SUOMEN SOODAKATTILAYHDISTYS
FINNISH RECOVERY BOILER COMMITTEE

**Suomen Soodakattilayhdistys ry**

# Kyberturvallisuuden perusteet soodakattiloiden automaatiojärjestelmissä

**Suvi Kaartinen ja Henry Haverinen**
**Insta Advance Oy**

**7.11.2022**

**Raportti 4/2022**

**(16A0913-E0218)**

KYBERTURVALLISUUDEN PERUSTEET

# SOODAKATTILOIDEN AUTOMAATIOJÄRJESTELMISSÄ

Toiminnanharjoittajan eli järjestelmän omistajan näkökulmasta

**Työn Tilaaja**: Suomen Soodakattilayhdistyksen Automaatiotyöryhmä (ATR)

**Työn tuottajat**: Suvi Kaartinen ja Henry Haverinen, Insta Advance Oy

Versio: 1.4, 12.10.2022

**Huomautus työn hyödyntämisestä**: Tämän materiaalien käyttö on toiminnanharjoittajan **omalla vastuulla** ja raportti liitteineen on tarkoitettu antamaan **vain yleisiä suuntaviivoja kyberturvallisuuden eri aspektien kartoittamiseksi**. Työ keskittyy laitostason suojaukseen, ei konsernitason järjestelmiin. Aineisto ei kata kaikkia 62443 standardin vaatimuksia, vaan näkökulmana on aloituskynnyksen madaltaminen, olemassa olevan aineiston perusteiden esittely, ja muutoshankkeessa onnistuminen. Aineistoa ei aktiivisesti päivitetä, vaan kyseessä on kertaluontoinen projekti.

SISÄLLYSLUETTELO

# 1. JOHDANTO

Tämä työ on tehty Suomen Soodakattilayhdistyksen Automaatiotyöryhmän (ATR) tekemän toimeksiannon pohjalta. Työn tavoitteen on antaa **soodakattilan käyttäjille** (järjestelmän omistajille) perustietoa tietoturvariskien hallinnasta erityisesti riskien tunnistamisen ja kartoittamisen osa-alueilla. Tähän osa-alueeseen halutaan panostaa, koska nykyisessä toimintaympäristössä riskit ovat muodostuneet aiempaa suuremmiksi, eikä sellutehtaan kokoisia valtavia inventointeja haluta vaarantaa kyberturvaongelmien vuoksi.

Soodakattilan automaation liittyvät riskit ja tietoturvan hallintakeinot ovat samankaltaisia kuin teollisuusautomaatiossa yleensä. Soodakattilan automaation riskien tunnistamiseen ja tietoturvallisuuden kehittämiseen voidaan siksi käyttää jo olemassa olevaa aineistoa. Koska Suomen mittakaavassa uusien järjestelmien rakentaminen on harvinaista, painopistealueena tässä on olemassa olevien järjestelmien päivittäminen ja ylläpito.

Tietoturvajulkaisuille ja aineistoille on tyypillistä yleispätevyys, laajuus ja sitä kautta huono lähestyttävyys. Tärkeää asiaa on paljon. Lisäksi tietoturvan hallinta on monimutkainen prosessi, jonka käyttöön ottaminen on hyvä ajatella muutosprojektina. Haasteeksi tuleekin, kuinka tietoturvan hallinnassa päästäisiin käytännössä liikkeelle, ja kuinka muutoksesta saadaan pysyvä. Tämän työn keskeinen näkökulma onkin aloituskynnyksen madaltaminen, olemassa olevan aineiston esittely, ja muutoshankkeessa onnistuminen.

Tätä tekstiä kirjoitettaessa on hyödynnetty etenkin Suomen Automaatioseuran kirjaa “Automaation tietoturva – Kriittisen tuotannon turvaaminen” ja IEC 62443 –standardisarjaa.

## 1.1 Toimintaympäristön kuvaus

Soodakattila on sellutehtaan ydin ja sen toiminta on sellutehtaan tuotannon jatkuvuuden ja turvallisuuden kannalta keskeisessä asemassa. Kuten tyypillistä teollisuuden automaatiolle, soodakattilan kyberturvallisuuden tärkeimmät tavoitteet ovat prosessin saatavilla olon, prosessin häiriintymättömyyden ja turvallisen toiminnan jatkumisen takaaminen. Pohjimmiltaan tässä on kyse jopa henkilöstöturvallisuudesta. Myös tuotantotietojen ja ajotapojen luottamuksellisuus voi olla tärkeää.

Soodakattiloiden automaation liittyy

- turva-automaatiojärjestelmä ja sähkön jakelujärjestelmiä
- kenttälaitteita, joista osa voi olla langattomia
- IoT-järjestelmiä
- kamerajärjestelmiä, kuten tulipesäkamerat ja muut soodakattilaa katsovat kamerat sekä aluekamerat
- Lämpötila- ja paineantureita, jotka voivat olla langallisia tai langattomia

Lisäksi ylätason järjestelmät kommunikoivat automaatiojärjestelmän kanssa – ne voivat osallistua esimerkiksi automaatiojärjestelmän asetusarvojen määrittelyyn tuotantotavoitteiden perusteella. Ulkoiset

rajapinnat ovat riskienhallinnassa ja toiminnan jatkuvuuden takaamisessa keskeisessä roolissa. On suojattava henkilöitä, laitteita ja itse prosessia.

Tärkeimmät suojattavat kohteet tässä ympäristössä ovat (prioriteetin mukaisessa järjestyksessä):

- Henkilöt
- Ympäristö
- Tuotanto-omaisuus (keskeytys- ja omaisuusvahingot)
- Soodakattilan prosessi (saatavilla olo, häiriintymättömyys)
- Apuenergioiden syötöt
- Automaatiojärjestelmä ja turva-automaatiojärjestelmä itsessään
- Tehtaan tietoverkot
- Tuotantotiedot
- Maine

Riskienhallinnassa nämä kaikki kohteet tulisi huomioida riittävän turvallisuustason varmistamiseksi.

Tyypillisiä automaatioympäristöissä meneillään olevia kehityshankkeita ovat:

- IoT-yhteydet ja data-alusta
- Keskitetysti kerättävän datan määrän kasvu
- Langattomat anturit
- Konenäkösovellukset
- Kompleksisuuden jatkuva lisääntyminen, osittain huomaamatta
- Edullisen ja lyhyen elinkaaren teknologian lisääntyminen

Monet näistä kehitysaskelista tuovat mukanaan tietoturvahaasteita – esimerkiksi IoT-puolella tietoturvataso saattaa olla riittämätön siihen nähden, että laitteet ovat yleensä jatkuvasti yhteydessä ulkomaailmaan, ja kuitenkin näitä (ja muita alhaisemman turvatason) laitteita tuodaan enenevässä määrin osaksi automaatiojärjestelmiä.

Toimintaympäristön muutospaineita tulee teknologian kehittymisen lisäksi myös kahdelta muulta suunnalta - lainsäädännöstä ja uhkaympäristön muutoksista. Prosessiturvallisuusstandardeissa (esim. IEC 61511) viitataan kyberturvallisuuteen. Euroopan komission ehdottama koneturvallisuusasetus korvaa aikaisemman konedirektiivin ja tuo kyberturvallisuuden myös koneturvallisuuden osaksi. Standardoinnin, erityisesti IEC 62443-standardardisarjan, merkitys kasvaa. Taustalla tässä on selkeä uhkaympäristön muutos – kyberrikolliset kohdistavat hyökkäykset sinne, missä suojaustaso on matala suhteessa lunnaiden maksukykyyn tai muuhun saavutettavissa olevaan etuun nähden - hyökkäykset automaatiojärjestelmiä kohtaan ovat jatkuvasti kasvussa.

## 1.2 Erot automaatio- ja toimistoympäristöjen välillä

Perinteisessä tietoturvassa on tärkeää tiedon ja sen käsittelyyn liittyvien järjestelmien luottamuksellisuuden, eheyden ja saatavilla olon turvaaminen. Näihin ominaisuuksiin liittyviä uhkakuvia ja tyypillisiä hallintakeinoja on lueteltu taulukossa Taulukko 1.

| Kuvaus | Saavuttamista tukevia keinoja | Tyypillisiä uhkakuvia |
|---|---|---|
| Tiedon luottamuksellisuus | Tiedon salaaminen, paikalliset palvelimet, pääsyn rajoittaminen | Tietovuodot, kiristäminen, tietosuojarikkomukset (sakot) |
| Tiedon ja järjestelmien eheys | Pääsyn rajoittaminen, järjestelmien valvonta | Tiedon tai järjestelmien muuntelu, prosessien häiriintyminen |
| Tiedon ja järjestelmien saatavilla olo | Kahdennukset, varmuuskopiointi | Haittaohjelmat, järjestelmän ylikuormitus, palvelun kaatuminen |

*Taulukko 1: Tyypillisiä tietoturvaominaisuuksia*

Kyberturvallisuudessa tätä tiedon suojaamiseen keskittyvää lähestymistapaa laajennetaan kattamaan myös muut liitännäisjärjestelmä ja –laitteet. Haavoittuvuus kotitietokoneessa voi johtaa tiedon menettämiseen, kun taas automaatiojärjestelmien yhteydessä vastaavalla tapahtumaketjulla voi olla vaikutuksia liitännäislaitteiden kautta ympäristöön ja ihmisten turvallisuuteen. Tämä kääntää perinteisen tiedon luottamuksellisuutta korostavan lähestymistavan päälaelleen - automaatioympäristössä keskeiseen asemaan nouseekin prosessin saatavilla olon ja häiriintymättömyyden turvaaminen. Seuraavaan taulukkoon (Taulukko 2) on listattu tyypillisiä eroja IT-järjestelmien ja automaatiojärjestelmien tietoturvaan liittyen.

