Niko Malmivaara

Kulunvalvontajärjestelmän toteutuksen suunnittelu asuinkiinteistöön

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Automaatiotekniikka

Insinöörityö

22.2.2022

Tiivistelmä

Tekijä:	Niko Malmivaara
Otsikko:	Kulunvalvontajärjestelmän toteutuksen suunnittelu asuinkiinteistöön
Sivumäärä:	42 sivua
Aika:	22.2.2022
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Sähkö- ja automaatiotekniikka
Ammatillinen pääaine:	Automaatiotekniikka
Ohjaaja:	Lehtori Matti Välikylä

Opinnäytetyö kohdistuu kulunvalvontajärjestelmän toteutuksen suunnitteluun, jonka käyttökohteena on asuinkiinteistö. Työn kokonaisuuteen ei kuitenkaan kuulunut kulunvalvontajärjestelmän fyysinen toteutus, sillä tavoitteena oli sen suunnittelu.

Työssä käydään läpi yleistä tietoa kulunvalvonnasta ja kulunvalvontajärjestelmistä, yleisistä käyttökohteista sekä niiden tunnistamistekniikoista. Työhön sisältyy myös pääsynhallinta ja yleisimpien pääsynhallintamallien esittely. Lisäksi käydään läpi pääsynhallintamallien vahvuudet ja heikkoudet sekä niille parhaiten soveltuvat käyttökohteet. Työssä esitellään suunniteltu kulunvalvontajärjestelmä vaiheittain ja käydään läpi järjestelmän toteuttamiseen tarvittavat komponentit sekä laitteistot. Kulunvalvontajärjestelmän erityyppiset topologiat ja niiden vahvuudet sekä heikkoudet esitellään. Näiden perusteella suunnitellun kulunvalvontajärjestelmän topologia valitaan. Työ kattaa suunnitellun kulunvalvontajärjestelmän asennuksen periaatteet ja opinnäytetyön käyttökohteen ja suunnitellun kulunvalvontajärjestelmän kokonaisuuden esittelyn.

Opinnäytetyöhön sisältyy myös käyttöönotto, testaus, raportointi, ylläpito ja huolto. Työssä käydään läpi riskejä ja haasteita, joita kulunvalvontajärjestelmän toteuttamisessa sekä suunnittelussa voi esiintyä. Lisäksi työhön kuuluu olennaista lakisäädäntöä, joka on syytä ottaa huomioon kulunvalvontajärjestelmän käyttökohteen suunnittelussa ja laillisuuden varmistamisessa.

Opinnäytetyön lopputuloksena päästiin tavoitteeseen ja kerättiin tietoa kulunvalvontajärjestelmän toteutukseen tarvittavista komponenteista sekä osa-alueista. Näiden tietojen perusteella saatiin suunniteltua kulunvalvontajärjestelmän toteutus asuinkiinteistöön.

Avainsanat: kulunvalvonta, pääsynhallinta, kulunvalvontajärjestelmä, suunnittelu, toteutus, käyttöönotto, riskitekijät

Abstract

Author:	Niko Malmivaara
Title:	Planning the Implementation of an Access Control System for a Residential Property
Number of Pages:	42 pages
Date:	22 February 2022
Degree:	Bachelor of Engineering
Degree Programme:	Electrical and Automation Engineering
Professional Major:	Automation Technology
Supervisor:	Matti Välikylä, Senior Lecturer

The thesis focuses on the design of the implementation of an access control system, which is used in residential real estate. However, the work did not include the physical implementation of the access control system, as the goal of the thesis was on its design.

The work covers general information about access control and access control systems, their general applications and identification techniques. The work includes an introduction to the most common access control models. In addition, the strengths and weaknesses of the access control models and the applications that are best suited to them are reviewed. The work presents the planned access control system in stages and reviews the components and equipment needed to implement the system. The different types of topologies in the access control system are presented as well as their strengths and weaknesses. Based on these, the topology of the designed access control system is selected. The work covers the principles of the installation of the planned access control system. In addition, the presentation of the planned application and the planned access control system are included.

The thesis also includes information concerning commissioning, testing, reporting, maintenance and service. The work reviews the risks and challenges that may arise in the implementation and design of the access control system. In addition, the work includes essential legal regulations that should be paid attention to when planning and ensuring the legality of the use of the access control system.

As the result of the thesis, the goal was achieved. Information of the required components and sub-areas for the implementation of an access control system was collected. Based on the information, the implementation of the access control system for the residential property was planned.

Keywords: access control, access control system, planning, implementation, commissioning, risk factors

Sisällys

Lyhenteet

QRC: *Quick Response Code.* Pikavastauskoodi on tyyppi kaksiulotteista viivakoodia.

RFID: *Radio Frequency Identification.* Radiotaajuinen etätunnistus, jota hyödynnetään muun muassa läheisyyskulunvalvontajärjestelmissä.

PIN: *Personal Identification Number.* Salasanana käytettävä luku, jolla voidaan tunnistautua järjestelmään.

MAC: *Mandatory Access Control*. Käyttöoikeustasoihin perustuva pääsynhallintamalli.

DAC: *Discretionary Access Control*. Henkilön identiteettiin perustuva pääsynhallintamalli.

ACL: *Access Control List*. DAC-pääsynhallintamallissa käytettävä käyttöoikeusluettelo, joka sisältää käyttäjiä ja ryhmiä.

ABAC: *Attribute Based Access Control*. Attribuutteihin perustuva pääsynhallintamalli.

RBAC: *Role-Based Access Control*. Rooleihin perustuva pääsynhallintamalli.

IoT: *Internet of Things*. Pilvipalveluihin perustuva teknologia.

GAN: *Generative Adversial Network.* Koneoppimisrakenteen luokka, jossa kaksi keinotekoista hermoverkkoa kilpailee keskenään nollasummapelin muodossa.

IP: *Internet Protocol*. Sääntöjoukko, joka säätelee Internetissä tai paikallisessa verkossa lähetettyjen tietojen muotoa.

LAN: *Local Area Network.* Lähiverkko, pienellä alueella toteutettu tietoliikenneverkko.

WAN: *Wide Area Network.* Suuralueverkko, laajoja maantieteellisiä alueita peittävä tietoliikenneverkko.

NO: *Normally Open.* Kosketin, joka ei kuljeta virtaa normaalitilassaan.

NC: *Normally Closed.* Kosketin, joka kuljettaa virtaa normaalitilassaan.

DI: *Digital Input.* Digitaalisen signaalin sisääntulo, digitaalinen signaali ilmaisee vain päällä- tai poissa-tilan.

DO: *Digital Output.* Digitaalisen signaalin ulostulo. Digitaalinen signaali ilmaisee vain päällä- tai poissa-tilan.

PoE: *Power over Ethernet.* Tekniikka, jolla pystytään syöttämään sähkövirtaa ja tietoa Ethernet-kaapeloinnilla.

USB: *Universal Serial Bus.* Sarjaväyläarkkitehtuuri oheislaitteiden liittämiseksi päälaitteeseen.

WLAN: *Wireless Local Area Network.* Langaton paikallinen tietoliikenneverkko, jossa internetiin kytketty reititin toimii tukiasemana.

SDK: *Software Development Kit.* Microsoftin ohjelmistokehityssarja, joka sisältää tietoja ja työkaluja, joita tarvitaan Microsoft Windows- ja .NET Framework -sovellusten kehittämiseen.

GDPR: *General Data Protection Regulation.* Yleinen tietosuoja-asetus, henkilötietojen käsittelyä sääntelevä laki kaikissa EU-maissa.

EMI: *Electromagnetic Interference.* Ulkoisen lähteen synnyttämä häiriö, joka vaikuttaa sähköpiiriin sähkömagneettisen induktion, sähköstaattisen kytkennän tai johtumisen kautta.

EMC: *Electromagnetic Compatibility.* Laitteen tai järjestelmän sähkömagneettinen yhteensopivuus.

DSP: *Digital Signal Processor.* Suoritin, joka on erityisesti suunniteltu digitaalista signaalinkäsittelyä varten.

1 Johdanto

Opinnäytetyössä keskityttiin suunnittelemaan kulunvalvontajärjestelmän toteutus asuinkiinteistöön. Työn asuinkiinteistöksi valittiin omakotitalo, sillä se on käyttökohteena realistinen ja lakisääteisesti suoraviivaisin toteuttaa. Kulunvalvontajärjestelmän ideana on luoda kulunvalvonta omakotitalon pää- ja takaovelle älylukijoita ja älykkäitä konenäkökameroita hyödyntäen. Fyysistä kulunvalvontajärjestelmän toteutusta ei kuitenkaan tässä opinnäytetyössä tehdä, vaan painopisteenä ja ideana on sen suunnittelu.

Työssä keskitytään lisäksi myös hieman laajemmin automaation käyttökohteeseen eli turvallisuuteen. Työn turvallisuuskokonaisuuteen liittyy kulunvalvonta sekä kulunvalvonnassa käytettävät eri kulunvalvontajärjestelmät. [1.] Erityisesti yritysten kulunvalvontaan liittyy keskeisesti myös pääsynhallinta, joka tarkoittaa fyysisessä turvallisuudessa ja tietoturvassa rajoitettua valikoivaa pääsyä paikkoihin tai tiettyihin resursseihin. [2.] Lisäksi työssä käydään pintaraapaisuna kulunvalvontajärjestelmän toteutuksessa olevia mahdollisia riskejä ja haasteita sekä hieman olennaisia lakisäädöksiä.

2 Kulunvalvonta

Kulunvalvonta tarkoittaa fyysistä pääsynhallintaa, kulunvalvontaa käytetään muun muassa asuinkiinteistöissä, yrityksissä ja teollisuudessa. Asuinkiinteistöissä kulunvalvonta usein perustuu kameravalvontaan ja ovien kulunvalvontajärjestelmiin. Yrityksissä ja teollisuudessa voidaan käyttää useampia eri kulunvalvontajärjestelmiä riippuen käyttökohteesta ja suojaustason vaatimuksista. Kulunvalvonnan yleinen syy on asiattomien henkilöiden kulun estäminen. [1.]

Koska turvallisuus ja fyysinen yksityisyyden suojaus on hyvin tärkeää maailmanlaajuisesti, kulunvalvontajärjestelmien valmistajia ja käytössä olevia kulun-

valvontajärjestelmiä on monia eri käyttökohteisiin. Näitä ovat esimerkiksi yritys-käyttöön tai teollisuuteen suunnitellut kulunvalvontajärjestelmät, joihin liittyy usein myös pääsynhallinta yrityksen tietoihin [2]. Tapahtumiin ja julkisiin tiloihin on suunniteltu kulunvalvontajärjestelmiä, jossa voi olla muun muassa sisällytettynä QR-koodin (Quick Response Code) tai viivakoodin lukija [3]. Ajoneuvojen tunnistamiseen on siihen suunniteltuja kulunvalvontajärjestelmiä, joihin yleensä kuuluu rekisterikilven automaattinen tunnistus [4]. Lisäksi asuinkiinteistöihin on olemassa siihen suunnitellut kulunvalvontajärjestelmät, joissa ovien lukituksen avaus tapahtuu esimerkiksi tunnisteella, PIN-koodilla tai älypuhelimella [5].

Tunnettuja ja maailmanlaajuisesti arvostettuja kulunvalvontajärjestelmäratkaisujen tarjoajia ovat muun muassa Assa Abloy, Johnson Controls, Dormakaba Holding, Allegion, HID-Global, IDEMIA, Safran Group, NEC Corporation, Identiv. [6.]

Kulunvalvontajärjestelmiä on saatavilla paikallisina sekä pilvipohjaisina, jolloin kulunvalvontajärjestelmä toimii tallentamalla tiedot pilveen paikan päällä olevan palvelimen sijaan, eli tällöin pilvi isännöi ohjelmistoa. Pilvipohjaisen kulunvalvontajärjestelmän tietoihin ja käyttäjien käyttöoikeuksiin voidaan tehdä muutoksia verkkoportaalin kautta millä tahansa laitteella, jossa on Internet-yhteys. [7.] Kulunvalvontajärjestelmien toiminta perustuu useimmiten joko biometriseen järjestelmään, läheisyysjärjestelmään tai ovien kulunvalvontajärjestelmään.

2.1 Biometrinen kulunvalvontajärjestelmä

Biometrinen kulunvalvontajärjestelmä perustuu yksilöiviin fysiologiaan perustuviin ihmisen ominaisuuksien tunnistamiseen. Biometrisia tunnistautumistapoja ovat muun muassa sormenjälkitunnistus, kasvojentunnistus ja iiristunnistus. [8.] Näistä vaihtoehdoista yleisin on sormenjälkitunnistus sen asettamisen helppouden ja kätevyyden takia. Biometrinen kulunvalvontajärjestelmä voidaan asettaa seuraamaan ja tallentamaan vieraiden ja työntekijöiden tai käyttäjien tietoja käyttöohjelmistonsa kautta. Biometrista kulunvalvontajärjestelmää käytetään

laajalti luottamuksellisissa paikoissa, sillä asennus on yksinkertaista ja sillä saavutetaan korkea turvallisuustaso. [9.]

