Sisäkulkuoikeuksien myöntämisperusteet ja hallinta tehdasympäristössä

19. Turvallisuusjohdon koulutusohjelma

Lopputyöraportti

Antti Suikkanen

Stora Enso Oyj

Imatra 30.3.2026

Aalto University Executive Education and Professional Development

Tiivistelmä

Tämän lopputyön tavoitteena on laatia ohjeistus tehdasalueen sisäkulkuoikeuksien myöntämisperusteista. Työssä tarkastellaan tilojen suojaamista ja kulun rajaamista siten, että pääsy myönnetään vain työtehtävien kannalta välittömään tarpeeseen perustuen. Kohteena ovat erityisesti kriittiset tilat, kuten IT-, sähkö- ja automaatiotilat, sekä kemikaali- ja räjähdysvaaralliset alueet.

Teoreettinen viitekehys pohjautuu lainsäädäntöön, kuten työturvallisuus- ja painelaitelakiin sekä lakiin yksityisyyden suojasta työelämässä ja keskeisiin ohjeistuksiin, kuten Katakri 2020, VAHTI ja ST-ohjeisto 4. Riskienhallinnassa hyödynnetään SFS-ISO 31000 -standardia, tietoturvan hallinnan SFS-EN ISO/IEC 27001- ja 27002-standardeja sekä Finanssialan murtosuojausohjeita.

Työssä analysoidaan fyysisen ja teknisen suojauksen menetelmiä suhteessa tilojen ja kriittisyyteen. Tuloksena syntyvä ohjeistus määrittelee perusteet oikeuksien myöntämiselle, seurannalle ja poistamiselle huomioiden tietosuojan, yksityisyyden suojan ja AEO-vaatimukset. Työ tarjoaa työkalun turvallisuuskulttuurin vahvistamiseen ja luvattoman käytön estämiseen

Abstract

This thesis establishes guidelines for granting internal access rights in a factory environment. The aim is to ensure access is granted only based on immediate, work-related needs. Focus areas include critical facilities such as ICT, electrical and automation rooms, and chemical and hazardous explosive areas.

The theoretical framework is based on legislation, including the Occupational Safety and Health Act, the Pressure Equipment Act, and the Act on the Protection of Privacy in Working Life. Key security guidelines include Katakri 2020, VAHTI, and ST-ohjeisto 4. Risk management is addressed using SFS-ISO 31000, the SFS-EN ISO/IEC 27001 and 27002 standards, and burglary protection guidelines.

The study analyzes physical and technical security methods relative to facility criticality. The outcome is a consistent policy for granting, monitoring, and revoking access rights, considering GDPR, privacy in working life, and AEO requirements. This work provides a practical tool for strengthening factory security culture and preventing unauthorized access.

Sisältö

1 Johdanto 1
1.1 Työn tausta ja tarve 1
1.2 Tutkimuskysymys ja tavoitteet 2
1.3 Työn rajaus ja keskeiset käsitteet 2
2. Yritysturvallisuus ja sääntelykehikko 4
2.1 Turvallisuusjohtamisen viitekehys ja riskienhallinta 4
2.2 Työturvallisuus ja tekninen turvallisuuslainsäädäntö 5
2.2.1 Työturvallisuuslaki (23.8.2002/738) 5
2.2.2 Painelaitelaki (16.12.2016/1144) 5
2.3 Tietosuoja ja yksityisyyden suoja kulunvalvonnassa 6
2.4 Kansainvälinen kauppa ja AEO-valtuutus 6
2.5 Turvallisuuspalvelut ja tekninen valvonta 7
2.6 Viranomaisten toimialan suositukset (Katakri ja VAHTI) 7
3 Riskienhallinta suojauksen perustana 9
3.1 Riskienhallintaprosessi ja viitekehys 9
3.2 Uhkien tunnistaminen ja sisäkulkuoikeuksien riskit 9
3.3 Murtoriskien arviointi ja suojaustason valinta 10
3.4 Pääsynhallinta osana jatkuvuuden hallintaa 11
3.5 Jäännösriski ja riskien hyväksyminen 11
4 Tehdastason tilaluokitukset ja turvallisuustasot 13
4.1 Vyöhykejaon periaatteet ja tilaturvallisuuden tasot 13
4.2 IT- ja tietoliikennetilat 14
4.2.1 Keskitetyt tietoliikennetilat 14
4.2.2 Tietoliikennekaapit ja NEC-kaapit (Hajautetut tilat) 14
4.3 Sähkö-, automaatio- ja kaapelitilat 14
4.4 Kemikaali- ja räjähdysvaaralliset sekä räjähdetilat 15
4.5 Hallinnolliset ja tukitilat 15
4.6 Tilatyyppien ja turvallisuustasojen yhteenveto 16
4.7 Tilojen suojaamisen erityispiirteet 16
5 Fyysisen ja teknisen suojauksen menetelmät 17
5.1 Rakenteellinen murtosuojaus 17
5.1.1 Ovet, seinät ja lukitus 17
5.1.2 Hajautetut kohteet (NEC-kaapit ja kotelot) 18
5.2 Tekninen kulunvalvonta ja tunnistautuminen 18
5.2.1 Tunnistautumismenetelmät 18
5.2.2 Järjestelmän hallinta ja lokitus 18
5.3 Kameravalvonnan rooli pääsynhallinnassa 19

5.4 Yksityiset turvallisuuspalvelut ja hälytysvaste 19
6 Ohjeistus: Sisäkulkuoikeuksien myöntämisperusteet 21
6.1 Kulkuoikeuksien hallintaprosessi ja vastuut 21
6.2 Yleiset myöntämisperusteet (Välitön tarve) 21
6.3 Kulkuoikeusryhmät ja roolipohjainen hallinta 22
6.4 Erikoiskohteiden erityisperusteet 22
6.5 Kulkuoikeuksien elinkaaren hallinta 23
6.6 Poikkeustilanteet ja tilapäiset oikeudet 23
6.7 Kulkuoikeusmatriisi 25
6.8 Tilakohtaiset myöntämisperusteet ja erityisvaatimukset 26
6.8.1 Laboratoriotilat (Laadunvalvonta ja Tutkimus ja kehitys) 26
6.8.2 LVI- ja tekniset tilat (mukaan lukien turvatekniset tilat) 27
6.8.3 Tuotevarastot ja logistiikan tilat (AEO) 27
6.8.4 Varasto- ja materiaalipalvelut 27
6.8.5 Sähkö- ja automaaatiotilat 28
6.8.6 IT-tilat ja hajautetut tietoliikennekaapit (NEC) 28
6.9 Ohjeistuksen yhteenveto ja jalkauttaminen 29
7 Johtopäätökset ja pohdinta 30
7.1 Tulosten yhteenveto ja tavoitteiden toteutuminen 30
7.2 Ohjeistuksen merkitys turvallisuuskulttuurille 31
7.3 Eettiset näkökulmat ja työntekijöiden yksityisyys 31
7.4 Luotettavuus ja työn hyödynnettävyys 32
7.5 Jatkokehitysehdotukset ja tulevaisuuden näkymät 32
7.6 Loppusanat 33
8 Lähteet: 34

1 Johdanto

1.1 Työn tausta ja tarve

Nykyaikaisessa teollisuusympäristössä fyysinen turvallisuus ja pääsynhallinta muodostavat perustan koko yrityksen toimintavarmuudelle. Turvallisuus ei ole enää erillinen tukitoiminto, vaan se on integroitava osaksi organisaation kokonaisvaltaista riskienhallintaprosessia (SFS-ISO 31000: 2018). Tehdasalueet ovat monimuotoisia ympäristöjä, joissa risteävät työntekijöiden, vierailijoiden ja ulkopuolisten urakoitsijoiden kulkureitit. Samalla tiloissa käsitellään kriittistä tietoa, vaarallisia kemikaaleja ja kalliita teknisiä laitteistoja, mikä asettaa korkeita vaatimuksia sisätilojen suojaukselle (Huoltovarmuuskeskus 2025).

Sisäkulkuoikeuksien hallinnan merkitys korostuu erityisesti silloin, kun tehtaalla on useita eri turvallisuustason tiloja. IT-infrastruktuuri, kuten tietoliikennehuoneet ja hajautetusti sijoitetut tietoliikennekaapit (mukaan lukien NEC-kaapit), vaativat erityistä suojaa, sillä ne ovat alttiita sekä fyysiselle sabotaasille että tietoturvaloukkauksille (Valtiovarainministeriö 2013). Lisäksi sähkö-, automaatio- ja kaapelitilat sisältävät riskejä, jotka liittyvät sekä laitteiston toimintavarmuuteen että työturvallisuuteen (Sähkötieto ry 2021).

Lainsäädännön ja kansainvälisten standardien vaatimukset, kuten AEO-valtuutetun toimijan kriteerit, edellyttävät yrityksiltä kykyä rajoittaa ja valvoa pääsyä kriittisiin tiloihin (Suomen Tulli 2023). Puutteellinen kulunhallinta voi johtaa paitsi taloudellisiin menetyksiin ja tietovuotoihin mutta myös vakaviin työturvallisuusriskeihin, jos ammattitaidottomat henkilöt pääsevät esimerkiksi painelaitteiden tai räjähdysvaarallisten aineiden läheisyyteen (Työturvallisuuslaki 23.8.2002/738; Painelaitelaki 16.12.2016/1144).

