KARELIA-AMMATTIKORKEAKOULU
sähkötekniikan koulutusohjelma

Markus Jurvanen

TOIMITILATURVALLISUUSLABORATORION PÄIVITYS

Opinnäytetyö
Toukokuu 2016

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Toukokuu 2016** **Sähkötekniikan koulutusohjelma** Karjalankatu 3 80200 JOENSUU p. 013 260 6800

Tekijä
Markus Jurvanen

Nimeke
Toimitilaturvallisuuslaboratorion päivitys

Toimeksiantaja
Karelia ammattikorkeakoulu

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli päivityssuunnitelman laatia Karelia ammattikorkeakoulun toimitilaturvallisuuden laboratorioon. Päivityksen yhteydessä laboratorio muutti uusiin tiloihin.

Lähtökohta suunnittelulle oli integraation toteuttaminen järjestelmien välille. Toisena lähtökohtana olivat päivityksen kustannustehokas toteuttaminen. Suunnitelmat käsittävät laitemäärittelyt, sijoituskuvat, kaapelointikuvat sekä kytkentäkuvat. Suunnitelmissa pyrittiin huomioimaan oikeaoppiset sijoittelut kenttälaitteille, kun se opetustilojen puitteissa oli mahdollista.

Suunnittelun tuloksena toimitilaturvallisuuslaboratorion laitteisto päivitettiin rikosilmoitin-, kulunvalvonta- ja kameravalvontajärjestelmän osalta. Suunnitelmaa varten luodut kytkentäkuvat ja kaaviot lisättiin järjestelmien dokumentaatioitten yhteyteen helpottamaan laitteistojen käyttöä.

Kieli	Sivuja 57
suomi	Liitteet 4

Asiasanat
toimitilaturvallisuus, kameravalvonta, kulunvalvonta, rikosilmoitin

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
May 2016
Degree programme in electrical engineerin

Karjalankatu 3
80200 JOENSUU
FINLAND
p. 013 260 6800

Author
Markus Jurvanen

Title
Update of Office Security Laboratory

Commissioned by
Karelia University Of Applied Sciences

Abstract

The aim of this thesis was to create an updateplan for office security laboratory of Karelia University Of Applied Sciences. The laboratory moved to new premises in connection with the update.

The basis of planning was to create integration between different security systems. Another basis was cost-effective execution of the update. The Plans include equipment specifications, equipment position pictures and coupling pictures. The aim was to ensure as correct positions for the equipment as possible in the teaching environment.

The burglar alarm system, access control system and CCTV system of the office security laboratory were updated as the result of the planning. The documents of systems were included in the systems documentation to simplify the use of the systems.

Language
Finnish

Pages 57
Appendices 4

Keywords
office security, CCTV, acces control, burglar alarm

Sisältö

1 Johdanto

Tämän työn tarkoituksena oli suunnitella Karelia-ammattikorkeakoulun tilaturvallisuuslaboratorion päivitys murto-, kulun- ja kameravalvonnan osalta. Lisäksi edellä mainittujen järjestelmien integroinnin suunnittelu oli myös osa opinnäytetyötä. Suunnittelun yhteydessä perehdyin edellä mainittujen järjestelmien suunnitteluprosessiin, jota myös kuvataan opinnäytetyössä. Lisäksi perehdyin suunnittelun kannalta olennaisiin seikkoihin, kuten laitteistojen sijoitteluun ja oikeiden kenttälaitteiden valintaan. Koska lainsäädäntö on olennainen osa etenkin kulun- ja kameravalvontaa niin myös lakeihin perehtyminen kuului opinnäytetyöhön.

Järjestelmien päivityksen lisäksi pyrin parantamaan niiden dokumentaatiota. Tavoitteena oli, että päivitetty kokonaisuus olisi helpommin ymmärrettävissä niin kaapeloinnin, kytkentöjen ja toiminnankin osalta. Olen pyrkinyt suunnittelussa vähentämään laitteiden välisiä kytkentäpisteitä, jolla saavutetaan selkeämpi fyysinen rakenne järjestelmälle.

Vanhoista järjestelmistä on yritetty hyödyntää mahdollisimman paljon olemassa olevia laitteita, jolloin päivityksen kustannukset saataisiin pidettyä mahdollisimman alhaisina. Suurimmat muutokset päivityksessä olivat ohjelmisto- ja lisenssipäivitykset.

Turvatekniikka kehittyy nopeasti. Markkinoille tuodaan entistä älykkäämpiä ja monipuolisimpia järjestelmiä, joiden avulla voidaan tuottaa huomattavaa lisäarvoa järjestelmien haltijoille. Koska järjestelmät kehittyvät nopeasti, on tärkeää että, opiskelijoiden käytössä olevat demojärjestelmät ovat nykyaikaisia. Nykyaikaiset järjestelmät helpottavat opiskelijoiden siirtymistä työelämään, jossa suunniteltavat järjestelmät ovat nykyaikaisia.

Toimeksiantoon tarve tuli Karelia ammattikorkeakoululta, kun toimitilaturvallisuuslaboratorio siirrettiin uusiin isompiin tiloihin. Kiinnostuin aiheesta, koska koen kyseisiin järjestelmiin tutustumisesta olevan apua työssäni turvallisuusalalla.

2 Turvatekniikka

Turvatekniikka kehittyy nopeasti. Ihmiset ja yritykset ovat entistä kiinnostuneempia erilaisiin elektronisiin turvallisuusratkaisuihin. Enää pelkkä mekaaninen lukitus ei riitä kaikille täyttämään käsitystä turvallisuudesta.

Turvatekniikkaa käytetään lähes poikkeuksetta jokaisessa paikassa, missä on ihmisiä. Turvatekniikalla pyritään helpottamaan turvallisen toimintaympäristön luomista, niin ettei siihen tarvita paljon henkilöstöresursseja. Teknisten valvontalaitteiden avulla esimerkiksi valvomossa työskentelevä henkilö pystyy valvomaan tapahtumia lukuisista kohteista, jotka voivat sijaita kaukana toisistaan. Kohteesta riippuen turvateknisillä järjestelmillä voi olla hyvinkin paljon toisistaan poikkeavia tehtäviä. Suunniteltaessa kohdetta, täytyy tarkalleen tietää, minkälaiseen käyttöön turvatekniikkaa ollaan hankkimassa. Tällöin tärkeää on, että suunnittelija ja työn tilaaja tekevät tiivistä yhteistyötä.

Turvatekniikan avulla suojellaan niin omaisuutta kuin ihmisiäkin. Turvatekniikan avulla voidaan toteuttaa seurantaa ja analysointia. Turvatekniikka käsittää muun muassa murto-, kulun- ja kameravalvonnan sekä paloturvallisuuteen liittyvät valvontajärjestelmät. Nykypäivänä on yleistä yhdistellä eli integroida edellä mainittuja järjestelmiä siten, että käyttäjä pystyy esimerkiksi samalla ohjelmistolla hallitsemaan koko kiinteistön turvatekniikkaa. Integraation avulla järjestelmät täydentävät toisiaan, jolloin ympäristöstä tulee entistä turvallisempi.

2.1 Lait, asetukset, määräykset ja ohjeet

Turvajärjestelmien suunnittelijan on tärkeää olla tietoinen laeista ja asetuksista, jotka liittyvät suunniteltavaan järjestelmään. Rikosilmoitin-, kulunvalvonta- ja kameravalvontajärjestelmät ovat kaikki teknisiä valvontajärjestelmiä, joiden asennusta ja käyttöä määrittelee seuraavanlaiset lait:

- Yksityisyyden, rauhan ja kunnian loukkaaminen 1.10.2000
- Henkilötietolaki 1.12.2000

- Laki yksityisyyden suojasta työelämässä 1.10.2004. [1,11.]

Lait koskevat etenkin kulunvalvonta- ja kameravalvontajärjestelmiä, joissa kerätään tietoa ihmisten liikkeistä valvottavissa kohteissa. Vaikka turvallisuusjärjestelmiä asentavan yrityksen on hyvä olla tietoinen järjestelmiä koskevista laeista ja asetuksista, niin vastuu lainmukaisesta käytöstä on yleensä laitteiston haltijalla.

Edellä mainitut lait määrittelevät teknisten turvajärjestelmien asennusta ja käyttöä. Näiden lisäksi on olemassa laki yksityisistä turvapalveluista, joka vaikuttaa suoraan kaikkiin turvallisuusalalla toimiviin henkilöihin, eli myös suunnittelijoihin. Laissa käsitellään turvasuojausta. Turvasuojauksella tarkoitetaan tehtäviä, joissa suunnitellaan, asennetaan tai muutetaan kohteen rakenteellista tai teknisin keinoin toteutettua suojausta. Turvasuojaaja on näitä toimenpiteitä suorittava henkilö. Laki määrittelee turvasuojaajaksi hyväksymisen edellytykset. Turvasuojaajalla on salassapitovelvollisuus suojaustehtäviinsä liittyen, joka säilyy myös tehtävien päätyttyä. [1, 12-13.]

2.2 Turvasuunnitelma

Ennen teknisten ratkaisujen suunnittelua, toteutettavaan kohteeseen on hyvä tehdä turvasuunnitelma. Turvasuunnitelmassa pohditaan, yhdessä kohteessa toimivan henkilöstön kanssa, seuraavanlaisia asioita:

- riskit joihin turvatekniikalla halutaan vaikuttaa
- tekijät kohteen sisällä, jotka vaikuttavat turvallisuuteen
- tavoitteet joihin turvateknisin ratkaisuin halutaan päästä
- ulkopuolelta tulevat määräykset ja vaatimukset, jotka järjestelmien pitää täyttää
- käytössä oleva budjetti. [2, 22-23.]

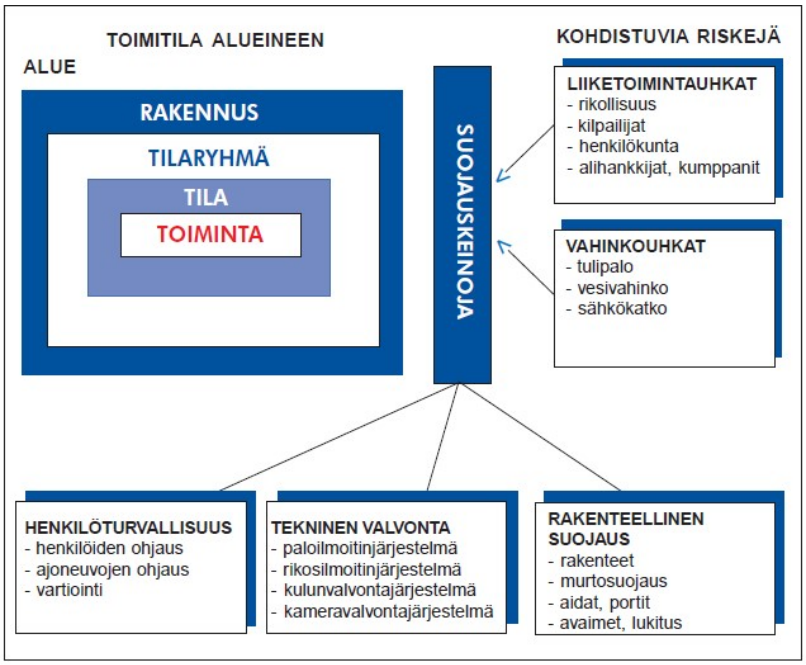
Henkilöstön turvallisuus, toimintaan ja prosesseihin liittyvät riskit, omaisuuden ja tietojen suojeleminen sekä ympäristöön liittyvät seikat ovat oleellisimpia riskejä, joihin turvatekniikalla voidaan vaikuttaa. Kun edellä mainittuja asioita otetaan huomioon, turvataan myös yrityksen mainetta. [3,1.]

Turvasuunnitelmassa kannattaa ottaa huomioon kohteen sijainti. Henkilökunnan määrä ja alueet, joilla he liikkuvat eri vuorokauden aikoina ovat yksi osatekijä, joka vaikuttaa toimitilaturvallisuuteen. Ulkopuolisten vieraitten ja esimerkiksi tavarantoimittajien toiminta alueella on otettava huomioon tehtäessä suunnitelmaa. Aina kun suojattavissa tiloissa liikkuu muuta kuin henkilökuntaa on varmistuttava siitä, että järjestelmiä ei päästä manipuloimaan siten, että niiden toiminta häiriintyy. [2, 23-24.]

Kohteesta riippuen sille on voitu jo lain tai määräysten puitteissa antaa turvallisuuteen liittyviä vaatimuksia, jotka tulee täyttää. Esimerkiksi palo- ja poistumisturvallisuuteen liittyvät määräykset on asetettu laissa. Finanssialan keskusliitto(FK) on antanut omia määräyksiään toimitilaturvallisuuteen liittyen. FK on julkaissut sivuillaan ohjeita ja määritellyt turvajärjestelmiä. [1, 14-19.]

Toimitilaturvallisuus on käsite, joka pitää sisällään sähköiset turvallisuusjärjestelmät, rakenteellisen turvallisuuden ja henkilöturvallisuuden. Tässä työssä keskitytään lähinnä sähköisiin turvajärjestelmiin osana toimitilaturvallisuutta. Sähköisillä turvajärjestelmillä pyritään suojaamaan omaisuutta, ihmisiä ja tietoja. Toimitilaturvallisuus on osa yritysturvallisuutta. [3, 3-4.]

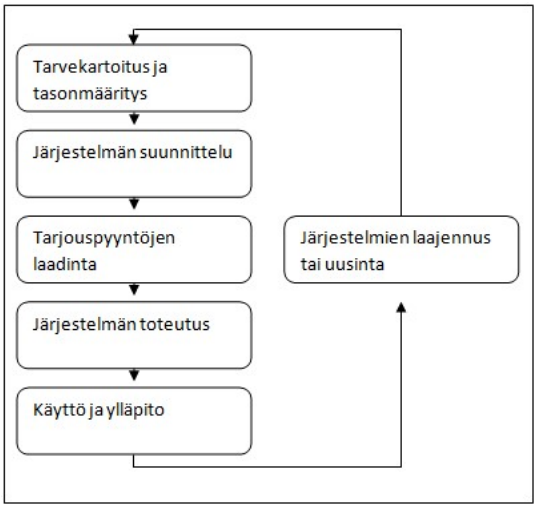
Toimitilaturvallisuuden avulla turvataan yritykselle häiriötön liiketoiminta. Kuvassa 1 näytetään, minkälaisia riskejä toimitilaan kohdistuu, sekä esitellään suojauskeinot riskejä vastaan.



Kuva 1. Toimitilaturvallisuus [3,3].

2.3 Turvallisuusjärjestelmän toteutus

Turvallisuusjärjestelmän hankkiminen toimitilaan on monivaiheinen projekti. Riippumatta kohteen koosta tai turvallisuusvaatimuksista vaiheet ovat yleensä hyvin samankaltaiset. Toteutuksen rakenne on usein kuvan 2 kaltainen:



Kuva 2. Toteutuksen vaiheet [3, 8-9].

Vaikka toteutuksen rakenne on hyvin monesti samankaltainen, siihen liittyvien toimijoitten määrä vaihtelee huomattavasti kohteen koosta riippuen. Pienimmillään projektissa on mu-

kana vain järjestelmätoimittaja ja tilaaja, jotka hoitavat yllä olevan ketjun vaiheet kokonaisuudessaan.

2.3.1 Tarvekartoitus ja tasonmääritys

Turvajärjestelmän hankkiminen on hankinta siinä missä muutkin yrityksen hankinnat. Lähtökohtaisesti tulisi miettiä, että mitä lisäarvoa yritysturvallisuuteen hankittava laitteisto antaa. Hyvä lähtökohta tarpeen määrittämiselle on järjestelmän tarkoituksenmukaisuuden arviointi ja kuinka se toimii yhdessä muitten yritysturvallisuuteen liittyvien järjestelmien kanssa, niin ettei se ole yli- tai alimitoitettu suhteessa muihin järjestelmiin. Kohteen koosta riippumatta onnistunut järjestelmän hankinta edellyttää ennalta mietittyjä toimintatapoja projektin läpiviemiseen. Hankkeella on myös tärkeää olla avainhenkilö, joka vie projektia eteenpäin ja koordinoi eri toimijoiden yhteistyötä. [3,8.]

Yksinkertaisimmillaan tarvekartoitus voidaan toteuttaa selvittämällä yrityksen nykyinen turvallisuustaso ja sen pohjalta määritellään haluttu turvallisuustaso ja päätetään keinot joilla tasolle päästään. Edellä mainittu yksinkertainen tarvekartoituksen toteutus on käyttökelpoinen tilanteessa jossa päivitetään tai laajennetaan jo olemassa olevia järjestelmiä tai tapauskohtaisesti myös laajuudeltaan pienissä järjestelmissä. Muussa tapauksessa tarvekartoitukseen tehdään laajempi selvitys, jossa tehdään seuraavanlainen selvitystyö:

1. Uhkakartoitus
2. Riskianalyysi
3. Riskinhallinta
4. Tarvekartoitus. [3,9.]

Selvitystyössä lähdetään liikkeelle yrityksen tai organisaation mahdollisista uhkista eli tehdään uhkakartoitus. Uhkakartoituksessa tunnistetaan yritystä tai organisaatiota vaarantavia uhkia. Uhkakartoituksessa on yleistä että mahdollisia uhkia löytyy paljon. Todetut uhkat kannattaa luetteloida, jolloin samoja uhkia ei tunnisteta useaan kertaan. Uhkien tunnistamisen jälkeen täytyy arvioida uhkat ja priorisoida niistä ne jotka ovat todennäköisiä vaarantamaan yrityksen tai organisaation toimintaa. Mahdollisia uhkia voivat olla esimerkiksi:

murtautuminen toimitiloihin, tulipalo, ilkivalta, yritysvakoilu tai sabotaasi. Näitten valikoitujen uhkien kanssa jatketaan riskianalyysiin. [3, 8.]

On luontevaa että riskianalyysin toteuttaa sama työryhmä, joka on aikaisemmin tehnyt kohteeseen uhkakartoituksen. Riskikartoituksessa yksinkertaisesti selvitetään millaisia riskejä uhkat aiheuttavat yrityksen tai organisaation omaisuudelle, henkilöstölle, liiketoiminnalle tai ympäristölle. Riskikartoituksessa voidaankin tehdä taulukko, jonka avulla saadaan selkeä kuva uhkista ja niihin liittyvistä riskeistä. Taulukossa 1 on yksinkertainen esimerkkikuvaus taulukosta, jossa pystyriveillä on valikoidut uhkat ja vaakarivillä kohteet joihin uhkat vaikuttavat. Taulukkoon merkitään uhkan vaikutus kohteeseen, vakavuus ja todennäköisyys, asteikolla 1-4, jossa 1 on vähäinen ja 4 erittäin suuri. [3,8; 4.]

Taulukko 1 Riskianalyysi [5,3].

Uhkat/Kohde	Henkilöstö	Liiketoiminta	Ympäristö
Murto	3	4	1
Palo	4	4	3
Ilkivalta	1	2	4
Vakoilu	1	3	1
Sabotaasi	1	4	1

Riskianalyysin avulla saadaan rajattua ne yrityksen kohteet joihin tarvitaan suojausta tiettyjä uhkia vastaan. Keinot joilla uhkia vastaan suojaudutaan suunnitellaan selvityksen seuraavassa vaiheessa eli riskinhallinnassa.

Riskienhallinta yrityksessä tai organisaatiossa on toimintaa, jolla pyritään estämään tai vähentämään riskeistä johtuvien vahinkojen laajuutta ja vakavuutta. Eli toimitilaturvallisuuden tapauksessa riskienhallinta tarkoittaa toimia siinä tilanteessa, kun aikaisemmin mainituista riskeistä murto, palo, ilkivalta, vakoilu tai sabotaasi tulee totta. Hyvä riskienhallinta on etupainotteista, eli toimenpiteet vahinkotilanteissa on ennalta suunniteltuja ja niihin on varauduttu. Toimitilaturvallisuudessa tämä tarkoittaa esimerkiksi murtohälytinjärjestelmän ja kameravalvontajärjestelmän hankkimista. Järjestelmien hankkimisen lisäksi riskienhallinnassa täytyy suunnitella toimenpiteet, joita tehdään kun jokin asennetuista järjestelmistä antaa hälytyksen. Tarkoitus on vahinkojen vaikutusten rajaaminen. Esimerkiksi vartiointi-

liikkeen nopea paikalle tulo vähentää merkittävästi vahinkoa yrityksessä tai organisaatiossa. Toimitilaturvallisuuden riskienhallinnassa suunnitellut toimenpiteet vaativat yleensä turvallisuusjärjestelmiä. Riskienhallinnan suunnittelun tuloksena syntyneitten järjestelmätarpeiden johdosta päästään itse tarvekartoitukseen, jossa tehdään suunnitelmat hankittavista järjestelmistä. [6.]