2.2 Läheisyyskulunvalvontajärjestelmä

Läheisyyskulunvalvontajärjestelmä on luottamuksellisempi kulunvalvontajärjestelmä ja on yksi suosituimmista käytössä olevista kulunvalvontajärjestelmistä. Läheisyyskulunvalvontajärjestelmä koostuu kolmesta komponentista: läheisyyslukijasta, läheisyystunnisteesta ja antenneista tunnisteessa ja lukijassa. Lisäksi verkkojärjestelmä tai verkko-ohjelmisto kuuluu järjestelmään, mikäli käytössä on useampi kuin yksi lukija. Järjestelmä toimii langatonta teknologiaa hyödyntäen, jolloin kulunvalvonta laitteisto pystyy olla vuorovaikutuksessa läheisyyskortin kanssa, jolla esimerkiksi ovien tai portaalien lukitustila saadaan muutettua halutuksi. Järjestelmän toiminta perustuu matalataajuiseen RFID-tekniikkaan (Radio Frequency Identification), jonka toimintataajuus on 120 kHz:n alueella. Läheisyyskulunvalvontajärjestelmän tyypillisiä käyttökohteita ovat muun muassa toimistot, tehtaat ja pankit. [9; 10.]

2.3 Ovien kulunvalvontajärjestelmä

Ovien kulunvalvontajärjestelmä on kompakti ja edullinen toteuttaa. Lisäksi järjestelmä toimii itsenäisesti. Se on käyttövalmis ja yksinkertainen asentaa. Ovien kulunvalvontajärjestelmän ohjaimia voidaan tarvita useampia suuriin kohteisiin, jolloin ne voivat olla toiminnassa linkitettyinä tai standardoituina organisaation koon ja erilaisten turvallisuustasojen perusteella. Kulunvalvontajärjestelmään sisällytettyjen ovien avaus voi tapahtua esimerkiksi tunnisteella, PIN-koodilla (Personal Identification Number) tai älypuhelimella [5]. Elektronisten ovilukkojen lisäksi saatavilla on kulunvalvontaan käytettäviä ohjaimia ja magneettisia ovilukkoja, joissa on keskeytymätön virtalähde. Ovien kulunvalvontajärjestelmän tyypillisiä käyttökohteita ovat muun muassa toimistot, palvelinhuoneet, asuinkiinteistöt, lentokentät, armeija ja tietokeskukset. [9.]

3 Pääsynhallinta

Kulunvalvonta liittyy pääsynhallintaan, joka sisältää fyysisen sekä tietoturvan valikoivan pääsyn paikkaan tai resurssiin. Esimerkiksi tietokannoissa käytetään usein pääsynhallintaa, jolla pystytään rajoittamaan henkilömäärää, jolla on oikeus päästä käsiksi tietyn turvaluokituksen tietoihin. Pääsynhallinnalla voidaan myös rajata käyttäjien tietyt käyttöoikeudet, kuten mahdollisuus katsoa, luoda tai muokata tiedostoja. [2.]

Tässä osiossa käydään läpi käytössä olevia yleisempiä eri pääsynhallintamalleja sekä niiden vahvuuksia ja heikkouksia. Osiossa ehdotetaan niiden mahdolliset parhaat käyttökohteet pääsynhallintamallien ominaisuuksien mukaan. [2.]

3.1 MAC

MAC (Mandatory Access Control) rajoittaa yksittäisten käyttäjien mahdollisuuksia myöntää tai estää pääsy tiedostojärjestelmän resursseihin tietojen luottamuksellisuuden ja käyttöoikeustasojen perusteella. Järjestelmänvalvoja määrittää MAC-kriteerit ja käyttöjärjestelmä noudattaa niitä tiukasti. MAC:ia pidetään usein pääsynhallintamalleista kaikista turvallisimpana. Tavalliset käyttäjät eivät voi vaikuttaa suojausattribuutteihin edes tiedoissa, jotka he ovat luoneet. MAC:ia käytetään hallitustasolla suojaamaan turvaluokiteltua tietoa ja tukemaan monitasoisia suojauskäytäntöjä ja -sovelluksia. Muita käyttäjäkohteita ovat hallitusjärjestöt, armeijat ja lainvalvontalaitokset. Vahvuuksina MAC-kulunvalvontamallilla on korkean tason tietosuoja ja manuaalisesti asetettavat käyttöoikeustasot sekä immuunius Troijan hevonen -virusten hyökkäyskohteeksi, sillä käyttäjät eivät voi poistaa tietojen luokitusta tai jakaa pääsyä turvaluokiteltuihin tietoihin. MAC:n heikkouksia on ylläpidettävyys, sillä asetukset ja selvitykset tehdään manuaalisesti, skaalautuvuus, sillä MAC ei skaalaudu automaattisesti eikä MAC ole käyttäjäystävällinen, koska käyttäjien on pyydettävä pääsyä jokaiseen uuteen tietoon eivätkä he voi määrittää pääsyparametreja omille tiedoilleen. [11; 12.]

3.2 DAC

DAC (Discretionary Access Control) eli harkinnanvarainen pääsynhallinta on identiteettiin perustuva pääsynhallintamalli, joka tarjoaa käyttäjille tietyn määrän hallintaa heidän tietoihinsa. Tietojen omistajat tai käyttäjät, joilla on oikeus hallita tietoja, voivat määrittää käyttöoikeudet tietyille käyttäjille tai käyttäjäryhmille. Kaikkien tietojen käyttöoikeudet tallennetaan käyttöoikeusluetteloon eli ACL:aan (Access Control List). ACL voidaan luoda automaattisesti, kun käyttäjä myöntää käyttöoikeuden jollekin, tai järjestelmänvalvoja voi luoda sen. ACL sisältää käyttäjiä ja ryhmiä, joilla on niihin sidonnaiset tieto- ja käyttöoikeustasot. Järjestelmänvalvoja voi pakottaa ACL-luettelon, jolloin ACL toimii suojauskäytäntönä, eivätkä tavalliset käyttäjät voi muokata tai ohittaa sitä. Hyviä käyttökohteita DAC:lle on pienemmät yritykset, joilla on rajoitettu IT-henkilöstö ja kyberturvallisuusbudjetti. Vahvuuksia DAC:lla on käyttäjäystävällisyys, sillä käyttäjät voivat hallita ja päästä käsiksi heidän ja toisten tietoihin. DAC on joustava kulunvalvontamalli, sillä käyttäjät voivat konfiguroida tiedonpääsyparametreja ilman järjestelmänvalvojaa. DAC on kulunvalvontamallina helppo ylläpitää, sillä uusien objektien tai käyttäjien lisäys on helpompaa. Heikkouksina on matalampi tiedonsuoja, sillä DAC ei pysty varmistamaan luotettavaa suojaa, koska käyttäjät voivat jakaa heidän tietojaan kuten haluavat. DAC voi olla myös epäselvä pääsynhallintamalli suuremmissa käyttökohteissa, sillä keskitettyä pääsynhallintaa ei ole, joten pääsyparametrien selvityksessä täytyy tarkistaa jokainen ACL. [11; 12.]

3.3 ABAC

Attribuuttipohjainen pääsynhallinta ABAC (Attribute Based Access Control) on pääsynhallintamalli, joka arvioi pääsyn määrittämiseksi attribuutteja tai ominaisuuksia roolien sijaan. ABAC:n tarkoitus on suojata objekteja, kuten dataa, verkkolaitteita ja IT-resursseja luvattomilta käyttäjiltä, joilla ei ole organisaation suojauskäytäntöjen mukaisia hyväksyttyjä ominaisuuksia. ABAC on loogisen pääsynhallinnan muotona tullut tunnetuksi viimeisen vuosikymmenen aikana, se on kehittynyt yksinkertaisemmista kulunvalvontaluetteloista ja roolipohjaisesta

pääsynhallinnasta eli RBAC:sta (Role-Based Access Control). ABAC:n vahvuuksia ovat joustavuus. Kulunvalvontamallina se usein mahdollistaa käyttää suurinta määrää resursseja ilman, että järjestelmänvalvojien on määritettävä suhteita kohteiden ja objektien välille. Heikkouksina on suunnittelun ja toteutuksen monimutkaisuus, joka on aikaa ja resursseja vievää. ABAC:n hyviä käyttökohteita ovat suuremmat yritykset, joissa on suuri käyttäjämäärä ja halu edistyksellisille pääsynhallintaominaisuuksille, sekä aikaa investoida työläämpään mutta hyödylliseen kulunvalvontamalliin, sekä jos on varmistettava yksityisyyden ja turvallisuuden noudattaminen. [13; 12.]

3.4 RBAC

RBAC on roolipohjainen pääsynhallintamalli, joka rajoittaa verkkoon pääsyä henkilön roolin perusteella organisaatiossa. RBAC on yksi edistyneen pääsynhallinnan tärkeimmistä menetelmistä [12]. RBAC:n roolit ovat sidoksissa työntekijöiden verkkoon pääsyn tasoihin. Työntekijöillä on oikeus ainoastaan tietoihin, jotka ovat tarvittavia heidän työtehtävien suorittamisen kannalta. Pääsyn tasoihin voivat vaikuttaa muun muassa toimivalta, vastuu sekä työpätevyys. Pääsy voidaan rajata tiettyihin toimintoihin kuten pääsyoikeus joko katsoa, luoda tai muokata tiedostoa. RBAC:n käyttäminen auttaa suojaamaan yrityksen arkaluontoiset tiedot ja tärkeät sovellukset. Vahvuuksia RBAC:ssa on hallinnollisen työn ja IT-tuen tarpeen vähentäminen. Roolien vaihto voidaan tehdä nopeasti ja ottaa ne käyttöön maailmanlaajuisesti käyttöjärjestelmissä, alustoissa ja sovelluksissa. Toisena vahvuutena on toiminnan tehokkuuden maksimointi, sillä lähestymistapa on virtaviivaistettu ja looginen, koska kaikki roolit voidaan kohdistaa yrityksen organisaatiorakenteeseen ja käyttäjät voivat tehdä työnsä tehokkaammin ja itsenäisemmin. Lopuksi vahvuutena on vielä paranneltu vaatimustenmukaisuus. Kaikki organisaatiot ovat liittovaltion, osavaltion ja paikallisten määräysten alaisia. Kun RBAC-järjestelmä on käytössä, yritykset voivat helpommin täyttää lakisääteiset yksityisyyttä ja luottamuksellisuutta koskevat vaatimukset, koska IT-osastoilla ja johtajilla on mahdollisuus hallita, miten dataa käsitellään ja käytetään. [14.] Heikkouksia RBAC:ssa on se, ettei sääntöjä pysty

määrittelemättömään käyttämällä järjestelmälle tuntemattomia parametreja ennen käyttäjän työskentelyn aloittamista. Käyttöoikeudet voidaan määrittää vain käyttäjärooleille, ei objekteille tai toiminnoille. RBAC:n avulla voidaan rajoittaa pääsyä tiettyihin toimintoihin järjestelmässä, mutta ei tiettyihin tietoihin. Käytännöllisimpiä käyttökohteita RBAC:lle ovat pienet ja keskisuuret yritykset, sillä hyötyjä on monia ja käyttöönotto on pienemmässä mittakaavassa helpompaa. [15.] ABAC on suunniteltu korvaamaan RBAC, muun muassa pääsynhallinnan joustavuuden parantamiseksi [13].

4 Kulunvalvontajärjestelmän toteutus

Opinnäytetyön pääaiheena on omakotitaloon sijoitettava kulunvalvontajärjestelmä. Siksi opinnäytetyöhön valittu järjestelmä on malliltaan paikallinen ovien kulunvalvontajärjestelmä asennuksen yksinkertaisuuden, edullisuuden, luotettavuuden, järjestelmän itsenäisen toimivuuden, toiminnan nopeuden sekä yleisesti asuinkiinteistöihin sopivuuden vuoksi. Kulunvalvontajärjestelmään sisältyy teknisenä lisäominaisuutena konenäköjärjestelmä, joka koostuu kasvojentunnistuksesta ja geometrisesta tunnistamisesta älykkäiden konenäkökameroiden ja konenäkösovelluksen avulla.

Toteutus on jaoteltu seuraavasti; kulunvalvontajärjestelmän komponenttien tai laitteiston esittely ja niiden tarpeellisuuden selitys sekä kulunvalvontajärjestelmän eri topologioiden esittely. Osiossa 4.1 käydään läpi järjestelmän asennusvaiheet, jonka jälkeen siirrytään järjestelmän käyttöönottoon, testaukseen, raportointiin sekä ylläpitoon ja huoltoon liittyviin asioihin.

4.1 Tarvittavat järjestelmän osat

Tässä osiossa on listattu kulunvalvontajärjestelmän toteutukseen tarvittavat komponentit ja laitteistot. Tämän lisäksi on selitetty komponenttien ja laitteistojen tarkoitus ja tarpeen syy.

4.1.1 Tunniste

Tunnisteella mahdollistetaan pääsy haluttuun paikkaan. Tämä voi olla esimerkiksi pääsykortti, henkilötunnus, biometrinen attribuutti tai älypuhelin [16]. Jokaisella tunnisteella on oma yksilöllinen koodinsa, jonka avulla voidaan hallita jokaisen yksittäisenkin henkilön kulkuoikeuksia ja kytkeä pääsy päälle tai pois eri aikoina tai rakennuksen eri osissa [17].

4.1.2 Lukija

Lukija on esimerkiksi kortinlukija, näppäimistö tai biometrinen skanneri. Lukija mahdollistaa järjestelmän havainnoida tunnisteen tiedot ja vertaa niitä tietokannassa oleviin tietoihin. [16.] Lukijat asennetaan yleensä oveen tai oven viereen, joten silloin kulunvalvontajärjestelmän sisältämien lukijoiden määrä on riippuvainen ovien lukumäärästä, joihin rajoitettua pääsyä tarvitaan. [17.]