1.2 Tutkimuskysymys ja tavoitteet

Tämän opinnäytetyön tavoitteena on laatia kattava ja käytännönläheinen yleisohje, joka määrittelee selkeät ja johdonmukaiset perusteet kulkuoikeuksien myöntämiselle tehdasalueen eri turvallisuustason sisätiloihin. Ohjeistuksen tarkoituksena on luoda standardoitu prosessi, jolla varmistetaan, että pääsy myönnetään vain niille henkilöille, joilla on siihen työtehtäviensä kannalta välitön ja dokumentoitu tarve.

Työn tutkimuskysymykset on muotoiltu seuraavasti:

1. Millaisia lainsäädännöllisiä ja teknisiä vaatimuksia erityyppisten sisätilojen (esim. kemikaalitilat, IT-tilat, sähkötilat) suojaamiselle asetetaan?
2. Millaiset ovat optimaaliset myöntämisperusteet, joilla tasapainotetaan työn sujuvuus ja tilaturvallisuuden vaatimukset?
3. Miten kulunvalvontajärjestelmän tuottamaa tietoa ja kameravalvontaa voidaan hyödyntää pääsynhallinnan tukena lainmukaisesti?

Tavoitteena on, että lopputuloksena syntyvä ohjeistus toimii yrityksen johdon ja turvallisuusorganisaation työkaluna, jolla minimoidaan inhimilliset virheet ja luvattomat pääsyt kriittisiin kohteisiin.

1.3 Työn rajaus ja keskeiset käsitteet

Tämä työ rajataan tiukasti koskemaan tehdasalueen ja niihin liittyviä hallinnollisia ja teknisiä kulkuoikeuksia. Rajauksen ulkopuolelle jäävät ulkoalueiden fyysinen suojaaminen, kuten aitaaminen ja porttiratkaisut, sekä yleinen aluevalvonta, ellei se liity välittömästi sisätiloihin pääsyyn. Painopiste on nimenomaan kulkuoikeuksien myöntämisperusteissa ja niiden luokittelussa tilojen kriittisyyden mukaan.

Työn kannalta keskeiset käsitteet määritellään seuraavasti:

Pääsynhallinta (Access Management): Hallinnollinen prosessi, jolla määritetään, valvotaan ja rajoitetaan henkilöiden pääsyä tiettyihin fyysisiin tiloihin tai tietojärjestelmiin. Perustuu tässä työssä roolipohjaiseen oikeuksien hallintaan.

Välitön tarve (Need-to Enter): Turvallisuusperiaate, jonka mukaan kulkuoikeus myönnetään vain, jos se on välttämätöntä kyseisen työtehtävän suorittamiseksi. Pääsyä ei myönnetä organisaatiossa olevan aseman vaan tosiasiallisen tarpeen perusteella.

Kulunvalvontajärjestelmä (Access Control System): Tekninen kokonaisuus, joka koostuu lukijoista, ohjainyksiköistä, ohjelmistosta ja tunnisteista. Järjestelmän tehtävänä on tunnistaa henkilö, todentaa kulkuoikeus ja ohjata lukitusta.

NEC-kaappi (Network Equipment Center): Tehdasalueella hajautetusti sijaitseva tietoliikennekaappi, joka sisältää kriittistä verkkoinfrastruktuuria. Kaapit luokitellaan osaksi kriittistä infrastruktuuria niiden sijainnista riippumatta.

AEO (Authorized Economic Operator): Tullin myöntämä valtuutetun talouden toimijan status, joka edellyttää yritykseltä todistettua turvallisuuden hallintaa koko toimitusketjussa mukaan lukien tilojen pääsynhallinta.

Katakri (Kansallinen turvallisuusauditointikriteeristö): Viranomaisen käyttämä työkalu, jolla arvioidaan organisaation kykyä suojata luottamuksellista tietoa. Työssä hyödynnetään Katakrin fyysisen turvallisuuden vaatimuksia.

Jäännösriski (Residual Risk): Riski, joka jää jäljelle, kun kaikki suunnitellut hallintatoimenpiteet ja suojaukset on toteutettu. Työssä analysoidaan, millainen jäännösriski on hyväksyttävissä eri tilatyypeissä.

GDPR (General Data Protection Regulation): Euroopan unionin yleinen tietosuoja-asetus, joka sääntelee kulunvalvontajärjestelmästä kertyvän henkilötiedon (lokitiedot) käsittelyä, säilyttämistä ja suojaamista.

2. Yritysturvallisuus ja sääntelykehikko

Tehdasympäristön turvallisuus rakentuu usean eri sääntelyalueen ja standardin leikkauspisteeseen. Pelkkä fyysinen lukitus ei riitä täyttämään nykyajan vaatimuksia, vaan sisäkulkuoikeuksien hallinnan on oltava osa strategista turvallisuusjohtamista, joka huomioi niin työntekijöiden turvallisuuden, omaisuuden suojan kuin tiedon eheydenkin.

2.1 Turvallisuusjohtamisen viitekehys ja riskienhallinta

Yritysturvallisuus määritellään usein prosessiksi, jolla suojataan yrityksen ihmisiä, mainetta, omaisuutta ja toiminnan jatkuvuutta (Turva-alan yrittäjät ry 2019). Tehdasympäristössä tämä tarkoittaa siirtymistä pois pistemäisistä suojatoimista kohti kokonaisvaltaista hallintamallia. Turvallisuusjohtamisen ytimessä on standardi SFS-ISO 31000 (2018), joka painottaa riskienhallinnan integroimista osaksi organisaation kaikkia prosesseja. Koska tässä työssä tarkastellaan erityisesti kulkuoikeuksia kriittisiin tiloihin, yleisstandardia täydennetään tietoturvallisuuden hallintajärjestelmiin keskittyvillä ISO/IEC 27001 ja ISO/IEC 27002 -standardeilla. Siinä missä ISO 31000 antaa menetelmät riskien arviointiin, ISO 27001 asettaa vaatimukset pääsynhallinnan hallinnolliselle rakenteelle. Standardi ISO 27002 puolestaan tarjoaa yksityiskohtaiset suositukset fyysisen turvallisuuden kontrolleista, kuten turvavyöhykkeistä ja sisäänpääsyn valvonnasta, jotka ovat keskeisiä määritettäessä tehtaan sisäkulkuoikeuksien perusteita.

Riskienhallinnan näkökulmasta sisäkulkuoikeuksien hallinta on kontrollimekanismi, jolla pyritään pienentämään tunnistettujen uhkien todennäköisyyttä. Uhkat voivat olla:

Ulkoisia: Kuten teollisuusvakoilu, sabotaasi tai murtovarkaudet (Finanssiala 2017).

Sisäisiä: Kuten inhimilliset virheet vaarallisissa tiloissa, tahallinen väärinkäytös tai työntekijän päätyminen tilaan, johon hänellä ei ole riittävää pätevyyttä tai perehdytystä.

Valtiovarainministeriö (2017) korostaa, että tehokas riskienhallinta vaatii jatkuvaa arviointia. Ei riitä, että kulkuoikeudet on kerran määritetty; ne on kyettävä päivittämään vastaamaan organisaation muuttuvia tarpeita ja uhkakuvia. Kulkuoikeuksien myöntämisperusteiden onkin oltava dynaamisia mutta silti tarkasti dokumentoituja.

2.2 Työturvallisuus ja tekninen turvallisuuslainsäädäntö

Lainsäädäntö asettaa työnantajalle ankaran velvollisuuden huolehtia siitä, etteivät työntekijät päädy vaarallisiin tilanteisiin. Tämä velvollisuus toteutuu tehdasympäristössä esimerkiksi rajoittamalla pääsyä vaarallisiin sisätiloihin.

2.2.1 Työturvallisuuslaki (23.8.2002/738)

Työturvallisuuslain 8 § määrittelee työnantajan yleisen huolehtimisvelvoitteen. Työnantajan on otettava huomioon työhön, työolosuhteisiin ja muuhun työympäristöön liittyvät seikat. Lain 10 § puolestaan vaatii vaarojen selvittämistä ja arviointia. Kulkuoikeuksien hallinta on tässä keskeinen työkalu: jos tila sisältää esimerkiksi puristumisvaaran, sähköiskun riskin tai kemikaalialtistuksen mahdollisuuden, on työnantajan rajoitettava pääsy vain niille, joilla on tarvittava ammattitaito ja suojaus (Työturvallisuuslaki 23.8.2002/738).

2.2.2 Painelaitelaki (16.12.2016/1144)

Tehdasympäristöissä sijaitsee usein painelaitteita, joiden vaurioitumisesta voi seurata suuronnettomuus. Painelaitelain (16.12.2016/1144) mukaan painelaitteiden sijoitustilat on suojattava ja niiden käyttö on rajattava päteville henkilöille. Kulunvalvonnan tehtävänä on varmistaa, ettei esimerkiksi huoltotiloihin tai höyrykattilalaitoksiin pääse asiattomia, jotka voisivat tahattomasti tai tahallaan aiheuttaa vaaratilanteen. Tämä asettaa tiukat vaatimukset nimenomaan sähkö- ja automaatiotilojen sekä kaapelihuoneiden pääsynhallinnalle.

2.3 Tietosuoja ja yksityisyyden suoja kulunvalvonnassa

Kun tehdasalueella käytetään sähköistä kulunvalvontaa, muodostuu järjestelmään väistämättä henkilörekisteri. Tämän käsittelyä ohjaa Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 (GDPR). Suomessa kansallinen laki yksityisyyden suojasta työelämässä (759/2004) täydentää tätä säädöskokonaisuutta asettamalla tiukat raamit teknisen valvonnan käytölle.