Tarvekartoituksessa selvitetään, minkälaisia turvallisuustarpeita yrityksellä on tai toisaalta määritteleekö jokin ulkopuolinen taho vaadittavia ratkaisuja hankittavaksi. Tarvekartoitus tehdään tilakohtaisesti, eli käydään yksityiskohtaisesti jokainen toimitilan huone läpi, koska erilaisilla huonetiloilla voi olla toisistaan poikkeavia vaatimuksia tai tarpeita. [3,8.]

Apuna tarvekartoituksessa voidaan käyttää ulkopuolisten toimijoiden tekemiä turvallisuuden tasomääritelmiä, joissa on kerrottu vaadittavat turvajärjestelmät tasokohtaisesti. Tasomääritelmiä ovat julkaisseet esimerkiksi Sähköinfo Oy teoksessaan ”ST 603.17 Tietoturvallisuuden tasoluokitusohje, toimitilat” ja Finanssialan Keskusliitto julkaisussaan ”Murtohälytysjärjestelmät ja - palvelut ohje 2008”, jossa on määritelty murtohälytysjärjestelmän ominaisuuksia kohteeseen suojaustasosta riippuen. Suojaustasot on yleensä jaettu neljään luokkaan. Joissa alhaisinta suojaustasoa kuvataan numerolla yksi ja korkeinta numerolla neljä. Taulukossa 2 on Finanssialan Keskusliiton laatima tasoluokitus murtohälytinjärjestelmistä.

Taulukko 2. Murtohälytysjärjestelmien luokitus [7,5].

kohteen suojaustaso	taso 4	taso 3	taso 2	taso 1
valvontatapa	ovet, aukot ja ikkunat sekä tila ja kohdevalvonta	ovet, aukot ja ikkunat sekä tila ja kohdevalvonta	ovet ja tila, kohdevalvonta tarpeen mukaan	ovet ja ikkunat tai tila
keskus ja ilmaisimet	4-luokka tai 3-luokka	3-luokka	2-luokka	1-luokka
radioteitse toimivat ilmaisimet	ei sallita	ainoastaan kohdevalvontaan ja henkilökohtaiset hälytyspainikkeet	sallitaan	sallitaan
savuilmaisimet	suositellaan paloilmoitinjärjestelmää	suositellaan paloilmoitinjärjestelmää	suositellaan	suositellaan
ilmoituksen-siirto	valvottu yhteys ja kaksi paikallishälytintä	valvottu yhteys ja paikallishälytin tai kahdennettu ilmoituksensiirto ja paikallishälytin	robottipuhelin ja paikallishälytin tai radiotaajuinen siirto ja paikallishälytin	robottipuhelin tai radiotaajuinen siirto ja paikallishälytin
siirrettävät tiedot	murto, päälle/pois, ryöstö, sabotaasi, vikatila	murto, päälle/pois, ryöstö, sabotaasi, vikatila	murto, päälle/pois, sabotaasi, vikatila	murto, sabotaasi
ilmoituksen vastaanotto	hätäkeskus tai FK:n hyväksymä vartioimisliikkeen hälytyskeskus	*ensisijainen ilmoituksensiirto* FK:n hyväksymä vartioimisliikkeen hälytyskeskus	24h miehitetty vartioimisliike	vartioimisliike tai kotinumerot
kohteeseen hälytettävät	poliisi ja kohdekoulutuksen saanut vartija	kohdekoulutuksen saanut vartija	vartija	vartija tai yksityishenkilöt
asennus	FK:n hyväksymä asennusliike	FK:n hyväksymä asennusliike	FK:n hyväksymä asennusliike	
käyttö	henkilökohtainen tunniste ja henkilökohtainen koodi, väh. 4 merkkiä	henkilökohtainen koodi, väh. 4 merkkiä	henkilökohtainen koodi	avain, tunniste tai koodi
käyttäjän ylläpitotoimet	käyttäjien henkilökohtaisten koodien täsmäytys kuukausittain. Järjestelmän ja ilmoituksensiirron kokeilu kuukausittain.	käyttäjien henkilökohtaisten koodien täsmäytys 4 kertaa vuodessa. Järjestelmän ja ilmoituksensiirron kokeilu 4 kertaa vuodessa.	käyttäjien henkilökohtaisten koodien täsmäytys kerran vuodessa. Järjestelmän ja ilmoituksensiirron kokeilu kaksi kertaa vuodessa.	tarvittaessa
huolto	vähintään kerran vuodessa	vähintään kerran vuodessa	vähintään joka toinen vuosi	tarvittaessa
palvelun toimivuuden testaus	vähintään kerran vuodessa	vähintään kerran vuodessa	tarvittaessa	tarvittaessa

Tarvekartoituksessa on huomattava että laitteistolle on määritelmät miten niiden täytyy toimia, mutta laitevalmistajaa tai merkkiä ei ole määritelty vaan laitemäärittely jää turvalaitesuunnittelijan tai laitetoimittajan mietittäväksi. On tosin mahdollista, että yrityksellä on määritelty laitteistot, joita käytetään, jolloin tarvekartoituksen jälkeen suunnittelijan täytyy vain suunnitella kenttälaitteiden sijoitukset.

2.3.2 Suunnittelu

Teknisten turvallisuusjärjestelmien suunnittelu voidaan toteuttaa kohteesta riippuen joko muun sähkösuunnittelun yhteydessä, jos kohteeseen riittää perustason suojaus, tai erillisenä suunnittelutyönä, jos kohde vaatii turvalaitteistolta erityisiä ominaisuuksia. Kohteissa, joissa turvallisuusjärjestelmät ovat olennainen osa riskienhallintaa, kannattaa järjestelmien suunnittelutyö tehdä erillisenä työnä valvontalaitteiden kanssa toimivien tai niihin perehtyneiden yritysten kanssa.

Jos valvontajärjestelmiä suunnitellaan uuteen rakenteilla olevaan kiinteistöön, joutuu turvasuunnittelija tekemään yhteistyötä muitten suunnittelijoiden kanssa, kuten arkkitehdin, sähkö- ja lvi-suunnittelijan kanssa. Arkkitehtisuunnittelija vastaa tilojen ja kalusteiden suunnittelusta. Yhteistyö arkkitehtisuunnitelian kanssa on tärkeää, koska turvallisuusjärjestelmien halutunlaisen toiminnan kannalta on tärkeää, että kalusteista ja muista rakenteista johtuvat katvealueet saadaan poistettua. [3, 10.]

Sähkösuunnittelijan kanssa sovitaan järjestelmän kaapeloinneista, kaapelityypeistä, sähkönsyötöistä ja esimerkiksi tietoliikenneyhteyksien kaapeloinneista. Kameravalvontaa suunnitellessa myös valaistukseen liittyvät asiat käydään läpi sähkösuunnittelijan kanssa. Yhteistyö sähkösuunnittelijan kanssa on kustannustehokkaan lopputuloksen kannalta tärkeää, kun turvalaitekaapelit saadaan vietyä samalla muitten kiinteistön kaapeleiden kanssa. Ja toisaalta kerralla onnistunut kaapelointi vähentää lisätyötä projektin loppuvaiheessa. [3, 10.]

LVI-suunnittelijan kanssa voidaan tarkastella esimerkiksi ilmanvaihto laitteiden sijoituksia kiinteistössä. Näillä on merkitystä etenkin paloilmaisimien sijoittelun kannalta. Lisäksi eri-

laisia lvi-hälytyksiä, kuten vesivahinkohälytys, voidaan liittää hälytin- tai kulunvalvontajärjestelmän piiriin. [3,10.]

Suunnittelussa olennaista on, että halutut ominaisuudet on määritelty mahdollisimman yksiselitteisesti. Yksiselitteisyys on tärkeää erityisesti siksi, että tällöin kilpailevien tarjousten vertailu on helpompaa, kun tarjouspyyntöasiakirjoissa ei ole tulkinnan varaa. On myös mahdollista tehdä suunnitelma, jossa on määritelty laitteisto ja ohjelmistot, sekä luettelo tarvittavista tuotteista. Tällöin turvaurakoitsijan tehtäväksi jää miettiä asennukseen ja käyttöönottoon tarvittavat resurssit. Muussa tapauksessa turvaurakoitsija käyttää parhaiten suunnitelmaan sopivaa laitteistoa. Käyttöönoton ja opastuksen laajuus on myös hyvä määrittää suunnittelussa. [3, 12.]

Järjestelmistä tehdään seuraavanlaiset asiakirjat:

- sähköselostus, jossa käy ilmi turvajärjestelmien toiminta
- sijoituskuvat, joista voidaan määritellä kappalemäärät esimerkiksi kameroille, liiketunnistimille tai kulunvalvonta päätteille
- johtokaaviot
- mahdollinen laiteluettelo, jos suunnitelmassa on määritelty laitteisto
- urakkarajaliite. [3,12.]

Turvajärjestelmiin liittyvien asiakirjojen säilytyksestä sovitaan tilaajan kanssa etukäteen. Koska asiakirjoista löytyy tarkkoja tietoja laitteistoista ja niiden toiminnasta, on tärkeää, että asiakirjojen käsittely on ennalta sovittua. Tämä tarkoittaa toimia asiakirjojen säilytyksestä, sekä ylimääräisten kopioitten tuhoamisesta. [3,13.]

2.3.3 Toteutus ja käyttöönotto

Suunnitelmien pohjalta kilpailutetaan yritykset. Hankkeen toteutukseen tarvitaan mahdollisesti lueteltuja toimijoita:

- rakennusurakoitsija
- ovitoimittaja
- lukkourakoitsija
- sähköurakoitsija

- turvalaiteasentaja ja laitetoimittaja. [3, 9.]

Rakennusurakoitsijaa ja ovitoimittajaa tarvitaan, jos kohteeseen täytyy tehdä rakenteellisia muutoksia, eli rakentaa tai muokata rakennuksen rakenteita tai asentaa uusia ovia. On myös mahdollista, että pelkästään yksi toimija hoitaa koko toteutuksen. Näin menetellään pienissä kohteissa. On kuitenkin yleistä, että sähköurakoitsija toteuttaa kaapeloinnin, johon turvalaiteasentaja ja lukkourakoitsija asentaa laitteistonsa. Yksi mahdollisuus on myös sopia, että turvalaitteet asentava urakoitsija ottaa koko projektin hoitaakseen, eli toimii pääurakoitsijana. Pääurakoitsija hankkii tarvittavat aliurakoitsijat ja hoitaa yhteydenpidon tilaajan ja urakoitsijoitten välissä, sekä vastaa tilaajalle aliurakoitsijoitten toiminnasta. [3, 13.]

Turvajärjestelmää hankittaessa turva- ja lukkourakoitsijan pätevyys työn suorittamiseen on tarkastettava. On huomioitava, että projektin kanssa tekemisissä olevilla henkilöillä täytyy olla turvasuojaajakortti. Tarvittaessa urakoitsijoita tai heidän edustajiaan voidaan vaatia allekirjoittamaan erillinen vaitiolovelvollisuuslomake tai heistä voidaan pyytää erillinen turvallisuusselvitys. [1,12; 8,26.]

Toteutuksen seurantaan tilaajan kannattaa hankkia ulkopuolinen valvoja, jolla on asiantuntemusta turvaurakoista. Toteutuksen aikana on järkevää pitää kokouksia, joissa käydään läpi projektin etenemistä ja mahdollisia muutoksia tai eteen tulleita arvaamattomia tilanteita. Etenkin, jos muutoksilla on taloudellisia vaikutuksia, täytyy miettiä ketä näistä lisätöistä laskutetaan. Myös työn laatua tulee seurata koko projektin ajan aktiivisesti. [3,13.]

Turvalaitteiston toimittajaa tai asentajaa valittaessa kannattaa kiinnittää huomiota siihen millainen käyttöönottokoulutus urakkaan sisältyy. Järjestelmien tehokas käyttö edellyttää osaavaa käyttäjäkuntaa, joten käyttökoulutus on välttämätön. On myös mahdollista ulkoistaa järjestelmien käyttö ja ylläpito turvalaiteet asentavalle yritykselle tai kolmannelle osapuolelle. Tästä yritys yleensä veloittaa kiinteää kuukausimaksua, johon sisältyy ennalta sovittuja toimenpiteitä. [3,14]

2.3.4 Käyttö ja ylläpito

Järjestelmien vertailussa kannattaa kiinnittää huomiota käytön ja ylläpidon kustannuksiin. On otettava huomioon laitteiston realistinen käyttöikä ja arvioida kuinka paljon kustannuk-

sia ylläpitoon ja huoltoon kuluu vuosittain. Luonnollisesti käyttöikä, sekä huolto- ja ylläpitokustannukset on otettava huomioon eri järjestelmiä vertailtaessa. On myös selvitettävä miten huolto tullaan hoitamaan, esimerkiksi huollon vasteaika. Vasteajalla tarkoitetaan aikaa huoltotilauksesta siihen, kun huoltotyö suoritetaan. [3,14.]

Käytöstä aiheutuvia kustannuksia ovat muun muassa:

- ohjelmistojen lisenssimaksut
- tukipalvelut
- hälytysten ja muun informaatio siirtämisestä aiheutuvat kustannukset
- henkilökunnan kouluttaminen

On myös arvioitava, kuinka paljon työaikaa järjestelmien käyttö vie, vai täytyykö tehtävään palkata täysipäiväinen henkilö. [3,14.]

3 Toimitilaturvallisuuden järjestelmät

3.1 Rikosilmoitinjärjestelmän toimintaperiaate ja rakenne

Rikosilmoitinjärjestelmän tarkoituksena on toimia yhdessä rakenteellisen murtosuojauksen kanssa murtautumista vaikeuttavana järjestelmänä. Rikosilmoitinjärjestelmän olemassa ololla on ennaltaehkäisevä vaikutus. Tunkeutumistilanteessa rikosilmoittimella saadaan välitettyä tietoa haluttuun kohteeseen, jolloin murtautumisesta aiheutuvat vahingot minimoidaan, kun niihin pystytään reagoimaan välittömästi. [9,2.]

Rikosilmoitinjärjestelmä koostuu keskuslaitteesta, käyttölaitteista, ilmaisimista, paikallishälyttimistä, siirtolaitteista ja teholähteestä. Keskuslaitteessa sijaitsee järjestelmän ohjelmisto ja liitännät muille laitteille. Keskuslaitteisto asennetaan koteloon, jossa on kansisuojaukset niin, että kantta ei pystytä luvattomasti avaamaan ilman hälytystä. Yleensä samaan koteloon sijoitetaan myös järjestelmän akku ja virtalähde. Yleisesti ottaen keskuslaitteet voidaan jaotella kolmeen eri ryhmään riippuen siitä, kuinka ilmaisimet on liitetty järjestelmään. Ilmaisimet kytketään keskukseen joko silmukka- tai väyläperiaatteella. Joissain kohteissa on myös sallittua, että ilmaisimet ovat yhteydessä keskukseen langattomasti, jolloin kyseessä on langaton järjestelmä. [9,2.]

Langattomat ilmaisimet keskustelevat keskuksen kanssa radiotaajuuksilla. Langattomia ilmaisimia voidaan käyttää kohteissa joissa on suojausluokka yksi tai kaksi, sekä kohdevalvontaan luokan kolme järjestelmissä. [7,5.]

Rikosilmoitinjärjestelmän käyttölaitteet ovat laitteita, joilla suoritetaan järjestelmän päälle- ja poiskytkennät sekä luetaan järjestelmän lokia. Käyttölaitteelta voidaan ohjelmoida järjestelmää. Käyttölaite keskustelee keskuslaitteen kanssa väylää pitkin. Käyttölaitteita voi olla järjestelmässä useampia, riippuen järjestelmän ominaisuuksista. Yleensä käyttölaitteet sijoitetaan niihin sisäänkäynteihin, joista kulku kohteeseen tapahtuu. [7,5.]

Hälytysjärjestelmän siirtolaitteella siirretään määriteltyjä tietoja eteenpäin esimerkiksi vartiointiliikkeelle tai poliisille. Yleisimpiä siirrettäviä tietoja ovat:

- päälle- ja poiskytkentätiedot
- sabotaasi hälytykset
- murtohälytykset
- ryöstöilmoitukset
- vikatilat. [7,6.]

Yleisimpiä siirtoteitä ovat GSM, IP, GPRS ja puhelinlinja. Korkean turvallisuustason kohteissa ilmoituksensiirto on kahdennettu, eli siirrettävällä tiedolla on aina varayhteys eri siirtotekniikkaa käyttäen. Esimerkiksi ensisijainen siirtotie voi olla IP-verkkoa pitkin ja varayhteys GSM-verkossa. Siirtoyhteys voi olla myös valvottu, jolloin rikosilmoitin lähettää testilähetyksiä, joiden perustella voidaan todeta linjan toimivuus. On myös mahdollista hankkia yhteyden ylläpitäjältä palvelu, jossa valvotaan yhteyttä. Kyseisiä palveluja voi ostaa muun muassa teleoperaattoreilta. [7,6.]

Rikosilmoitinjärjestelmän ilmaisimilla havaitaan liikettä, ääntä, oven tai ikkunan tilaa, paineenvaihtelua, tärinää ja paniikkipainikkeilla esimerkiksi ryöstö. Ilmaisimien tarkoitus on havaita luvaton liikkuminen kohteessa.

Paikallishälytin on esimerkiksi sireeni tai vilkkuvavalo. Paikallishälytin hälyttää nimensä mukaisesti kohteessa. Paikallishälytyksen tarkoituksena on ilmoittaa lähistöllä mahdolli-

sesti liikkuville ihmisille, että jotain tapahtuu. Paikallishälyttimellä on myös tarkoitus säikäyttää tunkeutuja ja vähintäänkin ilmoittaa, että hälytin on lauennut.

Murtohälyttimellä on mahdollista parantaa työntekijöiden turvallisuutta silloin, kun kohteessa on ihmisiä. Kohteeseen sijoitetuilla ryöstöpainikkeilla välitetään ilmoitus vartiointiliikkeeseen, silloin kun jotain uhkaavaa tapahtuu, esimerkiksi ryöstö tilanteissa. Ryöstöilmoituksessa tyypillistä on, että hälytys on niin sanotusti hiljainen, eli paikallishälyttimet eivät aktivoidu. [9,13.]

Murtoilmaisujärjestelmään on mahdollista liittää myös taloautomaatioon kuuluvia ilmaisimia, kuten vesivuoto ja sähkökatkon havaitsevat ilmaisimet, jolloin myös näistä saadaan hälytys. Palohälyttimiä voidaan myös kytkeä hälyttimeen, jos kohteeseen ei tule erillistä paloilmoitinta. [9,13.]

3.1.1 Rikosilmoitinjärjestelmän suojaustasot

Suojaustasot määrittelevät sen, minkä tasoista murtautumista vastaan rikosilmoitin on suunniteltu. Riskiarvioinnin perusteella kohteelle määritetään suojaustaso, jonka perusteella lähdetään valitsemaan sopivaa hälytinlaitteistoa. Tasot on jaettu neljään luokkaan:

- Taso 1: Alhainen
- Taso 2: Keskimääräinen
- Taso 3: Korkea
- Taso 4: Erittäin korkea

Suojaustasojen määrittelyssä on ratkaisevana tekijänä se, kuinka ammattimaista ja millaisilla työkaluilla kohteeseen todennäköisesti yritetään murtautua. Suojaustasoja vastaavat järjestelmävaatimukset on myös luetteloitu taulukossa 2. [7,4.]