4.1.3 Portaali ja lukituslaitteisto

Portaali ja lukituslaitteisto mahdollistaa fyysisen kulun hallinnan. Portaaliksi sopii esimerkiksi ovi tai kääntöportti. Lukituslaitteen ja valitun portaalin tulee olla yhteensopiva. Lukituslaitteita voi olla toimintatavaltaan erilaisia, kuten esimerkiksi sähkömagneettinen lukko tai salpa. [16.]

4.1.4 Ohjain

Ohjain mahdollistaa järjestelmän käytön määriteltyjen sääntöjen mukaan ja toimii kulunvalvontajärjestelmän keskuksena. Ohjain yhdistää kaikki muut kulunvalvontajärjestelmän osat, kuten lukijat ja lukituslaitteet. [16.] Ohjain käsittelee kulunvalvontatoiminnon koko rakennuksessa, eli se tekee ensisijaisesti päätöksen oven tai lukituksen avaamisesta. Ohjainten lukumäärä määräytyy rakennuksen koon, järjestelmän koon ja järjestelmän käyttöasteen mukaan, eri ohjaimet voivat kulunvalvontajärjestelmän topologiasta riippuen olla kytköksissä toisiinsa. Ohjain asennetaan yleensä puhelin-, sähkö- tai viestintäkaappiin. [17.]

4.1.5 Kulunvalvontaohjelmisto ja käyttöliittymä

Kulunvalvontaohjelmistoa voi kuvaannollisesti ajatella koko järjestelmän aivoina. Siihen on ohjelmoitu halutut ja tarvittavat toiminnot sekä ominaisuudet, joiden perusteella ohjain suorittaa toiminnot. Kulunvalvontaohjelmisto sisältää myös järjestelmän keskustietokannan ja tiedostonhallinnan. Ohjelmisto tallentaa järjestelmän toimintaa ja kommunikoi järjestelmän ohjaimen kanssa. Kulunvalvontaohjelmisto toimii perinteisessä tietokoneessa. Yleensä tähän tarkoitukseen on käytössä yksi tietokone, johon kulunvalvontaohjelmisto on ladattu, ja se on varattu ohjelmiston kokopäiväiseen käyttöön. [17.] Ohjelmiston tietokanta pitää sisällään käyttäjätiedot, jonka avulla järjestelmä saa selville valtuudet ja valtuutusprofiilit [16]. Tietokanta voi olla paikallinen, jolloin tiedot tallennetaan paikalliselle kovalevylle tai pilvipohjainen, jolloin tiedot tallennetaan pilveen. Käyttöliittymä voi olla sovellus- tai verkkopohjainen.

4.1.6 Konenäkökamera

Konenäkökamera on välttämätön konenäköjärjestelmän komponentti, jonka avulla järjestelmä tuottaa kuva- tai videotiedot, joiden pohjalta asetetut matemaattiset laskennat ja muut tunnistamisprosessit pystytään suorittamaan prosessorin avulla. Konenäkökameran valinnassa on hyvä huomioida kameratyyppi, kameran kuvanopeus ja resoluutio, jotta kameran kuvaama kuva on tarpeeksi sulava ja tarkka käyttökohdetta kohden. Optimaalisen resoluution voi laskea seuraavalla kaavalla:

$$Resoluutio = \frac{Näkökenttä}{Tarkastettavan\ ominaisuuden\ vähimmäiskoko}$$

Laajempi näkökenttä ja pienempi tarkastettavan ominaisuuden vähimmäiskoko asettaa suuremman resoluution tarpeen. [18.]

Konenäköjärjestelmässä on käytettävä siihen suunniteltuja konenäkökameroita, sillä konenäkökamerat tarvitsevat normaaleista kameroista eroavia ominaisuuksia. Näitä ovat esimerkiksi nopeampi suljinaika, suurempi kuvataajuus, laajempi

spektrialueen tuki, parempi suorituskyky ja luotettavuus, usein vaativampi ympäristöolosuhteiden kestävyys sekä pidempi käyttöaika. [18.]

Opinnäytetyön suunnitellun käyttökohteen eli omakotitalon konenäkökameroiksi valittiin älykkäät konenäkökamerat, jotta kasvojentunnistus saadaan mahdollistettua [19].

4.1.7 Konenäköjärjestelmä

Konenäössä yhdistetään useita tekniikoita, jotta kuvamateriaalin analysoinnista saavutetaan hyödyllisiä tuloksia [20]. Konenäköä hyödynnetään turvallisuustarkoituksissa tekoälyn kanssa, jolloin mahdollistetaan tehokkaampi valvontajärjestelmä, jossa on korkeampaa ohjelmoitua kohteiden havaitsemista ja seurantaa [21]. Konenäkösovellukset on perinteisesti suunniteltu tunnistamaan henkilöt heidän geometristen muotojensa perusteella, joita ovat pituus, leveys ja kehon osien mittasuhteet. Teknisenä lisänä tunnistusalgoritmissa voidaan huomioida esimerkiksi askeleen pituus ja käsivarren heilahtelun määrä, jolloin saadaan yksityiskohtaisempaa tietoa ja korkeampi tarkkuus henkilön tunnistamiseen eri kuvakulmissa, valaistuksissa ja etäisyyksissä konenäkökameraan nähden. [22.]

Konenäköjärjestelmä koostuu viidestä osa-alueesta. Nämä ovat valaistus, linssi, sensori, näön käsittely ja kommunikaatio. Valaistuksen avulla saadaan linssin kuvaamaan videokuvaan optimaalisempi valaistus, jolloin halutut yksityiskohdat tulevat kuvissa esiin paremmin. Linssi kuvaa kuvamateriaalin ja lähettää sen eteenpäin kameran sensorille valon muodossa, konenäkökameran sensori muuttaa valon muodossa saaman kuvan digitaaliseksi kuvaksi, joka lähetetään prosessorille analysoitavaksi, prosessori voi sijaita erillisessä, järjestelmään kytketyssä tietokoneessa tai älykkäässä konenäkökamerassa integroituna. Näön käsittely koostuu algoritmeista, jotka tarkistavat kuvan ja ottavat digitaalisesta kuvasta talteen tärkeän informaation, josta järjestelmä suorittaa konenäkösovelluksen avulla käyttäjän asettamat mittaukset, biometrisen ja geometrisen tunnistamisen sekä muut operaatiot, kuten hyväksymisen tai hylkäyksen päätökset

käsitellylle kuvamateriaalille. Koko prosessin lopputuloksen tieto kommunikoidaan eri laitteiden välillä. [23; 24.]

Konenäkö on suorituskyvyltään tehokkaampi kuin ihmisen näkö henkilöiden, ajoneuvojen tai muiden objektien tunnistamisessa. Konenäön GAN-tekniikalla (Generative Adversial Network) pystytään luomaan valokuvarealistisia kuvia, uudelleen kokoamaan vahingoittuneita kuvia sekä poistamaan kuvasta ulkoisesta tekijästä johtuvia epäselvyyksiä ja osittaisia hämärtymiä. [22.]

4.1.8 Kasvojentunnistus

Kasvojentunnistus on konenäköjärjestelmän ominaisuus. Kasvojentunnistuksessa hyödynnetään tekoälyä, koneoppimista sekä konenäköä. Kasvojentunnistus on osa biometrista tunnistamista, joka sisältää muun muassa sormenjäljen ja kämmenen tunnistuksen, iiristunnistuksen, kävelyn, äänen ja allekirjoituksen tunnistuksen. [25.]

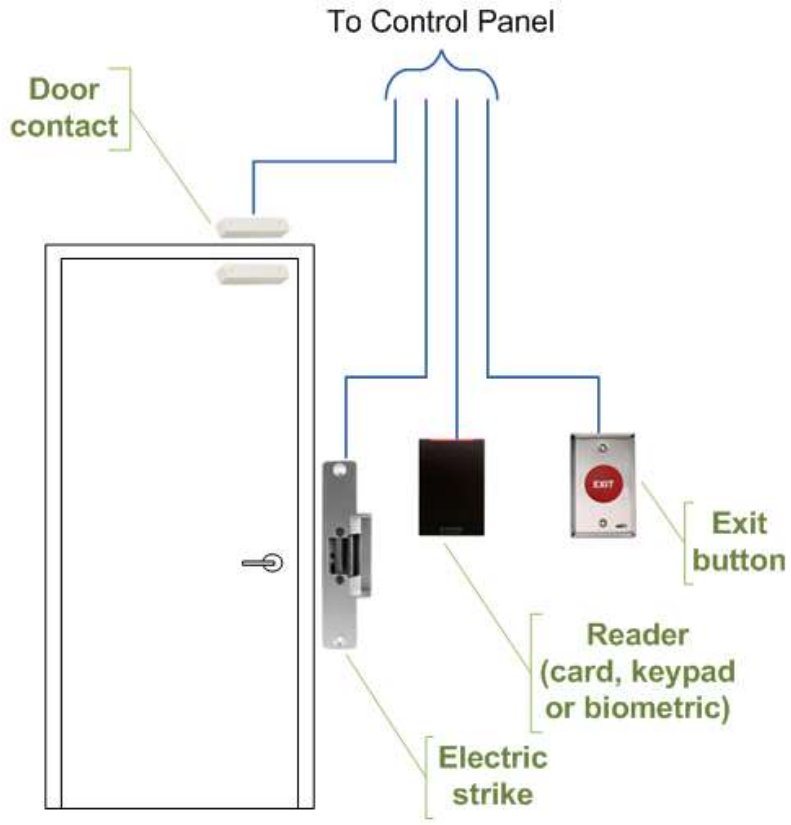
Kasvojentunnistus koostuu kasvojen tunnistamisella älykkäiden konenäkökameroiden avulla, jonka jälkeen ohjelmisto analysoi kasvojen ominaisuudet. Seuraavaksi algoritmi koodaa analysoiman kasvon esimerkiksi kaavaksi tai lukukannaksi ja vertaa sitä kulunvalvontajärjestelmän tietokantaan asetettuihin kasvoihin. Kasvojen vastatessa järjestelmän tietokantaan asetettuja kasvoja voidaan toteuttaa lisätoimenpiteitä, kuten tässä tapauksessa oven lukituksen avaus. [25.]

Julkisilla ja suurilla pilvipalveluiden tarjoajilla kuten Amazonilla, Googlella ja Microsoftilla on tarjolla yleiseen tarkoitukseen käytettäviä kasvojentunnistusratkaisuja [22].

4.2 Kulunvalvontajärjestelmän topologiat

Tässä osiossa käydään läpi kulunvalvontajärjestelmien eri topologioita sekä niiden vahvuuksia ja heikkouksia.

Kulunvalvontajärjestelmän toteutuksessa tarvitaan johdotus virransyötön ja kommunikoinnin mahdollistamiseksi. Langaton kommunikointi on myös mahdollista verkon avulla, mutta etäisyyden ja kaistanleveyden rajoitukset tekevät siitä vaikeasti toteutettavan useimmissa kulunvalvontajärjestelmän käyttökohteissa. Langattomat verkot ovat lisäksi alttiimpia jumiutumisille, jolloin tietoturvasovellukset voivat altistua todennäköisemmin tietoturvahyökkäyksille. [21.]

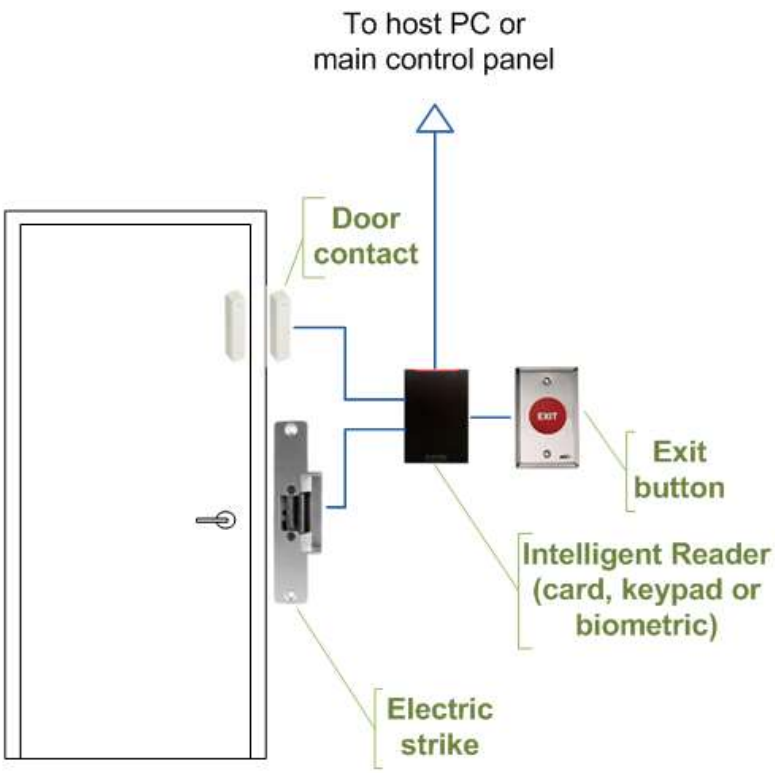


Kuva 1. Yksittäisen oven kulunvalvontajärjestelmän topologia perinteisillä lukijoilla. [26.]