Kulunvalvonnan ja pääsynhallinnan ohjeistuksessa on huomioitava seuraavat periaatteet:

1. Tarpeellisuusvaatimus (759/2004, 4§): Työnantaja saa käsitellä vain työntekijän työsuhteen kannalta välittömästi tarpeellisia henkilötietoja. Tämä säädös muodostaa juridisen pohjan työssä käytettävälle välitön tarve (Need-to-Enter) -periaatteelle.
2. Käyttötarkoitussidonnaisuus: Tietoja saa kerätä vain määriteltyihin ja laillisiin tarkoituksiin, kuten omaisuuden suojaamiseen ja työturvallisuuden varmistamiseen.
3. Tietojen minimointi: Järjestelmään ei tule tallentaa enempää tietoa kuin on välttämätöntä kulkuoikeuden varmentamiseksi.
4. Säilytyksen rajoittaminen: Lokitietoja ei saa säilyttää ikuisesti, vaan niiden säilytysajan on oltava perusteltu (GDPR 2016/679).

Kameravalvonta on usein kiinteä osa sisätilojen suojaamista. Se on erityisen tärkeää kriittisissä kohteissa kuten IT-tiloissa tai kemikaalivarastoissa. Turvaalan yrittäjät ry:n (2020) kameravalvontaopas muistuttaa, että valvonta on toteutettava siten, ettei se loukkaa työntekijöiden yksityisyyttä tarpeettomasti. Valvonnasta on tiedotettava selkeästi ja valvonnan tulee perustua todelliseen turvallisuustarpeeseen.

2.4 Kansainvälinen kauppa ja AEO-valtuutus

Monet suomalaiset tehtaat hakevat Tullilta AEO-valtuutusta (Authorized Economic Operator), joka helpottaa kansainvälistä kauppaa. Valtuutuksen saaminen edellyttää, että yritys täyttää tiukat turvallisuusvaatimukset (Suomen Tulli 2023).

Yksi AEO-kriteeristön keskeisimmistä vaatimuksista on toimitilojen fyysinen turvallisuus. Yrityksen on kyettävä osoittamaan:

- Miten pääsyä rakennuksiin valvotaan.
- Miten estetään luvaton pääsy lähetys- ja varastotiloihin.
- Miten työntekijöiden ja vierailijoiden kulkuoikeuksia hallinnoidaan.

Tämä asettaa suoria vaatimuksia ohjeistukselle: kulkuoikeuksien myöntämisperusteiden on oltava läpinäkyviä ja johdonmukaisia ja niiden on kestettävä viranomaisauditointi.

2.5 Turvallisuuspalvelut ja tekninen valvonta

Pääsynhallinta ei ole vain passiivista lukitusta, vaan se vaatii usein aktiivista valvontaa. Laki yksityisistä turvallisuuspalveluista (21.8.2015/1085) säätelee vartioimisliiketoimintaa ja turvasuojaustehtäviä. Teknisenä valvontana kulunvalvonta on kuitenkin altisteinen myös laille yksityisyyden suojasta työelämässä (759/2004)

Laki määrittelee muun muassa:

- Yhteistoimintamenettely (21§): Ennen teknisen valvonnan, kuten kulunvalvonnan lokituksen käyttöönottoa tai sen olennaista muuttamista työnantajan on suoritettava yhteistoimintalain mukainen neuvottelumenettely tai kuultava henkilöstöä. Tässä vaiheessa on määriteltävä valvonnan tarkoitus, menetelmät ja se miten lokitietoja käytetään.
- Turvasuojaaja: Kuka saa asentaa ja huoltaa kulunvalvontajärjestelmiä (turvasuojaaja).
- Vartijoiden toimivalta: Miten vartijat voivat puuttua luvattomaan oleskeluun tehdasalueen sisätiloissa.
- Hälytysvaste: Miten teknistä valvontaa (kuten kulunvalvonnan hälytyksiä) tulee hoitaa lainmukaisesti.

Teknisen valvonnan ja fyysisen suojauksen on toimittava saumattomasti yhteen. Huoltovarmuuskeskus (2025) painottaa fyysisen suojauksen ohjeessaan, että tekniset järjestelmät ovat vain niin hyviä kuin niitä tukevat hallinnolliset prosessit – tässä tapauksessa kulkuoikeuksien myöntämisperusteet.

2.6 Viranomaisten toimialan suositukset (Katakri ja VAHTI)

- Viimeisenä sääntelykehikon palasena ovat viranomaisten antamat suositukset ja ohjeistukset:

- Katakri (2020): Valtionhallinnon turvallisuusauditointityökalu, joka antaa selkeät vaatimukset fyysiselle turvallisuudelle eri turvallisuusluokissa. Vaikka kyseessä on viranomaistyökalu, se on laajalti käytössä myös teollisuudessa kriittisten tilojen suojaamisessa.
- VAHTI-ohje (Valtiovarainministeriö 2013): Toimitilojen tietoturvaohje, joka määrittelee tilojen vyöhykejaon ja pääsynhallinnan periaatteet erityisesti tietoturvan näkökulmasta. Se antaa pohjan sille, miten IT-tilat ja tietoliikennekaapit tulisi suojata.

Taulukko 1 Yhteenveto sääntelypohjasta

Sääntely / Ohje	**Keskeinen vaikutus kulkuoikeuksiin**
Työturvallisuuslaki (2002/738)	Pääsy on estettävä vaarallisiin tiloihin tehtyjen vaarojen arviointien perusteella.
GDPR (EU 2016/679)	Henkilötietojen käsittelyn minimointi kulunvalvonnassa ja lokitietojen asianmukainen suojaus.
AEO-valtuutus (Suomen Tulli 2023)	Toimitusketjun fyysisen turvallisuuden ja pääsynhallinnan aukoton todentaminen viranomaisille.
Katakri (2020 / VAHTI (2013)	Standardoidut tasot fyysiselle suojaukselle, rakenteelliselle murtosuojaukselle ja vyöhykejaolle.

3 Riskienhallinta suojauksen perustana

Turvallisuusratkaisut eivät saa olla itsetarkoitus, vaan niiden tulee perustua tunnistettuihin riskeihin ja riskien vaikutusten arviointiin. Tehdasympäristössä riskienhallinta on jatkuva prosessi, joka ohjaa resurssien kohdentamista sinne, missä on suurin suojaustarve. Tässä luvussa tarkastellaan riskienhallinnan prosessia ja murtoriskien arviointia sisäkulkuoikeuksien näkökulmasta.

3.1 Riskienhallintaprosessi ja viitekehys

Riskienhallinnan ytimessä on kansainvälinen standardi SFS-ISO 31000 (2018), joka määrittelee riskin "epävarmuuden vaikutukseksi tavoitteisiin". Sisäkulkuoikeuksien hallinnassa tavoitteena on turvata tehtaan häiriötön toiminta, henkilöstön turvallisuus ja kriittinen informaatio. Prosessi aloitetaan määrittelemällä toimintaympäristö, minkä jälkeen siirrytään riskien tunnistamiseen, analysointiin ja arviointiin.

Valtiovarainministeriö (2017) painottaa, että riskienhallinnan on oltava järjestelmällistä ja ennakoivaa. Tehdasympäristössä tämä tarkoittaa, että jokainen tila on analysoitava erikseen: mitä seurauksia olisi, jos asiaton henkilö pääsisi kyseiseen tilaan? Arvioinnissa on huomioitava sekä suorat taloudelliset menetykset mutta myös välilliset vaikutukset, kuten maineen menetys tai toiminnan pitkäaikainen keskeytyminen.

3.2 Uhkien tunnistaminen ja sisäkulkuoikeuksien riskit

Uhkien tunnistaminen on riskien arvioinnin kriittisin vaihe. Tehdasalueen sisätiloihin kohdistuvat uhat voidaan jakaa tahallisiin, vahingollisiin ja luonnonvoimista johtuviin uhkiin. Sisäkulkuoikeuksien hallinnalla pyritään hallitsemaan erityisesti seuraavia riskejä:

Luvaton tunkeutuminen ja varkaudet: Arvokkaan omaisuuden, kuten työkalujen, raaka-aineiden tai valmiiden tuotteiden anastus. Finanssiala (2017) muistuttaa, että murtoriski kasvaa, jos kohteen houkuttelevuus ja sieltä saatava hyöty ovat suuria suhteessa kiinnijäämisriskiin.

1. Sabotaasi ja ilkivalta: Kriittisten prosessien, kuten automaatiojärjestelmien tai sähkönjakelun tahallinen vaurioittaminen. Erityisesti tietoliikennekaapit ja hajautetut NEC-kaapit ovat alttiita fyysiselle manipuloinnille, jos niiden pääsynhallinta on puutteellista (Valtiovarainministeriö 2013).
2. Teollisuusvakoilu ja tietovuodot: Pääsy arkistoihin tai IT-tiloihin, joissa säilytetään yrityssalaisuuksia tai henkilötietoja. Tämä linkittyy suoraan GDPR (2016/679) vaatimuksiin suojata henkilötietoja asiattomalta pääsyltä.
3. Työturvallisuusriskit: Perehdyttämättömän henkilön pääsy vaaralliseen tilaan, esim kemikaalivarastoon tai korkeajännitealueelle, mikä voi johtaa vakavaan tapaturmaan (Työturvallisuuslaki 23.8.2002/738).

3.3 Murtoriskien arviointi ja suojaustason valinta

Kun uhat on tunnistettu, on määritettävä tarvittava suojaustaso. Finanssiala (2017) on julkaissut ohjeistuksen "Kohteen murtoriskien arviointi ja suojaustason valinta", joka toimii erinomaisena työkaluna tehdasympäristön sisätilojen luokittelussa.