Tasosta riippuen käytettävät laitteet on oltava vähintään samaa tasoa suojaustason kanssa. Esimerkiksi tason kolme järjestelmässä laitteet pitää olla tasoa kolme tai neljä. Muita suojaustasoon vaikuttavia tekijöitä ovat: ilmoituksensiirron toteutus ja mihin hälytykset siirretään, käyttäjäkoodien päivittäminen määräajoin, huollon tiheys, järjestelmän testaukset määräajoin ja asennuksen suorittavan liikkeen pätevyys. [7,5].

3.1.2 Rikosilmoitinjärjestelmällä valvottavat alueet

Valvottavat alueet on jaettu neljään eri tyyppiin, jotka ovat:

- kehävalvonta
- kuorivalvonta
- tilavalvonta
- kohdevalvonta.

Valvonnasta pyritään tekemään kerroksittainen. Koska valvonnan uloin kerros ulottuu aina tontin rajalle asti, murtautujan eteneminen kohteessa voidaan havaita hyvissä ajoin. Näin voidaan vähentää tai jopa estää murtautujaa tekemästä vahinkoa yrityksen tiloissa. Kerroksittaisuudella savutetaan myös parempi turvallisuustaso, kun valvontaa tapahtuu jo ulkona ja rakennuksen ulkopinnoilla. [9,7.]

3.1.3 Kehävalvonta

Kehävalvonta on valvonta-alueista uloimpana. Kehävalvonnalla tarkoitetaan kohteen ulkoalueitten valvontaa. Kehävalvonnan edellytyksenä yleensä on, että alue on rajattu aidoin ja portein, jolloin alueen kehästä tulee selkeästi hahmotettava. Kehävalvonnassa käytettäviä ilmaisimia ovat esimerkiksi:

- **aktiiviset IR ilmaisimet:** Aktiiviset infrapunailmaisimet toimivat pareittain muodostaen välilleen säteen, jonka katketessa ilmaisin reagoi. Aktiivisten infrapunailmaisimien sijoituksessa ja asennuskorkeudessa kannattaa huomioida mahdolliset eläimet, lumen aiheuttamat kinokset ja vesisateen aiheuttamat raparoiskeet. Oikealla sijoittelulla voidaan välttää vikahälytyksiä. Infrapunailmaisimet tarvitsevat myös säännöllistä puhdistusta. Kehävalvonnan lisäksi aktiivisilla IR ilmaisimilla voidaan toteuttaa kuorivalvontaa, sijoittamalla laitteet esimerkiksi pitkien ikkunarivistöjen molempiin päihin. Paras tehokkuus IR ilmaisimilla tapahtuvaan valvontaan saa, kun asentaa ilmaisimia eri korkeuksille, niin että päällekkäisten ilmaisimien väli on enintään noin 20 cm. [10, 20-21.]

- **aitavalvontajärjestelmät:** Järjestelmästä riippumatta aitavalvontajärjestelmät havaitsevat aidan tärinän ja heilumisen. Järjestelmiä on tärinäilmaisimilla toimiva aitavalvontajärjestelmä sekä ilmaisinkaapelia käyttävä

järjestelmä. Tärinäilmaisimet kiinnitetään yleensä aitaverkkoon tai vähäisemmän turvallisuuden kohteissa ilmaisimet voidaan asentaa myös aitatolppiin. Ilmaisimet kytketään analysaattorilaitteeseen, jonka avulla saadaan suodatettua tuulesta ja maan tärinästä johtuva huojunta signaalissa. Ilmaisinkaapelilla toimivassa aitavalvonnassa kaapelin taipuminen tai värähtely aiheuttaa hälytyksen. Ilmaisinkaapelia voidaan yksinkertaisuutensa vuoksi asentaa monipuolisesti myös esimerkiksi rakennuksen seinille tai katoille. Ilmaisinkaapeli kytketään elektroniseen tarkkailuyksikköön, joka mittaa kaapelia. Tarkkailuyksikköä säätämällä saadaan eliminoitua normaalit poikkeamat kaapelissa. [10,21-22.]

- **kapasitiivinen maakaapeli:** Valvonta perustuu sähkökentässä tapahtuvien muutosten aiheuttamaan hälytykseen. Maakaapelijärjestelmässä maanalle asennetaan kaksi johdinta, joista toinen luo sähkökentän ja toinen analysoi sähkökenttää. Ihmisen tai eläimen liikkuessa sähkökentän vaikutusalueelle sähkökenttä muuttuu. Tämän muutoksen toinen johdoista, tuntojohto, havaitsee. Tuntojohto kytketään vahvistimen kautta erilliseen prosessoriin, joka tarkkailee sähkökentän muutoksia. Huomioitavaa maakaapelin asennuksessa on, että kasvillisuus on hävitettävä valvottavalta alueelta. Kasvillisuus saattaa tuulessa heiluessaan antaa vikahälytyksiä. Maakaapelijärjestelmä tarvitsee hälyttääkseen kolme yhtäaikaista tapahtumaa. Nämä tapahtumat ovat: kohteen riittävä läheisyys kaapeleihin nähden, kohteen liikkeen täytyy rajoittua välille 0,2-2 Hz ja kohteen täytyy pysyä sähkökentässä riittävän kauan. [10,23.]

Kehävalvontaa suunniteltaessa täytyy arvioida, minkä tyyppisiä ilmaisimia voidaan asentaa ja kuinka ne asennetaan. Haastavaa kehävalvonnasta muihin valvonta alueisiin verrattuna tekee se, että valvottava alue on ulkona, jolloin siihen vaikuttaa sääolosuhteet, liikenteen aiheuttama tärinä ja luonnossa liikkuvat eläimet. Taulukossa 3 on joitain kehävalvontaa hankaloittavia seikkoja. Taulukossa näkyy myös mitkä seikat vaikuttavat kuhunkin valvontatapaan. [9, 8.]

Taulukko 3. Kehävalvontalaitteiden ongelmat [10,20].

Haitta/ilmaisin tyyppi	Aktiivinen IR-ilmaisin	Aitavalvonta järjestelmät	Kapasitiivinen maakaapeli
Lumisade	x		
Sumu	x		
Eläimet	x		
Kasvillisuus	x		
Tuuli		x	x
Kinokset	x		
Maanpinnan muodot	x		
Liikenne		x	x

3.1.4 Kuorivalvonta

Kuorivalvonta kattaa kohteen rakennuksien ulkokuorten valvonnan. Käytännössä tämä tarkoittaa kaikkien ovien, ikkunoiden ja luukkujen valvontaa. Valvonta tapahtuu magneettikoskettimin, värähtelyyn reagoivin ilmaisimin ja ikkunan rikkoontumisen havaitseviin ilmaisimin. Kuorisuojauksella valvotaan kaikki edellä mainitut ovet, ikkunat ja luukut kahden metrin korkeuteen asti maanpinnasta tai tasosta, jossa pystytään liikkumaan. Korkeamman turvaluokituksen kohteissa kuorivalvonta ulotetaan aina neljään metriin asti. [9,9.]

On mahdollista, että kohteessa on pelkästään kuorivalvonta. Tämä tulee kyseeseen tilanteessa, jossa kiinteistön sisällä on ihmisiä vuorokauden ympäri, mutta halutaan hälytys esimerkiksi luvattomasta sisääntulosta tai vaihtoehtoisesti poistumisesta. Esimerkiksi sairaalan dementiaosasto on kohde, jossa pelkkä kuorivalvonnan käyttö olisi toimiva ratkaisu.

Kuorivalvonnan ilmaisimet:

- **magneettikosketin:** Magneettikosketin koostuu kahdesta osasta, joissa toisessa on magneetti ja toisessa kytkin, joka joko yhdistää tai katkaisee johdinlenkin. Oven valvonnassa magneettikoskettimella, sijoitetaan toinen koskettimen osa karmiin ja toinen ovilehteen, riippuen siitä kuinka kaapeli

on helpompi asentaa. Yleensä kaapeli on helpompi asentaa karmiin, johon silloin asennettaisiin kytkinosa, mutta jos ovessa on esimerkiksi jo valmiina sähkölukko ja kaapeli, niin kytkinosan voidaan myös kytkeä samaan lukkokaapeliin sähkölukon kanssa. Hälytysjärjestelmissä kytkinosa on normaalisti auki ja kun magneettiosa tuodaan tarpeeksi lähelle kytkintä niin kytkin yhdistää johtimet. Magneettikosketin hälyttää, kun kytkinosa on tarpeeksi kaukana magneettiosasta, eli lenkki katkeaa. Magneettikosketin on asennettava siten, että ovea tai ikkunaa ei pysty avaamaan enempää kuin viisi senttimetriä aiheuttamatta hälytystä. Magneettikoskettimia on erilaisia ja ne soveltuvat normaalien käyntiovien valvonnan lisäksi, esimerkiksi nostooviin, ikkunoihin, savunpoistoluukkuihin ja portteihin. Jos magneettikosketin asennetaan parioveen, on huomioitava, että molemmat ovilehdet tarvitsevat omat koskettimensa. [10,17.]

- **tärinäilmaisin:** Tärinäilmaisimella valvotaan yleensä ikkunaruutuja, mutta ilmaisinta voidaan käyttää myös muun muassa ovien tai seinien valvontaan. Ilmaisin reagoi korkeataajuisiin runkoääniin tai iskuääniin. Tärinäilmaisin asennetaan ikkunan karmiin tai vaihtoehtoisesti voidaan käyttää liimattavaa mallia ikkunaruutuun. Ilmaisimessa tulee olla sabotaasikytkin, joka hälyttää, jos ilmaisin irtoaa kiinnityksestään. Jokainen ikkunaruutu tarvitsee oman tärinäilmaisimen. Ikkunaruutuun liimattavissa tärinäilmaisimissa on huomattava, että ne on asennettava vähintään viiden senttimetrin päähän karmista. Liimattavaa ilmaisinta ei suositella asennettavaksi yksikerroksisiin laseihin. [10, 17-18.]

- **kuunteleva lasirikkoilmaisin:** Kuuntelevalla lasirikkoilmaisimella valvotaan paljon lasia sisältäviä seiniä. Ilmaisimen mikrofonit kuuntelevat lasin rikkoutumisesta tulevaa ääntä. Asetetusta herkkyydestä riippuen kuuntelevalasirikkoilmaisin kattaa 200 - 400 kuutiota huonetilaa. Ilmaisin asennetaan kattoon tai valvottavan seinämän vastakkaiselle seinälle. Kuuntelevaa lasirikkoilmaisinta asennettaessa täytyy ottaa huomioon, että ikkunan ja ilmaisimen välillä ei saa olla äänenkulkua estäviä huonekaluja, verhoja tai muuta tavaraa. [10,18.]

3.1.5 Tilavalvonta

Tilavalvonta kattaa rakennuksen sisällä tapahtuvan valvonnan. Tilavalvontaan tarkoitetut ilmaisimet reagoivat liikkeeseen. Ilmaisimet sijoitetaan vähintään tiloihin, joista joudutaan kulkemaan liikuttaessa rakennuksessa, esimerkiksi käytävät ja aulatilat ovat hyviä sijoituspaikkoja tilavalvontailmaisimille. Jos tilavalvontailmaisimet asennetaan kohteeseen, joka ei ole vielä käytössä, täytyy selvittää mahdolliset huonekalujen sijainnit, että katvealueilta vältyttäisiin.

Tilavalvonnan ilmaisimet:

- **passiivinen IR ilmaisin:** Passiivinen infrapunailmaisin havaitsee lämpötilan muutoksia valvontakentässään. Ilmaisin ei lähetä valvottavalle alueelle mitään vaan analysoi ilmaisimeen tulevaa lämpösäteilyä. Optimaalisin asennuskorkeus ilmaisimelle on 2-2,5 metriä, siten että ilmaisin suunnataan hieman alaviistoon. Tehokkain havaitseminen tapahtuu kun kohde liikkuu poikittain ilmaisimeen nähden, tämä kannattaa huomioida ilmaisimen sijoittelussa. Auringonvalo voi aiheuttaa infrapunailmaisimessa vääriä hälytyksiä, joten ikkunaseinälle kohdistamista kannattaa välttää. [10,15.]

- **ultraääni-ilmaisin:** Ilmaisin soveltuu pieniin tiloihin, koska tehokas valvonta matka on 20 metriä. Ilmaisimen toiminta perustuu Doppler-ilmiöön. Ilmaisimessa on erikseen ääniaaltoja lähettävä lähetin ja vastaanotin, joka analysoi ympäristöstä tulevaa äänienergiaa. Liikkeet valvonta-alueella aiheuttavat muutoksen äänienergioissa, jotka vastaanotin havaitsee. Ultraääni-ilmaisin toimii parhaiten liikkeeseen, joka on kohtisuoraan ilmaisimeen. Ultraääni-ilmaisimen kanssa virhehälytyksiä voi aiheuttaa äänilähteet valvottavalla alueella, esimerkiksi ilmastointi. [10,16.]

- **mikroaalto-ilmaisin:** Mikroaalto ilmaisin lähettää valvonta-alueelle säteilyä ja analysoi alueelta heijastunutta säteilyä. Valvonta-alueella liikkuminen aiheuttaa muutoksia ilmaisimelle palaavan säteen taajuuteen, jonka ilmaisin havaitsee. Kuten ultraääni-ilmaisimessa, mikroaalto-ilmaisin toimii parhaiten, kun kohde liikkuu kohtisuoraan ilmaisinta kohden. Mikroaalto-ilmaisimen asennuksessa on oltava tarkka siitä, että asennuspaikka on tu-

keva eikä pääse heilumaan tai tärähtelemään. Pienetkin heilahtelut voivat aiheuttaa virhehälytyksiä, herkemmin kuin infrapuna- tai ultraääni-ilmaisimissa. [10,13.]

3.1.6 Kohdevalvonta

Kohdevalvonta valvoo nimensä mukaisesti kohteessa olevia tärkeitä kohteita, jotka oletettavasti kiinnostava murtautujaa [9,12]. Näitä kohteita ovat esimerkiksi kassakaapit ja taulut. Kohdeilmaisimet kiinnitetään valvottavaan kohteeseen.

Kohdevalvonnan ilmaisimet:

- **runkoääni-ilmaisimet:** Runkoääni-ilmaisin reagoi tärinään ilmaisimessa olevan mikrofonin avulla. Runkoääni-ilmaisimen asennuspaikan täytyy olla tasainen, tasaisuuden tulee olla pienempää kuin 0,1 mm. Muussa tapauksessa ilmaisimen alla täytyy käyttää metallista asennuslevyä. Jos ilmaisin asennetaan epätasaiseen alustaa, on mahdollista, että ilmaisimen mikrofoni vahingoittuu. [10,24]

- **tauluilmaisin:** Tauluilmaisin havaitsee painonmuutoksen, mutta sallii taulun koskettamisen. Ilmaisin asennetaan taulun taakse seinän sisään. [9,12.]

- **kapasitiivinen ilmaisin:** Kapasitiivinen ilmaisin havaitsee kapasitanssin muutoksen valvottavan kohteen ja sen ympäristön välillä. [10,24.]

3.1.7 Murtoilmaisujärjestelmän suunnittelu

Murtoilmaisulaitteista ei ole kansallisia viranomaismääräyksiä. Kappaleessa 2 mainittu laki yksityisistä turvallisuuspalveluista määrää sen, että järjestelmän suunnittelijan, asentajan, käyttöönottajan ja huoltajan täytyy omistaa turvasuojaajakortti.

Murtoilmaisujärjestelmä on yhdessä kiinteistön rakenteellisen murtosuojauksen kanssa tärkeä osa ennaltaehkäisevää rikoksen torjuntaa. Ensisijaisesti kohteen suojaus tulee toteuttaa rakenteellisin keinoin, jota täydennetään rikosilmoittimen ilmaisimilla. Hyvällä rakenteellisella suunnittelulla, voidaan minimoida tarvittavat ilmaisinlaitteet, ja tehdä murtoilmaisimesta luotettavampi ja edullisempi hankkia. [11,77.]

Järjestelmän suunnittelussa täytyy kohteesta tehdä riskikartoitus. Riskikartoituksessa pohditaan mahdollisia uhkatekijöitä, joiden perusteella määritetään laitteiston luokitus ja valvonnan laajuus. Kartoituksessa selvitetään minkälaisen riskin esimerkiksi yritys aiheuttaa omalla toiminnallaan, eli arvioidaan kuinka ammattimaista oletettu murtautuminen olisi. Seuraavia asioita tulisi pohtia suojauksen tasoa mietittäessä:

- kuinka arvokasta tavaraa kohteessa on
- tavaran jälleenmyyntiarvo ja myynnin helppous
- kuinka helposti tavara on vietävissä, eli fyysiset mitat ja paino
- kohteen sijainti
- rakenteellisen suojauksen aukot. [7,1.]

Kohteen koko ja mahdolliset ulkoalueet ovat myös otettava huomioon suojausta rakennettaessa. Oman haasteen suunniteluun luo tarve erotella luvallinen ja luvaton liikkuminen suojattavalla alueella. Riskejä arvioittaessa täytyy miettiä kuinka esimerkiksi yöaikaan kulkevat tavarantoimittajat voivat purkaa kuormansa aiheuttamatta hälytystä mutta toisaalta siten ettei samanaikaisesti kohteeseen pääse luvattomasti henkilöitä. Tärkeää on suojattavan kohteen jako alueisiin, jolloin hälytinjärjestelmä voi olla osittain kytkettynä päälle. [9,2.]

3.1.8 Keskuslaitteen mitoitus ja valinta

Riskikartoituksen avulla selvitetty kohteen suojaustaso määrittelee sen, että valittavalla keskuslaitteella täytyy olla vähintään yhtä hyvä turvaluokitus. Turvaluokituksen jälkeen ratkaiseva tekijä keskuksen valinnassa on siihen liitettävien ilmaisimien lukumäärä. Keskuksia on olemassa aina pienistä alle kymmenen silmukan järjestelmistä aina laajoihin satoja silmukoita käsittäviin keskuksiin. Silmukkamäärää mitoittaessa kannattaa keskus

hieman ylimitoittaa, jolloin mahdolliset ilmaisin lisäykset jälkikäteen ovat mahdollisia ilman koko keskuksen vaihtoa. [9, 3.]

Myös käyttölaitteiden määrät on oltava tiedossa keskusta valittaessa, koska keskuksesta riippuen ne tukevat käyttölaitteita eri määriä kuten myös käyttäjiä [7, 3]. Käyttölaitteilla käyttäjät kytkevät järjestelmän päälle ja pois, joten niiden sijoittelussa käyttäjän mielipide on tärkeä. Käyttäjillä rikosilmoittimessa tarkoitetaan koodien tai tunnisteiden määrää. Pois lukien tason 1 järjestelmät, täytyy jokaisella käyttäjällä olla henkilökohtainen koodi. Suojaustason 1 laitteistossa eri käyttäjät voivat käyttää halutessaan yhteistä koodia tai tunnistetta.

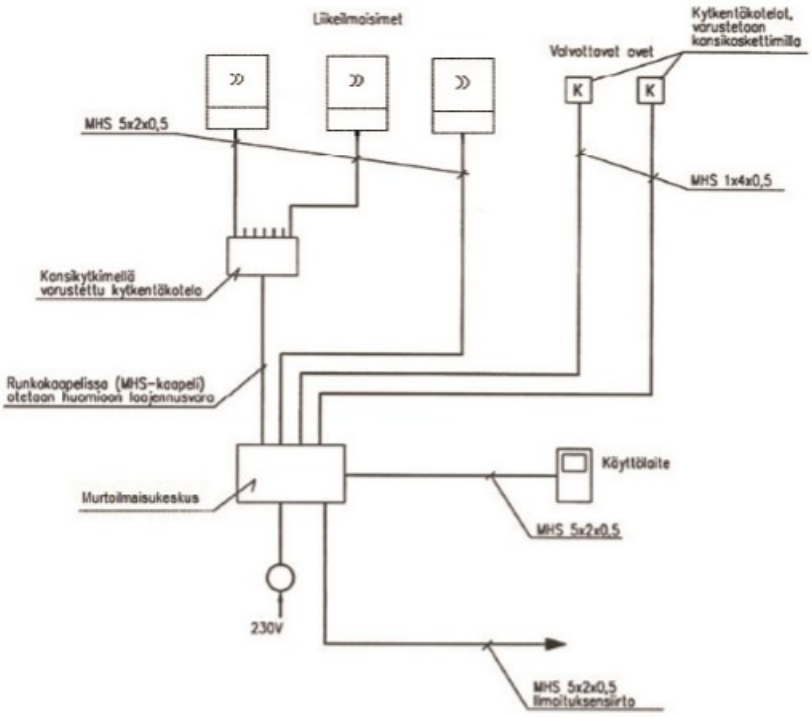
Tarvittavat integraatiot eli liitännät muihin järjestelmiin vaikuttavat keskuslaitteen valintaan. Joissain keskuslaitteissa on mahdollista tehdä ohjelmallinen integraatio esimerkiksi kulunvalvontaan ja kameravalvontaan, jolloin kaikkien järjestelmien hallinnointi ja ohjaukset pystytään ohjelmoimaan yhdestä järjestelmästä. Tämä toimii yleensä parhaiten silloin kun järjestelmät ovat saman valmistajan laitteita. Esimerkiksi opinnäytetyössäni suunnittelemat Hedegren Securityn HHL-rikosilmoitin ja Hedsam-kulunvalvonta. Integraatiota on myös mahdollista tehdä keskuslaitteen ohjatuilla tuloilla ja lähdöillä, joiden avulla saadaan jatko-ohjauksia esimerkiksi kulunvalvontaan tai päinvastoin. [9, 3.]

