Jesse Jokelainen

Tekoälypohjainen videoanalytiikka poikkeamien tunnistuksessa ja ennakoivassa turvallisuudessa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Sähkö- ja automaatiotekniikka

Insinöörityö

27.11.2025

Tiivistelmä

Tekijä:	Jesse Jokelainen
Otsikko:	Tekoälypohjainen videoanalytiikka poikkeamien tunnistuksessa ja ennakoivassa turvallisuudessa
Sivumäärä:	28 sivua
Aika:	27.11.2025
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Sähkö- ja automaatiotekniikka
Ammatillinen pääaine:	Sähkövoimatekniikka
Ohjaajat:	Lehtori Juha Kallunki Työpaikkaohjaaja Petteri Pekonen

---

Tämä insinöörityö käsittelee ja kertoo tekoälypohjaisesta videoanalytiikasta ennakoivassa turvallisuudessa sekä poikkeamien tunnistuksessa. Työ toteutettiin Rejlers Oy:n pyynnöstä tavoitteena kertoa ja oppia tekoälyjärjestelmien mahdollisuuksista turvakamerajärjestelmissä.

Työssä kerrotaan, minkälainen toimiva kameravalvontajärjestelmä on. Työn teoriapohja tukeutuu sähkötekniikan perusteisiin ja sähkötietokortiston ohjeisiin, esimerkkeihin ja malleihin. Tekoälyn teoriapohjana työssä toimii koneoppiminen ja syväoppiminen.

Tulosten perusteella tekoälypohjainen videoanalytiikka parantaa merkittävästi valvontajärjestelmien tehokkuutta, vähentää inhimillisiä virheitä ja mahdollistaa poikkeamien automaattisen tunnistamisen reaaliaikaisesti.

Tekoälyjärjestelmät osoittautuivat erityisen hyödyllisiksi ennakoivassa turvallisuudessa, sillä ne pystyvät tunnistamaan riskikäyttäytymistä ja mahdollisia uhkia ennen vaaratilanteen syntymistä. Lisäksi havaittiin, että järjestelmien integrointi muihin turvallisuusteknologioihin, kuten kulunvalvontaan ja hälytysjärjestelmiin, lisää kokonaisuuden toimintavarmuutta ja reagointinopeutta.

avainsanat: tekoäly, kameravalvontajärjestelmät, turvallisuus, integraatio, videonhallintajärjestelmä,

---

Abstract

Author:	Jesse Jokelainen
Title:	Video Analytics for Anomaly Detection and Predictive Security
Number of Pages:	28 pages
Date:	27 November 2025
Degree:	Bachelor of Engineering
Degree Programme:	Electrical and automation engineering
Professional Major:	Electrical power engineering
Supervisors:	Juha Kallunki, Senior lecturer Petteri Pekonen, Design manager

---

This bachelor's thesis discusses and examines AI-based video analytics in predictive security and anomaly detection. The work was carried out at the request of Rejlers Oy with the aim of exploring and learning about the possibilities of AI systems in security camera systems.

The thesis reviews and discusses the definition and classification of camera systems, various camera types, the fundamentals of Power over Ethernet (PoE) technology and relevant standard requirements, as well as the concept of artificial intelligence and its applicability in video analytics. Furthermore, it considers how video and image data produced by AI-enabled camera systems are stored, the functioning of video management systems, and the extent to which these systems can contribute to predictive security. The work also presents examples of integrations between different security systems.

The findings indicate that AI systems provide significantly more advantages for individuals and organizations than disadvantages. The challenges and limitations associated with their use are relatively minor and can be effectively managed. AI technologies are already widely adopted in contemporary security systems and integrations, and their utilization is expected to increase further in the future.

Keywords: Artificial intelligence, Camera surveillance systems, Safety, Integration, Video management system

Sisällys

Lyhenteet

CNNs: *Convolutional neural networks system eli konvoluutioneuroverkot ovat tekoälyn ja koneoppimisen malleja, joita käytetään erityisesti kuvantunnistuksessa ja videoanalytiikassa.*

EX: *Explosive eli räjähtävä.*

GANs: *Generative adversarial networks system eli syväoppimisen menetelmä, jossa kaksi yhteydessä olevaa neuroverkkoa kilpailevat toisiaan vastaan ja oppivat niille annettuja tehtäviä tämän prosessin aikana.*

IR: *Infrared eli infrapuna.*

PoE: *Power over Ethernet tarkoittaa tekniikkaa, jossa sekä sähkövirta että tiedonsiirto kulkevat saman Ethernet-verkkokaapelin kautta.*

PTZ-kamera:
Pan Tilt Zoom -kamera on valvontakamera, jota voidaan etäohjata kääntymään sivusuunnassa (pan), kallistumaan ylös ja alas (Tilt) sekä zoomaamaan lähemmäs tai kauemmas (Zoom).

RNNs: *Recurrent neural networks system eli toistuvat neuroverkot ovat tekoälymalleja, jotka on suunniteltu käsittelemään sarjallista dataa, kuten puhetta, tekstiä tai videokuvaa.*

VMS: *Video management system eli videonhallintajärjestelmä on ohjelmisto, jota käytetään valvontakameroiden tallenteiden, suorien videovirtojen ja hälytysten hallintaan sekä katseluun yhdestä keskitetystä käyttöliittymästä.*

1 Johdanto

Tämä insinöörityö käsittelee ja tutkii tekoälypohjaista analytiikkaa poikkeamien tunnistamisessa sekä ennakoivassa turvallisuudessa. Työssä tutkitaan ja tuodaan esiin kamerajärjestelmien määritelmä, erilaisia kameratyyppejä, PoE-tekniikan (Power over Ethernet) perusteet ja standardivaatimukset. Lisäksi selvitetään, mitä tekoäly on ja mihin sitä voidaan käyttää videoanalytiikassa, miten tekoälyä käyttävät kamerajärjestelmän videot ja kuvat tallennetaan, kuinka videonhallintajärjestelmät toimivat ja mitä mahdollisuuksia ne antavat ennakoimaan turvallisuutta sekä kerrotaan esimerkkejä turvallisuusjärjestelmien integroinneista keskenään.

Työssä käsitellään myös eettisiä kohtia, jotka on otettava huomioon, kun tekoälyä hyödynnetään videoanalytiikassa. Lisäksi työssä kerrotaan videoanalytiikkaan perustuvan kamerajärjestelmän eduista verrattuna perinteiseen kamerajärjestelmään, jossa ei käytetä tekoälyä. Työn lopussa esitetään yhteenveto ja pohdintaa insinöörityön aiheesta sekä tekoälyä hyödyntävistä kamerajärjestelmistä.

Insinöörityön toimeksiantaja on Rejlers Oy. Rejlers Oy on teknisen alan suunnittelu- ja konsultointiyhtiö, joka on perustettu vuonna 1942. Rejlers Oy:n visioina ja arvoina on tuoda asiakkaille uusinta tietoa sekä teknologiaa, joita tarvitaan nykypäivänä yhteiskunnan murroksessa. Suomessa Rejlers Oy:llä on yli 1000 asiantuntijaa yli 20 paikkakunnalla. Rejlers konserni on listattuna Tukholman pörssissä, ja konserni vaikuttaa Suomen lisäksi myös Ruotsissa, Norjassa sekä Abu Dhabissa. (1.)

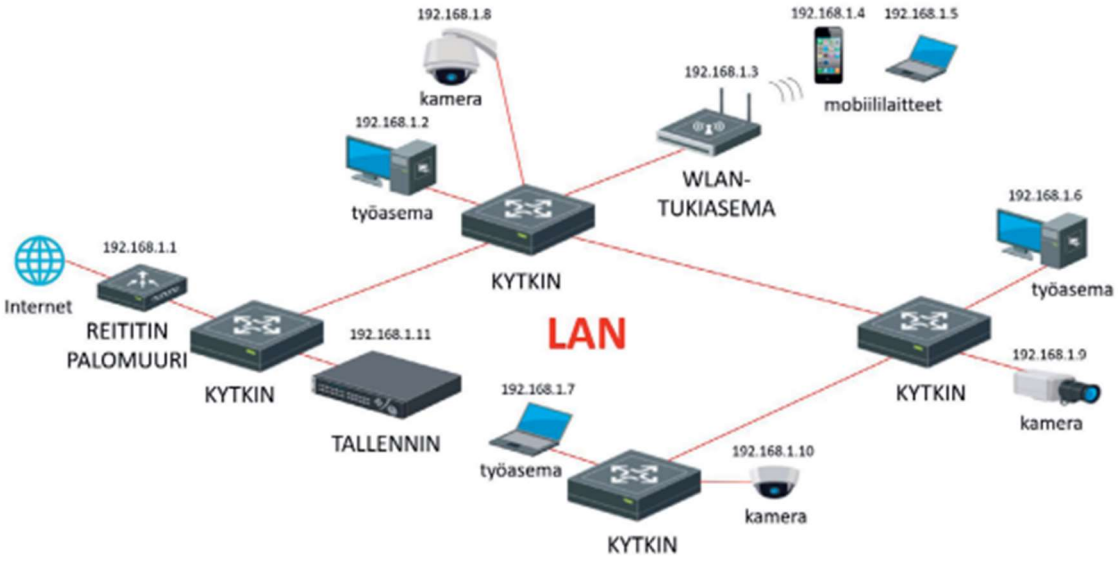
Opinnäytetyöraportin kieliasun muotoilussa ja tarkistamisessa on käytetty OpenAI:n ChatGPT:n versiota 5. Opinnäytetyön tekijä on vastuussa kaikesta opinnäytetyön sisällöstä ja muotoilusta.

2 Kamerajärjestelmät

2.1 Kamerajärjestelmän määritelmä ja perusteet

Kameravalvontajärjestelmä koostuu kamera-, tallennus- ja tarkkailulaitteista ja niihin integroiduista ohjelmistoista sekä laitteista, joita käytetään kuvan ja datan siirtoon sekä ohjaukseen. Kameravalvontajärjestelmän tarkoitus on valvoa ja kuvata erilaisia kohteita, mikä auttaa alueiden turvallisuuden valvonnassa. Kameravalvonta on lisääntynyt ja laajentunut perinteisestä valvonnasta ja rikoksien ehkäisystä myös kaupallisiin tarkoituksiin. Kaupallisiin tarkoituksiin soveltuvilla kamerajärjestelmillä voidaan kerätä esimerkiksi dataa, jota voidaan hyödyntää liiketoiminnan parantamisessa. (2.)

