perform 1500T. 2016. Tuotetietolomake. Zebra Technologies.

Materials Spec Sheet Zebra ZBR4000 Inlay. 2019. Tuotetietolomake. Zebra Technologies.

Min Chen, Yiming Miao, Xin Jian, Xiaofei Wang, Iztok Humar. 2018. Cognitive-LPWAN: Towards Intelligent WirelessServices in Hybrid Low Power Wide AreaNetworks. Verkkoaineisto. <https://www.researchgate.net/publication/328016136_Cognitive-LPWAN_Towards_Intelligent_Wireless_Services_in_Hybrid_Low_Power_Wide_Area_Networks>. Luettu 25.11.2019.

NB-IOT. Verkkoaineisto. Telia Finland Oyj. <https://www.telia.fi/yrityksille/iot/yhteydet/nb-iot?intcmp=b2b-iot-yhteydet-nb-iot>. Luettu 25.11.2019.

NFC Technology. Verkkoaineisto. NFC Forum. <https://nfc-forum.org/what-is-nfc/about-the-technology/>. Luettu 24.9.2019.

Nummela, Jussi. 2014. RFID-järjestelmän toteuttaminen helposti ja edullisesti. Verkkoaineisto. <https://docplayer.fi/2349287-Rfid-jarjestelman-toteuttaminen-helposti-ja-edullisesti-case-euroports.html>. Luettu 10.12.2019.

Nurminen, Timo 2006. The End of RFID Middleware? Verkkoaineisto. <https://www.rfidjournal.com/articles/view?2035>. Luettu 10.12.2019.

Pietikäinen, Matti & Silven, Olli. Konenäkö. Oulu: Oulun yliopisto, sähkötekniikan osasto.

Product Datasheet Advantenna-SP12. 2019. Tuotetietolomake. Keonn.

Product Datasheet Confidex Carrier Pro. 2013. Tuotetietolomake. Confidex.

Product Datasheet Confidex Crosswave Classic. 2019. Tuotetietolomake. Confidex.

Product Datasheet Mini-Guardrail Antenna. 2018. Tuotetietolomake. Impinj.

Product Datasheet MIRA-100. 2019. Tuotetietolomake. Kathrein.

Product Datasheet Omni-ID® IQ 800P. 2017. Tuotetietolomake. Omni-ID.

Product Datasheet Speedway Reader Family. 2019. Tuotetietolomake. Impinj.

Product Datasheet WRA 6060. 2019. Tuotetietolomake. Kathrein.

Product Datasheet WRA 7070. 2019. Tuotetietolomake. Kathrein.

Regulatory Constraints On The Use Of RFID. Verkkoaineisto. RFID in Europe. <http://www.rfidineurope.eu/SR>. Luettu 21.10.2019.

RFID Readers. Verkkoaineisto. IDnova. <https://www.idnova.it/>. Luettu 24.9.2019.

RFID Tags. 2014. Verkkoaineisto. Coresonant. <https://coresonant.appspot.com/html/Tags.html>. Luettu 18.9.2019.

SAP Auto-ID Infrastructure. Verkkoaineisto. SAP. <https://help.sap.com/doc/saphelp_aii710/7.1/en-US/48/d1d97590d75430e10000000a42189b/frameset.htm>. Luettu 30.11.2019.

SFS-käsikirja 301-1 RFID. Osa 1: Opas. Johdatus tekniikkaan. 2010. Helsinki: Suomen Standardisoimisliitto SFS Ry.

Toivonen, Antti 2012. Identifying and Controlling Stray Reads at RFID Gates. Diplomityö. Espoo: Aalto-yliopisto, Automaatio- ja systeemitekniikan laitos.

Usman Raza, Parag Kulkarni, Mahesh Sooriyabandara 2017. Low Power Wide Area Networks: An Overview. IEEE Communications Surveys & Tutorials Volume: 19 Issue: 2.

What is the LoRaWAN® Specification? 2019. Verkkoaineisto. LoRa Alliance. <https://lora-alliance.org/about-lorawan>. Luettu 1.10.2019.