Yksi keskuslaitteen tärkeimmistä ominaisuuksista on ilmoituksensiirtomahdollisuudet [9, 3]. Ilmoituksensiirto-ominaisuuksia mietittäessä kannattaa pohtia, mihin ilmoitukset siirretään, eli minkälaisella tekniikalla ilmoitus täytyy siirtää, että vastaanotin sen ymmärtää. Lisäksi on huomioitava Finanssialan Keskusliiton vaatimukset ilmoituksensiirrosta ja valittava keskus siten, että vaatimukset täyttyvät.

3.1.9 Kaapelointi

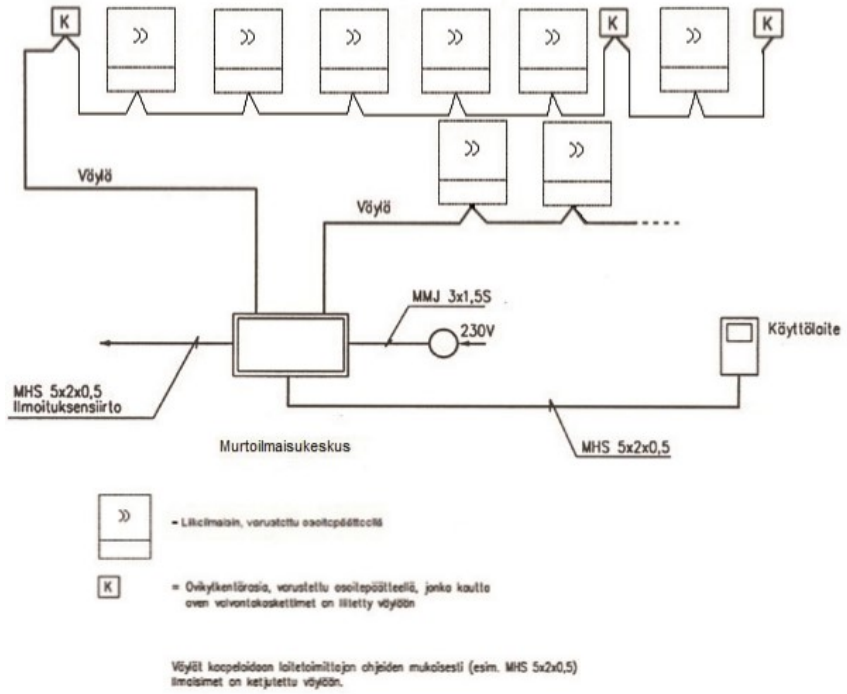
Kaapelointitavan määrittää käytettävä keskustyyppi. Kuten edellä mainittiin, keskuksia on joko osoitteellisia tai silmukkaperiaatteella toimivia. Silmukkaperiaatteella toimivassa keskuksessa ilmaisimet liitetään silmukoihin joko yksinään tai useamman ilmaisimen ryhmässä. Silmukkajärjestelmässä kaapelointi toteutetaan tähtimäisesti, joka saattaa joissain ti-

lanteissa kasvattaa kaapelointikustannuksia verrattuna väylä ratkaisuun. Kuvassa 3 on silmukoilla toimivan keskuksen kaapelointi ratkaisu. [9, 4.]



Kuva 3. Silmukkakaapelointi [9, 4.]

Silmukkakeskusten lisäksi on myös ilmaisinväylää käyttäviä keskuslaitteita, tällöin puhutaan osoitteellisesta järjestelmästä. Jokainen ilmaisin väylässä saa oman osoitteensa päätevastuksien avulla. Osoitteellisella järjestelmän kaapeloinnissa voidaan yhtä runkokaapelia pitkin tuoda kaikki järjestelmän ilmaisimet keskukselle, jolloin kaapelin määrä vähenee. Ilmaisimien määrä väylässä määräytyy keskuslaitteen mukaan. [9, 4.]



Kuva 4. Osoitteellinen järjestelmä [9, 5.]

Kaapelityyppinä yleisesti käytetään MHS-tyyppisiä puhelinkaapeleita, joiden halkaisija on vähintään 0,5 mm. Poikkeuksena ovi- ja ikkunakaapeloinnit, joissa voidaan käyttää ohuempia kaapeleita. Kaapeloinnissa on huomioitava kaapelin resistanssi, joka aiheuttaa jännitehäviöitä. Kaapelointi on mitoitettava siten, että jokaisen haaran viimeiselläkin ilmaisimella on valmistajan määrittelemä minimijännite. [12, 108.]

Muutoin kaapeloinnissa käytetään yleisesti määriteltyjä kaapelointitapoja. Rikosilmoitin kuuluu heikkovirtajärjestelmiin, joten sen kaapeloinnit tulee erottaa kaapelihyllyllä vahvavirtakaapeloinnista. Kaapelit täytyy merkitä molemmista päistään. Jos järjestelmään tulee maakaapelointia, täytyy kaapelit olla suojattu putkella tai kourusuojalla. Rikosilmoitinjärjestelmän kaapeloinnissa on myös huomattava, että kaikki kytkentäpisteet on suojattava rasioilla, joissa on kansikoskettimet, jolloin kytkentöjen sabotointi ei onnistu. [9, 13.]

3.2 Kulunvalvontajärjestelmät

Kulunvalvontajärjestelmä on laitteisto, jolla seurataan kulkua valvottujen ovien, porttien ja hissien kautta. Järjestelmällä on myös mahdollista ohjata ovia tai portteja, esimerkiksi ulko-ovet voidaan ohjata päivisin auki. Järjestelmän käyttöä varten käyttäjillä täytyy olla hen-

kilökohtainen tunniste, jolla he pääsevät kulkemaan kulunvalvotuista ovista, mikäli heillä on siihen oikeus. Kulku tallentuu myös kulunvalvontajärjestelmään, josta kulkutietoja voidaan tarkastella reaaliaikaisesti tai jälkikäteen. Tunnisteena voidaan käyttää esimerkiksi kulkukorttia, avaimenperätunnistetta, numerokoodia tai sormenjälkeä. [13, 41.]

Kulunvalvontajärjestelmää voidaan käyttää työajanseurantaan ja joihinkin järjestelmiin on mahdollista saada työajanseurantaa varten omat laitteistot, jotka pystyvät synkronoimaan esimerkiksi yrityksen palkanlaskuohjelman kanssa.

3.2.1 Kulunvalvontajärjestelmää koskevat lait ja määräykset

Kulunvalvontajärjestelmien asentamista ohjaavat samat turvasuojausta koskevat lait ja asetukset kuin rikosilmoittimienkin kohdalla. Koska kulunvalvontajärjestelmällä on mahdollista valvoa ja kerätä tietoa ihmisten liikkeistä kohteessa, täytyy sen asennuksessa ja käytössä ottaa huomioon henkilötietolaki ja laki yksityisyyden suojasta työelämässä.

Lain yksityisyyden suojasta työelämässä mukaan, työnantaja saa käsitellä työntekijöittensä henkilötietoja vain, mikäli ne ovat tarpeellisia työsuhteen kannalta, tai jos henkilötiedot liittyvät työnantajan tarjoamiin etuuksiin tai työ on luonteeltaan erityistä. Työnantajan täytyy pyrkiä saamaan tiedot ensisijaisesti työntekijältä henkilökohtaisesti. Tästä seuraa se, että kulunvalvontajärjestelmän keräämien tietojen tutkimiselle täytyy olla laissa annetut perusteet. [14.]

Henkilötietolaki määrittelee kulunvalvontatietojen asianmukaisen säilyttämisen sekä henkilörekisterin pitämisen. Kulunvalvontajärjestelmän muodostamalle henkilötietorekisterille täytyy olla vastuuhenkilö ja rekisterin olemassa ololle täytyy olla perusteet. On myös huomioitava, että henkilötietojen keräämiseen tarvitaan asianosaisen suostumus. Suostumus yleensä pyydetään samalla kuittauksella kulunvalvontatunnisteen luovutuksen yhteydessä. [15.]

3.2.2 Kulunvalvontajärjestelmän rakenne

Kulunvalvontajärjestelmään kuuluu seuraavia kokonaisuuksia:

- keskusyksikkö: sisältää järjestelmän ohjelmistot sekä tietokannat
- alakeskukset: järjestelmästä riippuen siinä voi olla alakeskuksia. Alakeskus kerää tietoa kenttälaitteilta ja välittää sen keskukselle. On myös mahdollista, että oviyksiköt ovat suoraan yhteydessä keskukseen, tällöin järjestelmässä ei ole alakeskuksia.
- akkuvarmennettu jännitteensyöttö: kulunvalvontajärjestelmän laitteet tarvitsevat akkuvarmennuksen, että ovien käyttö on mahdollista myös sähkökatkon aikaan.
- kenttälaitteet: muun muassa ovipäätteet, ruokalapäätteet, työajanseurantapäätteet ja mahdollisesti myös porttipuhelimet. [13, 43-44.]

Kulunvalvontajärjestelmästä riippuen kenttälaitteet kaapeloidaan keskuksiin tai alakeskuksiin, joko väylä- tai tähtityyppisesti. Joissain järjestelmissä on myös mahdollista liittää ovirasiat suoraan lähiverkkoon, josta keskusyksikkö löytää ne IP- ja MAC-osoitteen perusteella. Liitettäessä oviyksiköt kiinteistön tietoliikenneverkkoon kannattaa miettiä laskeeko se järjestelmän turvallisuustasoa, koska muiden samassa verkossa toimivien on mahdollista päästä käsiksi järjestelmään. Korkean turvallisuuden järjestelmissä kulunvalvontalaitteille voidaan rakentaa oma verkko, joka on irrallaan kiinteistön muusta tietoliikenneverkosta.

Kulunvalvontajärjestelmän keskusyksikkönä toimii yleensä PC. Joissakin tapauksissa keskusyksikkö voi olla myös pelkästään kyseessä olevaan järjestelmään suunniteltu tietokone. Kevyimmissä kulunvalvontalaitteistoissa oviyksiköt voivat olla älykkäitä, jolloin ne sisältävät tarvittavan ohjelmiston itsessään. Tällöin yhteys niihin otetaan esimerkiksi Internet-selaimen tai älypuhelinsovelluksen kautta. Kulunvalvonnan keskusyksikkö täytyy olla varmistettu siten, että sähkökatkon aikana siitä ei katoa tietoa. Henkilötietokannoista täytyy myös ottaa määräajoin varmuuskopiot mahdollisten laiterikkojen varalta. [13,43.]

Kulunvalvonnan henkilötietokantoja ja kenttälaitteita hallitaan kulunvalvonnan ohjelmistoilla. Ohjelmistojen kautta määritellään kenttälaitteitten toiminnallisuus, esimerkiksi ovien aikaohjaukset ja kulkuoikeudet. Lisäksi ohjelmistoilla luodaan ja muokataan henkilötieto-

kantoja, jossa määritellään käyttäjät ja heidän henkilökohtaiset tai ryhmäkohtaiset kulkuoikeutensa. Kulunvalvontaohjelmistolla pystytään esimerkiksi ryhmittelemään eri yritysten henkilöt omiin ryhmiinsä, joilla on samoja kulkuoikeuksia.

Varmennettu tehonsyöttö on olennainen osa luotettavasti toimivaa kulunvalvontajärjestelmää. Koska peruskäyttäjillä ei ole mahdollisuutta avata mekaanisesti kulunvalvottuja ovia, täytyy ovien ohjausten toimia myös sähkökatkon aikana vähintään tunnin [13,44]. Mitoittaessa tehonsyöttöä täytyy ottaa huomioon oviyksikön viemä teho, sekä lukkolaitteitten ja mahdollisten muitten hälytinlaitteiden viemät tehot. Joissain järjestelmissä on mahdollista käyttää oviyksiköiden tehonsyöttöön PoE-tekniikkaa, mutta lukot tarvitsevat tämän lisäksi oman tehonsyöttönsä. PoE:n kautta virtaa voidaan syöttää laitteelle ethernet-kaapelissa.

Ovipäätteet sisältävät liitännät oviympäristöön. Ovipäätteelle saadaan tuotua oven tilatietoja. Lisäksi oviyksikössä on lukon ohjausreleitä. Kulunvalvonnan lukijat liitetään myös oviyksikköön. Oviyksikkö kaapeloidaan keskukselle tai alakeskukselle. [13,44.]

3.2.3 Kulunvalvontajärjestelmän päätteet

Kulunvalvontajärjestelmän päätteillä käyttäjät käyttävät järjestelmää, eli esimerkiksi saavat avattua kulunvalvotun oven tai kirjauduttua töihin. Järjestelmän päätteet kuuluvat kenttälaiteisiin ja niitä on seuraavanlaisia:

- kulunvalvonnan lukija
- työaikapääte
- ruokalapääte

Kulunvalvonnan lukijat sijoitetaan valvottuun oveen tai sen välittömään läheisyyteen [13,47]. Etälukija voi olla näppäimistöllinen tai pelkkä lukija. Näppäimistöllistä lukijaa käytetään esimerkiksi jos halutaan korkeampaa turvallisuutta [13, 50]. Tällöin henkilölle voidaan tunnisteen lisäksi antaa henkilökohtainen koodi, joka pitää tunnisteen lisäksi syöttää lukijalle, että kulku hyväksytään. Etuna siinä on se, että jos käyttäjä kadottaa tunnisteensa, niin tunnisteella ei pääse suoraan kulkemaan ovesta ilman koodia. Näppäimistöllistä lukijaa voidaan käyttää myös pelkkänä koodilukkona ovelle, jossa ei ole kriittistä turvallisuusvaatimusta. Kulunvalvonnan kautta tehtävät jatko-ohjaukset, esimerkiksi murtohälyttimen pois- ja päälle kytkennät, onnistuvat myös näppäimistöllisellä etälukijalla. Etälukijaa käyte-

tään yleisesti myös hissin ohjaukseen. Tällöin hissin ohjauskeskukseen liitetään kulunvalvonnan hissiohjauksen relekortti, joka antaa käyttäjän mennä kerroksiin, johon hänellä on oikeus.

Työaikapäätettä käytetään työajan seurantaan. Päätteelle kirjataan töihin saapuminen, töistä poistuminen, sairaus poissaolot ja esimerkiksi työmatkat. Työaikapäätteeltä tiedot siirtyvät kulunvalvontajärjestelmään, josta ne saadaan siirrettyä palkanlaskuohjelmaan [16, 10]. Työaikapäätteet sijoitetaan yleensä henkilökunnan sisääntulo-ovien läheisyyteen, suojatulle puolelle [16, 12]. Työaikapääte sisältää etälukijan, näytön ja näppäimistön, jolla työntekijä pystyy valitsemaan haluamansa vaihtoehdon edellä mainituista kirjausmahdollisuuksista. Järjestelmästä riippuen työaikapääte liitetään sarjaliitännällä oviyksikköön, alakeskukseen tai tietoverkkoa pitkin keskuslaitteelle.

Ruokalapääte on periaatteeltaan työaikapäätteen kaltainen, johon käyttäjä kirjaa ostamansa ruoka-annoksen. Ostotiedot siirtyvät päätteeltä järjestelmään, josta ne siirtyvät laskutukseen. Ruokalapääte sijoitetaan tyypillisesti esimerkiksi ruokalassa kassan yhteyteen. [16,11.]

3.2.4 Kulunvalvontajärjestelmän suunnittelu

Kuten murtohälytinjärjestelmän suunnittelussa, myös kulunvalvontajärjestelmää varten tehdään turvallisuussuunnitelma. Jos kohteeseen tulee molemmat järjestelmät, voidaan näitä varten tehdä yhteinen turvallisuussuunnitelma. Kulunvalvontajärjestelmä on osana pääsynhallintaa, kun puhutaan toimitilaturvallisuudesta. Muita pääsynhallintaan liittyviä järjestelmiä on esimerkiksi mekaaninen avainjärjestelmä. [17,3.]

Kulunvalvontajärjestelmää ei ole yleensä järkevää asentaa jokaiseen kiinteistön oveen. Suunnittelussa täytyy miettiä, mitkä ovet varustetaan kulunvalvonnalla. Näin säästytään ylimääräisiltä kustannuksilta. Harvoin on tarkoituksenmukaista varustaa esimerkiksi siivouskomeroita kulunvalvonnalla, vaan näihin tiloihin riittää mekaaninen lukitus. Vain ne tilat, joitten kulkua halutaan seurata tai pääsyoikeuksia muuttaa säännöllisesti tai ajastaa, kannattaa varustaa sähköisellä lukituksella ja kulunvalvonnalla. [17, 3.]

Yksi kulunvalvonnan eduista on nopeat kulkuoikeuksien muutokset. Tästä syystä kiinteistön ulkokuoren ovet kannattaa varustaa kulunvalvonnalla. Jos käyttäjä kadottaa tunnisteensa, voidaan luvaton sisäänpääsy estää nopeasti ilman lukkojen sarjoituksia. Ulkoovien varustaminen kulunvalvonnalla mahdollistaa myös ovien aikaohjaukset, esimerkiksi päivisin auki asentoon, jolloin asiakkaat pystyvät kulkemaan sisään ja ulos ilman tunnistetta.

Poistumistiet täytyy ottaa kulunvalvonnan suunnittelussa huomioon. Poistumistieovet ovat ovia, joista täytyy päästä tarpeen tullen kulkemaan ilman avainta tai tunnistetta. Jos poistumistieoveen suunnitellaan kulunvalvonta, siten että poistumissuunta on valvottu, täytyy oviympäristöön suunnitella tuotteet joilla poistuminen on mahdollista ilman tunnistetta. Poistumistieovien kulunvalvontaratkaisut täytyy aina hyväksyttää paikallisella pelastusviranomaisella. Poistuminen tulee mahdollistaa palotilanteen lisäksi myös muissa hätätilanteissa. Yksi tapa on esimerkiksi varustaa oviympäristö lasirikkopainikkeella, joka aktivoi oven painikkeen siten, että ovesta päästään kulkemaan ilman tunnisteita. Tässä tapauksessa ovelle voidaan asentaa erillinen hälytin, joka hälyttää kun lasirikko painetaan, jolloin luvaton hätäpainikkeen laukaisu huomataan. [17, 12.]

Koska kulunvalvontajärjestelmä vaatii toimiakseen sähköisen lukituksen sekä lukijat ja oviyksiköt, tulee järjestelmän hankinnasta yleensä kallis investointi. Suunnittelijan kannattaa myös pohtia vaihtoehtoisia ratkaisuja, jos kohteen turvallisuusvaatimukset sallivat sen. Nykypäivänä ovet on myös mahdollista varustaa elektronisilla avainjärjestelmillä, joissa avaimia ja lukkoja pystytään ohjelmoimaan. Tällöin joustava kulkuoikeuksien muuttaminen on mahdollista ilman sarjoituksia. Tosin ovien tilatietoja ei tällaisesta järjestelmästä saada ja lukkojen ohjelmointi täytyy yleensä suorittaa ohjelmointilaitteella paikanpäällä. Mutta jos jatkuvaa ovivalvontaa ei tarvita voivat elektroniset avainpesäratkaisut olla kilpailukykyinen vaihtoehto. Elektroniset avainjärjestelmät sijoittuvat ominaisuuksiltaan ja hinnaltaan mekaanisen lukituksen ja kulunvalvonnan välimaastoon. [17,3.]