Kameravalvontajärjestelmillä on ominaista se, että ne voivat vastaanottaa kiinteistöjen muista järjestelmistä yksinkertaisia käskyjä integraatioiden kautta. Yleisimmät järjestelmäintegraatiot ovat kulunvalvonta-, murtoilmaisu-, paloilmoitin- ja prosessinvalvontajärjestelmä. Tiedon lähettäminen tapahtuu IP-osoitteiden eli internet protocol -osoitteiden avulla verkossa. (2.) Kuvassa 1 nähdään IP-pohjaisen kameravalvontajärjestelmän periaatekaavio. Periaatekaaviosta näkee, minkälainen laitekokonaisuus kameravalvontajärjestelmä voi esimerkiksi olla.



Kuva 1. IP-pohjaisen kameravalvontajärjestelmän periaatekaavio (2).

2.2 Kameratyyppejä

Suurimmassa ja tärkeimmässä osassa kameravalvontajärjestelmiä ovat itse kamerat. Kamerat valitaan aina valvottavan kohteen mukaan ja niiden suunnittelussa pitää ottaa huomioon asennuspaikan valaistus- ja sääolosuhteet sekä lisäksi muut toimintaympäristön erityisvaatimukset. Kamerat koostuvat yleisesti rungosta, optiikasta, piirilevystä, ohjelmistosta, virtalähteestä ja jalustasta. Kameroita myös suojataan tarpeen tullessa erilaisilla koteloilla. Kamerat voidaan jakaa niiden teknisten ja fyysisten ominaisuuksien mukaan. Kameroiden eri tyyppejä ovat kiinteät runkokamerat ja bulletkamerat, kiinteät kupukamerat, kääntökamerat, 360 asteen kamerat ja panoraamakamerat, lämpökamerat, droonit ja muut kameramallit. (3.)

Kiinteät runkokamerat ovat valvontakameroita, jotka kuvaavat yhtä tiettyä ja vakioitua kohdetta. Kamerat sisältävät kiinteän polttovälin objektiivin tai zoomattavan objektiivin. Nämä kamerat soveltuvat hyvin sisä- ja ulkokäyttöön. Luotikameroiden nimi tulee niiden luotia tai patruunaa muistuttavasta muodosta. Kiinteät runko- ja luotikamerat sisältävät todella usein sääsuojatun kotelon PoE-tuen analytiikkaominaisuuksia ja IR-valot (infrared-valot) yökuvauksia varten. (3.) Kuvassa 2 on esitetty runkokamera ulkokäyttöön ja luotikamerat sisä- ja ulkokäyttöön.

Kuva 2. Vasemmalta oikealle järjestyksessä Axis Communications AB:n runkokamera ulkokäyttöön, Hikvisionin luotikamera ja Robert Bosch Oy:n luotikamera (3).

Kiinteitä kupukameroita kutsutaan domekameroiksi. Domekameroissa objektiivi on sijoitettu suojakoteloon, jossa sitä suojaa ja peittää joko kirkas tai tummennettu akryyli- tai polykarbonaattikupu. Domekamerat ovat muuten teknillisesti samanlaisia kuin kiinteät runkokamerat. Ne ovat vain ulkomuodoltaan suunniteltu vähemmän silmiinpistäviksi. Näitä kameroita saa myös sisä- ja ulkokäyttöön. (3.) Kuvassa 3 on esitetty kolme erilaista domekameratyyppiä eri valmistajilta.

Kuva 3. Domekameroita vasemmalta oikealle järjestyksessä valmistajilta Hikvision, Axis Communications Ab ja Robert Bosch Oy (3).

Kääntöpääkameroita kutsutaan PTZ-kameroiksi (Pan Tilt Zoom). PTZ-kameroita käytetään laajojen ulkoalueiden ja esimerkiksi kauppakeskuksien valvonnassa. PTZ-kameroissa on moottoroitu kääntöpää ja moottoroitu zoomilla varustettu objektiivi, jonka ansiosta sillä voidaan zoomata ja tarkentaa kohteisiin kauko-ohjatusti. PTZ-kamerat ovat käytössä usein kulunvalvonta- ja murtoilmaisujärjestelmissä, koska kamerat saadaan helposti ohjelmoitua siten, että ne kääntyvät ja kuvaavat esimerkiksi avautuvaa porttia. (3.) Kuvassa 4 esitellään erilaisia PTZ-kameroita.

Kuva 4. Erilaisia PTZ-kameroita kameravalmistajilta Robert Bosch Oy, Axis Communications Ab ja Hikvision (3).

360 asteen kamerat kuvaavat koko kameran ympäristön. Kamerat koostuvat vähintään kahdesta, vastakkaisilla puolilla olevista objektiiveista, jotka yhdessä tuottavat yhden koko alueen kuvan. 360-kameroita käytetään tilojen yleisvalvontaan, jolloin halutaan nähdä yhdellä kuvalla, mitä alueella tapahtuu. Panoraamakameroita käytetään silloin kun halutaan erittäin laaja kuva-alue valvottavasta kohteesta. Panoraamakamerat ovat usealla kennolla toteutettuja laajakuvakameroita. Panoraamakameroiden kuva ei ole samanlainen kuin 360-kamerassa, vaan kuva-alue avautuu eteenpäin kameran linssistä ja voi esimerkiksi olla 160 astetta tai enemmän. (3.) Kuvassa 5 on nähtävissä yksi Mobotixin 360 asteen kamera ja yksi Axis Communications Ab:n panoraamakamera.

Kuva 5. Vasemmalla 360 asteen kamera ja oikealla panoraamakamera (3).

Lämpökameroiden kuvan tuotto perustuu lämpöön, joka säteilee kuvattavasta kohteesta. Lämpökameroiden kuva on mustavalkoista, mutta voidaan muokata ja tehostaa keinotekoisesti eri värein, mikä helpottaa havainnointia. Lämpökameroita käytetään yleensä esimerkiksi vankiloissa, lentokentillä, voimalaitoksissa, tunneleissa, silloilla ja raidealueilla, joissa tarvitaan ympärivuorokautista valvontaa. Lämpökameroita käytetään myös paloturvallisuuden ennakoinnissa ja tulipalojen havainnoinnissa. (3.) Kuvassa 6 on nähtävissä kaksi erilaista lämpökameraa valmistajilta Axis Communications Ab ja Hikvision.

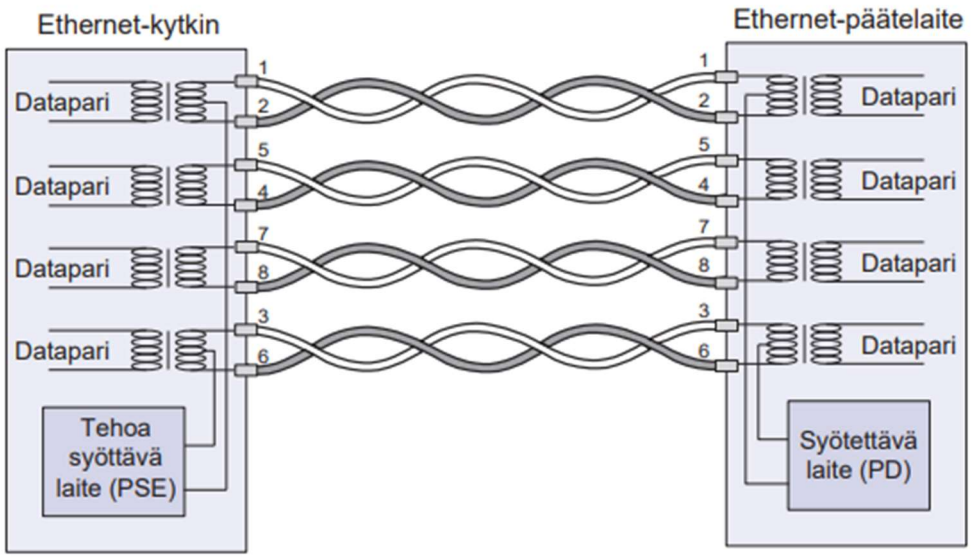
Kuva 6. Vasemmalla Axis Communications Ab:n lämpökamera ja vasemmalla Hikvisionin lämpökamera (3).

Maailmasta löytyy myös muita kameramalleja työssä edelle mainittujen lisäksi. Erikoisempia kameroita ovat esimerkiksi EX-kamerat (explosive-kamerat), jotka soveltuvat räjähdysvaarallisiin tiloihin, BI-spectrum-kamerat, joita käytetään esimerkiksi, paloriskien ennakointiin ja sitten vielä löytyy modulaarisia kameroita, jotka koostuvat erillisistä kamerapäistä ja keskusyksiköistä. Modulaariset kamerat soveltuvat vaativiin käyttöolosuhteisiin ja ahtaisiin tiloihin, kuten ajoneuvoihin, pankkeihin ja pankkiautomaateille. (3.) Kuvassa 7 nähdään esimerkkejä EX-kamerasta, BI-spectrum-kamerasta ja modulaarisesta kamerasta.

Kuva 7. Vasemmalta oikealle Axis Communications Ab:n EX-kamera, Hikvisionin BI-spectrum-kamera ja Mobotixin modulaarinen kamera (3).

2.3 PoE-tekniikka

PoE-tekniikka eli Power over Ethernet on yleinen valvontakamerajärjestelmissä käytetty tehonsyöttötekniikka. PoE-tekniikka on tarkoitettu Ethernet-lähiverkon päätelaitteiden tehonsyöttöön tasavirralla. Päätelaite, joka on PoE-syötettävä ei, tarvitse erillistä virransyöttöä sähköverkosta, vaan se saa käyttötehonsa parikaapelin kautta. Johdin, jota käytetään PoE-järjestelmässä virransyöttöön, muodostuu parikaapelin johdinparin rinnankytketyistä johtimista. PoE-virtapiiri tarvitsee vähintään kahta PoE-johdinta eli kahta parikaapelin johdinparia. (4.) Kuvassa 8 nähdään esimerkki kahden parin PoE-järjestelmästä.



