



KAMERAVALVONTAOPAS

Turva-alaan yrittäjät ry

Versio 2.0 2020



JULKAISIJA JA KUSTANTAJA

Turva-alan yrittäjät ry
www.turva-alanyrittajat.fi

PÄÄTOIMITTAJA

Kimmo Arenius, Turva-alan yrittäjät ry

KÄSIKIRJOITTAJAT

Vuoden 2020 Kameravalvontaoppaan työryhmä:

Kimmo Arenius, Turva-alan yrittäjät ry

Veijo Kauppi, Sähköinfo Oy

Roger Lehtonen, STUL ry

Aku Pänkäläinen, Finanssiala ry

Petri Käyhkö, Kesko Oyj

Pekka Sallinen, Poliisihallitus

Patrik Westerlund, Milestone Systems

Kim Kattilakoski, Oy Hedengren Security Ab

Jukka Siivonen, Certego Oy

Mats Lindeqvist, Stanley Security Oy

Jouni Virta, Axis Communications Ab

Veli-Matti Luukkanen, Web Your Services Oy

Reijo Hovinen

2., uudistettu painos

Kansi 123RF

ISBN 978-952-231-331-7 (nid.)

ISBN 978-952-231-310-2 (pdf)

Kameravalvontaoppaan sisältö on vapaasti käytettävissä ja opas on vapaasti jaettavissa, jos sen sisältöä ei muuteta ja julkaisija Turva-alan yrittäjät ry mainitaan.

Tämä on oppaan toinen versio. Sen käsikirjoitus perustuu kesällä 2020 voimassa olevaan lainsäädäntöön ja sen aikaisiin tietoihin.

Opasta päivitetään tarvittaessa ja se on ladattavissa osoitteessa www.turva-alanyrittajat.fi/kameravalvontaopas.

Kameravalvontaoppaan päivitystyötä ovat tukeneet seuraavat yritykset ja yhteisöt:

Stanley Security Oy, Oy Hedengren Security Ab, Certego Oy, Caverion Suomi Oy, BLC Turva Oy, Axis Communications Ab, Capitis Control Oy, Emsec Oy, WSP Finland Oy, Finanssiala ry ja Suomen Pelastusalan Keskusjärjestö ry.

SISÄLTÖ

1	JOHDANTO	6
1.1	Oppaan julkaisija	6
1.2	Oppaan tausta.....	6
1.3	Oppaan tarkoitus	7
1.4	Kameravalvonta turvallisuuden osatekijänä.....	7
2	RAKENNE JA TEKNIikka.....	10
2.1	Kameroita ja niiden käyttötapoja.....	10
2.2	Kameroiden tekniikka, kuvatahti ja resoluutio	16
2.3	Tallentimet.....	17
2.4	Yhteydet	18
2.5	Videohallintajärjestelmä	21
2.6	Analytiikkaohjelmistot.....	31
2.7	Kamerateknologian hyödyntäminen paloturvallisuudessa	33
3	SUUNNITTELU JA HANKINTA	36
3.1	Tarveselvitys.....	37
3.2	Hankesuunnitelma	41
3.3	Hankintakustannukset	41
3.4	Suunnittelijan valinta	42
3.5	Hankintaprosessin lainsäädäntö	43
3.6	Esimerkkejä kameravalvonnan laillisuudesta	43
3.7	Standardi ja K-menetelmä kameravalvonnan suunnittelun tukena	47
3.8	Olosuhteiden huomioiminen suunnittelussa	52
3.9	Valvomoiden ja kuvien katselupisteiden suunnittelu	57
4	TOTEUTUS	61
4.1	Toteutussuunnittelu	61
4.2	Tarjouspyyntöasiakirjat.....	61
4.3	Tarjousvertailu ja hankintapäätös	62
4.4	Asennus ja käyttöönotto	63
5	KÄYTTÖ JA YLLÄPITO	65
5.1	Käyttäjien valinta ja koulutus	65
5.2	Tallenteiden käsittely	66
5.3	Tallenteiden luovutus ja luovutusdokumentointi.....	67
5.4	Hyvät ylläpitokäytännöt	67

6	DOKUMENTOINTI.....	69
6.1	Järjestelmän dokumentointi	69
6.2	Tietosuojaseloste	71
7	TIETOTURVA.....	72
7.1	Suunnittelu ja hankinta	72
7.2	Toteutus	73
7.3	Käyttö ja ylläpito	75
8	LAINSÄÄDÄNTÖ JA SÄÄNTELYN TAUSTA.....	78
8.1	Salakatselu ja -kuuntelu	78
8.2	Yksityiselämää loukkaava tiedon levittäminen	80
8.3	Tietosuoja	80
8.4	Tietoturva.....	81
8.5	Yksityisyyden suoja työelämässä.....	82
8.6	Yhteistoiminta yrityksissä	83
8.7	Työturvallisuus	84
8.8	Yksityiset turvallisuuspalvelut	84
8.9	Luettelo kameravalvontaan liittyvästä lainsäädännöstä	86
9	ESIMERKKEJÄ KAMERAVALVONTAJÄRJESTELMIEN KÄYTTÖKOhteista	87
9.1	Huoltoaseman kameravalvonta	87
9.2	Hotellin tai majoitusliikkeen kameravalvonta.....	89
9.3	Kerrostalon kameravalvonta	90
9.4	Ajoportin kameravalvonta	91
9.5	Kauppaliikkeen kameravalvonta	93
9.6	Kaupunkien kameravalvonta.....	94
10	TERMIT JA KÄSITTEET	97
11	LÄHDELUETTELO JA AIHEESEEN LIITTYVÄÄ KIRJALLISUUTTA.....	101
	LIITE 1: ESIMERKKI-ILMOITUS TALLENTAVASTA KAMERAVALVONNASTA.....	103
	LIITE 2: TALLENTAVAN KAMERAVALVONNAN TIETOSUOJASELOSTE	104
	LIITE 3: MALLIKUVA KAUPPALIIKKEEN KAMERAVALVONNASTA.....	106
	LIITE 4: MALLIKUVA TEHTAAN PORTTIALUEEN KAMERAVALVONNASTA.....	107
	LIITE 5: MALLI TALLENTEIDEN LUOVUTUSDOKUMENTISTA	108
	JULKAISUN TUKIJAT	109

1 JOHDANTO

1.1 OPPAAN JULKAISIJA

Turva-alan yrittäjät ry on sähköisen turvatekniikan alalla toimivien yritysten järjestö, joka valvoo jäseniensä etuja turva-alaa koskevista kysymyksistä, vaikuttaa viranomaissäädöksiin, edistää alan ammattipätevyyttä ja arvostusta sekä auttaa turvaamaan pätevän henkilöstön saatavuutta. Sen toiminnan keskiössä ovat turva-alan toimintaympäristöä edistävä sidosryhmäyhteistyö, turvateknisen täydennyskoulutuksen järjestäminen ja alan hyvien käytäntöjen kehittäminen.

1.2 OPPAAN TAUSTA

Kameravalvonta ja siihen liittyvät tekniset järjestelmät ovat viimeisen kymmenen vuoden aikana kehittyneet valtavasti. Kameravalvonnasta on tullut osa päivittäistä kaupunkikuvaa, ja kameravalvonnan käyttö on lisääntynyt. Myös sen käyttötarkoitus on laajentunut rikoksien ennaltaehkäisystä ja selvittelystä. Tekniikan kehittymisestä huolimatta Suomessa ei ole kameravalvonnan erityislakia, joka säätelisi yksityiskohtaisesti valvonnan suorittamista. Kameravalvonnan laillisuus riippuukin eniten valvonnan suorittajasta, paikasta ja tarkoituksesta.

Sisäasiainministeriön poliisiosasto asetti vuonna 2009 sisäisen turvallisuuden ohjelman toteuttamiseen liittyvän kameravalvonnan kehittämisen jatkohankkeen (KAMEVA-hanke). Hankkeen tarkoituksena oli kehittää kameravalvonnan ohjeistusta ja samalla opastaa yksityistä turva-alaa eri ongelmatilanteissa. Hankkeen tuloksena julkaistiin viranomaisten ja yksityisen turvallisuusalan välisenä yhteistyönä Kameravalvontaopas vuonna 2011.

Turva-alan yrittäjät ry kokosi vuonna 2019 asiantuntijaryhmän tarkastelemaan oppaan päivitystarpeita. Tämä opas on päivitetty vuoden 2011 oppaasta vastaamaan nykyajan vaatimuksia. Päivitystarpeita oppaaseen ovat vuosien myötä aiheuttaneet muun muassa tekniikan kehittyminen ja muuttunut lainsäädäntö, ja ne on huomioitu tässä Turva-alan yrittäjät ry:n julkaisemassa uudistetussa painoksessa. Päivitystyötä valvoneen työryhmän kokoonpano selviää oppaan sivulta kaksi.

Kameravalvontaoppaan sisältö on vapaasti käytettävissä ja opas on vapaasti jaettavissa, jos sen sisältöä ei muuteta ja julkaisija Turva-alan yrittäjät ry mainitaan. Tämä on oppaan toinen versio. Sen käsikirjoitus perustuu keväällä 2020 voimassa olevaan lainsäädäntöön ja sen aikaisiin tietoihin. Opas on ladattavissa HTML- ja PDF-muodoissa osoitteessa <http://www.turva-alanyrittajat.fi/kameravalvontaopas> ja sitä päivitetään tarvittaessa.

1.3 OPPAAN TARKOITUS

Tämän kameravalvontaoppaan tarkoituksena on toimia käytännönläheisenä ohjeistuksena kameravalvonnan kehittämiseksi ja yhtenäistämiseksi. Oppaan tavoite on parantaa kameravalvonnan laatua ja selventää kameravalvonnan lainsäädäntöä, jotta yritykset ja kansalaiset voivat selvittää oikeutensa ja velvollisuutensa kameravalvonnan toteuttamisessa.

Suomessa on käytössä useita erilaisia kameravalvontajärjestelmiä, joiden kokoonpano, suorituskyky ja laatu vaihtelevat, mikä asettaa haasteita niiden kanssa työskenteleville tahoille. Viihdeteollisuuden luomat mielikuvat järjestelmien suorituskyvyistä eivät vastaa todellisuutta, ja esimerkiksi viranomaiset törmäävät rikostutkinnassa edelleen usein kelvottoman laatuisiin tallenteisiin.

Oppaassa selvitetään myös keskeisiä asioita kameravalvontajärjestelmien hankinnasta, käytöstä ja ylläpidosta. Opas on tarkoitettu suunnittelun ja päätöksenteon tueksi, mutta sitä ei ole tarkoitettu suoraan sopimuksenteon perustaksi.

Lisätietoa voimassa olevista kameravalvonnan säännöksistä ja ohjeista saa esimerkiksi Tietosuojavaltuutetulta, ammattijulkaisuista ja muista tietolähteistä, joita on lueteltu lähdeluettelossa oppaan lopussa.

1.4 KAMERAVALVONTA TURVALLISUUDEN OSATEKIJÄNÄ

Turvallisuus syntyy monen eri tekijän yhteisvaikutuksesta. Yritysturvallisuudessa keskeistä on erilaisten riskien tunnistaminen ja niiden hallinta. Pääosan käytännön turvallisuustyöstä tulee olla etupainotteista ja keskittyä ennalta ehkäisevään toimintaan, jonka avulla erilaiset onnettomuus- ja vaaratilanteet, vahingot sekä rikollinen toiminta pyritään estämään. Yrityksillä ja yhteisöillä on myös oltava harjoittelut toimintamallit poikkeustilanteiden varalta.

Oikein mitoitetuilla ja toteutetuilla turvallisuustoimilla tuetaan toiminnan häiriöttömyyttä ja jatkuvuutta. Kameravalvonta, kulunvalvonta ja murtoilmaisuus kehittävät sekä ylläpitävät turvallisuutta. Ne kuuluvat olennaisena osana toimitilojen teknisiin turvallisuusratkaisuihin ja menetelmiin, joiden tavoitteena on estää tai rajoittaa henkilö- ja omaisuusvahinkoja.

Kameravalvonta on yritysten, yhteisöjen ja viranomaisten laajalti käyttämä menetelmä, jolla saadaan tuotettua jatkuvaa kuvallista informaatiota halutuilta alueilta. Tallentavan kameravalvontajärjestelmän avulla pyritään estämään toimitiloissa ilmeneviä mahdollisia ongelmia (yleisestäävyys) sekä selvittämään tapahtumia jälkikäteen (erityisestäävyys). Näin toimimalla viestitetään ympäristölle, että yritykseen tai yhteisöön kohdistetut vahingonteot tai rikokset selvitetään.

Yritysten ja yhteisöjen lisäksi myös poliisi suorittaa kameravalvontaa erilaisin menetelmin. Esimerkiksi

Helsingissä poliisi käyttää kaupungin sille tarjoamaa kameravalvontajärjestelmää poliisilain mukaisesti yleisen järjestyksen ja turvallisuuden ylläpitämiseksi sekä rikostutkinnan apuna. Poliisi hyödyntää kame-roita myös liikennevalojen ja liikennevirtojen ohjauksessa.

Kameravalvonnalla on rikostorjunnan lisäksi myös paljon muita käyttöaloja. Kameroita käytetään muun muassa teollisuuden ja sairaaloiden prosessien valvonnassa, henkilö- ja ajoneuvoliikenteen kulunoh-jauksen tukena sekä tuottamassa kamerakuvaa esimerkiksi kaupunkien keskeisiltä paikoilta.

Emsec Oy



Kuva 1. Teollisuuden prosessivalvontaa.

Teknologian kehittyessä kameravalvonnan käyttö lisääntyy tulevaisuudessa entisestään. Kameroiden tuottamaa kuvaa voidaan hyödyntää myös esimerkiksi

- asiakas- ja liikennevirtojen analysoinnissa
- konseptikehityksessä
- kauppojen hyllytäydennyksissä
- joukkotapahtumissa häiriötilanteiden kehittymisen ennakoimisessa
- vartijan sijasta turvallisuusvalvonnassa

- alkavan tulipalon havaitsemisessa ja paloriskien ennakkoinnissa
- erilaisten toimenpiteiden käynnistämisessä
- tarvittavan tiedon tuottamisessa pelastuslaitoksen tilannejohtamisessa
- vahinkotapausten tutkimisessa.

Erilaisten käyttötapojen määrä on lisääntynyt räjähdysmäisesti.

Kameravalvontaa suoritetaan yleensä kahdella eri tavalla: joko reaaliaikaisena kuvan tarkkailuna tai jälkikäteisenä kuvamateriaalin analysointina. Esimerkkinä reaaliaikaisesta kameravalvonnasta on myymälätarkkailu, jossa henkilö käyttää kameroita tarkkailutehtävään tavoitteenaan paljastaa ja estää myymälävarkauksia tai häiriökäyttäytymistä. Tällöin käytön tarkoituksena on siis havainnoida ja estää mahdollisia rikoksia. Reaaliaikaisessa tarkkailussa kameroita käyttävä henkilö on yleensä radioyhteydessä kentällä oleviin vartijoihin ja voi ohjeistaa heitä tarpeen mukaan. Vastaavasti myös vartijat saattavat pyytää seuranta valvojalta esimerkiksi näpistysepäilyn tai kiinniottamisen tueksi. Kameravalvontaa voidaan myös tehdä keskitetystä valvomosta ja tarvittaessa myös eri paikkakunnalta.

Jälkikäteen tallenteita tutkimalla voidaan pyrkiä selvittämään erilaisten tapahtumien kulku analysoimalla kameroiden tallennemateriaalia esimerkiksi epäilyistä rikostapauksista tai onnettomuuksista. Tallenteet voivat myös tukea rikosasian käsittelyä tuomioistuimessa.

2 RAKENNE JA TEKNIikka

Kameravalvontajärjestelmä on valvottavan kohteen kuvaamiseen sekä tapahtumien valvontaan ja tallentamiseen perustuva turvallisuusjärjestelmä. Se koostuu kamera-, tallennus- ja tarkkailulaitteista ja niihin liitetyistä ohjelmistoista sekä muista liitetyistä laitteista ja ohjelmistoista, joita tarvitaan siirto- ja ohjaustarkoituksiin.

2.1 KAMEROITA JA NIIDEN KÄYTTÖTAPOJA

Kameravalvonnan tyypillisiä käyttökohteita ovat mm.

- yleisvalvonta: kiinteistöt, rakennukset, kauppakeskukset, puistot, torit jne.
- turvallisuusvalvonta: yleisötapahtumat, kauppakeskukset, teollisuus, satamat, lentokentät, laivat jne.
- omaisuusvalvonta: museot, näyttelyt, historialliset kohteet jne.
- prosessivalvonta: teollisuus, tuotanto, logistiikka jne.
- rajavalvonta: maarajat, merirajat, satamat, lentokentät jne.
- liikennevalvonta: tunnelit, maantiet, rautatiet jne.
- kelivalvonta: maantiet
- seuranta: sairaalat, maatilat tms.

Kameravalvonnan käyttö ei rajoitu nykyisin enää pelkästään turvallisuuteen, vaan kameroiden tallentamaa tietoa voidaan hyödyntää laajasti myös esimerkiksi liiketoiminnan kehittämiseen.

Kameroita on saatavana erityyppisiä ja erikokoisia niiden käyttötarkoituksen mukaan. Tavallisesti kamera koostuu rungosta, optiikasta, virtalähteestä sekä jalustasta. Kameran voidaan myös suojata säältä, pölyltä tai ilkivallalta lisävarusteilla ja koteloinnilla.

Kamerat valitaan aina käyttötarkoituksen mukaan kohteeseen sopiviksi huomioiden asennuspaikan valaistus- ja sääolot sekä muut toimintaympäristön erityisvaatimukset. Nykyisin kamerat ovat värikameroita, jotka tuottavat värikuvaa hyvinkin vähäisessä valomäärässä. Useimmat kamerat osaavat hyödyntää infrapunavaloa, jolloin kamerasta saadaan terävää mustavalkokuvaa. Täysin pimeisiin olosuhteisiin on saatavilla yhdysrakenteisilla IR-ledeillä varustettuja kameroita.

Kamerat voidaan jakaa teknisten ja fyysisten ominaisuuksiensa sekä käyttötarkoituksensa mukaan esimerkiksi seuraavasti:

Runko- ja bulletkamerat

Kiinteillä runkokameroilla tarkoitetaan valvontakameroita, jotka kuvaavat aina samaa vakioitua kuva-alaa. Kameroissa on kiinteän polttovälin objektiivi tai zoomattava objektiivi. Jälkimmäisen polttoväli

on säädettävissä kussakin kohteessa tarvittavan kuva-alan kuvaamiseksi. Tarvittaessa objektiivi voidaan vaihtaa. Ulkokäytössä runkokamerat suojataan vesi- ja lämpötila- ja kosteusturvalla koteloinnilla ja varustetaan tarvittaessa lämmityksellä.

Muodostaan ja pienestä koostaan nimensä saaneet bulletkamerat soveltuvat sekä sisä- että ulkokäyttöön. Bulletkamerat sisältävät yleensä sääsuojatun kotelon, PoE-tuen ja IR-valot yökuvausta varten sekä analytiikkaominaisuuksia.



Kuva 2. Bulletkameroita sisä- ja ulkokäyttöön sekä runkokamera ulkokäyttöön.

Kiinteät kupukamerat (dome-kamerat)

Kiinteissä kupukameroissa kameran objektiivi on sijoitettu suojakoteloon, jossa objektiivin peittää joko kirkas tai tummennettu akryylikupu. Ominaisuuksiltaan ja käyttötarkoitukseltaan kiinteät kupukamerat ovat samankaltaisia kuin kiinteät runkokamerat. Kupukamera ei kuitenkaan ole esineenä niin silmiinpistävä kuin tavallinen kiinteä kamera. Kiinteä kupukamera voidaan sijoittaa alas laskettuun välikattoon siten, että itse kamera on välikaton yläpuolella ja vain sen kupu on katossa nähtävänä. Kiinteitä kupukameroita valmistetaan sekä sisä- että ulkokäyttöön, ja niihin saa myös vandaalisuojatun koteloinnin. Ulkokäyttöön, eli ankariin olosuhteisiin, tarkoitetuissa kameroissa on kiinteä sisään rakennettu lämmitysvastus. Objektiivina käytetään zoomattavaa mallia. Joissakin kiinteissä kupukameroissa voi olla jopa 360 asteen näkymä. Objektiivia ei yleensä voida vaihtaa.



Kuva 3. Dome-kameroita.

Kääntöpääkamerat eli PTZ-kamerat (Pan Tilt Zoom)

PTZ-kameroita käytetään laajojen ulkoalueiden ja esimerkiksi ostoskeskusten valvonnassa. Kaikissa PTZ-kameroissa on moottoroidulla zoomilla varustettu objektiivi, jonka avulla kameralla voidaan kuvata yksityiskohtia kaukaakin.

PTZ-kameroita käytetään esimerkiksi 24/7-valvonnassa, jossa kohteita seurataan aktiivisesti valvottavalla alueella tai valvottavassa tilassa. Kamerat on mahdollista ohjelmoida ennalta määrätyn aikataulun mukaan kääntymään ja kuvaamaan esimerkiksi alueen kriittisiä kohteita eikä tällöin tarvita valvojan erillistä ohjausta. PTZ-kameroita ohjataan usein esimerkiksi kulunvalvonta- tai murtohälytysjärjestelmästä, jolloin kamera voidaan saada automaattisesti kääntymään avautuvan portin tai oven suuntaan. PTZ-kameroita on eri käyttöolosuhteisiin ja sekä sisä- että ulkokäyttöön. Kotelot voivat olla myös vandalismin tai jopa käsiaseiden luotien kestäviä.



Kuva 4. PTZ-kameroita.

Lämpökamerat

Lämpökamerat tuottavat kuvaa perustuen lämpöön, jota säteilee kuvattavasta kohteesta. Tuotettava kuva on yleensä mustavalkoista, mutta sitä voidaan tehostaa keinotekoisesti eri värein helpottamaan eri lämpötilojen havainnoimista. Lämpökameran kuva on parhaimmillaan, kun kohteessa on suuria lämpötilaeroja. Mitä kuumempi objekti kuvassa on, sitä kirkkaampana se erottuu kuvasta.

Lämpökamerat ovat parempia kuin optiset kamerat kohteissa, joissa on vähän valoa, mutta tarvetta havaita henkilöitä tai objekteja ympärivuorokautisessa valvonnassa. Lämpökamera ei häiriinny valaistuksen muutoksista, kuten varjoista, vahvasta taustavalosta tai pimeydestä, vaan pystyy tuottamaan kuvaa tehokkaasti ilman tarvetta kohteen lisävalaistukselle.

Lämpökameroita käytetään yleensä laajojen alueiden ja suurten etäisyyksien aluevalvontaan. Tyypillisiä käyttökohteita ovat esimerkiksi lentokentät, vankilat, voimalaitokset, tunnelit, sillat, raidealueet ja muut alueet, joissa asiattoman oleskelun ympärivuorokautinen havainnointi on tärkeää.

Axis Communications Ab



Hikvision



Kuva 5. Lämpökameroita.

Droonit

Drooni (engl. drone) on miehittämätön, kauko-ohjattava ilma-alus, jota kutsutaan myös esimerkiksi pienois-, neli- tai multikopteriksi tai kuvauskopteriksi. Kameralla varustetut droonit soveltuvat harrastuskäytön lisäksi monipuoliseen ammattikäyttöön esimerkiksi pelastus- ja etsintätehtävissä, tilannekuvan luomisessa tai suurien yleisötapahtumien valvonnassa. Teollisuudessa drooneja käytetään yhä enemmän erilaisissa tarkastuksissa, vuotojen paikantamisessa ja lämpökamerakuvauksissa.

Droonien kuvauskäytössä tulee huomioida niiden lennättämistä koskevat säännökset sekä rajoitukset ja lisäksi erityistä huomiota on kiinnitettävä yksityisyyden suojaan. Tietoa ja opastusta droonien lennättämisestä on koottu Liikenne- ja Viestintävirasto Traficomien droneinfo.fi-sivustolle.

VideoDrone Finland Oy



Kuva 6. Drooni.

Muita kameratyppejä

Alla on lueteltu muita kameratyppejä:

- 360 asteen kamerat eli yhdellä kalansilmäobjektiivilla toteutetut yleiskuvakamerat
- panoraamakamerat eli usealla kennolla toteutetut laajakuvakamerat
- EX-kamerat eli räjähdysvaarallisten tilojen kamerat
- EMP-kamerat eli elektromagneettisilta pulseilta suojatut kamerat
- bi-spectrum-kamerat eli sekä näkyvän valon että lämpösäteilyyn perustuvan kuvavirran kamerat
- modulaariset eli erillisistä kamerapäistä ja keskusyksiköistä koostuvat kamerat.

Hikvision



Axis Communications Ab



Axis Communications Ab



Kuva 7. Kalansilmäobjektiivilla varustettu kamera, EX-kamera ja panoraamakamera.

2.2 KAMEROIDEN TEKNIikka, KUVATAHTI JA RESOLUUTIO

Digitaalisessa tekniikassa IP-kameran CMOS-kuvakennossa kuva koostuu pikseleistä eli kuvapisteistä, joiden määrä kertoo IP-kameran kuvakennon tarkkuuden. Kasvanut pikselien määrä kuvakennossa mahdollistaa perinteistä analogista kameraa paremman kuvanlaadun. Vaikka ensimmäinen digitaalinen IP-kamera esiteltiin jo vuonna 1996, analogista tekniikkaa käytetään edelleen hyvin paljon. Tämä on seurausta kohteiden kaapeloinnista, jonka päivittäminen ethernet-kaapeloinniksi saattaa olla haastavaa. Siirtymää IP-maailmaan helpottavat enkooderit, jotka muuntavat analogisen kuvasignaalin IP-verkon yli siirrettäväksi digitaaliseksi bittivirraksi.

IP-kamerat käyttävät erilaista kuvansiirtotapaa ja formaattia kuin analogiset edeltäjänsä. Analoginen kamera siirtää kuvan analogisena videovirtana koaksiaalikaapelia pitkin tallenninlaitteelle tai tarkkailumonitorille, kun taas IP-kamera muuttaa kuvainformaation digitaaliseksi bittivirraksi. Bittivirran avulla kuva siirtyy tietoverkkoa pitkin digitaalisena tallentimelle. IP-kamerassa on yksi tai useampi mikroprosessori kuvan käsittelyä ja analysointia varten. IP-kamerassa voi lisäksi olla tiettyä käyttötarkoitusta varten kehitetty ohjelmisto.

Kuvatahdilla kameravalvonnassa tarkoitetaan joko valvontakameran tuottamaa kuvamäärää sekunnissa tai tallentimen tallentamaa kuvamäärää sekunnissa. Analogisessa kamerassa kameran tuottama kuvatahti on aina vakio: 25 kuvaa sekunnissa. Digitaalisissa IP-kameroissa kuvatahdit ovat pitkälti käyttäjän itsensä määriteltävissä.

Resoluutiolla eli erottelukyvyllä tarkoitetaan kuvapisteiden eli pikselien määrää kuvassa. Resoluutio määrittää yksityiskohtien erottelutarkkuuden. Mitä enemmän kuvassa on kuvapisteitä, sitä korkeampi on resoluutio. Kärjistäen voidaan sanoa, että mitä korkeampi resoluutio, sitä parempi kuva.

Kuvanlaatuun vaikuttavat erittäin oleellisesti myös kuvan pakkausmenetelmä, kuvakennon fyysinen koko, valaistus ja kameran objektiivin laatu. Mitä enemmän kuvaa pakataan, sitä huonompi kuvanlaatu on. Hämärässä pakkauksen merkitys kuvan laatuun vaikuttaa vielä enemmän.

Perinteisessä analogisessa järjestelmässä kuvakennon kautta piirtyvän kuvan tarkkuus eli resoluutio on parhaimmillaan 720×576 kuvapistettä. Moderni analoginen HD-kamera pystyy tuottamaan jopa 4K-resoluution kuvaa (4096×2160 pikseliä). Digitaalisessa kameravalvonnassa megapikselikameroilla päästään tarvittaessa vieläkin suurempiin resoluutioihin.

Valvottavan alueen koon pysyessä ennallaan resoluutiolla voidaan vaikuttaa tallennettavien yksityiskohtien määrään ja mahdollistaa kuvan digitaalinen zoomaaminen jälkikäteen. Alla on esitetty neljällä eri kameralla 15 metrin etäisyydeltä otetut kuvat. Kameroiden kuva-ala on säädetty objektiivilla samanlaiseksi, ja ainoastaan kennon resoluutio muuttuu eli kasvaa vasemmalta oikealle.



1280 x 720 pikseliä
1 MP



1920 x 1080 pikseliä
2 MP



3072 x 1728 pikseliä
5 MP



3840 x 2160 pikseliä
8 MP / 4K

Kuva 8. Resoluution vaikutus kuvan laatuun.

Suunnittelun tueksi esimerkiksi laite- ja tallenninvalmistajien kotisivuilla on työkaluja, joilla voi valita helposti sopivat tuotteet kohteeseen ja käyttötarkoitukseen.

2.3 TALLENTIMET

Kameravalvontajärjestelmän tallennin on kompakti laite, johon liitetään kamerat ja näyttö. Tallennin muodostuu integroidusta PoE-kytkimestä, tallennuskovalevyistä ja tallenninohjelmistosta. Kokonaisuus muodostuu usein vain yhdestä laitteesta. Tallentimissa ei ole erillistä käyttöjärjestelmää, vaan se on valmistajakohmainen sulautettu ohjelmistokokonaisuus.

Tallentimen käyttöönotto on tehty lähes automaattiseksi. Useimmissa tallentimissa näyttö, näppäimistö ja hiiri liitetään suoraan laitteeseen, mikä vaikuttaa laitteen sijoituspaikkaan. Tallentimiin on saatavilla hyvin rajallisesti web-käyttöliittymiä ja työasemakäyttöliittymiä, joilla on mahdollista katsoa reaaliaikaista kuvaa ja tallenteita muualla kuin laitteen sijoituspaikassa.

Kamerat liitetään tallenninlaitteen integroituun kytkimeen, jolloin kamerat tunnistetaan automaattisesti. Pääsääntöisesti tallentimet tukevat vain saman tallenninvalmistajan kameroita, ja ne on useimmiten vakioitu tietylle määrälle kameroita (4, 8, 12, 16, 24 tai 32 kameraa). Tallentimia ei juuri ole mahdollista laajentaa myöhemmässä vaiheessa. Kameroita on mahdollista liittää vapaisiin kytkinportteihin.

Useimmissa tallentimissa on yksi tallennuslevypaikka, johon asennetaan tavallinen tallennuskovalevy. Tyypillisesti yli 16 kamerakapasiteetin tallentimissa on 2 kovalevypaikkaa. Yleisesti tallentimissa on yksi liitäntä näytölle, minkä avulla on mahdollisuus katsoa reaaliaikaista kuvaa ja myös tallenteita.

Tallentimet ovat toiminnoiltaan ja liitettävyydeltään hyvin rajallisia, mikä näkyy myös niiden edullisissa hinnoissa. Ne sopivat erinomaisesti sellaisiin pieniin kohteisiin, joissa pääasiallinen tarve on tallentaa kuvaa, jota vain joskus saatetaan tarvita jälkikäteen. Tallentimen käyttö on tehty helpoksi, mikä on erityisen tärkeää silloin, kun laitetta käytetään hyvin harvoin. Tallentimista saadaan tehtyä videoleikkeitä esimerkiksi muistitikulle jälkeinpäin tapahtuvaa käyttöä varten. Joidenkin valmistajien tallentimiin saa liitettyä kameroita kyseisen valmistajan analytiikkaominaisuuksilla, mikä tuo merkittävästi lisää mahdollisuuksia tallentimien käyttöön.