3.2.5 Kulunvalvontajärjestelmän kaapelointi

Kulunvalvontajärjestelmän kaapelointi koostuu kahdesta osasta, runko- ja oviympäristönkaapeloinnista [17,4]. Runkokaapelointi sisältää kaapeloinnit kenttälaitteitten ja keskuslait-

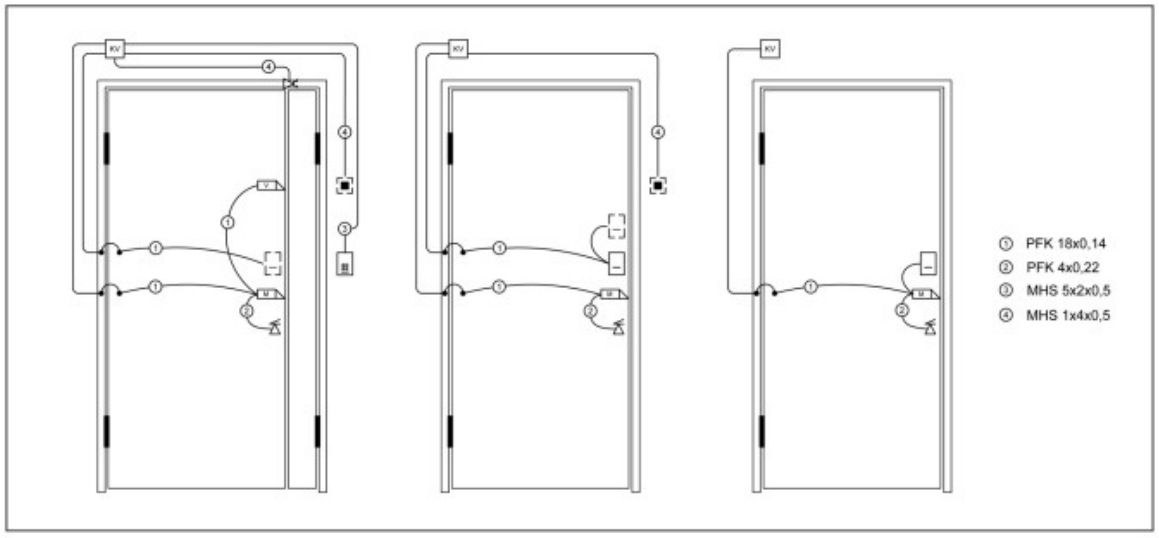
teiden välillä. Runkokaapelointiin kuuluu yleensä kaikki kenttälaitteiden kaapeloinnit, jotka eivät sijaitse oviympäristössä. Runkokaapeloinnin suunnittelee ja toteuttaa yleensä sähkösuunnittelija ja sähköurakoitsija. Oviympäristön kaapeloinnin suorittaa kulunvalvonta- tai lukkourakoitsija. [17,5.]

3.3 Sähköinen lukitus

Kulunvalvontajärjestelmä tarvitsee toimiakseen sähkölukkoja. Suomessa käytettävät sähkölukot ovat suurimmalta osin Abloy Oy:n valmistamia. Sähkölukon perusominaisuus on, että sitä voidaan ohjata sähköisesti auki tai kiinni. Lisäksi lukolta saadaan tilatieto siitä onko ovi lukittuna.

3.3.1 Oviympäristö

Ovessa sähkölukko kuuluu osaksi isompaa kokonaisuutta, jota kutsutaan oviympäristöksi. Oviympäristö sisältää kaikki oveen liittyvät tuotteet. Kuvassa 5 on kolme esimerkkiä oviympäristöjen laitteista.



Kuva 5. Oviympäristöjä [17, 20]

Oviympäristön termistö on osittain ristiriidassa muuhun rakentamiseen liittyvän termistön kanssa. Esimerkiksi oviympäristössä painike tarkoittaa ovenkahvaa, kun taas sähköurakassa painikkeella tarkoitetaan esimerkiksi valokytkintä. Siksi onkin tärkeää, että urakoitsi-

joilla on selkeät urakkarajat ja oviympäristöjen ovikortit ovat yksiselitteiset niin, ettei epäselvyyksiä synny.

3.3.2 Sähkölukon valinta

Valittaessa sähkölukkoa kulunvalvontaoveen täytyy suunnittelijalla olla tiedossa ainakin seuraavat asiat:

- Onko ovi profiiliovi, peltipalo-ovi vai umpiovi?
- Onko ovi palo-ovi?
- Onko kulunvalvonta yksi vai kaksi puoleinen?
- Kuinka paljon ovesta kulkee ihmisiä?
- Onko oveen tulossa oviautomatiikkaa?
- Tuleeko oveen vedin vai painike?
- Tarvitaanko oveen sähköistä varmuuslukkoa?

3.4 Kameravalvonta

Kameravalvonnan tarkoitus toimitilaturvallisuudessa on olla ennaltaehkäisevä pelote ja jälkiselvittelyn apuväline. Kameravalvontaa käytetään myös reaaliaikaiseen seurantaan esimerkiksi kaupoissa. Tällöin valvomotarkkailijalla on mahdollisuus seurata useampaa hyllyväliä ja nurkkausta yhdellä silmäyksellä, kun useampi kamera on liitetty monitoriin. [18, 3.]

Kameravalvontajärjestelmiä voidaan käyttää myös muihin kuin rikoksentorjuntaan ja kulunvalvontaan liittyviin sovellutuksiin. Esimerkiksi prosessiteollisuudessa kameravalvonnalla on koko ajan isompi rooli liukuhihnan seurannassa [18, 3]. Nykyaikaiset ohjelmistoratkaisut mahdollistavat monipuoliset analyysimahdollisuudet kamerakuvan perusteella. Esimerkiksi kauppakeskuksessa voidaan seurata ihmisten liikkumiskäyttäytymistä kaupan käytävillä.

3.4.1 Kameravalvonnan lainsäädäntö

Kameravalvontaa koskevat säädökset kerrotaan rikoslain luvussa 24. Tästä luvusta, kameravalvontaa koskettavat, salakatselu ja yksityiselämää loukkaava tiedon jakaminen. Kameravalvonta muodostaa myös henkilörekisterin, kuten kulunvalvontakin, joten rikoslain henkilörekisteririkos luvussa 38 sivuaa myös kameravalvontaa.

Kamerajärjestelmää suunniteltaessa ja etenkin käytettäessä täytyy olla tarkkana, ettei syyllisty salakatseluun. Salakatselu tarkoittaa seuraavaa:

> Salakatseluun syyllistyy rikoslain 24 luvun 6 §:n mukaan henkilö, joka oikeudettomasti teknisellä laitteella katselee tai kuvaa kotirauhan suojaamassa paikassa, käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa oleskelevaa henkilöä. Lisäksi salakatseluun voi syyllistyä kuvaamalla julkisrauhan suojaamassa paikassa oleskelevaa henkilöä tämän yksityisyyttä loukaten. Julkisrauhan suojaamia paikkoja ovat esimerkiksi aidatut yleisöltä suljetut rakennukset, huoneistot tai aidatut piha-alueet. [19, 51.]

Vaikka laissa sanotaan, että asunnossa kuvaaminen on kielletty, niin laki ei kiellä omassa asunnossa olevan tunkeutujan kuvaamista [19,51]. Kuvaaminen yksityistiloissa ei ole myöskään silloin kiellettyä, jos siihen on saatu kaikkien asukkaitten tai kohteessa kävijöiden suostumus. Tämmöisiä tilanteita on esimerkiksi kerrostalojen rappukäytävien kuvaaminen. Rappukäytävien kuvaaminen on mahdollista vain, jos siihen saadaan kaikkien asukkaiden suostumus, koska rappukäytävät ovat kotirauhan suojaamia alueita. [19,16.]

On huomattava, että salakatselun kohteena täytyy olla ihminen. Esineitten tai eläinten salakatselu tai kameralla valvominen ei ole rangaistavaa. Käyttäjällä on vastuu siitä, ettei salakatselua hänen kameroillaan tapahdu. Järjestelmän käyttäjä on siis henkilö ketä salakatselusta voidaan ainoastaan syyttää. [19,52.]

Lainvastaista on myös levittää salaa kuvaamalla saatua materiaalia esimerkiksi median kautta. On kuitenkin huomattava, että jaetun materiaalin täytyy sisältää jotain yksityiselämään liittyvää tietoa. Julkisilla paikoilla otettujen kameratallenteiden näyttö esimerkiksi uutisissa ei ole lainvastaista. [20.]

Työpaikoilla kameravalvonnan käyttöä säätelee laki yksityisyyden suojasta työelämässä. Lailla yritetään parantaa työntekijöiden yksityisyyden suojaa työpaikalla. Lain viidennessä

luvussa on lueteltu tapaukset, joissa työnantaja saa käyttää kameravalvontaa. Nämä tapaukset ovat:

- henkilöstön ja asiakkaiden turvallisuuden varmistaminen
- omaisuuden suojaaminen
- erilaisten prosessien valvominen, esimerkiksi liukuhihnan seuranta
- työturvallisuuden parantamiseksi. [14.]

Kameravalvontaa työpaikoilla ei voida käyttää tietyn työntekijän seurantaan, eikä myöskään työntekijöille osoitetuissa sosiaalitiloissa. Vaikka tietyn työntekijän seuraaminen kameroin on laitonta, niin on mahdollista seurata työpistettä, mikäli se on välttämätöntä työn takia. Tämmöisiä välttämättömiä tilanteita ovat esimerkiksi: työntekijään kohdistuu väkivallan uhka, työntekijä käsittelee merkittäviä rahamääriä tai muuta arvokasta ja työntekijän pyynnöstä toteutettu kameravalvonta. Työntekijä voi esimerkiksi pyytää kameravalvontaa parantaakseen omaa oikeusturvaansa epäselvissä tilanteissa. [14.]

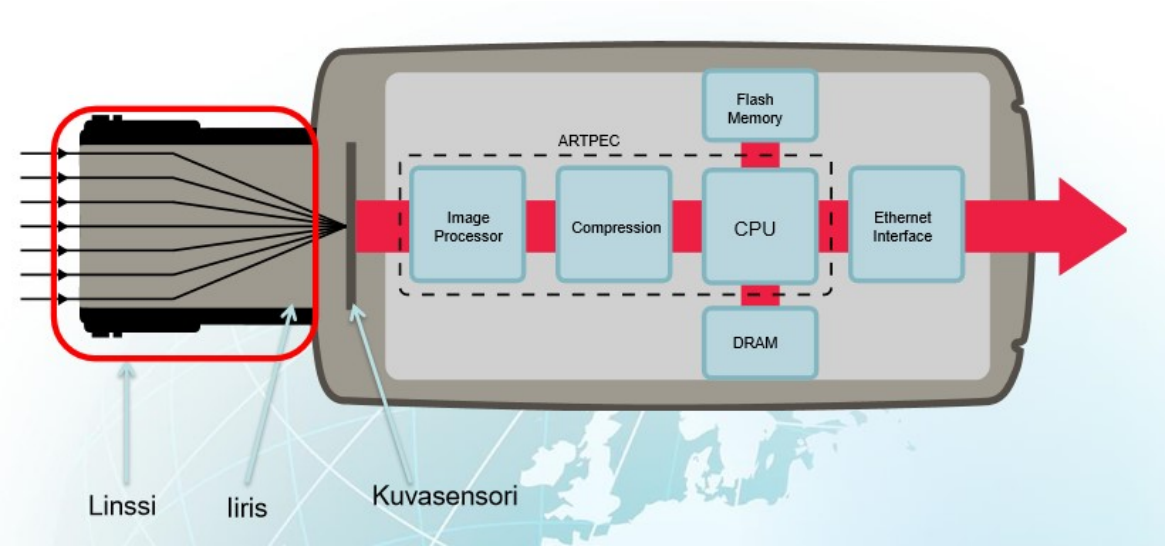
3.4.2 Kameratyypit

Kameroita on olemassa tekniikoiltaan kahta mallia, analogikameroita ja IP-kameroita. Analogikamerat ovat jäämässä vähemmälle ja tilalle tulee entistä enemmän IP-tekniikkaan perustuvia kameroita, varsinkin kun IP-kameroiden hankintakustannukset laskevat jatkuvasti.

Analogisessa kamerassa on CCD-kenno, joka siirtää kuvan suoraan sähköisenä signaalina koaksiaalikaapelia pitkin monitorille tai tallentimelle [18,7]. Kuvaa on mahdollista siirtää myös esimerkiksi MHS-tyyppisellä kaapelilla, mutta tällöin väliin tarvitaan muuntimet. Analogikamerassa tarkkuus ilmoitetaan pystyjuovien määränä kuva-alassa. [18, 7.]

IP-kamerassa käytetään CMOS- tai CCD-kennoa, johon kuva heijastuu kuvapisteinä eli pikseleinä. Pikseliluku kertoo kennon tarkkuuden [18,7]. Koska kuvapisteitten määrä kameroitten kennoissa on kasvanut, on IP-kameroitten tarkkuus mennyt huomattavasti analogisten edelle. Kennosta kuva muutetaan digitaaliseksi signaaliksi. Analogisesta kamerasta poiketen IP-kamerassa on sisällä mikroprosessori, omaa muistia ja ohjelmistoja. Ohjel-

mistojen avulla kuvaa pystytään muokkaamaan suoraan kamerassa, ja se pystytään esimerkiksi pakkaamaan tehokkaasti, jolloin se ei rasita tietoverkkoa läheskään niin paljon kuin raakakuvan siirtäminen. IP-kameran ohjelmistot mahdollistavat myös kamerakuvan tarkastelun ilman tallenninta tai monitoria. IP-kameran kuvamateriaalin siirto tapahtuu TCP/IP-protokollan siirtoverkkoa pitkin. Siitä tulee myös nimitys, IP-kamera. Jokaiselle kameralle pystytään määrittelemään oma IP-osoite ja lisäksi jokaiselta kameralta löytyy oma MAC-osoite.



Kuva 6. IP-kameran rakenne. [20.]

Koska IP-kameroilla päästään huomattavasti suurempiin tarkkuuksiin, pystytään tällöin yhdellä kameralla kuvaamaan laajempaa aluetta tarkkuuden siitä kärsimättä. Vaikka uusista kamerajärjestelmistä ehdottomasti suurin osa on IP-kameroita, on myös tilanteita joissa analogisten kameroitten käyttö on yhä perusteltua. Seuraavaksi on lueteltu molempien kamera tyyppien hyvät ja huonot puolet:

IP-kamerajärjestelmä:

+ Parempi kennon tarkkuus mahdollistaa laajemmat kuva-alat ja esimerkiksi laajakuvan käytön

+ Joustavat kaapelointimahdollisuudet. Pystytään kaapeloimaan suoraan tallentimelle tai käyttämään hyväksi jo olemassa olevaa lähiverkkoa.

+ Yhä useammassa kamerassa on tuki muistikortille, jolloin tallenninta ei välttämättä edes tarvita tai muistikortti toimii hyvänä varatallennus välineenä jos verkon yhteys tallentimeen katkeaa.
+ Kameran reaaliaikaista kuvaa voidaan tarkastella monelta päätteeltä yhtä aikaa
+ PoE-tekniikka mahdollistaa virransyötön ethernet-kaapelia pitkin, jolloin kameralle ei tarvitse vetää erikseen virransyöttökaapelia.
- Korkeat hankintakustannukset
- Tietoturvallisuuden huomioiminen, jos IP-kamera on kiinteistön yleisessä LAN-verkossa.
- Suuret kameramäärät saattavat hidastaa verkon muita laitteita
- Herkät kennot tarvitsevat myös enemmän valoa toimiakseen kunnolla

Analoginen kamerajärjestelmä:

+ Edullisempi verrattuna IP-kameroihin. Tosin koko ajan tulee edullisempia IP-kameroita markkinoille.
+ Kaikki kamerat keskenään vaihdettavissa ilman yhteensopivuusongelmia, koska kameroitten sisällä ei ole valmistajakohtaisia ohjelmistoja.
- Kaapeloinnin jäykkyys: kameroille on vedettävä omat kaapelit ja ne on tuotava tallentimelle tai monitorille asti. Ei voida käyttää hyväksi esimerkiksi kiinteistön tietoliikenne verkkoa.
- Huonompi kuvanlaatu verrattuna IP-kameroihin.

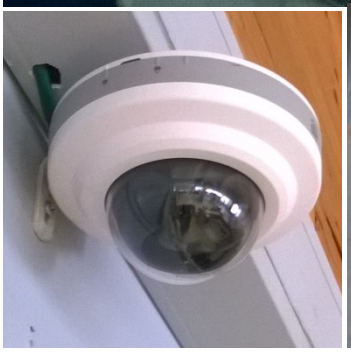
3.4.3 Kameratyypin valinta

Koska nykypäivänä käytetään yhä enemmän IP-kameroita, esimerkit ovat IP-kamera maailmasta. Osa ominaisuuksista pätee myös analogisiin kameroihin, kuten linssien tyypit.
Mietittäessä sopivaa kameraa on otettava huomioon lukuisia seikkoja, joista tärkeimpiä ovat muun muassa:

- Tuleeko kamera sisälle vai ulos?
- Halutaanko kameralla tunnistaa kohde vai vaan havainnoida liikkuminen alueella?
- Virransyöttö tapa: PoE tai erillinen syöttö?
- Joutuuko kameran kuva alttiiksi vastavalolle, jos tulee niin kuinka paljon vastavaloa tulee?

- Kuinka laajalta alueelta kameralla halutaan kuvata?
- Kameran ulkonäön merkitys, halutaanko että kamera on esillä niin sanotusti pelokkeena vai esteettisesti huomaamaton. Myös kameran suojausvaatimukset ilkivaltaa vastaan kuuluvat tähän.

Ensimmäisenä kameran valinnassa täytyy tietää onko kamera tulossa sisä- vai ulkokäyttöön. Sisäkäyttöön suunnitelluissa kameroissa IP-luokitus on sellainen, ettei se kestä vettä tai kylmyydestä aiheutuvaa kosteutta. Sisäkameroissa ei myöskään ole lämmitystä, joten kylmyys aiheuttaa linssin huuruistumista. Ulkokameran voi asentaa myös sisälle, mutta kustannussyistä niin harvoin tehdään, koska ulkokamerat ovat arvokkaampia kuin vastaavat sisämallit. Jos käytetään runkokameroita, niin itse kamerassa ei ole eroteltu sisä- tai ulkomalleja, vaan suojaus toteutetaan ulkona kotelolla ja lämmittimellä. Dome- ja bullet-kameroilla taas on mallit erikseen sisä- ja ulkokäyttöön.



Kuva 7. Sisäkäyttöön tarkoitettu runkokamera käsin säädettävällä objektiivilla

Kuva 8. Dome kamera

Kuva 9. Bullet kamera

Kamerasta haluttava informaatio voidaan jaotella neljään tunnistustasoon: yleiskuva, havaitseminen, tunteminen ja yksilöinti. Analogisten kameroiden kanssa käytettään K-menetelmää, kun määritellään yllä olevia luokkia. K-menetelmässä määritellään se kuinka monta prosenttia ruudun korkeudesta kohteen täytyy täyttää, että se on hyväksyttävä.

Yleiskuvalla K arvo on K5 eli 5 % ruudun korkeudesta täyttyy kohteesta. Havaitsemiskuvalla arvo on K10 = 10 %, tunnistamiseen tarvittava K-arvo on K50 ja yksilöintiin on määritelty K = 120. [21.]

IP-kameroiden kanssa K-arvo menetelmää ei kannata käyttää, koska IP-kameran kuva koostuu pikseleistä, toisinkuin analogisten kameroitten kuva koostuu pystyjuovista, joitten määrä vaihtelee kameran tarkkuudesta riippuen. Lisäksi IP-kameroiden tarkkuuksissa on eroja, joten K-arvo ei kerro mitään kuvasta saatavasta informaatiosta. K-arvon käyttö analogistenkin kameroiden kanssa on ongelmallista, koska myös analogisissa kameroissa on tarkkuuseroja vaikka juovaluvut olisivat samat. [21.]