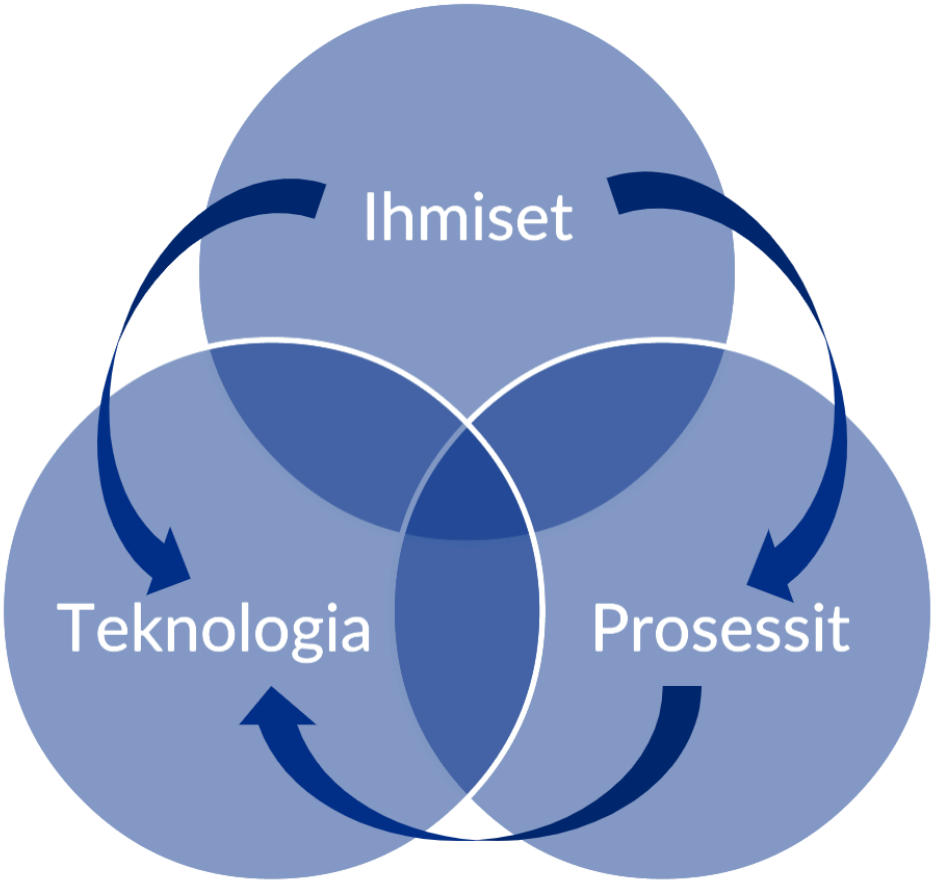
| Osa-alue | IT-tietoturva | Automaation tietoturva |
|---|---|---|
| Standardit | ISO 27001 | IEC 62443 |
| Suojaus-prioriteetit | 1. Tiedon luottamuksellisuus<br>2. Tiedon eheys<br>3. Tiedon saatavilla olo | 1. Prosessin saatavilla olo<br>2. Prosessin eheys<br>3. Tiedon luottamuksellisuus |
| Toimitusketju | IT-osaston hallinnoimat monitoimittajaympäristöt ovat tyypillisiä. | Monitoimittajaympäristöissä tarvitaan yhteistyötä tilaajan ja toimittajien IT- ja automaatio-osastojen kesken. |
| Ihmisten ja ympäristön turvallisuus | Yleensä ei vaikutuksia. | Ihmiset tai ympäristö voivat vaarantua, koska järjestelmä ohjaa fyysistä prosessia ja kriittistä infrastruktuuria. |
| Reaali-aikaisuus | Reaaliaikaisuusvaatimukset eivät yleensä ole ehdottomia. | Prosessista riippuen reaaliaikaisuusvaatimukset voivat olla ehdottomia. |
| Elinkaari | Elinkaaren pituus vaihtelee. | Yleensä hyvin pitkä verrattuna IT-järjestelmiin. |
| Ylläpito | Normaali käytäntö. Suunnitellut huoltokatkot yleensä mahdollisia. | Huoltoikkuna voi toistua harvoin. Käyttökatkot eivät välttämättä ole sallittuja huoltoikkunoiden ulkopuolella. |

*Taulukko 2: Tyypillisiä eroja IT-tietoturvan ja automaation tietoturvan välillä.*

Erilaisten suojausprioriteettien lisäksi automaatioympäristössä korostuvat kompleksiset toimitusketjut, pitkät elinkaaret ja vähäiset käyttökatkojen mahdollisuudet. Nämä kaikki erityispiirteet tulee ottaa huomioon kyberturvallisuuden hallintajärjestelmää rakennettaessa.

# 2. KYBERTURVALLISUUDEN HALLINTA

Monet ihmiset tuntuvat yhä nykypäivänä ajattelevan, että tietoturvallisuus on tietotekninen ongelma, joka voidaan ratkaista tekemällä teknisiä suojaustoimenpiteitä, kuten asentaa tietokoneeseen virustorjuntaohjelmiston. Tämä ajatus ei kuitenkaan päde - hyvä tietoturvallisuus tai kyberturvallisuustaso voidaan saavuttaa vain ihmisten, prosessien ja teknologian yhteispelillä. Nämä osa-alueet tulisi huomioida kyberturvallisuuden hallintajärjestelmää rakennettaessa ja niiden olisi hyvä näkyä myös kyberturvallisuuspolitiikan tasolla.

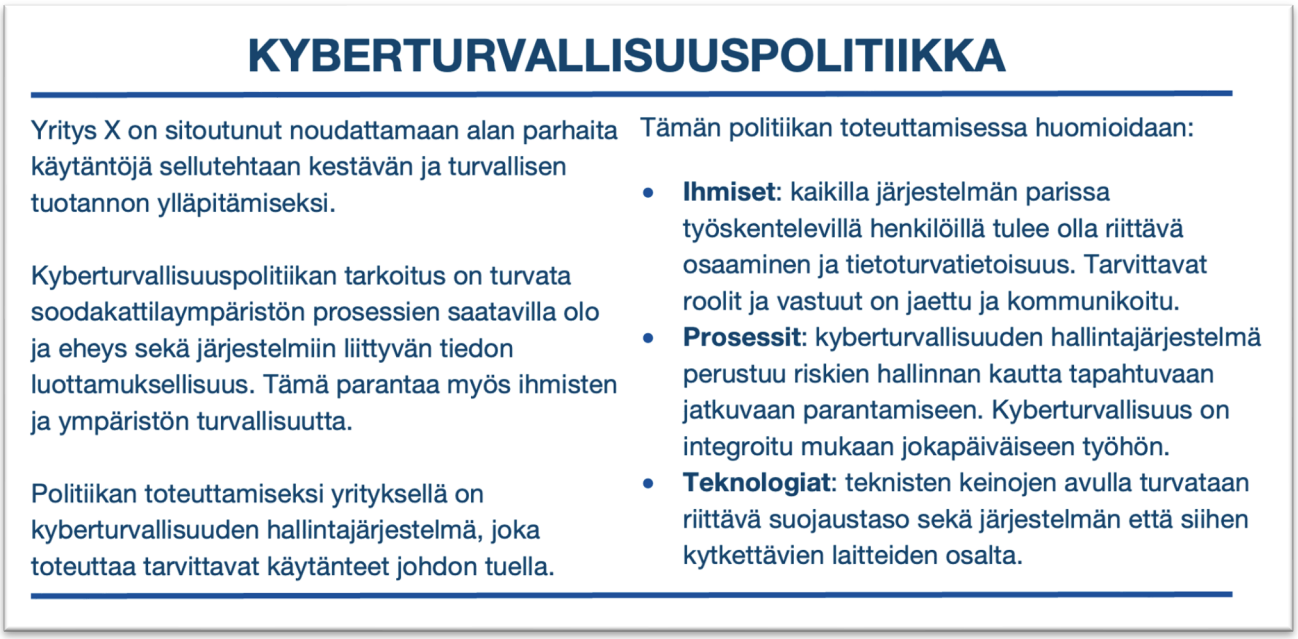



*Kuva 1: Kyberturvallisuuden hallinnassa huomioitavat osa-alueet*

Tämän kolminaisuuden osa-alueet eivät ole toisistaan riippumattomia, vaan sekä teknologiat että prosessit tarvitsevat toimiakseen osaavia ihmisiä, joilla on riittävä tietoturvatietoisuuden taso. Prosessit ovat myös keskeisessä roolissa teknologioiden suhteen, sillä hyväkään teknisen kontrollin suunnittelu ei auta, elleivät prosessit tue sen käyttöönottoa ja ylläpitoa.

Ylätasolla kyberturvallisuuden hallinta lähtee liikkeelle ylimmän johdon hyväksymän kyberturvallisuuspolitiikan määrittelystä. Tämä politiikka olisi hyvä tiivistää esimerkiksi yhteen kalvoon

siten, että siitä käy selkeästi ilmi johdon sitoutuminen, keskeiset tavoitteet sekä kunkin osa-alueen keskeinen rooli kyberturvallisuuden kannalta. Tästä on annettu esimerkki kuvassa Kuva 2.



**KYBERTURVALLISUUSPOLITIIKKA**

Yritys X on sitoutunut noudattamaan alan parhaita käytäntöjä sellutehtaan kestävän ja turvallisen tuotannon ylläpitämiseksi.

Kyberturvallisuuspolitiikan tarkoitus on turvata soodakattilaympäristön prosessien saatavilla olo ja eheys sekä järjestelmiin liittyvän tiedon luottamuksellisuus. Tämä parantaa myös ihmisten ja ympäristön turvallisuutta.

Politiikan toteuttamiseksi yrityksellä on kyberturvallisuuden hallintajärjestelmä, joka toteuttaa tarvittavat käytänteet johdon tuella.

Tämän politiikan toteuttamisessa huomioidaan:

- **Ihmiset**: kaikilla järjestelmän parissa työskentelevillä henkilöillä tulee olla riittävä osaaminen ja tietoturvatietoisuus. Tarvittavat roolit ja vastuut on jaettu ja kommunikoitu.
- **Prosessit**: kyberturvallisuuden hallintajärjestelmä perustuu riskien hallinnan kautta tapahtuvaan jatkuvaan parantamiseen. Kyberturvallisuus on integroitu mukaan jokapäiväiseen työhön.
- **Teknologiat**: teknisten keinojen avulla turvataan riittävä suojaustaso sekä järjestelmän että siihen kytkettävien laitteiden osalta.