Mikäli myöhemmässä vaiheessa käytölle tulee lisävaatimuksia ja tarvitaan uusia toiminnallisuksia, tallennin on mahdollista korvata videonhallintajärjestelmällä (VMS). Kameroita ei tarvitse vaihtaa, jos alun perin on hankittu kamerat, jotka mahdollistavat myös muita liitäntärajapintoja kuin liittämisen ainoastaan kyseiseen tallenninlaitteeseen. Ja vaikka tallenninlaitteisto olisi pieni ja edullinen, sen käyttöä määrittävät samat tietoturvallisuuden ja tietosuojaan säädökset kuin laajojen videonhallintajärjestelmienkin käyttöä.



2.4 YHTEYDET

2.4.1 Analogiset yhteydet

Analogisen videokuvan siirtäminen on yksinkertaista: videovirtaa siirretään sähköisenä signaalina yleensä joko koaksiaalikaapelia tai kierrettyä parikaapelia pitkin. Ainoa tekninen haaste on saada sähköinen signaali kulkemaan haluttu matka.

Kaapelointi on analogisessa kuvansiirrossa tähtiverkon muotoinen. Jokaiselle kameralle menee oma kaapelinsa tallenninlaitteelta tai videovaihteelta, eikä tiedonsiirtokapasiteetti muodostu tällöin ongelmaksi.

Analogisen kuvansiirron ainoa tietoturvaongelma on, miten estää asiattomien pääseminen käsiksi kaapeleihin, kameroihin ja tallenninlaitteisiin. Yleensä analogiset tiedonsiirron ongelmat ovat seurausta jostain fyysisesti todennettavasta syystä, kuten kaapelin katkeamisesta.

Signaalin vaimennus määrittää analogisen kuvan siirtoetäisyyden. Koaksiaali- tai parikaapelia käytettäessä voidaan siirtää analogista kuvaa vain pari sataa metriä ilman erillistä signaalin välivahvistamista.

Välivahvistimia käyttäen voidaan siirtoetäisyyttä nostaa jopa kilometriin. Analogistakin kuvasignaalia voidaan siirtää valokaapelissa, jolloin siirtoetäisyydet voivat olla useita kilometrejä. Tämä vaatii kuitenkin valokaapelilähettimien ja vastaanottimien käyttöä. Nämä lisäävät huomattavasti siirtokustannuksia, kuten itse valokaapelikin.

2.4.2 Digitaaliset yhteydet

Verkkopohjaisessa tekniikassa kuva siirtyy suoraan kameralta digitaalisessa muodossa verkon ylitse TCP/IP-protokollaa hyödyntäen. TCP/IP-protokollaa käytettäessä on jokaisella verkon päätelaitteella, kuten esimerkiksi kamerat, kytkimet, reitittimet ja tallentimet, kiinteä IP-osoite, jonka avulla verkossa kulkeva tieto ohjautuu oikeisiin päätelaitteisiin.

IP-osoitteet eivät ole yrityksen tai kodin sisäisissä paikallisverkoissa ongelmallisia. Kun sen sijaan hyödynnetään vapaata internetiä esimerkiksi yksityistalouksien valvonnassa, tarvitaan operaattorilta usein kiinteä IP-osoite, joka nostaa kokonaiskustannuksia merkittävästi.

Kaistantarve

Digitaalisen kuvan siirtämistä tietoverkoissa rajoittaa eniten kaapeleiden ja siirtolaitteiden kapasiteetti. Suuri osa suomalaisista lähiverkoista on kaapeloitu siten, että suurin laskennallinen tiedonsiirtokapasiteetti on 100 megabittiä sekunnissa (Mbps).

Tämän lisäksi Suomessa on runsaasti vanhempia verkkoja, joiden kapasiteetti on 10 Mbps. Yhden gigabitin sekuntisiirtonopeuteen kykeneviä verkkoja on lähinnä uusissa rakennuksissa ja parannetuissa kohteissa. Vaikka vanhojenkin lähiverkkojen siirtonopeutta voidaan parantaa uusimalla verkon aktiivilaitteita, kuten kytkimiä ja reitittimiä, ilman tehokkaita pakkausmenetelmiä videokuvan siirto tietoverkoissa ei olisi mahdollista.

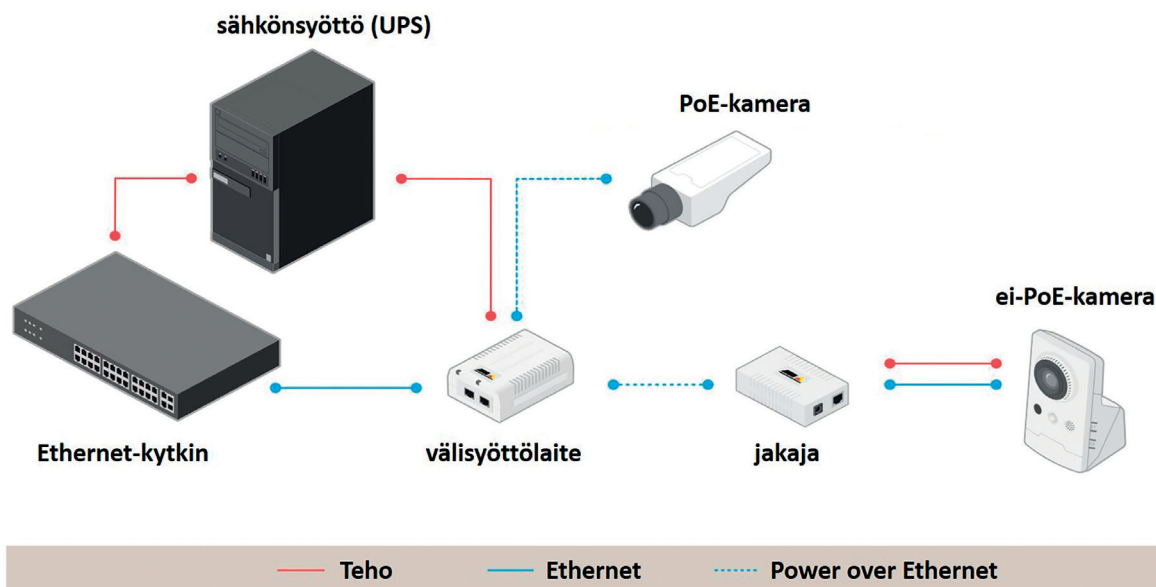
Tarvittavaan tiedonsiirtokaistan määrään ja tiedonsiirron nopeuteen vaikuttavat

- kameroiden määrä verkossa
- pakkaustekniikan määräämä kuvatiedostojen koko
- kameroiden kuvatahti.

Yleensä organisaatioiden tietoverkoissa siirretään muutakin tietoa kuin valvontakuvaa. Organisaation toiminnan kannalta kuvaa tärkeämpiä tietoja ovat muun muassa kassojen tietoliikenne ja sähköposti. Mikäli kuormitus ylittää verkon siirtokyvyn, kaikki tiedonsiirto verkossa alkaa pätkiä tai katkeaa kokonaan. Tämä ei ole ongelma ainoastaan kuvansiirrossa, vaan kaikessa ja usein vielä organisaation kannalta kuviakin kriittisemmissä tiedoissa.

Power over Ethernet -tekniikka (PoE)

PoE-tekniikassa Ethernet-verkkoon kytkettyjen kameroiden virransyöttö ja kuvansiirto voidaan hoitaa samalla kaapelilla, eikä kameralle tai muulle verkkolaitteelle tarvitse vetää erillistä virtakaapelia. Tehoa syöttävä laite voi olla integroitu Ethernet-kytkimeen (PoE-kytkin) tai se voi olla erillinen laite (välisyöttölaite, midspan-laite), joka liitetään kaapelointiin kytkimen ja syötettävän laitteen väliin. Tekniikka säästää huomattavasti kaapelointikustannuksia, koska erillisten virtalähteiden ja kaapelointien määrä vähenee.



Kuva 9. Tehon syöttäminen kameroille välisyöttölaitteella.

PoE-tyyppejä on neljä, ja ne määritellään maksimilähtötehon mukaan seuraavasti:

- tyyppi 1: 15,4 W
- tyyppi 2: 30 W
- tyyppi 3: 60 W
- tyyppi 4: 90 W.

Tyyppien 2–4 teholla kamerakotelo voidaan pitää vastuksen avulla lämpimänä ja ohjata esimerkiksi PTZ-kameraa.

2.4.3 Langattomat yhteydet

Analogiset langattomat linkkiyhteydet toimivat esimerkiksi radiotaajuuksilla tai infrapunalinkin avulla. Niiden lähetystapa ja teho vaikuttavat niin, että linkkien siirtoetäisyydet vaihtelevat kymmenistä metreistä kilometreihin. Yhteyksien ongelmana on usein niiden salaamattomuus ja häirinnän mahdollisuus.

Salaamattomia langattomia valvontakameroita ei pidä käyttää kriittisen tiedon siirtämiseen. Sen sijaan jo muutenkin näkyvissä olevien kameroiden kaapelointikustannuksissa voi tarvittaessa säästää käyttämällä langattomia siirtoyhteyksiä.

Digitaalisissa langattomissa verkkoyhteyksissä käytetään usein langatonta lähiverkkotekniikka (WLAN). Useat IP-kamerat sisältävät myös WLAN-lähettimen, mikä mahdollistaa kuvan katselun tietokoneelta ilman kaapelia.

Pidemmissä siirtoetäisyyksissä langattomaan kuvansiirtoon soveltuvat 4G/5G- ja WiMAX-tekniikat.

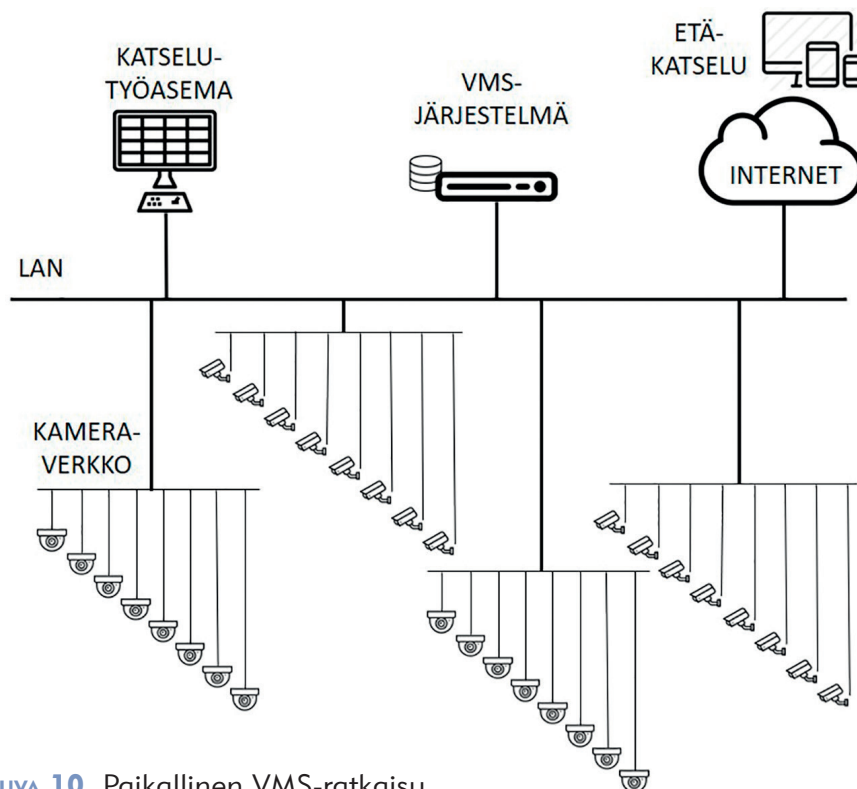
Digitaalisen langattoman kuvansiirron heikkoutena pidetään sen ajoittaista katkeamista. Siksi kriittisten kohteiden kuvansiirto kannattaa toteuttaa kaapelilla. Tarvittaessa langattoman kuvansiirron toimintavarmuutta voi parantaa GSM-ohjatulla sähkönsyötöllä, jonka avulla laitteen saa käynnistettyä uudelleen etäohjauksella, esimerkiksi matkapuhelimella.

2.5 VIDEOHALLINTAJÄRJESTELMÄ

Videohallintajärjestelmä (Video Management System eli VMS) on ratkaisukokonaisuus, joka mahdollistaa erilaisten kameroiden ja myös toimintaa tehostavien sovellusten liittämisen samaan kokonaisuuteen. VMS-järjestelmiä käytetään pääsääntöisesti kohteissa, joissa kamerakuvaa hyödynnetään laajasti sekä reaaliaikaiseen katseluun että tallenteiden katseluun.

Suurten, useita kymmeniä tai jopa tuhansia kameroita käsittävien kameravalvontakokonaisuuksien toteutukset tehdään VMS-järjestelmillä. Niiden avulla saadaan myös useita kohteita ja toimipaikkoja sisältävät ratkaisut yhdistettyä siten, että palvelujen käyttö on mahdollista etänä. VMS-järjestelmä voidaan rakentaa yhteiseksi alustaksi, jossa tiettyjä kameroita voidaan antaa hallittavaksi eri tahoille, kuten yrityksille. Kyseessä on niin kutsuttu monikäyttäjäjärjestelmä, jossa kukin yritys hallinnoi vain omat kameransa ja niiden kautta saatuja tallenteita. Tämän tyyppisellä järjestelmällä on hyvä olla pääkäyttäjä, joka hallinnoi koko järjestelmää ja sen ylläpitoa sekä käyttöoikeuksia ja niin edelleen.

VMS-järjestelmiä on perinteisesti hyödynnetty turvallisuuteen liittyvissä toiminnoissa, mutta nykyisin niitä käytetään myös esimerkiksi tilojen käytön analysoinnissa, markkinoinnissa, asiakaspalvelussa, toimintojen kehittämisessä ja erilaisissa prosesseissa ja niiden automatisoinnissa. Lähitulevaisuudessa käyttö laajenee niin, että eri valmistajien kamerat voidaan liittää järjestelmiin.



Kuva 10. Paikallinen VMS-ratkaisu.

2.5.1 VMS-ohjelmisto

VMS-ohjelmisto tallentaa IP-kameroiden ja -palvelimien lähettämää reaaliaikaista kuvaa tallennusjärjestelmän sisäisille tai ulkoisille levyasemille. Lisäksi voidaan tallentaa kuvaan liittyvää ääntä ja dataa. Kameroiden lähettämää tietoa esimerkiksi liiketunnistuksesta, analytiikasta tai kameran toiminnasta voidaan hyödyntää määrittelyjen mukaisesti esimerkiksi luoden erilaisia hälytyksiä ja tapahtumia, jotka on mahdollista liittää myös tallenteeseen.

VMS-ohjelmistot kykenevät ohjaamaan kameraa ja muun muassa muuttamaan kameran kuvanopeutta ja resoluutiota ohjelmiston saaman hälytyksen tai ulkoisen järjestelmän lähettämän tiedon perusteella. Ohjelmistoihin määritellään usein niin kutsuttu esitallennusaika, jonka mukaisesti tallennetaan ennen havaittua tapahtumaa olevaa kamerakuvaa.

Toiminnallisuudet määritellään yksilöllisesti kullekin kameralle ja liitetään usein myös aikaperusteiseen

profiilin, jolloin kameran toiminta muuttuu kellonajan ja viikonpäivän mukaan. Ohjelmiston tallennuskapasiteetti määritellään liitettyjen kameroiden lukumäärän, kuvatahdin, resoluution, tallennukseen tulevan kuvastriimin sekä käytettävän videopakauksen (esimerkiksi H265) perusteella. Tallennukseen tuleva kuvastriimi voi olla jatkuvaa joistakin tai kaikista kameroista. Usein sen ohjaus perustuu tapahtumiin, hälytyksiin tai aikaan. Myös manuaalinen ohjaus on mahdollinen.

Kamerat lähettävät VMS-ohjelmistolle kaksi eri kuvastriimiä, toinen tallennusta ja toinen reaaliaikaista katselua varten. Tallennusstriimi on usein korkearesoluutioisempaa ja pienemmällä kuvatahdilla (esimerkiksi 20 kuvaa sekunnissa) kuin reaaliaikainen katselustriimi, joka puolestaan on yleensä alhaisella resoluutiolla ja korkealla kuvatahdilla (esimerkiksi 30 kuvaa sekunnissa). Reaaliaikainen katselustriimi ohjataan suoraan kameralta katselutyöasemalle ja selainkäyttöliittymien käyttämälle web-palvelimelle. Suoraan ohjauksella pienennetään merkittävästi reaaliaikaisen katselustriimin viiveitä ja vähennetään palvelimen tarpeetonta kuormitusta verrattuna siihen, että katselustriimi kierrätettäisiin VMS-palvelimen kautta. Lisäksi varmistetaan reaaliaikaisen videokuvan saatavuus tilanteissa, joissa tallennin on mahdollisesti rikkoutunut.

VMS-ohjelmisto asennetaan yleensä sitä varten varatulle palvelimelle tai virtuaalipalvelimelle. Jos kyseessä on pieni järjestelmä, eli joitakin kymmeniä kameroita, asennus on mahdollista tehdä myös tehotyöasemalle. Palvelimissa ja tehotyöasemissa käytetään käyttöjärjestelmänä joko Windows-, Windows Server - tai Linux-käyttöjärjestelmää. Jos ratkaisukokonaisuus muodostuu useista eri VMS-palvelimista, niitä kaikkia ohjaa niin kutsuttu hallintapalvelin, jonka kautta ei kulje lainkaan kuvastriimejä.

2.5.2 Reaaliaikainen käyttö

VMS-järjestelmän jatkuvassa reaaliaikaisessa käytössä hyödynnetään kamerakuvan seurantaan työasemasovelluksia, joihin on liitetty useimmiten kahdesta neljään näyttöä samanaikaisesti seurattavien kameroiden määrän mukaan. Näyttöjen asetteluita voi vapaasti muokata, ja samassa näytössä voi olla erikokoisia kuvia.

Usein yhdellä 24 tuuman työasemanäytöllä on samanaikaisesti 18–24 kuvaa, jolloin 4 näytölle saadaan näkymään samanaikaisesti jopa 96 videokuvaa. Se, miten monta kuvaa näkyy samanaikaisesti, vaihtelee katselutyöaseman ja näytönohjaimen tehon lisäksi kuvastriimin resoluution ja kuvanopeuden mukaan. Usein käytetään samanaikaisesti sekä normaalinäyttöjä että isoja 50–100 tuuman näyttöjä, jotka toimivat reaaliaikaisen kuvan näyttöinä pienempien näyttöjen toimiessa työskentelynäyttöinä. Kamerakuvat voi valita vapaasti ja näkymät tehdä käyttäjäkohtaisiksi. Jos kameroita on paljon, voidaan käyttää vähemmän tärkeiden kameroiden kamerakuvakiertoa.

Katselutyöasemalle lähetetään kameroilta suoraan katselustriimiä, joka on konfiguroitu reaaliaikaiseen katseluun sopivaksi. Tyypillinen kuvatahti on 30 kuvaa sekunnissa, ja resoluutio määräytyy käytettävän näytön resoluution ja näytöllä olevan kuvamäärän mukaan. Jos lähettävän kuvastriimin resoluutio on liian suuri näytölle, katselutyöasema koodaa uudelleen kuvastriimin näytölle sopivaksi. Tämä kuormittaa työasemaa ja näytönohjainta. Kun käyttäjä haluaa katsoa tarkempaa kuvaa, hän valitsee halutun kuvan, joka muuttuu koko näytön kokoiseksi. Tällöin VMS-ohjelmisto vaihtaa automaattisesti reaaliaikaisesta kuvastriimistä tallennusstriimin, jossa on korkeampi resoluutio, mikä mahdollistaa tarkemman kuvan näytölle. Kun käyttäjä palaa aiempaan kuva-asetteluun, ohjelmisto siirtyy takaisin reaaliaikaiselle kuvastriimille.

Käyttäjällä on mahdollisuus tehdä reaaliaikaiseen kuvaan erilaisia merkintöjä, jotka tallentuvat kameraan myöhempää käyttöä varten. Usein merkinnät ovat käyttäjän havaitsemia poikkeavia tilanteita. Yhä useammin reaaliaikainen kuvaseuranta perustuu älykkään analytiikan, jonkin ulkoisen järjestelmän tai järjestelmien tapahtumien tai tapahtumayhdistelmien perusteella käynnistettyyn automaattiseen prosessiin, joka aukaisee reaaliaikaiset kuvat tapahtumaan liittyvistä kameroista. Usein samalla käynnistetään automaattisesti myös tallenteet samoista kameroista, ja ne toistetaan muutamalta minuutilta ennen tapahtumaa.

Yhdessä VMS-järjestelmässä voi olla useita katselutyöasemia, ja ne ovat vapaasti sijoitettavissa käyttötarpeen mukaan. Web-käyttöliittymiä käytetään ensisijaisesti hetkittäisiin ja tilapäisiin tarkoituksiin. VMS-ohjelmistoon liitetty web-palvelin muokkaa kuvanopeuden ja resoluution automaattisesti web-käyttöön soveltuviksi.

2.5.3 Tallenteiden käyttö

Kameroiden määrän ja käytetyn kuvatahdin kasvu ovat lisänneet VMS-ohjelmistojen tallenneaineistojen määrää merkittävästi. Tallenteiden käytön helpottamiseksi ohjelmistoihin on sisällytetty hakutyökaluja, jotka perustuvat esimerkiksi haettavaan kohteeseen (henkilö, henkilöauto, pyöräilijä, kuorma-auto jne.), kohteen väriin, muutoksiin tai ulkoisten järjestelmien tapahtumiin. Lisäksi käytetään erilaisia aikarajauksiin ja käyttäjien reaaliaikaiseen kuvaan tekemiin merkintöihin perustuvia hakuja. Näitä yhdistelemällä löydetään nopeasti tallenteet etsitystä tapahtumasta. Tallenteita katsotaan usein samassa paikassa kuin niitä käytetään reaaliaikaisesti, jolloin käytettävissä ovat kaikki samat kuvaominaisuudet kuin reaaliaikaisessa käytössä. Työasemakäyttöliittymissä on usein huomattavasti tehokkaammat hakutyökalut kuin web-käyttöliittymissä.

Tallennetusta materiaalista on mahdollisuus tehdä erillisiä videoleikkeitä tietystä tapahtumasta esimerkiksi viranomaisia varten. Erilliset videoleikkeet tehdään usein erilliselle verkkolevyille, josta ne siirretään ulkoiselle medialle edelleen toimitettavaksi, tai vastaanottajalle toimitetaan kertakäyttöinen latauslinkki tallenteen noutamista varten. Videoleikkeitä on nykyään alettu korvata medialeikkeillä, joihin on mahdollista lisätä kuvan ja äänen lisäksi myös tekstiä kuvaamaan tarkemmin aineistossa olevia tapahtumia ja niihin liittyviä asioita.

VMS-ohjelmistot siirtävät automaattisesti määriteltyjen tapahtumien aineistot niin kutsuttuihin arkistotallenteisiin, jolloin ne säilytetään pidempään kuin varsinaiset tallenteet. Käyttäjän on myös mahdollista tehdä vastaava arkistotallennus manuaalisesti.

Tallenteiden käsittelyssä on aina varmistuttava tietoturvasta ja tietosuojasta. Tallenteet on hävitettävä heti, kun niitä ei enää tarvita valvonnan tarkoituksen toteuttamiseksi ja viimeistään vuoden kuluessa.

2.5.4 Kameroiden liitântä

Kamerat liitetään tietoverkkoon, jota kautta VMS-ohjelmistolla on yhteys kameroihin. Jos järjestelmässä on vanhoja analogisia kameroita, ne liitetään videopalvelimeen, joka liittyy tietoverkkoon. VMS-ohjelmistossa pitää olla kameroille ja videopalvelimelle liitântärajapinta, jonka avulla kamerat ja ohjelmisto kommunikoivat keskenään. Liitântärajapinta määrää, mitä kamerakohtaisia toiminnallisuuksia ohjelmisto pystyy käyttämään. Eri VMS-ohjelmistojen liitântärajapintojen toiminnallisuudet poikkeavat merkittävästi toisistaan jopa samojen kameramallien osalta. Usealla eri ohjelmistolla saattaa olla liitântärajapintoja useille tuhansille eri kameramalleille, mutta liitântärajapintojen kamerakohtaiset toiminnallisuudet poikkeavat toisistaan merkittävästi.

Kameroissa on yhä enemmän toiminnallisuuksia, jotka tekevät niistä älykkäitä sensoreita, ja niiden tuottama datamäärä kasvaa. VMS-järjestelmät on kehitetty ensisijaisesti käsittelemään kamerakuvaa ja sen toiminnallisuksia. Datamäärän kasvaessa markkinoille on tulossa uusia ratkaisuja, jotka keskittyvät kameroiden tuottaman datan käsittelyyn. Nämä uudet järjestelmät kommunikoivat myös VMS-järjestelmien kanssa, mikä mahdollistaa kameroiden datan ja kuvan hyödyntämisen.

VMS-ohjelmistossa kullekin kameralle konfiguroidaan eri parametrit kuvastriimeihin ja kameran toimintaan, kuten esimerkiksi resoluutio, kuvatahti, videopakkaus ja tallennuksen aloituksen määrittely. Kamera voi olla jatkuvasti tallentava tai tallennus voi aktivoitua liikkeen tunnistuksesta, analytiikasta tai ulkoisen järjestelmän tuottamasta hälytyksestä sekä manuaalisesta tallennuksen käynnistyksestä. Myös tallenteiden säilytysaika määritellään kamerakohtaisesti. Kameroiden ominaisuuksien monipuolisella hyödyntämisellä parannetaan merkittävästi koko ratkaisukokonaisuuden tuottamaa hyötyä.

2.5.5 Analytiikka

Analytiikka kehittyy nopeasti. Aiemmin analytiikkaa tehtiin ainoastaan VMS-ohjelmistojen erillisillä analytiikkasovelluksilla ja VMS-ohjelmistoon liitettyä analytiikkapalvelimella. Nykyisin, kun kameroiden prosessorien tehot kasvavat, yhä suurempi osa analytiikasta toteutetaan kamerassa. Kameroiden tehon kasvua hidastavat lähinnä PoE-tehonsyötön rajoitukset.

Vallitseva kehityssuunta on hyvä, sillä se pienentää verkkokuormaa ja VMS-palvelimien kuormitusta. Suoritustehoa vaativia analytiikkasovelluksia toteutetaan erillisillä analytiikkapalvelimilla, ja tällöin ovat pääsääntöisesti kyseessä tallenteista tehtävät erityiset analyysit.

Analytiikan käytöstä kameravalvonnassa on kerrottu tarkemmin kohdassa 2.6 Analytiikka.

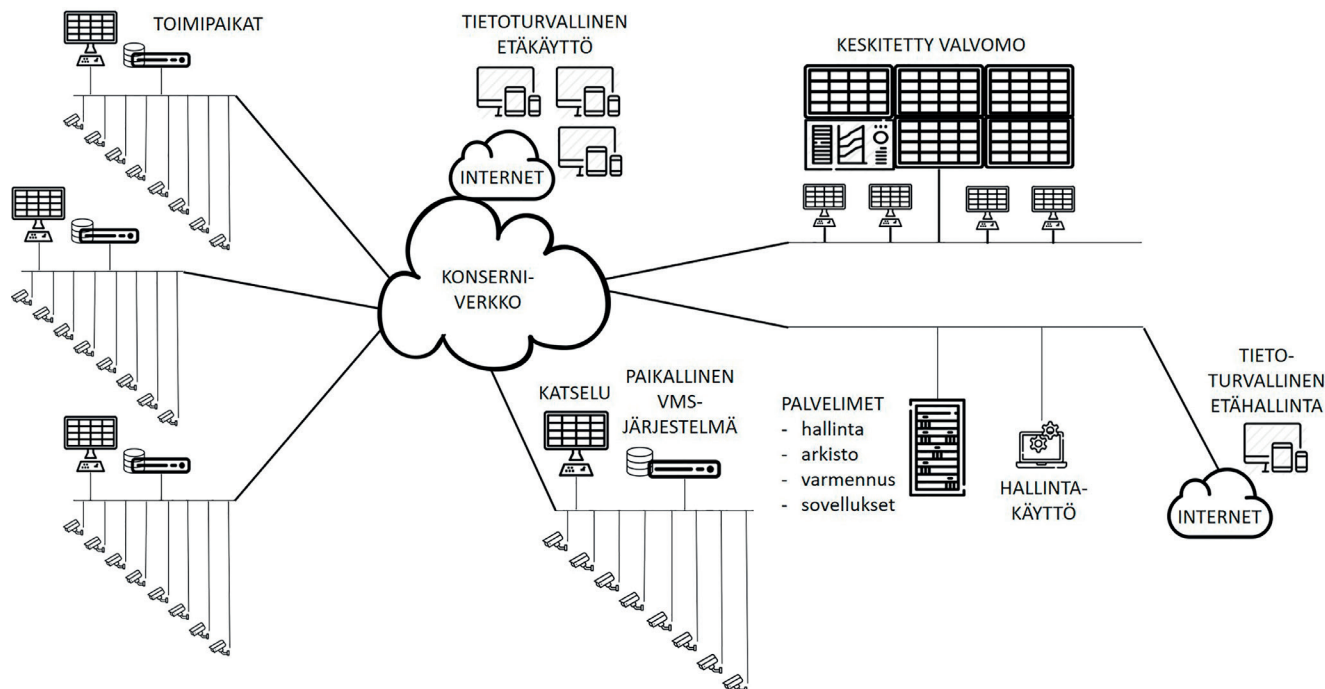
2.5.6 Monitoimipaikkaratkaisut

VMS-ohjelmistot mahdollistavat useiden eri toimipaikkojen liittämisen samaan loogiseen kokonaisuuteen, jolloin kokonaisuus toimii käyttäjien kannalta aivan vastaavasti kuin yksittäinen kohde. Ratkaisuja on mahdollista toteuttaa useilla eri topologioilla ja niiden yhdistelmillä.

Useimmiten ratkaisu toteutetaan siten, että paikalliset VMS-järjestelmät liitetään yhteen hallintapalvelimeen. Se hallitsee kaikkia yksittäisiä kohteita ja käyttäjien oikeuksia. Tämän hajautetun topologian yksi suurimmista eduista on korkea käytettävyys, koska mikään yksittäinen vika ei keskeytä kokonaisuuden toimintaa. Vikatilanteiden välttämiseksi ja verkon kuormituksen minimoimiseksi tallennus tapahtuu paikallisesti. Paikallisista tallenteista huolimatta tallenteet ovat käytettävissä kaikkialla ratkaisukokonaisuudessa.

Toinen toteutustapa on täysin keskitetty VMS-järjestelmä, jolloin tallennus tapahtuu keskitetysti yhteen tallennusjärjestelmään. Tässä keskitetyssä topologiassa pitää olla hyvät ja suorituskykyiset verkkoyhteydet, jotta kaikki tarvittavat kuva-aineisto saadaan siirrettyä keskitettyyn tallennusjärjestelmään.

Hajautetun ja keskitetyn topologian yhdistelmä on useimmiten kaikkein kustannustehokkain ratkaisu, koska silloin päästään optimoimaan hyvin erikokoisten toimipaikkojen tarpeet ja välttämään tarpeettomilta laiteinvestoinneilta pienissä toimipaikoissa.



Kuva 11. Monitoimipaikkainen VMS-ratkaisu.

2.5.7 Sovellukset

VMS-ohjelmistoihin on tarjolla monia eri sovelluksia, kuten visuaalista raportointia, статистиikka, laitteiden tilan visuaalista valvontaa, laitteiden käytettävyyden ja käytön seuranta. Sovellusten avulla parannetaan ohjelmistosta saatavaa hyötyä ja myös käytettävyyttä. Sovellusten tarvetta ovat merkittävästi lisänneet kameroiden monipuoliset analytiikkaominaisuudet. Useimmat sovellukset pystyvät ohjaamaan VMS-järjestelmiä, mikä tuo automaattisia toimintoja VMS-ohjelmistojen päivittäiseen käyttöön.