Käyttökelpoisempia ominaisuuksia IP-kameroissa niiden määrittelyyn on kuva-ala(Field of View = FoV) ja kuvapistettä/metri (PPM = Pixels Per Meter). Tällöin havainnointiin voidaan käyttää määritelmää 20 kuvapistettä/metri ja edelleen tunnistamiseen 50 kuvapistettä/metri ja yksilöintiin 500 kuvapistettä/metri.

Kun tiedetään kameran tarkkuus ja haluttu tunnistustaso esimerkiksi 1 280x720 kuvapistettä ja 500 kuvapistettä/metri, voidaan laskea kamerasta saatava näkymän leveys $\frac{1280p}{500p/m} = 2{,}56m$. Jos taas halutaan havaitsemiseen riittävää kuvan tarkkuutta, kuvan leveydeksi saadaan $\frac{1280p}{20p/m} = 64m$. Kaavasta nähdään että mitä enemmän kamerassa on kuvapisteitä, sitä isompi kuva-ala pystytään esittämään tarkkuuden kärsimättä. Tarkkuudella tässä tapauksessa tarkoitetaan kuvapistettä/metri mittayksikköä. [21.]

Kameran linssien polttoväli määrittelee sen, kuvaako kamera kauas pienellä katselukulmalla vai lähelle laajemmalla kuvakulmalla. Katselukulmaan vaikuttaa myös kameran kuvasensorin eli kennon koko. Kameramallista riippuen polttoväli voi olla vakio, käsin säädettävä tai sähköisesti säädettävä esimerkiksi tallennin ohjelmiston kautta. Kamerat, joissa on motorisoitu polttovälin säätö eli moottorizoomaus, ovat yleensä jonkin verran kalliimpia verrattuna käsin säädettäviin, joten niiden käyttöä on syytä harkita. Esimerkiksi kohteisiin joissa on jatkuvasti henkilö tarkkailemassa ja säätelemässä kameroita tai kohteissa joissa kamerat ovat sijoitettu paikkoihin joista niitä on vaikea käydä jälkikäteen säätämässä, kannattaa määritellä kamera, jossa on moottorilla säädeltävä polttoväli.

Katselualan ja tarkkuuden lisäksi ympäristön valaistus vaikuttaa kameran valintaan. Jos kameran kuvaan tulee paljon häiritsevää vasta-valoa, täytyy valita kamera jossa on vasta-valonsuodatus ominaisuus. Kuitenkin ensisijaisesti täytyy pyrkiä asentamaan ja suuntaamaan kamerat siten ettei vastavaloa tule.

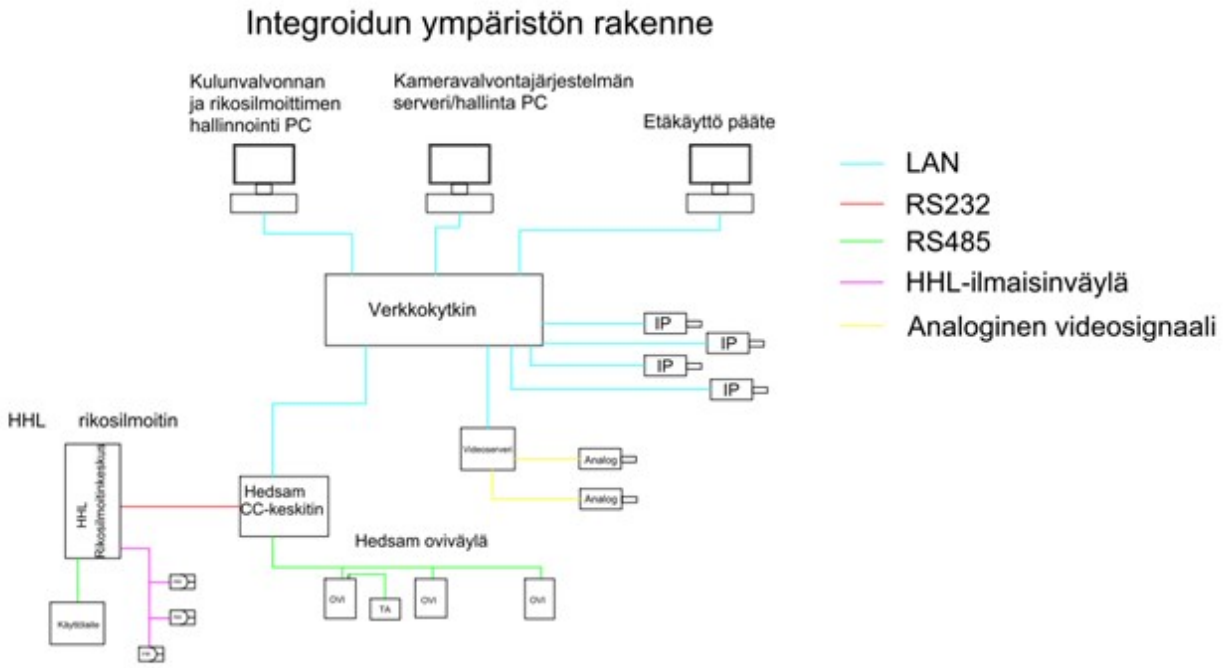
3.4.4 Kameravalvontajärjestelmän suunnittelu

Kameravalvontajärjestelmä koostuu kameroitten lisäksi tallentimesta ja valvontamonitoreista. Kameroitten määrä ja niiden tuottaman kuvamateriaalin vaativa kovalevytila asettavat vaatimuksen tallentimen kapasiteetille. Tallentimien ohjelmistoissa on myös eroja, nykyisin suurinta osaa tallentimista pystytään käyttämään Internet-yhteyden avulla. Tallenninta suunniteltaessa olisi hyvä tietää integroidaanko kameravalvontaa johonkin muuhun järjestelmään kuten kulunvalvontaan. Tallennintyypistä riippuen niissä on erilaiset integraatio mahdollisuudet.

Kameroitten sijoittelu ja suuntaus on tärkeää, että kameravalvonnasta saadaan riittävän kattava. Hyvällä sijoittelulla ja suuntaamisella pystytään myös vähentämään kameroitten määrää. Varsinkin ulkokameroissa valaistussuunnittelu on olennaista. Kameroissa itsessään olevat infrapuna-valot harvoin riittävät selkeään kuvaan pimeällä

3.5 Integraatio

Monen järjestelmän erillinen käyttö voi aiheuttaa tilanteen, jossa kukaan eri järjestelmien käyttäjistä ei saa kunnollista kokonaiskuvaa tapahtuneesta. Integraation avulla järjestelmät saadaan yhdistettyä siten, että tilanteen kartoitukseen voidaan käyttää kaikkia turvatekniikan järjestelmiltä saatuja tietoja. Esimerkiksi kamerakuvan yhdistäminen palo- tai murtohälytykseen antaa käyttäjälle tarkempaa tietoa tapahtuneesta. Täsmällisempien tietojen avulla toimenpiteitten suorittaminen helpottuu ja nopeutuu. Laboratorioon suunnittelemassani integroidussa kokonaisuudessa eri järjestelmät keskustelevat keskenään lähiverkon ja CC-keskittimen kautta (kuva 10).



Kuva 10. Integroitu ympäristö

4 Toimeksianto ja toteutus

Toimeksiantona oli suunnitella järjestelmien päivitys toimitilaturvallisuuden laboratorioon. Järjestelmien päivitys edellytti tutustumista laboratorion järjestelmiin ja arvioimaan niiden käyttökelpoisuuden. Päivityksen yhteydessä laboratorion sijainti myös vaihtui, joten laitteiden uudelleen sijoittelu oli myös osa suunnitelmaa. Suunnitelmat sisältävät kytkentä- sekä pistesijoituskuvia. Lisäksi päivitystä varten on tehty tuotelistauksia lähinnä kulunvalvonnan osalta. Sijoittelussa on pyritty huomioimaan aiemmin todetut seikat ilmaisimien ja muiden kenttälaitteiden ominaisuuksista.

4.1 Päivityksen lähtökohdat

Aloittaessani päivitys työn laboratoriossa oli seuraavanlaiset järjestelmät ja laitteet:

Kulunvalvonnassa oli kaksi kulunvalvontajärjestelmää. Toinen järjestelmistä oli Hedengrenin Hedsam ja toinen Stanley Securityn Timecon. Hedsam järjestelmä koostui kolmesta ovesta sekä työaika- ja ruokalapäätteistä. Timecon oli kahden oven järjestelmä, jossa yksi ovilukija toimi myös työaikapäätteenä. Molempien järjestelmien tietokannat ja ohjelmistot olivat asennettu Windows XP käyttöjärjestelmään, joka oli myös yksi syy päivityksen tekemiseen. Laboratoriossa ovet ovat liikuteltavia pienoiskoossa olevia ovia, joissa on pyörät alla. Lukuun ottamatta yhtä Hedsam ovea, joka oli toteutettu asentamalla kulunvalvontalaitteet pienen komeron oveen.

Rikosilmoitinjärjestelmiä laboratoriossa oli kolme. Kaksi kappaletta Hedengrenin HHL-16 keskuksia ja lisäksi OUMAN-kotihälytinjärjestelmä. HHL-järjestelmien ilmaisimet sijaitsivat osittain kulunvalvontaovien yhteydessä ja osittain laboratorion seinillä ja valaisin kiskoissa. Keskukset olivat asennettuina ja kaapeloituina levyn päälle laboratorion seinustalle. OUMAN järjestelmä oli kokonaisuudessaan irrotettavan levyn päälle asennettu.

Kameravalvontaa varten laboratoriossa oli kaksi tallenninta ja hallinnointiohjelmistoa, DINA ja ASAN. Tallentimiin kytketyt kamerat olivat sekä analogisia että IP-kameroita. Osa analogi-kameroista oli kytketty tallentimeen videoserverin kautta.

Paloilmoitin laitteina laboratoriossa olivat Hedengrenin Prodex-100 keskus ilmaisimineen ja Panasonicin EBL-keskus ilmaisimineen. Prodexin keskukseen oli lisäksi liitetty palonsulkuovi.

4.2 Laitteiden sijoittelu uusiin tiloihin

Päivitystä varten tein sijoituskuvan, johon sijoitin tilaturvallisuuden järjestelmät ja niiden kenttälaitteet (kuva 11). Pistesijoittelussa pyrin huomioimaan kenttälaitteiden oikeaoppinen sijoittelun. Lisäksi integraation tuomat mahdollisuudet on huomioitu sijoittelussa. Tilan käytöstä johtuen lopullista laitteistoa ei pystytty asentamaan suunnitelmien perusteella.

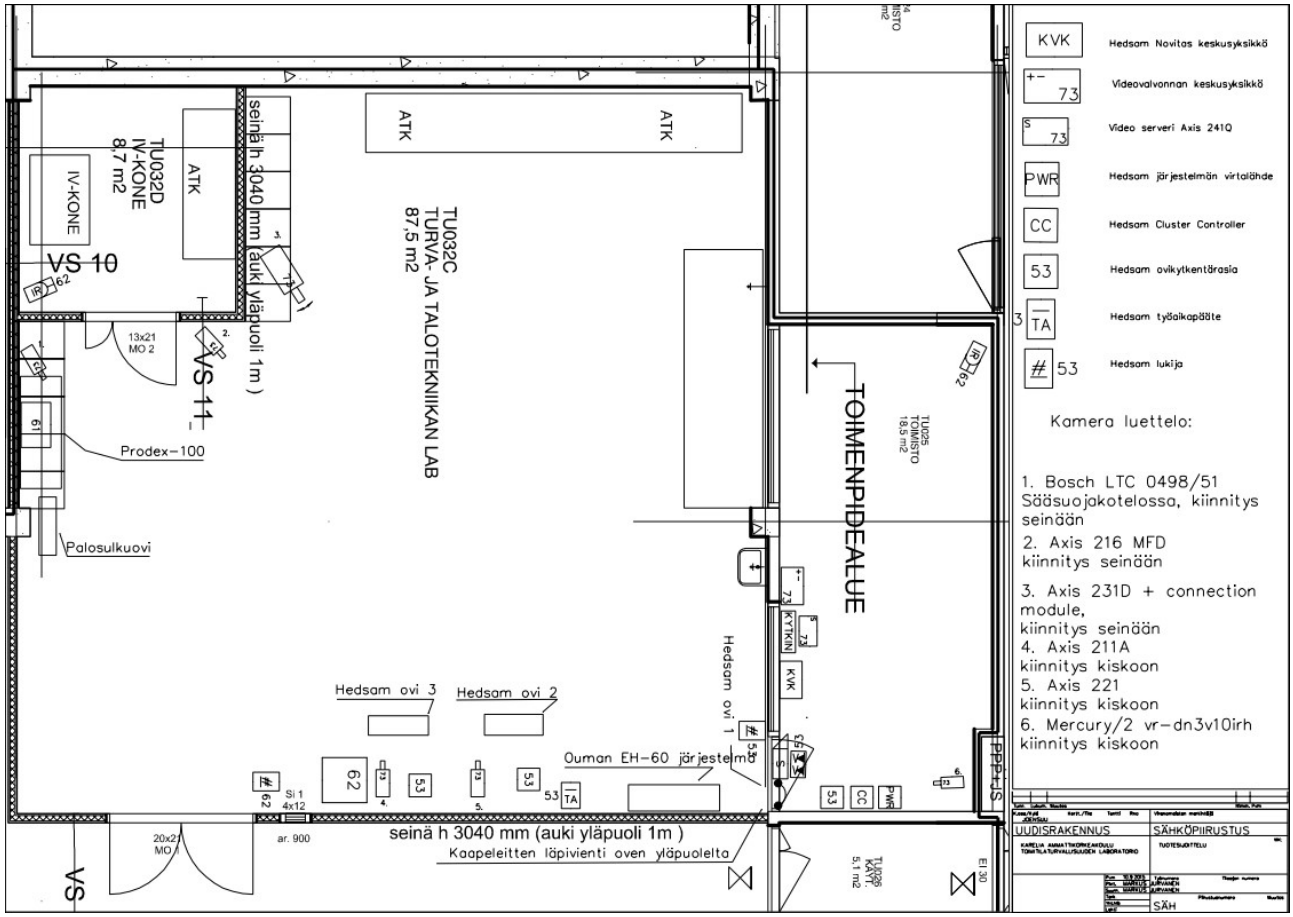
Suunnitelmassani sijoitin jokaisen kulunvalvontaoven taakse kameran. Tällöin integraation avulla saadaan ovilta tarvittaessa kuvaa esimerkiksi tilanteessa, jossa joku käyttää ovea ilman oikeuksia. Loput kamerat on sijoitettu siten, että ne sijaitsevat luokan perillä ja ovat

suunnattu kulunvalvontaovia kohti. Sijoittelulla ja suuntauksella pystytään rajaamaan se, että oppilaitten käyttämien koneitten näytöt eivätkä näppäimistöt näy kamerakuvissa. Myös kamerat jotka kuvaavat kulunvalvontaovia luokan seinustalla, tulee suunnata niin alas, että työpisteet eivät päädy kuvaan. Näppäimistön ja näyttöpäätteen näkyminen kamerakuvassa on ongelmallista yksityisyyden suojan kannalta, koska henkilökohtaiset tiedot näkyisivät tallenteissa. Toisaalta henkilöitten kuvaaminen työpisteittensä äärellä on myös määritelty tarkkaan laissa ja kuvaamiseen pitäisi löytyä hyvät perusteet. Kamerat ovat kuitenkin tarkoitettu vain opiskelukäyttöön eikä kuvamateriaalia käytetä jälkeenpäin.

Rikosilmoittimen passiivisten infrapunailmaisimien sijoittelussa on otettu huomioon ilmaisimen ominaisuus havaita parhaiten poikittaista liikettä ilmaisimeen nähden. Sijoittamalla infrapunailmaisin huoneen nurkkaan saadaan kattava havaitsemisalue. Ilmaisimet on suunnattu siten, että poikittaista liikettä tulisi mahdollisimman paljon. Ilmaisimien sijoittelussa on myös huomioitu testaamisen helppous. Laboratoriotilassa ei ole yhtään liikeilmaisinta, jolloin ilmaisimia pystytään testaamaan niin, ettei ilmaisimen alueella ole jatkuvaa liikettä. Käyttölaite on sijoitettu sisääntulo-oven viereen, kuten käyttölaitteet sijoitetaan oikeissakin ympäristöissä. Itse keskuksen sijoituksessa lähtökohtana oli sopivan seinätilan löytäminen.

Kulunvalvontalaitteisto on sijoitettu luokan seinustalle. Oviohjainkortit asennetaan seinälle ja oville kaapelointi viedään ovikorteilta suoraan. Ovien liittämisessä käytetään irrotettavia liittimiä, jolloin ovet on mahdollista siirtää helposti, jos tarvetta ilmenee. Kuten vanhassa laboratoriossa niin myös tähän suunnittelin yhdeksi kulunvalvontaoveksi oikean käytössä olevan oven, joka johtaa pohjakuvassa näkyvälle toimenpide alueelle. Oikean oven käyttö simuloinnissa antaa paremman kuvan järjestelmän toiminnasta. Työaikapääte on sijoitettu seinustalle oviohjauskortin viereen, jolloin kaapelointi päätteelle on helppo toteuttaa.

Järjestelmien keskusyksiköt ja käyttöpäätteet on sijoitettu toimenpidealueelle. Toimenpide alue on pieni huone, jossa on iso lasi-ikkuna laboratorioon. Toimenpidealue on ikään kuin valvomo, josta järjestelmiä käytetään.



Kuva 11. Suunniteltu sijoituskuva.

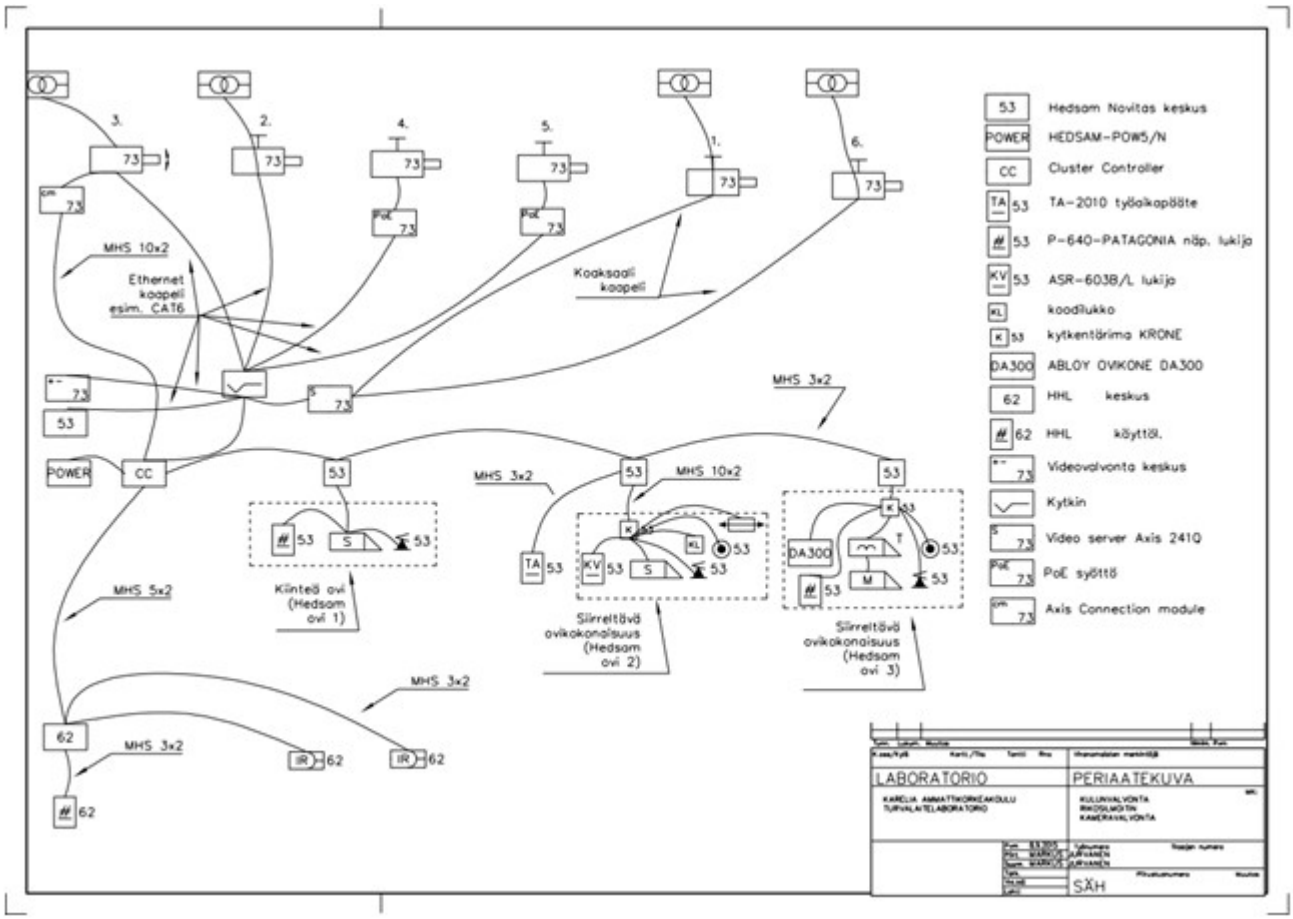
4.3 Runkokaapeloinnin suunnittelu

Järjestelmien integraatiota varten kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmät kytketään samaan lähiverkkoon. Lähiverkon hyödyntäminen helpottaa kaapelointia, koska laboratoriossa olevia verkkokaapelointeja voidaan hyödyntää. Kulunvalvonnan kenttälaitteet kaapeloidaan MHS-puhelinkaapelilla. Oviyksiköt kytketään väylään, jolloin yhdellä runkokaapelilla saadaan kaapeloitua kaikki oviyksiköt ja työaikapääte. Kenttälaiteväylä alkaa keskittimeltä, joka kytketään lähiverkkoon.