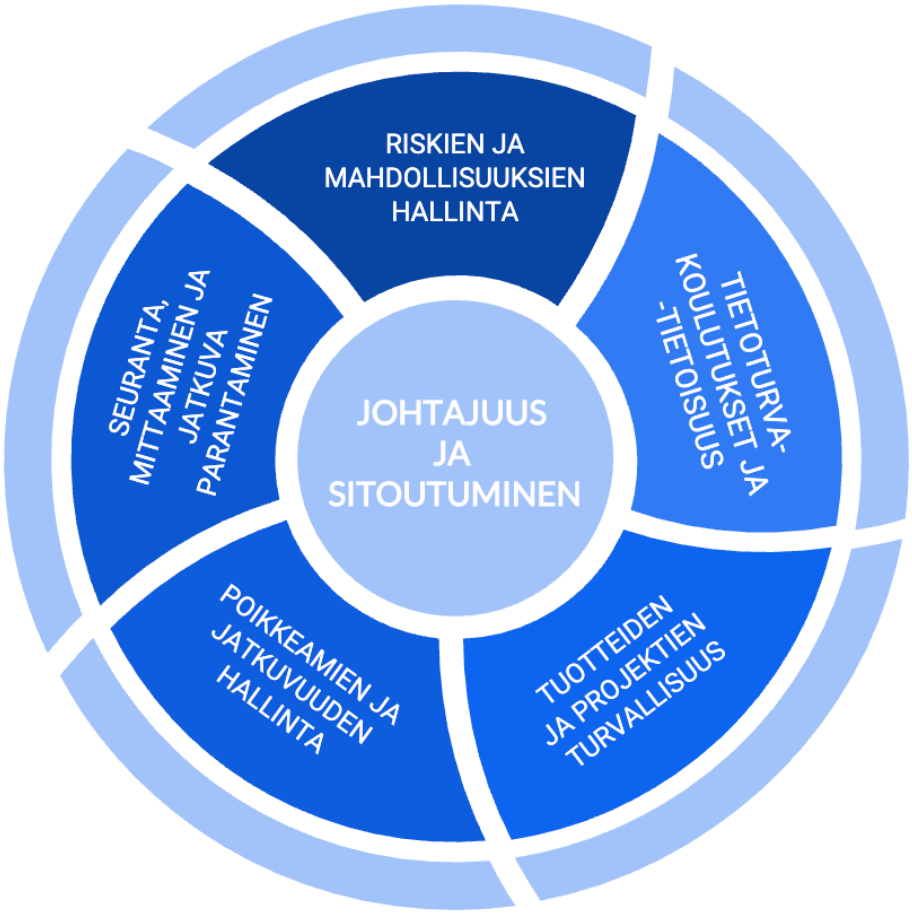
*Kuva 2: Esimerkki kyberturvallisuuspolitiikasta*

Tätä ylätason dokumenttia täydennetään yksityiskohtaisemmilla toimintaperiaatteilla.

Käytännön tasolla kyberturvallisuuden hallinnassa on viisi keskeistä jatkuvaa käytäntöä:

- Riskien ja mahdollisuuksien hallinta
- Riittävän osaamisen ja tietoturvatietoisuuden varmistaminen
- Tuotteiden ja projektien tietoturvallisuuden hallinta
- Poikkeamien ja jatkuvuuden hallinta
- Seuranta, mittaaminen ja hallintajärjestelmän jatkuva parantaminen

Nämä keskeiset osa-alueet on tiivistetty alla olevaan kuvaan.




*Kuva 3: Kyberturvallisuuden hallintamallin keskeiset jatkuvat käytännöt.*

Onnistumisen avain on johdon sitoutumisessa, joka näkyy esimerkiksi riittävien resurssien turvaamisessa ja kyberturvallisuuspolitiikan johtamisena.

## 2.1 Sellutehtaan omistajan näkökulma

Automaatioympäristöjen kyberturvallisuuden tulisi perustua yleisesti tunnustettujen standardien mukaisesti rakennettuun kyberturvallisuuden hallintajärjestelmään, jota varten perustetaan organisaatioon kyberturvallisuusohjelma. Kyberturvallisuusohjelman perustaminen teollisuusautomaatio- ja ohjausjärjestelmiä varten on IEC 62443 standardin osan 2-1 aihe. Tämän standardin mukainen hallintajärjestelmä rakennetaan (ISO 27001 -standardin tapaan) riskien hallinnan ympärille, kolmeen osaa jakautuen:

- Riskianalyysi, jossa tunnistetaan ja arvioidaan riskit liiketoiminnan tarpeista lähtien
- Riskien käsittely, joka jakautuu hallinnollisiin kontrolleihin, valikoituihin vastatoimenpiteisiin ja sekä näiden toteuttamiseen
- Hallintajärjestelmän seuranta ja parantaminen

Nämä kolme osa-aluetta ovat jatkuvassa vuorovaikutuksessa keskenään ja luovat jatkuvasti toimivan kyberturvallisuuden hallintamallin. Tässä luvussa käsitellään valikoituja hallintakeinoja henkilöstöön ja pääsynhallintaan liittyen. Näiden lisäksi luodaan katsaus konfiguraationhallintaan, ohjelmistopäivityksiin ja elinkaaren hallintaan.

Elinkaarimalliajattelu on avuksi lähes kaikissa tässä luvussa käsiteltävissä asioissa. Työsuhteen osalta elinkaareen kuuluu ennen työsuhdetta, työsuhteen aikana ja työsuhteen lopuksi tehtävät asiat. Ne on tiivistetty seuraavaan taulukkoon (Taulukko 3).

| Ennen työsuhdetta | Työsuhteen aikana | Työsuhteen lopuksi |
|---|---|---|
| Määritellään tehtävään tarvittava kyberturvallisuus-osaaminen ja -vastuut | Huolehditaan osaamisesta ja sen ylläpidosta | Huolehditaan osaamisen siirrosta seuraajalle |
| Työsopimuksessa mukana vastuu kyberturvallisuudesta | Tiedotus, valvonta ja tarvittaessa kurinpidolliset toimenpiteet | Muistutus salassapitovelvol-lisuuden jatkumisesta |
| Tarvittavien pääsyoikeuksien määrittely | Roolin mukaisten pääsy-oikeuksien myöntäminen ja säännöllinen katselmointi | Pääsyoikeuksien poistaminen ja omaisuuden palautus |

*Taulukko 3: Työsuhteen keskeiset tietoturva-asiat elinkaarimallin mukaisesti jaoteltuna*

Tarpeen mukaan kannattaa harkita myös taustaselvitysten käyttöä ennen työsopimuksen tekemistä, erityisesti kriittisiin töihin tai asemiin liittyen. Keskeistä henkilöstön tietoturvaosaamisen hallinnassa on kuitenkin se, että tietoturvaan liittyvät roolit ja vastuut on selkeästi määritelty ja niihin liittyvät koulutukset uusitaan säännöllisesti. Tätä tulee myös seurata, muuten kouluttautuminen jää helposti muiden töiden jalkoihin.

Pääsynhallintaan liittyy kolme tukijalkaa: käyttäjätilien hallinnointi, todentaminen (engl. authentication) ja valtuutus (authorization). Fyysinen turvallisuus luo pohjan pääsynhallinnalle. Sen perustana on tilaluokittelu ja kullakin rajalla suoritettavat kulunvalvonta. Automaation osalta tilojen lukitsemisella ja kulunvalvonnalla hallitaan erityisesti pääsyä sähkö- ja automaatiotiloihin ja ristikytkentöihin sekä muihin laitetiloihin (laitteet, johdot, laitekaapit yms.) Lisäksi kaikki ulkopuoliset kytkennät tulisi suojata peukaloinnilta ja vahingoittumiselta.

Fyysiseen turvallisuuteen kuuluu oleellisena osana myös toimintaedellytysten turvaaminen. Tämä kattaa esimerkiksi sähkönjakelun turvaamisen, valvontakamerajärjestelmät ja tilaturvajärjestelmät. Hyväkään kulunvalvonnan toteuttaminen ei auta, jos sähkökatkon aikana kaikki ovet menevät lukkoon, eikä valvomon ja tuotantoalueiden välillä pääse enää liikkumaan. Toki sekin tilanne olisi hankala, että kaikki ovet avautuisivat sähkökatkon sattuessa. Fyysisen turvallisuuden osa-alueeseen kuuluu myös laitteiston asianmukainen huolto ja turvallinen käytöstä poistaminen.

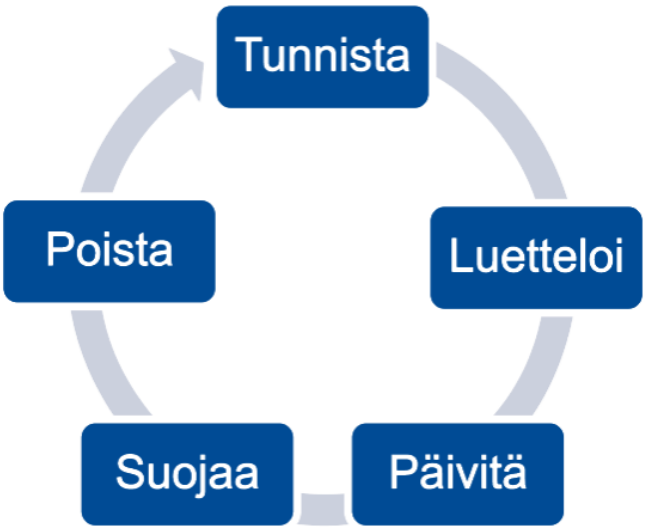
Koko henkilöstöltä (mukaan lukien kolmannet osapuolet) tulisi vaatia kirjallinen sitoumus tietoturvaohjeistusten noudattamiseen. Vierailijoiden osalta tämä pitää sisällään myös henkilöllisyyden varmentamisen, salassapitovelvoitteen ja seuraavat ohjeistukset

- Vierailun aikana tulee pitää vierailijakorttia ja tarvittavia suojavarusteita

- Valokuvaaminen, videoiminen ja nauhoittaminen ovat vierailun aikana kiellettyjä
- Järjestelmiin kytkeytyminen, pois lukien mahdollinen vierailijaverkko, on kiellettyä
- Vierailijan tulee pysyä isännän valvonnan alaisuudessa ja noudattaa isännän antamia turvallisuus- ja tietoturvallisuusohjeistuksia vierailunsa aikana

Yleensä vierailijoiden tietoturvasitoumukset ja vierailun ajankohta tallennetaan määräajaksi, joten näistä muodostuu jonkinlainen henkilörekisteri, jonka osalta tulee laatia tietosuojaseloste ja huolehtia että tietosuojalainsäädännön velvoitteet täyttyvät.