Murtoriskiä arvioitaessa tarkastellaan kahta päämuuttujaa:

- Houkuttelevuus: Kuinka helposti realisoitavaa ja arvokasta omaisuutta tilassa on? Esimerkiksi pientoimiston tulostinhuone on vähemmän houkutteleva kuin keskitetty ATK-tila tai kalliita erikoiskemikaaleja sisältävä varasto.
- Sijainti ja valvonta: Kuinka syvällä rakennuksessa tila sijaitsee ja millaisen teknisen valvonnan piirissä se on?

Suojaustasot jaetaan yleensä luokkiin 1–3 (tai 1–4 kohteen vaativuuden mukaan). Mitä korkeampi riskitaso, sitä vaativampia rakenteellisia ja teknisiä suojatoimia edellytetään (Finanssiala 2017b). Esimerkiksi korkean riskin sähkö- ja automaatiotiloissa tai IT-tiloissa ei riitä pelkkä mekaaninen lukitus,

vaan se on yhdistettävä sähköiseen kulunvalvontaan ja mahdollisesti kameravalvontaan (Turva-alan yrittäjät ry 2020).

3.4 Pääsynhallinta osana jatkuvuuden hallintaa

Huoltovarmuuskeskus (2025) painottaa fyysisen suojauksen ohjeessaan, että suojaamisen tavoitteena on varmistaa yhteiskunnan ja yritysten kriittisten toimintojen jatkuvuus kaikissa olosuhteissa. Tehdasympäristössä sisäkulkuoikeuksien hallinta on yksi jatkuvuuden hallinnan tärkeimmistä työkaluista.

Jos tehtaan kriittinen ohjausjärjestelmä vaurioituu hallitsemattoman pääsyn seurauksena, voivat seuraukset olla katastrofaaliset tuotannolle. Siksi suojaus on rakennettava "syvyyssuuntaisen suojauksen" periaatteella:

- Ennaltaehkäisy: Selkeät kulkuoikeudet ja fyysiset esteet.
- Havaitseminen: Kulunvalvontajärjestelmän hälytykset ja kameravalvonta (Turva-alan yrittäjät ry 2019).
- Viivyttäminen: Rakenteellinen murtosuojaus, joka hidastaa luvatonta pääsyä ja antaa aikaa reagoida (Finanssiala 2017b).
- Reagointi: Turvallisuushenkilöstön tai vartioinnin toimenpiteet (Laki yksityisistä turvallisuuspalveluista 21.8.2015/1085).

3.5 Jäännösriski ja riskien hyväksyminen

Kaikkia riskejä ei voida poistaa kokonaan ilman, että työn tekeminen muuttuu kohtuuttoman vaikeaksi. Tätä hallintatoimien jälkeen jäljelle jäävää riskiä kutsutaan jäännösriskiksi. SFS-ISO 31000 (2018) mukaan organisaation johdon on määritettävä riskinottohalunsa eli se riskitaso, jonka organisaatio on valmis hyväksymään saavuttaakseen tavoitteensa. Tämän tason on pysyttävä organisaation objektiivisen riskinkantokyvyn puitteissa.

Esimerkiksi tulostinhuoneen kohdalla organisaation riskinottohalu voi olla korkeampi operatiivisen sujuvuuden edistämiseksi. Tällöin hyväksytään matalampi suojaustaso ja laajempi kulkuoikeusryhmä, vaikka se sisältäisi pienen tietoturvariskin. Sen sijaan kriittisten IT-tilojen kohdalla riskinsietokyky on erittäin matala: Pääsy verkkokomponentteihin vaarantaa koko tehtaan tietoturvan ja jatkuvuuden, minkä vuoksi jäännösriski on minimoitava ehdottoman tiukalla kulunrajauksella. (Valtionvarainministeriö 2013; Katakri 2020).

Taulukko 2 Yhteenveto riskienhallinnan perusteista

Analysoitava kohde	**Keskeinen lähde**	**Suojauksen painopiste**
Kokonaisprosessi	SFS-ISO 31000	Systemaattinen riskien arviointi ja käsittely.
Murtosuojaus	Finanssiala 2017	Rakenteellinen kestävyys ja kohteen houkuttelevuus.
Tietoturvallisuus	VAHTI / Katakri	Luottamuksellisen tiedon ja IT-laitteiden suojaaminen.
Henkilöturvallisuus	Työturvallisuuslaki	Tapaturmien ehkäisy rajoittamalla pääsyä vaarallisiin tiloihin.

4 Tehdastason tilaluokitukset ja turvallisuustasot

Tehdasympäristön sisätilojen suojaaminen perustuu syvyyssuuntaiseen puolustukseen ja vyöhykejakoon. Tavoitteena on luoda kerroksellinen turvallisuusmalli, jossa sisemmät, kriittisemmät vyöhykkeet on suojattu tiukemmin kuin ulommat. Tässä luvussa määritellään tilojen luokitteluperusteet ja analysoidaan eri tilatyyppien erityisvaatimukset.

4.1 Vyöhykejaon periaatteet ja tilaturvallisuuden tasot

Tehdasalueen sisätilat jaetaan eri turvallisuusvyöhykkeisiin niiden sisältämän riskin ja kriittisyyden perusteella. Valtiovarainministeriön VAHTI-ohje (2013) ja Katakri (2020) määrittelevät neliportaisen jaon, jota sovelletaan teollisuusympäristöön seuraavasti:

1. Julkinen vyöhyke (Public Zone): Tilat, joihin on pääsy ilman erityistä valvontaa (esim. portit tai vastaanotto).
2. Perusvyöhyke (Basic Zone): Yleiset tuotanto- ja toimistotilat, joihin pääsy vaatii työntekijätunnisteen.
3. Rajoitettu vyöhyke (Restricted Zone): Tilat, joissa käsitellään luottamuksellista tietoa tai kriittistä tekniikkaa (esim. arkistot ja sähkötilat).
4. Erittäin rajoitettu vyöhyke (Highly Restricted Zone): Kriittisin infrastruktuuri, kuten keskitetyt palvelinhuoneet.

Sähkötieto ry:n ST-ohjeisto 4 (2021) täydentää tätä jakoa määrittelemällä kiinteistö- ja tilaturvallisuuden tasot. Ohjeisto antaa tekniset kriteerit sille, millaisia rakenteellisia ja teknisiä ominaisuuksia kunkin tason tilalta edellytetään, jotta kulunvalvonta on tehokasta.

4.2 IT- ja tietoliikennetilat

Tietoliikenneyhteydet ja palvelimet muodostavat tehtaan "hermoston". Niiden suojaaminen on kriittistä toiminnan jatkuvuuden ja tietoturvan kannalta.

4.2.1 Keskitetyt tietoliikennetilat

Keskitetyt IT-tilat luokitellaan yleensä rajoitetuiksi tai erittäin rajoitetuiksi vyöhykkeiksi (VAHTI 2013). Näissä tiloissa sijaitsevat keskeiset kytkimet ja palvelimet. Pääsynhallinnan on oltava yksilöityä, ja jokaisesta käynnistä on jäätävä lokitieto. Huoltovarmuuskeskus (2025) painottaa, että näiden tilojen fyysinen murtosuojaus on oltava vähintään Finanssialan (2017b) rakenteellisen suojauksen tason 3 mukainen.

4.2.2 Tietoliikennekaapit ja NEC-kaapit (Hajautetut tilat)

Erityinen haaste tehdasympäristössä ovat tietoliikennekaapit ja niin sanotut NEC-kaapit (Network Entry Cabinet), jotka sijaitsevat usein yleisissä tuotantotiloissa tai teknisissä käytävissä. Vaikka tila itsessään olisi perusvyöhykettä, kaapin sisällön on oltava suojattu kuin se olisi rajoitetussa tilassa.

- Suojausperiaate: Kaappien on oltava lukittuja, ja niiden avainhallinta tai sähköinen lukitus on integroitava osaksi kulunvalvontaa. Osa suojausperiaatetta on lukituksen ohella tietoverkkojen ja verkkolaitteiden tietoturva.
- Riski: Hajautettu sijainti lisää fyysisen sabotaasin tai luvattoman kytkennän riskiä, mikä vaatii tiukkaa pääsyrajoitusta vain nimettyjen IT-asentajien välittömään tarpeeseen perustuen.

4.3 Sähkö-, automaatio- ja kaapelitilat

Nämä tilat ovat tehtaan operatiivisen toiminnan kannalta elintärkeitä ja työturvallisuusnäkökulmasta vaarallisia.

ST-ohjeisto 4 (2021) asettaa sähkötiloille korkeat vaatimukset. Pääsy näihin tiloihin on rajattava sähköalan ammattihenkilöille tai opastetuille henkilöille (Työturvallisuuslaki 23.8.2002/738).

- Automaatiotilat: Ohjausjärjestelmien suojaaminen on osa kyberturvallisuutta. Fyysinen pääsy automaatiokaappeihin mahdollistaa prosessien manipuloinnin, minkä vuoksi pääsy on myönnettävä vain asianomaisille kunnossapitohenkilöille.
- Kaapelitilat: Usein unohdettu kohde, jossa sijaitsee tehtaan kriittinen kaapelointi. Nämä on suojattava ilkivallalta ja tulipaloilta (Huoltovarmuuskeskus 2025).

4.4 Kemikaali- ja räjähdysvaaralliset sekä räjähdetilat

Tämä tila-alue on lainsäädännöllisesti erityisesti säädelty. Pääsynhallinta ei ole tässä vain omaisuuden suojaa, vaan se on suoraan sidoksissa suuronnettomuuksien ehkäisyyn. Kyseisten tilojen osalta vaaditaan aina erityinen riskienarviointi.