Kuva 8. Periaatekuva PoE-järjestelmästä. Kuvassa siirretään tehoa kahdella parilla ja dataa neljällä parilla. (4.)

Ensimmäisessä PoE-standardissa IEEE 802.3af, joka julkaistiin vuonna 2003, määrättiin tehoa syöttävän laitteen enimmäislähtötehoksi 15,4 W ja syötettävälle laitteelle 12,95 W:n teho. Vuonna 2009 julkaistussa PoE-standardissa IEEE 802.3at oli huomattavia parannuksia verrattuna ensimmäiseen vuonna 2003 julkaistuun standardiin. Vuonna 2009 julkaistussa standardissa määriteltiin tehoa syöttävän laitteen enimmäistehoksi 30 W, joka mahdollistaa syötettävälle laitteelle 25,5 W:n tehon. Vuoden 2009 standardissa tehoa syöttävät laitteet jaettiin kahteen eri tyyppiin: tyyppiin 1, jossa lähtöteho 15,4 W ja tyyppiin 2, jossa lähtöteho 30 W. Järjestelmät perustuvat kahden parin käyttöön. (4.)

Vuonna 2018 julkaistiin tämän hetken uusin PoE-standardi IEEE 802.3bt, joka mahdollistaa neljän johdinparin käytön tehonsyötössä. Standardi IEEE 802.3bt määrittää kaksi uutta tehoa syöttävän laitteen tyyppiä tyypit 3 ja 4, joiden vastaavat enimmäislähtötehot ovat 60 W ja 90 W. Syötettävän laitteen saatavat tehot ovat tyypeillä 3 ja 4 vastaavasti 51 W ja 71 W. Standardi IEEE 802.3bt on taaksepäin yhteensopiva standardin 802.3at kanssa kuin myös standardi IEEE 802.3at on yhteensopiva taaksepäin standardin IEEE 802.af kanssa. (4.)

3 Tekoäly

3.1 Tekoälyn perusteet ja määritelmä

Kun puhutaan tekoälystä AI (artificial intelligence) tarkoitetaan tietokonejärjestelmiä, jotka pystyvät suorittamaan erilaisia tehtäviä, joihin normaalisti tarvittaisiin ihmisen päättelykyky taitoa, oppimista, suunnittelua, luovuutta ja päätöksentekoa (5).

Tekniset järjestelmät pystyvät tekoälyn ansiosta havainnoimaan ympäristöään, käsittelemään havaintoja ja ratkaisemaan ongelmia niihin ohjelmoituun päämäärään. Teknisissä järjestelmissä tietokone vastaanottaa tietoa esimerkiksi kameralta tai joltain tunnistinanturilta, jonka jälkeen tekoäly käsittelee kerätyn datan ja vastaa annettuun kysymykseen datan pohjalta. Tekoälyjärjestelmiä on erilaisia, joista parhaat pystyvät jopa muokkaamaan käytöstään tiettyyn

pisteeseen saakka analysoimalla ja käyttämällä aiempaa dataa, mitä järjestelmään on syötetty. Nykypäivänä tekoälyä pidetään hyvinkin keskeisenä osana yhteiskunnan digitalisaatiota ja se on saanut jopa paikkansa yhtenä Euroopan unionin prioriteeteista. (5.)

Tekoäly voidaan jakaa eri muotoihin, ja Euroopan komission määritelmässä tekoälyä on kahta erilaista. Ensimmäinen tekoälymuoto on ohjelmistot, jotka sisältävät esimerkiksi virtuaaliset avustajat, kuvia analysoivat ohjelmistot, hakukoneet, puheen- ja kasvojentunnistusjärjestelmät. Toinen tekoälymuoto on niin sanotusti ruumiillistettu tekoäly, johon sisältyy esimerkiksi robotit, itseohjautuvat autot ja droonit. Tekoäly on arkielämässä hyvinkin läsnä ja jopa niin huomaamaton, ettei edes aina tiedosta, milloin tekoälyä käyttää. Esimerkkeinä tekoälysovelluksista arkielämässä ovat verkko-ostokset ja niiden mainonta, hakukoneet, digitaaliset avustajat, konekäännökset sekä älykkäät kodit, kaupungit ja infrastruktuuri. (5.)

3.2 Koneoppiminen

Koneoppiminen on tekoälyn osa-alue, jossa keskitytään siihen, että tietokoneet ja laitteet voivat jäljitellä ihmisen oppimista, suorittaa tehtäviä itsenäisesti sekä parantaa suorituskykyään kokemusten ja datan avulla. Koneoppimisen algoritmin oppimisjärjestelmän voi jakaa kolmeen pääosaan. Pääosat ovat päätöksentekoprosessi, virhefunktio ja mallin optimointiprosessi. (6.)

Päätöksentekoprosessissa koneoppimisalgoritmeja käytetään ennusteen tai luokituksen tekemiseen. Päätöksentekoprosessi käyttää syötedataa, joka voi olla nimettyä tai nimetöntä ja josta sitten algoritmi tuottaa arvion datassa olevasta kuviosta. Virhefunktio taas arvioi mallin ennusteen. Jos on olemassa tunnettuja esimerkkejä, virhefunktio voi verrata mallin tulosta näihin esimerkkeihin ja arvioida uuden mallin tarkkuuden. Mallin optimointiprosessissa algoritmi toistaa, arvioi ja optimoi prosessia päivittäen annettuja arvoja itsenäisesti, kunnes saavutetaan ennalta määritetty tarkkuus. (6.)

Koneoppimisen koneoppimismallit voidaan myös jakaa kolmeen pääluokkaan. Pääluokat ovat valvottu oppiminen, valvomaton oppiminen ja puolivalvottu oppiminen. Valvottu oppiminen määritellään sen käytöllä merkityillä aineistoilla, joilla algoritmeja koulutetaan luokittelemaan tietoja tai ennustamaan tuloksia. Valvottu oppiminen auttaa ratkaisemaan erilaisia ongelmia, kuten roskapostin luokittelun erilliseen kansioon sähköpostissa. Valvotussa oppimisessa käytettyjä menetelmiä ovat neuroverkot, lineaarinen regressio, logistinen regressio ja tukivektorikone (SVM support vector machine). (6.)

Valvomaton oppiminen käyttää koneoppimisalgoritmeja analysoimaan ja klusteroimaan merkitsemättömiä aineistoja. Valvomattoman oppimisen algoritmit pystyvät löytämään piilotettuja kuvioita tai tietorakenteita ilman ihmisen väliintuloa. Valvomattoman oppimisen kyky löytää samankaltaisuuksia ja eroavaisuuksia tiedoista tekee siitä hyvän työkalun esimerkiksi tutkivaan data-analyysiin, asiakassegmentointiin sekä kuvan- ja kuviontunnistukseen. (6.)

Puolivalvottu oppiminen on nimensä mukaisesti välimalli valvotun ja valvomattoman oppimisen malleista. Ohjelmoinnin aikana puolivalvottu oppiminen käyttää pienempää merkittyä aineistoa ohjaamaan luokittelua ja ominaisuuksien poimintaa suuremmasta merkitsemättömästä aineistosta. Puolivalvottu oppiminen kykenee ratkaisemaan ongelman, jossa valvotun oppimisen algoritmilla ei ole tarpeeksi tietoa. (6.)

3.3 Syväoppiminen

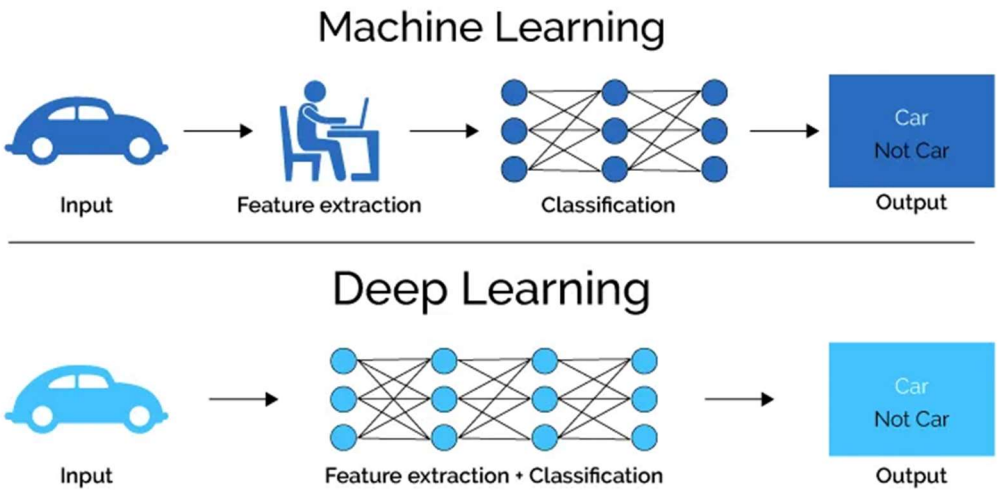
Syväoppiminen on yksi koneoppimisen osa-alue, joka käyttää monikerroksisia neuroverkkoja, joita kutsutaan syviksi neuroverkoiksi. Nykypäivänä suuri osa arkipäiväisistä tekoälysovelluksista käyttää jotakin syväoppimisen muotoa. Suurin ero syväoppimisen ja koneoppimisen välillä on niiden neuroverkkojen arkkitehtuurisessa rakenteessa. Ei-syvät koneoppimismallit käyttävät neuroverkkoja, joissa on yksi tai kaksi laskennallista kerrosta, kun taas syväoppimismallit käyttävät kolmea tai useampaa kerrosta. Tyypillisesti syväoppimismalli käyttää satoja tai jopa tuhansia kerroksia mallien kouluttamiseen. Syväoppiminen on

tekoälyn osa-alue, joka ohjaa monia sovelluksia ja palveluita, jotka parantavat automaatiota suorittaen analyyttisia ja fyysisiä tehtäviä ilman ihmistä. Syväoppiminen mahdollistaa palveluita, kuten digitaaliset avustajat, ääniohjatut TV-kaukosäätimet, itseohjautuvat autot ja generatiivisen tekoälyn. (7.)