Pääsynhallinnan lisäksi toinen keskeinen asia sellutehtaan omistajan näkökulmasta on järjestelmän elinkaaren hallinta. Tähän liittyvät keskeiset asiat ovat seuraavat:




*Kuva 4: Järjestelmän hallinnan elinkaarimallin runko.*

Näiden osa-alueiden keskeiset asiat ovat seuraavat:

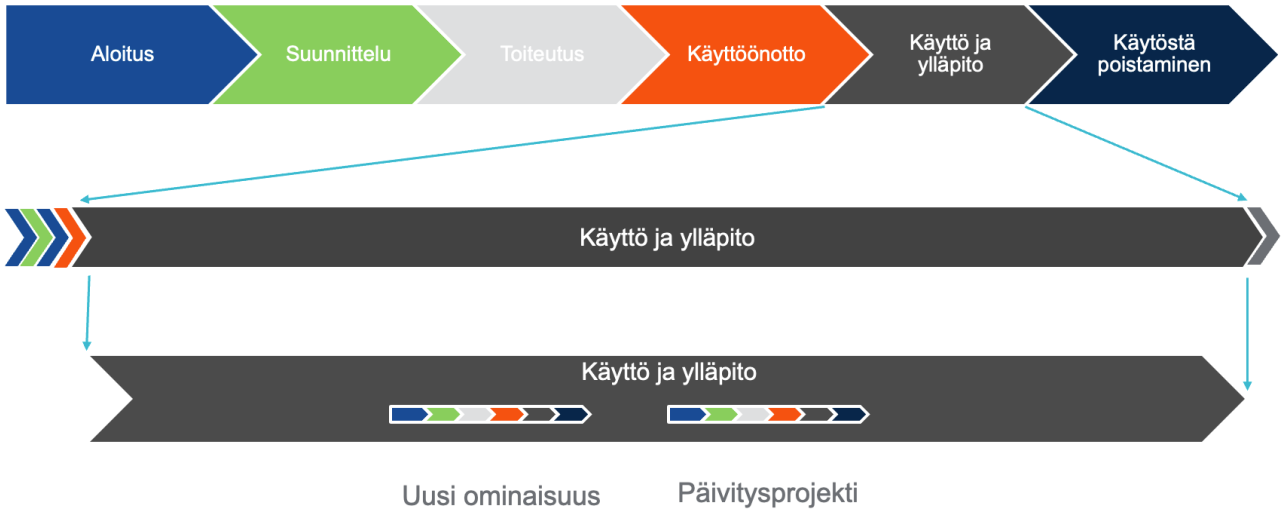
- **Tunnistaminen**: Elinkaarinhallintamallin pohjan muodostaa järjestelmään kuuluvien laitteiden ja ohjelmistokomponenttien tunnistaminen. Näin syntyvän luettelon tulisi päivittyä, uusien tai poistuvien laitteiden/komponenttien myötä.
- **Luettelointi**: Fyysisten laitteiden osalta tiedossa tulee olla laitteiden arvioitu käyttöikä ja korvaavien laitteiden saatavuus. Ohjelmistokomponenttien osalta tulee olla selvillä ainakin kullakin hetkellä käytettävistä lisensseistä ja ohjelmistojen versionumeroista. Järjestelmän teknisen inventaarioluettelon lisäksi tarvitaan myös varsinainen konfigurointi, joka toteutetaan erilaisten asetusten sekä konfigurointitiedostojen ja –ohjelmien avulla. Nämä yhdessä muodostavat järjestelmän kokoonpanon/konfiguraation.
- **Päivittäminen**: Perinteisessä IT-ympäristössä käytetään usein automaattipäivityksiä, mutta automaatioympäristöissä niihin liittyy merkittäviä riskejä. Saatavilla olevia ohjelmistopäivityksiä tulee

kuitenkin seurata yhdessä palvelujen tarjoajien ja toimittajien kanssa ja arvioida riskit ja mahdolliset tarvittavat lisäkontrollit tapauksiin, joissa hyväksikäytettäviä haavoittuvuuksia ei ole mahdollista päivittää välittömästi. Muutostenhallintaan tulee olla määriteltynä prosessi, jonka tuotoksena muutokset ovat hallittuja ja samalla säilyy ymmärrys järjestelmän nykytilasta ja muutoshistoriasta, jotta tarvittaessa voidaan palata historiassa myös taaksepäin.

- **Suojaaminen**: Tyypillisiä suojauskeinoja ovat pääsynhallinnan lisäksi järjestelmien koventaminen ja virustorjuntaohjelmistojen käyttö. Virustorjuntaohjelmiston yhteensopivuus tulee testata ja huolehtia, että viruskuvaukset päivittyvät säännöllisesti. Näistä lisää teknisiä hallintakeinoja käsittelevässä luvussa.
- **Poistaminen**: Elinkaaren lopussa on laitteiden hävittäminen ja mahdollisesti korvaaminen uusilla laiteilla. Tässä yhteydessä tulee huolehtia luottamuksellisen tiedon asianmukaisesta hävittämisestä poistettavilta laitteilta. Tässä yhteydessä tulee muistaa päivittää myös inventaariota.

On hyvä huomioida, että tämä luettelo muodostaa vain elinkaarimallin rungon asioista, joista on hyvä lähteä liikkeelle. Kokonaisuutena muutosten- ja konfiguraationhallinta on kompleksinen prosessi.

Tärkeä osa automaationjärjestelmien elinkaaren hallinnassa on muistaa, että käyttö ja näin ollen myös ylläpitovaiheet ovat pitkiä, mitä on havainnollistettu seuraavassa kuvassa (Kuva 5):

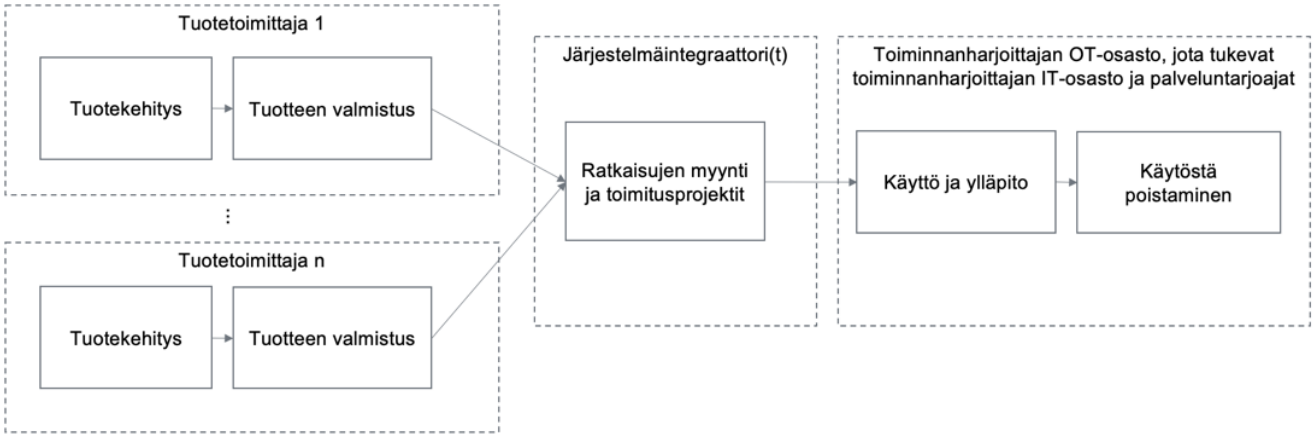



*Kuva 5: Automaatiojärjestelmien elinkaaressa korostuu käyttö- ja ylläpitovaihe.*

Tällaisessa ympäristössä manuaalinen konfiguraationhallinta on tuomittu epäonnistumaan ja prosessi tulisikin automatisoida mahdollisimman pitkälle esimerkiksi erilaisten skriptien avulla. Käytännössä tässä on kuitenkin usein paljon käsityötä, joten konfiguraationhallinnan valittu tarkkuustaso tulisi olla riskien valossa perusteltu. Keskeiseen rooliin nousee myös yhteistyö palvelun tarjoajien ja toimittajien kanssa.