2.5.8 Liitännät muihin järjestelmiin

VMS-ohjelmistot liittyvät yhä useammin muihin organisaation käytössä oleviin järjestelmiin, kuten hälytys-, kulunvalvonta-, paloilmoin-, ajoneuvojen kulunhallinta-, kiinteistöautomaatio- ja prosessiautomaatiojärjestelmiin. Kaikki edellä mainitut ja monet muut organisaation järjestelmät liittyvät älykkääseen palvelualustaan, joka prosessoi eri järjestelmien tuottaman datan ja sen perusteella antaa erilaisia ohjauksia ja tietoa eri järjestelmille. Älykäs palvelualusta ohjaa VMS-järjestelmää eri järjestelmien tuottaman tiedon perusteella. Se näkyy VMS-ohjelmiston käyttäjille automaattisina toimenpiteinä, jotka tehostavat toimintaa merkittävästi.

Esimerkkejä VMS-ohjelmistojen liitännöistä muihin järjestelmiin

- Kassajärjestelmä: tallenteita voidaan ottaa jokaisen kassatapahtuman yhteydessä, mikä nopeuttaa ongelmatapauksien selvittämistä.
- Kiinteistönhallinta: voidaan yhdistää ohjaamaan lämmitystä, ilmanvaihtoa tai ilmastointia ja laajentaa kuulutuksiin, valaistukseen tai esimerkiksi paloilmoinjärjestelmään
 - rikkoutuneet laitteistot voidaan havaita kameroista ja järjestelmä välittää tietoa kiinteistönhoidolle
 - paloilmoinjärjestelmä voi ohjata kamerat näyttämään tai tallentamaan kuvaa uloskäynneiltä, jolloin saadaan pelastushenkilökunnalle ja kiinteistöhdolle mahdollisimman reaaliaikaista kuvaa siitä, missä apua tarvitaan eniten
 - videoanalytiikka voi havaita epämääräistä liikehdintää, onnettomuustilanteita tai yleisöryntäyksiä kiinteistöissä hätätilanteissa
 - automaattisia hälytyksiä voidaan lähettää, jos liikehdintää tapahtuu suljetuilla alueilla tai huoneissa, IP-kaiuttimilla voidaan ohjata kuulutuksia tai avata vartijan puheysteys kohteelle
 - kameroiden liikkeentunnistusta voidaan hyödyntää valaistuksen ja lämmityksen ohjaukseen energian säästämiseksi.
- Paloturvallisuusjärjestelmät: paloriskejä voidaan ennakoida ja havaita poikkeamia normaalista toiminnasta ja olosuhteista, jolloin on mahdollista järjestää ennakoiva huolto selvittämään tilanne.
- Teolliset ohjausjärjestelmät: etäyhteydellä tapahtuva prosessien tarkkailu ja ohjaus voidaan mahdollistaa videohallintajärjestelmän avulla. Automatisoidut tallenteet ja niiden eteenpäin lähettäminen voidaan rakentaa tapauskohtaisesti.
- Kulunvalvonta: hallinta, havainnointi ja ohjaustieto kulunvalvonnasta voidaan rakentaa videohallinta- ja kameravalvontajärjestelmän yhteyteen keskitetysti, jolloin sekä kamerat että kulunvalvonta, kulkukorttilukijat ja ovipuhelimet ovat käytettävissä samassa järjestelmässä.

2.5.9 Valvomo

Suuri, useita satoja tai tuhansia kameroita käsittävä VMS-järjestelmä liittyy usein valvomoon, jossa työskentelee useita henkilöitä samanaikaisesti. Valvomoon liittyy usein myös muita järjestelmiä, kuten eri turvallisuus- ja kiinteistöautomaatiojärjestelmiä.

Valvomo muodostuu suurista seinänäyttöjä ohjaavista näyttöpalvelimistä ja valvojien työasemista. Valvojien työasemista on mahdollista ohjata automatisoituja valvomonäyttöjä. Valvojat työskentelevät omilla työasemillaan, joissa on useita näyttöjä, tyypillisesti neljä näyttöä.

VMS-järjestelmät mahdollistavat useiden valvomoiden liittämisen samaan kokonaisuuteen. Kullakin valvomolla voi olla oma toiminnallinen roolinsa kokonaisuudessa, esimerkiksi alueellinen, päiväkäyttö-valvomo tai varavalvomo.

2.5.10 Varmennukset

VMS-ohjelmistojen toiminnan varmentaminen vikatilanteiden varalta, eli niin kutsuttu Fail-over, on erityisen tärkeää silloin, kun on kyse toiminnallisesti tärkeästä järjestelmästä. VMS-palvelimen varmentaminen on niin toiminnallisesti kuin taloudellisestikin järkevintä tehdä virtuaalipalvelinympäristössä. Parhaimmillaan varmennetussa ympäristössä katkokset ovat enintään muutaman sekunnin luokkaa. VMS-järjestelmän varmennuksia suunniteltaessa pitää huomioida myös tietoverkon kriittiset solmukohdat, jotta yksittäinen verkkovika ei keskeytä järjestelmän toimintaa.

2.5.11 Itsediagnostiikka

VMS-järjestelmän itsediagnostiikka (Audit Trail -toiminnallisuus) muodostuu tyypillisesti kolmesta eri kokonaisuudesta, joita ovat VMS-järjestelmän tekninen toiminta, sen käyttö ja yksittäisten käyttäjien tekemät käyttötoimenpiteet.

Itsediagnostiikka seuraa järjestelmän ja siihen liitettyjen kameroiden toimintaa, kirjaa toimintavirheet lokiin ja tekee ilmoituksen havaitsemaan vikatilanteesta. Ohjelmisto kirjaa automaattisesti lokiin myös järjestelmään tehdyt muutokset, kuten kameroiden lisäykset, uusien käyttäjien luonnin jne. Lokiin kirjautuvat määrittelyjen mukaisesti myös seuraavat käyttäjien tekemät toimenpiteet: kamerakuvien aukaisut, kamerakierrokset, tallenteiden katselut, videoleikkeiden tekemiset jne.

Kaikki lokitapahtumat saadaan visuaalisiin raportteihin, joista vastuulliset henkilöt näkevät nopeasti tehdyt toimenpiteet. Raporteista on erityistä hyötyä esimerkiksi tietosuoja-asioiden selvittelyssä.

2.5.12 Hallinta

VMS-ohjelmistojen hallinta tapahtuu keskitetysti joko etäyhteydellä tai sen tietoverkon sisältä, johon järjestelmä on liitetty. Hallinta tapahtuu joko erillisellä hallintasovelluksella tai selainkäyttöliittymällä. Jos käytetään hallintasovellusta, sen tulee olla asennettuna kaikkien niiden henkilöiden tietokoneisiin, jotka tekevät järjestelmän hallintaa. VMS-ohjelmiston asetus- ja konfiguraatiodietoista pitää olla ajantasaiset varmuuskopiot sekä asiakkaalla että ylläpitävällä organisaatiolla. Uudet varmuuskopiot pitää tehdä jokaisen muutoksen jälkeen.

Käyttäjäorganisaatio itse yleensä hallitsee käyttäjiä ja heidän käyttöoikeuksiaan. Isoissa organisaatioissa VMS-ohjelmistot liitetään usein tietoverkon käyttäjähallintaan (esimerkiksi Microsoft AD). Kun henkilöltä suljetaan tietoverkon palvelut, sulkeutuvat samalla myös VMS-järjestelmän käyttöoikeudet.

2.5.13 Käyttöoikeudet

VMS-ohjelmistot mahdollistavat käyttöoikeuksien yksilöllisen luonnin käyttäjille. Kuva-aineisto on usein hyvin luottamuksellista, ja siksi on erityisen tärkeää ennaltaehkäistä mahdollisia väärinkäyttötilanteita. Yksi keskeisimmistä asioista on käyttöoikeuksien suunnittelu ja sen perusteella luotavat käyttäjäprofiilit. Käyttäjäprofiilit perustuvat usein työtehtäviin.

Käyttävät henkilöt liitetään ennalta luotuihin käyttäjäprofiileihin, jolloin heillä on profiilin mukainen käyttöoikeus. Profiileihin tehtävät muutokset päivittyvät kaikille henkilöille, jotka kuuluvat kyseiseen käyttäjäprofiiliin.

2.5.14 Verkon rakenne

VMS-järjestelmän suunnittelussa tulee kiinnittää erityistä huomiota tietoverkon suunnitteluun, koska kameroiden lähettämät useat kuvastriimit tuottavat merkittävän kuorman tietoverkkoon ja siihen kuuluville aktiivilaitteille, kuten kytkimille ja reitittimille. Kameroiden lähettämä datamäärä ei ole vakio, vaan se muuttuu olosuhteiden mukaan esimerkiksi hämärässä valaistuksessa. Kameroissa on mahdollista asettaa datamäärä vakioksi, mutta silloin kuvanlaatu saattaa huonontua olosuhteiden muuttuessa.

Tietoverkon kuormitusta laskettaessa on myös huomioitava liikenteen solmupisteet, joissa eri kameroista tulevat kuvastriimit yhtyvät. Vastaavasti on huomioitava tallennusjärjestelmän ja VMS-ohjelmiston verkkoliitännöjen kapasiteetin riittävyys.

Suuret liikennemäärät edellyttävät tallennusjärjestelmän levyasemilta riittävää kirjoitusnopeutta, mistä saattaa muodostua joissakin tilanteissa pullonkaula. Tämä voidaan välttää hajauttamalla tallennukseen tulevaa liikennettä.

2.6 ANALYTIikkaOHJELMISTOT

Analytiikan käyttö kameravalvonnassa perustuu siihen, että kameroiden tuottamaa dataa hyödynnetään muuhunkin kuin perinteiseen turvallisuusvalvontaan. Tyypillisesti sitä käytetään yleensä alueelliseen valvontaan, liiketoiminnan kehittämiseen ja esimerkiksi henkilölaskentaan, asiakasluokituksen ja asiakkaiden käyttäytymisen sekä kulkemisen arviointiin, tilojen käyttöasteiden seurantaan tai esimerkiksi rekisterikilpien tunnistamiseen.

Kameralaitteiden prosessoritehot ovat viime vuosina kasvaneet huomattavasti, ja kamerat ovatkin jo itsessään pieniä tietokoneita. Niiden laskentatehoa voidaan hyödyntää tulkitsemaan, mitä kuvassa tapahtuu. Tämänkaltaiset niin kutsutut Edge-analytiikat sijoittavat nimensä mukaisesti enemmän käsittelytehoa ”verkon reunalle” mahdollisimman lähelle sensoria, joka kerää dataa. Näin data voidaan käsitellä, ennen kuin se siirretään pilveen palvelinkeskukseen.

Jo suunnitteluvaiheessa tulee kiinnittää erityistä huomiota tietosuojasäännösten noudattamiseen, jos tallenteista voi suoraan tai epäsuorasti tunnistaa henkilöitä. Toteutusvaiheessa valitaan käyttötarpeeseen sopivat laitteet ja määritellään niiden asennuspaikat ja suuntaukset oikeanlaisiksi. Kameroiden asennuspaikoilla ja -korkeuksilla on suuri merkitys onnistuneelle lopputulokselle. Lisähaastetta tuovat muuttuvat olosuhteet, kuten ulkotiloissa erityisesti sään vaihtelut.

Erilaiset hahmontunnistustekniikat ovat lisänneet kameravalvontajärjestelmien käytettävyyttä huomattavasti. Henkilön, ajoneuvon tai kulkuvälineen hahmo ei ole erityinen henkilötieto, joten niitä voi etsiä tallennemassasta vapaasti. Hahmontunnistusta ei pidä sekoittaa kasvontunnistukseen, jossa henkilön biometristä tietoa eli kasvokuvaa verrataan algoritmin avulla taustalla oleviin järjestelmin. Kasvontunnistusta saa suorittaa lähinnä henkilön suostumuksella esimerkiksi kulunvalvonnan yhteydessä.

2.6.1 Esimerkkejä analytiikan käytöstä kameravalvonnassa

Kamera-analytiikalla tehtyjen havaintojen pohjalta voidaan ottaa tallenteita, laukaista hälytyksiä ja lähettää ilmoituksia henkilökunnalle tai vartijoille. Mikäli kamerasyöte yhdistetään IP-verkossa toimiva kaiutin ja ääniyhteys, voidaan kohteelle käynnistää automaattisia kuulutuksia tai mikrofonin avulla jopa kaksisuuntainen puhe-yhteys. Alla on lueteltu tyypillisiä esimerkkejä analytiikan käytöstä kameravalvonnassa.

Hahmontunnistus

Hahmontunnistuksella tarkoitetaan tekniikkaa, jossa tunnistetaan hahmojen ja niiden liikkeen perusteella esimerkiksi henkilöitä ja ajoneuvoja. Kuva-alaan voidaan piirtää aitaviiva, jonka ylittäminen voidaan havainnoida.



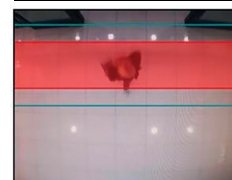
Asiattoman oleskelun havaitseminen

Asiattoman oleskelun havainnointiin on tarkoitettu niin kutsuttu Loitering-analytiikka. Se havaitsee henkilöt, jotka ovat viipyneet alueella tietyn, määritellyn ajan.



Kävijälaskenta ja tilannetieto

Kävijälaskentaa tai tilannetietoa kohteen asiakasmääristä voidaan suorittaa suoraan kameroissa, joiden tietoa kävijämääristä voidaan viedä eteenpäin erilliseen raportointityökaluun. Myös väärän kulkusuunnan perusteella voidaan tehdä hälytyksiä tai kuulutuksia.



In ↓ Out ↑
991 1068

	In	Out
9 seconds ago	1	0
12 seconds ago	1	1
14 seconds ago	0	1
16 seconds ago	1	0
33 seconds ago	0	1
36 seconds ago	0	1
58 seconds ago	1	0
1 minute ago	3	0
2 minutes ago	0	4
3 minutes ago	1	0

Test accuracy

Jonovahti

Asiakasvirran optimointiin voidaan määritellä avustavaa kamera-analytiikkaa jakamaan henkilöstön työkuormaa ja vähentämään asiakkaiden odotusaikaa. Kameran havainnoimaa tietoa voidaan välittää henkilökunnalle reaaliaikaisesti.



Yksityisyyden suojaaminen

Kamerakuvaa voidaan myös suodattaa reaaliaikaisesti yksityiskohtaista henkilötietoa häivyttämällä. Suodattamatonta tallennetta kuvasta voidaan viedä tallentimelle ja hallita sitä tallentimen tai VMS-järjestelmän käyttöoikeuksien kautta.



Äänimaailman hyödyntäminen

Kamerajärjestelmien yhteydessä hyödynnetään nykyään myös ääntä automatisoimalla kuulutuksia kamera-analytiikan havaitsemien tilanteiden perusteella. Kameran liikkeentunnistus voi esimerkiksi käynnistää kohteessa kuulutuksia tiedottaen kameravalvonnasta tai ilmoittaa, että paikassa on asiaton oleskelu kielletty. Mikäli kameraan on yhdistetty tai se on varustettu sisäänrakennetulla mikrofonilla, voidaan kohteelle myös käynnistää kaksisuuntainen puheysteys, esimerkiksi valvottavan ja vartiointiliikkeen välille.

Kohteen äänistä voidaan myös tehdä havaintoja ja tämän pohjalta tehdä hälytyksiä tai kameratallenteita. Kameran äänianalytiikka voi tunnistaa ääniä, kuten esimerkiksi lasin rikkoutumisen, autohälyttimen, aseiden laukauksen, huudon ja joissain tapauksissa myös aggressiiviset äänenpainot taustapuheessa. Kyseinen äänihavainnointi voidaan tehdä suoraan kamerassa lähettämättä sitä eteenpäin tai ääntä erikseen tallentamatta.

2.7 KAMERATEKNOLOGIAN HYÖDYNTÄMINEN PALOTURVALLISUUDESSA

Palontorjunta on muutakin kuin vain palon tunnistamista ja pysäyttämistä sekä niistä ilmoittamista. Paloturvallisuus on myös ennakointia, jota voidaan tukea ja kehittää muilla nykyaikaisilla integroiduilla ratkaisuilla, kuten kamerateknologialla. Tähän kuuluvat myös oppaassa tarkastellut kamerateknologiat, joilla kyetään havaitsemaan tulipalon syttyminen ja savun muodostuminen, mutta voidaan myös tunnistaa muita tekijöitä alkavan palon taustalla. Tämä mahdollistaa perinteisen paloilmoitinjärjestelmän toimin-

nan tukemisen ja täydentämisen, jolloin kameroilla saatavaa dataa voitaisiin hyödyntää enemmänkin uusissa käyttökohteissa. Kameravalvonta mahdollistaa prosessien tehostamisen tekemällä esimerkiksi hälytyksiä toimintaympäristön poikkeamista ja riskitilanteista.

Kuten perinteiset kiinteistötekniikan ratkaisut, niin myös kameravalvontajärjestelmän integroiminen kiinteistönhallintajärjestelmään mahdollistaa tiedon keräämisen ja hyödyntämisen myös muissa järjestelmissä, kuten paloturvallisuusjärjestelmissä ja vahinkojen ennakoinnissa sekä analysoinnissa mahdollistaen jälkioppimisen tapahtumien jälkeen.

Paloriskien ennakointi

Perinteistä kameravalvontaa voidaan täydentää opettamalla tunnistettavia kohteita ja analysoimalla kameralla saatavaa kuvaa. Yksinkertaisia keinoja edistää paloturvallisuutta kameravalvonnalla ovat lämpö- tai savupatsaita tunnistavat kamerateknologiat. Lämpökameralla voidaan valvoa esimerkiksi sähkölaitetta ja asennuksia, jolloin voidaan ennaltaehkäistä sähköpaloja ja saada ennakoivaa tietoa huoltotarpeesta ja mahdollisista tulipaloriskeistä.

Usein palon taustalla on jokin tekijä, joka voidaan tunnistaa ja reagoida ennakoivasti, ennen kuin paloriski konkretisoituu. Tällöin kameravalvonta toimii ennaltaehkäisynä, ja tunnistettavana tekijänä voi olla normaalitoiminnasta poikkeavan tai toistuvan liikkeen tunnistaminen. Saatavilla olevasta kuvasta ja datasta voidaan myös erotella liikkeen ja toistuvuuden lisäksi liikkuvan kohteen kokoa tai tilassa olevia olosuhteita. Merkitsevä tekijä on normaalista poikkeavien olosuhteiden tai toiminnan tunnistaminen ja siihen reagointi. Merkitsevää voi olla myös aika, jonka perusteella voidaan arvioida, että kyseessä on tilanne, johon tulee reagoida, ja että tapahtuma on sellainen, joka ei kuulu kyseisen kohteen normaaliin toimintaan.



Analysointi ja jälkioppiminen

Ennakoinnin ja paloturvallisuuden varmistamisen lisäksi kameravalvonta voi myös auttaa vahinkojen selvittämisessä, jolloin voidaan selvittää turvallisuutta vaarantaneita tapahtumia jälkikäteen ja analysoida tapahtumia. Tallenteista saatavalla tiedolla voidaan taas kehittää järjestelmäkokonaisuutta, jossa paloturvallisuus on osana. Kameravalvonnan datan ja tapahtumien analysoinnilla on merkittävä kehittymismahdollisuus onnettomuuksista oppimisen ja palontutkinnan näkökulmasta. Kameravalvonta pystyy analysoimaan kuvasta erilaisia tapahtumia, ja analytiikan keräämän tiedon perusteella saadaan tehtyä nopeasti tapahtumien tutkimista helpottavia hakuja.

Kameravalvontaa voidaan käyttää erityisesti tuhopolttoriskien hallintakeinona, jolloin teknologiaa käytetään ilkivallan ja rikosten torjuntaan sekä tapahtumien selvittämiseen tallenteita tarkastelemalla. Tapahtuneiden palojen lisäksi kamerateknologiaa on mahdollista hyödyntää esimerkiksi paloilmoittimien ei toivottujen, erheellisten, hälytysten taustatekijöiden selvittämisessä.

Tilannekuvan kehittäminen pelastustoimen tukena

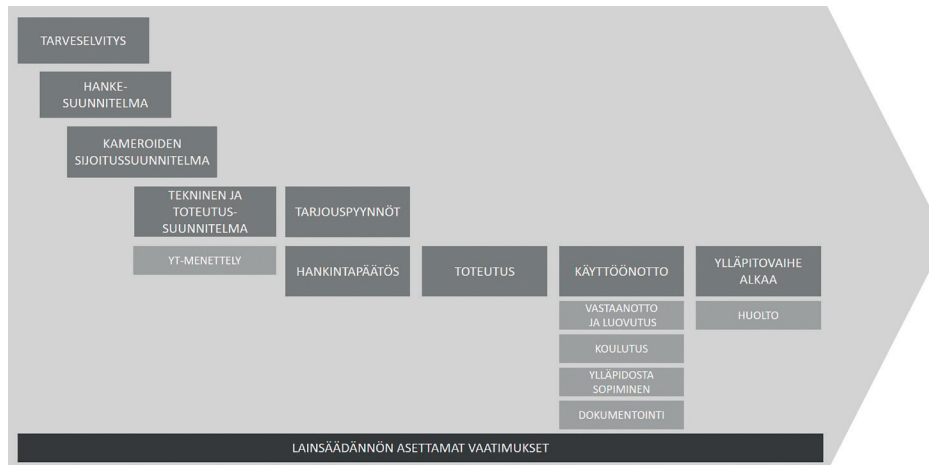
Valvontakamerat mahdollistavat reaaliaikaisen rakennuksen onnettomuus- ja vaaratilanteen tilannekuvan luomisen, jolloin tilannejohtamiseen saadaan tietoa ihmisten määrästä, palon vakavuudesta ja mahdollisista lisävaaraa aiheuttavista tekijöistä. Näin pelastuslaitos pystyy tekemään nopean tilannearvion näkemänsä perusteella ja tehdä tarvittavia ohjeistavia toimia, jotta kaikki henkilöt saadaan turvallisesti ohjattua pois vaaratilanteesta. Mitä nopeammin palohenkilöstö pystyy reagoimaan mahdollisiin riskitekijöihin, sitä pienemmät ovat vahingot. Saatava tieto voi myös jälkikäteen auttaa pelastusviranomaisia omassa kehitystyössä.

3 SUUNNITTELU JA HANKINTA

Kameravalvonnan suunnittelua, hankintaa ja toteutusta voidaan kuvata oheisen prosessikuvan avulla (kuva 12). Prosessin päävaiheet ovat yleensä samankaltaiset kaikissa kameravalvontajärjestelmäprojekteissa:

- tarveselvitys (miksi järjestelmä hankitaan ja mitä sillä halutaan saavuttaa tai estää tapahtumasta)
- hankesuunnittelu (toteutettavan järjestelmän sisältö)
- suunnitelma kameroiden ja käyttölaitteiden sijoittelusta tavoitteen saavuttamiseksi (lainsäädännön huomioiminen)
- tekninen ja toteutussuunnitelma
- tarjouspyynnöt (järjestelmän tai palvelun hankinta- ja elinkaarikustannukset)
- tarjousvaihe
- hankintapäätös
- toteutus (järjestelmän asennus)
- käyttöönotto (järjestelmän luovutus, vastaanotto, käyttäjien kouluttaminen)
- ylläpidosta sopiminen
- dokumentointi.

Eri vaiheet työllistävät hankkijaa sen mukaan, minkä kokoinen järjestelmä on. Lisäksi järjestelmää hankittaessa on huomioitava kameravalvontaa säätelevä lainsäädäntö ja vastuullisuus.



Kuva 12. Kameravalvonnan prosessi.

3.1 TARVESELVITYS

3.1.1 Kameravalvonnan tarpeellisuuden selvittäminen

Kiinteistö- ja toimitilaturvallisuuden perustana on rakenteellinen suojaus, jota täydennetään muilla turvallisuusjärjestelmillä, kuten kameravalvonnalla. Kameravalvontajärjestelmää hankittaessa on tärkeää määritellä sen käyttötarkoitus ja asiat, joihin järjestelmällä on tarkoitus vaikuttaa: mitä järjestelmällä on tarkoitus saada aikaiseksi tai mitä sillä halutaan estää tapahtumasta. Lisäksi tulee pohtia, voiko jollain muulla menetelmällä päästä samaan tavoitteeseen.

Halutun lopputuloksen saavuttamiseksi hanke tarvitsee vastuuhenkilön, joka ymmärtää hankittavan järjestelmän tavoitteen ja jolla on kokemusta hankinta- ja asennusprojekteista. Mikäli tilaajalla ei ole riittävää osaamista, on suositeltavaa käyttää kokenutta konsulttia hankintaprosessissa tai sen osissa. Konsultin tai konsulttiyrityksen osaaminen kannattaa varmistaa pyytämällä konsultilta referenssejä. On myös hyvä tiedustella käyttökokemuksia eri järjestelmistä ja tarvittaessa vieraillla kohteissa, joissa on omia tarpeita vastaavia järjestelmiä, sillä myyntipuheiden ja teknisten tietojen pohjalta on vaikea hahmottaa järjestelmien toimivuutta. Hankinnan suunnittelussa kannattaa olla kriittinen.

Kaikkien sidosryhmien edustajien osallistuminen tarveselvitykseen on tärkeää, jotta saavutetaan haluttu lopputulos. Sidosryhmien kuuleminen helpottaa myös kameravalvonnan suunnittelua, ja samalla tulee huomioitua lainsäädännön edellyttämä avoimuus kameravalvonnan toteuttamisessa.

Tarveselvityksessä on määriteltävä seuraavat asiat:

- mitä ja miksi halutaan kuvata (tavoite)
- missä ja milloin kuvaa tai tallenteita katsotaan
- kuka katsoo kuvaa tai tallenteita
- miten käyttöoikeuksia ja käyttöoikeustasoja hallitaan
- mihin ja miten tallennus, kuvansiirrot ja kuvien katselupisteet toteutetaan
- tietohallinnon tarjoamat mahdollisuudet ja sen asettamat raja-arvot
- lainsäädännön ja viranomaisten asettamat vaatimukset
- onko vakuutusyhtiön vaatimukset huomioitava
- tallenteiden käsittelyprosessi (katseluoikeudet, tallennusaika, luovutusprosessi ja tiedon hävittäminen).

Tarveselvityksessä selvitetään kysymysten avulla tarpeet ja esitetään toteutusvaihtoehtoja tavoitteiden saavuttamiseksi. Kartoituksesta on esimerkiksi käytävä ilmi, onko tarkoitus suorittaa yleisvalvontaa, tunnistaa henkilöitä sisäntuloväyliltä tai rekisterikilpiä porteilta ja minkälaisia kameramalleja asennetaan jne.

Kameravalvontaa suunniteltaessa on selvittävä tietohallinnon kanta kameravalvontajärjestelmän liittämisestä tietoverkkoon.

Tällöin on huomioitava

- olemassa olevan kaapeloinnin tai verkon hyödynnettävyys (kapasiteetti, rajoitukset)
- valvonnan etäkäytön mahdollisuudet
- kysymykset verkon hallinnasta ja huollosta
- käyttöön liittyvät riskit.

Olemassa olevan kameravalvontajärjestelmän uudistamishankkeen määrittelyissä ja ratkaisumalleissa voidaan käyttää apuna edellä mainittua luetteloa asioista, jotka määritellään tarveselvityksessä. Sen lisäksi on selvitettävä

- nykyisen järjestelmän tekniikka ja laatutaso (kunto)
- järjestelmän mahdollinen laajennettavuus ja hyödynnettävyys (integrointimahdollisuudet)
- järjestelmän jäljellä oleva käyttöikä.

Ostamisen sijaan vaihtoehtona on hankkia järjestelmä palveluna. Tällöin hankittavat laitteet ja mahdollinen tallennuskapasiteetti vuokrataan ulkoiselta toimijalta. Vuokrattaessa on hyvä selvittää, onko palvelutoimittajalla tarjolla myös kameravalvonnan etäpalvelu.

3.1.2 Muiden turvallisuuskeinojen selvittäminen

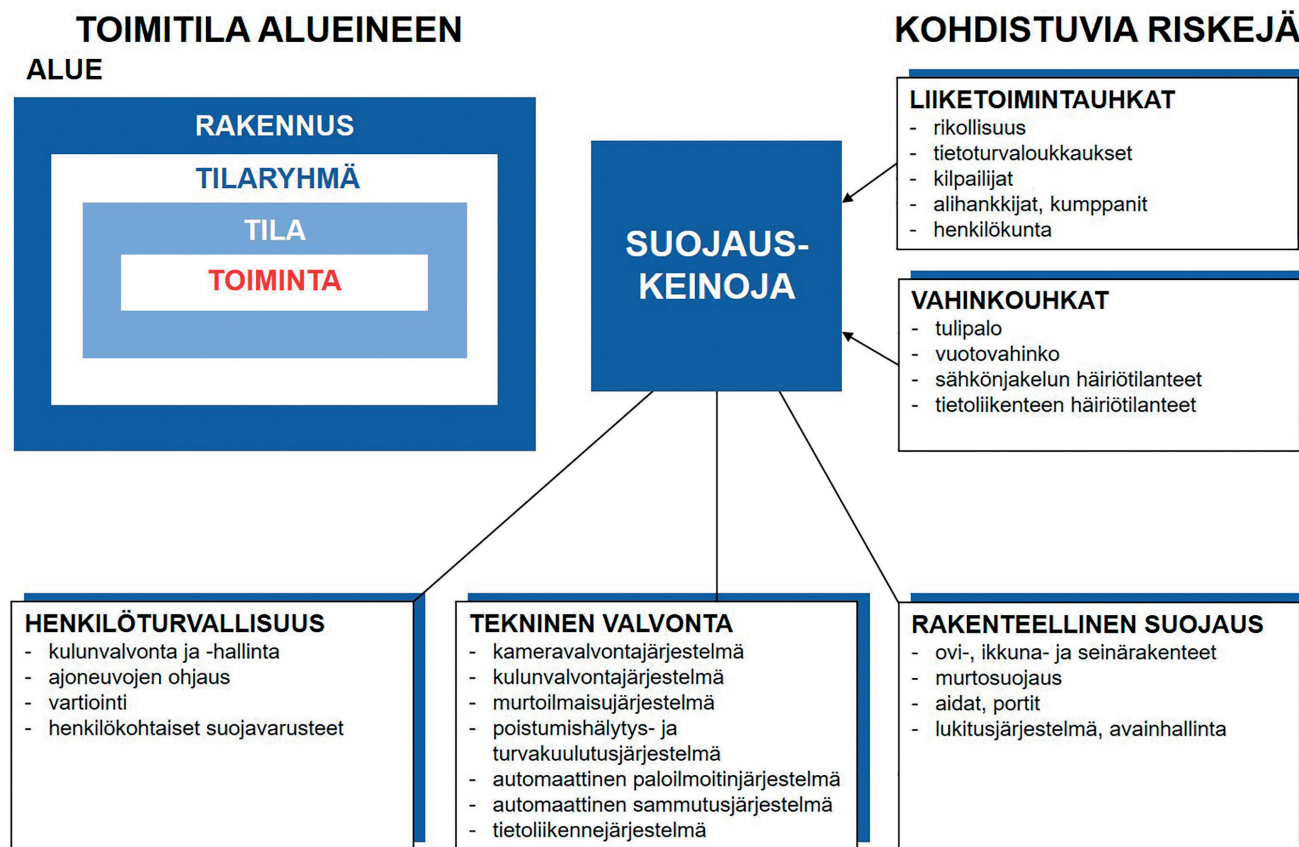
Laajoissa tarveselvityksissä on hyvä tehdä perusteellinen omaisuuden ja henkilöstön uhkakartoitus, jonka pohjalta laaditaan riskiarvio. Tämän jälkeen tunnistetuille riskeille asetetaan hyväksyttävät rajat ja määritellään turvallisuustaso sekä tavoitteet. Kartoitusta tehtäessä on tarkasteltava myös yrityksen tai yhteisön turvallisuusjohtamisen ja -hallinnan kokonaisuus käsittäen resurssit, toimintamallit sekä tekninen ja rakenteellinen turvallisuus.