Neuroverkot pyrkivät matkimaan ihmisaivoja yhdistelemällä datan syötteitä, painoja ja vinoumia, jotka kaikki toimivat piirisirujen hermosoluina. Yhdessä nämä elementit toimivat tunnistaakseen, luokitellakseen ja kuvatakseen data-aineiston kohteita hyvin tarkasti. Syvät neuroverkot koostuvat monista toisiinsa yhdistettyjen solmujen kerroksista, joista jokainen rakentuu edellisen kerroksen päälle tarkentaakseen ja optimoidakseen ennusteen tai luokittelun. Laskentaprosessin etenemistä verkon läpi kutsutaan eteenpäin suuntautuvaksi propagoinniksi. (7.)

Syvän neuroverkon syöttö- ja tulostekerroksia kutsutaan näkyviksi kerroksiksi. Syöttökerroksessa syväoppimismalli ottaa datan vastaan käsittelyä varten, ja tulostekerros on paikka, jossa lopullinen ennuste tai luokittelu tehdään. Toinen syväoppimisprosessi on takaisinpropagaatio, joka käyttää algoritmeja, kuten gradienttilaskua, laskeakseen virheitä ennustaessaan ja säätää sitten funktion painoja ja vinoumia liikkumalla taaksepäin kerrosten läpi mallin kouluttamiskeksi. Eteenpäin suuntautuva propagointi ja takaisinpropagaatio yhdessä mahdollistavat sen, että neuroverkko pystyy tekemään ennusteita ja korjaamaan mahdolliset virheet. Mitä enemmän tätä algoritmia käyttää, sitä tarkempi siitä tulee ajan myötä. (7.)

Syväoppimisalgoritmit ovat äärimmäisen monimutkaisia, ja sen takia on olemassa erityyppisiä neuroverkkoja erilaisten ongelmien tai aineistojen ratkaisemiseksi. Erilaisia neuroverkkoja on esimerkiksi CNNs (convolutional neural networks), RNNs (recurrent neural networks), Auto- ja variaatioenkooderit, GANs (generative adversarial networks), diffuusiomallit ja transformermallit. (7.) Kuvassa 9 esitetään yksinkertaistetusti, miten koneoppiminen ja syväoppiminen eroavat käytännössä toisistaan.



Kuva 9. Kuvaus miten koneoppiminen ja syväoppiminen eroaa toisistaan työvaiheissa (8).

4 Videoanalytiikka

Kun puhutaan videoanalytiikasta, tarkoitetaan kuva- ja videomateriaalin analysointia tekoälyn avulla. Koneoppimista käyttämällä pystytään muodostamaan tarkkaa kuvaa ihmisten käyttäytymisestä, tunteista ja kohtaamisista. Videoanalytiikan avulla pystytään myös tunnistamaan esineitä ja asioita reaaliaikaisesti. (8.) Videoanalytiikkaa voidaan käyttää esimerkiksi liiketoiminnan kehittämiseen, henkilölaskentaan, alueelliseen valvontaan, asiakasluokitukseen ja rekisterikilpien tunnistamiseen (3).

4.1 Keskeiset tekoälymenetelmät videoanalytiikan sovelluksissa

Kun kamera-analytiikalla tehdään havaintoja, voidaan niistä muodostaa tallenteita, kytkeä hälytyksiä sekä ilmoittaa hädästä henkilökunnalle tai vartijoille. Keskeisiä tekoälymenetelmiä videoanalytiikan sovelluksissa ovat hahmontunnistus, linjan ylitys, asiattoman oleskelun havaitseminen, kävijälaskenta ja tilannetieto, jonovahti, yksityisyyden suojaaminen sekä äänimaailman hyödyntäminen. (3.)

Hahmontunnistus on tekniikka, jonka avulla tunnistetaan hahmoja niiden liikkeiden ja koon perusteella. Hahmoja, joita kameralla voidaan tunnistaa, ovat esimerkiksi ihmiset, eläimet ja ajoneuvot. Hahmontunnistuksessa voidaan tekoälylle määrittää, mistä ja minkä kokoisista hahmoista halutaan hälytysilmoitus tai kirjaus. (3.)

Linjan ylityksessä kamerananalytiikalla määritetään halutulle alueelle viiva, jonka ylitystä sen tulee seurata reaaliaikaisesti. Tämä tekniikka on käytännöllinen esimerkiksi silloin kun halutaan tieto jokaisesta ajoportin sisään ajavasta autosta. (3.) Kuvassa 10 nähdään, kuinka linjan ylitys toimii kamerakuvassa.

Asiattoman oleskelun havaitsemisessa käytetään Loitering-analytiikkaa, joka on tarkoitettu asiattoman oleskelun havainnointiin. Loitering-analytiikka havaitsee henkilöitä tai hahmoja määritetyltä alueelta ja voidaan ohjelmoida antamaan hälytys, kun alueella oleskelu ylittää tietyn, määritellyn ajan. (3.) Kuvassa 10 nähdään esimerkki, miten kamera tunnistaa hahmot ja rajaa alueen.

Kuva 10. Esimerkkejä siitä, miten hahmontunnistus, linjan ylitys ja asiattoman oleskelun havaitseminen toimivat (3).

Kävijälaskentaa ja tilannetietoa pystytään suorittamaan suoraan kameroissa. Tekoäly kameroissa kykenee laskemaan kappalemääriä, jotka voidaan suoraan lähettää kamerasta raportointityökaluun. Raportointityökalusta nähdään suoraan esimerkiksi, kuinka monta asiakasta on kaupassa käynyt päivän aikana. (3.) Kuvassa 11 nähdään esimerkki minkälaisen taulukon raportointityökalu pystyy luomaan.

Jonovahti kameroissa auttaa henkilökuntaa havainnoimaan tietoa reaaliaikaisesti. Analytiikan avulla pystytään optimoimaan asiakasvirran tieto, joka parhaimmillaan vähentää henkilöstön työkuormaa ja asiakkaiden odotusaikaa. (3.) Kuvassa 11 nähdään esimerkki jonovahdista, joka informoi henkilöstöä, kuinka paljon kaupan kassalla on jonoa reaaliaikaisesti.

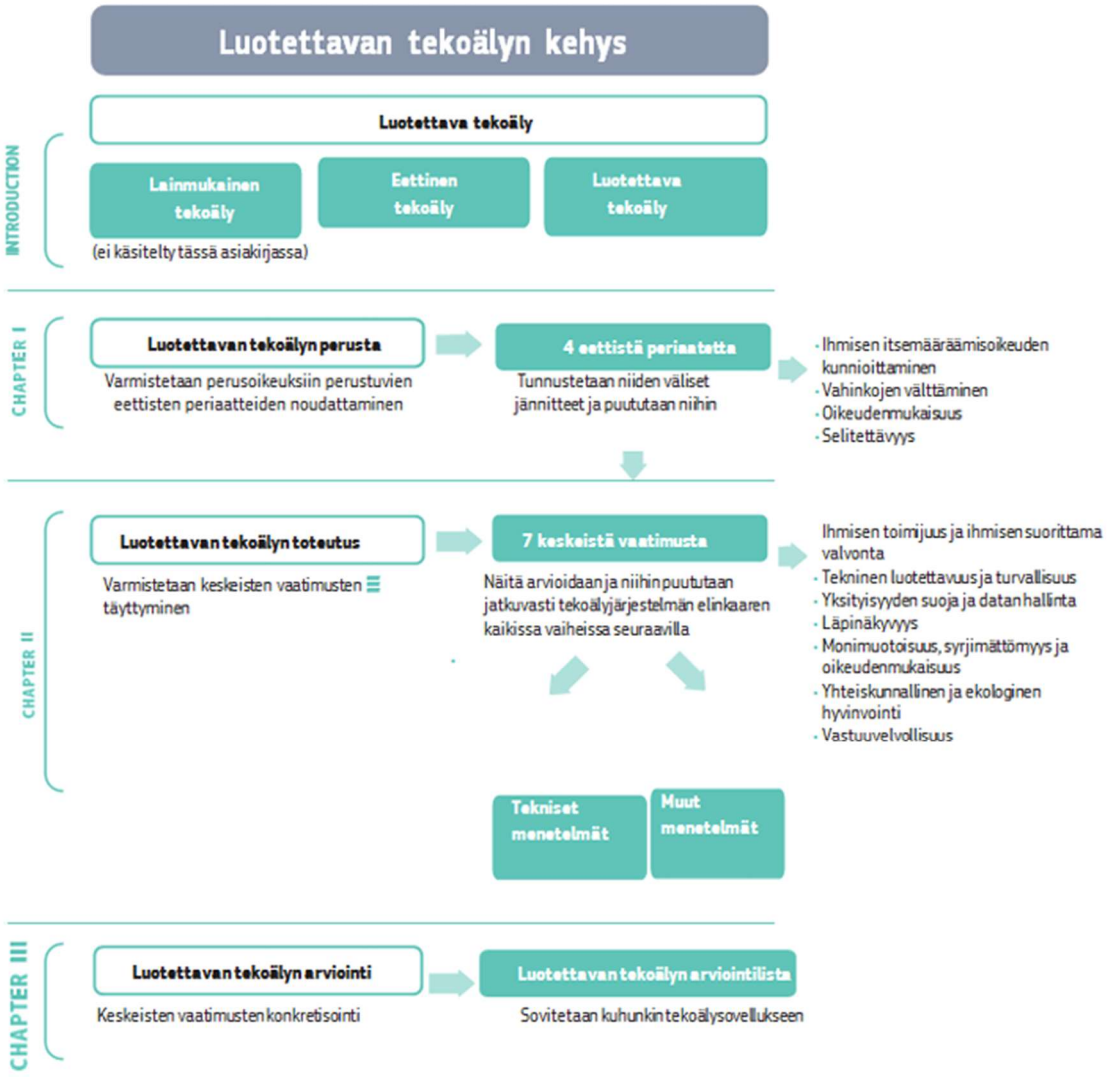
Kuva 11. Esimerkkejä kävijälaskenta- ja tilannetiedosta sekä jonovahdista (3).