- Räjähde- ja kemikaalivarastot: Kulkuoikeudet on rajattava minimiin ja kulkuoikeudet ovat kertakäyttöisiä tai uudelleen aktivoitavia. Painelaitelaki (16.12.2016/1144) ja kemikaaliturvallisuusnormit edellyttävät, että tiloihin pääsee vain asianmukaisen koulutuksen saaneet henkilöt.
- AEO-vaatimus: Koska tehtailla käsitellään usein vaarallisia aineita, on Suomen Tullin (2023) AEO-valtuutetun kyettävä luottamaan siihen, että näihin tiloihin ei pääse ulkopuolisia, jotka voisivat aiheuttaa häiriöitä toimitusketjuun.

4.5 Hallinnolliset ja tukitilat

Vaikka näiden tilojen riskitaso on matalampi, ne sisältävät merkittäviä tietoturvariskejä.

- Arkistot: Sisältävät usein yrityssalaisuuksia tai työntekijöiden henkilötietoja (GDPR 2016/679). Arkistojen on oltava murtosuojattuja ja pääsyn on perustuttava nimenomaiseen hallinnolliseen tarpeeseen.
- Tulostinhuoneet: Tulosteet, joita ei noudeta heti, muodostavat tietovuotoriskin. Vaikka tila on usein työntekijöille avoin, pääsy on syytä rajata vain kyseisellä osastolla työskenteleville, jotta asiattomien liikkumista valvotaan. Erityisesti tilat, joissa käsitellään AEO:n alaisia tuonti- ja vientiasiakirjoja tulee olla kulunvalvottuja.

4.6 Tilatyyppien ja turvallisuustasojen yhteenveto

Seuraava taulukko tiivistää eri tilojen vaatimukset perustuen Finanssialan (2017) ja ST-ohjeiston (2021) tasoihin:

Taulukko 3 Tilojen vaatimukset

Tilatyyppi	**Vyöhyke (VAHTI)**	**Murtosuojaus (FA)**	**Keskeinen pääsyperuste**
IT-tilat	Erittäin rajoitettu	Taso 3-4	Vain IT-ylläpito
NEC-kaapit	Perus (kaappi lukittu)	Taso 2-3)	Vain nimetty huolto
Sähkötilat	Rajoitettu	Taso 2	Sähkötyöoikeudet
Kemikaalitilat	Erittäin rajoitettu	Taso 2-3	Erityiskoulutus & tarve
Arkistot	Rajoitettu	Taso 2-3	Hallinnollinen tarve
Tuotantotilat	Perusvyöhyke	Taso 1-2	Työsuhde

4.7 Tilojen suojaamisen erityispiirteet

Suojaustason valinnassa on huomioitava myös Finanssialan (2017) ohje murtoriskien arvioinnista. Jos tilassa säilytetään esimerkiksi kemikaaleja, joilla on korkea jälleenmyyntiarvo tai sabotaasiarvo, suojaustasoa on nostettava riskienarvioinnin perusteella, vaikka tila ei olisi IT-tila. Valtioneuvoston ohje riskienhallintaan muistuttaa, että turvallisuustasojen on oltava johdonmukaisia läpi organisaation; yksi heikko lenkki (kuten lukitsematon NEC-kaappi perusvyöhykkeellä) voi vaarantaa koko järjestelmän eheyden.

5 Fyysisen ja teknisen suojauksen menetelmät

Kun tehdasalueen tilat on luokiteltu niiden kriittisyyden mukaan, on määritettävä ne konkreettiset menetelmät, joilla pääsyä rajoitetaan ja valvotaan. Suojauksen on oltava tasapainossa: liian kevyt suojaus vaarantaa omaisuuden ja turvallisuuden, kun taas liian raskas suojaus haittaa operatiivista toimintaa. Huoltovarmuuskeskus (2025) korostaa, että fyysisen suojauksen on oltava kerroksellista, jotta yhden suojatason pettäminen ei johda koko järjestelmän murtumiseen.

5.1 Rakenteellinen murtosuojaus

Rakenteellinen suojaus muodostaa fyysisen esteen luvattomalle pääsylle. Sen ensisijainen tehtävä on viivyttää tunkeutujaa riittävän pitkään, jotta hälytys ehditään havaita ja siihen ehditään reagoida (Finanssiala 2017b).

5.1.1 Ovet, seinät ja lukitus

Tehdasympäristössä sisätilojen rakenteellinen kestävyys vaihtelee tilan käyttötarkoituksen mukaan.

- Kriittiset tilat (IT, sähkö, kemikaalit): Näiden tilojen ovien ja seinien on täytettävä vähintään murtosuojaluokan 3 vaatimukset (Finanssiala 2017b). Tämä tarkoittaa vahvistettuja ovirakenteita, jotka kestävät mekaanista murtamista ja työkaluja.
- Lukitusjärjestelmät: Mekaaninen lukitus on usein perussuoja, mutta tehdasympäristössä se on lähes aina korvattu tai täydennetty sähkömekaanisella lukituksella. Turva-alan yrittäjät ry (2019) muistuttaa, että lukituksen on oltava viranomaisten hyväksymä ja vastattava tilan muuta suojaustasoa.
- Heikkojen lenkkien hallinta: Erityistä huomiota on kiinnitettävä teknisiin läpivienteihin, ilmanvaihtokanaviin ja alakattojen yläpuolisiin

tiloihin, joita pitkin tunkeutuminen rajoitettuun tilaan on mahdollista, vaikka ovi olisi lukittu (Katakri 2020).

5.1.2 Hajautetut kohteet (NEC-kaapit ja kotelot)

Koska kaikki tietoliikennelaitteet eivät sijaitse varsinaisissa IT-tiloissa, on kaappien ja koteloiden rakenteellinen suojaus elintärkeää. Valtiovarainministeriö (2013) ohjeistaa, että tällaiset kaapit on ankkuroitava kiinteisiin rakenteisiin ja niiden on oltava varustettu murtosuojatulla lukituksella, joka on kytketty keskitettyyn valvontaan.

5.2 Tekninen kulunvalvonta ja tunnistautuminen

Tekninen kulunvalvonta mahdollistaa yksilöllisen ja dynaamisen pääsynhallinnan. Se korvaa perinteiset avaimet digitaalisilla tunnisteilla, joiden oikeuksia voidaan muuttaa reaaliajassa.

5.2.1 Tunnistautumismenetelmät

Pääsyn varmistaminen perustuu yleensä yhteen tai useampaan seuraavista tekijöistä:

1. Mitä käyttäjällä on: RFID-tunniste, älykortti tai mobiilitunniste.
2. Mitä käyttäjä tietää: PIN-koodi tai salasana.
3. Mitä käyttäjä on: Biometrinen tunniste (sormenjälki, iiris).

Tehdasympäristön korkean turvallisuustason tiloissa, kuten IT-, kemikaali- tai räjähdysvaarallisissa tiloissa, on suositeltavaa käyttää monivaiheista tunnistautumista (Multi-Factor Authentication, MFA). ST-ohjeisto 4 (2021) suosittelee, että kriittisissä kohteissa yhdistetään fyysinen tunniste ja henkilökohtainen koodi, jolloin kadonnut tunniste ei yksinään mahdollista pääsyä.

5.2.2 Järjestelmän hallinta ja lokitus

Kulunvalvontajärjestelmän tuottama lokitieto on keskeistä sekä turvallisuuden että lainsäädännön kannalta. GDPR (2016/679) vaatimukset on huomioitava siten, että lokitietoja käytetään vain ennalta määriteltyihin tarkoituksiin, kuten rikosten selvittämiseen tai työturvallisuuden varmistamiseen. Lokitiedot mahdollistavat myös "välittömän tarpeen" jälkikäteisen auditoinnin: jos työntekijä pyrkii tilaan, johon hänellä ei pitäisi olla työtehtävien mukaista asiaa, järjestelmään jää tästä jälki (Valtioneuvoston ohje riskienhallintaan).

5.3 Kameravalvonnan rooli pääsynhallinnassa

Kameravalvonta ei ole suora este, mutta se on olennainen osa valvontaketjua. Se toimii ennaltaehkäisevänä pelotteena, hälytysten varmistajana ja jälkikäteisenä todisteena.

Turva-alan yrittäjät ry:n Kameravalvontaopas (2020) painottaa, että kameroiden sijoittelun on oltava strategista:

- Sisäänkäynnit ja siirtymät: Kameroiden tulee kuvata henkilöt, jotka siirtyvät perusvyöhykkeeltä rajoitetulle vyöhykkeelle (esim. IT-tilaan johtava ovi).
- Kriittiset laitteet: Valvonta on kohdistettava suoraan kohteisiin, joiden vaurioittaminen on kriittistä, kuten IT tilat, NEC-kaapit tai automaatiotilat.
- Integraatio: Nykyaikainen turvallisuusjärjestelmä yhdistää kulunvalvonnan ja kameravalvonnan. Kun ovi avataan tunnisteella, järjestelmä voi tallentaa videoleikkeen tai ottaa kuvan sisääntulijasta, jolloin voidaan varmistua, ettei tunnisteen käyttäjä ole joku muu kuin sen oikea omistaja (Turva-alan yrittäjät ry 2020).

5.4 Yksityiset turvallisuuspalvelut ja hälytysvaste

Tekniset järjestelmät vaativat tuekseen inhimillistä toimintaa. Laki yksityisistä turvallisuuspalveluista (21.8.2015/1085) luo raamit sille, miten vartiointipalveluita voidaan käyttää tehdasalueella.