Vaatimusmäärittely

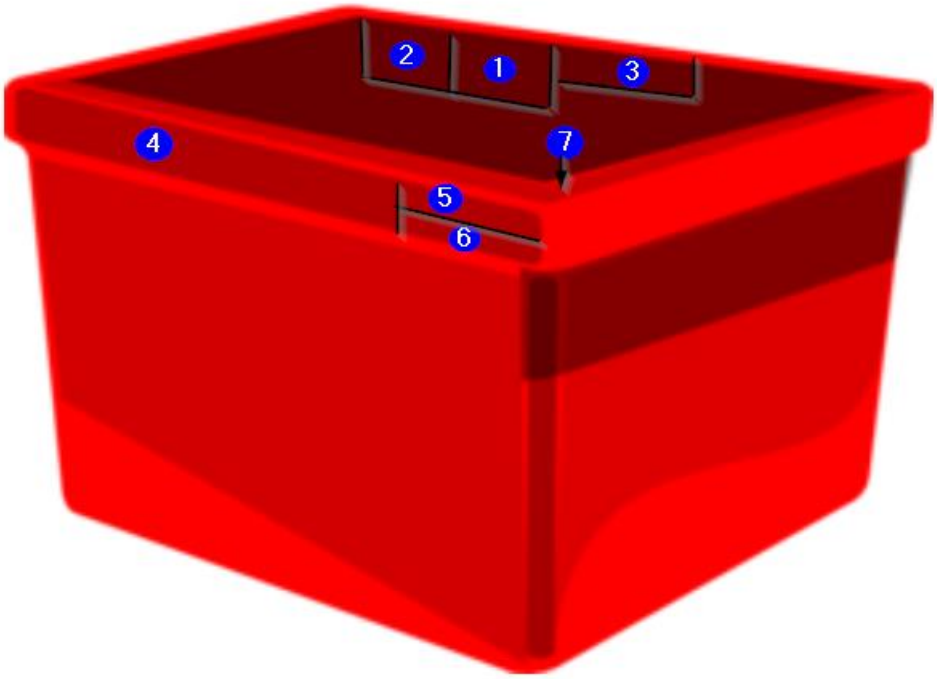
Käyttöympäristö			
Luokka	**ID**	**Vaatimus**	**Tärkeys**
Tunniste	V1.1.1	Pysyvän tunnisteen tulee kestää lämpötila-välillä -35°C… + 60°C	Pakollinen
	V1.1.2	Pysyvän tunnisteen tulee pystyä operoi-maan lämpötilavälillä 0°C… + 40°C	Pakollinen
	V1.1.3	Pysyvän tunnisteen IP-luokitus tulee olla vähintään IP67	Pakollinen
	V1.1.4	Pysyvän tunnisteen tulee kestää pesuko-neen vedenpaine 30 bar	Pakollinen
	V1.1.5	Pysyvän tunnisteen tulee kestää pesuko-neen kemikaalit	Pakollinen
	V1.1.6	Pysyvän tunnisteen tulee kestää vähintään 500 pesusykliä	Pakollinen
	V1.1.7	Pysyvän tunnisteen tulee kestää laatikon fyysinen käsittely	Pakollinen
	V1.1.8	Tulostettavan tunnisteen tulee kestää läm-pötilavälillä -35°C… + 40°C	Pakollinen
	V1.1.9	Tulostettavan tunnisteen tulee pystyä ope-roimaan lämpötilavälillä 0°C… + 40°C	Pakollinen
	V1.2.0	Tulostettavan tunnisteen tulee kestää laati-kon fyysinen käsittely	Pakollinen
Lukija	V1.2.1	Lastauslaiturin lukijan tulee pystyä operoi-maan lämpötilavälillä -20°C… + 40°C	Pakollinen
	V1.2.2	Lastauslaiturin lukijan IP-luokitus tulee olla vähintään IP52	Pakollinen
	V1.2.3	Lastauslaiturin lukijan tulee olla häiriösuo-jattu	Pakollinen
	V1.2.4	Muiden lukualueiden lukijoiden tulee pys-tyä operoimaan lämpötilavälillä 0°C… + 40°C	Pakollinen
	V1.2.5	Muiden lukualueiden lukijoiden IP-luokitus tulee olla vähintään IP52	Pakollinen
Antenni	V1.3.1	Lastauslaiturin antennin tulee pystyä ope-roimaan lämpötilavälillä -20°C… + 40°C	Pakollinen
	V1.3.2	Lastauslaiturin antennin IP-luokitus tulee olla vähintään IP52	Pakollinen
	V1.3.3	Muiden lukualueiden antennien tulee pys-tyä operoimaan lämpötilavälillä 0°C… + 40°C	Pakollinen