Tarveselvityksen yksi tavoite on selvittää tapahtumat, jotka voitaisiin estää etukäteen kameravalvonnalla. On kuitenkin hyvä ymmärtää, ettei kameravalvonta yksin ratkaise turvallisuuden haasteita, vaan täydentää olemassa olevia turvallisuusjärjestelyitä. Siksi kameravalvonnan kustannuksia on verrattava muiden suojauskeinojen kustannuksiin suhteessa asetettuihin tavoitteisiin. Olemassa olevista suojauskeinoista valitaan omaan toimintaan parhaiten sopivien suojaustapojen yhdistelmä, ja sen perusteella laaditaan kattava suunnitelma.

Muita kameravalvonnan sijaan tai rinnalla käytettäviä turvallisuuskeinoja voivat olla:

- kulunvalvonnan, lukitusjärjestelmän ja avaintenhallinnan kehittäminen
- rakenteellisen suojauksen tehostaminen parantamalla rakenteiden kestävyyttä
- valaistuksen lisääminen piha-alueilla ja sisäänkäyntien kohdalla
- tilojen varustaminen murto- ja ryöstöilmaisulaitteilla
- varkausalttiin omaisuuden sijoittaminen parempaan suojaan (kassakaappi, lukittu tai muu tila jne.) tai valvonnan kannalta parempaan paikkaan
- vartiointi- ja valvomotoiminnan tehostaminen esimerkiksi kuulutusten tai äänitteiden avulla.

Laajoissa kartoituksissa voi käyttää apuna ST-kortiston julkaisua ST-ohjeisto 4 Kiinteistö- ja tilaturvallisuuden tasot sekä siihen liittyvää lomaketta ST 660.40 Kiinteistö- ja tilaturvallisuustasojen määrittäminen. Myös oheinen kaavio toimitilaturvallisuudesta kokonaisuutena auttaa hahmottamaan yritystoimintaan kohdistuvia riskejä.



Kuva 13. Toimitilaturvallisuus kokonaisuutena.

3.2 HANKESUUNNITELMA

Tarveselvityksen pohjalta tehtävässä järjestelmän hankesuunnittelussa asetetaan tavoitteet toteutettavan järjestelmän laajuudelle, toimivuudelle, laadulle, toimituksen ajoitukselle ja järjestelmän ylläpidolle. Hankesuunnitelman tarkoituksena on

- kuvata toteutettavan järjestelmän sisältö kiinteistön omistajalle ja käyttäjille
- toimia jatkosuunnittelun ohjausasiakirjana.

Lisäksi tehdään kustannusarviot järjestelmän investoinnista ja käytöstä sekä ylläpidosta.

Kameravalvontajärjestelmän hankesuunnitelmaesimerkki

(Lähde: ST-esimerkit 11 Hankesuunnitelmaesimerkki. Toimitilakiinteistö, sähkö- ja tietotekniset järjestelmät)

T550 KAMERAVALVONTAJÄRJESTELMÄ

Järjestelmäkuvaus

Kameravalvontajärjestelmä on valvottavan kohteen kuvaamiseen ja kuvan seurantaan sekä sen tallentamiseen perustuva turvallisuusjärjestelmä.

Kameravalvonta ehkäisee ennalta rikostapahtumia ja antaa mahdollisuuden selvittää turvallisuuteen liittyviä tapahtumia jälkikäteen.

Tämä määrittäminen sisältää kiinteistön hallinnassa olevien tilojen kameravalvonnan. Käyttäjillä on mahdollisuus hankkia tiloihinsa omat kameravalvontajärjestelmänsä tai liittyä kiinteistön kameravalvontaan erillisen sopimuksen mukaisesti.

Ominaisuudet ja varustelutaso

Kameravalvonnan tarkoitus on havaita ja tallentaa kameran kohteena olevan alueen tapahtumat ja tunnistaa valvontakohteessa olevat henkilöt.

Kameravalvontajärjestelmä sisältää keskuslaitteet, tallennintilan erillisellä palvelimella, valvontakamerat sekä tarvittavat varasähkölaitteet ja kaapeloinnin.

Kiinteistön hallinnassa olevalla kameravalvontajärjestelmällä valvotaan ulkoalueita, sisääntuloväyliä, ulko-ovia, yhteiskäyttöisiä sisätiloja, kuten kulkureittejä, pääaulaa sekä pysäköintitiloja.

Kameravalvontajärjestelmä valvoo tiloja aikaajotellusti.

Kameroiden kuvat tallennetaan 96 h ajaksi erilliselle palvelimelle.

Rajaukset

Kiinteistön hallinnassa olevien yhteiskäyttöisten tilojen kameravalvontajärjestelmä sisältyy kiinteistön hankintaosuuteen. Vuokralaisen, asukkaan tai käyttäjän hallinnassa olevien tilojen kameravalvontajärjestelmä on käyttäjän erillishankinta.

T550 Kameravalvontajärjestelmä / kiinteistön tilat					
	Investointi / uusiminen		Huolto / kunnossapito		Lisätietoja
	Kiinteistön omistaja / vuokranantaja	Vuokralainen / asukas	Kiinteistön omistaja / vuokranantaja	Vuokralainen / asukas	
Valvontayhteydet	X		X		
Keskuslaitteet	X		X		
Tallentimet	X		X		
Monitorit	X		X		
Kaapeloinnit	X		X		
Valvontakamerat	X		X		

3.3 HANKINTAKUSTANNUKSET

Kameravalvontajärjestelmän hankinnassa on heti alusta pitäen varauduttava kustannuksiin. Kustannuksia syntyy laitehankintojen lisäksi muun muassa seuraavista asioista:

- tarveselvitys
- hankesuunnittelu
- suunnittelu
- tarjouskilpailun järjestäminen
- järjestelmä- ja laitekokonaisuuksien hankinnat
- kaapelointi, kytkimet ym. verkon aktiivilaitteiden konfigurointi
- asennus- ja ohjelmointityöt
- katselupisteiden toteutus
- koulutus
- järjestelmän dokumentointi
- käyttö-, ylläpito- ja huoltotyö.

Käyttö- ja ylläpitokustannuksissa kannattaa huomioida mahdollisten verkkoyhteyksien, etäpalveluiden ja muiden ylläpitotoimien, kuten ohjelmisto- ja tietoturvapäivitysten, aiheuttamat kustannukset. Kustannusarvioinnin perusteella tulee laatia hankkeelle budjetti ja alustava aikataulu. Jos budjetti on jo ennalta määrätty ja kiinteä, hankkeen eri osat tulee priorisoida ja toteuttaa tärkeysjärjestyksessä. Tällöin on syytä huomioida erityisesti järjestelmien mahdollinen laajennettavuus tulevaisuudessa.

Esimerkki

Huoltoasemalle hankittavan laadukkaan kahdeksan kameran kameravalvontajärjestelmän hinnaksi muodostuusuunnittelu-, verkko-, asennus-, koulutus- ja dokumentointitöineen noin 5 000 – 7 000 euroa.

3.4 SUUNNITTELIJAN VALINTA

Seuraavaksi hankkeelle valitaan ammattitaitoinen suunnittelija, jolta edellytetään turvallisuustekniikan ja kameravalvonnan hyvää tuntemusta eri käyttö- ja ICT-ympäristöissä. Suunnittelija valitaan kohteen vaativuuden perusteella. Esimerkiksi tavanomaisen kameravalvontajärjestelmän toteutussuunnittelu voidaan toteuttaa erillisenä sähkösuunnittelun yhteydessä, jos kyseisellä yrityksellä on kokemusta suunnittelusta. Vaativimpien kohteiden suunnittelu on tehtävä perusteellisemmin, ja tekijäksi valitaan turvasuunnitteluun perehtynyt suunnittelija. Lisäksi apuna on käytettävä verkkosuunnittelijoita.

Suunnittelun voi ostaa urakkatyönä kiinteällä hinnalla, jos työ on selkeä ja helposti toteutettavissa. Suunnittelutyön voi ostaa myös palveluna. Vaativimmissa kohteissa työ tehdään usein tuntityönä, jolle asetetaan tarvittaessa yläraja. Kaikki suunnittelutyön toimeksiannot ja sopimukset on tehtävä kirjallisina. Niistä on selvittävä muun muassa

- hankkeen kuvaus
- suunnittelun tai muun tehtävän kuvaus ja rajaaminen
- hankkeen ja suunnittelun toteutusaikataulut
- palkkiomuoto ja palkkioperusteet
- sopimus
- toteutuksen urakkamuoto
- suunnittelun esitysmuoto
- suunnittelussa käytettävät tietokoneohjelmat, tallennusmuodot yms.
- sisältääkö suunnittelu työmaakäyntejä tai valvontaa.

Jos turvallisuushanke on esimerkiksi osa isoa rakennushanketta, siinä voi olla mukana tilaajan ja toimitajan lisäksi myös muita tahoja. Tällöin on olennaista, että kaikkien mukana olevien toimijoiden yhteistyö sujuu jo suunnitteluvaiheessa. Asetetusta turvallisuustasosta ei tarvitse tinkiä esimerkiksi arkkitehtonisten seikkojen vuoksi. Suunnittelijan tehtävä on valita tarkoitukseen sopivat laitteet, jotka täyttävät parhaiten kaikkien osapuolien vaatimukset.

Valittu suunnittelija aloittaa tilaajan tarveselvityksen perusteella järjestelmän teknisen suunnittelun. Ensimmäisten luonnossuunnitelmien perusteella selviävät järjestelmän pääkomponentit, kuten kamerat ja tallentimet, sekä toteutuksen arvioitu kokonaiskustannus. Tilaajan on tarvittaessa tarkennettava teknisiä vaatimuksia, kommentoitava suunnitelmia ja valittava kokonaistaloudellisesti järkevimpiä vaihtoehtoja. Jos tilaaja on eri taho kuin järjestelmän käyttäjä, myös käyttäjän on kommentoitava luonnossuunnitelmia hyvissä ajoin ja niin, että kommentointiin varataan riittävästi aikaa.

3.5 HANKINTAPROSESSIN LAINSÄÄDÄNTÖ

Kameroiden käyttämisestä, sijoittelusta ja tallenteiden säilytyksestä säädetään pääosin EU:n tietosuojasetuksessa, kansallisessa tietosuojalainsäädännössä ja rikoslaissa. Asennustoiminnan harjoittamista säädel­lään yksityisistä turvallisuuspalveluista annetussa laissa. Kameravalvontajärjestelmien teknisestä suori­tuskyvystä tai laadusta ei ole viranomaismääräyksiä. Järjestelmät ja niihin kuuluvat laitteet ovat soveltuvin osin yleisten sähköturvallisuutta, sähkömagneettista yhteensopivuutta, telepäätelaitteita ja radiolaitteita koskevien säädösten alaisia.

Vastuu kameravalvontajärjestelmän käytön lainmukaisuudesta ja tietoturvallisuudesta kuuluu yleensä järjestelmän omistajalle, haltijalle tai käyttäjälle. Siksi järjestelmän omistajan ja haltijan on oltava tietoisia vastuistaan ja velvollisuuksistaan. Myös hyvä suunnittelu- ja urakointitapa edellyttävät, että toimeksiantajaa tiedotetaan hänen velvollisuuksistaan.

Lainsäädännössä määrätty henkilöstön yhteistoimintamenettely on huomioitava suunnittelussa ja käytävä läpi ennen käyttöönottoa. Menettelyssä koko teknisen turvallisuusvalvonnan osa-alue suositellaan käsiteltäväksi yhtenä kokonaisuutena.

Yhteistoimintamenettelyssä käydään läpi alustava luonnossuunnitelma kameravalvonnan toteuttamisesta eri tiloissa. Lisäksi menettelyssä on käsiteltävä järjestelmän tietosuojaseloste sekä menettelyt, joiden avulla toteutetaan avoin tiedottaminen, tietojen tarkistusoikeus sekä muut lainsäädännön velvoitteet. Näin menetellen kameravalvonnan käyttöönotto palvelee kaikkia osapuolia ja sujuu kitkattomasti koko organisaatiossa.

3.6 ESIMERKKEJÄ KAMERAVALVONNAN LAILLISUUDESTA

Kameravalvonnan laillisuudesta on vaikea antaa yksiselitteistä ohjetta. Lakien ja oikeuskäytännön perusteella kameravalvonnan laillisuus määräytyy eniten seuraavien tekijöiden mukaan:

- mihin oikeutettuun etuun järjestelmän käyttö perustuu
- missä tarkoituksessa valvontaa suoritetaan
- kuka valvontaa suorittaa
- missä paikassa oleskelevaan henkilöön valvonta kohdistuu
- onko kysymyksessä pelkkä katselu vai myös kuvan tallentaminen
- kuunnellaanko tarkkailtavaa tai talletetaanko puhetta
- kuinka salaista tai avointa valvonta on, eli miten valvonnasta on ilmoitettu
- mihin talletettuja tietoja käytetään ja kuinka kauan niitä säilytetään

- luovutetaanko tietoja johonkin tarkoitukseen ja miten
- miten tiedot hävitetään.

Jotta kameravalvonta olisi sallittua, sen tulee täyttää sekä salakatselusäännösten että tietosuoja-asetuksen asettamat edellytykset. Jos kuuntelu liitetään valvontaan, sen on täytettävä rikoslain 24 luvun 5 §:n salakuuntelusäännöksessä asetetut edellytykset. Yleensä äänen tallentamiselle ei ole esteitä, kunhan se on perusteltua ja tallentamisesta ilmoitetaan siten, että puhuja voi olettaa ulkopuolisen kuulevan ja tallentavan hänen puhettaan. Tällöin rikoslain salakuuntelun tunnusmerkistö ei täyty. Vastaavasti tiettyissä puhelimitse hoidettavissa asiakaspalvelutilanteissa puheluiden tallentaminen on nykyisin yleinen käytäntö, ja siitä myös ilmoitetaan puhelun alussa.

Oikeuskäytännön perusteella muun muassa seuraavanlainen salakatselu valvontakameroilla on ollut rangaistavaa:

- ensiapuhuoneen oven kuvaaminen valvontakameralla huoneen sisäpuolelta valvonnasta ilmoittamatta
- työntekijöiden taukutilojen kuvaaminen valvontakameralla valvonnasta ilmoittamatta
- työntekijöiden turvavalvomon kuvaaminen valvontakameralla valvonnasta ilmoittamatta
- kerrostalon rappukäytävän kuvaaminen ovisilmäkameralla valvonnasta ilmoittamatta
- kameravalvonnan työnjohdollinen käyttäminen työntekijöiden tarkkailuun työpaikalla.

Onkin korostettava, että työntekijän työtehtävien laiminlyönnin selvittäminen kameralla on rikoslaissa kiellettyä salakatselua. Myöskään mahdollinen työtehtävien laiminlyönti ei oikeuta salakatseluun. Tosin olemassa olevia kameroita ja niiden tallenteita voi käyttää työsuhteen päättämisen perusteen toteen näyttämiseksi.

Kameralaitteistojen sijoitusta suunnittelevien sekä laitteistoja myyvien ja asentavien henkilöiden on syytä opastaa tilaajia ja käyttäjiä kameravalvonnan lainmukaiseen käyttöön. Jos esimerkiksi taloyhtiö tilaa kameravalvontajärjestelmän, tilaajalle on syytä mainita, että kotirauhan suojaamia paikkoja ovat myös asuintalojen porraskäytävät ja asukkaiden yksityisaluetta olevat pihat.

Seuraavaan taulukkoon on kerätty suuntaa antavia esimerkkejä kameravalvonnan sallittavuudesta eri kohteissa. Esimerkkiluettelo on osa tätä ohjetta, eikä sitä tule käyttää irrallisena tutustumatta ohjeen muuhun sisältöön. Taulukkoa avaavaa kameravalvonnan lainsäädäntöä on selostettu yksityiskohtaisemmin **LUVUSSA 8.**

	Kyllä	Ongelma	Ei
KERROSTALOT			
- porraskäytävät ja rapun ovi		x ¹⁾	
- varastotilat	x		
- piha-alueet	x		
- parkkihallit	x		
- kellari- ja ullakotilat	x		
OMAKOTITALOT JA RIVITALOT			
- piha-alueet ja sisäänkäynnit		x ²⁾	
KIOSKIT, KAUPAT JA MARKETIT			
- myymälätilat	x		
- kassavalvonta	x		
- sovituskopit			x
- pukutilat			x
- varasto- ja takatilat	x ³⁾		
- yleisöltä suljetut piha-alueet	x ³⁾		
- aitaamattomat piha-alueet	x ³⁾		
RAVINTOLAT			
- sali, baari ja aula	x		
- rulettipöytä ja pelipöydät	x		
- WC-tilat			x
TUOTANTOLAITOKSET			
- toimistotilat	x ⁴⁾		
- prosessivalvonta	x ⁴⁾		
- aidatut piha-alueet	x ⁴⁾		
- aitaamattomat piha-alueet	x		
- portit	x		

	Kyllä	Ongelma	Ei
VIRASTOT, LIIKEHUONEISTOT, TOIMISTOT JA KOKOUSTILAT			
- yleisölle avoimet sisätilat	x		
- yleisöltä suljetut sisätilat	x ³⁾		
SAIRAALAT, HOITOLAITOKSET JA PALVELUTALOT			
- yleisölle avoimet sisätilat	x		
- hoitohuoneet, asukashuoneet			x
- potilas- ja asukashuoneet			x
- henkilökunnan pukutilat			x
- asukkaiden yhteiset tilat	x ³⁾		
URHEILU- JA LIIKUNTAHALLIT			
- suoritustilat ja sisäänkäynnit	x		
- puku-, suihku- ja saunatilat			x
HUOLTOASEMAT			
- mittarikenttä, myymälä ja pesuhalli	x		
ASEMARAKENNUKSET			
- hallit, tavaransäilytys ja ravintolat	x		
LIIKENNEALUEET JA -VÄLINEET			
- kaupunkien yleisvalvonta ja tievalvonta	x		
- raitiovaunut, junat, metro ja linja-autot	x		

1) Kerrostalon porraskäytävän valvontaan on saatava taloyhtiön hallituksen tai yhtiökokouksen suostumus ja valvonnan tulee perustua asukkaiden turvallisuuden ja omaisuuden suojaamiseen. Ulko-oveen on laitettava ilmoitus tallentavasta kameravalvonnasta. Kameravalvonta ei saa ulottua asuntojen sisätiloihin.

2) Kameravalvonta on sallittu, kun kotirauhan suojaamassa paikassa tarkkaillaan oikeudettomasti paikassa oleskelevaa. Kameravalvonta ei saa ulottua omilta yksityisiltä piha-alueilta naapurien kotirauhan piiriin.

3) Yleisöltä suljetuissa julkisrauhan suojaamissa paikoissa oleskelevan katseleminen ja kuvaaminen kameravalvonnan avulla on kielletty, jos se tapahtuu oikeudettomasti ja tarkkailtavan yksityisyyttä loukaten. Kameravalvonnasta on myös ilmoitettava näkyvästi.

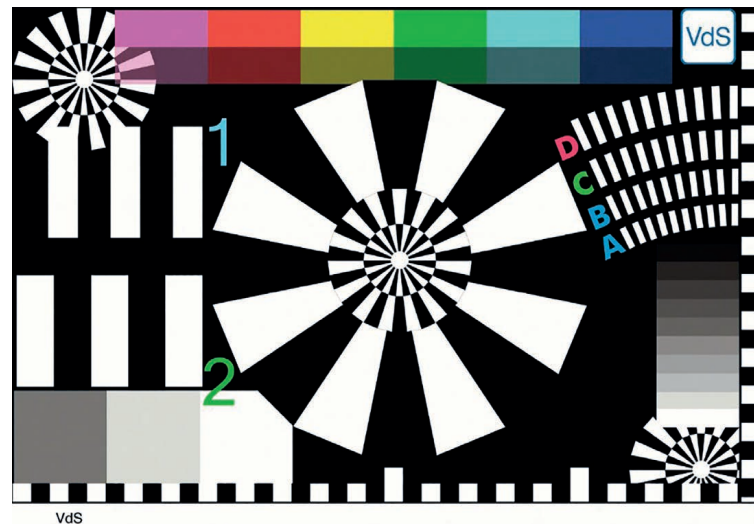
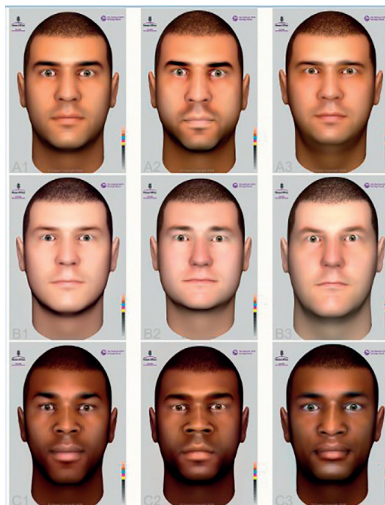
4) Kameravalvontaa voidaan työelämän tietosuojalain määrittelemissä tilanteissa kohdentaa myös tiettyyn työpisteeseen, esimerkiksi hotellien tai vastaavien kiinteistöjen vastaanottotiloihin. Työntekijöihin kohdistuva kameravalvonta kuuluu yhteistoiminta- tai kuulemismenettelyn piiriin.

3.7 STANDARDI JA K-MENETELMÄ KAMERAVALVONNAN SUUNNITTELUN TUKENA

3.7.1 Standardi SFS-EN 62676-4

Standardin SFS-EN 62676-4 Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 4: Soveltamisohjeet mukaan tehdyn teknisen hyväksyttävyyden mukaisessa testissä käytetään testitauluja, joilla todennetaan valvontakameroiden kuvanlaatu katselussa ja tallenteissa. Digitaalisten kameravalvontajärjestelmien kameroiden ja näytön resoluution välinen yhteys pitää huomioida: jos kamerasuoritus ei vastaa näytön resoluutiota, katsottava kohde ei näy välttämättä niin yksityiskohtaisesti kuin on suunniteltu.

Tässä menetelmässä käytetään kuvan laadun mittauksessa luonnollisen kokoista testikasvokuvasarjaa ja kuvanlaadun arvioitiin testitaulua. Hyväksyttävän kuvanlaadun varmentamiseksi tarvitaan kaksi ihmistä tekemään testit. Toinen näyttää kuvia tarkasteltaville kameroille ja toinen arvioi näkemänsä ja tekee samalla pöytäkirjan tarkastuksesta. Näiden perusteella tehdään yhteenveto siitä, ovatko kamerat oikeissa säädöissä ja kameroiden tuottamat kuvat kohteen tilaajan vaatimusten mukaisia.

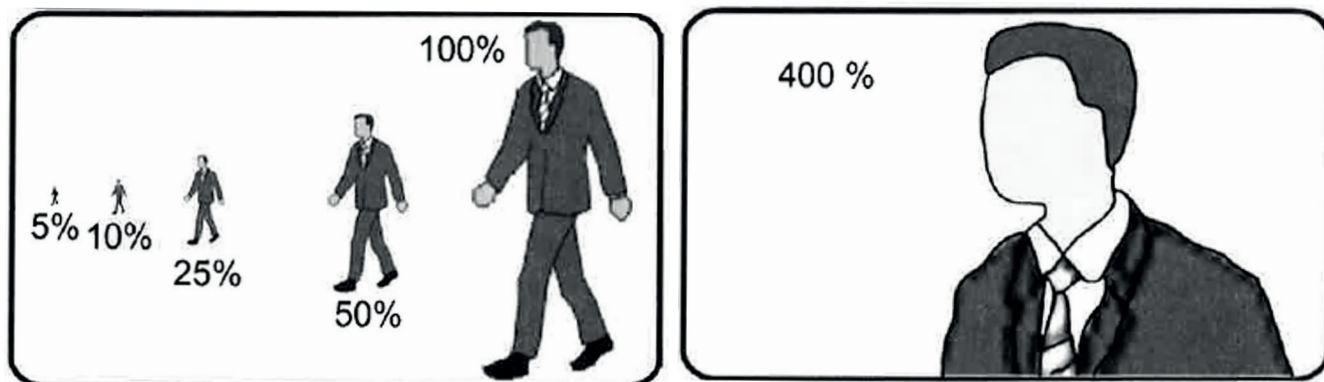


Kuva 14. Esimerkki kasvokuvista (itäintialainen, eurooppalainen ja afrikkalainen) sekä kuvan laadun testitaulu.

Eräät kameratoimittajat ovat määritelleet omille kameroilleen etäisyydet, joissa eri tunnistusetäisyydet täyttyvät kyseisen kameratyyppin ja asennetun linssin mukaan. Tarkastusmenetelmät on selvitetty tarkemmin itse standardissa esimerkiksi rekisterikilven tunnistuksessa.

Standardin mukaiset näkymät (kohteen koko) PAL-resoluutiolla (alla myös taulukko):

- seuranta tai ihmisjoukon hallintaa varten: kohteen on oltava vähintään 5 % kuvan korkeudesta tai yli 80 mm pikseliä kohti
- havaitseminen: kohteen on oltava vähintään 10 % kuvan korkeudesta tai yli 40 mm pikseliä kohti
- tarkkaileminen: kohteen on oltava 25 % kuvan korkeudesta tai yli 16 mm pikseliä kohti
- hahmon tunnistus: kohteen on oltava vähintään 50 % kuvan korkeudesta tai yli 8 mm pikseliä kohti
- yksilöiminen: kohteen on oltava vähintään 100 % kuvan korkeudesta tai yli 4 mm pikseliä kohti
- tutkiminen: kohteen on oltava vähintään 400 % kuvan korkeudesta tai yli 1 mm pikseliä kohti.



Luokka	PAL	NTSC	1080p	720p	WSVGA	SVGA	4CIF	VGA	2CIF	CIF	QCIF
Tutkiminen	400	450	150	250	300	300	300	350	600	600	1200
Yksilöiminen	100	120	40	60	70	70	70	85	150	150	300
Hahmon tunnistus	50	60	20	30	35	35	35	45	70	70	150
Tarkkaileminen	25	30	10	15	20	20	20	25	35	35	70
Havaistaminen	10	10	10	10	10	10	10	10	15	15	30
Seuranta	5	5	5	5	5	5	5	5	10	10	15

Kuva 15. Eri digitaalisia resoluutioita vastaava näytöllä näkyvän henkilön korkeus prosentteina.

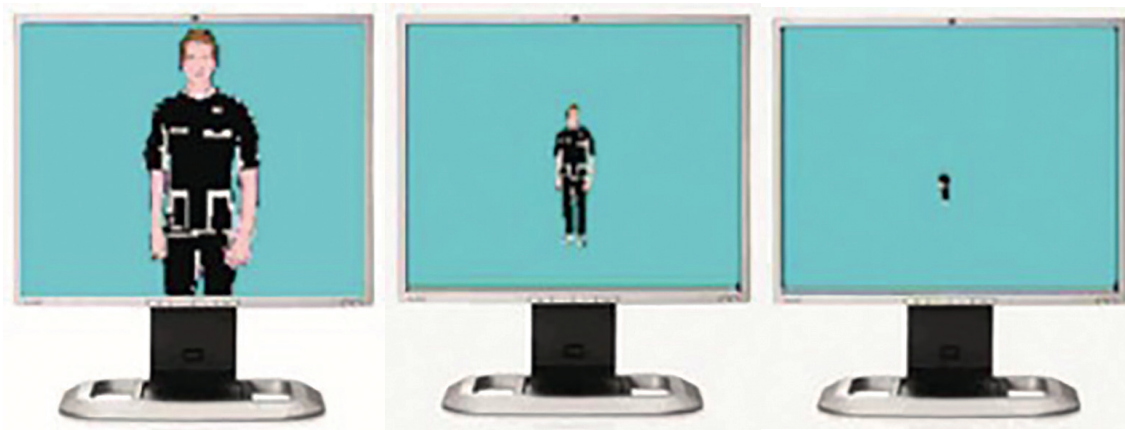
3.7.2 K-menetelmä

Luonnos- ja ominaisuussuunnittelun sekä teknisen suunnittelun apuna voi myös käyttää Finanssiala ry:n laatimaa kameravalvonnan K-menetelmää. Se on tarkoitettu kuvainformaation yksityiskohtaisuuden suunnittelu- ja tarkistusmenetelmäksi, kun valvottavat kohteet ovat henkilöitä. K-menetelmä on tarkoituksenmukainen kiinteillä kameroilla valvottavissa sisätiloissa, joissa olosuhteet, kuten esimerkiksi valaistus, eivät muutu.

Kameravalvonnan K-menetelmä on ladattavissa osoitteesta www.vahingontorjunta.fi.

K-menetelmässä määritellään tuotettavan kuvan tarkkuus henkilöitä kuvattaessa. Eri näkymien vaatimustasoja ovat tällöin

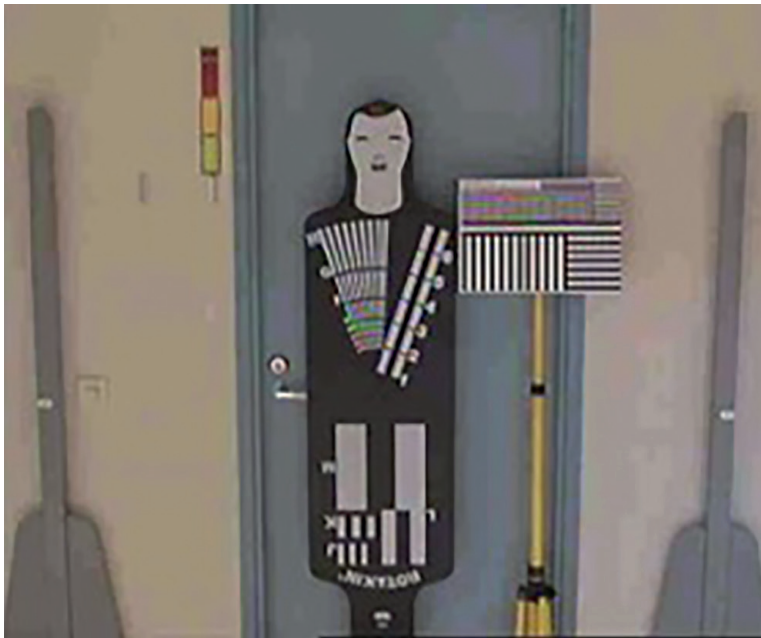
- yksilöinti (K120), näkökuva, kohteen oltava vähintään 120 % ruudun korkeudesta
- tunteminen (K50), kohteen oltava vähintään 50 % ruudun korkeudesta
- havaitseminen (K10), kohteen oltava vähintään 10 % ruudun korkeudesta
- yleiskuva (K5), kohteen oltava vähintään 5 % ruudun korkeudesta.



Kuva 16. Yksilöinti (K120), tunteminen (K50) ja havaitseminen (K10).

Jos valvottava kohde on muu kuin henkilö, on suunniteltava vastaavanlainen riittävä näkymä. Menetelmän idea on saada jokaisesta kamerasta mahdollisimman tarkoituksenmukaista kuvaa.

K-testitaulun avulla testataan järjestelmän suunnitelmanmukaisuus. Testitaulu on sekä asennukseen että tarkistukseen soveltuva työväline, jonka avulla kamerapaikan asennus ja säätö voidaan tehdä suunnitelman mukaisesti. Testitaulun etuna on sen hyödynnettävyys järjestelmää dokumentoitaessa. Tällöin kameroiden tallenteista otetuilla tulosteilla voidaan testitaulun avulla todistaa niiden suunnitelmanmukaisuus ja laatu.



Kuva 17. Standardin mukainen Rotakin-testitaulu ja K-testitaulu.

Ennakointi

K-menetelmän mukaisesti kameravalvonnan suunnittelussa muodostetaan tapahtumaennusteita. Ennakoinnin avulla varaudutaan riskien toteutumiseen ja tarkoituksenmukaisen kuvainformaation saamiseen. Tällöin kamerat sijoitetaan siten, että niistä pystytään seuraamaan loogisessa järjestyksessä esimerkiksi murron etenemistä.