- Hälytyskeskuspalvelut: Kulunvalvontajärjestelmän hälytykset (esim. "ovi auki liian pitkään" tai "pääsy evätty useasti") on ohjattava valvomon tai hälytyskeskuksen tietoon.
- Piirivartiointi: Vartijat voivat suorittaa tarkastuskierroksia erityisesti sellaisissa sisätiloissa, joissa ei ole jatkuvaa miehitystä, kuten etäällä sijaitsevissa kaapelihuoneissa tai arkistoissa.
- Oikeudet ja velvollisuudet: Vartijan rooli on suojata toimeksiantajan omaisuutta ja valvoa pääsyä. Tämä on erityisen tärkeää poikkeustilanteissa, kuten tulipalon tai onnettomuuden sattuessa, jolloin kulunvalvonta saattaa joutua hätäaukaisutilaan (Työturvallisuuslaki 23.8.2002/738).

Taulukko 4 Suojauksen tekninen kokonaisuus

Suojausmenetelmä	**Tarkoitus**	**Keskeinen viite**
Mekaaninen este	Viivyttää tunkeutumista (ovet, lukot)	Finanssiala 2017b
Elektroninen tunnistus	Varmistaa oikeus pääsyyn (RFID, mobiili)	ST-ohjeisto 4
Kuvatallennus	Todentaa tapahtumat ja ennaltaehkäisee	Kameravalvontaopas 2020
Hälytyssiirto	Mahdollistaa nopean reagoinnin	Huoltovarmuuskeskus 2025

6 Ohjeistus: Sisäkulkuoikeuksien myöntämisperusteet

Sisäkulkuoikeuksien hallinnan perusperiaatteena on **välitön tarve**. Tämä tarkoittaa, että työntekijälle ei myönnetä oikeuksia tiloihin varmuuden vuoksi tai hierarkkisen aseman perusteella vaan ainoastaan niiden tehtävien suorittamiseksi, jotka kuuluvat hänen aktiiviseen työnkuvaansa. Valtiovarainministeriö (2017) korostaa, että hallitsematon oikeuksien kertyminen on yksi merkittävimmistä sisäisistä turvallisuusriskeistä.

6.1 Kulkuoikeuksien hallintaprosessi ja vastuut

Tehdasalueen kulkuoikeuksien hallinta edellyttää selkeää vastuunjakoa. Prosessi on jaettava kolmeen rooliin, jotta varmistetaan riittävä valvonta ja eturistiriitojen välttäminen (Katakri 2020):

1. Oikeuden omistaja (Substanssivastaava): Esimerkiksi IT-päällikkö vastaa IT-tilojen oikeuksista ja sähkökäytönjohtaja sähkötilojen oikeuksista. Hänellä on paras asiantuntemus arvioida, onko hakijalla todellinen tarve päästä tilaan.
2. Myöntäjä (Turvallisuusorganisaatio): Henkilö tai osasto, joka teknisesti toteuttaa oikeuden järjestelmään oikeuden omistajan hyväksynnän jälkeen.
3. Hakija (Esimies): Työntekijän lähiesimies, joka todentaa työtehtävän tarpeellisuuden.

6.2 Yleiset myöntämisperusteet (Välitön tarve)

Kulkuoikeuden myöntämisen on täytettävä aina vähintään kaksi kriteeriä: asiallinen yhteys ja pätevyys.

- Asiallinen yhteys: Työntekijällä on tehtävä, jota ei voi suorittaa ilman pääsyä kyseiseen tilaan. Esimerkiksi siivoojalla on tarve päästä toimistoon, mutta IT-konesaliin vain, jos se on erikseen aikataulutettu ja valvottu suorite (Valtiovarainministeriö 2013).
- Pätevyys ja perehdytys: Erityisesti sähkö-, kemikaali- ja räjähdysvaarallisissa sekä räjähdetiloissa pelkkä työtehtävä ei riitä. Hakijalla on oltava voimassa olevat pätevyydet (esim. sähkötyöturvallisuuskortti) ja tilaan liittyvä turvallisuusperehdytys (Työturvallisuuslaki 23.8.2002/738).

6.3 Kulkuoikeusryhmät ja roolipohjainen hallinta

Jotta kulkuoikeuksien hallinta pysyisi mahdollisimman johdonmukaisena, tulisi hyödyntää roolipohjaista pääsynhallintaa (Role-Based Access Control, RBAC). Tällöin oikeuksia ei jaeta yksittäin, vaan ne on sidottu työrooliin. Roolipohjaisesti annetaan työtehtävään liittyvät peruskulkuoikeudet. Tarvittavat erityiskulkuoikeudet on haettava erikseen ja ne myönnetään erillisellä päätöksellä josta tulee jäädä lokikirjaus.

Esimerkkejä kulkuoikeusrooleista

- Kunnossapito (Sähkö): Pääsy perusvyöhykkeelle sekä sähkö- ja kaapelitiloihin mutta ei pääsyä IT-palvelinhuoneisiin tai arkistoihin.
- IT-ylläpito: Pääsy perusvyöhykkeelle, palvelinhuoneisiin sekä kaikkiin NEC-kaappeihin.
- Tuotantohenkilöstö: Pääsy vain kyseisen tuotantolinjan tiloihin ja sosiaalitiloihin.
- Ulkopuoliset urakoitsijat: Oikeudet rajataan ajallisesti ja paikallisesti vain työskentelyalueelle tehtävän mukaisesti. (Suomen Tulli 2023, AEO-vaatimukset).

6.4 Erikoiskohteiden erityisperusteet

Tietyissä tiloissa kynnys oikeuden myöntämiseen on huomattavasti korkeampi:

- Tietoliikennekaapit ja NEC-kaapit: Koska nämä sijaitsevat hajautetusti, oikeus myönnetään vain IT-henkilöstölle ja ulkopuolisille verkkotoimittajille erillisellä luvalla. Pääsyn on oltava valvottua sekä jäljitettävää (ST-ohjeisto 4 2021).

- Erityistä vaaraa aiheuttavat- tai räjähdetilat: Oikeus myönnetään vain nimetyille vastuuhenkilöille. Satunnainen käyntitarve hoidetaan aina saattajan kanssa, eikä pysyvää kulkuoikeutta myönnetä (Painelaitelaki 16.12.2016/1144).

6.5 Kulkuoikeuksien elinkaaren hallinta

Oikeuksien myöntäminen on vain osa prosessia. Huoltovarmuuskeskus (2025) ja GDPR (2016/679) edellyttävät myös elinkaariajattelua:

1. Haku ja hyväksyntä: Kirjallinen tai sähköinen hakuprosessi, josta jää auditointijälki.
2. Määräaikainen tarkastus: Oikeuden omistajien on tarkastettava vähintään kerran vuodessa tai riskiarvion perusteella, onko kaikilla listatuilla henkilöillä edelleen tarve pääsyyn. Tarkastuksesta tulee olla suunnitelmallinen muistutus.
3. Välitön poistaminen: Työsuhteen päättyessä tai tehtävänkuvan muuttuessa oikeudet on poistettava viipymättä. Tämä on kriittistä erityisesti AEO-statuksen säilyttämiseksi (Suomen Tulli 2023).

6.6 Poikkeustilanteet ja tilapäiset oikeudet

Poikkeustilanteet, kuten laiterikot tai tulipalot, vaativat omat menettelytapansa:

- Hätäpääsy: Turvallisuusvalvomo voi avata ovia etänä varmistuttuaan henkilön henkilöllisyydestä ja tarpeesta (esim. pelastuslaitos).
- Vierailijat: Vierailijoille ei koskaan myönnetä itsenäisiä kulkuoikeuksia rajoitetuille tai erittäin rajoitetuille vyöhykkeille. Heidän on liikuttuttava aina isännän saattamana (Turva-alan yrittäjät ry 2019).

Taulukko 5 Tiivistetty ohjetaulukko myöntämisperusteista

Tila / Kohde	**Pääasiallinen peruste**	**Lisävaatimus**
Perusvyöhyke	Voimassa oleva työsuhde/sopimus	Yleinen turvallisuusperehdytys
IT-tilat ja NEC	IT-ylläpitotehtävät	Salassapitositoumus (NDA)
Sähkö- ja automaatiotilat	Kunnossapitotehtävät	Sähköturvallisuuslakiin perustuva pätevyys
Kemikaalitilat	Prosessinvalvonta / Kemikaalien käsittely	Erityinen kemikaaliturvallisuusperehdytys
Arkistot	Hallinnollinen / Juridinen tehtävä	Tiedonhallintalain mukainen tarve

6.7 Kulkuoikeusmatriisi

Taulukko 6 Kulkuoikeusmatriisi

Tila / Henkilöstöryhmä	Hallinto /Johto	Tuotantohenkilöstö	Kunnossapito (oma)	IT-ylläpito	Varasto / Logistiikka	Laboratoriohenkilöstö	Vakituiset urakoitsijat	Satunnaiset urakoitsijat
Toimisto & Yleiset tilat	K	T	K	K	K	K	K	T
Tuotantoalueet	K	K	K	K	K	K	K	T
LVI & tekniset tilat	-	-	K	T	-	-	K	T
Sprinkleritilat	-	-	K	K	-	-	K	T
Sähkö- ja IT-tilat /NEC	-	-	K	K	-	-	K	S
Tuotevarasto (AEO)	T	-	T	T	K	T	T	S
Varastopalvelut (Saapuva)	T	T	T	T	K	-	T	S
Laboratorio	T	T	T	T	T	K	T	S

(QC & R&D)								
Kemikaali ja räjähdetilat	-	T	T	-	T	K	S	S

Merkintöjen selitykset:

- K (Kulkuoikeus): Pysyvä oikeus, perustuu jatkuvaan työtehtävään.
- T (Tarveperusteinen): Oikeus aktivoidaan erillisen pyynnön tai työmääräimen perusteella tietyksi ajaksi.
- S (Saattajavelvoite): Pääsy sallittu vain isännän valvonnassa.
    - (Ei pääsyä): Ei perusteltua tarvetta pääsyyn.