## 2.2 Yhteistyö palvelun tarjoajien ja toimittajien kanssa

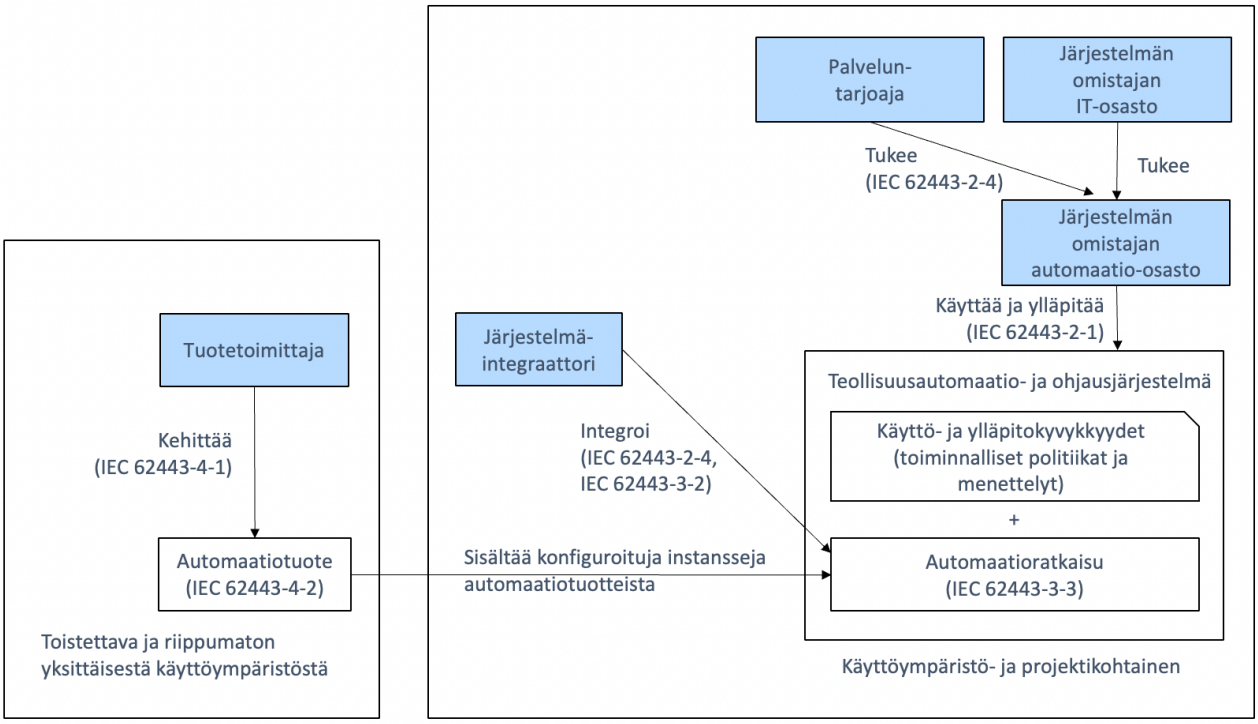
Nykypäivän automaatioympäristöt ovat kompleksisia monitoimittajaympäristöjä, joissa on monenlaisia vastuita. Automaatioympäristön elinkaaren vaiheet ja niihin osallistuvat toimijat on esitelty kuvassa Kuva 6.




*Kuva 6: Automaatioratkaisun elinkaaren vaiheet ja tyypilliset toimijat.*

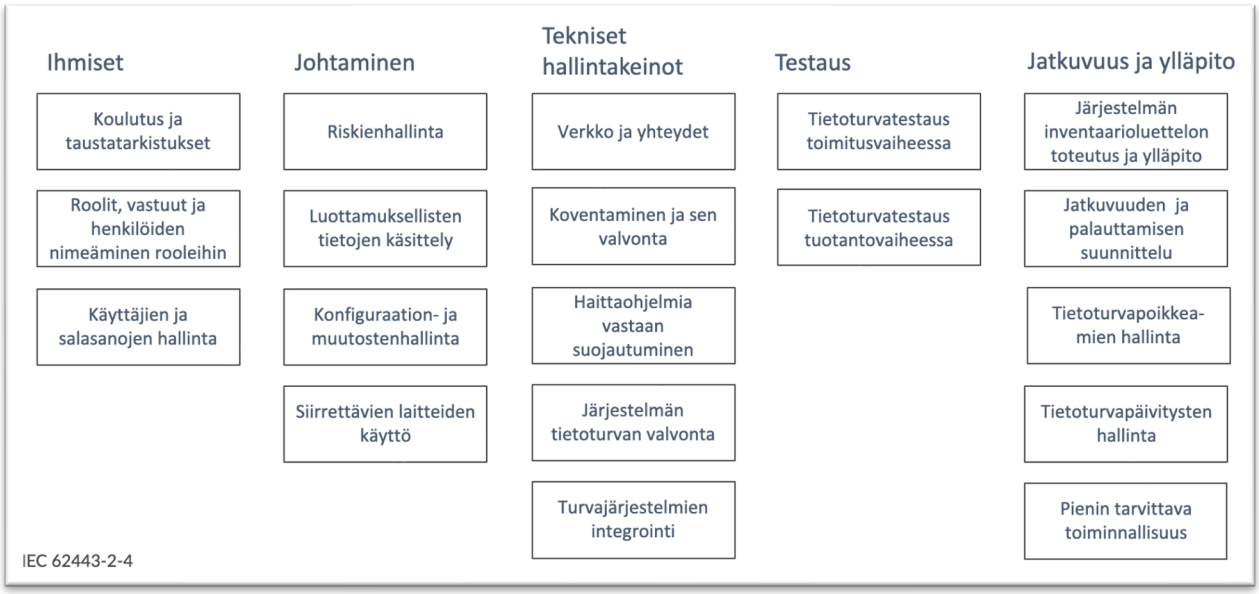
Tällaisissa ympäristöissä yhteistyö tilaajan, toimittajien ja palvelun tarjoajien välillä korostuu. Perinteisesti toimittajasopimuksissa on korostettu teknisiä kyvykkyyksiä, esimerkki viittaamalla IEC-62443 standardin osaan 3-3. Teknologiat vaativat kuitenkin toimiakseen myös prosesseja ja niitä pyörittäviä ihmisiä, joten erityisesti palveluntarjoajien osalta sopimuksissa on tärkeää huomioida myös muut kyberturvallisuuden hallintaan liittyvä osa-alueet.

Kuvassa Kuva 7 esitellään tarkemmin automaatioympäristön toimijoiden vastuut ja niihin liittyvät IEC-62443-standardit. Kuvassa prosesseihin liittyvät standardit on merkitty toimintaa kuvaavien nuolten yhteyteen, ja automaatiotuotteen ja automaatioratkaisun teknisiin vaatimuksiin liittyvät standardit on merkitty tuotteen ja ratkaisun yhteyteen. Kuvassa kannattaa huomioida, että sama toimittaja toimii usein monessa roolissa. Esimerkiksi järjestelmäintegraattorilla voi olla omaa tuotekehitystä, jolloin järjestelmäintegraattori on myös tuotetoimittaja. Samoin järjestelmäintegraattori saattaa jatkaa käytön ja ylläpidon aikaisena palveluntarjoajana.




*Kuva 7: Automaatioympäristön toimijoiden vastuut ja niihin liittyvät IEC-62443-standardit*

IEC-62443 standardin osa 2-4 keskittyy palvelun tarjoajien kyberturvallisuuden hallintajärjestelmien vaatimuksiin. Nämä vaatimukset voidaan ryhmitellä esimerkiksi seuraavan Kuvan 8 mukaisesti.




*Kuva 8: Kyberturvallisuuden hallintajärjestelmän vaatimukset palvelun tarjoajille.*

Kaikki nämä osa-alueet olisi hyvä huomioida sopimusteknisesti toimitus- tai palvelulaajuuteen soveltuvassa laajuudessa ja vaatimukset tulisi ulottaa myös alihankintaketjuihin. Tässäkin on hyvä muistaa, että kohtuus on hyväksi - jos sopimuksessa vaaditaan sokeasti koko IEC 62443 standardin noudattamista ja pari muuta standardia päälle, saatetaan päätyä siihen tilanteeseen, että monet pienemmän toimittajat suljetaan kilpailun ulkopuolelle tai luvataan enemmän kuin oikeasti pystytään toimittamaan. Parempi tapa on huolehtia aluksi siitä, että järjestelmän turvaamisen ja liiketoiminnan jatkuvuuden kannalta keskeisimmät tekniset ja organisatoriset asiat ovat oikeasti kunnossa.

## 2.3 Riskienhallinta

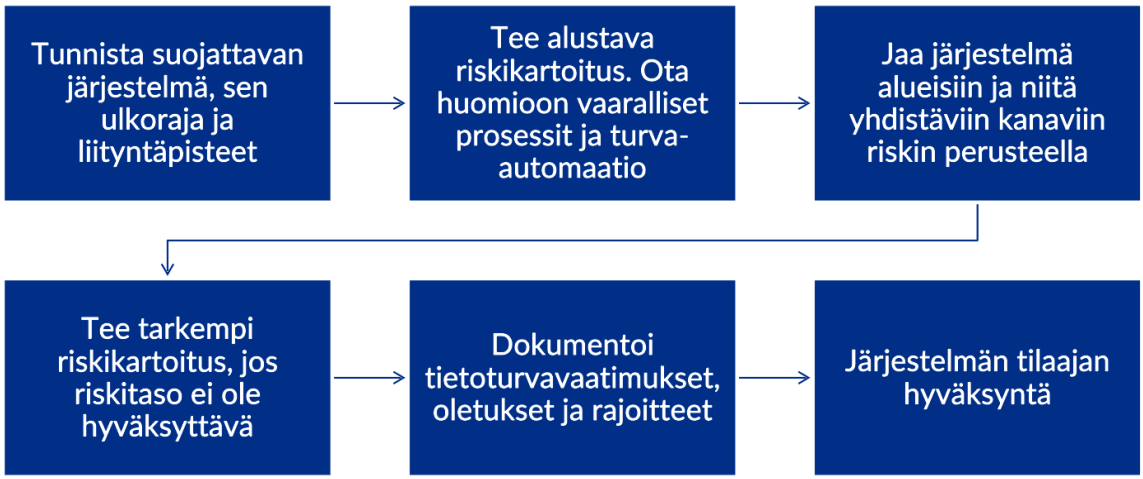
Riskienhallinta on kyberturvallisuuden hallintajärjestelmän ydin, jonka onnistuakseen tulee lähteä liikkeelle liiketoiminnan tavoitteiden ymmärtämisestä ja niiden kannalta keskeistä suojattavien kohteiden tunnistamisesta. Nämä luovat yhdessä pohjan riskien ja mahdollisuuksien tunnistamiselle ja arvioinnille.


*Kuva 9: Askeleet onnistuneeseen riskienhallintaan.*

Tunnistettujen ja arvioitujen riskien pohjalta luodaan riskien hallintasuunnitelma, jossa tavoitteena on, että riskitaso tulisi saada hyväksyttävällä tasolle käytettävissä olevilla resursseilla. Liikkeelle voidaan lähteä isoimmista parannuksista tai vaikkapa niistä, jotka on helppo ja nopea ottaa käyttöön. Toisinaan tämä tarkoittaa myös sitä, että vaikutusten pienentämisen sijaan riski hyväksytään tai otetaan vaikkapa vakuutus pahan päivän varalle. Myös kyberturvallisuuden avaamat uudet mahdollisuudet liiketoiminnalle kannattaa hyödyntää. Riskien ja mahdollisuuksien pohjalta luodaan tavoitteet kyberturvallisuuden kehittämiseksi vuositasolla. Ja muistetaan, että riskien hallinnan ja kyberturvallisuutavoitteiden etenemistä tulee seurata säännöllisesti, etteivät ne jää muun tekemisen jalkoihin.