Poliisin kannalta ennakkoinnissa tulee pyrkiä siihen, että rikoksesta epäilystä saadaan tapahtumapaikalta tunnistuskelpoista kuvaa mahdollisimman usein.

Havaittava liike

Yleensä valvontakamerat tallentavat materiaalia kuva-alassa tapahtuvan liikkeen perusteella. Tietyissä kriittisissä kohteissa, kuten metroissa, kuvamateriaalia tallennetaan kuitenkin jatkuvasti.

Pelkästä liikkeestä tallentaminen säästää tallentimien kovalevytilaa ja helpottaa tapahtumien etsimistä. Tallentimien tallennusherkyys on säädettävä kuitenkin tarpeeksi pienelle, että esimerkiksi hämärässä tapahtuva liike tallentuisi järjestelmään.

Valvonta-ajat

Valvontakameroiden tallennusajoille voidaan määrittää eri ajankohtia. Yleensä on kuitenkin paras valvoa ja tallentaa kaikkina ajankohtina.

3.8 OLOSUHTEIDEN HUOMIOIMINEN SUUNNITTELUSSA

Valaistus

Riittävä valotasoa on hyvän valvontakuvan edellytys. Siksi valaistukseen on kiinnitettävä huomiota ja lisättävä valoa, jos luonnonvaloa ei ole riittävästi.

Lisättävä valo voi olla joko tavallista valkoista valoa tai silmälle näkymätöntä infrapunavaloa. Nykyisin valaistus on suositeltavaa toteuttaa energiatehokkaalla valaisulla. Suunnittelussa on huomioitava, että varsinkin megapikselikamerat tarvitsevat paljon valoa. Osa ledivalaisimista tukee myös PoE-virransyöttöä. Tarvittavan valaistuksen voi saada aikaan myös kameroihin integroidulla infrapunaLED:illä.



Kuva 18. Valkoista valoa tuottava ledivalaisin ja vastaava infrapunavalaisin.

Kameroita asentaessa on huomioitava auringon nousu- ja laskusuunnat. Lisäksi suurten ikkunoiden kiinteistöissä on huomioitava auringon paisteen vaikutus kameroiden toimintaan.

Kiinteistön valaisimet tulee sijoittaa oikein kameroihin nähden. Jos kirkkaimman ja pimeimmän kohteen valaistustason suhde on liian suuri valvottavalla alueella, kamera ei kykene käsittelemään eroja. Erityisesti mainoskylttivalojen aiheuttamaa häirintää kameran kuva-alassa tulisi välttää.

Tarvittaessa värikameran sijaan voidaan käyttää kaksitoimisia kameroita, jolloin mustavalkokameran valoherkkyyttä saadaan hyödynnettyä pimeään aikaan.

Valaistussuunnittelua ohjaavat standardit SFS-EN 12464-1 Valo ja valaistus. Työkohteiden valaistus. Osa 1: Sisätilojen työkohteiden valaistus sekä SFS-EN 12464-2 Light and lighting. Lighting of work places. Part 2: Outdoor work places.

Esimerkki

Kuvassa näkyy megapikselikameran infrapunavalaistuksen vaikutus tallenteen laatuun verrattuna kuvaan, jossa valaistusta ei käytetä ollenkaan.



Esimerkki

Kuvasta näkyy, kuinka kuva-alassa sijaitseva valonlähde pilaa hämärässä kameran käyttötarkoituksen.

**Näkymäesteet ja katveet**

Varsinkin kauppaliikkeissä on huomioitava erilaisten mainosten ja opaskylttien sijainti kameraan nähden. Aivan liian usein esimerkiksi mainokset peittävät kameran kuva-alaa. Myöskään erilaisten teemapäivien aikaan mainokset eivät saa peittää kameroiden näkyvyyttä.

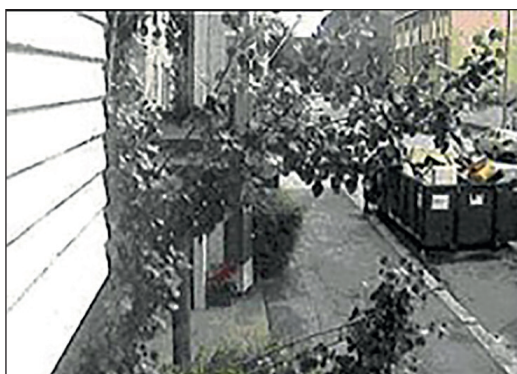
Mahdollisten suurten ajoneuvojen pysäköinti kameroiden eteen on huomioitava suunnittelussa. Toisaalta kameroiden sijoittamista liian ylös pitää välttää, koska tällöin mahdollisista epäilyistä ei saa tunnistuskelpoista kuvaa.

Talvella on otettava huomioon mahdollisten lumikasojen aiheuttamat näkymäesteet. Puut ja pensaat on myös syytä leikata siten, etteivät niiden oksat peitä kameroiden näkyvyyttä.

Sijoittamalla kamerat oikein päästään mahdollisimman pieniin katvealueisiin. Niitä voidaan myös pienentää muuttamalla kameran optiikka tai vaihtamalla kameratyyppiä. Esimerkiksi myymälässä katvealuille voi sijoittaa vähemmän houkuttelevaa tavaraa, jolloin näpistelijät eivät pääse hyötymään katvealueesta.

Esimerkki

Helsingissä sijaitseva pankki ryöstettiin kahdesti samalla tavalla. Ensimmäisellä kerralla kameran edessä olleet oksat vaikeuttivat pakoauton tunnistamista. Viikkoa myöhemmin oksat olivat poissa ja toisen ryöstönyhteydessä käytetty pakoauto tallentui kameraan paremmin. Kummassakin tapauksessa ryöstäjät saatiin kiinni osin valvontakameroiden avulla.



Järjestelmän vakaus

Järjestelmän vakautta voivat uhata esimerkiksi ympäristötekijät, ilkimä tai sähköjakelun häiriöt. Kyseisiin riskeihin on varauduttava riittävällä suojaustasolla.

Kamera itsessään voi olla rakennettu kestävämmän ulkoisia olosuhteita tai se varustetaan erillisellä, käyttötarkoitukseen sopivalla koteloinnilla. Koteloinnin antaman suojauksen taso määritellään IP-luokituksella. IP-koodissa on tunnuksen IP jälkeen kaksi numeroa, joista ensimmäinen tarkoittaa suojausta vierailta esineiltä ja toinen suojausta vedeltä. Esimerkiksi ulkokäyttöön tarkoitettu IP66 tarkoittaa pölytiivistä, voimakkaalta vesisuihkulta suojaavaa kotelo, IP-luokitusta koskee standardi SFS-EN 60529 Sähkölaitteiden kotelointiluokat.

Mekaanista iskunkestävyyttä kuvataan IK-koodilla. Se muodostuu tunnuksesta IK ja numeroista 00–10+. Mitä korkeampi luokitus on, sitä paremmin kamera kestää ilkimä. Yleensä IK10-luokiteltu kameran kotelo on alumiinia tai terästä, ikkuna on polykarbonaattia ja kaapelointi upotettu rakenteisiin. IK-luokat määritellään standardissa SFS-EN 62262 Sähkölaitteiden kotelointien mekaanisen iskunkestävyyden lujuusluokat.

Sähkökatkoon voidaan varautua UPS-varmistuksella siten, että kameroiden sähkönsyöttö, verkko ja tallennus on varmistettu.

Tiettyihin ympäristötekijöihin, kuten sumuun, varautuminen voi olla vaikeaa. Suunnittelussa sumukin voidaan ottaa huomioon luomalla tarpeeksi tiheä valvontaverkosto. Tällöin sumun haittavaikutukset jäävät vähäisiksi.

Kamerakohtainen tarkistus

Kameravalvonnan tarkoituksenmukaisuuden vuoksi on jokaisen kamerasuunnittelun eri vaiheissa pohdittava seuraavia seikkoja:

- kiinteästi suunnattu tai kauko-ohjattava (onko ohjauksen käyttäjiä)
- sijoitus valaisimiin nähden (mahdollinen ledikameroiden käyttö)
- kiinnitys rakenteisiin (pitkä polttoväli, zoom, vaatii huojumatonta rakennetta)
- yksityisyyden suojaus otoksissa (työnteon alue)
- katveiden esto, tilan ja alueen ympäristöllisten muutosten hallinta
- ympäristöolosuhteiden vaatimukset (kotelointiluokitus, käyttölämpötila-alue)
- ilkkivaltariskit (upotettu, vandaalisuojakotelo)
- huoltotoimien työskentely- ja työturvallisuusjärjestelyt sekä niiden kustannukset.

Esimerkki

Vakaa ja huojumaton rakenne on tärkeää. Usein esimerkiksi valaisupylväät huojuvat tuulessa, vaikeuttavat kamerasuunnittelun ja aiheuttavat heilumisellaan ylimääräistä liikettä kuva-alaan.



3.9 VALVOMOIDEN JA KUVIEN KATSELUPISTEIDEN SUUNNITTELU

Suunnitteluvaiheessa on huomioitava kameravalvontajärjestelmän lopullinen käyttötarkoitus erityisen huolellisesti. Jos kameravalvontaa ei käytetä aktiivisesti, valvonnassa käytettävään valvomoon on turha investoida huomattavasti.

Suunnittelussa on huomioitava myös järjestelmän käytön ja ylläpidon vaatimukset. Tällöin on jo heti alkuvaiheessa pohdittava, soveltuuko hankittava järjestelmä esimerkiksi etävalvontaan. Viranomaiset hoitavat valvontatehtäviä ja vastaanottavat hälytystietoja hätäkeskuksiin vain, kun tärkeä yhteinen etu sitä edellyttää.

Aktiivinen valvonta

Aktiivisen kameravalvonnan keskus on valvomo, joka vastaanottaa kamerakuvaa ja muita hälytystietoja. Valvomossa katsellaan valvontakameran kuvia näytöiltä ja ohjaillaan tarvittaessa kameroita. Erilaisten hälytystietojen pohjalta valvomossa tehdään tilannearvioita ja käynnistetään toimenpiteitä vahinkojen torjumiseksi.

Aktiivinen valvonta toteutetaan yleensä

- yrityksen tai yhteisön omasta valvomosta
- yrityksen tai yhteisön keskitetystä valvomosta, johon kuuluu useita kiinteistöjä tai
- kolmannen osapuolen tarjoamana palveluna etävalvontakeskuksesta.

Aktiivisessa valvonnassa kameravalvojien käyttämät kuvaruudut kannattaa tallentaa erikseen tallentimelle. Tällöin tallentimelta on suoraan nähtävissä, mitä kameravalvoja näki ja tarkkaili töissä ollessaan.

Aktiivisen valvomon tai katselupisteen suunnittelussa kannattaa huomioida

- valvontatapa ja aktiivisen valvonnan tarve
- käyttöliittymän kieli ja helppokäyttöisyys
- käyttöliittymän karttapohjaisuus
- kameroiden hallinta- ja ohjausmahdollisuudet
- kameroiden tuottamien hälytysten ilmaisutavat
- näyttöjen ja ulkoisten näyttöjen määrät ja käyttömahdollisuudet
- kameroiden, tallentimien ja matriisien kytkeminen samaan keskuskelloon.

Esimerkki

Kuvassa kameravalvojan käyttämät kolme kuvaruutua tallentuvat suoraan tallentimelle Helsingin Kampin keskuksen valvomossa.

**Puoliaktiivinen valvonta**

Puoliaktiivisessa valvonnassa kameroita seurataan vain hetkittäin esimerkiksi kuva-alassa tapahtuvan liikehälytyksen perusteella. Puoliaktiivinen valvonta voidaan toteuttaa pienissä myymälöissä ja huoltoasemilla sijoittamalla näyttöruutu kassan viereen. Tällöin näyttöruutu myös ennaltaehkäisee tehokkaasti rikoksia.

Passiivinen valvonta

Passiivisessa kameravalvonnassa ei valvomoa tarvita lainkaan. Tällöin suojatussa tilassa olevalta tallentimelta haetaan ainoastaan jälkikäteen informaatiota jonkin asian selvittämiseksi. Tallentimelle voi olla myös etäyhteys, jolloin tallenteita voidaan katsoa lähiverkon tai internetin välityksellä omalta työasemalta.

Valvomoon ja tallenteisiin pääsyn tulee olla rajattua mutta mahdollista. Esimerkiksi loma-aikojen ongelmat eivät saa aiheuttaa sitä, ettei kukaan yrityksestä pääse selailemaan ja luovuttamaan tallenteita. Myös käyttäjien näkymäoikeuksia voidaan rajoittaa tilanteen mukaan.

Varsinainen tallenninlaite on varustettava näytöllä, hiirellä ja näppäimistöllä, mikä helpottaa ja nopeuttaa valvontakamerakuvien lataamista. Joissakin suurissa rikostapauksissa poliisi saattaa ladata tallentimelta useamman vuorokauden materiaalin, eikä etäkäyttöyhteyden nopeus riitä latauksen suorittamiseen.

Etävalvonta

Yritykset ovat usein ulkoistaneet kameravalvonnan kokonaan tai tiettyinä ajankohtina etävalvomaille. Tällöin etävalvomot tekevät esimerkiksi hälytyskuvavalvontaa ja kamerakierroksia. Ne myös tallentavat materiaalia viranomaisille ja varmistavat laitteiden toimivuuden. Palvelut tuotetaan asiakkaiden ja etävalvomoiden välillä internetin kautta suojatulla yhteydellä.

Varsinkin hälytyskuvavalvonta ja kamerakierrokset ovat tehokkaita rikostorjunnan keinoja. Hälytyskuvavalvonnassa etävalvomon ruudulle ponnahtaa kuva valvottavasta kohteesta, jossa järjestelmä on havainnut liikettä poikkeavaan aikaan. Paikka voi olla esimerkiksi lukitun teollisuuskiinteistön piha-alue. Kamerakierroksilla korvataan tai täydennetään muita vartiointipalveluja. Niillä valvoja etävalvomossa tarkastaa tietyin aikavälein kiinteistön kameroiden avulla, että kaikki on kunnossa.

Kameravalvonnalla tapahtuva etävalvonta antaa usein lisäaikaa reagoida tilanteisiin jo silloin, kun tapahtumat ovat vasta aluillaan. Tavallinen hälytysjärjestelmä hälyttää sen sijaan vasta, kun jotain konkreettista tapahtuu, ja reagointiaikakin jää lyhyemmäksi.

Etävalvomoissa pitää toiminnan tehokkuuden varmistamiseksi olla hyvät kamerakartat kohteista. Ne voivat olla paperiversioita tai järjestelmään sisäänrakennettuja karttoja kameralinkkeineen. Mahdollisten hälytysten varalta kiinteistöissä on mentävä käymään. Tällöin on oltava selvää, kuka sinne menee ja kuinka nopeasti.

Esimerkki

Etävalvonnasta ja ulkoistuksesta huolimatta valvontakameroiden materiaalia pitää pystyä purkamaan myös paikalla, jotta poliisi saa tietoa mahdollisimman nopeasti. Kuvan materiaalia ryöstetystä kaupapaliikkeesta siirrettiin suoraan näytölle kaapelia pitkin.



4 TOTEUTUS

4.1 TOTEUTUSSUUNNITTELU

Toteutussuunnittelussa esitetään yksityiskohtainen järjestelmäsuunnitelma, josta selviävät järjestelmältä vaadittavat toiminnalliset ominaisuudet ja tekniset suoritusarvot. Tilaaja ja suunnittelija tarkistavat suunnitelman huolellisesti, koska se toimii myös järjestelmästä jätettävän tarjouskilpailun pohjana. Suunnitteluasiakirjoista tulee selvittää hankittavat laitteet (ohjelmineen) ja kaapeloinnit, tiedonsiirtorat-kaisut, asennukset ja kytkennät sekä konfiguroinnit urakkarajoineen.

Järjestelmien laajennettavuus tulee huomioida ja määritellä asiakirjoissa. Jos vanhaa järjestelmää ollaan laajentamassa, sen rakenne pitää kuvata yksityiskohtaisesti suunnitelmissa. Myös mahdolliset urakkarajat on kuvattava selkeästi.

Hyvästä suunnitelmasta selviävät

- tallentimet ja keskuslaitteet toiminnallisine vähimmäisvaatimuksineen
- kameroiden kaapelointi ja sähkönsyötöt varmistuksineen
- kameroiden tyypit, sijoitukset ja K-menetelmän mukaiset halutut kuva-alat (K5, K 10, K50, K120) ja resoluutiot
- jälleenannot ja ohjaukset sekä niiden toiminta
- tiedonsiirtoyhteydet (ja niiden hankintarajat sekä nopeus- ja kaistavaatimukset)
- valvonta- ja etäkäyttöpaikat, niiden varustelu ja toiminta (käyttöliittymät ja käyttötavat)
- ylläpidon vaatimukset ja järjestelmän joustavuus muutoksissa.

Laadullisena mittarina voi käyttää kameravalvonnan K-menetelmää. Lisäksi suunnittelun apuna suositellaan käytettäväksi Sähkötieto ry:n julkaisemia ohjeita.

4.2 TARJOUSPYYNTÖASIAKIRJAT

Kameravalvontaprojektissa erilaisia tarjouspyyntöasiakirjoja laaditaan projektin laajuuden mukaan useassa eri vaiheessa. Tarjouksia voidaan pyytää esimerkiksi suunnittelijoista ja järjestelmäkokonaisuuksista. Julkisen puolen hankinnoissa on noudatettava lakia julkisista hankinnoista.

Järjestelmästä tehtävän tarjouspyynnön pohjana olevissa suunnitelmissa ja hankinta-asiakirjoissa tulee kuvata mahdollisimman tarkkaan tarjouksen kohde. Pyynnöstä on selvittävä

- yhteyshenkilöt, tarjouksen jättämistapa ja aikataulu
- hankinnan tausta
- järjestelmältä halutut toiminnot, sen laajuus sekä tekniset vaatimukset

- kohteessa tehtävät kaapelointi-, kytkentä- ja asennustyöt
- urakkaohjelma kohteissa, joissa on monta suunnittelijaa ja urakoitsijaa
- urakkarajaliite, joka sisältää eri urakoitsijoiden väliset velvoitteet
- asiakirjaluettelo, joka sisältää luettelon kaikista urakan asiakirjoista
- tarjouslomake, jossa esitetään tarjottavat asiat pääkohdittain
- yksikköhintaluettelo mahdollisia muutostöitä varten
- asemapiirros ja tasopiirustukset
- järjestelmäkaaviot (kunnolliset kaaviot havainnollistavat hyvin järjestelmäkokonaisuutta)
- laite-/massaluettelot (jos on kunnollinen massaluettelo, kaikki tarjoavat oikean määrän laitteita ja tarjouksia voi helpommin vertailla)
- mahdolliset erikoispiirustukset ja yksityiskohtaiset kuvat jakamoista, infotiskeistä, valvomopöydistä jne.
- selvitys ohjelmistojen konfiguroinnista ja laskutuksesta
- laitteiston takuu-aika ja käyttökoulutuksen järjestäminen.

Asiakirjat tulee laatia standardien mukaisilla piirrosmerkeillä ja täydentää merkkien selityksillä. Lisäksi tarjouksessa voi kysyä huolto- ja tukipalveluiden yksikköhintaa.

Urakasta kannattaa pyytää kokonaishinta. Sen on sisällettävä kaikki urakkaan liittyvät kustannukset asennustöistä koulutukseen asti. Laadun varmistamiseksi tarjouskilpailun vertailu- ja valintaperusteena voidaan käyttää pisteytystä. Tällöin esimerkiksi järjestelmän hinnan osuus voi olla 60 %, laadun osuus 25 % ja urakoitsijan kokemuksen ja ammattitaidon osuus 15 % urakasta.

4.3 TARJOUSVERTAILU JA HANKINTAPÄÄTÖS

Toimittajaa ja järjestelmää valittaessa vertaillaan tarjouksien vastaavuuksia hankintasuunnitelmaan. Puolueettoman vertailun tekemiseen tarvitaan riittävää asiantuntemusta. Vertailu on suoritettava sekä taloudellisesta että teknisestä näkökulmasta. Teknisessä vertailussa on huomioitava vaihtoehdot, jotka mahdollisesti täydentävät suunnitelmaa.

Parasta tarjousta valittaessa kannattaa kiinnittää huomiota järjestelmään kokonaisuutena. Myös järjestelmän laajennettavuus on erityisesti huomioitava tarjouksen valinnassa. Halvin hinta ei yleensä takaa parasta laatua ja hyvää toimitus- sekä huoltovarmuutta.

Turva-alan sopimuksia tehtäessä on suositeltavaa käyttää ainoastaan hyväksytyjä järjestelmien toimittajia. Henkilöstö- ja yritysarviointi Seti Oy myöntää vapaaehtoisia turvaurakointi- ja talotekniikkasertifikaatteja (TU- ja TT-sertifikaatteja) turva-alan yrityksille ja asiantuntijoille (lisätietoja www.seti.fi).

Kannattaa sopia, että toimitus katsotaan vastaanotetuksi vasta, kun vastaanottaja on kirjallisesti hyväksynyt laitteen ja tarkastanut sen käyttökunnon.

4.4 ASENNUS JA KÄYTTÖÖNOTTO

4.1.1 Asennus

Asennuksessa huomioidaan alkuperäiseen suunnitelmaan tehdyt lisäykset. Kameran ja muut laitteet säädetään vastaamaan suunniteltua käyttötarkoitustaan. Asennuksen toteutumista on seurattava aktiivisesti. Tarvittaessa on pidettävä työmaakokouksia työn edistymisen mukaan. Kaikki asennuksiin ja toimituksiin liittyvät seikat, joilla on taloudellista merkitystä, suositellaan kirjattavaksi pöytäkirjoihin.

Asennuksen yhteydessä tapahtuvassa konfiguroinnissa säädetään järjestelmän kamerakohtaiset ominaisuudet. Tällöin on huomioitava seuraavat seikat:

- liikkeentunnistuksen käyttö tallentamisessa
- kuva-alan rajaukset
- kuvatahti ja tallennuslaatu
- esiohjelmoinnit häilyyksille ja kamerakierroille.

Liikkeentunnistuksesta tapahtuva taltiointi säästää tallentamisen levytilaa huomattavasti. Usein se myös helpottaa tapahtumien etsimistä, koska pienemmän tallennemäärän ansiosta etsiminen käy nopeasti. Liikkeentunnistuksen käytössä on huomioitava erilaiset häiriölähteet, kuten liikettä peilaavat pinnat.

Rajauksella kameran kuva-alasta rajataan osa pois. Tällöin kamera ei tallenna tapahtumaa, vaikka rajatun kuva-alan kohdalla tapahtuisikin liikettä. Siksi rajauksen vuoksi kameran tallenteista saattaa jäädä jotain oleellista pois. Myös ennen rikosta tapahtuva tiedustelu voi jäädä tallentumatta. Rajauksella säästetään kovalevytilaa. Jos kovalevytilaa on riittävästi, rajauksen voi korvata käyttämällä ohjelmistojen liikehakuominaisuuksia halutun tapahtuman etsimiseen.

Esimerkiksi poliisi saattaa kerätä kuvamateriaalia laajoissa rikostapauksissa useita viikkoja. Tällöin on tärkeää, että tallenteet säilyvät koneella vähintään kuukauden.

Kuvien tallennustiheydessä on huomioitava esimerkiksi se, että ihminen juoksee sekunnissa pitkäkhön matkan. Tällöin esimerkiksi sekunnin välein tallentavaan K120-kameraan ei välttämättä jää mitään materiaalia pakenevasta tekijästä. Siksi on suositeltavaa tallentaa vähintään kolme kuvaa sekunnissa.



4.1.2 Käyttöönotto

Uusi järjestelmä on tarkastettava kamera kerrallaan. Kameran sijoitetaan niin, että saadaan haluttua kuvaa. Tarkistusmenetelmänä voidaan käyttää kameravalvonnan K-menetelmää ja sen testitaulua. Toinen tapa on käyttää standardin SFS-EN 62676-4 Turvasovelluksissa käytettävät kameravalvontajärjestelmät osa 4: Soveltamisohjeet mukaista menetelmää ja testitauluja.

Ennen käyttöönottoa järjestelmän on toimittava moitteettomasti tilaajan ja toimittajan sopiman koe-käyttöjakson ajan. Varsinaisessa luovutuksessa on tarkistettava tai sovittava seuraavista kohdista:

- laitteiden asennuksen visuaalinen tarkastus

Esimerkki

Jos järjestelmän tarkoitus on, että auton rekisterikilvet pystytään lukemaan hämärässä, tallenteen laatu kannattaa testata eri valaistusolosuhteissa.

- kuvalaadun tarkastus K-menetelmän tai standardin mukaisesti
- kuvien ja videoleikkeiden testitallennus
- toiminnallinen koekäyttö tilaajan valvonnassa sopimuksen mukaisen ajan
- käyttäjille järjestettävän koulutuksen ajankohta
- kaikkien järjestelmän laitteiden varmistukset (backup) ja niiden luovutukset
- salasanamenetelmät ja salasanojen luovutukset.

Luovutuksen yhteydessä on tarkistettava myös järjestelmää koskevat dokumentit. Näihin kuuluvat

- laitteiston käyttöohjeet
- järjestelmäkaavio kaikkine laitteineen ja laitesijoituksineen
- kameravalvontakartta
- toteutusta vastaavan kamerasuunnitelman tarkistus
- siirtoyhteyksikaaviot (jos eivät sisälly järjestelmäkaavioon)
- kameravalvontajärjestelmän lokikirja
- kameravalvontajärjestelmän mittaus- ja toteutuspöytäkirjat.

Asennetun järjestelmän tarkastuksessa ja käyttöönotossa voidaan käyttää ST-kortiston lomaketta ST 663.40 Kameravalvontajärjestelmän tarkastuspöytäkirja. Lomaketta on suositeltavaa käyttää yhdessä lomakkeen ST 663.43 Kameravalvontajärjestelmän toteutuspöytäkirja kanssa. Toteutuspöytäkirja soveltuu myös käytettäväksi vastaanottotarkistuksessa.

5 KÄYTTÖ JA YLLÄPITO

5.1 KÄYTTÄJIEN VALINTA JA KOULUTUS

Järjestelmän tilaaja luo laitteistoille asianmukaisen käyttäjäorganisaation ja mahdollisesti etävalvontasopimuksen. Valinnoissa on kiinnitettävä huomiota henkilöiden tarvitsemiin käyttöoikeuksiin ja niiden rajoituksiin.

Käyttäjäorganisaation rakenne voi olla seuraavanlainen:

1. Pääkäyttäjä/järjestelmänvalvoja
 - hallinnoi kaikkien käyttäjien toimintoja
 - luo käyttäjäprofiiileja
 - voi lukea, katsella ja tallentaa tallenteita sekä tapahtumalokeja
 - luo virtuaalisia kamerakarttoja järjestelmään
 - luo hälytystoimintojen kuten pop-up-ikkunoiden asetuksia
 - pystyy tarvittaessa muokkaamaan tallentimien asetuksia.
2. Käyttäjä, voi olla myös etävalvoja
 - näkee kameroiden ja tallentimien kuvia
 - pystyy tarvittaessa ohjaamaan kameroita
 - osaa tallentaa ja luovuttaa materiaalia järjestelmästä viranomaisille.
3. Kehittäjä, on usein järjestelmän toimittaja, jolla on kaikki pääkäyttäjän toiminnot sisältävä käyttäjätunnus
 - tekee ohjelmistopäivitykset
 - lisää ja poistaa laitteita järjestelmästä
 - tekee muita pääkäyttäjän haluamia toimintoja.

Kameravalvonnan käyttöönottovaiheessa koulutetaan kaikki kameravalvonnasta vastaavat henkilöt. Koulutuksessa on korostettava yhteistoimintamenettelyssä luotujen toimintaperiaatteiden noudattamista. Tarvittaessa pääkäyttäjille ja valvomohenkilökunnalle järjestetään erillinen koulutus.

Koulutuksessa kaikkien valvonnan vastuuhenkilöiden on pyrittävä omaksumaan järjestelmän tekninen käyttö. Valitettavan usein yrityksissä vain yksi henkilö osaa käyttää järjestelmää, mikä johtaa ongelmiin esimerkiksi loma-aikoina.

Jos yrityksessä ei ole riittävää määrää koulutettua henkilöstöä, vähäiset rikostapaukset voivat jäädä ratkaisematta tallenteiden puuttumisen vuoksi.



Monissa kiinteistöissä huoltomiehet hoitavat kamerajärjestelmiä, joten heidätkin on koulutettava. Uudet huoltomiehet täytyy myös aina kouluttaa.

Käyttöohjeiden on oltava aina tarvittaessa saatavilla.

5.2 TALLENTEIDEN KÄSITTELY

Tallenteita käytetään lähtökohtaisesti vain niihin tarkoituksiin, joita varten valvontaa on suoritettu. Tallenteiden käsittelyssä on noudatettava tietosuoja-asetuksen periaatteita.

Tallenteet on suojattava siten, että asiaton ja oikeudeton käyttö on estetty. Kun tieto on käsitelty ja säilytetty määritellyn ajan, se pyyhkiytyy automaattisesti kovalevyiltä uuden tiedon myötä.

Mahdolliset ylimääräiset tulosteet ja tallenteet on hävitettävä niiden käytyä tarpeettomiksi. Vanhoja tallentimia hävitettäessä on kovalevyjen tietosisältö tuhottava asianmukaisesti.

Tallenteita ei saa käyttää tai tulostaa sukupuolisiveyttä loukkaavasti.

Mahdollista esitutkinnan tai muun tutkinnan materiaalia saa tarvittaessa säilyttää pidempäänkin tapahtumailmoitusten liitteenä tulevien oikeusvaateiden varmistamiseksi. Tapahtumailmoituksissa on hyvä viitata kuvatallenteen olemassaoloon. Viranomaisille luovutetuista tallenteista ja niiden käyttämisestä vastaa asianomainen viranomainen.

Vartioimistehtävissä havaituista rikoksista ja niissä epäillyiksi tai syylliseksi todetuista henkilöistä ei saa muodostaa omia rekistereitä. Sen sijaan esitutkintaviranomaisille voi sovittuja tietojenvaihtokanavia pitkin lähettää vihjeitä havaituista rikoksista. Tämän jälkeen esitutkintaviranomainen informoi parhaaksi katsomallaan tavalla muita toimijoita rikoksen vaarasta.

Esimerkki

Helsingin keskustan hotellissa havaitaan aamiaistarjoilun yhteydessä epäilyttävää toimintaa. Tietyn mieshenkilön kiinnostus hotellin asiakkaiden käsilaukkuja kohtaan on silmiinpistävä. Hotellin henkilökunnan tiedusteltua asiaa mieheltä tämä poistuu nopeasti hotellista. Vastaanottopäällikkö epäilee miehen olleen sama, joka varasti aiemmin hotellin aamiaispöydästä erään rouvan käsilaukun. Vastaanottopäällikkö päättää lähettää kuvan herrasta Helsingin poliisin vihjetietopalveluun. Poliisi tunnistaa henkilön samaksi aamiaispöytävarkaaksi, joka on kaksi kuukautta ollut epäiltynä varkauksista hotelleissa. Rikosten ennalta ehkäisemiseksi poliisi päättää varoittaa hotelleja vaarasta ja lähettää tutkinnanjohtajan päätöksellä valvontakameran kuvat muille hotelleille.

5.3 TALLENTEIDEN LUOVUTUS JA LUOVUTUSDOKUMENTOINTI

Lähtökohtaisesti valvontakameramateriaalia saa luovuttaa vain järjestelmän tietosuojaselosteen mukaisiin tarkoituksiin. Materiaalia luovutettaessa on noudatettava turvallisia tiedonkäsittely- ja siirtotapoja. Luovutusdokumentoinnin tarkoitus on tukea hyvää tiedonhallintatapaa.