6.8 Tilakohtaiset myöntämisperusteet ja erityisvaatimukset

Pääsynhallinnan toteuttaminen tehdasympäristössä vaatii yksityiskohtaista ymmärrystä kunkin tilan käyttötarkoituksesta, siellä sijaitsevista riskeistä sekä tilaa säätelevästä lainsäädännöstä. Seuraavassa esitetään yksityiskohtaiset perusteet kulkuoikeuksien myöntämiselle tehdasalueen kriittisissä sisätiloissa.

6.8.1 Laboratoriotilat (Laadunvalvonta ja Tutkimus ja kehitys)

Laboratoriot ovat kriittisiä ympäristöjä, joissa yhdistyvät työturvallisuusriskit, omaisuuden suoja ja immateriaalioikeuksien turvaaminen.

- Pääsynhallinnan perusteet: Pääsy myönnetään ensisijaisesti laboratoriohenkilöstölle. Muiden ryhmien (kuten kunnossapito) pääsy on aina tarveperusteista (T) ja vaatii usein tilakohtaisen turvallisuusperehdytyksen (Työturvallisuuslaki 23.8.2002/738).
- Tietoturva ja Katakri: Tuotekehityslaboratorioissa (T&K) käsitellään yrityssalaisuuksia. Katakri (2020) ja VAHTI (2013) edellyttävät, että tällaiset tilat ovat erittäin rajoitettuja vyöhykkeitä, joissa pääsyä valvotaan ja lokitetaan aukottomasti.

- Kemikaaliturvallisuus: Laboratorioissa käsiteltävät vaaralliset aineet vaativat pääsyn rajoittamista vain koulutetulle henkilöstölle onnettomuusriskien minimoimiseksi.

6.8.2 LVI- ja tekniset tilat (mukaan lukien turvatekniset tilat)

Tekniset tilat muodostavat tehtaan infrastruktuurin selkärangan.

- Kriittisyys ja Huoltovarmuus: Huoltovarmuuskeskus (2025) painottaa, että teknisten tilojen suojaus on avainasemassa toiminnan jatkuvuuden kannalta. Turvateknisten tilojen pääsynhallinta on erityisen kriittistä: luvaton pääsy ja laitteiston manipulointi voi estää esimerkiksi automaattisen palonsammutuksen (Turva-alan yrittäjät ry 2019).
- Turvallisuusnormit: Lämpökeskusten ja muiden painelaitteita sisältävien tilojen pääsyä säätelee Painelaitelaki (16.12.2016/1144), joka edellyttää pääsyn rajoittamista vain päteville ja opastetuille henkilöille.

6.8.3 Tuotevarastot ja logistiikan tilat (AEO)

Logististen tilojen pääsynhallinta on suoraan sidoksissa yrityksen kaupallisiin toimintaedellytyksiin.

- Tullin vaatimukset: Suomen Tullin (2023) AEO-valtuutettu talouden toimija -status edellyttää, että tuotevarastot ja lähetysalueet on suojattu luvatonta pääsyä vastaan. Kulkuoikeuksien on oltava rajattuja, ja vierailijoiden (kuten kuljettajien) liikkumista on valvottava tiukasti.

6.8.4 Varasto- ja materiaalipalvelut

- Omaisuuden suojaus: Murtoriskien arvioinnissa varastot luokitellaan usein korkean houkuttelevuuden kohteiksi. Suojaustasot määritellään Finanssialan (2017) ohjeiden mukaan ja niissä korostetaan teknisen kulunvalvonnan ja kameravalvonnan integraatiota epäilyttävän toiminnan havaitsemiseksi reaaliajassa.
- Toimistotilat ja yleiset tilat
- Vaikka toimistotilat mielletään usein matalan riskin alueiksi, ne sisältävät merkittäviä tietoturvauhkia.
- Tietosuoja (GDPR): Toimistotiloissa käsitellään henkilötietoja ja sopimuksia. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679

velvoittaa organisaation suojaamaan nämä tiedot. Pääsynhallinnalla varmistetaan, ettei tiloissa liiku ylimääräisiä henkilöitä ilman valvontaa.

- Arkistot ja tulostinhuoneet: Näiden tilojen kulunhallinta on osa fyysistä tietoturvaa, jolla estetään luottamuksellisen aineiston joutuminen vääriin käsiin. Pääsynhallinnan on perustuttava nimenomaiseen hallinnolliseen tarpeeseen ja vierailijoiden liikkuminen on oltava aina valvottua (Valtiovarainministeriö 2013).

6.8.5 Sähkö- ja automaaatiotilat

- Pätevyysperusteisuus: Pääsy sähköpääkeskuksiin ja muuntamoihin myönnetään vain sähköalan ammattihenkilöille tai heidän opastamilleen henkilöille. ST-ohjeisto 4 (2021) asettaa tekniset standardit näiden tilojen luokitukselle. Vääränlainen toiminta sähkötilassa voi johtaa välittömään hengenvaaraan tai laajaan tuotantoseisokkiin.
- Automaation suojaaminen: Tehtaan ohjausjärjestelmät sijaitsevat usein näissä tiloissa. Fyysinen pääsy on rajattava tiukasti kunnossapidon asiantuntijoille, jotta estetään ohjelmistoihin tai kytkentöihin kohdistuvat luvattomat muutokset, jotka voisivat sabotoida tuotantoprosessia.

6.8.6 IT-tilat ja hajautetut tietoliikennekaapit (NEC)

Tietoliikenneyhteydet ovat digitaalisen tehtaan perusedellytys ja niiden suojaaminen on usein tietoturvan haavoittuva lenkki.

- Tuotantotiloissa sijaitsevat NEC-kaapit on suojattava samalla periaatteella kuin keskitetyt palvelinhuoneet. Vaikka tila itsessään olisi perusvyöhykettä, on kaapin oman lukituksen vastattava rajoitetun tilan vaatimuksia (Vahti 2013; Katakri 2020)
- Identiteetin ja eheyden varmistus: IT-tilojen kulkuoikeudet rajataan vain nimetyille ylläpitohenkilöstölle. Jokainen käynti on kyettävä varmentamaan jälkikäteen lokitietojen avulla Valtiovarainministeriö (2017). Tämä on kriittistä vikatilanteiden selvittämisessä ja mahdollisten tietomurtoyritysten havaitsemisessa.

6.9 Ohjeistuksen yhteenveto ja jalkauttaminen

Tämä ohjeistus luo perustan sille, miten tehdasalueen sisäturvallisuutta johdetaan. Sen toteuttaminen vaatii:

1. Laki- ja lupaperusteet: Kaikkien toimien on perustuttava tunnistettuun riskiin ja lain suomaan oikeuteen käsitellä kulkutietoja.
2. Hallinnolliset ja toiminnalliset prosessit: Säännölliset kulkuoikeuksien tarkastukset ja välitön oikeuksien poistaminen työsuhteen päättyessä (Valtioneuvoston ohje riskienhallintaan).
3. Tekniset järjestelmät: Pääsynhallinnan tekninen toteutus nojaa kerrokselliseen suojaukseen, joka pitää sisällään sähköisen kulunvalvonnan, murtosuojauksen sekä kameravalvonnan. Teknisten järjestelmien jatkuva toimivuus varmistetaan säännöllisellä kunnossapidolla ja varavirransyötöllä (UPS), jotta suojaustaso säilyy myös sähkökatkojen aikana.
4. Käyttäminen ja hallinta: Käyttäjien perehdyttäminen ja selkeä ohjeistus muodostavat merkittävän osan järjestelmän todellisesta turvallisuustasosta. Osa turvallisuudesta jää toteutumatta, mikäli loppukäyttäjät eivät tunne tai noudata ohjeistusta.

7 Johtopäätökset ja pohdinta

Tämän opinnäytetyön tavoitteena oli laatia selkeä ja johdonmukainen ohjeistus tehdasalueen sisäkulkuoikeuksien myöntämisperusteille. Työssä on analysoitu laajasti eri tilatyyppien suojaustarpeita, lainsäädännöllisiä vaatimuksia sekä teknisiä ja hallinnollisia menetelmiä, joilla pääsynhallintaa toteutetaan. Johtopäätöksissä tarkastellaan, miten työlle asetetut tavoitteet saavutettiin ja millainen vaikutus luodulla ohjeistuksella on tehtaan kokonaisturvallisuuteen.

7.1 Tulosten yhteenveto ja tavoitteiden toteutuminen

Opinnäytetyön keskeisin tulos on luvussa 6 esitetty ohjeistus, joka perustuu välitön tarve -periaatteeseen. Työn aikana kävi ilmeiseksi, että tehdasympäristössä ei voida nojata yhteen yleiseen suojaustasoon, vaan tilat on luokiteltava niiden kriittisyyden ja riskien perusteella (Finanssiala 2017; ST-ohjeisto 4 2021).

Laadittu ohjeistus vastaa asetettuihin tutkimuskysymyksiin:

1. Luokittelu: Tilat on jaettu vyöhykkeisiin (VAHTI 2013). Erityiskohteet, kuten hajautetut NEC-kaapit ja vaaralliset kemikaalitilat on huomioitu omina erityisryhminään.
2. Myöntämisperusteet: Työ loi standardoidun prosessin, jossa kulkuoikeuden myöntäminen vaatii sekä asiallisen työtehtävään liittyvän perusteen että tarvittavan turvallisuuspätevyyden (Työturvallisuuslaki 23.8.2002/738).
3. Laki- ja standardivastaavuus: Ohjeistus varmistaa, että yritys täyttää AEO-valtuutuksen kriteerit ja GDPR:n vaatimukset lokitietojen hallinnassa.