Kuvassa 1 nähdään kulunvalvontajärjestelmän yksittäisen oven topologia, mikäli toteutus tehdään perinteisillä lukijoilla.

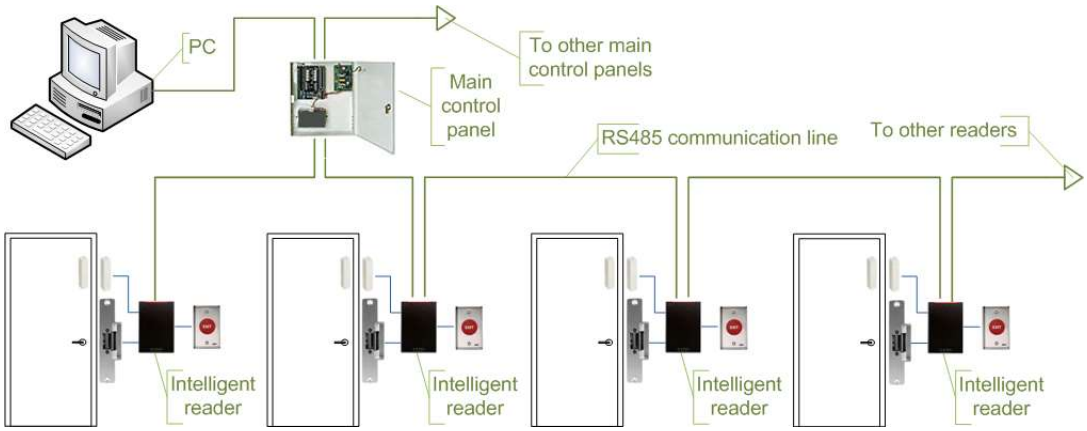
Kulunvalvontajärjestelmän yksittäisen oven topologiasta saadaan kompaktimpi, kun käytetään älylukijoita kuvan 2 mukaisesti. Tällöin asennuksessa tarvitsee käyttää vähemmän sähköjohtoa. Älylukijoihin sisältyy älykkäät ja puoliälykkäät lukijat, joissa on kummassakin kaikki sisääntulot ja lähdöt, joita tarvitaan oven

laitteiston ohjaamiseen. Älylukijat voivat tarvittaessa tehdä kulun päätökset itsenäisesti, kun taas puoliälykkäät lukijat lähettävät tiedon pääohjaimelle ja odottavat sen vastausta. [27.]



Kuva 2. Yksittäisen oven kulunvalvontajärjestelmän topologia älylukijoita hyödyntäen. [28.]

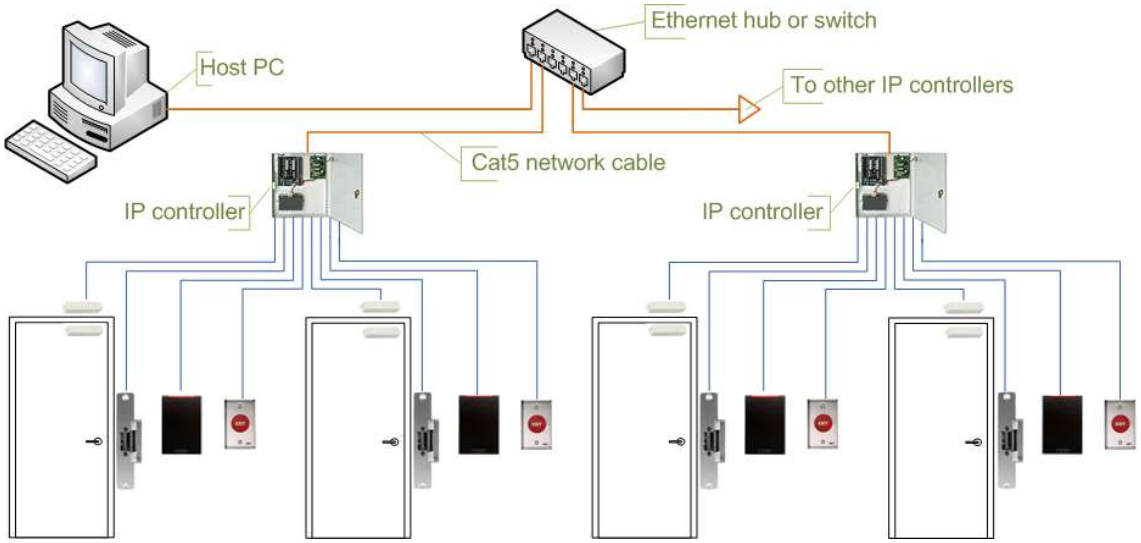
Kulunvalvontajärjestelmän topologia käyttäen sarjapääohjaimia ja älylukijoita näyttää kuvan 3 mukaiselta. Kaikki ovien laitteisto on kytketty suoraan älylukijoihin, jotka on kytketty pääohjaimiin. Yleensä toiminta perustuu pääohjaimien kulun päätöksiin riippumatta siitä, onko käytössä älykäs tai puoliälykäs lukija. Tällöin älykäs lukija pystyy tekemään itsenäisen päätöksen sisäisen tietokantansa perusteella, mikäli yhteys pääohjaimeen ei ole saatavilla. [27.]



Kuva 3. Useamman oven kulunvalvontajärjestelmä, jossa käytetään sarjapääohjaimia ja älylukijoita. [29.]

Topologian vahvuudet ovat isäntätietokoneen työkuormituksen merkittävä väheneminen, alhaisemmat kokonaiskustannukset, RS-485-standardin mahdollistama pitkä kaapelointi, lyhyt vasteaika, korkea luotettavuus ja turvallisuus. Topologian heikkoudet ovat järjestelmän toiminnan riippuvuus pääohjaimista sekä pääohjaimien kallis hinta. [27.]

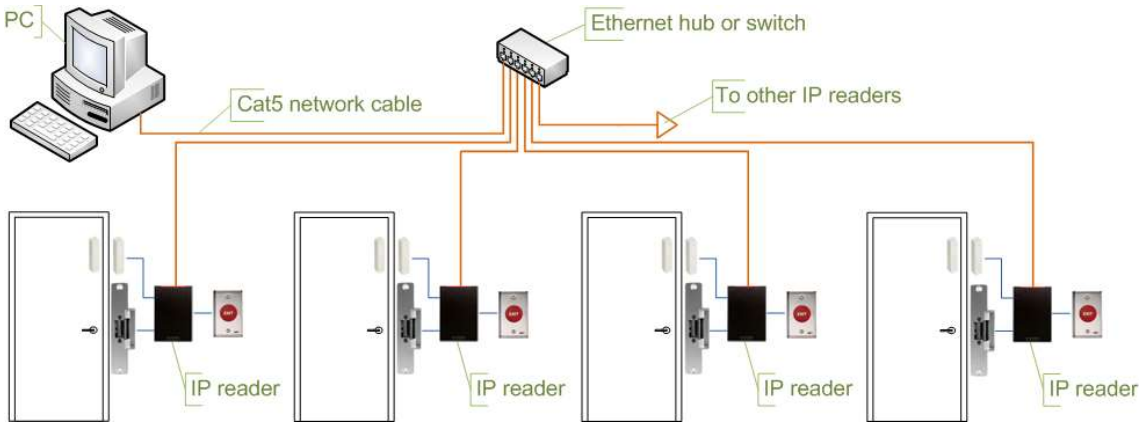
Topologisesti ja ominaisuuksiltaan eroava vaihtoehto kulunvalvontajärjestelmälle on kulunvalvontajärjestelmän toteuttaminen kuvan 4 mukaisesti IP-ohjaimia (Internet Protocol) käyttäen. Tällöin ohjaimet on kytketty isäntätietokoneeseen Ethernet LAN- (Local Area Network) tai WAN-verkon (Wide Area Network) kautta. [27.]



Kuva 4. Useamman oven kulunvalvontajärjestelmä, jossa käytetään IP-ohjaimia. [30.]

Topologian vahvuudet ovat olemassa olevan verkkoinfrastruktuurin täysi hyödyntäminen ja ohjainten lukumäärän rajoittamattomuus. Myöskään RS-485-sarjaliitännän asennus-, päättämis-, maadoitus- ja vianetsintätietoa ei vaadita. Lisäksi kommunikaatio ohjainten välillä voidaan tehdä täydellä verkon nopeudella ja hälytyksen sattuessa ohjaimet voivat muodostaa yhteyden isäntätietokoneeseen vähentäen tarpeetonta verkkoliikennettä. Vahvuuksina on myös yksinkertaistettu asennus useista eri paikoista koostuville järjestelmille ja verkkolaitteiden laaja valikoima. Topologian heikkoudet ovat järjestelmän herkkyys verkkoon liittyville ongelmille ja ohjaimien sekä tietokoneiden riski tulla hakkereiden ulottuville, mikäli organisaation verkko ei ole suojattu asianmukaisesti. Lisäksi heikkouksiin lukeutuvat maksimietäisyyden rajoitus keskittimen tai kytkimen ja ohjaimen välillä kuparikaapelia käyttäessä, sekä järjestelmän toiminnan vahva riippuvaisuus isäntätietokoneesta. [27.]

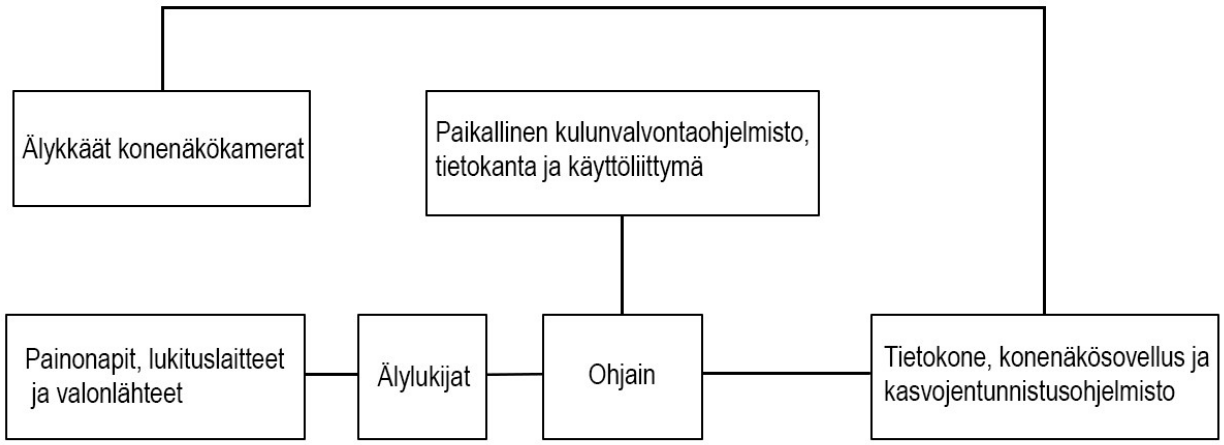
Topologiaan vaikuttavana mahdollisuutena on myös käyttää IP-lukijoita kuvan 5 mukaisesti. Tällöin IP-lukijat on kytketty isäntätietokoneeseen Ethernet LAN- tai WAN-verkon kautta [27].



Kuva 5. Useamman oven kulunvalvontajärjestelmä, jossa käytetään IP-lukijoita. [31.]

Topologian vahvuudet ovat useimpien IP-lukijoiden PoE-yhteensopivuus (Power over Ethernet) ja IP-lukijat poistavat ohjaimien tarpeen. Lisäksi IP-lukijoita käytettäessä kapasiteettia ei mene hukkaan ja IP-lukijajärjestelmät skaalautuvat helposti, sillä uusia pää- tai aliohjaimia ei tarvitse asentaa. Yhden IP-lukijan vika ei myöskään vaikuta muihin järjestelmän lukijoihin. Topologian heikkoudet ovat IP-lukijoiden käytön mahdollisuus korkean turvallisuuden alueilla ja vaatimus erityistulo- tai lähtömoduuleille, joilla estetään tunkeutuminen lukitus- tai poistumispainikkeen johtoja käyttäen. IP-lukijat ovat myös peruslukijoita kehittyneempiä, jonka vuoksi ne ovat niitä kalliimpia ja toiminnaltaan herkempiä. Tämä voi aiheuttaa rajoituksia tai haasteita erityisesti niiden ulkokäyttökohteisiin. [27.]

Tässä opinnäytetyössä keskityttiin kuvan 6 mukaiseen kahden oven kulunvalvontajärjestelmän topologiaan älylukijoita hyödyntäen, sillä suunnitellussa käyttökohteessa on tarpeellista vain ulko-ovien kulunvalvonta. Älylukijat valittiin järjestelmän luotettavuuden lisäämiseksi, sillä ne pystyvät tarpeen vaatiessa suorittamaan kulunvalvonnan, mikäli ohjaimen ja älylukijan välinen yhteys katkeaisi. Lisäksi topologian kompaktiudesta on hyötyä [27]. Luotettavuutta pyritään parantamaan myös tietokannan ja kulunvalvontaohjelmiston paikallistamisella, jolloin verkkoyhteyden katkos ei vaikuta kulunvalvonnan toimintaan [7]. Kahden oven kulunvalvontaan riittää yksi ohjain, joten sarjapääohjaimille ei ole tarvetta tässä käyttökohteessa. Älylukijat kommunikoivat ohjaimen kanssa usein RS-485-sarjaliitännän kautta. [27.]