Poliisin tai muun viranomaisen suorittama esitutkinta on yleisin syy materiaalin luovutukseen. Rikostutkinnassa materiaalin luovutus kannattaa toteuttaa esitutkintaviranomaisten, kuten poliisin, kautta.

Jos materiaalia luovutetaan, kannattaa se vastuukysymysten välttämiseksi dokumentoida. Luovutuksen yhteydessä on tarkastettava vastaanottavan virkamiehen virkamerkki. Luovutuksen voi kirjata liitteen 5 mukaiseen dokumenttiin.

Varsinaisten tallenteiden luovutuksessa voi käyttää esimerkiksi USB-muistitikkua. Pienemmät tallenteet tai yksittäiset kuvat voi lähettää myös suoraan sähköpostilla tietoturvallisesti viranomaisen luotettavaan sähköpostiosoitteeseen (esim. @poliisi.fi). Vastaavasti tiedostoja voi siirtää poliisin sähköpostilla lähettämällä linkillä Pouta-pilvipalvelun kautta.

Luovutuksen yhteydessä on varmistuttava siitä, että tallenne aukeaa viranomaisten tietokoneilla. Tämän varmistamiseksi kameravalvontajärjestelmästä on annettava järjestelmän pakkausta tukeva ohjelma tallenteen mukaan.

Esitutkintaa suorittava viranomainen päättää, käytetäänkö sille luovutettua materiaalia esimerkiksi tiedottamisen yhteydessä. Tarvittaessa tallennemateriaalin luovuttaja voi kieltää materiaalilta muun kuin rikostutkintaan liittyvän käytön tekijänoikeuslain (404/1961) 49a §:n perusteella. Tällöin yrityksen henkilökunnalle mahdollisesti kiusallisia kuvia ei voi julkaista ilman lupaa.

HUOM! Viranomaisten yhteydenottoa varten varmistetaan järjestelmästä seuraavat seikat:

- mihin kohteisiin kamerat kuvaavat
- kuinka pitkään kuvat säilyvät keskimäärin tallentimella
- tallentavatko kamerat koko ajan vai liikkeestä
- mihin formaattiin tallenteet saa tallennettua
- kuka osaa tallentaa materiaalin järjestelmästä.

5.4 HYVÄT YLLÄPITOKÄYTÄNNÖT

Hankinnan jälkeen alkaa järjestelmän käyttäminen ja ylläpitäminen. Toiminnot vaativat määräaikaisia tarkastuksia ja ennakkohuoltoja, jotka parantavat järjestelmän toimintavarmuutta.

Takuuaikana järjestelmän ylläpito ja huolto kuuluvat yleensä alkuperäiseen hankintaan. Sen jälkeen vastaavista toimista on hyvä sopia huolto- ja ylläpitosopimuksella. Sen tarkoitus on varmistaa

- järjestelmän käytettävyys ja toipuminen vikatilanteista
- varaosien ja tarvikkeiden saatavuus sekä vaihtopalvelu
- ennakoiva huolto.

Järjestelmän haltijan on ilmoitettava huollolle keskeisistä vioista ja muusta poikkeavasta toiminnasta keskitetysti. Huollon tehtävänä taas on korjata viat sovittujen vasteaikojen puitteissa.

Ennaltaehkäisevällä huollolla vältetään yllättävät katkokset. Huollossa vaihdetaan kuluvia osia ja puhdistetaan laitteista pöly ja lika. Laitteiden puhdistus suositellaan tehtäväksi puolen vuoden välein.

Mahdolliset huolto- ja ylläpitotoimet kirjataan pääpiirteissään kiinteistön huoltokirjaan. Kamerajärjestelmän huollot kirjataan yksityiskohtaisesti järjestelmän lokikirjaan.

Suosittelavaa on, että järjestelmää huoltaa ainoastaan tehtävään koulutettu henkilöstö, jolla on käytössään tarvittavat varaosat ja dokumentit. Toki tavallinen asiaan perehtynyt käyttäjä voi esimerkiksi käynnistää järjestelmän uudelleen, päivittää sen ohjelmiston ja muuttaa järjestelmän asetuksia.

6 DOKUMENTOINTI

6.1 JÄRJESTELMÄN DOKUMENTOINTI

Kameravalvontajärjestelmän toimittaja vastaa järjestelmän dokumentoinnista. Sen tarkoituksena on antaa tarvittava tieto järjestelmän kanssa työskenteleville tahoille, kuten esimerkiksi valvontahenkilö, kiinteistön omistajat, suunnittelijat ja urakoitsijat. Järjestelmän dokumentoinnin sisältö vaihtelee sen mukaan, missä vaiheessa järjestelmän rakentaminen on.

Luonnosvaiheen dokumentointia käytetään yleensä suurien järjestelmien rakentamisessa. Siinä esitetään selkeästi rakennettavan järjestelmän laajuus, valvottavat alueet sekä kameroiden, tallentimien ja katselupisteiden sijoituspaikat.

Urakalaskentavaiheen dokumentointi on huomattavasti luonnosdokumentointia tarkempi. Dokumentoinnissa esitetään yksityiskohtaisesti järjestelmän osat, joiden pohjalta urakka voidaan kilpailuttaa. Dokumentoinnissa on tärkeä kiinnittää huomiota kameroiden, optiikoiden, monitorien ja muiden järjestelmän osien laatuvaatimuksiin.

Toteutusvaihe dokumentoidaan järjestelmän asennusta ja käyttöönottoa varten. Dokumentointi sisältää kaiken järjestelmäkaavioista toimintaselostuksiin asti.

Lopullinen käyttöönoton dokumentointi palvelee kameravalvontajärjestelmän käyttöä, ylläpitoa ja huoltoa. Dokumentoinnin on oltava riittävän tarkka. Siihen on kirjattava kaikki asennetut laitteet, laitteiden sijainnit ja ohjelmistot.

Standardin tai K-menetelmän mukaisessa tarkastuksessa uusi järjestelmä tarkastetaan ja dokumentoidaan kamera kerrallaan. Tarkistuksen ja dokumentoinnin apuna käytetään joko standardin mukaista tai K-menetelmää ja näihin liittyviä testitauluja. Tarkistus suoritetaan ja dokumentoidaan tallentamalla testitaulun kuva tallentimelta. Tallennettua kuvaa verrataan kamerasäädöksiin. Tallennettujen kuvien avulla todistetaan järjestelmän suunnitelmanmukaisuus ja laatu. Saadut tallenteet tai tulosteet arkistoidaan järjestelmän dokumenttien yhteyteen. Tällöin esimerkiksi kamerasäädösten yhteydessä uuden kamerasäädöksen asentaja näkee dokumentista suoraan halutun kuva-alueen. Dokumentoidun järjestelmän jokainen kamera tarkastetaan puolen vuoden välein.

Poliisilaitokset ovat myös kiinnostuneita alueellaan olevista valvontakameroista erilaisten rikosten selvittämiseksi. Ilmoita kamerasi kameravalvontakartastoon, jonka yhteystiedot löydät osoitteesta www.poliisi.fi/kameravalvontakartasto.

ST 13.52 Rakennusten sijainti- ja asennuspiirustuksissa käytettäviä tietoteknisten järjestelmien (T) piirrosmerkkejä

T550 Kameravalvontajärjestelmä

- T550-01 Videovahvistin
- T550-02 Kamera
- T550-03 Kamera, säännestävä koteloit
- T550-04 Kamera, kiinteästi asennettu (katolle/seinälle)
- T550-05 Zoom-kamera
- T550-06 Dome-kamera
- T550-07 Verkkokamera
- T550-08 Analoginen kamera
- T550-09 Kääntöpääkamera
- T550-10 Kääntöpää- ja zoom-kamera
- T550-11 Nauhatalennin (videonauhuri)
- T550-12 Ohjaus- ja käyttölaite
- T550-13 Videokuvatulostin
- T550-14 Monitorin pistorasia
- T550-15 Monitori
- T550-16 Infrapunavalonheitin
- T550-17 Videovaihdin
- T550-18 Videomultiplexeri
- T550-19 Ohjauspaneelin pistorasia
- T550-20 Kytkenärasia
- T550-21 Digitaalinen tallennin
- T550-22 Verkkotallennin
- T550-23 Teholähde
- T550-24 Optinen tai galvaaninen erotin

Suomalainen piirrosmerkki	IEC-piirrosmerkki				
T550-001, Videovahvistin	IEC-piirrosmerkki	T550-005, Zoom-kamera	IEC-piirrosmerkki	T550-009, Kääntöpääkamera	IEC-piirrosmerkki
IEC-piirrosmerkki on johdettu soveltaen piirrosmerkkejä 501239 ja 500060.		IEC-piirrosmerkki on johdettu soveltaen piirrosmerkkejä 501887 ja 500097.		IEC-piirrosmerkki on johdettu soveltaen piirrosmerkkejä 501887 ja 500096.	
T550-002, Kamera	IEC-60617-nro 501887	T550-006, Dome-kamera	IEC-piirrosmerkki	T550-010, Kääntöpää- ja zoom-kamera	IEC-piirrosmerkki
IEC-piirrosmerkki on johdettu soveltaen piirrosmerkkejä 501887 ja 500419.		IEC-piirrosmerkki on johdettu soveltaen piirrosmerkkejä 501887 ja 500419.		IEC-piirrosmerkki on johdettu soveltaen piirrosmerkkejä 501887, 500096 ja 500097.	
T550-003, Kamera, säännestävä koteloit	IEC-piirrosmerkki	T550-007, Verkkokamera	IEC-piirrosmerkki	T550-011, Nauhatalennin (videonauhuri)	IEC-piirrosmerkki
IEC-piirrosmerkki on johdettu soveltaen piirrosmerkkejä 501887 ja 500419.		IEC-piirrosmerkki on johdettu soveltaen piirrosmerkkejä 501887 ja 501898.		IEC-piirrosmerkki on johdettu soveltaen piirrosmerkkejä 501075 ja 501047.	
T550-004, Kamera, kiinteästi asennettu (katolle/seinälle)	IEC-60617-nro 501887	T550-008, Analoginen kamera	IEC-piirrosmerkki	T550-012, Ohjaus- ja käyttölaite	IEC-piirrosmerkki
		Ei tiedossa			
IEC-piirrosmerkkissä asennustapa esitetään soveltamisohjeen A00266 kirjainkoodilla: T = katto, S = seinäpinta.		IEC-piirrosmerkki on johdettu soveltaen piirrosmerkkejä 501887 ja 500216.		IEC:n ja ISO:n piirrosmerkki-standardissa ei ole vastaavaa käsitettä kuvaavaa piirrosmerkkiä.	

Kuva 19. Kameravalvontajärjestelmän piirrosmerkkejä.

Verkkopohjaisessa valvonnassa kaikkien laitteiden IP-osoitteet on dokumentoitava käyttäjätunnuksineen ja salasanoineen. Mahdollisia oletussalasanoja ei saa käyttää.

Käyttöönoton jälkeen dokumentteja on ylläpidettävä niiden käyttökelpoisuuden varmistamiseksi. Esi-merkiksi kaikki huoltotoimet, laitteistojen vaihdot ja ohjelmistopäivitykset on kirjattava rutiininomaisesti järjestelmän lokikirjaan.

Kaiken dokumentaation on oltava sen tasoista, että järjestelmän huolto ja ylläpito onnistuu kolmannelta osapuolelta.

Kaikkia kameravalvonnan dokumentteja on säilytettävä siten, etteivät ne vahingossa joudu asiattomiin käsiin.

Dokumentoinnissa voi hyödyntää muun muassa seuraavaa ST-aineistoa:

- ST 664.30 Kameravalvontajärjestelmät. Asennusohje
- ST 98.57 Kameravalvontajärjestelmät. Käyttö, ylläpito ja huolto
- ST 663.43 Kameravalvontajärjestelmän toteutuspöytäkirja
- ST 663.40 Kameravalvontajärjestelmän tarkastuspöytäkirja
- ST 664.40 Kameravalvontajärjestelmän kaapeloinnin tarkastus- ja mittauspöytäkirja.

6.2 TIETOSUOJASELOSTE

Tallennettu kuva tai ääni rinnastetaan tietosuoja-asetuksessa henkilötietoon. Jos henkilö on suoraan tai epäsuorasti tunnistettavissa tallenteista, niistä syntyy tietosuoja-asetuksen mukainen henkilörekisteri.

Rekisterinpitäjän on laadittava henkilörekisteristä tietosuojaseloste, josta on ilmentävä rekisterinpitäjän nimi ja yhteystiedot, kameravalvonnan perustiedot ja vastuuhenkilöt, henkilötietojen käsittelyn tarkoitus ja se, mihin tietoja toistuvasti luovutetaan. Sen tulee olla jokaisen saatavilla. Kameravalvontaa toteutettaessa on myös otettava huomioon säännökset tietojen suojaamis- ja hävittämisvelvollisuudesta.

Tietosuojaselosteen tekemiseen voi käyttää liitteessä 2 olevaa lomaketta ST 664.01 Tallentavan kameravalvonnan tietosuojaseloste.

Tietosuoja-asetus ei koske kameravalvontaa silloin, kun luonnollinen henkilö suorittaa valvontaa yksinomaan henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiinsa. Näin ollen esimerkiksi omakotitalon kameravalvonnasta ei tarvitse tehdä tietosuojaselostetta, jos valvonta ulottuu vain talon omistaja hallinnoimille alueille.

7 TIETOTURVA

Tietoturvan näkökulmasta kameravalvonta on erittäin kriittinen kokonaisuus, ja järjestelmän sabotointi mahdollistaa rikoksien tekemisen normaalia pienemmällä kiinnijäämisriskillä. Nykyiset IP-pohjaiset järjestelmät saattavat mahdollistaa tunkeutujalle pääsyn kamerajärjestelmän verkkoon, jos IP-kamera on sijoitettu julkisiin tiloihin tai kiinteistön ulkopuolelle niin, että verkon kaapelointi tai liitännät ovat näkyvissä. Jos verkkoa ei ole kunnolla suojattu, tunkeutujalle saattaa avautua reitti myös kiinteistön muihin järjestelmiin.

Kameroiden lisäksi tallenninlaitteet ja niiden ohjelmistot ovat haavoittuvia. Kuvamateriaalin tai verkossa olevien henkilötietojen paljastumisen lisäksi järjestelmän resurssit saattavat joutua tietomurron yhteydessä hakkereiden käyttöön osaksi suurempaa verkkohyökkäystä, jossa käytetään hyväksi sekä IP-kameroiden että tallentimien laskentatehoa.

7.1 Suunnittelu ja hankinta

Kameravalvontajärjestelmien tietoturvariskit voivat toteutuessaan aiheuttaa ongelmia sekä itse järjestelmien toiminnalle että myös muulle toiminnalle kiinteistössä. Kun halutaan suojautua mahdollisilta tietoturvaloukkauksilta ja minimoida riskit joutua sellaisten kohteeksi, suunnitelmallisuus ja ennakointi ovat ensiarvoisessa asemassa. Siksi tietoturva vaatimusten huomioiminen jo järjestelmien suunnittelu- ja hankintavaiheessa on tärkeää, jotta voidaan varmistaa järjestelmien luotettava toiminta koko niiden elinkaaren ajan.

7.1.1 Kustannukset ja päivitettävyys

Tietoturvan vaatimuksilla saattaa olla myös merkittäviä kustannusvaikutuksia. Mitä paremmin tietoturvallisuuden osa-alueet on kuvattu suunnitelmissa ja urakkalaskenta-asiakirjoissa, sitä vähemmän vastuuasioissa tulee epäselvyyksiä. Suunnitelmat ja asiakirjat siis ovat avainasemassa tietoturvallisuuden kannalta.

On myös tärkeää tehdä yhteistyötä sellaisten kumppaneiden kanssa, jotka tarjoavat tukea ja ohjeistusta tietoturvasta huolehtimiseen. Projektiin osallistuvat tahot tulee edellyttää tarjoamaan tietoa siitä, miten lisätä järjestelmien tietoturvasoa ja ylläpitää sitä. Tietoturva tulee käydä läpi yhdessä projektin eri osapuolten kanssa ja varmistaa, että keskeiset tietoturva-asiat on asianmukaisesti huomioitu ja vastuut jaettu oikein.

7.1.2 Käyttötapausten vaatimukset järjestelmälle

Suunnitteluvaiheessa tulee kiinnittää erityistä huomiota siihen, millaisia vaatimuksia järjestelmän eri käyttötapaukset ja loppukäyttäjät asettavat järjestelmän toimivuudelle. Näin varmistutaan siitä, että suunniteltu järjestelmä palvelee tarkoitustaan mahdollisimman hyvin. Käyttötapauksissa erityistä huomiota tulee kiinnittää käytetyn tiedonsiirtoverkon suojaukseen sekä etäkäytön ja mahdollisten pilvipalveluiden tietoturvaan. Järjestelmän fyysinen suojaus tulee suunnitella siten, että järjestelmien kriittiset osat sijoitetaan lukittuihin ja, jos mahdollista, kulunvalvottuihin laite- ja teletiloihin.

Käyttötapaukset asettavat myös vaatimuksia laite- ja järjestelmätoimittajille sekä esimerkiksi analytiikkaohjelmistojen toimittajille. Näiden tulisi olla hyvämaineisia, seurata alan parhaita käytäntöjä ja olla toiminnassaan avoimia ja läpinäkyviä. Jos tietoturva-aukkoja havaitaan missä tahansa järjestelmän osassa, niiden tulee olla nopeasti paikattavissa ohjelmistopäivityksillä tai korjaustiedostoilla sekä yksittäisissä laitteissa että koko järjestelmässä.

7.1.3 Luottamuksellisten tietojen dokumentointi

Kameravalvontaprojekteissa käsitellään runsaasti luottamuksellista tietoa jo suunnitteluvaiheessa. Siksi on tärkeää sopia, miten tietoturva-asiat dokumentoidaan. Projektiin osallistujien tulee sitoutua noudattamaan määriteltyä tietoturvaohjeistusta. Sitoutuminen varmistetaan tarvittaessa kirjallisella sopimuksella.

Laissa yksityisistä turvapalveluista (LYTP, 1085/2015) salassapitovelvollisuudesta säädetään lain 67 §:ssä. Projektiin osallistujan tulee huolehtia myös tehtävien päätyttyä siitä, että kaikki toimeksiannon dokumentit, tallenteet sekä materiaali palautetaan tilaajalle tai tuhotaan. Salassapitovelvollisuus säilyy myös tehtävien päätyttyä.

7.2 TOTEUTUS

Järjestelmien toteutusvaiheessa tulee varmistua siitä, että työt tehdään suunnitelmassa esitettyjen tietoturvanäkökohtien mukaisesti ja noudatetaan sovittuja tietoturvakäytäntöjä. Koko alihankintaketjussa on varmistuttava, että kaikki projektiin osallistuvat henkilöt ovat tietoisia tietoturvakäytännöistä ja toteutustavat ovat näiden käytäntöjen mukaiset.

Keskeisiä käytännön asioita kameravalvontajärjestelmän toteutusvaiheen tietoturvan hallinnassa ovat mobiililaitteiden ja kannettavien tietokoneiden käsittely ja niiden suojauskäytännöt sekä työmaan turvallisuusjärjestelyt, kuten kulunhallinta- ja muut valvontaratkaisut. Luottamuksellisiksi luokiteltuja projektiasiakirjoja ei saa käsitellä valvomatta työmaalla tai sen ulkopuolella, ja sähköpostitse lähetettävät luottamukselliset tiedot tulee lähettää salattuina. Salassapitovelvollisuus (LYTP 1085/2015, 67 §) on velvoittava pykälä, joka turvasuojaustehtäviä tekevien yritysten ja henkilöiden on huomioitava toiminnassaan.

Asennusvaiheessa on tärkeää varmistua siitä, että asennukset tehdään suunnitelmien mukaisesti sekä noudattaen järjestelmä- ja laitevalmistajan ohjeita järjestelmän arkkitehtuurista ja asennuksesta. Usein toteutuksen aikana joudutaan tekemään väliaikaisia ratkaisuja, kuten väliaikaisia verkkoja tai etäyhteyksiä, jotta projekti olisi tehokkaasti toteutettavissa. Kaikista väliaikaisista projektin aikaisista ratkaisuista tulee sopia käytännöt ennen projektin aloitusta. Samalla pitää sopia, miten ratkaisut dokumentoidaan. Ennen tilaajalle luovutusta tulee kaikki väliaikaiset ratkaisut purkaa. Laitteisiin tai järjestelmiin vielä jääneet väliaikaiset käyttöoikeudet täytyy viimeistään tässä vaiheessa purkaa ja vaihtaa mahdolliset oletussalasanat.



Kuva 20. Väärin tehty asennus: kameraverkkoon on suora pääsy esiin jätetyn verkkorasian kautta.

Järjestelmän luovutuksen yhteydessä tilaajalle on suositeltavaa luovuttaa dokumentti kaikista järjestelmän ja laitteiden tunnuksista ja salasanoista sekä ohjeistaa niiden päivitykseen. Dokumentti on arkaluontoinen ja sen tallennuksessa ja lähetyksessä on noudatettava äärimmäistä varovaisuutta. Luovutusvaiheessa on myös sovittava tilaajan kanssa, säilyvätkö toteuttajan käyttöoikeudet järjestelmään esimerkiksi korjaustöiden, muiden takuuaikaisten velvoitteiden tai ylläpidon takia.

7.3 KÄYTTÖ JA YLLÄPITO

Käyttäjän toiminta aiheuttaa tietoturvalle suurimman yksittäisen riskin. Siksi toiminnalle ja käytännöille tulee olla sovitut ohjeistukset, joiden avulla tietoturvan huomioiminen ja mahdollisten ongelmien korjaaminen on järjestelmällistä.

7.3.1 Salasanakäytännöt ja käyttöoikeudet

Käytönopastuksessa annetaan perehdytys järjestelmän oikeanlaiseen käyttöön, ja siihen on syytä sisällyttää myös oleelliset tietoturva-asiat, kuten käyttäjätunnusten ja salasanojen hallinta. Salasanakäytännöt tulee ohjeistaa, ja niissä tulee opastaa käyttämään vahvoja salasanaja: vaaditaan esimerkiksi tietty määrä tietyn tyyppisiä merkkejä sekä salasanan vaihtaminen tietyin väliajoin. Kaikki laitteet ja järjestelmät, joissa kirjautumiseen tarvitaan salasana, tulee määrittää käyttämään käyttäjä- tai sijaintikohtaisia salasanaja. Järjestelmätason salasanaja tai oletussalasanoja ei tule sallia.

Koska järjestelmien käyttöoikeuksiin tulee usein muutoksia, järjestelmillä on hyvä olla omasta organisaatiosta koulutuksen saanut pääkäyttäjä, joka voi antaa käyttöoikeuksia tai poistaa niitä. Käyttöoikeuksien hallinta on myös syytä olla ohjeistettu ja ohjeistuksessa määriteltä, millä perusteella oikeuksia annetaan tai ollaan antamatta. Määräajoin tulee myös varmistaa, että tunnukset on poistettu henkilöiltä, jotka eivät enää työskentele organisaatiossa. Tarvittaessa pääkäyttäjälle annetaan perehdytys myös ohjelmisto- ja tietoturvapäivitysten hallinta- ja päivityskäytännöistä.

7.3.2 Etäkäyttö

Etäkäytössä ennalta määritellyt henkilöt pystyvät hallitsemaan järjestelmää paikasta riippumatta tyypillisesti internetiä tai muuta verkkoyhteyttä hyödyntäen, mikä helpottaa ja nopeuttaa mahdollisiin ongelmiin ja muutostarpeisiin reagointia. Suunniteltaessa järjestelmän ylläpitoa tulee päättää, sallitaanko järjestelmän etäkäyttö ja jos sallitaan, mitkä ovat sallitut tekniikat ja miten varmistetaan pääsy etäkäyttöön vain niille henkilöille, joilla on siihen valtuutus.

Pilvipohjaiset valvomopalvelut ovat yksi tapa järjestää etäkäyttö. Niitä käytetään useimmiten verkkoselaimella tai erillisellä tietokoneella tai mobiililaitteella asennettavalla ohjelmalla. Ne toimivat usein

julkisessa internetissä, jolloin on syytä vaatia ja varmistua tietoliikenteen salauksesta. Myös hyvän käyttäjätunnuksen ja vahvan salasanan merkitys edelleen korostuu. Pilvipalveluita käytettäessä moni vastuu tietoturvassa on käyttäjän sijaan pilvipalvelun toimittajalla. Palveluita hankittaessa kannattaa varmistua, että palveluntarjoajalla on edellytykset toteuttaa lupaamansa palvelutaso ja että sen tietoturvan käytännöt on dokumentoitu sekä säännöllisesti päivitettyinä.

Koska järjestelmän toiminta pilvipalveluita käytettäessä voi olla ainakin osittain riippuvainen verkkoyhteyksistä, tulee huomioida järjestelmän toiminta silloin, kun verkkoyhteys ei ole saatavilla. Järjestelmien toiminnan jatkuvuuden varmistamiseksi varmuuskopiointilla mahdollistetaan järjestelmän palautus poikkeustilanteissa. Näitä voivat olla esimerkiksi laiterikot, tahattomat käyttäjien virheet tai tahalliset tietoturvaloukkaukset tai muut vahingonteot. Useimmissa järjestelmissä on mahdollista tehdä varmuuskopiointi automaattisesti ja ajastetusti esimerkiksi laitteen omalle muistille tai muistikortille. Myös varmuuskopioiden sijainti tulee suunnitella: säilytyksessä on huomioitava, että varmuuskopio sisältää yleensä järjestelmästä paljon tietoa, joka vääriin käsiin joutuessaan voi aiheuttaa vahinkoa.

7.3.3 Ohjelmistopäivitykset

Verkkoon liitettävät laitteet ja järjestelmät täytyy pitää ajan tasalla ohjelmistopäivityksillä, jotta tietoturva ja toiminta pysyvät hyväksyttävällä tasolla. Järjestelmien ja laitteiden päivitysten tulee olla osa järjestelmän jatkuvaa ylläpitoa, ja on suunniteltava etukäteen, kuka tekee päivitykset ja milloin. Ennalta on myös hyvä selvittää päivitysten kustannukset, joihin voivat vaikuttaa esimerkiksi mahdolliset lisenssikulut ja se, voidaanko työ tehdä etänä vai vaatiiko se paikan päällä käyntiä.

Päivitysprosessilta tulee vaatia helppokäyttöisyyttä, ja laite- sekä järjestelmätoimittajat usein tarjoavatkin päivityksiä helpottavia työkaluja. Jotta viestintä tietoturvapäivityksistä tai mahdollisista haavoittuvuuksista olisi mahdollisimman avointa, monet valmistajat tarjoavat ilmoituspalvelua. Loppukäyttäjät voivat rekisteröityä palveluun saadakseen suoraan valmistajalta tietoja havaituista haavoittuvuuksista.

7.3.4 Ylläpito

Kameravalvontajärjestelmän ja kameroiden toiminta tulee tarkastaa säännöllisesti. Poikkeuksista kameroiden toiminnassa on useissa järjestelmissä mahdollista saada myös hälytys esimerkiksi kotelon avaamisesta, kameran kuva-alan peittämisestä tai kameran irrottamisesta verkosta.

Kaikilla järjestelmillä ja niiden laitteilla on elinkaari, jonka aikana niitä toimitetaan ja ylläpidetään. Elinkaarisuunnittelussa on tärkeää ottaa huomioon myös tietoturva ja varmistettava muun muassa laitteiden saatavuus ja teknisen tuen säilyminen. Elinkaaren hallinnassa on otettava huomioon kaikki järjestelmän kannalta olennaiset osat mukaan lukien ohjelmistot ja käyttöjärjestelmät.

Laitevalmistajat tarjoavat usein laiteohjelmistoille pitkäaikaista tukea varten toimintoja, jolla varmistetaan, että tuotteita ylläpidetään ja tuetaan virheiden ja haavoittuvuuksien korjaamiseen keskittyvillä laitteistopäivityksillä ja -korjauksilla. IT-maailmassa näitä kutsutaan LTS-ohjelmistopäivityksiksi (Long Term Support), ja näitä käytäntöjä on tuotu myös kameravalvontajärjestelmiin. Mikäli mahdollista, laitevalmistajalta tulee edellyttää tällaisten ohjelmistojen saatavuutta, jotta ohjelmisto- ja tietoturvapäivitykset ovat turvattuja koko laitteiden elinkaaren ajan.

Laitevalmistajilla on yleisesti tarjolla ohjelmistopohjaisia työkaluja myös muun muassa seuraavien tehtävien hallintaan:

- käyttäjien ja salasanojen hallinta
- laitesalasanan määrittäminen monelle laitteelle yhdellä kertaa
- HTTPS-varmenteiden käyttöönotto
- 802.1x-varmenteiden käyttöönotto
- varmenteiden uusinta ja hallinta
- määritysten kopioiminen laitteesta toiseen
- laiteohjelmiston päivittäminen
- kameroiden päivittäminen, kun saatavilla on LTS-laiteohjelmisto.

8 LAINSÄÄDÄNTÖ JA SÄÄNTELYN TAUSTA

8.1 SALAKATSELU JA -KUUNTELU

Säädökset salakatselusta ja -kuuntelusta ovat rikoslain (531/2000) 24 luvussa, jossa säädetään yksityisyyden, rauhan ja kunnian loukkaamisesta. Kameravalvonnalla voidaan syyllistyä lähinnä salakatseluun ja -kuunteluun sekä yksityiselämää loukkaavan tiedon levittämiseen, mutta salakatselua- ja kuuntelua pohdittaessa on huomioitava myös koti- ja julkisrauhan lainsäädäntö. Lisäksi kameravalvontaa sivuaa rikoslain 38 luvun 9 §:n (1051/2018) tietosuojarikos, jota käsitellään myöhemmin tietosuoja-asetuksen yhteydessä. Myös rikoslain 47 luvun (217/2018) 1 §:n työturvallisuusrikos voi tulla sovellettavaksi kameravalvonnassa.

Salakuunteluun syyllistyy rikoslain 24 luvun 5 §:n mukaan henkilö, joka oikeudettomasti teknisellä laitteella kuuntelee tai tallentaa keskustelua, puhetta tai yksityiselämästä kuuluvaa muuta ääntä kotirauhan suojaamassa paikassa tai puhetta muussa paikassa, jossa ei ole syytä olettaa ulkopuolisen kuulevan puhetta.

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

Salakatselussa- ja kuuntelussa rangaistavaa on erityisesti katseleminen, kuvaaminen ja kuunteleminen teknisellä laitteella. Teknisillä laitteilla tarkoitetaan yleensä kiikareita, kameroita, videokameroita tai näihin rinnastettavia laitteita, matkapuhelimia ja mikrofoneja. Ollakseen rangaistavaa katselun ja kuuntelun on tapahduttava oikeudettomasti ja samalla tarkkailtavan yksityisyyttä loukaten. Rangaistavaa ei tietenkään ole lain suojaamassa paikassa oikeudettomasti oleskelevan tunkeilijan tarkkailu. Kuka tahansa voi tarkkailla salaisellakin valvontakameralla esimerkiksi omakotitaloonsa tunkeutunutta. Oikeudetonta tarkkailu ei ole silloinkaan, kun siihen on saatu tarkkailtavan suostumus.

Sen seikan tallentaminen, mikä olisi muutoinkin omin silmin nähtävissä tai kuultavissa, ei oikeuta katseluun tai kuvaamiseen suojatulla alueella. Normaalina ja avointa kameravalvontaa, jossa tarkkailtavat joutuvat valvonnan kohteeksi vain ohimennen siihen varautuen, ei yleensä pidetä yksityisyyttä loukkaavana. Tosin tiettyjen henkilöiden pitkäaikainen tarkkailu esimerkiksi työpaikalla voi olla yksityisyyttä loukkaavaa ja siten rangaistavaa salakatselua.