7.2 Ohjeistuksen merkitys turvallisuuskulttuurille

Onnistunut pääsynhallinta ei ole pelkkä tekninen suorite, vaan se on osa yrityksen turvallisuuskulttuuria. Ohjeistuksen jalkauttaminen selkeyttää työntekijöiden ja urakoitsijoiden rooleja. Kun kaikki ovat tietoisia, miksi tiettyihin tiloihin pääsy on rajoitettu, sitoutuminen turvallisuussääntöihin paranee (Valtioneuvoston ohje riskienhallintaan).

Erityisesti sähkö- ja automaatiotilojen sekä kemikaalivarastojen kohdalla ohjeistus toimii kriittisenä työturvallisuuden varmistajana. Rajoittamalla pääsy vain päteville henkilöille minimoidaan inhimillisen virheen mahdollisuus kohteissa, joissa vahingon seuraukset voisivat olla katastrofaalisia (Painelaitelaki 16.12.2016/1144). Samalla tekninen suojaus, kuten kameravalvonta, toimii paitsi turvana myös työntekijän oikeusturvana mahdollisissa poikkeamatilanteissa (Turva-alan yrittäjät ry 2020).

7.3 Eettiset näkökulmat ja työntekijöiden yksityisyys

Pääsynhallinnan ja kulunvalvonnan kehittäminen vaatii jatkuvaa tasapainoilua turvallisuuden ja yksityisyyden suojan välillä. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 (GDPR) asettaa tiukat rajat sille, miten työntekijöiden liikkumista saadaan seurata. Tätä säädöstä täydentää kansallinen laki yksityisyyden suojasta työelämässä (759/2004), joka määrittelee tarkasti teknisen valvonnan reunaehdot suomalaisilla työpaikoilla.

Pohdinnassa on huomioitava seuraavat eettiset ja juridiset periaatteet:

- Valvonnan kohdistaminen: Valvonta on kohdistettava kohteisiin (kuten kriittisiin IT-tiloihin tai kemikaalivarastoihin), ei yksittäisiin työntekijöihin.
- Tarpeellisuus ja YT-menettely: Kansallisen lain (759/2004) mukaisesti valvonnan on oltava välttämätöntä turvallisuuden tai omaisuuden suojaamiseksi ja sen toteuttamisesta on käytävä avoin vuoropuhelu henkilöstön kanssa ennen järjestelmän käyttöönottoa.
- Lokitietojen käyttö: Lokitietojen käyttö on rajattava vain turvallisuuspoikkeamien selvittämiseen. Niitä ei tule käyttää työntekijöiden päivittäisen suorituksen tai työajan tarkkailuun.
- Avoimuus ja tiedottaminen: Nämä ovat avainasemassa, jotta valvonta ei tunnu ahdistavalta tai perusteettomalta (Turva-alan yrittäjät ry

2020). Kun työntekijät ymmärtävät valvonnan perusteet, sitoutuminen yhteiseen turvallisuuskulttuuriin paranee.

7.4 Luotettavuus ja työn hyödynnettävyys

Työn luotettavuus perustuu laajalle lähdeaineistolle, joka kattaa niin kansallisen lainsäädännön, kansainväliset standardit kuin toimialakohtaiset asiantuntijaohjeet. Huoltovarmuuskeskuksen (2022) ja Katakrin (2020) hyödyntäminen varmistaa, että esitetyt linjaukset ovat valtiollisen tason turvallisuusvaatimusten mukaisia.

Tämä lopputyö on hyödynnettävissä teollisuuslaitoksissa, jotka haluavat auditoida nykyiset käytäntönsä tai rakentaa uuden pääsynhallintajärjestelmän. Erityisesti ohjeistuksen jaottelu eri vyöhykkeisiin ja tilatyyppeihin tarjoaa valmiin matriisin kulkuoikeusryhmien määrittelyyn.

7.5 Jatkokehitysehdotukset ja tulevaisuuden näkymät

Tässä työssä luotu ohjeistus on vankka perusta nykyhetken tarpeisiin. Turvallisuuden hallinnan on oltava kuitenkin jatkuva hallintaprosessi, joka mukautuu toimintaympäristön ja uhkakuvien muutoksiin. Teknologian kehitys tuo uusia mahdollisuuksia ja uhkia sisäkulkuoikeuksien hallintaan. Jatkokehityskohteina voitaisiin tutkia esimerkiksi:

- Biometrisen tunnistuksen laajentaminen: Miten sormenjälki- tai kasvojentunnistus voitaisiin integroida tietosuojaystävällisesti kriittisimpiin kohteisiin (ST-ohjeisto 4 2021).
- Tekoälypohjainen analytiikka: Poikkeavien kulkujen automaattinen tunnistaminen, joka voisi ennaltaehkäistä esimerkiksi teollisuusvakoilua. Järjestelmä voisi antaa automaattisen hälytyksen esimerkiksi, jos työntekijä yrittää päästä epätyypillisiin tiloihin poikkeavana kellonaikana tai jos samaa tunnistetta käytetään epäloogisen nopeasti eri puolilla tehdasaluetta.
- Mobiilikulunhallinta: Fyysisistä korteista luopuminen ja siirtyminen dynaamisiin mobiilitunnisteisiin, jotka mahdollistavat entistä tarkemman ajallisen ja paikallisen rajauksen.

7.6 Loppusanat

Sisäkulkuoikeuksien hallinta on jatkuva prosessi, joka vaatii säännöllistä ylläpitoa ja reagointikykyä. Tässä työssä laadittu ohjeistus tarjoaa vankan perustan tehdasalueen turvallisuudelle. Sen todellinen vaikuttavuus riippuu kuitenkin viime kädessä organisaation sitoutumisesta määritettyjen periaatteiden noudattamiseen ja päivittämiseen.

Turvallisuusketju on niin vahva kuin sen kriittisin tekijä – ihminen. Tämän ohjeistuksen avulla inhimillistä virheriskiä on pienennetty selkeyttämällä vastuita ja myöntämisperusteita. Kun jokainen organisaation jäsen ymmärtää kulkuoikeuksien rajauksen merkityksen, muodostuu teknisestä valvonnasta ja inhimillisestä toiminnasta saumaton kokonaisuus, joka turvaa tehtaan toiminnan jatkuvuuden kaikissa olosuhteissa.

8 Lähteet:

Euroopan parlamentti ja neuvosto. 2016. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 (yleinen tietosuoja-asetus). Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016R0679

Finanssiala. 2017. Kohteen murtoriskien arviointi ja suojaustason valinta. Saatavissa: https://www.finanssiala.fi/wp-content/uploads/2017/08/Kohteen_murtoriskien_arviointi.pdf

Finanssiala. 2017b. Rakenteellinen murtosuojausohje I. Saatavissa: Rakenteellinen murtosuojausohje I

Huoltovarmuuskeskus. 2025. Fyysisen suojauksen opas. Saatavissa: Fyysisen suojauksen opas

Katakri. 2020. Kansallinen turvallisuusauditointikriteeristö. Ulkoministeriö. Saatavissa: Katakri 2020

Laki yksityisistä turvallisuuspalveluista 21.8.2015/1085. Laki yksityisistä turvallisuuspalveluista | 1085/2015 | Suomen säädöskokoelma | Finlex

Laki yksityisyyden suojasta työelämässä 13.8.2004/759. Laki yksityisyyden suojasta työelämässä | 759/2004 | Lainsäädäntö | Finlex

Painelaitelaki 16.12.2016/1144. https://www.finlex.fi/fi/laki/ajantasa/2016/20161144

SFS-EN ISO/IEC 27001:2022. Tietoturvallisuus, kyberturvallisuus ja tietosuojan varmistaminen. Tietosuojan hallintajärjestelmät. Vaatimukset.

SFS-EN ISO/IEC 27002:2022. Tietoturvallisuus, kyberturvallisuus ja tietosuojan varmistaminen. Tietoturvakontrollit. Vaatimukset.

SFS-ISO 31000:2018. Riskienhallinta. Ohjeet.

Suomen Tulli. 2023. AEO-valtuutettu talouden toimija. Saatavissa: https://tulli.fi/yritykset/asiakkuus/aeo-toimija

Sähkötieto ry. 2021. ST-ohjeisto 4. kiinteistö- ja tilaturvallisuuden tasot. Espoo: Sähköinfo Oy.

Turva-alan yrittäjät ry. 2019. Turvaa oikein -opas. Saatavissa: https://www.turva-alanyrittajat.fi/doc/2019/Turvaa-oikein--opas_v2_0.pdf

Turva-alan yrittäjät ry. 2020. Kameravalvontaopas. Saatavissa: https://www.turva-alanyrittajat.fi/doc/Kameravalvontaopas_2020/Kamera-valvontaopas-2020.pdf

Työturvallisuuslaki 23.8.2002/738. https://www.finlex.fi/fi/laki/ajantasa/2002/20020738

Valtiovarainministeriö. 2013. VAHTI 2/2013 Toimitilojen tietoturvaohje. PDF-dokumentti. Saatavissa RAPORTTI_20130530141501.PDF

Valtiovarainministeriö. 2017. Ohje riskienhallintaan. (Kirjoittanut Kimmo Rousku). Saatavissa: Ohje riskienhallintaan