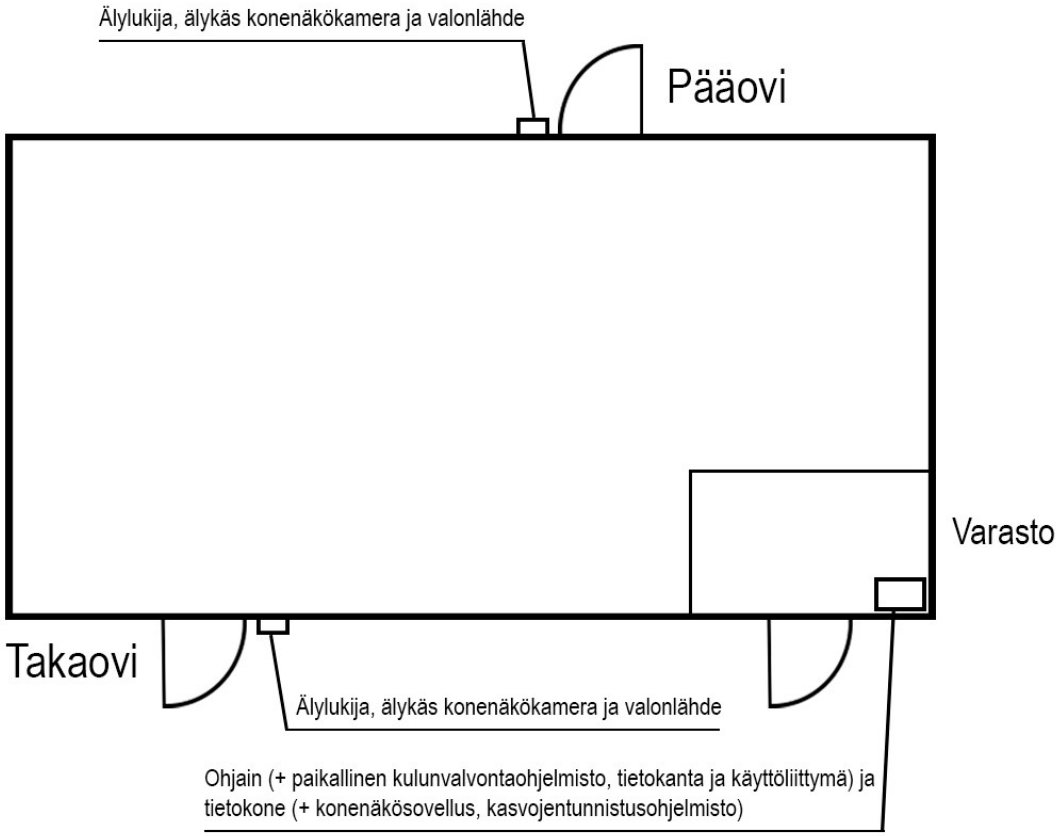


Kuva 6. Opinnäytetyön kulunvalvontajärjestelmän yksinkertaistettu topologia.

Kuvassa 6 on hahmottelemani paikallisen ovien kulunvalvontajärjestelmän topologia. Suunniteltuun kulunvalvontajärjestelmään kuuluu lisäominaisuutena konenäköjärjestelmä, joten sen mahdollistamiseksi ohjaimeen on kytketty erillinen tietokone. Tietokone sisältää konenäkösovelluksen ja kasvojentunnistusohjelmiston, sekä siihen on kytketty älykkäät konenäkökamerat. Näiden komponenttien avulla kasvojentunnistus on mahdollista.

4.3 Kulunvalvontajärjestelmän asennus

Opinnäytetyön valittu järjestelmä oli malliltaan paikallinen ovien kulunvalvontajärjestelmä, jossa on konenäköjärjestelmä lisäominaisuutena, jonka avulla ovien lukituksen hallinta on myös mahdollista. Valitun kulunvalvontajärjestelmän asennus koostuu tunnisteiden asentamisesta ja käyttöönotosta, lukijoiden asennuksesta, portaalin ja lukituslaitteiden asennuksesta, ohjaimen asennuksesta, paikallisen kulunvalvontaohjelmiston ja tietokannan asennuksesta ja käyttöönotosta sekä älykkäiden konenäkökameroiden, konenäkösovelluksen ja kasvojentunnistusohjelmiston asennuksesta [16].



Kuva 7. Kulunvalvontajärjestelmän käyttökohteena oleva omakotitalo

Suunniteltu kulunvalvontajärjestelmä sijoitetaan omakotitaloon ja kulunvalvontaa suoritetaan kiinteistön pää- ja takaovelle kuvan 7 mukaisesti. Kulunvalvonta toimii tunnisteen ja älylukijoiden tai älykkäiden konenäkökameroiden, tietokoneen, konenäkösovelluksen sekä kasvojentunnistusohjelmiston mahdollistaman kasvojentunnistuksen avulla. Älylukijat, älykkäät konenäkökamerat ja valonlähteet on sijoitettu kummankin oven oikealle puolelle. Pää- ja takaoven turvalliselle puolelle eli sisäpuolelle asetetaan kummankin oven läheisyyteen omat oven lukituksen avauspainikkeet. Kulunvalvontajärjestelmän ohjain ja tietokone asetetaan omakotitalon lukittuun varastoon vierekkäin.

4.3.1 Tunnisteiden asennus

Tunnisteiden käyttöönotto tapahtuu muun muassa tunnisteiden rekisteröintilukijaa hyödyntäen. Tunnisteiden käyttöönottoprosessi on usein yksinkertainen, tyypillisesti asetetaan haluttu tunniste, kuten tässä tapauksessa kuvan 8 tapainen tunniste rekisteröintilukijaan. Tätä ennen kuitenkin tulee asettaa henkilötiedot ja kulkulupataso kyseiselle henkilölle, joka liitetään kulunvalvontajärjestelmän tietokannassa henkilökohtaiseen tunnisteeseen [32].

Kuva 8. Tunnistekortti. [33.]

Rekisteröintilukijan käyttöönotto tapahtuu asettamalla virta rekisteröintilukijaan. Useat rekisteröintilukijat saavat virtansa tietokoneen USB-johdon (Universal Serial Bus) kautta. Tällöin rekisteröintilukija pystyy kommunikoimaan myös kulunvalvontaohjelmiston kanssa [32]. Suunnitellun kulunvalvontajärjestelmän tunnisteeksi valittiin tunnistekortti, sillä sen avulla kulku on luotettavaa ja silti nopeaa [9].

4.3.2 Älylukijoiden asennus

Tunnisteiden lukija asennetaan halutun pääsyrajoitetun tilan ulkopuolelle. Suunnitellussa käyttökohteessa käytetään kahta älylukijaa luotettavuuden parantamiseksi, sillä älylukijat kykenevät tekemään kulunvalvontapäätökset, mikäli yhteys ohjaimeen katkeaa. Älylukijat kytketään ohjaimeen johdotuksen avulla tässä tapauksessa. Virtajohto, maadoitusjohto, DI-johdot (Digital Input) sekä muut mahdollisesti tarvittavat johdot kytketään ohjaimen terminaaleihin [32].

Kuva 9. Tunnisteiden lukija. [34.]

Koska käyttökohteena on tässä tapauksessa omakotitalo ja älylukijat asennetaan asuinkiinteistön ulkoseinään, tulee niiden olla tarvittavan IP-luokituksen omaavia, sekä kestää vaihtelevia lämpötiloja [27]. Kuvassa 9 on esimerkkinä tarvittavan IP-luokituksen omaava lukija [34].

4.3.3 Portaalin ja lukituslaitteiden asennus

Oven tai portaalin sekä lukituslaitteen yhteensopivuus tulee varmistaa. Lukituslaitteisiin kuuluu lukituslaite, kuten kuvassa 10, että ulospääsyyn tarvittava poistumispainike tai vastaava komponentti. Poistumispainike mahdollistaa pääsyn lukitusta tilasta ulos ilman tarvittavaa kulkuluvan esittämistä [32].

Suunnitellussa kulunvalvontajärjestelmässä poistumispainikkeen tarvittavat johdot, eli DI-johto, maadoitusjohto sekä virtajohto kytketään ohjaimen terminaaleihin. Tässä tapauksessa halutaan järjestelmän olevan normaalitilassa lukossa, joten johdotuksen kytkentä täytyy tapahtua sen mukaisesti. Painikkeen toimintaperiaate toimii siten, että poistumispainiketta painaessa piirin virta katkeaa hetkellisesti, jolloin lukitus aukeaa virran katkeamisen ajaksi. Lukituslaite asennetaan ovenkarmiin, sekä oveen itsessään. Lukituslaitteen virta- ja maadoitusjohto sekä DO-johto (Digital Output) kytketään ohjaimen terminaaleihin. [32.]

Kuva 10. Sähkömagneettinen lukituslaite. [35.]

Lukituslaite asennetaan oven turvalliselle puolelle, eli sisäpuolelle.

4.3.4 Ohjaimen asennus

Ohjaimen asennuksessa kytketään virransyöttö ohjaimelle. Ohjain voi saada tiedonkulun että virransyötön Ethernet-kaapelin avulla PoE-tekniikkaa hyödyntäen [32]. Power over Ethernet on tapa toimittaa sähköä LAN-kaapeloinnin kautta verkkoon liitettyihin laitteisiin [36; 37]. Tällöin Ethernet-kaapeli liitetään ohjaimen PoE-kytkimeen. Tässä tapauksessa ohjaimen virransaanti olisi täysin riippuvainen tietokoneesta, joten käytännöllisempi vaihtoehto olisi erillinen virtalähde. Virtalähteen sisääntulon virtajohto kytketään tavalliseen 230 V:n vaihtoverkkovirtaan ja virtalähteen ulostulon virtajohto kytketään ohjaimen virransyöttöterminaaliin [37]. Erillisellä virtalähteellä järjestelmän toteuttaen ohjain täytyy kytkeä Ethernet-kaapelilla reitittimeen, johon myös kulunvalvontajärjestelmän tietokone

kytketään tai käyttää WLAN-tekniikkaa (Wireless Local Area Network), jotta kommunikointi mahdollistuu [38].

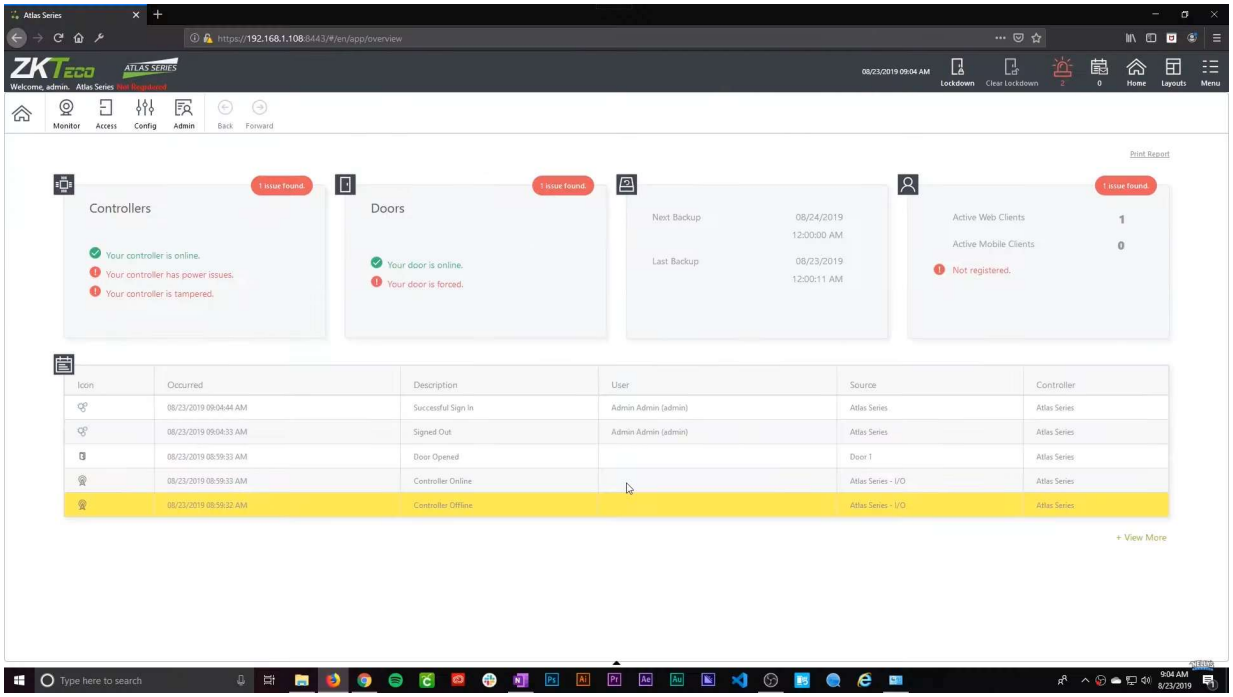
Kuva 11. Ohjain. [39.]

Ohjain voi sisältää tilattaessa myös ohjaimen suojakaapin. Ohjaimilla on mallikohtaisesti rajoitettu ovien lukituslaitteiden tuen maksimimäärä, tämä on syytä huomioida käyttökohteen mukaan. Ohjaimia pystyy myös käyttämään tarvittaessa useampia sarjassa, jolloin saadaan lisäkapasiteettia ovien lukituksen säädön lukumäärälle. [40; 32.] Suunniteltuun käyttökohteeseen eli omakotitaloon riittää yksi kuvan 11 mukainen ohjain, kunhan siinä on tuki minimissään kahdelle ovelle. Syynä on se, että suunnitellussa käyttökohteessa kulunvalvontaa suoritetaan kahdelle ulko-ovelle, kuten kuvassa 7 nähdään.