Salakatselusäännöksessä on selkeästi erotettavissa kotirauhan suojaamat paikat ja muut tilat, kuten yleisöltä suljetut julkisrauhan suojaamat rakennukset ja tilat. Vaikka laissa mainitaan erityisesti käymälät ja pukeutumistilat, muita vastaavia paikkoja ovat esimerkiksi suihkuhuoneet ja saunat. Tällaisissa paikoissa

käyvä luonnollisesti olettaa olevansa turvassa ulkopuolisten katseilta tai ainakin kuvaamiselta, koska paikoissa harrastetaan intiimejä yksityisyyteen kuuluvia toimia.

Salakatselun ja oikeudettoman kameravalvonnan kohteena voi olla vain joku ihminen. Pelkän tilan, eläinten, esineiden, rakennusten tai muun ympäristön katseleminen tai kuvaaminen ei ole salakatseluna rangaistavaa.

Kuvaaminen voi olla valokuvaamisen kaltaista, tietyn hetken kuvaamista tai luonteeltaan jatkuvaa videokameralla kuvaamista. Kuvaamista voi olla kaikkien sellaisten tekniikoiden käyttäminen, joilla informaatiota tallennetaan tai siirretään tallennettavaksi niin, että se voidaan myöhemmin saattaa kuvan muotoon. Kameran sijainnilla tai tarkkailun suorittamispaikalla ei ole merkitystä. Säännöksen mukaan rangaistavaan tekoon syyllistyy kameraa käyttävä henkilö eli kameravalvonnan käyttäjä.

Salakatselun ja -kuuntelun valmistelu on säädetty rikoslain 24 luvun 7 §:ssä rangaistavaksi. Valmisteluna rangaistaisiin erilaisten teknisten laitteiden sijoittaminen salakatselussa tai -kuuntelussa käytettäväksi, jos laitteet olisivat paikoillaan käyttövalmiina.

Esimerkki

Jos järjestelmän tarkoitus on, että auton rekisterikilvet pystytään lukemaan hämärässä, tallenteen laatu kannattaa testata eri valaistusolosuhteissa.



8.2 YKSITYISELÄMÄÄ LOUKKAAVA TIEDON LEVITTÄMINEN

Rikoslain 24 luvun 8 §:ssä säädetään yksityiselämää loukkaavasta tiedon levittämisestä. Siinä loukkaavan tiedon levittämiseen syyllistyy se, ”joka oikeudettomasti – joukkotiedotusvälinettä käyttämällä tai muuten toimittamalla lukuisten ihmisten saataville – esittää toisen yksityiselämästä tiedon, vihjauksen tai kuvan siten, että teko on omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa. . .”. Huomioitavaa on, ettei yksityiselämää loukkaavan tiedon levittämisenä pidetä vastaavien tietojen levittämistä julkisuuden henkilöstä, jos esittäminen on tarpeen yhteiskunnallisesti merkittävän asian käsittelemiseksi tai henkilön toiminnan arvioimiseksi mainitussa tehtävässä.

Valvontakameroita käytettäessä yksityiselämää loukkaavan tiedon levittämiseen voi syyllistyä lähinnä levittämällä salakatselulla tuotettuja kuvia tai videoita. Levittäminen voi tapahtua esimerkiksi internetin yhteisöpalveluiden kautta tai reaaliaikaisen katselumahdollisuuden tuottamisena ja jakamisena. Huomioitavaa on, että tunnusmerkistön täyttääkseen materiaalin pitää sisältää tietoa yksityiselämästä. Tietyissä tapauksissa rikoslain kunnianloukkaus voi myös tulla kysymykseen.

Yksilöiden on hyväksyttävä julkisilla paikoilla erilainen tarkkailu kuin kotonaan. Avointa kameravalvontaa, jonka kohteeksi henkilöt joutuvat satunnaisesti julkisilla paikoilla, ei pidetä yksityisyyttä loukkaavana.

8.3 TIETOSUOJA

EU:n yleinen tietosuoja-asetus (2016/679) eli GDPR (General Data Protection Regulation) tuli sovellettavaksi kevästä 2018 alkaen. Sitä täydentävä kansallinen tietosuoja laki (1050/2018) tuli voimaan vuoden 2019 alusta ja samalla vanha henkilötietolaki kumoutui. Lisäksi Euroopan tietosuojaneuvosto (EDPB) on julkaissut ohjeen tietosuoja-asetuksen soveltamisesta kameravalvontaan. Ohjeen tavoitteena on varmistaa tietosuoja-asetuksen yhdenmukainen soveltaminen, ja se sisältää myös useita esimerkkejä kameravalvonnan toteuttamisesta tietosuoja säännösten mukaisesti. Ohje on ladattavissa tietosuoja-valtuutetun toimiston kotisivuilta osoitteesta <https://tietosuoja.fi/euroopan-tietosuojaneuvoston-ohjeet>.

Lähes kaikki kameravalvontajärjestelmät keräävät tai tallentavat tietoja, ja näin ollen ne kuuluvat tietosuoja-asetuksen piiriin. Tallennettu kuva tai ääni on henkilötieto, jos siitä on henkilö tunnistettavissa suoraan tai epäsuorasti. Tallennetuista kuvista syntyy henkilörekisteri, eikä tallenteiden säilytysajalla ole vaikutusta tietosuoja-asetuksen sovellettavuuteen. Ratkaisevaa on vain se, tallentuuko tietoa ylipäättänsä. Jos tietoa ei tallennu, tietosuoja-asetus ei tule sovellettavaksi.

Kameravalvonnan edellytyksenä on, että sen tulee olla henkilötietoa käsittelevän toiminnan kannalta asiallisesti perusteltua. Kameravalvonnan ohjeessa edellytetään valvonnan ilmoittamista, koska ihmisten tulee tietää kameravalvonnasta voidakseen varautua siihen. Ilmoituksesta on käytävä ilmi tarvittaessa

myös valvonnan tarkoitus ja sen suorittaja. Säännös perustuu siihen, että rekisterinpitäjällä on velvollisuus ilmoittaa rekisteröitävälle häntä koskevien tietojen keräämisestä. Ilmoituksesta olisi syytä näkyä myös, tallentaako kameravalvontajärjestelmä.

Tietosuojaselosteen on oltava tarkkailtavien saatavilla. Siitä tulee ilmetä kameravalvonnan perustiedot ja vastuuhenkilöt. Kameravalvontaa toteutettaessa on myös otettava huomioon säännökset tietojen suojaamis- ja hävittämisvelvollisuudesta.

Muun muassa seuraavat henkilötietojen käsittelyä sisältävät toimet edellyttävät tietosuoja-asetuksen noudattamista: tiedon kerääminen, tallentaminen, käyttö, luovuttaminen, siirto, säilyttäminen ja hävittäminen. Kameravalvonnan kautta tapahtuva henkilötietojen käsittely ei edellytä ilmoituksen tekoa tietosuojaviranomaisille.

Rikoslain 38 luvun 9 §:ssä säädetään tietosuojarikoksesta, johon voi syyllistyä käsittelemällä tietosuoja-asetuksen, tietosuojalain, henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain tai henkilötietojen käsittelyä koskevan muun lain vastaisesti henkilötietoja. Rangaistavaa on esimerkiksi henkilötietojen käsittely tahallaan tai törkeästä huolimattomuudesta ilman henkilötietojen käyttötarkoitussidonnaisuutta. Tällöin vaaditaan kuitenkin, että teko loukkaa rekisteröidyn henkilön yksityisyyden suojaa tai aiheuttaa hänelle olennaista haittaa tai muuta vahinkoa.

Valvontakameroita käytettäessä rangaistavaa voi olla lähinnä se, ettei ole laadittu tietosuojaselostetta, kameravalvonnasta on jätetty ilmoittamatta tai tietoja on käsitelty virheellisesti. Rikkomuksen täyttymiseen vaaditaan kuitenkin, että teko vaarantaa rekisteröidyn yksityisyyden suojaa tai hänen oikeuksiaan. Näin ollen kovin vähäiset ja merkityksettömät laiminlyönnit eivät helposti johda rangaistusseuraamuksiin.

8.4 TIETOTURVA

EU:n verkko- ja tietoturvadirektiivissä (ns. NIS-direktiivi, 2016/1148) säädetään yhteiskunnan kriittisen infrastruktuurin tarjoajien ja toimijoiden tietoturvalvelvollisuuksista sekä tietoturvahäiriöistä ilmoittamisesta. Suomessa velvoitteet säädetään eri sektoreiden (energia, terveydenhuolto, finanssiala, finanssialan infrastruktuuri, liikenne, vesihuolto, digi-infrastruktuuri ja digitaaliset palvelut) omassa lainsäädännössä, ja niitä valvovat sektoreiden omat valvontaviranomaiset.

Huoltovarmuuskriittisten toimijoiden on huolehdittava palvelujensa ja infrastruktuurinsa tietoturvas- ta sekä raportoitava havaitsemansa tietoturvauhat ja -loukkaukset toimialan valvontaviranomaiselle. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus koordinoi kansallista ja kansainvälistä yhteistyötä, kerää tilannekuvaa ja toimii raportijana EU:n suuntaan.

8.5 YKSITYISYYDEN SUOJA TYÖELÄMÄSSÄ

Laki yksityisyyden suojasta työelämässä (759/2004) ja siihen liittyvät yhteistoimintalain säännökset säätelevät kameravalvonnan käyttöä työpaikoilla ja virastoissa. Lainsäädännön taustalla on tarve parantaa työntekijöiden yksityisyyden suojaa ja samalla täydentää muuta lainsäädäntöä, jonka ei katsota vastaavan riittävän tarkasti työpaikoilla ilmeneviin yksityisyyden suojan ongelmiin.

Lain mukaan työnantaja saa harjoittaa kameravalvontaa käytössään olevissa tiloissa:

- työntekijöiden ja muiden tiloissa oleskelevien henkilökohtaisen turvallisuuden varmistamiseksi
- omaisuuden suojaamiseksi
- tuotantoprosessien asianmukaisen toiminnan valvomiseksi
- turvallisuutta, omaisuutta tai tuotantoprosessia vaarantavien tilanteiden ennaltaehkäisemiseksi tai selvittämiseksi.

Kameravalvontaa ei kuitenkaan saa käyttää:

- tietyn työntekijän tai tiettyjen työntekijöiden tarkkailuun työpaikalla
- käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa tai muissa henkilöstötiloissa
- työntekijöiden henkilökohtaiseen käyttöön osoitetussa työhuoneessa.

Työnantaja voi kuitenkin kohdentaa kameravalvonnan tiettyyn työpisteeseen, jossa työntekijöitä työskentelee, jos tarkkailu on välttämätöntä:

- työntekijän työhön liittyvän ilmeisen väkivallan uhkan tai hänen turvallisuudelleen tai terveydelleen ilmeisen haitan tai vaaran ehkäisemiseksi
- omaisuuteen kohdistuvien rikosten estämiseksi ja selvittämiseksi, jos työntekijän tehtävän olennaisena osana on käsitellä arvoltaan tai laadultaan merkittävää omaisuutta, kuten rahaa, arvopapereita tai arvoesineitä
- työntekijän etujen ja oikeuksien varmistamiseksi, jos kameravalvonta perustuu tarkkailun kohteeksi tulevan työntekijän pyyntöön ja asiasta on sovittu työnantajan ja työntekijän välillä.

Kameravalvonnan on oltava mahdollisimman avointa ja työnantajan on kameravalvontaa suunnitellessaan ja toteuttaessaan pidettävä huolta seuraavasta:

- Ennen kameravalvonnan käyttöönottamista selvitetään työntekijöiden yksityisyyteen vähemmän puuttuvien muiden keinojen käyttömahdollisuudet.
- Työntekijän yksityisyyteen ei puututa enempää kuin on välttämätöntä toimenpiteiden tarkoituksen saavuttamiseksi.
- Valvonnalla saatujen henkilötallenteiden käsittelyyn sovelletaan tietosuoja-asetuksen periaatteita.
- Tallenteita käytetään vain niihin tarkoituksiin, joita varten tarkkailua on suoritettu.
- Työntekijöille tiedotetaan yhteistoiminta- tai kuulemismenettelyn jälkeen kameravalvonnan alka-

misesta, toteuttamisesta ja siitä, miten ja missä tilanteissa tallenteita käytetään, sekä kameroiden sijainnista, jos ne on kohdennettu työpisteisiin, joissa työskentelee työntekijöitä.

- Kameravalvonnasta ja sen toteuttamistavasta ilmoitetaan näkyvällä tavalla niissä tiloissa, joihin kamerat on sijoitettu.

Työnantajalla on kuitenkin edellisestä huolimatta oikeus käyttää tallenteita:

- työsuhteen päättämisen perusteen toteennäyttämiseksi
- naisten ja miesten välisestä tasa-arvosta annetussa laissa tarkoitetun häirinnän tai ahdistelun, yhdenvertaisuuslaissa (1325/2014) tarkoitetun häirinnän taikka työturvallisuuslaissa tarkoitetun häirinnän ja epäasiallisen käytöksen selvittämiseksi ja toteennäyttämiseksi, jos työnantajalla on perusteltu syy epäillä työntekijän syylistyneen häirintään, ahdisteluun tai epäasialliseen käytökseen
- työtapaturman tai muun työturvallisuuslaissa tarkoitettua vaaraa tai uhkaa aiheuttaneen tilanteen selvittämiseksi.

Kameravalvonnalla saadut tallenteet on pääsääntöisesti hävitettävä heti, kun ne eivät ole tarpeen valvonnan tarkoituksen toteuttamiseksi ja viimeistään vuoden kuluessa. Tallenteen saa kuitenkin säilyttää tämän määräajan jälkeen, jos se on tarpeen viimeksi mainitussa luettelossa tarkoitetun asian käsittelyn loppuun saattamiseksi tai jos työnantaja tarvitsee tallennetta työsuhteen päättämisen asianmukaisuuden toteennäyttämiseksi.

Yksityisyyden suojasta työelämässä annetun lain 7 luvun 24 §:n rangaistussäännöksen mukaan kameravalvonnan toteuttamisen tai avoimuuden säännöksiin rikkomisesta voidaan tuomita sakkorangaistus. Rankaiseminen edellyttää kuitenkin tahallisuutta tai törkeää huolimattomuutta. Lisäksi kameravalvonnan kohdalla rikoslaissa oleva salakatselusäännös voi tulla sovellettavaksi.

8.6 YHTEISTOIMINTA YRITYKSISSÄ

Laki yhteistoiminnasta yrityksissä eli yhteistoimintalaki (334/2007) velvoittaa työnantajan käsittelemään yhteistoimintamenettelyissä työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin tapahtuvan valvonnan. Menettelyssä on käytävä läpi valvonnan tarkoitus, käyttöönotto ja niissä käytettävät menetelmät.

Yhteistoimintalakia sovelletaan teknisin menetelmin toteutettavassa valvonnassa tietyin poikkeuksin yrityksissä, joissa työskentelee säännöllisesti vähintään 30 ihmistä. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi.

Esimerkki

Työpaikalla vallitsevan avoimuuden lisäämiseksi työnantaja voi myöntää esimerkiksi työsuojeluvaltuutetulle tallenteiden tarkastusoikeuden. Tällöin työntekijät voivat tarvittaessa valtuutetun kautta tarkastaa, ettei heidän työntekoaan seurata asiaan kuulumattomilla tavoilla.

8.7 TYÖTURVALLISUUS

Työturvallisuuslain (738/2002) 5 luvun 27 §:n mukaan ”työssä johon liittyy ilmeinen väkivallan uhka työ ja työolosuhteet on järjestettävä siten, että väkivallan uhka ja väkivaltatilanteet ehkäistään mahdollisuuksien mukaan ennakolta”. Lain mukaan työpaikalla on oltava väkivallan uhan ja konkreettisen väkivallan torjumiseen soveltuvat turvallisuusjärjestelyt ja laitteet sekä mahdollisuus avun hälyttämiseen. Tarvittaessa työnantajan on myös tarkistettava erilaisten turvallisuuslaitteiden toimivuus.

Valvontakameroilla välitettävä reaaliaikainen kuva on usein yksi työturvallisuuskeino esimerkiksi poliisilaitoksissa, vankiloissa, ravintoloissa ja terveydenhoitoalan kohteissa. Myös hallituksen esityksessä eduskunnalle työturvallisuuslaiksi mainitaan yhtenä mahdollisena turvajärjestelynä kameravalvonta. Käytännössä kameravalvonta kuuluu kiinteästi työturvallisuuteen ainakin silloin, kun kameran tuottaman kuvan perusteella tehdään ratkaisu jonkin tilan turvallisuudesta. Näin voi olla esimerkiksi silloin, kun johonkin tilaan mennään kameran tuottaman informaation perusteella.

Työturvallisuuslain vastaisista laiminlyönneistä voidaan rangaista joko työturvallisuuslain 8 luvun 63 §:n työturvallisuusrikkomuksena tai rikoslain 47 luvun 1 §:n mukaan työturvallisuusrikoksena. Rikoslain mukaisesti työturvallisuusrikoksesta voidaan tuomita työnantaja tai sen edustaja, joka tahallaan tai huolimattomuudesta jättää noudattamatta työturvallisuusmääräyksiä ja työsuojelun edellytyksiä työpaikalla.

Näin ollen työpaikan turvajärjestelyissä keskeisessä asemassa olevan kamerajärjestelmän huollon laiminlyöminen voisi joissakin tapauksissa olla rangaistavaa. Työturvallisuusrikoksesta voidaan tuomita sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

8.8 YKSITYISET TURVALLISUUSPALVELUT

Laki yksityisistä turvallisuuspalveluista (LYTP, 1085/2015) kohdistuu vartioimisliiketoimintaan, järjestyksenvalvojatoimintaan ja turvasuojaustoimintaan. Laissa oleva vaatimus turvallisuusalan elinkeinoluvasta koskee vartioimisliiketoimintaa, osaa järjestyksenvalvojatoimintaa ja turvasuojaustoiminnan osalta hy-

väksymistä edellyttäviä turvasuojaustehtäviä. Näitä ovat ansiotarkoituksessa suoritettavat sähköisten ja mekaanisten lukitusjärjestelmien, murtohälytysjärjestelmien ja kulunvalvontajärjestelmien asentaminen, korjaaminen tai muuttamista niihin kuuluvaa kaapelointityötä lukuun ottamatta. Sen sijaan hyväksymistä edellyttäviä turvasuojaustehtäviä eivät ole esimerkiksi edellä mainittujen järjestelmien tai kameravalvontajärjestelmien pelkät suunnittelu- ja konsultointityöt tai kameravalvontajärjestelmien asennustyöt silloin, kun kameravalvontajärjestelmää ei integroida kulunvalvonta-, murtoilmaisu- tai lukitusjärjestelmään.

Hyväksymistä edellyttäviä turvasuojaustehtäviä käsittävää turvasuojaustoimintaa saavat harjoittaa yritykset, joilla on tähän oikeuttava turvallisuusalan elinkeinolupa ja palveluksessaan vastaava hoitaja, joka vastaa yrityksen toiminnan lainmukaisuudesta. Kyseisiä tehtäviä suorittavalla henkilöllä tulee olla mukanaan voimassa oleva hyväksyminen turvasuojaajaksi eli turvasuojaajakortti, joka on esitettävä pyydettyäessä.

Turvallisuusalan elinkeinoluvat ja hyväksynnät vastaavaksi hoitajaksi myöntää Poliisihallituksen Turvallisuusalan valvontayksikkö. Turvaajasuojakorttia sen sijaan haetaan poliisilaitokselta, joka suorittaa suppean turvallisuusselvityksen hakijasta. Ammatilliseen pätevyyyteen selvityksessä ei oteta kantaa.

Valvontakameroiden tyypillisiä käyttäjiä ovat vartiointiliikkeet. Vartiointiliikkeen ja toimeksiantajan välille on laadittava aina kirjallinen toimeksiantosopimus, jossa on otettava huomioon yksityisistä turvallisuuspalveluista annetun asetuksen (874/2016) 17 §:n sisältö. Sopimuksessa on määriteltävä muun muassa toimeksiannon vartioimistehtävät, vartioimisalue ja vartioimiskohteet. Kameravalvontalaitteita saa käyttää vain niihin toimeksiantosopimuksen mukaisiin tarkoituksiin, joihin ne on hankittu. Tallenteiden katsominen ja tulkitseminen rikoksenpaljastustehtävänä muuten kuin poliisin pyynnöstä vaatii vartioimisliiketoimintaan oikeuttavan elinkeinoluvan ja vartijakortin.

Teknisiä apuvälineitä käytettäessä korostuvat tarkoitussidonnaisuus- ja objektiivisuusperiaate. Välineitä ei saa käyttää työtehtävien kannalta perusteettomaan seurailuun tai kenenkään yksityisyyttä loukkaavaan tallentamiseen. Teknistä tarkkailua saa ohjeen mukaan kohdistaa epäiltyyn henkilöön vain, kun hän on vartioimiskohteessa yleisellä paikalla. Tällöin on voitava olettaa, että henkilö käyttäytymisen tai muun syyn perusteella myötävaikuttaa tai syyllistyy rikoksiin. Tarkkailun peruste ei saa olla syrjivä tai loukkaava. Sen ajallista kestoja ei ole tarkasti määritelty, mutta sen on lopetettava välittömästi, jos perusteita toiminnalle ei ole.

Lisäksi LYTP kieltää vartioimisliike- tai turvasuojaustoiminnan harjoittajaa ilmaisemasta tai käyttämästä hyödyksi sitä, mitä tämä on saanut tietää toimeksiantajan salassa pidettävistä turvallisuusjärjestelyistä tai yksityisyyteen kuuluvista seikoista.

Koska kameravalvonta on nykyisin keskeinen osa yritysten turvallisuusjärjestelmiä, voi salassapitorikokseen syyllistyä ilmaisemalla järjestelmästä sellaisia tietoja, joita joku voi käyttää hyödyksi esimerkiksi rikosta suunnitellessaan. Tällaiset tiedot voivat olla esimerkiksi käyttäjätunnuksia tai IP-osoitteita, joiden avulla rikollinen voi tunkeutua kameravalvontajärjestelmään ja helpottaa esimerkiksi pankkiin suunniteltua ryöstöä.

8.9 LUETTELO KAMERAVALVONTAAN LIITTYVÄSTÄ LAINSÄÄDÄNNÖSTÄ

Laki	Luku, pykälä ja momentti
Rikoslaki (531/2000)	24 luku, 38 L 1–2 ja 9 § ja 47 L 1 §.
EU:n tietosuoja-asetus (2016/679)	Kokonaisuudessaan.
Tietosuojalaki (1050/2018)	6–7 §.
EU:n verkko- ja tietoturvadirektiivi (2016/1148)	Kokonaisuudessaan.
Laki yksityisyyden suojasta työelämässä (759/2004)	4 §, 16–17 §, 21§ ja 24 §.
Laki yhteistoiminnasta yrityksistä (334/2007)	19 §.
Työturvallisuuslaki (738/2002)	27 § ja 63 §.
Laki yksityisistä turvallisuuspalveluista (1085/2015)	6 §, 9 §, 34 §, 73 §, 102 § ja 104 §.

9 ESIMERKKEJÄ KAMERAVALVONTAJÄRJESTELMIEN KÄYTTÖKOHTEISTA

9.1 HUOLTOASEMAN KAMERAVALVONTA

Tarveselvitys

Huoltoaseman kameravalvonnan tärkein tarkoitus on tunnistaa polttonesteitä varastavat henkilöt ja heidän ajoneuvonsa. Lisäksi kameravalvonnan tarkoitus on estää aseman sisätiloissa varkauksia ja muita häiriöitä. Kameravalvonta myös lisää työntekijöiden turvallisuuden tunnetta.

Vaihtoehtoiset turvallisuuskeinot

Vaihtoehtoisena turvallisuuskeinona on myydä polttonesteitä ainoastaan kortti- tai seteliautomaatilta. Keinoa ei ole otettu laajamittaisesti käyttöön, koska se vaikuttaa asiakaskäyntien määriin huoltoaseman myymälässä.

Myymälävarkauksia voidaan havaita myös peilien avulla. Myymälävarkauksiin voidaan lisäksi vaikuttaa sijoittamalla varkauksille alttiita tuotteita valvonnan kannalta helpompiin paikkoihin.

Suunnittelu

Itsepalvelutankkaajista ja heidän ajoneuvojensa rekisterikilvistä on saatava tunnistuskelpoista kuvaa varkauksien varalta.

Huoltoaseman sisäänkäynneistä sekä maksu- ja rahankäsittelypisteistä yksilöintikuvaa (K120) ja muista tiloista tunnistuskelpoista kuvaa (K50). Sisäänkäynnissä on huomioitava tunnistuskuvaa tallentavan kamerasen-
nuskorkeus riittävän matalalle.

Työntekijöiden kanssa sovitaan yt-neuvotteluissa, että heidän työpisteensä käyttämä kassaa voi valvoa.



Kameravalvonnasta olemassa oleva tietosuojaseloste päivitetään. Rekisterinpitäjänä toimii esimerkiksi huoltoaseman yrittäjä tai myymäläpäällikkö.

Toteutus

Tallentavasta kameravalvonnasta ilmoitetaan tankkausalueella ja ulko-ovella kyltillä "Kiinteistössä tallentava kameravalvonta".

Huoltoaseman yrittäjä tai myymäläpäällikkö toimii järjestelmän pääkäyttäjänä. Hän vastaa myös talenteiden käsittelystä ja niiden toimittamisesta viranomaisille tarvittaessa.

Järjestelmän toimittaneen yrityksen kanssa laaditaan käyttö- ja ylläpito- sekä tietojenkäsittelysopimus (DPA), joihin kuuluvat järjestelmän ennakoinva huolto- ja puolivuotistarkastukset.

Yrittäjä tai myymäläpäällikkö vastaa itse kameroiden linssien tarkistuksista ja puhdistuksista huoltokäyntien välillä.

Kameravalvonnan tehokkuutta voidaan parantaa sijoittamalla kamera oikealle korkeudelle kiinteisiin rakenteisiin sisä- ja uloskäyntien lähetyville. Tällöin lippalakkeja ja kalastajahattuja käyttävät henkilöt ovat helpommin tunnistettavissa. Kamera voidaan sijoittaa esimerkiksi oven karmin sisään tai kuvassa olevan putken kaltaisiin rakenteisiin. Optimaalinen korkeus on 160 cm.



Kameran oikea kuvakulma helpottaa rikollisten kiinnisaamista poliisin kasvojentunnistukseen käyttämällä KASTU-järjestelmällä.

9.2 HOTELLIN TAI MAJOITUSLIIKKEEN KAMERAVALVONTA

Tarveselvitys

Hotellin tai majoitusliikkeen kameravalvonnan tarkoituksena on suojata vastaanoton henkilökuntaa sekä auttaa vahingontekojen ja aamiaispöytien käsilaukkuvarkauksien tai muiden varkauksien selvittämisessä. Kameravalvonnan tarkoituksena on myös estää häiriökäyttäytymistä ja lisätä turvallisuuden tunnetta öisin työskenteleville.

Vaihtoehtoiset turvallisuuskeinot

Vaihtoehtoisena turvallisuuskeinona toimii hotellivieraiden valistus ja tiedottaminen. Keinoa ei kuitenkaan välttämättä käytetä leimautumisen pelossa. Hyvä, avoin ja aktiivinen asiakaspalvelu on toimiva menetelmä vähentämään häiriökäyttäytymistä.

Vastaanoton suunnittelun apuvälineenä kannattaa käyttää Sähköinfo Oy:n julkaisua ST-ohjeisto 13 Palvelutyö-
pisteen turvasuojauksen suunnittelu, toteutus ja ylläpito.

Suunnittelu

Hotellin kaikille oville asennetaan kamera kuvaamaan yksilöintikuvaa (K120) sisääntulijoista. Lisäksi pääovelle asennetaan kamera kuvamaan yksilöintikuvaa (K120) myös ulosmenijöistä.

Leveän vastaanottotiskin taakse asennetaan kamera tai kamerat yksilöintikuvan saamiseksi (K120). Asennuksen yhteydessä huomioidaan vastaanottotiskin valaistuksen riittävyys.

Ravintolan sisäänkäynnille asennetaan kamera yksilöintikuvan (K120) saamiseksi. Ravintolasaliin asennetaan K50-kamera varkaustapahtumien havaitsemiseksi.

Eri kerroksien hissiauloihin asennetaan K50-kamerat. Myös



pitkille ja avoimille käytäville voidaan asentaa kullekin oma kameransa.

Matkalaukkujen säilytyshuoneeseen asennetaan K50-kamera.

Hotellin ulkopuolelle asennetaan liikuteltava kupukamera. Kameralla voidaan valvoa muun muassa taksien saapuminen.

Työntekijöiden kanssa käydään yt-neuvottelut. Niissä sovitaan, että heidän työpisteensä käyttämää vastaanottopistettä voidaan valvoa.

Kameravalvonnasta laaditaan tietosuojaseloste.

Toteutus

Kameravalvonnasta ilmoitetaan ulko-ovilla kylteillä ”Kiinteistössä tallentava kameravalvonta”.

Majoitusliikkeen esimiehet, kuten esimerkiksi vuoropäälliköt, koulutetaan järjestelmän käyttäjiksi. Hotellin tai majoitusliikkeen johtaja vastaa tallenteiden käsittelystä ja niiden toimittamisesta viranomaisille tarvittaessa. Tehtävän hän voi delegoida esimerkiksi vuoropäälliköille, mutta vastaa kuitenkin itse toiminnan lainmukaisuudesta.

Majoitusliike tekee järjestelmän toimittaneen yrityksen kanssa käyttö-, ylläpito- ja tietojenkäsittelysopimuksen (DPA), joihin kuuluvat järjestelmän ennakoiva huolto- ja puolivuotistarkastukset.

9.3 KERROSTALON KAMERAVALVONTA

Tarveselvitys

Kerrostalon kameravalvonnan tarkoituksena on ehkäistä tai auttaa selvittämään kellari- ja vinttikomeromurtoja sekä asuntomurtoja ja muita vahingontekoja.

Vaihtoehtoiset turvallisuuskeinot

Vaihtoehtoisina turvallisuuskeinoina on parantaa rakenteellista murtosuojausta tai avainten hallintaa, valistaa asukkaita tai asentaa huoneistokohtaisia murtoilmaisu-järjestelmiä.



Suunnittelu

Kerrostalon rappukäytävään asennetaan yksilöintikuvaa (K120) kuvaava kamera. Kellarin ja vintin sisäänkäynneille (sisäpuolelle) asennetaan myös vastaavat kamerat, jotka koteloidaan suojaan ilkeivallalta.

Kuvien säilyttämisajaksi määritellään neljä kuukautta, koska usein kellarin ja vinttikomeroihin kohdistuneet murrot selviävät asianomistajalle vasta viikkojen tai kuukausien kuluttua teosta.

Suunnittelun yhteydessä taloyhtiön hallituksessa tai yhtiökokouksessa hankitaan lupa kotirauhan piiriin kuuluvan rappukäytävän valvonnalle. Lisäksi kamera-valvonnasta tehdään tietosuojaseloste, joka asetetaan nähtäville taloyhtiön käyttämälle ilmoitustaululle.



Toteutus

Kameravalvonnasta ilmoitetaan ulko-ovilla kylteillä "Kiinteistössä tallentava kameravalvonta".

Taloyhtiön hallituksen puheenjohtaja ja varapuheenjohtaja koulutetaan järjestelmän pääkäyttäjiksi. Lisäksi tarvittava määrä muita taloyhtiön hallituksen jäseniä koulutetaan järjestelmän käyttäjiksi. Puheenjohtaja vastaa tallenteiden käsittelystä ja niiden toimittamisesta viranomaisille tarvittaessa. Tehdävän hän voi delegoida esimerkiksi muille hallituksen jäsenille, mutta vastaa kuitenkin itse toiminnan lainmukaisuudesta.

Taloyhtiö solmii järjestelmän toimittaneen yrityksen kanssa käyttö-, ylläpito- ja tietojenkäsittelysopimuksen (DPA), johon kuuluvat järjestelmän ennakkoiva huolto- ja puolivuotistarkastukset.