Äänimaailman hyödyntäminen on myös nykypäivänä mahdollista kamerajärjestelmissä. Äänimaailmaa hyödynnetään automatisoimalla kuulutuksia analytiikan havaitsemien tietojen perusteella. Liikkeentunnistusominaisuuden avulla pystytään esimerkiksi käynnistämään kohteessa kuulutuksia tiedottaen alueen kameravalvonnasta tai kertomaan, että paikassa asiaton oleskelu on kiellettyä. Kameroihin on mahdollista myös yhdistää sisäänrakennettu mikrofoni, jonka avulla kohteeseen pystytään muodostamaan kaksisuuntainen puheyhteys, esimerkiksi valvottavan alueen ja vartiointiliikkeen välille. (3.)

Kameran mikrofonin ja äänianalytiikan avulla pystytään myös tehdä erilaisista äänistä havaintoja. Kameran äänianalytiikka pystyy tunnistamaan erilaisia ääniä kuten lasin rikkoutumisen, aseen laukauksen, auton varashälyttimen, huudot ja jopa aggressiiviset äänenpainot puheessa. Edellä mainittujen äänihavainnointien avulla pystytään tehdä hälytyksiä ilman, että ääniä tarvitsee tallentaa minnekään. (3.)

4.2 Eettiset näkökohdat tekoälyn soveltamisessa videoanalytiikkaan

Tekoälyn soveltamisessa videoanalytiikkassa nostaa esille eettisiä kysymyksiä. Luotettavan tekoälyn eettisyyttä voidaan arvioida Euroopan parlamentin kehittämällä ohjeistuksella. Luotettavan tekoälyn kehykseen kuuluu luotettavan tekoälyn perusta, luotettavan tekoälyn toteuttaminen ja luotettavan tekoälyn arviointi. Luotettavan tekoälyn kehys jaetaan siis kolmeen eri vaiheeseen, joissa jokaisessa kerrotaan ja käydään läpi erilaisia eettisiä periaatteita ja ohjeita. (10.) Kuvassa 12 nähdään luotettavan tekoälyn kehys ja sen eri vaiheiden sisältöjä.



Kuva 12. Luotettavan tekoälyn kehys ja vaiheiden sisältö tiivistetysti (10).

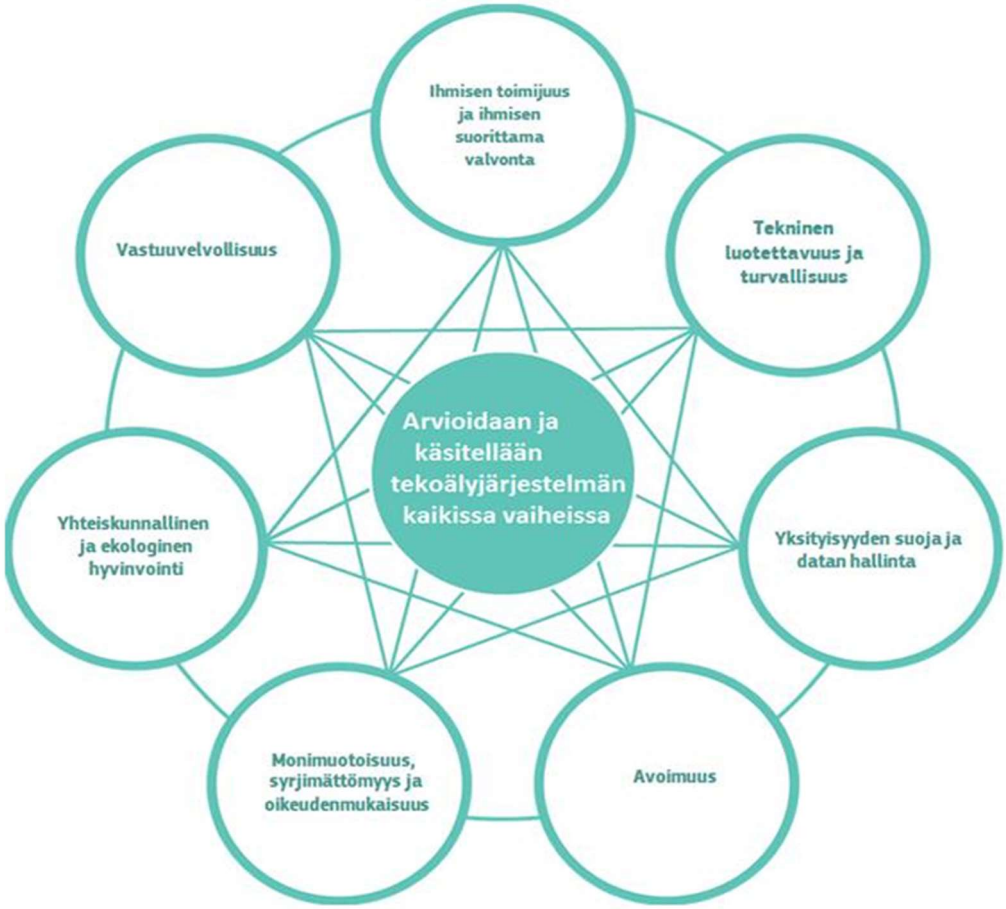
4.2.1 Luotettavan tekoälyn perusta

Luotettavan tekoälyn perustan idea on ohjeistaa, kuinka perusoikeuksiin perustuva lähestymistapa liitetään tekoälyjärjestelmien kehitykseen, käyttöönottoon ja käyttöön. Keskeiset eettiset ohjeet tekoälyjärjestelmien käytössä on muistaa kunnioittaa ihmisen itsemääräämisoikeutta, vahinkojen välttämistä ja olla selvillä järjestelmän oikeudenmukaisuudesta ja selitettävyydestä. Erityisesti huomiota tarvitsee kiinnittää tilanteisiin, joihin liittyy heikompia ryhmiä, kuten vammaisia, lapsia ja henkilöryhmiä, jotka ovat alttiita tilanteisiin, joissa vallitsee vallan tai tiedon epätasapaino. (10.)

Tekoälyjärjestelmien suunnittelussa ja käytössä kannattaa myös pitää mielessä, että tekoälyjärjestelmät hyödyttävät merkittävästi aina joitakin ihmisiä. Pahimmillaan tekoälyjärjestelmät pystyvät vaikuttamaan demokratiaan, oikeusvaltioperiaatteeseen ja oikeudenmukaisuuteen, minkä takia on huolehdittava tarvittaessa asianmukaisista toimenpiteistä näiden riskien lieventämiseksi. (10.)

4.2.2 Luotettavan tekoälyn toteuttaminen

Luotettavaa tekoälyä voidaan toteuttaa seuraamalla seitsemää vaatimusta, jotka tekoälyjärjestelmän tulisi täyttää. Seitsemän vaatimusta, joita tekoälyjärjestelmien kehittämisessä, käyttöönotossa ja käytössä pitäisi noudattaa, ovat ihmisen toimijuus ja ihmisen suorittama valvonta, tekninen luotettavuus ja turvallisuus, yksityisyyden suoja ja datahallinta, yhteiskunnallinen ja ekologinen hyvinvointi, vastuuvelvollisuus, läpinäkyvyys sekä monimuotoisuus, syrjimättömyys ja oikeudenmukaisuus. Tekoälyjärjestelmien toteuttamisessa olisi hyvä prosessin aikana olla mahdollisimman avoin ja opettavainen kaikille. Avoimuus ja opettaminen poistaa järjestelmien väärinkäyttöä, väärinkäsityksiä ja pitää tekoälyjärjestelmän valmiudet ja ihmisten odotukset realistisina. (10.) Kuvassa 13 nähdään seitsemän vaatimuksen keskinäiset suhteet.



Kuva 13. Seitsemän vaatimusta ja niiden keskinäiset suhteet (10).

4.2.3 Luotettavan tekoälyn arviointi

Luotettavan tekoälyn arvioinnin keskeiset ohjeet ovat laatia tekoälyjärjestelmän suunnittelu-, käyttöönotto- tai käyttövaiheessa luettelo kysymyksistä, joita tarvitsisi huomioida luotettavan tekoälyn arvioinnissa. Luettelon olisi hyvä sisältää kysymyksiä luotettavan tekoälyn toteuttamisessa esitetyistä vaatimuksista. (10.)

Tekoälyn arviointi on koko ajan jatkuva prosessi. Arviointiprosessin avulla pyritään kehittämään ja parantamaan tekoälyjärjestelmää sen koko elinkaaren aikana. Arviointiprosessi on mukautettava jokaiseen järjestelmään sopivaksi. Yhdellä ja tietyllä arviointilistalla ei pysty arvioimaan kaikkia järjestelmiä, koska järjestelmiä on niin moneen eri tarkoitukseen. Ohjeena on laatia jokaiselle

tekoälyjärjestelmälle oma kysymys ja arviointiluettelo parhaan lopputuloksen saamiseksi. (10.)

Tekoälyn mahdollistamat tehokkaat henkilötunnistusmenetelmät, kuten kasvojentunnistus ja muut biometriset teknologiat, tuovat mukanaan sekä etuja että vakavia eettisiä ja oikeudellisia huolenaiheita. Vaikka tällaisia menetelmiä voidaan käyttää hyödyllisiin tarkoituksiin, kuten petosten ja terrorismin torjuntaan, niiden hallitsematon käyttö voi uhata ihmisten itsemääräämisoikeutta. (10.)