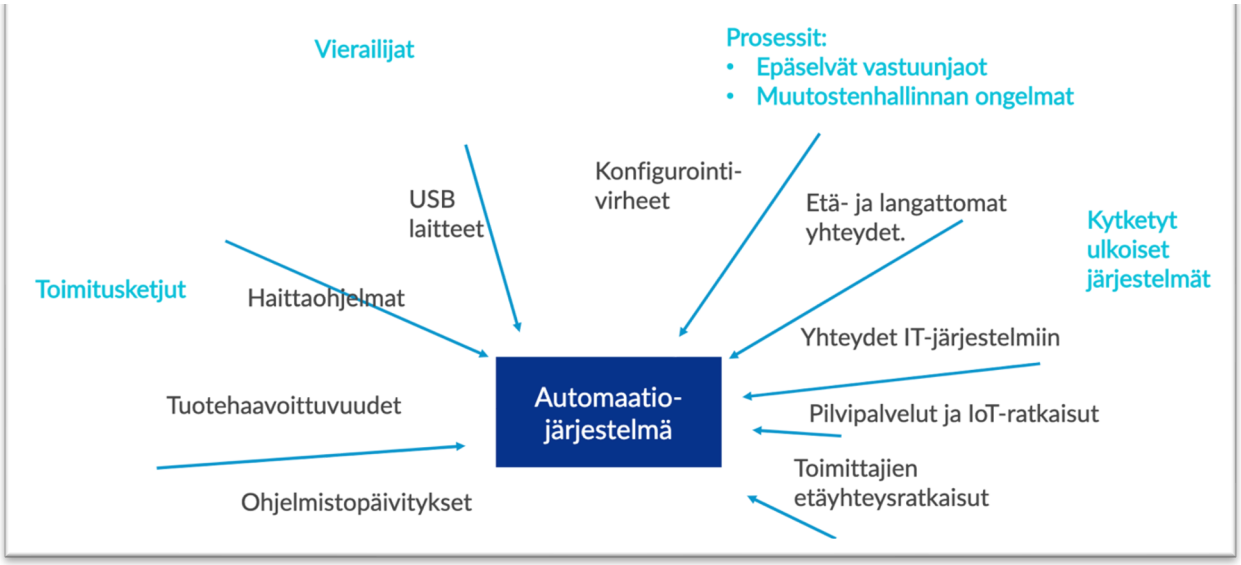
Onnistuakseen riskien hallintaa tulee tehdä useilla tasoilla, ainakin organisaation, yksiköiden ja järjestelmien näkökulmasta. Ylätason riski voisi olla esimerkiksi organisaation joutuminen kyberhyökkäyksen kohteeksi, jolloin alemmilla tasoilla tämän vaikutuksia ja tarvittavia kontrolleja

arvioitaisiin edelleen yksiköiden ja järjestelmien näkökulmista. Järjestelmää koskevien riskien arviointia käsittelee IEC-62443 standardin osa 3-2, jonka mukaista riskiarvion tekoa havainnollisestaan seuraavassa Kuvassa 10.




*Kuva 10: Uuden järjestelmän riskiarvion tekemisen vaiheet 62443-3-2 standardin mukaisesti.*

Käytännön tasolla riskien hallinnassa on hyvä tiedostaa suojattavien kohteiden lisäksi myös mahdolliset hyökkäysvektorit, joista esimerkkejä on esitelty Kuvassa 11.




*Kuva 11: Tyypillisiä hyökkäysvektoreita.*

Uhkien ja hyökkäysvektoreiden (ja mahdollisesti muiden haavoittuvuuksien) avulla tunnistetuille riskeille määritellään todennäköisyydet ja vaikuttavuudet perinteisen riskiarvioinnin mukaan, mutta järjestelmien yhteydessä kontrollien valinnassa tulee huomioida myös tavoiteltu suojaustaso, ks. Kuva 12.

| Taso (Security Level / SL) | Kuvaus |
|---|---|
| SL 0  | Ei suojausvaatimuksia |
| SL 1  | Suojaus tahattomien vahinkojen varalta – "konfigurointivirhe" |
| SL 2  | Suojaus tahallisten loukkausten varalta.<br>Hyökkääjällä yksinkertaiset keinot, vähäiset resurssit, yleinen osaaminen ja matala motivaatio. |
| SL 3  | Suojaus tahallisten loukkausten varalta.<br>Hyökkääjällä hienostuneet keinot, kohtuulliset resurssit, osaaminen teollisuusjärjestelmistä ja kohtuullinen motivaatio. |
| SL 4  | Suojaus tahallisten loukkausten varalta.<br>Hyökkääjällä hienostuneet keinot, laajat resurssit, osaaminen teollisuusjärjestelmistä ja korkea motivaatio. |

*Kuva 12: IEC-62443 standardin mukaiset suojaustasot.*

Tavoitteena tässä on kybersuojauksen tasapaino, jolloin suojauksen toimenpiteet ovat järkeviä riskien näkökulmasta kustannuksiltaan ja vaikeudeltaan sekä kohdennettu oikein.

## 2.4 Turvallinen arkkitehtuuri

Automaatiojärjestelmän turvallisen arkkitehtuurin perusta on järjestelmän segmentointi eli verkon ja automaatiosovelluksen jakaminen erillisiin mahdollisimman riippumattomiin alueisiin (engl. zone), ja tietoliikenteen rajoittaminen näiden osien välisissä kommunikointikanavissa (engl. conduit). Vaatimuksia alueiden ja kanavien muodostamiseen on annettu IEC 62443 -standardin osassa 3-2.

Segmentoinnin idea on pienentää riskejä erottamalla toisaalta järjestelmän suojauksen kannalta tärkeimmät asiat omiksi alueikseen ja toisaalta riskejä sisältävät asiat omiksi alueikseen. Kun alueita yhdistävien kanavien tietoliikennettä rajoitetaan, niin ongelmien leviämistä alueiden välillä voidaan estää ja vahinkojen suuruutta rajata.

Segmentoinnin lähtökohtana on erottaa riskiperustaisesti eri osajärjestelmät seuraavilla perusteilla:

- Kriittinen tuotanto-omaisuus
- Erillinen toiminnallisuus, kuten ohjattavan prosessin eri osa-alueet. Kullakin prosessialueella voidaan lisäksi mennä syvemmälle erottamalla esimerkiksi prosessialueen MES-järjestelmät, valvomoverkot ja varsinaiset ohjausverkot. Näin järjestelmään syntyy kerroksittainen suojaus.
- Erillinen fyysinen tai looginen sijainti
- Pääsynhallinta: rajataan vaadittavien oikeuksien mukaisesti
- Erillinen vastuussa oleva organisaatio

Näillä perusteilla soodakattilan automaatio on syytä erottaa sellutehtaan muusta automaatiojärjestelmästä omaksi alueekseen, koska soodakattila on erillinen toiminnallisuus ja hyvin kriittistä tuotanto-omaisuutta. Lisäksi soodakattilan automaatiojärjestelmään kannattaa rakentaa kerroksittainen suojaus. Kerroksittaisen suojauksen lisäksi kannattaa mahdollisuuksien mukaan soveltaa

luottamattomuuden periaatetta (zero trust), jossa valmistaudutaan verkkotason suojauksen pettämiseen varmistamalla jokainen pyyntö erikseen.

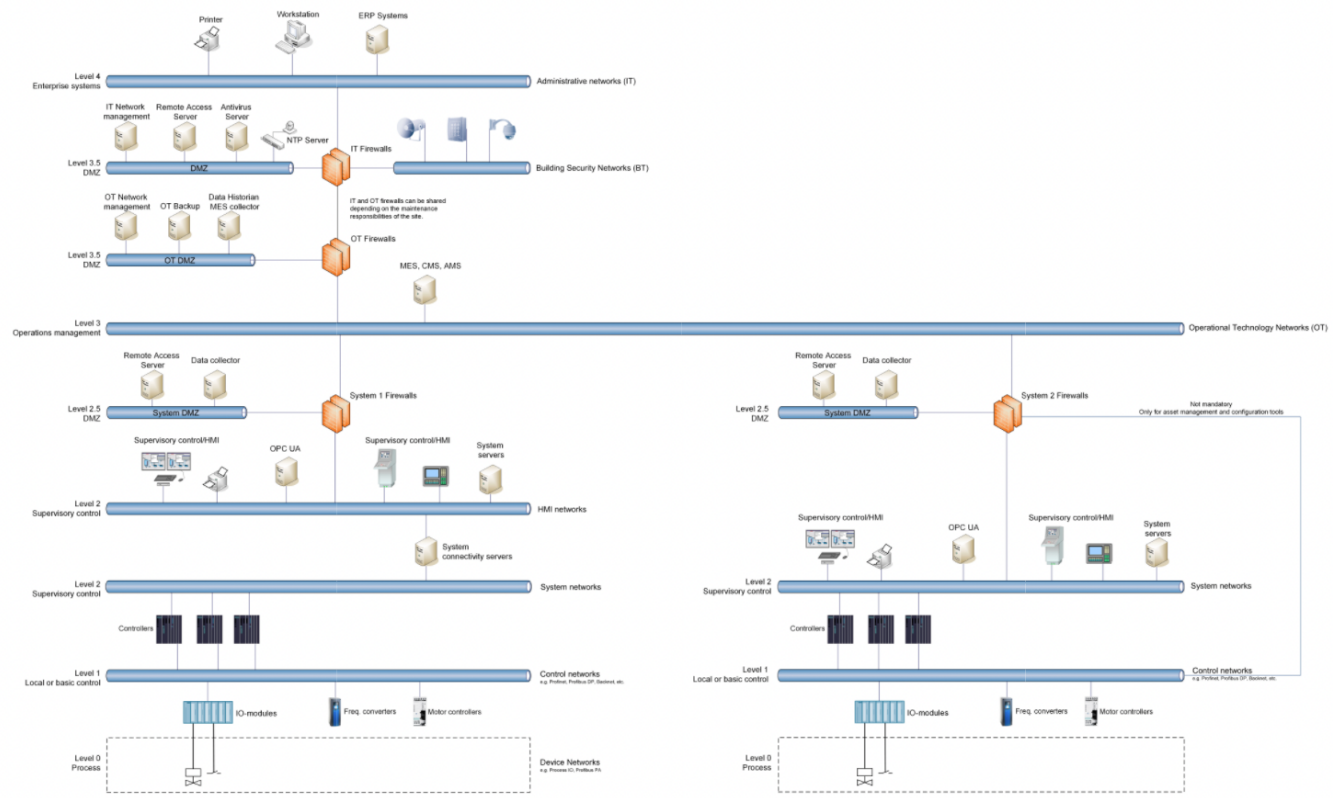
Taulukko 4 esittää tiettyjä tapauksia, joissa voi olla tekniset perusteet muodostaa erillisiä alueita. Nämä erilliset alueet lisäävät järjestelmän kerroksittaista suojausta ja vähentävät vahinkojen leviämisen riskiä. Taulukon tapaukset ovat relevantteja myös soodakattilan automaatiojärjestelmissä.