Rikosilmoitinkeskuksen ilmaisimet kytketään väylään. Ilmaisimet erotellaan toisistaan osoitepäätteillä. Käyttölaite kaapeloidaan keskukseen omalla väylällä, johon ei voi kytkeä il-

maisimia. Myös rikosilmoittimen kaapeloinnit kaapeloidaan MHS-kaapelilla. Keskus kaapeloidaan samaan keskittimeen kulunvalvonnan kenttälaitteiden kanssa.

Kameroita on kuusi, joista neljä IP-kameraa ja kaksi analogi-kameraa. Videoserverin avulla myös analogiset kamerat saadaan kytkettyä lähiverkkoon. Osa IP-kameroista saa käyttöjännitteensä PoE–kytkimen kautta ja loput erilliseltä virtalähteeltä. Kamerat kaapeloidaan CAT6-kaapelilla, lukuun ottamatta analogisia kameroita, jotka kaapeloidaan videoserverille koaksaalikaapelilla. Videoserveri kytketään verkkoon muitten laitteiden kanssa.



Kuva 12. Järjestelmien runkokaapelointi.

4.4 Kulunvalvontajärjestelmän päivitys

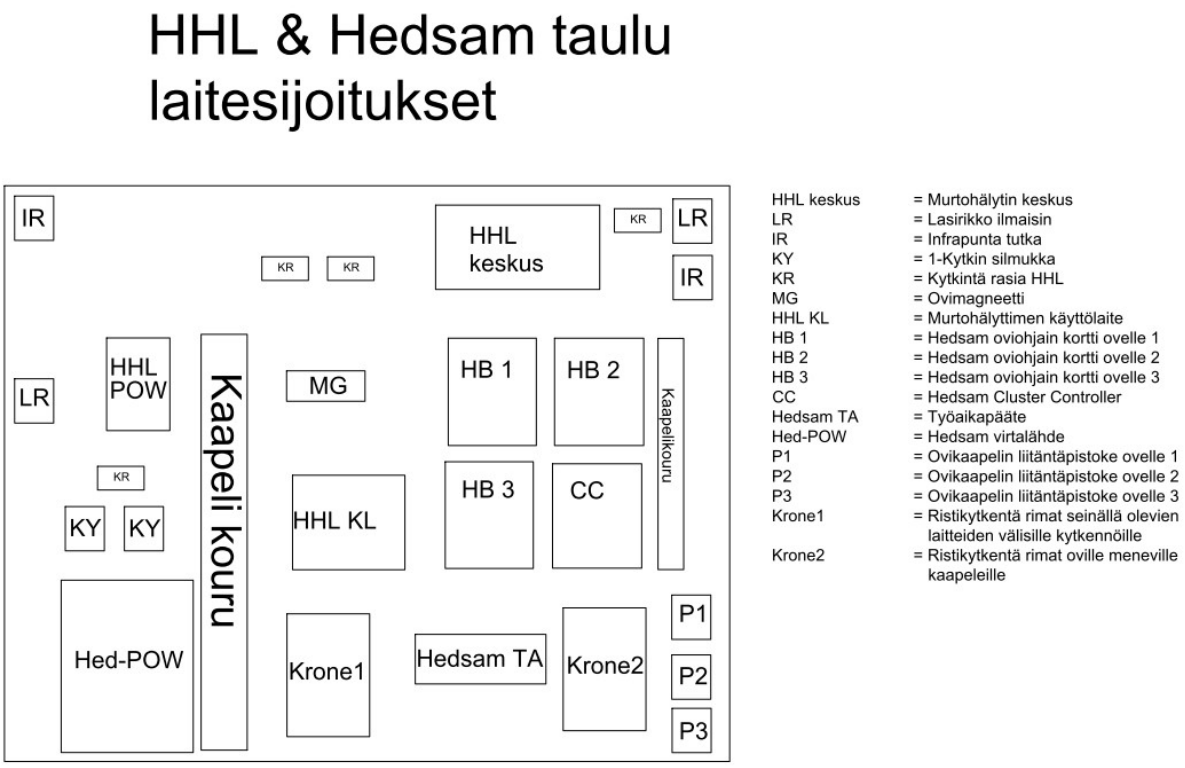
Kulunvalvontapäivityksen lähtökohtana oli se, että vain yksi järjestelmä päivitetään. Näin päivityksen kustannukset pysyvät mahdollisimman matalana. Päivitettäväksi järjestelmäksi

valittiin Hedsam Novitas-kulunvalvonta. Hedsam-kulunvalvonnan päivitykseen päädyttiin, koska laboratoriossa on myös muita Hedengrenin laitteistoja, kuten HHL-rikosilmoitin ja Prodex-paloilmoitin. Yhteinen valmistaja mahdollisti integraatiot monipuolisemmin kuin monen eri valmistajan laitteistot.

Laitteiston osalta käytöstä poistettiin ruokalapääte ja työaikapääte, joka korvattiin uudella työaikapäätteellä. Lukijat säilyvät ennallaan. Oviyksiköihin tehdään PROM-piirien päivitys uudempaan ohjelmaversioon, jolloin oviyksiköt saadaan Novitas yhteensopiviksi. Kaikki ohjelmistot ja lisenssit uusittiin, koska vanhat versiot olivat vanhentuneita. Kulunvalvonta-järjestelmän keskusyksikköä ei tilattu erikseen, koska koululta löytyy tarkoitukseen sopiva tietokone.

Suurin ero vanhaan järjestelmään on integraatio HHL-rikosilmoittimen kanssa. Integraatio-ta varten järjestelmään hankittiin Cluster Controller-keskitin, jonka välityksellä Hedsamin oviväylä ja HHL:n tietoliikenneväylä keskustelevat kulunvalvontaserverin kanssa. Cluster Controller liitetään samaan verkkoon serverikoneen kanssa. Kulunvalvonnan serverikoneeseen asennetaan myös rikosilmoittimen ohjelmistot.

Koska alkuperäistä sijoittelua ei pystytty toteuttamaan, niin kaikki kulunvalvontalaitteet, pois lukien keskusyksikkö ja lukijat, on sijoitettu seinällä olevalle levylle. Oviyksiköiden väliset kytkennät on toteutettu ristikytkentärimoilla. Selkeyden vuoksi oville lähtevät kaapelit ja oviyksiköiden väliset kaapelit on sijoitettu eripuolille seinää. Kuvassa 13 näkyvät kaikki seinälle asennetut Hedsam ja HHL-tuotteet.



Kuva 13. Kulunvalvonta ja rikosilmoitin Laitesijoittelu.

4.4.1 Hedsam Novitas

Hedsam Novitas on Hedengren Securityn Hedsam-kulunvalvontaperheen uusin versio. Novitasta pystytään käyttämään selaimella, joka helpottaa järjestelmän hallintaa. Kulunvalvonnan ovet liitetään verkkoon keskittimellä, joka mahdollistaa käytännössä hajautetun kulunvalvontajärjestelmän. Tähän samaan keskittimeen liitetään HHL-rikosilmoitinkeskus. Oviympäristöjen kaapeloinnissa voidaan hyödyntää olemassa olevia lähiverkkoja. Novitaksessa on myös mahdollista käyttää matkapuhelinta kulkutunnisteena, jolloin järjestelmä tunnistaa henkilön GSM-numeron perusteella.

4.4.2 Kulunvalvontaovet

Laboratorion kulunvalvontajärjestelmään sisältyy kolme kulunvalvontaovea. Ovet ovat liikuteltavia. Huoneen rajallisen tilan vuoksi, ovet kytketään kulunvalvonta rasioille 24 -napaisilla liittimillä, jolloin ne pystytään irrottamaan tarvittaessa helposti ja siirtämään esimerkiksi toiseen huoneeseen. Ovesta lähtevä kaapeli on tyyppiä MHS 10x2. Ovissa on toisistaan poikkeavia lukitusratkaisuja.

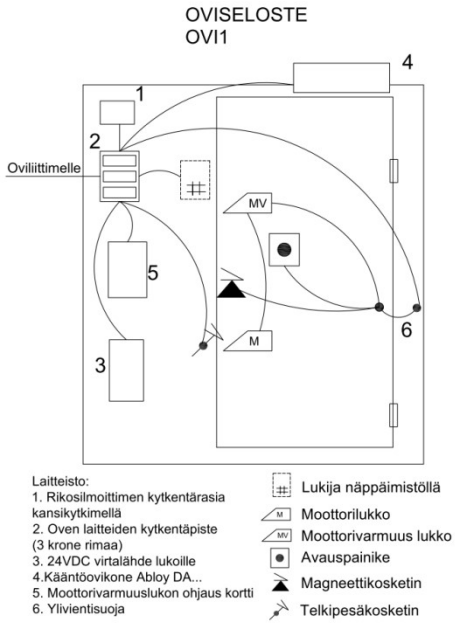
Jokaisella ovella on kolme Krone-kytkentärimaa, joihin on päätetty ovikortilta tuleva kaapeli, sekä oven laitteilta tulevat kaapelit, kuten lukon ja kääntöovikoneen kaapelit. Lisäksi jokaiseen oveen on asennettu kytkentärasia kansikoskettimella murtohälytin tietoa varten. Taulukossa 4 on ovikortilta tulevan MHS 10x2-kaapelin johtimien selitykset. Tämä ovikortilta tuleva kaapeli on jokaisessa ovessa päätetty ylimpään rimaan.

Taulukko 4. Ovelle tulevan kulunvalvontakaapelin värikoodaukset

Väri	Selite
SI	+24 VDC: jännitesyöttö lukolle, ja muille ovi ympäristön laitteille, poislukien lukijat, joille on oma jännitesyöttönsä.
SIVA	GND: jännitesyötön maa
OR	RD+: kulunvalvontalukijan jännite
ORVA	RD-: kulunvalvontalukijan jännite
VI	RD0: kulunvalvontalukijan 0 bitti
VIVA	RD1: kulunvalvontalukijan 1 bitti
RU	DO: avauspainike tieto kulunvalvonnalle
RUVA	I3: ohjelmoitava digitaalinen input
HA	I2: ohjelmoitava digitaalinen input
HAVA	I1: ohjelmoitava digitaalinen input
SI	R1: kulunvalvontalukijan ledin indikointi
SIMU	G1: kulunvalvontalukijan ledin indikointi
OR	-: DO ja I1-I3 sisääntulojen maa
ORMU	-: DO ja I1-I3 sisääntulojen maa
VI	Rele 2 NO/NC: kulunvalvonnalta saatava releteto, jolla ohjataan esimerkiksi lukkoa, releen kärki vaihdettavissa normaalisti auki tai normaalisti kiinni tilaan
VIMU	Rele 2 COM: releen yhteinen kosketin

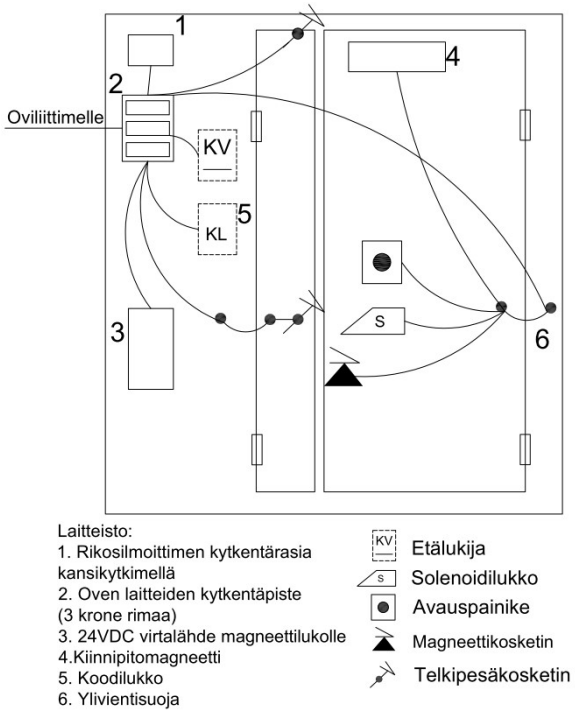
RU	Rele 1 NO/NC: kulunvalvonnalta saatava releteto, jolla ohjataan esimerkiksi lukkoa, releen kärki vaihdettavissa normaalisti auki tai normaalisti kiinni tilaan
RUMU	Rele 1 COM: releen yhteinen kosketin
HA	Hälytinlinja HHL keskukseen, johtimet jatketaan ovirasialta kulunvalvonnan runkokaapeliin
HAMU	Hälytinlinja HHL keskukseen, johtimet jatketaan ovirasialta kulunvalvonnan runkokaapeliin

Oviympäristö 1 koostuu metalliovesta, jossa on moottorilukko Abloy 8329, moottorivarmuuslukko Abloy EL651, avauspainonappi sisäpuolella sekä kääntöovikone Abloy DA300 (kuva 14). Lisäksi oven karmissa on mikrokytkintelkipesä, jonka kosketintieto välitetään ovikoneelle. Ovessa on näppäimistöllä varustettu Hedsam-kulunvalvontalukija, jolla ovi avataan ulkopuolelta. Sisäpuolelta kulku tapahtuu avauspainonappia painamalla. Oven ollessa auki asennossa kääntöovikone avaa oven myös ulkopuolen tutkalla. Myöhempää kehittelyä varten oveen voitaisiin asentaa sisäpuolelle myös jokin impulssilaite kääntöovikoneelle. Moottorivarmuuslukkoa ja moottorilukkoa varten oven karmiin on myös asennettu ohjainkortti EA400. Ohjainkortin avulla voidaan ohjata molempia lukkoja auki tai kiinni ja kortilta saadaan myös oven tilatiedot molemmilta lukoilta. Murtohälytintä varten oveen asennettiin magneettikosketin, sekä kansikytkimellä varustettu kytkentärasia, johon kytkettiin HHL:n osoitepääte. Kytkentärasiasta magneettitieto liitettiin MHS 10x2 runkokaapeliin.



Kuva 14. Oviympäristö 1

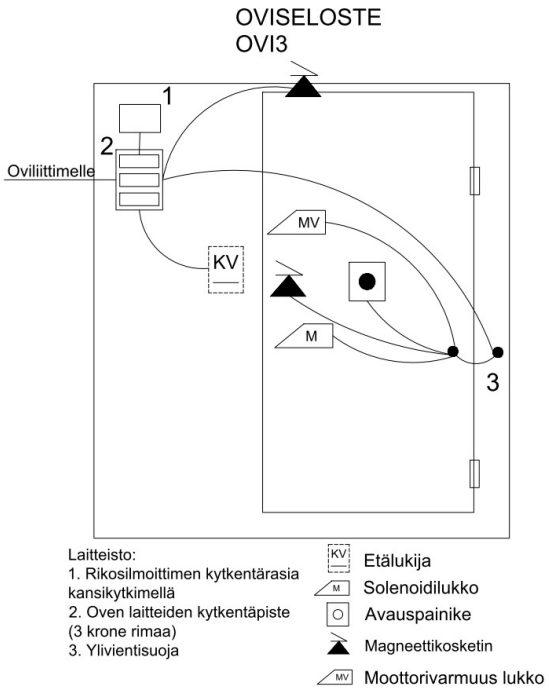
Oviympäristössä 2 on solenoidilukko Abloy EL580, sekä lisälukituksena kiinnipitomagneetti (kuva 15). Ovi avataan sisäpuolelta avauspainonapilla. Solenoidilukko voidaan avata myös sisäpuolen painikkeesta, mutta magneettilukon ollessa lukittuna, täytyy painonappia käyttää poistumiseen. Oviympäristöön voitaisiin lisätä hätäpoistumista varten rikolasi-painike, joka katkaisisi magneettilukon jännitteen. Tällöin poistuminen ovesta olisi myös mahdollista, jos avauspainike on otettu poiskäytöstä esimerkiksi aikaohjelmalla. Ovessa on myös magneettikosketin, josta kulunvalvonta saa oven auki/kiinni tiedon. Lukitustieto kulunvalvonnalle saadaan solenoidilukon telkitiedosta. Oveen on liitetty kulunvalvontalukija ilman näppäimistöä, jolla ovi voidaan avata sähköisesti. Kulunvalvontalukijan lisäksi oveen on myös liitetty koodilukko, joka myös antaa avausimpulssin kulunvalvonnalle ja sieltä edelleen lukolle. Kuten ovessa yksi, myös ovesta kaksi viedään tieto rikosilmoittimelle. Tässä ovessa käytetään hälytystietona karmin telkipesäkosketinta, josta telkitieto kaapeloidaan kytkentärasian kautta runkokaapelointiin.



Kuva 15. Oviympäristö 2

Kolmannessa oviympäristössä on moottorilukko 8329 sekä moottorivarmuuslukko EL655 (kuva 16). Ovi avataan sisäpuolelta avauspainonapilla ja ulkopuolelta kulunvalvonta lukijalla. Moottorivarmuuslukkoa ohjataan EA450 ohjauskortin kautta kulunvalvonnalla. Moottori-

lukkoa ohjataan suoraan kulunvalvonnalla. Ovessa on magneettikosketin kulunvalvonnan tilatietoa varten. Lukitustieto saadaan käyttölukon telkitiedosta, sekä varmuuslukon ohjauskortilta. Myös tähän oviympäristöön on asennettu erillinen magneettikosketin ja kytkentärasia, rikosilmoitinta varten.



Kuva 16. Oviympäristö 3

4.5 Rikosilmoittimen päivitys

Laboratoriossa on kaksi rikosilmoitinjärjestelmää. OUMAN-järjestelmä säilytettiin entisellään omana järjestelmänä. Sen sijaan HHL-16-rikosilmoitinkeskus täytyy päivittää uudempaan HHL-versioon, koska HHL-16 ei tue Hedbus-väylä protokollaa. HHL keskustelee Hedbus-väylän kautta CC:n kanssa. CC-keskitin yhdistää rikosilmoittimen verkkoon ja mahdollistaa muun muassa ryhmäohjaukset kulunvalvonnan ohjelmistolla.

Hälytinjärjestelmään lisättiin jokaiselta ovelta kosketintieto, jolloin pystytään simuloimaan hälyttimen käyttöä myös kulunvalvontaovilta. Ovien magneettikoskettimet toimivat kuorivalvonnan tavoin. Lisäksi kulunvalvonnan oviyksiköitten kansisuojat kytketään rikosilmoittimeen, näin saadaan hälytys jos kansia avataan luvattomasti. HHL-rikosilmoittimen sarjaporttiliitäntä kytketään Hedsamin keskittimeen Hedbus-väylällä, josta tiedot välittyvät yhdessä kulunvalvonta tietojen kanssa keskusyksikölle.