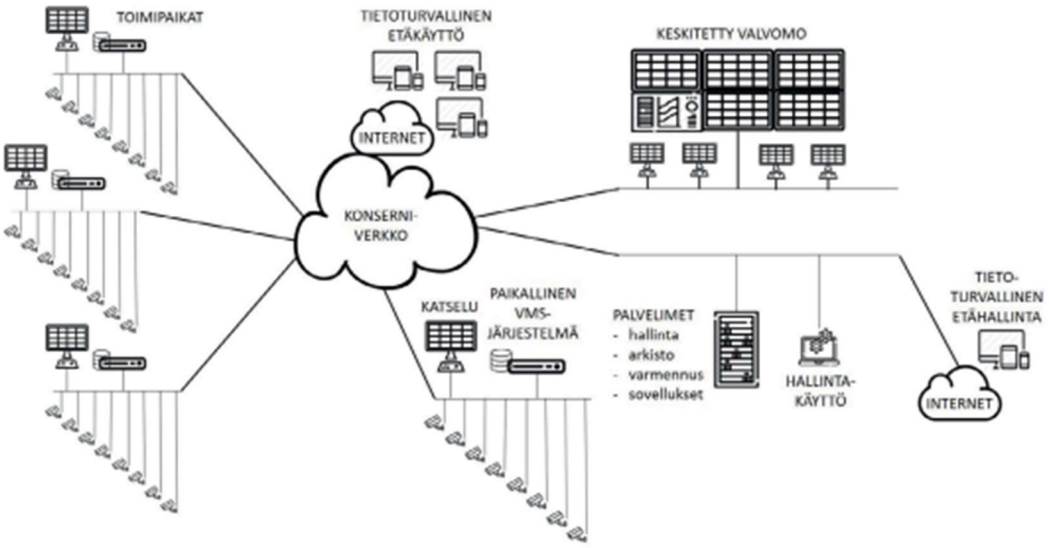
Tämän vuoksi on olennaista luoda luotettavan tekoälyn kehys, joka määrittää selkeästi, milloin ja miten automaattista tunnistusta voidaan käyttää. On tärkeää erottaa toisistaan tunnistaminen, jäljittäminen ja kohdennettu valvonta joukkovalvonnasta. Lisäksi tällaisen teknologian käyttö on sallittava ainoastaan voimassa olevassa lainsäädännössä. Jos perusteena on henkilön suostumus, on varmistettava, että suostumuksen antaminen on aitoa ja tietoista. Tämä pätee myös silloin, kun käytetään tunnistamattomia tietoja, jotka on mahdollista palauttaa tunnistettavaan muotoon. (10.)

5 Hallinta ja tallentaminen

Kamerajärjestelmien kuvien ja videoiden tallentamiseen sekä hallintaan voidaan käyttää monia erilaisia tekniikoita ja menetelmiä. Erilaisia tallennuspaikkoja ovat esimerkiksi kovalevy, verkkotallennin, muistikortti, videonhallintajärjestelmä ja pilvipalvelut. Erilaisia tallennintekniikoita ovat taas esimerkiksi perinteinen tallennin, verkkotallennin, hybriditallennin, ohjelmistopohjainen tallennus sekä videohallintajärjestelmä. Tallentamistekniikan ja menetelmän valintaan vaikuttaa tallennusten tallennustilan tarve. Videokuvan tiedosto kokoon vaikuttaa esimerkiksi, millä resoluutiolla ja kuvatahdilla kuvaa tallennetaan, mitä kuvan tallennusformaattia käytetään, mikä on vikasietoisuus ja tallennusten varmistusväli sekä se, kuinka kauan kuvaa halutaan säilyttää. (3.)

5.1 Videonhallintajärjestelmä

VMS (video management system) eli videonhallintajärjestelmä on järjestelmä, jonka avulla pystytään käsittelemään kameroiden kamerakuvaa ja niiden toimintaa. Videonhallintajärjestelmällä pystytään tallentamaan IP-kameroiden ja -palvelimien reaaliaikaista kuvaa sisäisille tai ulkopuolisille levyasemille. VMS-järjestelmä on suunniteltu suurten kameravalvontajärjestelmien hallintaa varten. VMS-järjestelmän avulla pystytään valvomaan useita kohteita ja paikkoja samaan aikaan yhdestä paikasta etänä. Kun valvotaan useita eri kohteita samaan aikaan, kutsutaan järjestelmää silloin nimellä monikäyttäjäjärjestelmä. Monikäyttäjäjärjestelmällä on tärkeää olla pääkäyttäjä, joka pitää huolta koko järjestelmästä ja sen käyttöoikeuksista. (3.) Kuvassa 14 nähdään esimerkki monitoimipaikkaisesta VMS-järjestelmästä.



Kuva 14. Esimerkki minkälainen VMS-järjestelmän monikäyttäjäjärjestelmä on (3).

5.1.1 VMS-järjestelmän käyttö ja hallinta

VMS-järjestelmä on sovellus, jota käytetään työaseman tai selaimen käyttöliittymällä. VMS-järjestelmää pystytään käyttämään pöytäasemilla, kannettavissa tietokoneissa, tableteissa ja älypuhelimissa. VMS-järjestelmiä voidaan hallita

kahdella erilaisella tavalla, jotka ovat tekninen hallinta ja käyttäjähallinta. Teknisessä hallinnassa hallitaan järjestelmää ja siihen liittyvien laitteiden konfiguraatioita sekä toimivuutta. Käyttäjähallinnassa taas hallitaan ja määritellään eri käyttäjien käyttöoikeuksia VMS-järjestelmään. Käyttöoikeuksia hallitsee pelkästään järjestelmän pääkäyttäjä. Varsinkin suuria VMS-järjestelmiä hallitaan valvomoista, joihin on keskitetty kaikki tarpeelliset koneet ja laitteet järjestelmän hallitsemiseksi. (3.)

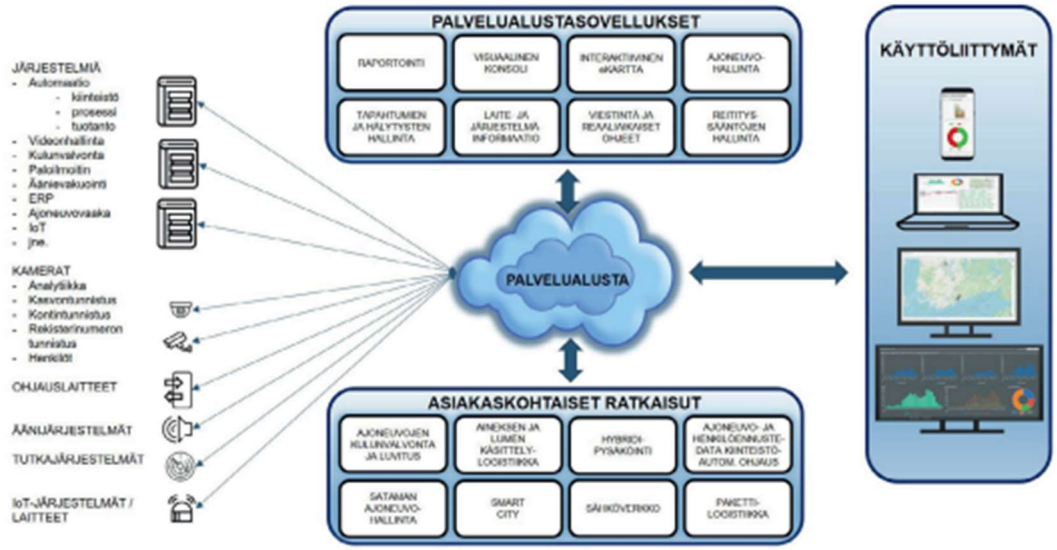
Valvomoita voi olla erilaisia käyttötarkoitukseen mukautettuja. Valvomot voivat olla pienikokoisia ja paikallisia, laajempia ja alueellisia tai sitten suuria koko järjestelmän kattavia valvomoita. Valvomoissa pystytään seuraamaan kamerajärjestelmien reaaliaikaista kuvaa, jonka avulla pystytään ennakoimaan ja havaitsemaan vaarallisia sekä poikkeavia tilanteita kohteissa. VMS-järjestelmään pystytään integroimaan havaitsemista helpottavia lisäsovelluksia ja ohjelmistoja. (3.)

5.1.2 Lisäsovellukset ja -ohjelmistot

VMS-järjestelmään liitettävät lisäsovellukset ja -ohjelmistot ovat erilaiset analytiikkasovellukset. Analytiikkasovellukset voivat olla esimerkiksi hahmontunnistus tai rekisterikilventunnistusohjelma. Usein analytiikkasovellukset ovat erillinen lisäohjelmisto, joka asennetaan VMS-järjestelmään joko erilliselle palvelimelle tai samalle palvelimelle kuin itse VMS-järjestelmä. Jotkut analytiikkasovellus valmistajat tuottavat myös sovelluksia, jotka ovat suoraan osa VMS-järjestelmää eikä niitä tarvitse asentaa erikseen. (3.)

Nykypäivänä kamerat itsessään sisältävät monipuolisia analytiikkasovelluksia ja tämä hyödyttää erityisesti VMS-järjestelmiä. Kun kameroissa on integroituna analytiikkasovellus, ei sitä tarvitse asentaa erikseen VMS-järjestelmään. VMS-järjestelmän avulla voidaan ohjata ja muokata kameran ominaisuuksia kuten muuttaa kuvanopeutta ja resoluutiota tilanteen vaatimalle tasolle. VMS-palvelualusta on laaja ja mahdollisuuksia täynnä analytiikkasovelluksien ja

ohjelmistojen ansiosta. (3.) Kuvassa 15 nähdään esimerkkikuva VMS-palvelualustakokonaisuudesta.



Kuva 15. Esimerkki VMS-palvelualusta mahdollisuuksista (3).

5.1.3 Kameroiden liitäntä VMS-järjestelmään

Kamerat on liitetty asiakkaan tietoverkkoon, joka on virtuaalinen erillisverkko tai fyysinen verkko. VMS-ohjelmistolla otetaan yhteys kameroihin asiakkaan oman tietoverkon sisällä. Vanhojen analogisten kameroiden liittäminen asiakkaan tietoverkkoon ei ole myöskään ongelma, koska ne voidaan liittää VMS:n erillisen videopalvelimen avulla tietoverkkoon. Jotta kamerat ja VMS-ohjelmisto pystyvät kommunikoimaan yhdessä, tarvitsee molempiin yhteensopivan liitäntärajapinnan. (3.) Liitäntärajapinta on tiedonvälittäjä kahden eri sovelluksen välissä, minkä avulla ne pystyvät kommunikoimaan. Liitäntärajapinnassa tapahtuu tietojen lähettämistä, lataamista ja eri toimintojen suorittamisen hyväksyntä. (11.) Liitäntärajapinta on olennainen tekijä siinä, mitä toiminnallisuuksia VMS-ohjelmisto pystyy käyttämään kameroissa. (3.)