| Alue | Miksi kannattaisi jakaa erilliseksi alueeksi |
|---|---|
| **Automaatiojärjestelmän ulkopuoliset liiketoiminta-järjestelmät** | Toimistoverkko ja liiketoimintajärjestelmät ovat yleensä eri organisaation vastuulla. Automaation kyberturvallisuuden perusasia on, että tämä dynaaminen ympäristö täytyy erottaa automaatiojärjestelmästä sen suojaamiseksi. |
| **Turva-automaatio** | Turva-automaatioon liittyy henkilö- ja ympäristövahinkojen riski |
| **Väliaikaisesti kytkeytyvät laitteet** | Väliaikaisesti kytkettävät huoltokoneet ja massamuistit kytkeytyvät myös muihin järjestelmiin ja voivat levittää niistä peräisin olevia ongelmia |
| **Langattomat laitteet** | Langattomien verkkojen tarjoamat laajemmat kytkeytymismahdollisuudet lisäävät riskiä. Langaton verkko voi kuulua fyysisellä turvallisuudella suojatun alueen ulkopuolelle. |
| **Ulkopuolisiin verkkoihin yhteydessä olevat laitteet** | Ylläpito-, optimointi- ja raportointijärjestelmät kuten IoT-järjestelmät kytkeytyvät automaatiojärjestelmän ulkopuolelle, joka lisää riskiä. |

*Taulukko 4: Järjestelmän segmentoiminen.*

Taulukosta kannattaa huomioida etenkin turva-automaatio, jonka olisi hyvä olla erillinen alueensa. Turva-automaation ja kyberturvallisuuden suhde on jatkossa entistä laajemmin säädeltyä, mihin on hyvä varautua. Lisäksi taulukosta kannattaa huomioida myös kaikenlaisiin ulkopuolisiin ylläpito-, IoT- tai raportointijärjestelmiin kommunikoivat laitteet, joiden tulisi myös olla omalla alueella. Toisin sanoen ei ole suositeltavaa lisätä IoT-laitteita suoraan automaatiojärjestelmän alemmille kerroksille, koska silloin rikotaan automaatiojärjestelmän kerroksittainen suojaus. Yhteydet ulkomaailmaan ja Internetiin tulee järjestää hallitusti järjestelmän kerroksittaisen rakenteen kautta.

Kuva 13 on esimerkki järjestelmän rakenteesta, jossa on sovellettu osaa yllä esitetyistä periaatteista. Business-järjestelmät on selkeästi erotettu OT-järjestelmistä, ja kaksi erillistä osajärjestelmää System 1 ja System 2 on erotettu palomuurilla. Ulkopuolisiin verkkoihin yhteydessä olevat laitteet on sijoitettu erillisiin DMZ-verkkoihin. Kuvan 13 esimerkki on kuitenkin yksinkertaistettu, eikä siitä käy ilmi kaikki taulukon 4 periaatteet. Esimerkiksi turva-automaation, langattomien laitteiden tai väliaikaisesti kytkeytyvien laitteiden erotusta ei ole kuvassa havainnollistettu.




*Kuva 13: Esimerkki järjestelmän rakenteesta.*

Tällainen kerroksittainen rakenne on keskeisessä roolissa järjestelmän suojaamisessa.

# 3. TEKNISET HALLINTAKEINOT

Tässä luvussa käydään läpi teknisten hallintakeinojen viisi keskeisintä aluetta ja niiden keskeisimmät hallintakeinot. On hyvä huomata, että tämä esittely ei kata kaikkia IEC 62443 -standardin vaatimuksia, vaan luvussa painotetaan perusasioita ja alempien turvallisuustasojen vaatimuksia. Automaatiojärjestelmän teknisiin hallintakeinoihin liittyviä vaatimuksia on annettu IEC 62443 -standardin osassa 3-3 ja niihin liittyviä järjestelmän omistajan prosesseja on käsitelty osassa 2-1. Tarkemmat kuvaukset ja tästä pois jätetyt vaatimukset löydät tutustumalla ko. standardeihin. Tässä luvussa teknisiä hallintakeinoja ajatellaan kokonaisuutena: järjestelmässä täytyy olla vaaditut kyvykkyydet, jotka täytyy myös ottaa käyttöön osana järjestelmän omistajan käytännön prosesseja.

Tekniset kyberturvallisuuden hallintakeinot tulee toteuttaa siten, että ne eivät vaaranna järjestelmän suorituskykyä tai saatavilla oloa. Esimerkiksi toimistoverkon palveluihin kuten todennuspalveluun ei tulisi olla sellaista riippuvuutta, joka voisi häiritä automaatiojärjestelmän saatavilla oloa, tai varmuuskopioinnin aiheuttama kuorma tietokoneille ja verkolle ei saisi vaarantaa automaatiojärjestelmän varsinaista ydintehtävää.

## 3.1 Pääsynhallinta

Pääsynhallinnan tarkoitus on varmistaa, että oikeat käyttäjät pääsevät oikeisiin resursseihin oikeista syistä oikeaan aikaan. Käyttäjillä tarkoitetaan henkilöiden lisäksi myös ohjelmistoprosesseja ja laitteita. Pääsynhallinta on kyberturvallisuuden ytimessä.

Automaatiojärjestelmissä pääsynhallintaa tehdään eri tasoilla: verkkolaitteissa, käyttöjärjestelmissä ja ohjausjärjestelmien sovellustasolla. IEC 62443 -standardin osassa 3-3 käsitellään pääsynhallinnan teknisiä vaatimuksia luvussa 5: *FR1 – Identification and authentication control* ja luvussa 6: *FR 2 – Use control*.

IEC 62443-2-1 standardin mukaan perustason käytänteitä ovat seuraavan luettelon asiat. Automaatiojärjestelmässä tulee luonnollisesti olla mukana näiden käytänteiden edellyttämät tekniset ominaisuudet.

- Pääsy- ja käyttöoikeuksien minimointi, esimerkiksi roolien ja työtehtävien mukaisesti. Käyttäjillä tulisi olla pienimmät mahdolliset käyttöoikeudet, joilla käyttäjien tehtävät voidaan tehdä.
- Kaikkien henkilöiden tunnistaminen riskeihin nähden riittävillä menetelmillä. Tämä koskee kaikilla tasoilla olevia tunnuksia. Vähimmäistasona on käyttäjätunnus ja salasana. Yhteiskäyttötunnuksia ei tulisi käyttää ainakaan, jos järjestelmän alueen vaadittu IEC 62443 -suojataso on 2 tai korkeampi. Joskus voi olla pakko turvautua korvaaviin fyysisisiin turvamekanismeihin.
- Oletussalasanojen vaihtaminen ennen järjestelmän käyttöönottoa
- Vahvat todennuskäytännöt eli usean tekijän todentaminen (MFA, multi-factor authentication) järjestelmänhallintatileillä, sovellusten konfigurointitileillä sekä vuorovaikuttavien etäkäyttäjien tileillä
- Kriittisten järjestelmien pääsy-yritysten valvonta (lokitiedostojen käyttö ja valvonta)

Kannattaa ottaa käyttöön yhtenäinen käyttäjätilien hallintaratkaisu. Usein tällaista ratkaisua ei voida soveltaa ainakaan kaikkien käyttäjätilien osalta, jolloin voidaan käyttää salasanojen hallintasovellusta. Ihmisten todentamisen lisäksi myös tehtävien välisen tietoliikenteen todennus (esim. laitetunnisteiden avulla) on kuvattu perustason käytänteenä standardissa IEC 62443-2-1. Standardissa IEC 62443-3-3 tämä kuuluu suojatasolle 2. Tällä hetkellä monet automaatiotuotteet eivät vielä tue tätä, mutta tulevaisuudessa myös tähän kannattaa kiinnittää huomiota.

## 3.2 Järjestelmän eheys

Automaatiojärjestelmän eheydellä tarkoitetaan sitä, että sen komponenttiversiot, asetukset, järjestelmän tila ja sen kaikki muut tiedot ovat aitoja, oikeita, sisäisesti ristiriidattomia, kattavia, ajantasaisia ja käyttökelpoisia. Eheys on keskeistä järjestelmän luotettavan toiminnan kannalta. IEC 62443 -standardin osassa 3-3 käsitellään järjestelmän eheyttä luvussa 7: *FR3 – System integrity*.