9.4 AJOPORTIN KAMERAVALVONTA

Tarveselvitys

Tehtaan tai logistiikkakeskuksen portin kameravalvonnan tarkoituksena on yksilöidä alueelle saapuvat ja poistuvat henkilöt sekä ajoneuvot. Yksilöinti estää ja selvittää tehdasalueella ilmeneviä ongelmia. Kameroilla suoritetaan myös alueen yleisvalvontaa. Kameravalvonta lisää turvallisuuden tunnetta valvomossa työskenteleville.

Vaihtoehtoiset turvallisuuskeinot

Vaihtoehtoisia täydentäviä turvallisuuskeinoja ovat alueen aitaaminen, hyvä valaistus ja murtoilmaisujärjestelmä, johon on liitetty aluevalvontaan soveltuvia ilmaisimia sekä piirivartiointi.

Suunnittelu

Portille asennetaan ajoneuvojen rekisterikilpien yksilöimiseksi kamerat (K50) sekä tulo- että menosuuntaan. Lisäksi valvomon sisälle asennetaan kamerat (K120), jotta siellä vierailevat henkilöt voidaan yksilöidä.

Aitalinjaa ja piha-aluetta varten asennetaan tapahtumien havaitsemista varten kamerat (K10–K50). Kamerat ovat kupukameroita, joita voidaan liikutella ja zoomata valvomosta. Näin piha-aluetta on tarpeen tullen helppompi tarkkailla.

Työntekijöiden kanssa sovitaan yt-neuvotteluissa, että heidän työpisteensä käyttämänsä valvomoa saa valvoa kameroilla.

Valvonnasta tehdään tietosuojaseloste, ja rekisterinpidosta vastaa turvallisuudesta vastaava henkilö.

Toteutus

Kameravalvonnasta ilmoitetaan alueen reunalla ja valvomon ovella kylteillä ”Alueella tallentava kameravalvonta”. Turvallisuusvastaava toimii järjestelmän pääkäyttäjänä. Hän vastaa myös tallenteiden käsittelystä ja niiden toimittamisesta viranomaisille.

Valvomon työntekijät toimivat järjestelmän käyttäjinä, ja heillä on tallenteiden katselu- ja tallennusoikeus.

Vartiointiliike huolehtii järjestelmän ennakoivista huolto- ja puolivuotistarkastuksista.

Valvomon työntekijät vastaavat itse kameroiden linssien tarkistuksista ja puhdistuksista.

Kaaviokuva ajoporttialueen kameravalvonnasta on **LIITTEESSÄ 4.**



9.5 KAUPPALIIKKEEN KAMERAVALVONTA

Tarveselvitys

Kauppaliikkeen kameravalvonnan tarkoituksena on estää rikoksia ja häiriökäyttäytymistä sekä auttaa rikoksesta epäiltyjen tunnistamisessa. Kameravalvonta tuo myös lisäturvaa liikkeessä työskenteleville henkilöille.

Vaihtoehtoiset turvallisuuskeinot

Vaihtoehtoisina turvallisuuskeinoina toimivat valvontapeilit, tuotesuojajärjestelmä, murtoilmaisujärjestelmä, kulunvalvontajärjestelmä, tekniset rahaturvallisuusjärjestelmät, aktiivinen asiakaspalvelu, vartiointipalvelut ja arvokuljetuspalvelut. Myymälävarkauksiin voidaan vaikuttaa myös sijoittamalla varkauksille alttiit tuotteet helpommin valvottavaksi.

Kameravalvontajärjestelmä on tärkeä turvallisuustekijä edellä lueteltujen lisäksi, eivätkä muut järjestelmät kykene korvaamaan kameravalvonnan tuomaa hyötyä.

Suunnittelu

On tärkeää saada sekä kauppaliikkeeseen saapuvista että sieltä poistuvista henkilöistä yksilöivää (K120) kuvaa. Lisäksi kaikista maksu- ja rahankäsittelypisteistä, muilta ovilta sekä tavarantoimituksesta on saatava yksilöivää (K120) kuvaa.

Muista tiloista, kuten juomahyllyjen läheltä, on saatava tunnistettavaa (K50) kuvaa.

Työntekijöiden kanssa yt-neuvotteluissa sovitaan, että heidän työpisteensä käyttämiään kassoja voi valvoa.

Kauppaliikkeen yrittäjä tai myymäläpäällikkö laatii kameravalvonnan tietosuojaselosteen ja toimii rekisterinpitäjänä.



Toteutus

Kameravalvonnasta ilmoitetaan kauppaliikkeen ovella kyltillä ”Kiinteistössä tallentava kameravalvonta”.

Kauppaliikkeen yrittäjä tai myymäläpäällikkö on järjestelmän pääkäyttäjänä. Hän vastaa myös tallenteiden käsittelystä ja niiden toimittamisesta tarvittaessa viranomaisille. Tehtävän hän voi delegoida, mutta vastaa kuitenkin itse toiminnan lainmukaisuudesta.

Yrittäjä tai myymäläpäällikkö solmii myös järjestelmän toimittaneen yrityksen kanssa käyttö-, ylläpito- ja tietojenkäsittelysopimuksen (DPA), joihin kuuluvat järjestelmän ennakoiva huolto- ja puolivuotistarkastukset.

Kauppaliike vastaa itse kameroiden linssien tarkistuksista ja puhdistuksista huoltokäyntien välillä mahdollisuuksiensa mukaan.

Kaaviokuva kauppaliikkeen kameravalvonnasta on **LIITTEESSÄ 3.**

9.6 KAUPUNKIEN KAMERAVALVONTA

Kaupungit ja kunnat voivat yritysten tavoin valvoa kameroilla omistamiaan kiinteistöjä ja muita alueita.

Kaupunkien erilaisten työpaikkojen valvonnassa on noudatettava lakia yksityisyyden suojasta työelämässä.

Kaupunkien julkisten alueiden, kuten puistojen ja torien, valvonta on järkevää suorittaa yhteistyössä poliisin kanssa. Jako voi olla esimerkiksi seuraavanlainen: kaupunki kustantaa poliisille valvontaan tarvittavan laitteiston, jota poliisi käyttää ja hallinnoi.

Poliisi suorittaa teknistä valvontaa poliisilain (872/2011) 4 luvun 1 §:n mukaisesti ”yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, rikosten ennalta estämiseksi, rikoksesta epäillyn tunnistamiseksi sekä erityisten valvontakohteiden vartioimiseksi”.



Tarveselvitys

Kameravalvonnan tarkoitus on lisätä kansalaisten turvallisuutta levottomiksi koetuissa paikoissa. Sen tarkoitus on myös ennalta estää ja selvittää ilkeiden tekoja ja muita rikoksia yleisillä paikoilla.

Kaupungin kameravalvonnan tarpeita koottaessa kannattaa turvallisuussuunnittelun apuna käyttää paikallisia toimijoita. Poliisin ja muiden toimijoiden yhteistyön avulla kartoitetaan ne alueet, joissa valvontaa tarvitaan eniten.

Hyvää tietoa suunnittelun pohjaksi saa aiemmista kaupungin turvallisuussuunnitelmista. Lisäksi hyviä tietolähteitä ovat poliisin tietojärjestelmät, lähipoliisit, nuorisotyöntekijät ja kaupungin eri palveluyksiköiden johtajat.

Tarveselvityksen yhteydessä voidaan samalla kartoittaa jo olemassa olevat järjestelmät ja mahdollisuus hyödyntää niitä uudessa järjestelmässä. Tällöin voidaan esimerkiksi pohtia, voidaanko kaupungin ylläpitämää tietoverkkoa hyödyntää kameravalvonnassa.

Tarvittaessa neuvotellaan myös eri kiinteistöjen omistajien kanssa kameroiden kiinnitysmahdollisuuksista.

Vaihtoehtoiset turvallisuuskeinot

Vaihtoehtoisia turvallisuuskeinoja ovat nuorten valistaminen, valaistuksen lisääminen sekä kaupunkikuvan avartaminen.

Tietyt paikat voidaan myös jättää kokonaan valvomatta, jos valvonnan ei katsota olevan siellä taroituksenmukaista.

Suunnittelu

Tarveselvityksessä selvinneiden kipupisteiden jälkeen aloitetaan yksityiskohtaisempi suunnittelu. Kaupungin kameravalvonnassa on tarkoituksenmukaista käyttää liikuteltavia ja zoomattavia kameroita.

Kukin kamera on sijoitettava siten, että sillä voidaan hallinnoida mahdollisimman suurta aluetta. Tällaisia paikkoja ovat esimerkiksi risteysalueet ja laajat torialueet.



Kaupungin kameravalvontajärjestelmä on suositeltavaa toteuttaa tietoverkkopohjaisesti. Tällöin järjestelmä on dynaaminen ja helposti muunneltavissa. Verkon tietosuojaan on myös kiinnitettävä huomiota.

Järjestelmän käytöstä ja hallinnoinnista vastaa ensisijaisesti poliisi. Sen sijaan tietoverkon ja järjestelmän ylläpidosta voi vastata asianomainen kaupunki.

Jos valvontaa suoritetaan kaupungin työntekijöiden työpaikkojen yhteydestä, valvonnasta käydään yt-neuvottelut.

Toteutus

Julkisille paikoille asennettavien kameroiden asetukset säädetään niin, ettei kameroilla voi nähdä ihmisten kotirauhan suojaamiin paikkoihin.

Kameravalvonnasta ilmoitetaan valvottavilla alueilla kylteillä "Alueella poliisin tallentava tekninen valvonta".

Kameravalvonnan rekisterinpitäjänä toimii Poliisihallitus, tai tarvittaessa kunta ja Poliisihallitus voivat toimia yhteisrekisterinpitäjinä rikosasioiden tietosuojalain 16 §:n mukaisesti.

Kaupunki solmii myös järjestelmän toimittaneen yrityksen kanssa käyttö- ja ylläpitosopimuksen, johon kuuluvat järjestelmän huolto- ja puolivuotistarkastukset.

Kaupungin tekninen osasto vastaa kameroiden linssien tarkistuksista ja puhdistuksista kolmen kuukauden välein.

Kameravalvontaan kohdistuvia ennakkoluuloja voidaan tarvittaessa vähentää järjestämällä kaupungissa kameravalvontaan liittyviä avoimet ovet -päiviä. Tällöin ihmisille voidaan antaa mahdollisuus tutustua kameravalvontajärjestelmiin ja niiden kanssa työskenteleviin ihmisiin.

10 TERMIT JA KÄSITTEET

CMOS-kenno

Megapikselikameroissa käytettävä kuvakenno.

Dome-kamera

Kuvun alle sijoitettu kamera, kupukamera.

DPA (Data Processing Agreement)

Tietojenkäsittelysopimus.

Drooni (drone)

Miehittämätön, kauko-ohjattava ilma-alus. Kameralla varustettuja drooneja käytetään mm. kamera-valvontaan.

Edge-analytiikka

Tekniikka, jossa sijoitetaan tietoverkon datan keruu, analyysi, prosessointi ja käsittely tuodaan mahdollisimman lähelle päätelaitetta ja käyttötilannetta.

EDPB (European Data Protection Board)

Euroopan tietosuojaneuvosto.

EMP-kamera

Elektromagneettiselta pulssilta suojattu kamera.

Enkooderi

Muuntaa analogisen kuvasignaalin IP-verkon yli siirrettäväksi digitaaliseksi bittivirraksi.

Ethernet

Datapakettipohjainen tietoverkkoratkaisu.

EX-kamera

Räjähdysvaarallisen tilan kamera.

GDPR (General Data Protection Regulation)

EU:n yleinen tietosuoja-asetus.

Hahmontunnistus

Tekniikka, jossa erotetaan datasta merkityksellisiä kokonaisuuksia.

IK-luokitus

Mekaanista iskunkestävyyttä kuvataan IK-luokituksella. IK-koodissa tunnuksen IK jälkeen ovat numerot 00–10+. Mitä suurempi numero, sitä paremmin kamera kestää ilkivaltaa.

IP-kamera

Verkkokamera, tietoverkkoa kuvansiirrossa käyttävä kamera.

IP-luokitus

Koteloinnin antaman suojauksen taso ulkoisia uhkia, kuten pölyä ja vettä vastaan, määritellään IP-luokituksella. IP-koodissa on tunnuksen IP jälkeen kaksi numeroa, joista ensimmäinen tarkoittaa suojausta vierailta esineiltä ja toinen suojausta vedeltä. Mitä suurempi numero, sitä parempi suojaus.

K-menetelmä

Kuvainformaation (näkymän, otoksen, näytteen) yksityiskohtaisuuden suunnittelu- ja tarkistusmenetelmä, joka on tarkoitettu käytettäväksi silloin, kun valvonnan kohteet ovat henkilöitä.

Kasvontunnistus

Tekniikka, jossa henkilön biometristä tietoa eli kasvokuvaa verrataan algoritmin avulla taustalla oleviin järjestelmin.

Kuvataajuus (kuvatahti)

Kuvien lukumäärä sekunnissa (FPS, Frames Per Second).

Loitering-analytiikka

Tekniikka, jolla havainnoidaan kameran kuvasta esimerkiksi henkilön tai ajoneuvon oleskelu alueella tietyn, määritellyn ajan ja tämän perusteella tehdään hälytys tai muita esiohjeltaituja toimenpiteitä.

LTS (Long Term Support)

Pitkäaikainen päivitystuki.

LYTP

Laki yksityisistä turvallisuuspalveluista.

Megapikselikamera

Kamera, jonka kuvakennossa on miljoonia (mega) kuvapisteitä (pikseleitä) kuvanmuodostusta varten.

NAS (Network Access Storage)

Tallennusjärjestelmä, joka jakaa tiedostoja verkossa yhteiskäyttöön.

Pakkaaminen

Datatiedoston (kuvatiedoston) koon pienentäminen.

Pikseli

Kuvapiste, kuvan pienin yksittäinen osa.

PoE (Power over Ethernet)

Jännitteensiirto tietoverkkokaapelointia pitkin.

PTZ-kamera (Pan Tilt Zoom)

Kääntöpääkamera.

Resoluutio

Kuvatarkkuus, erottelukyky, terävyys.

Rotakin

Standardin SFS-EN 62676-4 mukainen kameravalvonnan testitaulu (rotating kinetic target).

ST-kortisto

Sähkö-, tele-, turva- ja automaatioalan tietopalvelu, joka koostuu mm. ST-korteista ja -lomakkeista sekä ST-ohjeistoista ja -käsikirjoista, Sähköinfo Oy:n palvelu.

TCP/IP (Transmission Control Protocol)

Yleisimmin käytetty tietoverkkojen tiedonsiirtoprotokolla.

UPS-suojaus

Ylijännite- ja sähkökatkosuojaus.

Videohallintajärjestelmä (VMS, Video Management System)

Videohallintajärjestelmä on osa kameravalvontajärjestelmää. Sen avulla voidaan kerätä ja hallita digitaalista kuvaa, ääntä ja dataa kameroista, tallentimista ja muista lähteistä. Se tarjoaa myös käyttöliittymän sekä reaaliaikaisen että tallennetun kuvan katseluun ja käsittelyyn.

WiMAX (Worldwide Interoperability for Microwave Access)

Langaton laajakaistatekniikka.

WLAN (Wireless Local Area Network)

Langaton lähiverkko.

11 LÄHDELUETTELO JA AIHEESEEN LIITTYVÄÄ KIRJALLISUUTTA

Lait ja asetukset

- Rikoslaki (531/2000) 24 luku yksityisyyden, rauhan ja kunnian loukkaamisesta
- EU:n yleinen tietosuoja-asetus (2016/679)
- Tietosuoja laki (1050/2018)
- EU:n verkko- ja tietoturvadirektiivi (2016/1148)
- Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki yhteistoiminnasta yrityksistä (334/2007)
- Työturvallisuuslaki (738/2002)
- Laki yksityisistä turvallisuuspalveluista (1085/2015)
- Poliisilaki (872/2011)
- Tekijänoikeuslaki (404/1961)

Standardit

- CLC/TR 50531:fi. Hälytysjärjestelmät. Termit ja määritelmät
- SFS-EN 50398-1 Hälytysjärjestelmät. Yhdistetyt ja integroidut hälytysjärjestelmät. Osa 1: Yleiset vaatimukset
- SFS-EN 62676-1-1. Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 1-1: Järjestelmävaatimukset. Yleiset vaatimukset
- SFS-EN 62676-1-2. Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 1-2: Järjestelmävaatimukset. Videonsiirtoa koskevat suorituskykyvaatimukset
- SFS-EN 62676-4 Turvasovelluksissa käytettävät kameravalvontajärjestelmät. Osa 7: Soveltamisohjeet
- SFS-EN 60529 Sähkölaitteiden kotelointiluokat (IP-koodi)
- SFS-EN 62262 Sähkölaitteiden kotelointien mekaanisen iskunkestävyyden lujuusluokat (IK-koodi)

ST-julkaisut

- ST 664.10 Kameravalvontajärjestelmät. Suunnitteluohje
- ST 664.30 Kameravalvontajärjestelmät. Asennusohje
- ST 663.43 Kameravalvontajärjestelmän toteutuspöytäkirja
- ST 663.40 Kameravalvontajärjestelmän tarkastuspöytäkirja

- ST 664.40 Kameravalvontajärjestelmän kaapeloinnin tarkastus- ja mittauspöytäkirja
- ST 664.01 Tallentavan kameravalvonnan tietosuojaseloste
- ST 98.57 Kameravalvontajärjestelmät. Käyttö, ylläpito ja huolto
- ST-käsikirja 13 Kameravalvontajärjestelmät
- ST 682.10 Tietoteknisten järjestelmien integrointi
- ST 710.02 Sähkö- ja tietoteknisten järjestelmien tietoturva
- ST 730.05 Sähkö- ja tietoteknisten järjestelmien tietoturvan tarkastuspöytäkirja
- ST-ohjeisto 22 Verkottuneen talotekniikan tietoturva
- ST-ohjeisto 4 Kiinteistö- ja tilaturvallisuuden tasot
- ST-ohjeisto 13 Palvelutyöpointeen turvasuojauksen suunnittelu, toteutus ja ylläpito
- ST 660.40 Kiinteistö- ja tilaturvallisuustasojen määrittäminen
- ST 13.52. Rakennusten sijainti- ja asennuspiirustuksissa käytettäviä tietoteknisten järjestelmien (T) piirrosmerkkejä
- ST 51.25 Sähkö- ja tietoteknisten järjestelmien laitteiden ja tilojen merkitseminen

Muuta ohjeistusta

- The European Data Protection Board (EDPB): Guidelines on processing of personal data through video devices
- Tietosuojavaltuutetun toimisto: www.tietosuojafi.fi
- Liikenne- ja viestintävirasto Traficom: Kyberturvallisuuskeskus: www.kyberturvallisuuskeskus.fi
- Turvaa oikein -opas – turvallisuusjärjestelmien hankinnan sekä turvasuunnittelun ja -urakoinnin hyvät käytännöt, Turva-alan yrittäjät ry
- Turva-alan tietokansiot, Turva-alan yrittäjät ry ja Sähköinfo Oy
- Kameravalvonnan suunnitteluohje. Kameravalvonnan K-menetelmä, Finanssiala ry
- Toimitilojen tietoturvaohje VAHTI 2/2013, Valtiovarainministeriö
- Kansallinen turvallisuusauditointikriteeristö Katakri, Puolustusministeriö

LIITE 1: ESIMERKKI-ILMOITUS TALLENTAVASTA KAMERAVALVONNASTA

Tyypillinen esimerkki-ilmoitus tallentavasta kameravalvonnasta:



Euroopan tietosuojaneuvoston (EDPB) julkaiseman GDPR-ohjeen suosittelema esimerkki-ilmoitus tallentavasta kameravalvonnasta:

Kameravalvonta!

Rekisterinpitäjä: Oy Yritys Ab, Osoite 123 0123456 Postitoimipaikka, www.yritys.fi
 Rekisterinpitäjän edustaja: Etunimi Sukunimi, etunimi.sukunimi@yritys.fi, (09) 1234 5678
 Tietosuojavastaava: Etunimi Sukunimi, tietosuojavastaava@yritys.fi, (09) 1234 4321

Kameravalvonnan tarkoitukset

Kameravalvonnalla kerättävien tietojen tarkoitus on työntekijöiden turvallisuuden varmistaminen, omaisuuden suojaaminen ja toiminnan valvominen sekä turvallisuutta, omaisuutta tai toimintaa vaarantavien tilanteiden ennaltaehkäiseminen ja selvittäminen.

Käsiteltävä henkilötieto, tietojen säilytys ja niiden luovutus

Kameravalvonnan rekisteriin tallentuvat tiedot kameroiden valvonta-alueella olevista henkilöistä. Kuvan lisäksi tallennetaan tieto tallennusajankohdasta. Ääntä ei tallenneta. Tietoja säilytetään 30 vuorokautta, jonka jälkeen tiedot hävitetään. Tietoja säilytetään pidemmän ajan, jos oikeusvaatimuksen käsittely niin vaati. Rekisterinpitäjä käsittelee henkilötietoja itse. Tietoja voidaan luovuttaa vakuutusyhtiölle vahinkotapauksen korvauskäsittelyä varten. Poliisiviranomaisilla on lakiin perustuva tiedonsaantioikeus.

Rekisteröityjen oikeudet

Rekisteröidyllä on oikeus vaatia rekisterinpitäjää oikaisemaan, rajoittamaan tai poistamaan epätarkat tai muuten virheelliset henkilötiedot. Katso lisätietoja tästä kameravalvonnasta tietousojaselosteesta vasemmalla olevien linkkien kautta.

Lisätietoja:
www.yritys.fi/tietosuojaseloste

LIITE 2: TALLENTAVAN KAMERAVALVONNAN TIETOSUOJASELOSTE



ST 664.01

1 (1)

TALLENTAVAN KAMERAVALVONNAN
TIETOSUOJASELOSTE

PERUSTIEDOT			
Päivämäärä			
Rekisterin pitäjä	Yritys		
	Katuosoite	Postinumero	Postitoimipaikka
Rekisteriasioista vastaava henkilö ja/tai tietosuojavastaava	Nimi		
	Katuosoite	Postinumero	Postitoimipaikka
	Sähköpostiosoite	Puhelinnumero	
1. Käsiteltävä tieto			
2. Henkilötietojen käsittelyn tarkoitukset ja oikeusperuste			
3. Henkilötietojen säilyttämisäika			
4. Henkilötietojen vastaanottajat ja luovutukset			
5. Rekisteröidyn oikeudet			
6. Valitusoikeus			



ST 664.01

1 (1)

TALLENTAVAN KAMERAVALVONNAN TIETOSUOJASELOSTE

PERUSTIEDOT			
Päivämäärä 9.6.2020			
Rekisterin pitäjä	Yritys		
	Katuosoite	Postinumero	Postitoimipaikka
Rekisteriasioista vastaava henkilö ja/tai tietosuojavastaava	Nimi		
	Katuosoite	Postinumero	Postitoimipaikka
	Sähköpostiosoite	Puhelinnumero	

1. Käsiteltävä tieto

Kameravalvonnan rekisteriin tallentuvat tiedot kameroiden valvonta-alueella olevista henkilöistä. Kuvan lisäksi tallennetaan tieto tallennusajankohdasta. Ääntä ei tallenneta.

2. Henkilötietojen käsittelyn tarkoitukset ja oikeusperuste

Kameravalvonnalla kerättävien tietojen tarkoitus on työntekijöiden turvallisuuden varmistaminen, omaisuuden suojaaminen ja toiminnan valvominen sekä turvallisuutta, omaisuutta tai toimintaa vaarantavien tilanteiden ennaltaehkäiseminen ja selvittäminen.

Tallentava kameravalvontajärjestelmä vähentää rikollisuudesta aiheutuvaa pelkoa, ehkäisee ja paljastaa rikollisuutta, turvaa omaisuutta, tukee järjestyksen ja turvallisuuden ylläpitoa sekä tuottaa todistusaineistoa mahdollisten tutkintapyyntöjen, rikosilmoitusten ja oikeuskäsittelyiden tueksi.

3. Henkilötietojen säilyttämis aika

Tietoja säilytetään 30-365 vuorokautta, jonka jälkeen tiedot hävitetään. Tietoja säilytetään pidemmän ajan, jos oikeusvaatimuksen käsittely niin vaati, kunnes asia on lainvoimaisesti ratkaistu.

4. Henkilötietojen vastaanottajat ja luovutukset

Rekisterinpitäjä käsittelee henkilötietoja itse. Tietoja voidaan luovuttaa vakuutusyhtiölle vahinkotapauksen korvauskäsittelyä varten. Poliisiviranomaisilla on lakiin perustuva tiedonsaantioikeus.

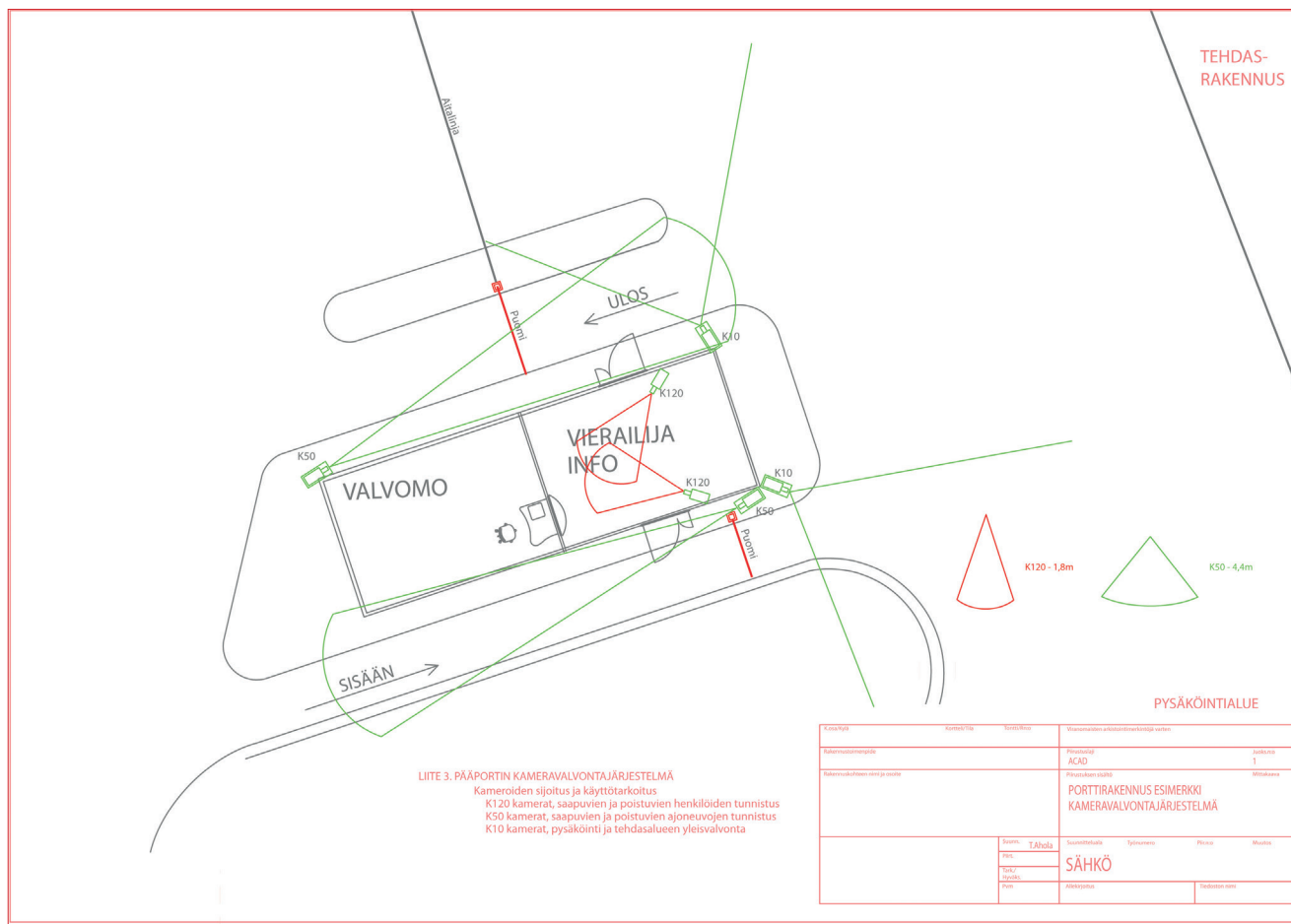
5. Rekisteröidyn oikeudet

- Rekisteröidyllä on oikeus
- saada pääsy itseään koskeviin tietoihin
 - pyytää itseään koskevien epätarkkojen ja virheellisten tietojen oikaisemista
 - pyytää itseään koskevien tietojen käsittelyn rajoittamista tai poistamista
 - vastustaa itseään koskevien tietojen käsittelyä
 - pyytää itseään koskevien tietojen siirtämistä järjestelmästä toiseen
 - joshenkilötietojen käsittely perustuu rekisteröidyn suostumukseen, peruuttaa suostumus
 - tehdä valitus tietojen käsittelystä tietosuojavaltuutetulle.

6. Valitusoikeus

Jos katsot, että tietosuojaoikeuksiasi on loukattu, ole yhteydessä rekisterinpitäjään. Rekisteröidyllä on oikeus tehdä valitus rekisterinpitäjän toimista valvontaviranomaiselle, joka Suomessa on tietosuojavaltuutettu, www.tietosuoja.fi.

LIITE 4: MALLIKUVA TEHTAAN PORTTIALUEEN KAMERAVALVONNASTA



LIITE 3. PÄÄPORTIN KAMERAVALVONTAJÄRJESTELMÄ
Kameroiden sijoitus ja käyttötarkoitus
K120 kamerat, saapuvien ja poistuvien henkilöiden tunnistus
K50 kamerat, saapuvien ja poistuvien ajoneuvojen tunnistus
K10 kamerat, pysäköinti ja tehdasalueen yleisvalvonta

LIITE 5: MALLI TALLENTEIDEN LUOVUTUSDOKUMENTISTA

TALLENTEIDEN LUOVUTUSDOKUMENTTI				
Tilaaja		Osoite		
Organisaatio		Puhelin	Sähköposti	
Vastaanottaja		Osoite		
Organisaatio		Puhelin	Sähköposti	
Kohde josta tallenteet halutaan		Osoite		
Yhteyshenkilö		Puhelin	Sähköposti	
Tallennusjärjestelmä		Merkki	Malli	
Päivämäärä	Aloitusaika	Lopetusaika	Tapahtuma/henkilökuvaus	Tallenteiden määrä
Lisätietoja				
Allekirjoitus		Aika ja paikka		
		Nimenselvennys		
Tallenteiden luovutus				
Saako tallennetta luovuttaa muihin kuin esitutkintaviranomaisten tutkinnallisiin tarkoituksiin?				
☐ Kyllä ☐ Ei				
Luovuttajan allekirjoitus		Aika ja paikka		
		Nimenselvennys		
Vastaanottajan allekirjoitus		Aika ja paikka		
		Nimenselvennys		

JULKAISUN TUKIJAT

Seuraavat yritykset ja yhteisöt ovat tukeneet Kameravalvontaoppaan päivitystyötä:



STANLEY SECURITY OY

www.stanleysecurity.fi



OY HEDENGREN SECURITY AB

www.hedengren.com/fi/security/



BLC TURVA OY

www.blcturva.fi



AXIS COMMUNICATIONS AB

www.axis.com



WSP FINLAND OY

www.wsp.com/fi-FI



FINANSSIALA RY

www.finanssiala.fi



CERTEGO OY

www.certego.fi



capcon

TURVAPALVELUT

CAPITIS CONTROL OY

www.capcon.fi



**SUOMEN PELASTUSALAN
KESKUSJÄRJESTÖ**

www.spek.fi

Caverion

CAVERION SUOMI OY

www.caverion.fi



kamerapilvipalvelu ja teollisuuden prosessivalvonta

EMSEC OY

www.emsec.fi