5.2 Pilvipalvelut

Pilvipalvelut ovat yksi hyvä vaihtoehto, minkä avulla voidaan toteuttaa kameroiden käyttö, hallinta, tallennukset ja niiden katselu, tapahtumailmoitukset sekä analytiikat. Tämä edellyttää sitä, että asiakkaalla on oma tietoverkkonsa, tarvittavat ohjelmistot palveluntoimittajalta käyttöä ja hallintaa varten sekä riittävästi tallennuskapasiteettiä kuvaa ja dataa varten pilvessä. Pilvipalveluverkossa tärkeintä on se, että verkossa on tarpeellinen määrä IP-portteja kameroita ja verkon muiden komponentteja varten. (3.)

Pilvipalveluun yhdistämisessä valvontakamerajärjestelmät vaativat lisenssejä toimiakseen, ja nämä lisenssit yhdistävät kamerat ulkoiseen palveluun. Kun kamerat otetaan käyttöön ja niihin kirjaudutaan, niiden kuvasyöte avautuu verkkosovelluksissa sekä tietokone- ja mobiilisovelluksissa. Jokainen laite, joka liitetään verkkoon, tarvitsee oman lisenssinsä, kuten IP- tai kanavalisenssin, mikä mahdollistaa niiden sujuvan ja turvallisen toiminnan osana kokonaisjärjestelmää. (3.)

5.3 Datan tallentaminen

Datan tallentaminen kamerajärjestelmissä tapahtuu erilaisten tallentimien tai pilvipalvelun avulla. Valvontakamerajärjestelmissä kuvamateriaalin tallennus on olennainen osa kokonaisuutta, ja tallennusratkaisun valinta riippuu useista tekijöistä. (3.)

Tyypillisesti materiaali tallennetaan levyasemille, jotka voivat sijaita joko samassa työasemassa tai palvelimessa kuin videohallintajärjestelmä. Vaihtoehtoisesti voidaan käyttää erillistä levyjärjestelmää. Tallennustilan tarve määräytyy ensisijaisesti tallennettavan aineiston määrästä ja siitä, kuinka pitkään materiaalia on säilytettävä. Lisäksi varmennuksen tarve vaikuttaa valintaan, sillä kriittisen materiaalin on oltava turvallisesti tallennettuna. Jos jotakin tallennettua aineistoa tarvitsee säilyttää pidempään kuin alkuperäinen tallennusaika mahdollistaa, se voidaan siirtää automaattisesti toiseen tallennuspaikkaan. Toinen

tallennuspaikka mahdollistaa materiaalin jatkokäsittelyn ja arkistoinnin, mikä on tärkeää esimerkiksi tutkintatapauksissa tai muissa tilanteissa, joissa materiaalia voidaan tarvitaan myöhemmin. (3.)

Tallennin on laite, johon kytketään valvontakamerajärjestelmän kaikki kamerat ja seuranta näytöt. Tallentimet koostuvat usein sisäänrakennetusta PoE-kytkimestä, kovalevystä ja tallenninohjelmistosta. Tallentimissa ei ole omaa käyttöjärjestelmää, vaan ne ovat käytännössä valmistajakohtaisia sulautettuja ohjelmistokokonaisuuksia. Tämän ansiosta tallentimien käyttöönotto on helppoa ja lähes automaattista. Jokaisen tallentimen yhteensopivuus kameroiden kanssa pitää kuitenkin tarkistaa laitetoimittajilta. (3.)

Tallentimiin on mahdollista saada erilaisia internetti- ja työasemakäyttöliittymiä, joiden ansiosta tallentimista voidaan katsoa reaaliaikaista kuvaa muualtakin kuin laitteen sijoituspaikasta. Tallentimia on erikokoisia, ja tärkein kriteeri tallentimen valitsemiseen on kamerajärjestelmän kameramäärä. Yhdellä tallentimella voidaan tallentaa jopa kolmenkymmenenkahden eri kameran videokuvaa. (3.)

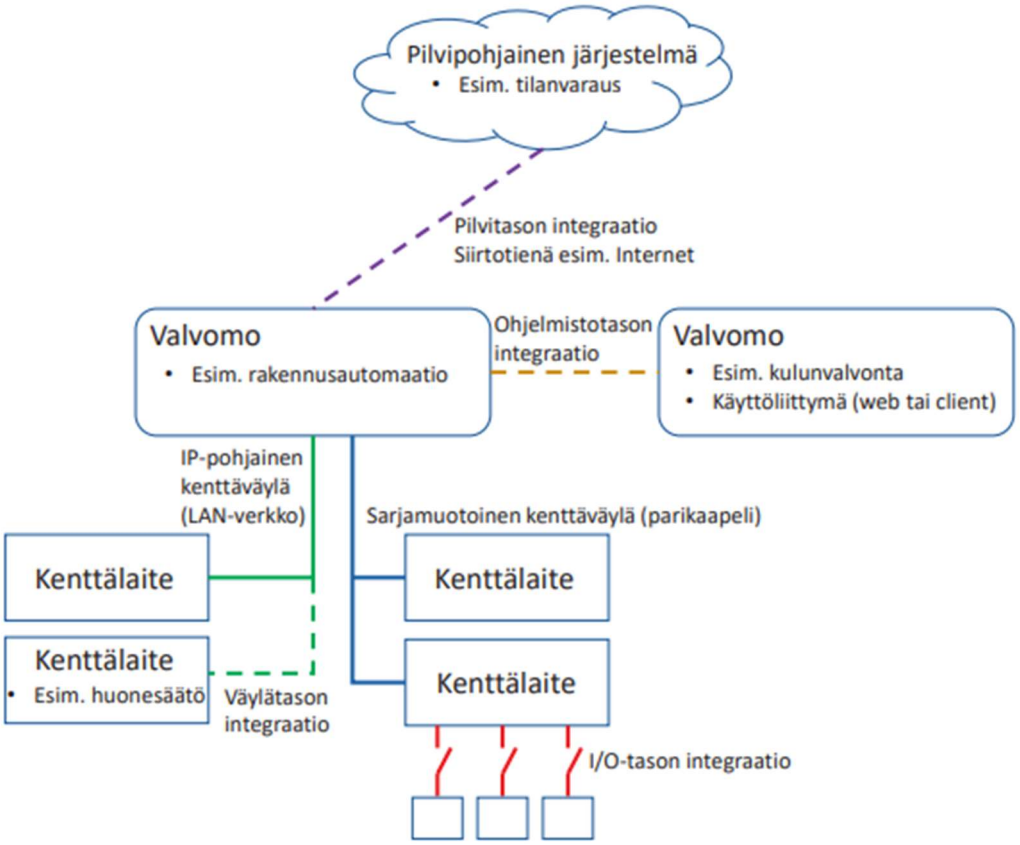
6 Turvallisuusjärjestelmien integrointi

Turvallisuusjärjestelmien integroinnilla tarkoitetaan erilaisten järjestelmien yhteen liittämistä. Integrointia voidaan tehdä hyvin yksinkertaisena toteutuksena, esimerkiksi yhden relekoskettimen yhteisohjauksena tai integrointi voidaan viedä hyvinkin pitkälle, jolloin se perustuu tietoliikenneverkon avoimeen arkkitehtuuriin ja toimintojen sekä ominaisuuksien yhteisohjaukseen graafisten käyttöliittymien avulla. (12.)

Järjestelmä integraatioiden tavoitteena on helpottaa erilaisten järjestelmien käyttöä ja luoda helposti hallittavia kokonaisuuksia. Integroinneilla pystytään luomaan automaattisia toimintoja eri osajärjestelmiin toisista osajärjestelmistä saaduilla tiedoilla. Esimerkiksi paloilmoitinjärjestelmä voi ilmoittaa palosta, jonka

jälkeen tieto siirtyy ilmanvaihtojärjestelmään, joka sulkee tai säätää ilmanvaihtoa automaattisesti. (12.)

Järjestelmien integraatioita voidaan toteuttaa erilaisilla tasoilla. Järjestelmien integraatiotasoja ovat fyysisesti kaapelointitasolla, fyysisesti kenttälaitetasolla, fyysisesti tai ohjelmallisesti keskustasolla ja ohjelmallisesti käyttöliittymätasolla. Integroinneissa käytetään myös aina jotakin teknistä ratkaisua, ja niitä ovat esimerkiksi I/0-tason, väylätason, valvomo- ja ohjelmistotason, pilvitason ja käyttöliittymätason integrointi, kenttäväylätekniikat, lähiverkon ja internetin käyttö sekä operaattoreiden tarjoamat palvelut ja verkkoratkaisut. (12.) Kuvassa 16 nähdään hahmotelma, kuinka nämä erilaiset integraatiotasot liittyvät toisiinsa.



Kuva 16. Hahmotelma erilaisista integraatiotasoista (12).

Integrointeja esiintyy erilaisissa turvallisuusjärjestelmissä. Turvallisuusjärjestelmiä, joissa on integraatioita, ovat esimerkiksi kulunvalvonta-, murtoilmaisu-, poistumisovi-, kameravalvonta-, paloilmoitin- ja valaistusjärjestelmät. (12.)

Kulunvalvontajärjestelmät eivät toimi ainoastaan erillisinä teknisinä ratkaisuina, vaan ne voidaan liittää osaksi laajempaa organisaation tietojärjestelmäkokonaisuutta. Perusohjelmiston tueksi voidaan ottaa käyttöön erilaisia sovelluksia, jotka mahdollistavat järjestelmän integroinnin esimerkiksi turvatekniikkaan ja henkilöstöhallintoon. Kulunvalvontajärjestelmän ylläpito voidaan keskittää määrätyille työasemille, joista käsin hallinta tapahtuu lähiverkon kautta. Tällainen liitäntätapa tarjoaa mahdollisuuden hyödyntää olemassa olevia tiedonsiirtoverkkoja sekä niihin kehitettyjä suojaus- ja etäkäyttöratkaisuja. Integraation avulla kulunvalvonta muuttuu pelkästä ovien hallinnasta osaksi turvallisuuden ja hallinnan tukijärjestelmäkokonaisuutta. (12.)

Murtoilmaisujärjestelmää voidaan tehostaa kulunvalvonnan integraation avulla. Yleisin integraatio murtoilmaisen ja kulunvalvonnan välillä on ovivalvonnan ohitus. Järjestelmien yhteisten käyttöliittymien avulla pystytään vastaanottaamaan ilmoituksia alueiden tilatiedoista, ilmaisimien hälytyksistä sekä kulunvalvonnassa kerätyt ovitiedot saadaan tallennettua ja käsiteltyä järjestelmien yhteisessä valvontagrafiikassa. (12.)