4.6 Kameravalvonnan päivitys

Vanhassa laboratoriossa oli useampi käytössä oleva kameravalvontajärjestelmä. Ongelmaksi vanhoissa järjestelmissä muodostui ohjelmistot, jotka olivat Windows XP- tai Linux-pohjaisia. Tästä syystä laboratorioon hankittiin uusi kameravalvontajärjestelmä. Järjestelmän valinnassa päädyttiin Mirasys-verkkotallentimeen, koska tällöin eripuolella laboratoriotiloja sijaitsevat kamerat saadaan lähiverkon kautta kytkettyä tallentimeen. Lisäksi Mirasys-järjestelmän integraatiomahdollisuus kulunvalvonta- ja rikosilmoitinlaitteistojen kanssa oli ratkaiseva tekijä. Mirasys-järjestelmä tulee valmiina pakettina, joka sisältää valmiiksi asennetun serverikoneen lisensseineen. Kameroita ja muita kameravalvonnan kenttälaitteita laboratoriossa oli jo entuudestaan riittävästi, joten niitä ei päivityksessä tarvinnut hankkia lisää.

Kameroita oli sekä IP- ja analogi-kameroita. IP-kamerat liitettiin suoraan tallentimen verkkoon ja analogi-kamerat olemassa olevien video servereitten avulla.
Kamerajärjestelmän päivityksessä on huomattava, että laitteiden tulee olla samassa aliverkossa kulunvalvonta ja rikosilmoitin järjestelmän kanssa, että integraatio toimii.

4.7 Dokumentointi

Koska kyseessä on oppimisympäristö niin kaikki kytkentä- ja sijoituskuvat ovat käyttäjien käytössä. Normaalissa tilanteessa nämä dokumentit pitäisi säilyttää suojatussa paikassa. Kytkentäkuvien avulla järjestelmän rakenne on mielestäni helpompi ymmärtää, sekä myöhemmässä vaiheessa vikatilanteiden selvittely helpottuu. Liitteenä on jokaisen oven risti-

kytkentäkuvat. Loput dokumentointiin tarvittavat kuvat on toimitettu suoraan toimeksiantajalle.

5 Yhteenveto

Opinnäytetyön tarkoituksena oli tehdä suunnitelmat toimitilaturvallisuuden laboratorion päivitykselle. Aihetta päivitykselle antoi laboratorion siirtäminen uusiin tiloihin, sekä se että laitteisto oli osin vanhentunutta. Lisäksi integraation lisääminen järjestelmien välille vaati eri järjestelmäosien päivitystä.

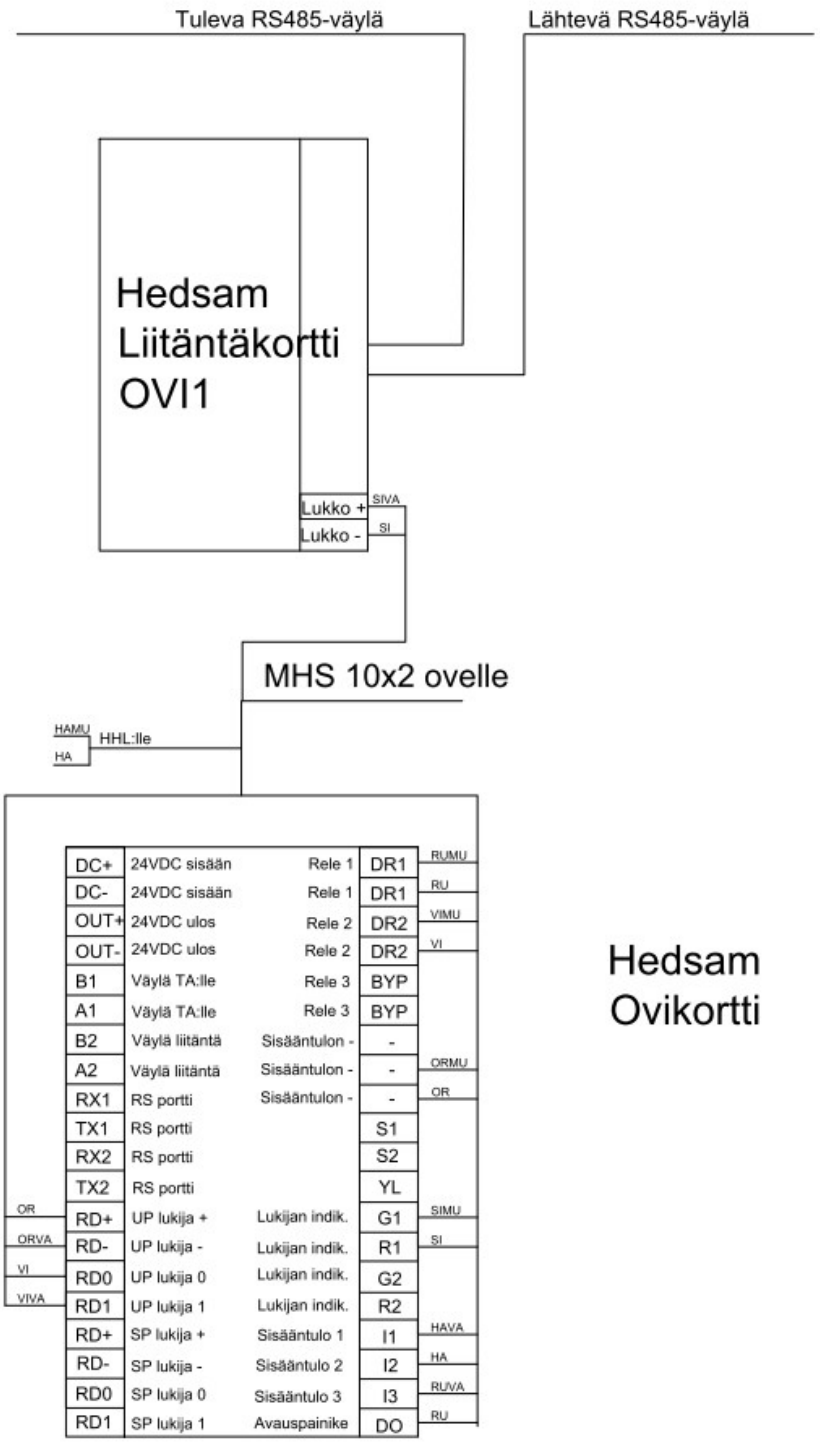
Aloitin työni perehtymällä huolellisesti olemassa olevaan laboratorioon sekä sen laitteisiin. Tämän vaiheen tarkoituksena oli saada käsitys siitä, että mitkä laitteista olivat toimintakelpoisia. Testasin muun muassa rikosilmoittimen ja oviympäristön tuotteiden toiminnat. Tässä vaiheessa päätin jo olla puuttumatta osaan järjestelmistä, joitten päivitys ei mielestäni ollut tarpeellista uutta integroitua kokonaisuutta ajatellen. Nämä järjestelmät siirrettiin sellaisenaan uuteen laboratoriotilaan. Rajausta oli välttämätöntä tehdä myös sen takia, ettei aika riittänyt suunnitella kaikkia järjestelmiä.

Toisessa vaiheessa lähdin suunnittelemaan uutta integroitua kulunvalvonta-, rikosilmoitin- ja kamerajärjestelmää. Kartoittaessani eri järjestelmävaihtoehtoja konsultoin hälytinlaitevalmistajia mahdollisuuksista järjestelmän toteuttamiseen. Järjestelmävalintoja tehdessä myös projektin kustannukset olivat yksi kriteeri uuden järjestelmän valintaan. Tästä syystä päädyin Hedsam Novitas-kulunvalvontaan ja HHL-rikosilmoittimeen, koska vanhoja laitteita pystyttiin hyödyntämään mahdollisimman paljon. Mirasys-kamerajärjestelmän valintaan päädyin, siksi että sen yleisyyden takia integraatio mahdollisuudet ovat hyvät.

Järjestelmävalintojen jälkeen piirsin kaapelointi- ja sijoittelukuvat laboratorioon. Näiden perusteella asensin laitteet yhteistyössä koulun oppilaiden ja henkilökunnan kanssa. Käyttöönotto ja järjestelmien ohjelmointi sekä käytönopastus jäi opinnäytetyön ulkopuolelle, eikä sitä siksi käsitellä.

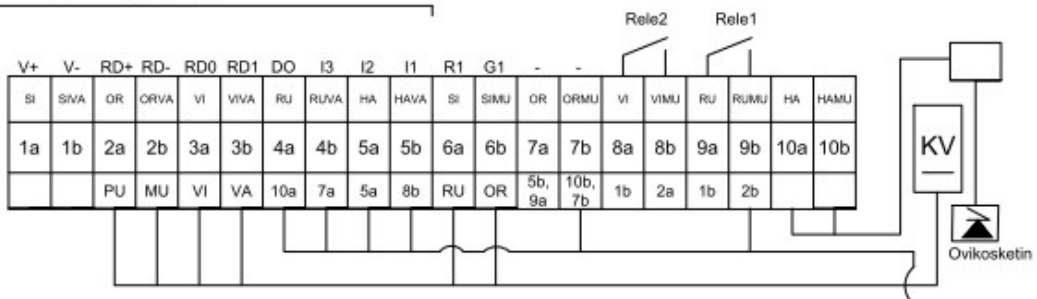
Lähteet

1. Kauppi, V. 2007. Lait, asetukset, määräykset ja ohjeet. Teoksessa Kauppi, V(toim.). Kulunvalvonta- ja rikosilmoitinjärjestelmät ST-käsikirja 11. Espoo. Sähköinfo Oy. 9-17.
2. Vuorinen, A. 2007. Turvallisuusprojektin toteutus. Teoksessa Kauppi, V(toim.). Kulunvalvonta- ja rikosilmoitinjärjestelmät ST-käsikirja 11. Espoo. Sähköinfo Oy. 22-25.
3. Leskinen, M. 2004. Toimitilaturvallisuus ja sähköiset turvallisuusjärjestelmät. Espoo. Sähköinfo Oy.
4. Hyytinen, T. 2012. Riskikartoitus. Tampereen teknillinen yliopisto. http://webhotel2.tut.fi/turvapaikka/Riskikartoitus.html. 11.2.2016.
5. Hyytinen, T. 2012. RISKIKARTOITUSTYÖKALUN KÄYTTÖOHJE. Tampereen teknillinen yliopisto. http://webhotel2.tut.fi/turvapaikka/riskikartoitusmenetelma.pdf. 11.2.2016.
6. Suomen riskienhallintayhdistys Ry, 2016. Mitä on riskienhallinta.. http://www.pk-rh.fi/. 15.2.2016.
7. Finanssialan Keskusliitto. 2008. omaisuusrikostoimikunta. Murtohälytysjärjestelmät ja –palvelut ohje 2008. Helsinki. Finanssialan Keskusliitto.
8. Vuorinen, A. 2007, Luottamuksellisuus ja asiakirjojen käsittely. Teoksessa kauppi, V(toim.). Kulunvalvonta- ja rikosilmoitinjärjestelmät ST-käsikirja 11. Espoo. Sähköinfo Oy. 26-28.
9. Sähkötieto ry, 2003. Murtoilmaisujärjestelmät. tekninen suunnitteluohje. Espoo. Sähköinfo Oy.
10. Finanssialan Keskusliitto, Turvallisuusjärjestelmien suunnittelu. Teoksessa Turvallisuusjärjestelmien suunnittelijan opiskelumateriaali. Helsinki. Finanssialan keskusliitto. Ei julkinen.
11. Vironen, V. 2007. Rikosilmoitinjärjestelmät sekä rakenteellinen murtosuojaus. Teoksessa Kauppi, V(toim.). Kulunvalvonta- ja rikosilmoitinjärjestelmät ST-käsikirja 11. Espoo. Sähköinfo Oy. 77-78.
12. Lekinen, M. 2007. Asennus. Teoksessa Kauppi, V(toim.). Kulunvalvonta- ja rikosilmoitinjärjestelmät ST-käsikirja 11. Espoo. Sähköinfo Oy. 106-108.
13. Leskinen, M. 2007. Kulunvalvontajärjestelmät. Teoksessa Kauppi, V(toim.). Kulunvalvonta- ja rikosilmoitinjärjestelmät ST-käsikirja 11. Espoo. Sähköinfo Oy. 41-45.
14. Laki yksityisyyden suojasta 759/2004
15. Henkilötietolaki 523/1999
16. Sähkötieto ry, 2016. Kulunvalvonta- ja työajanseurantajärjestelmät. asennusohje. Espoo. Sähköinfo Oy.
17. Sähkötieto ry, 2016. Kulunvalvonta- ja työajanseurantajärjestelmät. suunnitteluohje. Espoo. Sähköinfo Oy.
18. Sähkötieto ry, 2015. Kameravalvontajärjestelmät. tekninen suunnitteluohje. Espoo. Sähköinfo Oy.
19. Turva-alan yrittäjät ry, 2011. Kameravalvontaopas. Espoo. Sähköinfo Oy.
20. Laki rikoslain muuttamisesta 531/2000.
21. Laiso, M. 2014. ADIn ja Axiksen IP-kamerakoulutus. Ei julkinen.

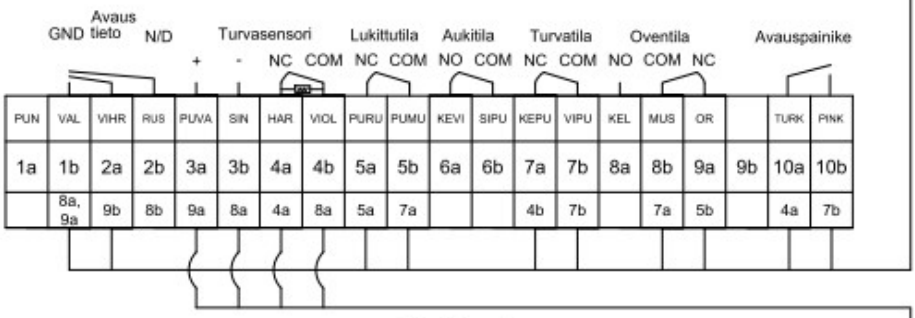

Tuleva RS485-väylä
Lähtevä RS485-väylä
Hedsam
Liitäntäkortti
OVI1
Lukko +
Lukko -
SIVA
SI
MHS 10x2 ovelle
HAMU
HA
HHL:lle
DC+ 24VDC sisään
DC- 24VDC sisään
OUT+ 24VDC ulos
OUT- 24VDC ulos
B1 Väylä TA:lle
A1 Väylä TA:lle
B2 Väylä liitäntä
A2 Väylä liitäntä
RX1 RS portti
TX1 RS portti
RX2 RS portti
TX2 RS portti
RD+ UP lukija +
RD- UP lukija -
RD0 UP lukija 0
RD1 UP lukija 1
RD+ SP lukija +
RD- SP lukija -
RD0 SP lukija 0
RD1 SP lukija 1
Rele 1 DR1
Rele 1 DR1
Rele 2 DR2
Rele 2 DR2
Rele 3 BYP
Rele 3 BYP
Sisääntulon - -
Sisääntulon - -
Sisääntulon - -
S1
S2
YL
Lukijan indik. G1
Lukijan indik. R1
Lukijan indik. G2
Lukijan indik. R2
Sisääntulo 1 I1
Sisääntulo 2 I2
Sisääntulo 3 I3
Avauspainike DO
RUMU
RU
VIMU
VI
ORMU
OR
SIMU
SI
HAVA
HA
RUVA
RU
OR
ORVA
VI
VIVA
Hedsam
Ovikortti

Ovi 1 ristikytkennät

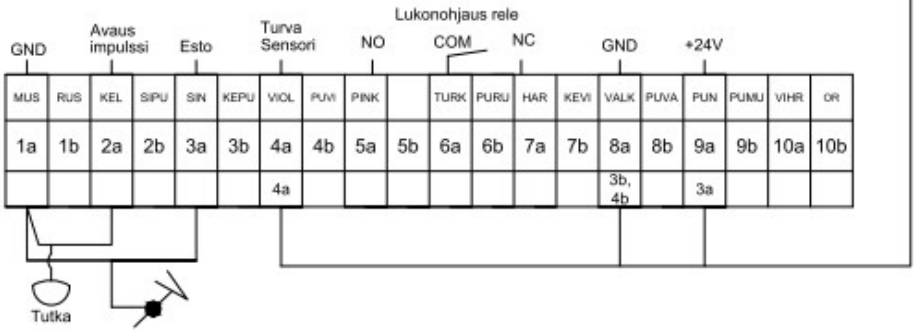
MHS 10x2 ovirasialta



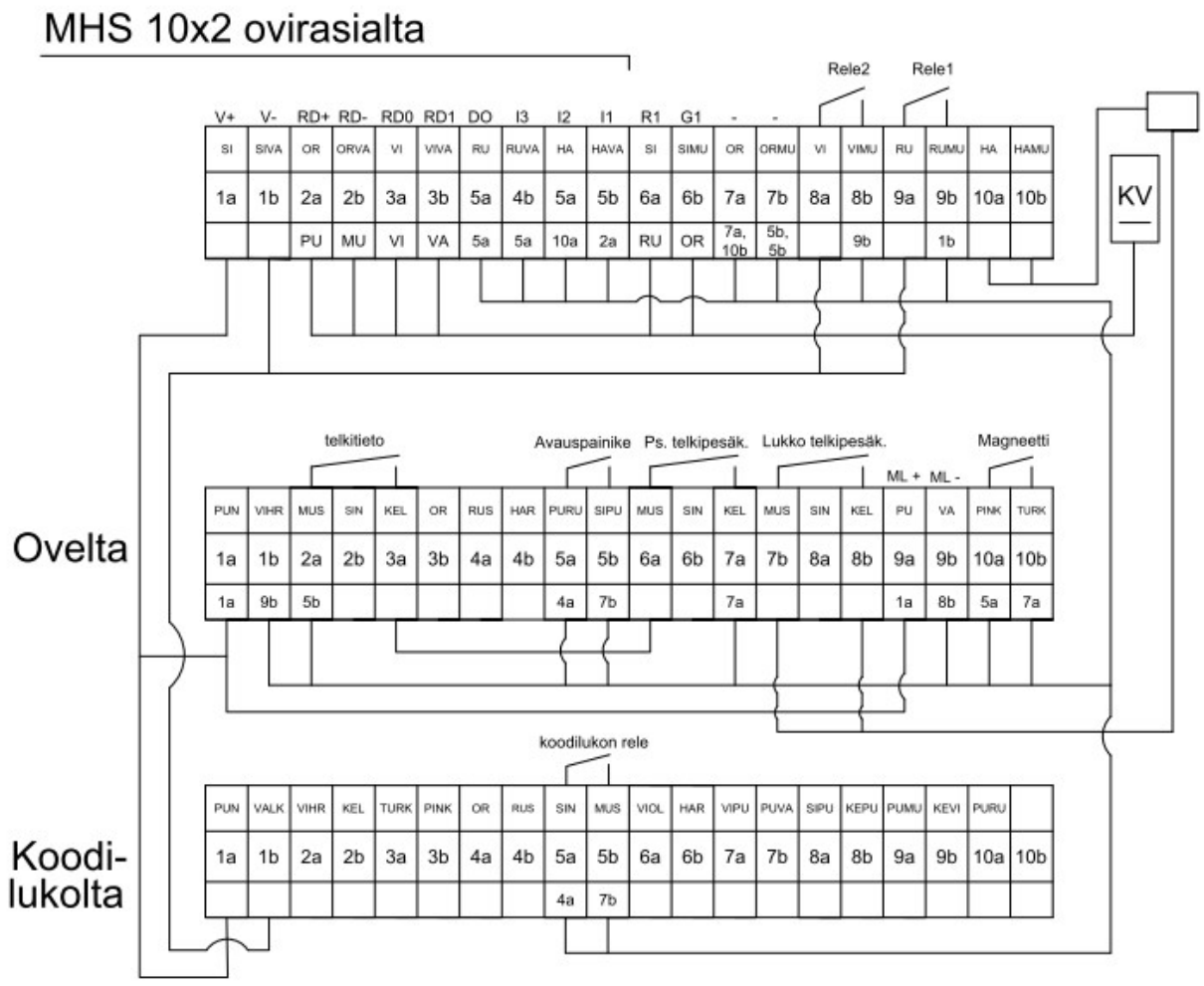
EA400



DA300



Ovi 2 ristikytkennät



Ovi 3 ristikytkennät

MHS 10x2 ovirasialta