4.3.5 Kulunvalvontaohjelmiston ja käyttöliittymän asennus

Kulunvalvontajärjestelmän ohjelmisto, tietokanta ja käyttöliittymä voi olla joko paikallinen tai pilvipohjainen. Paikallinen ohjelmisto ei vaadi välttämättä internetyhteyttä, sen asentaminen ja käyttöönotto tehdään perinteisesti asentamalla kulunvalvontaohjelmisto- ja käyttöliittymäsovellukset. [6.] Pilvipohjaisen käyttöliittymän asennus tapahtuu usein syöttämällä tietokoneen verkkoselaimeen tarvittava IP-osoite, jossa pystytään asettamaan kulunvalvontaohjelmiston asetukset. [7; 32.]

Kulunvalvontajärjestelmän tietokantaan pystytään asettamaan monia kulunvalvontaan liittyviä asetuksia ja ominaisuuksia, kuten esimerkiksi kulkuoikeustasoihin sidonnaiset käyttäjäryhmät, ajankohtaisesti muuttuvat yksittäisten ovien lukitustilat tai henkilökohtaiseen tunnisteeseen sidonnainen PIN-koodi ja kulkuluvan taso. Tietokantaan asetetaan myös henkilö- ja yhteystiedot. Kulunvalvontaohjelmiston käyttöliittymästä voi nähdä mahdollisesti käyttäjien kulkuhistorian henkilötietoineen, joka voi olla erityisesti yrityskäytössä hyödyllinen ominaisuus. [27.]



Kuva 12. Pilvipohjainen kulunvalvontakäyttöliittymä [41.]

Kulunvalvontaohjelmiston tukiessa käyttöliittymään voi päästä myös käsiksi mobiililaitteella, jolloin tarvittavilla käyttöoikeuksilla voidaan avata tietty ovi väliaikaisesti. Tämä voisi olla käytännöllistä, mikäli tunniste ei olisi saatavilla ja mikäli järjestelmän kasvojentunnistukseen tarkoitettu älykäs konenäkökamera ei olisi toiminnassa [27]. Esimerkkinä käyttöliittymästä on kuvassa 12 näkyvä kulunvalvontajärjestelmän käyttöliittymä.

4.3.6 Älykkäiden konenäkökameroiden asennus

Älykkäiden konenäkökameroiden asentaminen aloitetaan valitsemalla konenäkökameroiden valvontapaikat, jotka ovat suunnitellussa käyttökohteessa pää- ja takaoven oikea puoli, älylukijoiden yläpuolella. Kiinnityksen jälkeen kohdennetaan kameran kulma haluttuun suuntaan, jotta valvonta alue on optimaalinen. [42.]

Älykkäiden konenäkökameroiden asennuksessa asennustapoja on erilaisia käyttöalustoista ja kameroiden malleista riippuen. Tässä opinnäytetyössä keskitytään konenäkökameran asennukseen Windows-käyttöjärjestelmälle. Älykäs konenäkökamera tarvitsee kytkemisen mahdollistamiseksi Windows SDK:n (Software Development Kit), eli Microsoftin ohjelmistokehityssarjan, joka on usein valmiiksi asennettuna älykkäissä konenäkökameroissa. Seuraavaksi ladataan tarvittaessa valmistajan muut ohjelmistot sekä konenäkösovellus, jossa pystytään säätämään konenäkökameran attribuutteja, kuten valotusaikaa, jotta kameran kuvaama kuva on kirkkaudelta ja kontrastilta sopiva käyttötarkoitukseen. [43.]

Useissa käyttökohteissa joudutaan lisäämään konenäkökameraan vahvistusta, joka lisää kuvan kirkkautta, mikäli sitä ei saada valotusajan avulla tarpeeksi kirkkaaksi. Liian suuri vahvistus kuitenkin heikentää kuvanlaatua tuomalla siihen visuaalista kohinaa. Lopuksi asetetaan konenäkökameran valkotasapaino, mikäli kamera on värikamera, jotta saavutetaan realistisemmat värit kameran kuvaa-

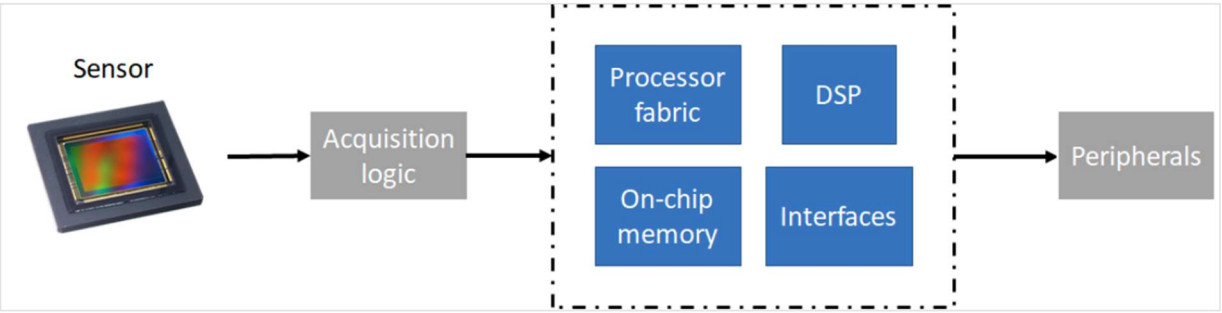
miin kuviin tai videoihin. Valkotasapainon asetukseen on olemassa automaattisia asetusominaisuuksia. Konenäkökameroiden virransyöttö voi tapahtua esimerkiksi erillisellä virtalähteellä tai tietokoneen USB-portista. [43.]

Suunniteltuun kulunvalvontajärjestelmään valitaan älykkäät konenäkökamerat perinteisten konenäkökameroiden sijaan. Niiden ja tietokoneessa olevan konenäkösovelluksen sekä kasvojentunnistusohjelmiston avulla saadaan suoritettua kasvojentunnistus. [19.]

4.3.7 Konenäköjärjestelmän asennus

Konenäköjärjestelmän asennus koostuu siihen kuuluvien komponenttien asennuksesta, jotka ovat suunnitellussa käyttökohteessa valonlähteet, älykkäät konenäkökamerat, tietokone ja konenäkösovellus. Konenäkökameroiden asennus käytiin läpi edellisessä luvussa. [27.]

Valonlähteiden asennus tapahtuu kiinnittämällä valonlähde asuinkiinteistön ulkopuolelle. Tietokoneen asennuksessa kytketään virtajohto, monitori sekä muut ihmisrajapintalaitteet. Konenäkösovelluksessa yhdistetään älykkäiden konenäkökameroiden ja konenäkösovelluksen välille yhteys tietokoneen avulla. Seuraavaksi määritellään ja optimoidaan tarvittavat mittaukset ja muut näön käsittelyyn liittyvät prosessit sekä määritellään, mihin perustuen järjestelmä hyväksyy tai hylkää mittausten ja muiden prosessien lopputulokset. Kulunvalvontajärjestelmän konenäkösovelluksessa hyödynnetään tässä tapauksessa biometrista ja geometrista tunnistamista. Ovien lukituksen hallinnan mahdollistamiseksi konenäköjärjestelmän mittauksien ja tunnistamisen perusteella, tarvitaan tiedonkulku esimerkiksi Ethernet-kaapelin avulla ohjaimelle. [44.]



Kuva 13. Korkean tason konenäköjärjestelmän arkkitehtuuri [45.]

Lopuksi varmistetaan, että kommunikointi eri laitteiden välillä toimii sovelluksen ympäristössä [44]. Esimerkkinä konenäköjärjestelmän arkkitehtuurista on kuva 13.

4.3.8 Kasvojentunnistusohjelmiston asennus

Kasvojentunnistusohjelmiston asennuksessa asennetaan kasvojentunnistukseen tarvittavat ohjelmistot ja mahdolliset kirjastot. Seuraavaksi lisätään kasvojentunnistusjärjestelmän tietokantaan hyväksyttävät kasvot, joihin järjestelmä vertaa konenäkökameroiden tallentamaa kuvainformaatiota. Tämän jälkeen tulee asettaa kuvien koodaus koodikielelle, jotta järjestelmä pystyy vertaamaan tuloksia, esimerkkinä kuva 14. Vertailun lopputulos on riippuvainen asetetusta toleranssista, jonka rajoissa eroavaisuutta tietokantaan asetetun ja analysoitujen kasvojen kuvamateriaalin välillä sallitaan. Lopputulokseksi saadaan arvo tosi tai epätosi, jonka avulla oven lukituksen hallinta tapahtuu. [46.]

[-0.23, -0.54, ..., 0.27]

Kuva 14. Kasvojentunnistuksen kuvan koodaus 128 reaaliluvun vektoriksi. [47.]

Kasvojentunnistuksen lopputulos kommunikoidaan konenäkösovelluksen välillä, jotta saadaan suoritettua mahdolliset muut mittaukset ja prosessit sekä lopuksi tieto kommunikoidaan kulunvalvontajärjestelmän ohjaimelle [23].

4.4 Kulunvalvontajärjestelmän käyttöönotto

Kulunvalvontajärjestelmän käyttöönottoon liittyy olennaisesti järjestelmän toiminnan testaus sekä työn ja muiden olennaisten tietojen raportointi sekä ylläpito ja huolto, jotta järjestelmän elinkaari pitenee ja toimivuus varmistuu.

4.4.1 Käyttöönotto

Kulunvalvontajärjestelmän käyttöönotossa tehdään käyttäjäprofiilit järjestelmään ja syötetään mahdolliset tarvittavat tiedot tietokantaan. Tunnisteiden aktivointi voi tapahtua esimerkiksi tunnisteiden rekisteröintilukijan avulla, tästä esimerkkinä kuva 15. [27.]

Kuva 15. Tunnisteiden rekisteröintilukija. [48.]

Konenäköjärjestelmän käyttöönotto tapahtuu kytkemällä virta valvontaan tarkoitettuun tietokoneeseen ja käynnistämällä konenäkökamera sekä konenäkösovellus [24]. Tässä kohdassa voidaan asettaa konenäköjärjestelmän mittauksien ja tunnistamisen lopputuloksen perusteella ovien lukituksen hallinta.

4.4.2 Testaus

Testataan, että järjestelmä toimii halutulla tavalla sekä henkilökohtaiset tunnisteet on liitetty onnistuneesti tietokantaan ja siten antavat oikean kulkulupatason henkilöille. Älykkäiden konenäkökameroiden ja konenäkösovelluksen osalta tulee testata, että järjestelmä tunnistaa henkilön, sekä mahdollisesti määritetyt kielletyt esineet. Lisäksi varmistetaan konenäkökameroiden ja kulunvalvontajärjestelmän tietokoneen välisen yhteyden toimivuus. [42.]

Konenäköjärjestelmän osalta varmistetaan testauksessa valonlähteen riittävyys ja oikeanlainen valonvoimakkuuden asetus, jotta konenäköjärjestelmä pystyy

suorittamaan kasvojentunnistuksen kaikissa tarvittavissa valaistusolosuhteissa [24].

4.4.3 Raportointi

Kulunvalvontajärjestelmän toteutuksessa tulee raportoida työvaiheet ja niiden aikataulu ja niiden käyttöönottovaiheet sekä testaukset ja niiden tulokset. Raportoinnilla saadaan kokonaisvaltainen tietokokonaisuus aikataulusta ja työn etenemisestä sekä suoritetuista työvaiheista. Raportoinnin tiedoista voi olla suuri hyöty esimerkiksi ongelmatilanteiden selvityksessä.

4.4.4 Ylläpito ja huolto

Kulunvalvontajärjestelmien komponenttien kuluminen voi luoda haavoittuvuuden järjestelmään ja turvallisuuteen. Tiettyjen komponenttien kuluman huomaa helpommin, kuten esimerkiksi oven ja sen lukituksen, mutta teknisemmät kokonaisuudet, kuten mahdollinen hälytyksen luominen ja kulunvalvontajärjestelmän optimaalinen toiminta voivat jäädä helpommin huomaamatta. Huoltotarkistuksessa on hyvä tarkistaa järjestelmä visuaalisesti, tehdä järjestelmän tehokkuuden analyysi tietokoneella, tarkistaa järjestelmän virtalähteiden kunto, puhdistaa ohjauskomponentit, käydä läpi kaikki järjestelmän komponentit ja mahdollisten muutosten kirjaaminen, tarkistaa järjestelmän eri laitteiden välinen yhteys, katsoa läpi tietolokit ja lopuksi kirjata tarkistuksen tulokset. [49.]

Kulunvalvontajärjestelmän sisältäessä IoT-järjestelmän (Internet of Things) sen avulla saavutetaan ennaltaehkäisevää huoltoa, joka mahdollistaa mittaukset ja valvonnan järjestelmän komponentteihin ja ilmoittaa käyttäjälle, kun osa tai komponentti on huollon tai vaihdon tarpeessa. Lisäetuna saavutetaan reaaliaikainen tiedon analysointi, jolloin ongelmakohtiin ehditään puuttumaan varhaisemmassa vaiheessa ennen varsinaisen rikkoutumisen tapahtumista. Järjestelmän komponenttien suorituskykyä pystytään valvomaan ja automaation avulla pystytään tukeutua tiedon luotettavuuteen. Laitteiden ja komponenttien rikkoutu-

essa tai vikaantuessa vikatietoja eri lähteistä voidaan kerätä, koota ja analysoida reaaliajassa pilvessä. Korjausvaihtoehdot voidaan tehdä automaattisesti järjestelmässä ja toimenpiteistä voidaan tehdä ilmoitus huoltoon. [50.]