	V1.3.4	Muiden lukualueiden antennien IP-luokitus tulee olla vähintään IP52	Pakollinen
Tunnistetulostin	V1.4.1	Tunnistetulostimien tulee kestää lämpötila-välillä 0° C… + 40° C	Pakollinen
	V1.4.2	Tunnistetulostimien IP-luokitus tulee olla vähintään IP52	Pakollinen
Tunnistaminen			
Luokka	**ID**	**Vaatimus**	**Tärkeys**
Lastauslaituri	V2.1.1	Luennan lukuetäisyys min. 3 m	Pakollinen
	V2.1.2	Luennan lukunopeus min. 100 tunnistetta/s	Pakollinen
	V2.1.3	Luennan tulee olla laiturikohtaista, viereisten laitureiden laatikoita ei saa lukea	Pakollinen
	V2.1.4	Luennan tulee tunnistaa laatikoiden liikesuunta	Toivottava
Muut lukualueet	V3.2.1	Luennan lukuetäisyys 0,1 m	Pakollinen
	V3.2.2	Luennan lukunopeus min. 1 tunnistetta/s	Pakollinen
	V3.2.3	Tunnisteettomat laatikot poistetaan linjalta pesukoneen jälkeen	Pakollinen
Keräilyn aloitus	V4.3.1	Tunnisteettomat laatikot ohjataan virheradalle ennen keräilyn aloitusta	Toivottava
Käyttäjät			
Luokka	**ID**	**Vaatimus**	**Tärkeys**
Kuljetusliikkeen työntekijä	V3.1.1	Kuljetusliikkeen työntekijä liittää lastattavan reitin tai reitille luodun ajoneuvon käytettävään lastauslaituriin	Pakollinen
	V3.1.2	Kuljetusliikkeen työntekijä saa hälytyksen reitille kuulumattomista laatikoista	Pakollinen
	V3.1.3	Kuljetusliikkeen työntekijä saa ilmoituksen reitin ollessa valmis	Toivottava
Pakkaamon työntekijä	V3.2.1	Tulostaa tunnistetarran	Pakollinen
Järjestelmätoiminnot			
Luokka	**ID**	**Vaatimus**	**Tärkeys**
Varastonohjausjärjestelmä	V4.1.1	Laatikon lastaustieto tulee lähettää varastonohjausjärjestelmään	Pakollinen

Yleiset	V4.2.1	Varastossa ja asiakkailla olevien laatikoiden kokonaismäärät tulee olla saatavilla	Pakollinen
	V4.2.2	Lähettämöön saapuneet laatikot tulee voida tunnistaa	Pakollinen
	V4.2.3	Laatikoiden kiertosykli tulee olla saatavilla	Toivottava
Liitynnät ja rajapinnat			
Luokka	**ID**	**Vaatimus**	**Tärkeys**
Laitteistorajapinnat	V5.1.1	Lukijat saavat käyttöjännitteen verkkovirrasta	Pakollinen
	V5.1.2	Tunnistetulostimet saavat käyttöjännitteen verkkovirrasta	Pakollinen
Tietoliikennerajapinnat	V5.2.1	Lukijat liitetään lähiverkkoon RJ45-kaapeleilla	Pakollinen
	V5.2.2	Tunnistetulostimet liitetään lähiverkkoon RJ45-kaapeleilla	Pakollinen
Ohjelmistorajapinnat	V5.3.1	Varastonohjausjärjestelmä	Pakollinen
Tiedon eheys ja tietoturva			
Luokka	**ID**	**Vaatimus**	**Tärkeys**
Tunnistaminen	V6.1.1	Siirretyn tiedon eheys tarkistettava	Pakollinen
	V6.1.2	Tunnisteen sisältöä ei tule pystyä lukemaan ulkopuolisten toimesta	Pakollinen
	V6.1.3	Tunnisteen sisältöä ei tule pystyä tyhjentämään tai uudelleenkirjoittamaan ulkopuolisten toimesta	Pakollinen
Käytettävyystestaus			
Luokka	**ID**	**Vaatimus**	**Tärkeys**
	V7.1.1	Tunnisteiden pesunkestävyys tulee testata	Pakollinen
	V7.1.2	Tunnistaminen tulee testata	Pakollinen
	V7.1.3	Tunnisteelle kirjoittaminen tulee testata	Pakollinen
	V7.1.4	Lastattavan reitin tai reitille luodun ajoneuvon käytettävään sitominen lastauslaituriin tulee testata	Pakollinen
Koulutus ja tuki			
Luokka	**ID**	**Vaatimus**	**Tärkeys**