Kameravalvontajärjestelmien toimintaa voidaan tehostaa merkittävästi integroimalla niihin ohjauksia muista turvajärjestelmistä. Tällöin kamerat eivät ainoastaan tallenna kuvaa passiivisesti, vaan ne reagoivat automaattisesti erilaisiin tapahtumiin. Esimerkiksi kulunvalvonnasta saatu tieto voi ohjata kameran kääntymään ja tarkentumaan tietylle ovelle, jolloin tilanne näkyy välittömästi valvomossa ja tallentuu järjestelmään. Vastaavasti kamerat voidaan aktivoida ovipuhelimen kutsun, portin käytön tai murtohälytyksen perusteella. (12.)

Paloilmoitinjärjestelmään pystytään integroimaan muiden pelastustehtäviä edistävien laitteiden toimintakäskyjä. Relelähdöillä pystytään paloilmoitinkeskuksesta ohjaamaan esimerkiksi palosulkukoneistoa, savunpoistoluukkuja, paloovia sekä hätäkuulutusjärjestelmää. I/0-tason lisäksi paloilmoitinjärjestelmiin

voidaan integroida järjestelmiä, joiden avulla pystytään tuottamaan esimerkiksi ennakointia helpottavia ilmoituksia kiinteistönhallintajärjestelmiin ilmaisimien likaantumisesta. Rakennusautomaation avulla paloilmoitinjärjestelmät pystyvät ennakoimaan mahdollisia palotilanteita ja sillä tavoin parantamaan turvallisuutta huomattavasti. (12.)

Valaistusjärjestelmien integroinneilla voidaan parantaa turvallisuutta esimerkiksi kulunvalvonta-, paloilmoitin- ja rakennusautomaatiojärjestelmien avulla. Valaistusjärjestelmän ohjauksella pystytään pitämään esimerkiksi palohälytysten aikana poistumistiet selkeästi valaistuna niin, että ihmiset löytävät ja näkevät tiensä ulos helposti sekä turvallisesti. (12.)

Poistumisteiden ja hätäovien varmuuslukituksella on tärkeä rooli turvallisuuden varmistamisessa, koska niitä ei saa pitää päiväkäytössä kiinni, jotta poistuminen olisi aina esteetöntä. Suurissa myymälöissä ja tavarataloissa varmuuslukot toimivat usein sähköisesti ja niitä voidaan hallita omalla järjestelmällään tai kulunvalvonnan kautta. (12.)

7 Tekoälypohjaisen ja perinteisen kamerajärjestelmätoteutuksien vertailu

Tekoälyn määrä on kasvanut kamerajärjestelmissä viime vuosina ja näin ollen syrjäyttänyt kamerajärjestelmiä, joissa ei käytetä tekoälyä lainkaan. Tekoälyn tuomia etuja kamerajärjestelmissä ovat esimerkiksi kuvantunnistuksen ja automaation avulla saavutettava parempi tehokkuus ja tarkkuus. Tekoälyn avulla pystytään käsittelemään suuria määriä videodataa, mikä mahdollistaa huomattavasti nopeampaa reagointia eri tilanteisiin. Tekoälyjärjestelmät auttavat automaation ja hälytyksien avulla turvahenkilöitä sekä vartijoita keskittymään heille tärkeämpiin työtehtäviin ja tapahtumiin. Tekoälyn avulla pystytään myös ennakoimaan mahdollisesti epäilyttävää toimintaa todella paljon nopeammin ja tarkemmin kuin perinteisellä kamerajärjestelmällä pystytään. (13.)

Varsinkin yrityksille tekoäly kameravalvontajärjestelmissä tuo etuuksia. Kustannussäästöt ovat yksi merkittävä etuus yrityksille, koska tekoälyllä pystytään vähentämään manuaalisen työn tarvetta. Tekoäly pystyy automaattisesti analysoimaan ja monitoroimaan valvontadataa. Tekoälykamerajärjestelmillä pystytään myös ehkäisemään tehtailla ja tuotannoissa mahdollisesti alkavia ongelmia. Ongelmien ennakointi estää tehtaiden ja tuotantolinjojen seisokkeja sekä parantaa myös yleisesti turvallisuutta. (13.)

Tekoälyllä varustetut kamerajärjestelmät voivat tukea myös vastuullisuutta ja yritysten vastuullisuustavoitteita. Tekoälyn avulla saadaan optimoitua valvontajärjestelmiä säästämään energiaa, ja niistä saadaan näin ollen hyvinkin energiatehokkaita. Tekoäly parantaa ja tukee turvallisuusprosesseja jatkuvasti ennakoimalla vaaratilanteita, ja näin saadaan luotua kaikille turvallisempia ympäristöjä tulevaisuudessa. (13.)

Vaikka tekoäly kameravalvontajärjestelmissä antaa useita hyötyjä ja etuja, tulee sen mukana myös vähän haasteita. Suurin haaste on yksityisyyssuojan turvaaminen. Järjestelmät tuottavat todella suuren määrän dataa, jonka tallentaminen ja käsittely saattaa olla vaikeaa, kun noudatetaan tietosuojalainsäädännön sääntöjä. Eettiset kysymykset ja datan hallinta ovat keskeisiä huolenaiheita tekoälyjärjestelmissä, jota ei taas ole perinteisissä kameravalvontajärjestelmissä. (13.)

8 Yhteenveto ja pohdinta

Tästä insinöörityöstä voidaan todeta, että videoanalytiikka ja tekoäly parantavat ennakoivaa turvallisuutta sekä helpottavat poikkeamien tunnistusta. Työssä esitettiin ja käytiin läpi kamerajärjestelmän määritelmä ja perusteet, erilaiset kameratyypit, PoE-tekniikan perusteet, tekoälyn perusteet ja määritelmä sekä mitä koneoppiminen ja syväoppiminen on, videoanalytiikan keskeiset tekoälymenetelmät, eettiset näkökohdat tekoälyn soveltamisessa videoanalytiikkaan, videonhallintajärjestelmien toiminta ja tallentaminen, turvallisuusjärjestelmien

integrointi sekä mitä hyötyjä tekoälyllä toimiva kamerajärjestelmä tuo verrattuna perinteiseen kamerajärjestelmään.

Mielestäni tekoälyjärjestelmä ennakoivassa turvallisuudessa tulee olemaan tulevaisuudessa koko ajan suuremmassa roolissa. Näillä järjestelmillä pystytään tarkentamaan ja automatisoimaan niin monia eri asioita, mihin ihmisten ei kannata käyttää omia resursseja. Vaikka tekoälyllä varustetut kamerajärjestelmät tuovat omia haasteitaan eettisestä näkökulmasta ja tietosuojalain puitteissa ovat niiden tuomat hyvät puolet, kuten ennakoiva turvallisuus ja hahmontunnistus huomattavasti kannattavampia ihmisille ja yrityksille.

Tälle työlle luonnollinen jatkokehityskohde olisi tutkia ja syventyä lisää järjestelmäintegraatioihin. Tässä työssä järjestelmäintegraatioista kerrotaan perustietoja ja käyttökohteita, mutta niihin syventymällä pystyisi melkein toteuttamaan toisen insinöörityön laajuudeltaan. Jos aloittaisin työn tekemisen uudestaan alusta, niin jättäisin itse kamerajärjestelmien toiminnan tutkimisen vähemmälle ja keskittyisin enemmän juuri järjestelmäintegraatioihin. Työn toteutus ja läpi vieminen onnistui suunnitelman mukaisesti ilman haasteita.

Lähteet

1 Meistä. Verkkoaineisto. Rejlers Oy. < https://www.rejlers.com/fi/meista/>. Luettu 12.9.2025.

2 Kameravalvontajärjestelmän suunnitteluohje. 2017. ST664.10. Sähköinfo.

3 Arenius, K; Hovinen, R & Sähkötieto. 2021. Kameravalvontajärjestelmät. E-kirja. Sähköinfo Oy.

4 Koivisto, P; Jaakohuhta, H; Härkönen, P & Sähkötieto. 2021. PoE-tekniikka käytännössä. E-kirja. Sähköinfo Oy.

5 Mitä tekoäly on ja mihin sitä käytetään? 2023. Verkkoaineisto. Euroopan parlamentti. <https://www.europarl.europa.eu/topics/fi/article/20200827STO85804/mita-tekoaly-on-ja-mihin-sita-kaytetaan>. Päivitetty 20.6.2023. Luettu 13.8.2025.

6 What Is Machine Learning? Verkkoaineisto. IBM. <https://www.ibm.com/think/topics/machine-learning>. Luettu 14.8.2025.

7 What Is Deep Learning? Verkkoaineisto. IBM. <https://www.ibm.com/think/topics/deep-learning>. Luettu 19.8.2025.

8 A.I. Technical: Machine vs Deep Learning. Verkkoaineisto. Lawtomated. <https://lawtomated.com/a-i-technical-machine-vs-deep-learning/>. Luettu 20.8.2025.

9 Videoanalytiikka. Verkkoaineisto. CGI. <https://www.cgi.com/fi/fi/data-analytiikka/videoanalytiikka>. Luettu 21.8.2025.

10 Luotettavaa tekoälyä koskevat eettiset ohjeet. 2018. Verkkoaineisto. Euroopan parlamentti. <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_FI.pdf>. 18.12.2018. Luettu 26.8.2025.

11 Mikä on ohjelmointirajapinta (API)? Verkkoaineisto. SAP. <https://www.sap.com/finland/products/technology-platform/integration-suite/what-is-api.html>. Luettu 1.9.2025.

12 Tietoteknisten järjestelmien integrointi. 2025. ST682.10. Sähköinfo.

13 Kameravalvonnan ja tekoälyn tulevaisuus. 2025. Verkkoaineisto. Asiantuntijakeskus BEPOP.

<https://www.asiantuntijakeskusbepop.fi/asiantuntijat/kameravalvonnan-ja-tekoalyn-tulevaisuus-360-security-solutions/>. 26.3.2025. Luettu 1.9.2025.