5 Riskitekijät kulunvalvontajärjestelmissä

Automatisoituihin ja teknisiin järjestelmiin liittyy riskejä ja haasteita. Riskit jakautuvat käyttäjien aiheuttamiin riskeihin ja järjestelmän sisäisiin riskeihin.

5.1 Riskit tai puutteellisuus

Anturiteknologioihin perustuvat IoT-järjestelmät, jotka tunnistavat liikettä tai muita ympäristöön liittyviä muuttujia toimivat usein testausvaiheessa hyvin, mutta käytössä ollessa voivat laukaista monesti vääriä hälytyksiä. Tästä johtuen usein erittäin suuri kokoiset videotallenteet ovat käytössä vain rikoksen tai vahingon sattumisen jälkeen eikä reaaliajassa silloin, kun rikos tai tapaturma tapahtuu. [22.]

Yleinen kulunvalvontajärjestelmän kautta tapahtuva tunkeutumisen turvallisuusriski on luvallisen käyttäjän seuraaminen ovesta. Tämä riski voidaan minimoida käyttäjien turvallisuuskoulutuksella tai laitteiston avulla, kuten kääntöportilla. Erittäin korkean turvatason sovelluksissa tämä riski minimoidaan käyttämällä turvallisuuseteistä, jossa vaaditaan vartijoita tai henkilökuntaa tunnistamisen oikeellisuuden varmistamiseksi. Toinen yleinen riski on oven avaaminen vipuvarren avulla, joka on kuitenkin suhteellisen vaikeaa kunnolla kiinnitetyissä ovissa, joissa on iskut kestävät tai suuren pitovoiman magneettilukot. Edistyksellisesti toteutetut kulunvalvontajärjestelmät sisältävät ovissa hälyttimet, jotka aistivat oveen kohdistuvat suuret voimat ja luovat hälytyksen niiden perusteella. Käytännössä tämän ominaisuuden tehokkuus vaihtelee, mikä mahdollistaa vääriä hälytyksiä. [27.]

Kulunvalvontajärjestelmän toimintaa on mahdollista manipuloida esimerkiksi operoimalla solenoidin ohjauspultteja sähköisissä lukituslaitteistoissa voimakkaan magneetin avulla. Myös virransyöttöä oven lukitukselle on mahdollista manipuloida vähentämällä tai lisäämällä syötettävän virran määrää. Useimmat kulunvalvontajärjestelmät sisältävät akun varajärjestelmät ja lukituslaitteet sijaitsevat melkein aina oven turvallisella puolella. [27.]

Muita kulunvalvontajärjestelmään liittyviä riskejä ovat tunnisteiden turvallisuuden puute sen vaihtuessa toisen henkilön kanssa tai tunnisteen kadotessa, jolloin altistutaan kopioinnin riskille. Biometriikan ja älypuhelimien tunnistamisen rajoitukset, kuten biometristen tietojen tunnistamisen hitaus ja älypuhelimen tietojen tunnistuksen epävarmuus verrattuna paikalliseen tunnistusjärjestelmään. Kyberturvallisuusriski, jossa kulunvalvontajärjestelmän toimintaa voidaan manipuloida tai päästä käsiksi järjestelmän tiedostoihin tai videotallenteisiin, sekä muokata tai poistaa niitä. Riskitekijöitä on myös kulunvalvontaohjelmiston päivittämättömyys, jolloin siihen voi jäädä piileviä tietoturvariskejä. Riskiä pyritään välttämään pitämällä järjestelmät uuden yleisen tietosuoja-asetuksen eli GDPR:n (General Data Protection Regulation) mukaisena. [51; 52.]

5.2 Haasteet

Konenäkösuunnitteluun liittyviä haasteita ovat muun muassa lämmönhallinta, EMI (Electromagnetic Interference) tai EMC (Electromagnetic Compatibility) ja virraneheys. Korkearesoluutioiset kamerat voivat vastaanottaa paljon lämpöä käytön aikana, joka saattaa vaatia lämmön kontrollointia. EMI tai EMC on myös konenäköjärjestelmien haaste, sillä ne ovat yleensä sekasignaalijärjestelmiä. Tämän takia vaaditaan oikeanlainen komponenttien asettelu, jotta häiriöt voidaan estää digitaalisten komponenttien välillä. Konenäköjärjestelmissä voi esiintyä sähkön eheysongelmia, mikäli suunnitelmaa ei ole toteutettu oikein. [53.]

Tulevaisuuden kannalta haasteena voi olla seuraavan sukupolven älykkäiden kulunvalvontajärjestelmien suunnittelu kohtuullisen kustannuksen ja koon mukaisina. Yksi tärkeimmistä syistä on taakka, jonka jokainen kuvan resoluution lisäys asettaa muulle järjestelmän suunnittelulle kuvan 16 mukaisesti. [21.]

Horizontal Resolution	Vertical Resolution	Picture Elements	Single-Frame 24-bit	1 Second Buffer	Standard
320	240	76,800	230,400	6,912,000	1/4 VGA
640	480	307,200	921,600	27,648,000	VGA
800	600	480,000	1,440,000	43,200,000	SVGA
1024	768	786,432	2,359,296	70,778,880	XVGA
1280	768	983,040	2,949,120	88,473,600	WXGA
1280	1024	1,310,720	3,932,160	117,964,800	SXGA
1400	1050	1,470,000	4,410,000	132,300,000	SXGA+
2048	1536	3,145,728	9,437,184	283,115,520	QXGA
3200	1800	5,760,000	17,280,000	518,400,000	WQXTA+
4096	3072	12,582,912	37,748,736	1,132,462,080	HXGA
7680	4800	36,864,000	110,592,000	3,317,760,000	WHUXGA

Kuva 16. Kameran kuvan resoluution kasvattamisen aiheuttamat laitteistovaatimukset muistille, videon prosessoinnille, tallennukselle ja lähetykselle. [54.]

Rakennus- ja turvallisuusmääräykset muuttuvat ja vaikuttavat yleisiin järjestelmän asennustapoihin, sillä ne eivät välttämättä täytä uusia määräyksiä. Standardeja yhdistetään ja päivitetään, jolloin järjestelmien komponentit saattavat olla muutoksen tai päivityksen tarpeessa, mikäli ne eivät täytä uusimpia standardeja. Euroopassa sijaitsevien rakennusten kriittisiin uloskäyntipisteisiin asennettujen hallintalaitteiden pitäisi olla vikaturvallisia, ja mekaaninen oven avaus tulee mahdollistaa suoran ulospääsyn hätätilanteessa. [51.]

Roolipohjaisessa pääsynhallinnassa haasteena on, että käyttäjille annetaan vain tarvittavat pääsyoikeudet. Pääsyoikeudet tulisi tarkistaa ja tarvittaessa muuttaa säännöllisin väliajoin osana turvallisuuden hallintaprosessia. Käyttäjien kouluttaminen turvallisuuden osalta on yksi tärkeimmistä osa-alueista, sillä käyttäjät voivat oikoa turvatoimia ja ottaa tietämättään suuria riskejä. Inhimillinen virhe on aina yksi yrityksen suurimpia turvallisuusriskejä. [55.]

Haasteisiin lukeutuu myös käyttökohteeseen sopivimman pääsynhallintamallin valitseminen. Pääsynhallintamallin valinta perustuu usein yrityksen rakenteen monimutkaisuuteen. [56.]

5.3 Olennaisia lakisäädöksiä

Suomessa lukitus-, kulunvalvonta- ja hälytysjärjestelmien asentaminen sekä niihin liittyvät tehtävät tulivat luvanvaraiseksi vuoden 2019 alusta alkaen, jonka jälkeen kaikilla niitä asentavilla, korjaavilla ja muuttavilla yrityksillä tulee olla turvallisuusalan elinkeinolupa haettuna poliisihallitukselta. Luvanvaraiseksi tulivat muun muassa lukkojen tai sen komponenttien asennus, vaihto, huolto, sarjatietojen käsittely, avausten suunnittelu ja käsittely tietojärjestelmissä tai manuaalisesti. Laissa jätettiin osa turvasuojausalan tehtävistä pois, joten turvallisuusalan elinkeinolupaa ei tarvitse muun muassa kameravalvontajärjestelmien ja niihin liittyvien komponenttien asentamisessa, korjaamisessa ja muuttamisessa sekä muiden järjestelmien kaapelointitöissä. [57.]

Asunto- ja kiinteistöosakeyhtiöissä sekä vuokrataloissa asukas saa itse päättää hallinnassaan olevien tilojen valvonnasta kuten asuinhuoneistostaan. Muita alueita valvottaessa tulee ottaa huomioon yhteisön päätöksentekoon liittyvät normit. Valvottavan alueen ollessa yhtiön muita tiloja esim. porraskäytävä, piha-alue tai pyörävarasto kuuluu päätöksen tekeminen yhtiömuodosta riippuen hallitukselle tai yhtiökokoukselle. Omakotitalon omistaja on oikeutettu päättämään omistamansa kiinteistön, kodin sekä piha-alueen valvonnasta. Naapurien piha-alueita ei ole luvallista kuvata, joka tulee huomioida kameroiden kuvakulman sijoittamisessa. Rivitalojen ja muiden asukkaiden hallinnassa olevien piha-alueiden ja niihin välittömästi liittyvien rakennusten kameravalvontaan tulee olla asukkaiden suostumus. [58.]

Henkilötietolakia sovelletaan henkilötietojen käsittelyyn. Henkilötiedoilla tarkoitetaan henkilöä tai hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa tai liittää häntä tai hänen perhettään koskeviksi. Kameravalvontajärjestelmä, joka kerää ja tallentaa tietoa eli kuvaa tai ääntä

henkilöstä, kuuluu henkilötietolain piiriin. Henkilötietolaista johtuen kameravalvonnan tulee olla henkilötietoa käsittelevän toiminnan kannalta asiallisesti perusteltua. Henkilötietoa kerättäessä tulee valvonnan kohteeksi joutuvalle ilmoittaa tietojen keräämisestä esimerkiksi tarroilla tai kylteillä. Kameravalvonnan omistajan tulee laatia valvonnalla saatavista henkilötiedoista rekisteriseloste, joka tulee olla kaikkien saatavilla. Rekisteriselosteesta tulee ilmetä henkilötietojen käsittelyn tarkoitus, rekisterinpitäjän yhteystiedot, tietojen säännönmukainen luovutus ja tietojen suojauksen periaatteet. [58.]

Työpaikalla työnantajan suorittamasta kameravalvonnasta on omat erityisehtonsa. Työntekijä voidaan asettaa teknisen tarkkailun kohteeksi ainoastaan, mikäli siitä on sovittu yhteistoiminta- ja kuulemismenettelyssä. Työnantajan on määriteltävä työntekijöihin kohdistuvan teknisen valvonnan käyttötarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä tiedotettava niistä työntekijöille. Perusteltuja ja hyväksyttäviä syitä tallentavalle kameravalvonnalle ovat esimerkiksi työntekijöiden ja muiden henkilöiden turvallisuuden varmistaminen, omaisuuden suojaaminen, tuotantoprosessien valvominen sekä turvallisuutta, omaisuutta tai tuotantoprosessia vaarantavien tilanteiden ennaltaehkäiseminen tai selvittäminen. Kameravalvontaa ei saa käyttää yksittäisen työntekijän tarkkailuun työpaikalla, eikä kameravalvontaa saa olla wc-tiloissa, pukeutumistiloissa, henkilötiloissa, työntekijän henkilökohtaisessa työhuoneessa tai muissa paikoissa, joissa yksityisyyttä oletetaan. Työntekijän työpisteeseen voidaan kuitenkin kohdistaa kameravalvontaa, jos sen todetaan olevan välttämätöntä esimerkiksi selkeän uhan vuoksi. [59.]

Salakatselun säännös ei rajoita valvontakameroiden käyttöä liiketiloissa sulkemisajan jälkeen, sillä silloin tarkkailtavat henkilöt ovat luvattomasti tilassa [58].

6 Yhteenveto

Kulunvalvontajärjestelmän toteutukseen suunnitteluun liittyy paljon tietoa, joten yksityiskohtaisuuksiin perehtyminen vie aikansa. Konenäköjärjestelmän ja kasvojentunnistuksen sovellutus kulunvalvontajärjestelmään on pintaa syvemmiltä yksityiskohdiltaan vaativampi tehtävä. Tästä huolimatta turvallisuus on tärkeää ja kulunvalvonta- tai pääsynhallintajärjestelmä voi olla välttämätön esimerkiksi yrityspuolella. Asuinkiinteistöissä kulunvalvontajärjestelmällä saadaan ylellisyyden tunnetta luovia tekijöitä, kuten mahdollisuuden oven lukituksen kontrollointiin ilman perinteisiä avaimia.

Kulunvalvontajärjestelmän käytännöllisimmät käyttökohteet ovat sovitusti yrityskäyttö sekä omakotitalot. Tällöin vältytään ehdottomalta muiden asukkaiden luvan tarvitsemiselta, joka on pakollinen kulunvalvontajärjestelmän laillisuuden kannalta. Tämä huomioitiin opinnäytetyön suunnitellun käyttökohteen valinnassa. [58.]