Laitteet	V8.1.1	Ylläpidon ja huollon vastuut sovittava laite-toimittajan kanssa	Pakollinen
	V8.1.2	Tunnistetulostimen koulutuksesta sovittava laitetoimittajan kanssa	Pakollinen
Järjestelmä	V8.2.1	Koulutus sovittava	Pakollinen

Uudelleen käytettävä kuljetusyksikkö



1 108 x 36 mm

2 110 x 36 mm

3 110 x 18 mm

4 230 x 36 mm

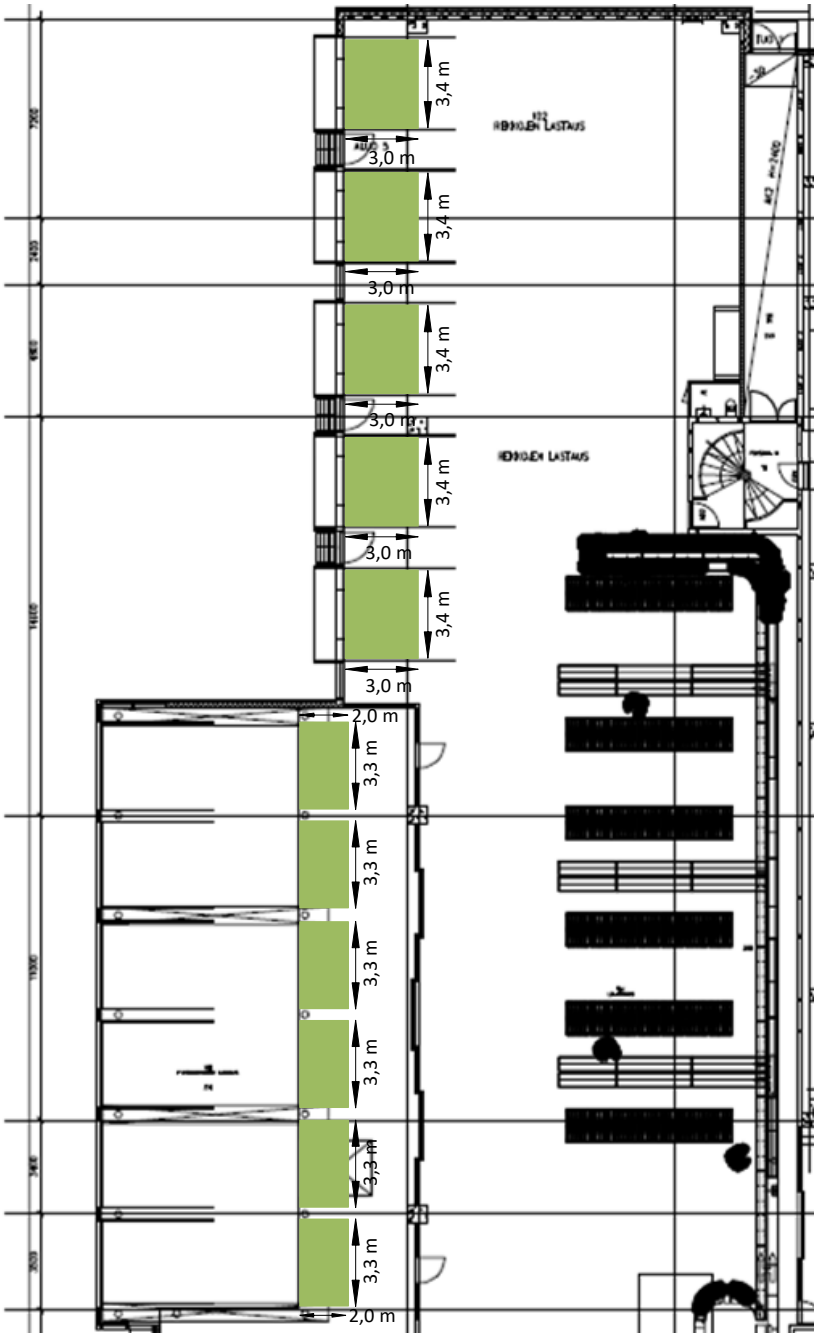
5 235 x 20 mm

6 235 x 10 mm

7 7 x 2 x 40 mm

Lukualueiden sijainnit lastauslaitureilla

Lastauslaituri 1: Lukualueita 11 kpl. Lukualueiden korkeus 2,5 m.