Lähteet

1 Kulunvalvonta. Verkkoaineisto. Saatavissa: https://fi.wikipedia.org/wiki/Kulunvalvonta. Luettu 25.10.2021.

2 Pääsyn valvonta. Verkkoaineisto. Saatavissa: https://fi.wikipedia.org/wiki/P%C3%A4%C3%A4syn_valvonta. Luettu 25.10.2021.

3 SiteKiosk. COVID Certificate Verifier. Verkkoaineisto. Saatavissa: https://www.sitekiosk.com/covid-certificate-verifier/. Luettu 15.11.2021.

4 Neural Labs. Access Control. Verkkoaineisto. Saatavissa: https://www.neurallabs.net/en/solutions/access-control. Luettu 15.11.2021.

5 SALTO Systems. Smart access control solutions for Residential. Verkkoaineisto. Saatavissa: https://saltosystems.com/en-fi/industries/residential-solution/?gclid=CjwKCAiAp8iMBhAqEiwAJb94zzrcCJTT5Td3fgwls-WQzvNkeMeeJCZLY9ZESL4k_VDV5AUUmdkWFFxoCA9UQAvD_BwE. Luettu 15.11.2021.

6 360 Quadrants. Best Access Control Systems. Verkkoaineisto. Saatavissa: https://www.360quadrants.com/semiconductor-and-electronics/access-control-solutions. Luettu 15.11.2021.

7 Murray, Meredith. 2020. 8 Best Cloud-Based Access Control Systems in 2022. Verkkoaineisto. Saatavissa: https://butterflymx.com/blog/best-cloud-based-access-control-systems/. Luettu 17.11.2021.

8 Biometrinen tunnistaminen. Verkkoaineisto. Saatavissa: https://fi.wikipedia.org/wiki/Biometrinen_tunnistaminen. Luettu 16.11.2021.

9 Elprocus. Know about Access Control Systems and Their Types with Features. Verkkoaineisto. Saatavissa: https://www.elprocus.com/understanding-about-types-of-access-control-systems/. Luettu 4.11.2021.

10 Salmane, Kristina. 2020. How Does Proximity Access Control Work? Verkkoaineisto. Saatavissa: https://blog.nortechcontrol.com/proximity-access-control-work. Luettu 16.11.2021.

11 Ekran. 2020. Mandatory Access Control vs Discretionary Access Control: Which to Choose? Verkkoaineisto. Saatavissa: https://www.ekransystem.com/en/blog/mac-vs-dac. Luettu 25.10.2021.

12 Risk, Erin. 2021. Access Control Models: MAC, DAC, RBAC, & PAM Explained. Verkkoaineisto. Saatavissa: https://www.twingate.com/blog/access-control-models/. Luettu 2.11.2021.

13 Casey, Keith. 2020. What Is Attribute-Based Access Control (ABAC)? Verkkoaineisto. Saatavissa: https://www.okta.com/blog/2020/09/attribute-based-access-control-abac/. Luettu 2.11.2021.

14 Zhang, Ellen. 2020. What is Role-Based Access Control (RBAC)? Examples, Benefits, and More. Verkkoaineisto. Saatavissa: https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more. Luettu 4.11.2021.

15 Ekran. 2019. Role-based Access Control vs Attribute-based Access Control: How to Choose. Verkkoaineisto. Saatavissa: https://www.ekransystem.com/en/blog/rbac-vs-abac. Luettu 4.11.2021.

16 Sopp, Mike. 2017. Automatic access control systems in laboratories. Verkkoaineisto. Saatavissa: https://app.croneri.co.uk/feature-articles/automatic-access-control-systems-laboratories. Luettu 27.10.2021.

17 USI Security. 2018. What are the Components of an Access Control System? Verkkoaineisto. Saatavissa: https://inbound.usisecurity.com/blog/what-are-the-components-of-an-access-control-system. Luettu 15.12.2021.

18 Kashyapa, Raghava. 2020. The Ultimate Guide to Machine Vision Camera Selection. Verkkoaineisto. Saatavissa: https://qualitastech.com/the-ultimate-guide-to-machine-vision-camera-selection/. Luettu 8.11.2021.

19 Fisher Smith. Smart Cameras. Verkkoaineisto. Saatavissa: https://fishersmith.co.uk/components/smart-cameras/. Luettu 13.2.2022.

20 Turek, Fred D. 2011. Machine Vision Fundamentals: How to Make Robots ‘See’. Verkkoaineisto. Saatavissa: https://www.techbriefs.com/component/content/article/tb/supplements/it/features/articles/10531. Luettu 26.10.2021.

21 Gabay, Jon. Applying Modern Machine Vision Technologies to Security. Verkkoaineisto. Saatavissa: https://www.mouser.fi/applications/modern-machine-security/. Luettu 26.10.2021.

22 Mahmood, Khurram. 2019. Four Ways Computer Vision Is Transforming Physical Security. Verkkoaineisto. Saatavissa: https://www.forbes.com/sites/forbestechcouncil/2019/09/23/four-ways-computer-vision-is-transforming-physical-security/?sh=73ee8aa75846. Luettu 26.10.2021.

23 Omron Microscan. 2012. Introduction to Machine Vision Part 3: Key Parts of a Vision System. Verkkoaineisto. Saatavissa: https://www.microscan.com/en-us/resources/videos/introduction-to-machine-vision-part-3. Luettu 9.11.2021.

24 Industrial Vision Systems. 5 proven methods for successful vision system installs in industry. Verkkoaineisto. Saatavissa: https://www.industrialvision.co.uk/applications/5-proven-methods-for-successful-vision-system-installs-in-industry. Luettu 10.11.2021.

25 Gladchuk, Veronica. 2020. Facial Recognition Algorithms for Machine Learning: Application and Safety. Verkkoaineisto. Saatavissa: https://labelyourdata.com/articles/facial-recognition-algorithms-for-machine-learning. Luettu 11.1.2022.

26 Kuva 1. Yksittäisen oven kulunvalvontajärjestelmän topologia perinteisillä lukijoilla. Luettu 18.11.2021. Saatavissa: https://en.wikipedia.org/wiki/Access_control.

27 Access control. Verkkoaineisto. Saatavissa: https://en.wikipedia.org/wiki/Access_control. Luettu 27.10.2021.

28 Kuva 2. Yksittäisen oven kulunvalvontajärjestelmän topologia älylukijoita hyödyntäen. Luettu 18.11.2021. Saatavissa: https://en.wikipedia.org/wiki/Access_control.

29 Kuva 3. Useamman oven kulunvalvontajärjestelmä, jossa käytetään sarjapääohjaimia ja älylukijoita. Luettu 18.11.2021. Saatavissa: https://en.wikipedia.org/wiki/Access_control.

30 Kuva 4. Useamman oven kulunvalvontajärjestelmä, jossa käytetään IP-ohjaimia. Luettu 18.11.2021. Saatavissa: https://en.wikipedia.org/wiki/Access_control.

31 Kuva 5. Useamman oven kulunvalvontajärjestelmä, jossa käytetään IP-lukijoita. Luettu 18.11.2021. Saatavissa: https://en.wikipedia.org/wiki/Access_control.

32 How To Set Up an Access Control System: Complete Step-By-Step Guide for Beginners 2019. YouTube. Nelly's Security, 21.10.2019. Saatavissa: https://www.youtube.com/watch?v=trn_R5TOaGU. Katsottu 28.10.2021.

33 Kuva 8. Tunnistekortti. Luettu 28.10.2021. Saatavissa: https://www.zkteco.com/en/product_detail/Card&Tag.html.

34 Kuva 9. Tunnisteiden lukija. Luettu 28.10.2021. Saatavissa: https://zkteco.eu/products/access-control/reader/rfid-reader/kr501el-legic.

35 Kuva 10. Sähkömagneettinen lukituslaite. Luettu 28.10.2021. Saatavissa: https://zkteco.eu/products/locks/electromagnetic-locks/lm-500.

36 Cisco. 2016. Cisco Universal Power Over Ethernet - Unleash the Power of your Network White Paper. Verkkoaineisto. Saatavissa: https://web.archive.org/web/20171128140727/http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/white_paper_c11-670993.html. Luettu 28.10.2021.

37 ZKTeco. 12VDC 3A Power Supply with battery backup. Verkkoaineisto. Saatavissa: https://www.zkteconz.com/product/12vdc-3a-power-supply-with-battery-backup/. Luettu 28.10.2021.

38 Verizon. Wi-Fi. Verkkoaineisto. Saatavissa: https://www.verizon.com/info/definitions/wifi/. Luettu 28.10.2021.

39 Kuva 11. Ohjain. Luettu 28.10.2021. Saatavissa: https://zkteco.eu/products/access-control/multi-door-controller/rfid-multi-door-controller/atlas-prox-series.

40 ZKTeco. Atlas Prox Series. Verkkoaineisto. Saatavissa: https://zkteco.eu/sites/default/files/content/downloads/atlas-proxx00-series-datasheet.pdf. Luettu 29.10.2021.

41 Kuva 12. Pilvipohjainen kulunvalvontakäyttöliittymä. Katsottu 28.10.2021. Saatavissa: https://www.youtube.com/watch?app=desktop&v=trn_R5TOaGU.

42 Jaeger, Saul. 2021. How to Install a Security Camera System for a House. Verkkoaineisto. Saatavissa: https://www.wikihow.com/Install-a-Security-Camera-System-for-a-House. Luettu 10.11.2021.

43 GeT Cameras. 2018. QuickStart 5 steps to easily install a machine vision camera and acquire an image. Verkkoaineisto. Saatavissa: https://www.vision-camera.nl/QuickStart-5-steps-to-easily-install-a-machine-vision-camera-and-acquire-an-image. Luettu 10.11.2021.

44 Cognex. VisionPro Software. Verkkoaineisto. Saatavissa: https://www.cognex.com/en-fi/products/machine-vision/vision-software/visionpro-software. Luettu 11.11.2021.

45 Kuva 13. Korkean tason konenäköjärjestelmän arkkitehtuuri. Luettu 16.12.2021. Saatavissa: https://octopart.com/blog/archives/2021/08/components-for-machine-vision-system-design.

46 Rosebrock, Adrian. 2018. Face recognition with OpenCV, Python, and deep learning. Verkkoaineisto. Saatavissa: https://www.pyimagesearch.com/2018/06/18/face-recognition-with-opencv-python-and-deep-learning/. Luettu 12.1.2022.

47 Kuva 14. Kasvojentunnistuksen kuvan koodaus 128 reaaliluvun vektoriksi. Luettu 27.1.2022. Saatavissa: https://www.pyimagesearch.com/2018/06/18/face-recognition-with-opencv-python-and-deep-learning/.

48 Kuva 15. Tunnisteiden rekisteröintilukija. Luettu 28.10.2021. Saatavissa: https://www.zktecousa.com/product-page/card-enrollment-reader-cr10e.

49 Mehl, Bernhard. 2018. Access Control System Maintenance Is More Important Than You Think. Verkkoaineisto. Saatavissa: https://www.getkisi.com/blog/access-control-system-maintenance. Luettu 11.11.2021.

50 O'Brien, Jeff. Improve Maintenance with the Internet of Things. Verkkoaineisto. Saatavissa: https://www.reliableplant.com/Read/29962/internet-of-things. Luettu 24.11.2021.

51 EdgeConnector. 10 costly access control security pitfalls to avoid. Verkkoaineisto. Saatavissa: https://www.edgeconnector.com/costly-access-control-security-pitfalls/. Luettu 29.11.2021.

52 Mid-Atlantic Controls. 2017. Problems with Access Control Systems. Verkkoaineisto. Saatavissa: https://info.midatlanticcontrols.com/blog/problems-with-access-control-systems. Luettu 30.11.2021.

53 Peterson, Zachariah. 2021. Components for Machine Vision System Design. Verkkoaineisto. Saatavissa: https://octopart.com/blog/archives/2021/08/components-for-machine-vision-system-design. Luettu 16.12.2021.

54 Kuva 16. Kameran kuvan resoluution kasvattamisen aiheuttamat laitteistovaatimukset muistille, videon prosessoinnille, tallennukselle ja lähetykselle. Luettu 26.10.2021. Saatavissa: https://www.mouser.fi/applications/modern-machine-security/.

55 Grant McGregor Blog. 2016. The Three Most Common Access Control Issues. Verkkoaineisto. Saatavissa: https://blog.grantmcgregor.co.uk/2016/the-three-most-common-access-control-issues. Luettu 30.11.2021.

56 Chhabra, Atin. 2019. Understanding Challenges in Access Control Systems. Verkkoaineisto. Saatavissa: https://blog.se.com/building-management/2019/01/15/understanding-challenges-in-access-control-systems/. Luettu 30.11.2021.

57 AM Lukkoasema Oy. 2019. Turvasuojaustoiminta luvanvaraiseksi vuoden 2019 alusta alkaen. Verkkoaineisto. Saatavissa: https://www.amlukkoasema.fi/files/AML_elinkeinolupa_www.pdf. Luettu 26.10.2021.

58 Tilavahti.com. Kameravalvonta ja laki. Verkkoaineisto. Saatavissa: https://www.tilavahti.com/page/13/kameravalvonta-ja-laki. Luettu 2.12.2021.

59 Minilex. Rikoslaki ja kameravalvonta. Verkkoaineisto. Saatavissa: https://www.minilex.fi/a/rikoslaki-ja-kameravalvonta. Luettu 2.12.2021.