Lastauslaituri 2: Lukualueita 3 kpl. Lukualueiden korkeus 2,5 m.

Laitteiston kustannuksia eri toimittajilta

Finn-ID				
	Malli	Yksikköhinta	Lukumäärä	Kokonaishinta
Pysyvä tunniste	Confidex Carrier Pro	0,59 €	100000	59 000,00 €
Lastauslaiturin lukija	Impinj Speedway Revolution R420	1 821,30 €	14	25 498,20 €
Lastauslaiturin antenni	Kathrein WRA-7070	202,00 €	56	11 312,00 €
Kuljetushihnan lukija	Impinj Speedway Revolution R120	966,70 €	2	1 933,40 €
Kuljetushihnan antenni	Kathrein WRA-6060	225,00 €	2	450,00 €
RFID-tulostin	Zebra ZT410	3 235,00 €	10	32 350,00 €
Cisper				
	Malli	Yksikköhinta	Lukumäärä	Kokonaishinta
Pysyvä tunniste	Confidex Carrier Pro	0,36 €	100000	36 250,00 €
Lastauslaiturin lukija	Impinj Speedway Revolution R420	1 477,00 €	14	20 678,00 €
Lastauslaiturin antenni	Kathrein WRA 7070	120,00 €	56	6 720,00 €
Kuljetushihnan lukija	Impinj Speedway Revolution R120	741,00 €	2	1 482,00 €
Kuljetushihnan antenni	Kathrein WRA 6060	138,00 €	2	276,00 €
Lukijan virtalähde	Impinj Universal Power Supply	70,00 €	16	1 120,00 €
Antennikaapeli	Kathrein R-AC 10 TNC-TNCR	43,45 €	58	2 520,10 €
RFID-tulostin	Zebra ZT410	4 165,00 €	10	41 650,00 €
Kertakäyttöinen tunniste	Confidex Crosswave Classic 4x6" M4E	0,20 €	280000	56 000,00 €
CoreRFID				
	Malli	Yksikköhinta	Lukumäärä	Kokonaishinta
Pysyvä tunniste	Confidex Carrier Pro	0,76 €	100000	76 000,00 €
Lastauslaiturin lukija	Impinj Speedway Revolution R420 + Power Supply	1 537,02 €	14	21 518,28 €

Lastauslaiturin antenni	Kathrein WRA-7070	193,59 €	56	10 841,04 €
Kuljetushihnan lukija	Impinj Speedway Revolution R220 + Power Supply	1 220,23 €	2	2 440,46 €
Kuljetushihnan antenni	Impinj Mini-Guardrail	287,46 €	2	574,92 €
therfidstore				
	Malli	Yksikköhinta	Lukumäärä	Kokonaishinta
Tunniste	Omni-ID IQ 800P	0,56 €	100000	56 000,00 €
Lastauslaiturin lukija	Impinj Speedway Revolution R420 + Power Supply	1 075,00 €	14	15 050,00 €
Lastauslaiturin antenni	Advantenna-SP12	152,00 €	56	8 512,00 €
Kuljetushihnan lukija	Impinj Speedway Revolution R120 + Power Supply	680,00 €	2	1 360,00 €
Kuljetushihnan antenni	Kathrein RFID MIRA 100	126,00 €	2	252,00 €
Päätelaitteet				
Lastauslaiturin päätelaite Gigantti1	Samsung Galaxy Tab A 10,1 WiFi 32 GB	219,00 €	14	3 066,00 €
Lastauslaiturin päätelaite Gigantti2	iPad Air 2 32 GB WiFi	349,00 €	14	4 886,00 €
Lastauslaiturin päätelaitteen teline PadSolutions	PadBuddy Wall	159,00 €	14	2 226,00 €
Lastauslaiturin päätelaitteen teline Jimm's	Vogel's PTS 1214 Tab-Lock	143,90 €	14	2 014,60 €