Järjestelmän eheyteen liittyviä keskeisiä suojauskeinoja ovat

- Suojautuminen haittaohjelmia vastaan virustorjunnalla ja/tai application control -ominaisuuksilla, jotka estävät haitallisia, ei-luotettavia tai ei-toivottuja sovelluksia toimimasta
- Laitteiden, työasemien, palvelimien, verkon ja tärkeimpien sovellusten koventaminen. Koventamisella tarkoitetaan niin sanotun hyökkäyspinta-alan pienentämistä. Se tehdään tarpeettomia ominaisuuksia poistamalla tai estämällä ja varmistamalla, että asetukset ovat turvallisia. Esimerkiksi laitteiden tarpeettomat USB-liitynnät ja tietoliikenneportit tulee poistaa käytöstä.
- Ohjelmistopäivitysten hallinta. Seurataan toimittajien tiedotteita sekä arvioidaan ja mahdollisuuksien mukaan testataan päivitysten tarpeellisuus, soveltuvuus ja yhteensopivuus. Jos päivitys hyväksytään asennettavaksi, suunnitellaan sopiva asennusajankohta.
- Myös erilaiset ohjelmistolisenssit ja virusohjelmien tietokantojen päivitykset kannattaa ottaa hallintaan.
- Menetelmät siirrettävien massamuistien ja siirrettävien laitteiden hallintaan ja näitä reittejä pitkin mahdollisesti tulevia haittaohjelmia vastaan suojautuminen. Tähän voidaan käyttää esimerkiksi USB-massamuistien pesurilaitetta tai tiedonsiirtoyhdyskäytävää. Minimissään tulee olla käytänteet, jotka varmistavat, että ne käyttäjät, jotka tuovat siirrettäviä laitteita tai massamuisteja, käyttävät suojausta haittaohjelmia vastaan.

Nämä keinot auttavat haittaohjelmien ennaltaehkäisyssä, leviämisen rajoittamisessa sekä tunnistamisessa. Keskeisessä osassa eheyden turvaamisessa on myös kokoonpanon (konfiguraation) ja sen muutosten hallinta. Kokoonpanolla tarkoitetaan valittuja komponentteja, niiden versioita ja kaikenlaisia parametrejä, asetuksia ja asetustiedostoja. Tähän luokkaan kuuluvat esimerkiksi GSD-, ja ESD-tiedostot. Kokoonpano- ja muutoshallinnan tavoite on varmistaa, että muutokset ovat valtuutettuja ja niistä jää jälki, ja että järjestelmän nykyinen kokoonpano ja haluttu kokoonpano ovat yksiselitteisesti tiedossa.

## 3.3 Verkon ja tietoliikenteen suojaaminen

Hajautettuna järjestelmänä automaatiojärjestelmä nojaa lähiverkon yli tapahtuvaan tietoliikenteeseen. Verkon ja tietoliikenteen suojaus on tärkein tapa toteuttaa järjestelmän turvallinen arkkitehtuuri. IEC 62443 -standardin osassa 3-3 käsitellään järjestelmän verkon ja tietoliikenteen suojausta luvussa 9: *FR 5 – Restricted data flow* ja luvussa 8: *FR 4 – Data confidentiality*.

### Keskeiset hallintakeinot

Keskeisiä verkon ja tietoliikenteen suojaamiseen liittyviä kyberturvallisuuden hallintakeinoja ovat

- Luvussa 2.4 Turvallinen arkkitehtuuri käsitelty turvallinen arkkitehtuuri ja järjestelmän segmentoiminen
- Sekä lähtevän että tulevan tietoliikenteen rajoittaminen alueiden välillä siten, että oletuksena tietoliikenne on estetty ja vain välttämätön tietoliikenne on sallittu. Tämä tehdään yleensä verkkolaitteissa olevilla palomuureilla. Niiden konfiguraatio täytyy suunnitella ja tarkistaa tämän periaatteen mukaisesti aina kun järjestelmään tehdään muutoksia ja säännöllisesti
- Yleiskäyttöisten viestintäohjelmien rajoittaminen automaatioverkossa. Ei käytetä sähköpostia, Teamsia, chattejä tai vastaavia.

Korkeammilla suojaustasoilla pyritään myös käyttämään sellaisia kommunikointiprotokollia, joissa on mukana liikenteen eheyden suojaus.

### Staattiset osoitteet ja DHCP

Automaatiojärjestelmissä käytetään perinteisesti kiinteitä IP-osoitteita ja kiinteästi asetettuja verkkoasetuksia. Tämä on jatkossakin hyvä lähtökohta. Kiinteät osoitteet eivät kuitenkaan aina toimi, esimerkiksi jos kyseessä on väliaikaisesti kytkeytyviä laitteita varten muodostettu verkko. Kun kiinteitä osoitteita ei voida käyttää, hakevat laitteet osoitteen dynaamisesti käyttämällä DHCP-protokollaa (Dynamic Host Configuration Protocol). DHCP-protokollaan voi kuitenkin liittyä uhkia: ei-valtuutetut laitteet voivat varata liikaa IP-osoitteita, järjestelmässä voi olla vale-DHCP-palvelin, tai yhteydet DHCP-palveluun voidaan menettää. DHCP:tä käytettäessä kannattaa huomioida seuraavat suositukset:

- DHCP-palvelimet tulisi olla samassa verkkosegmentissä kuin sitä käyttävät laitteet (esim. reitittimessä).
- DHCP Relay -toimintoja ei kannata käyttää
- Kytkimissä kannattaa ottaa käyttöön DHCP snooping, joka suojaa vale-DHCP-palvelimia vastaan

Näillä toimenpiteillä mainitut uhat saadaan torjutuksi.

### Etäyhteydet

Etäyhteydet ovat yksi keskeisimmistä hyökkäysvektoreista automaatiojärjestelmiin. Turvallisten etäyhteyskäytäntöjen perusteita ovat:

- Etäyhteyden tulee perustua standardiprotokolliin ja -menetelmiin, kuten esimerkiksi VPN-ratkaisuihin (Virtual Private Network) tai PAM-ratkaisuihin (Privileged Access Management)
- Etäyhteydet toteutetaan keskitetyn ja hallitun yhdyskäytävän kautta. Monitoimittajaympäristössä ei sallita toimittajakohtaisia etäyhteyskäytäntöjä.
- Etäyhteyden yhdyskäytävää tulee ylläpitää. Siinä tulee olla suojaus haittaohjelmia vastaan, ja sitä tulee valvoa.
- Etäyhteyttä avattaessa tulisi kytkeytyvälle laitteelle tehdä tietoturvatarkastus
- Käytetään vähintään kahden tekijän käyttäjäkohtaista todentamista. Ei yhteiskäyttötunnuksia.
- Etäyhteyksistä tulee jäädä sellainen jälki, jonka perusteella nähdään, kuka on kytkeytynyt, milloin ja kuinka kauaksi aikaa.
- Etäyhteys tulisi liittää organisaation keskitettyyn identiteetin- ja pääsynhallintaratkaisuun. Tällä varmistetaan esimerkiksi, että työsuhteen päättyessä myös etäyhteystunnukset sulkeutuvat.
- Etäyhteyden yhdyskäytävä on ulkopuolelle kommunikoiva laite, joten se tulee olla verkossa segmentoituna DMZ-alueelle
- Etäkäyttäjän käyttämää automaatiokäyttöliittymää ei tulisi ajaa suoraan etäkäyttäjän omalla koneella. Toisin sanoen *päästä-päähän*-protokollayhteys etäkäyttäjän koneen ja automaatiojärjestelmän kohdekoneen välillä tulisi katkaista jonkinlaisella käyttöliittymän ”striimauksella”. Tämä voidaan toteuttaa esimerkiksi hyppykoneella ja RDP:llä (Remote Desktop Protocol). Tätä ei yleensä pidetä minimivaatimuksena.

Käyttäjille tulee myös tarjota asianmukainen koulutus, jotta he osaavat käyttää etäyhteyksiä turvallisesti.

## 3.4 Järjestelmän valvonta

Varautumisesta ja suojaamisesta huolimatta järjestelmä voi joutua murron tai muun kyberturvapoikkeaman kohteeksi. Jotta tällaisessa tilanteessa osattaisiin toimia nopeasti ja asianmukaisesti, se on ensin huomattava. Samoin poikkeaman jälkeen on pystyttävä selvittämään, mitä on tapahtunut. Siksi järjestelmän valvonta on yksi keskeisistä teknisistä hallintakeinoista. Valvontakeinoissa on otettava huomioon automaatiojärjestelmän suorituskyvyn säilyttäminen: valvontakeinot eivät saa vaarantaa järjestelmän normaalia toimintaa. IEC 62443 -standardin osassa 3-3 käsitellään järjestelmän valvontaa luvussa 10: *FR 6 – Timely response to events*.

Lokienhallinta on järjestelmän valvonnan lähtökohta. Sen toteuttaminen etenkin vanhoihin järjestelmiin voi kuitenkin olla haastavaa. Toinen tyypillinen valvontakeino on työasemien ja palvelimien valvonta-agenttien käyttäminen.

Järjestelmän komponenteista kerätään ainakin seuraavat tapahtumat:

- Pääsynhallinnan tapahtumat. Etenkin kriittisten järjestelmien pääsy-yritykset.
- Virheelliset pyynnöt
- Käyttöjärjestelmien tietoturvaan liittyvät tapahtumat
- Tietoturvan valvontamekanismien tapahtumat kuten Intrusion Detection System (IDS) ja haittaohjelmia vastaan suojautuminen

- Verkkolaitteiden tietoturvaan liittyvät tapahtumat
- Automaatiojärjestelmän diagnostiikan tapahtumat (ks. alla)
- Varmuuskopiointiin ja palauttamiseen liittyvät tapahtumat
- Konfiguraatiomuutokset
- Lokienhallintaan liittyvät tapahtumat kuten lokien katselu

Automaatiojärjestelmän oma diagnostiikka on hyödyllinen osa kyberturvallisuuden valvontaa. Automaation diagnostiikalla voidaan yleensä seurata esimerkiksi CPU-kuormia, muistin käyttöä, levytilan täyttymistä ja verkon liikenteen ruuhkaisuutta. Näihin mittareihin liittyvät hälytykset kertovat järjestelmän saatavilla olon vaarantumisesta.

Lokienhallintaan liittyviä suosituksia:

- Lokeihin ei tule kerätä salasanoja, salausavaimia, tarpeettomia henkilötietoja tai muuta luottamuksellista tietoa
- Lokienhallinnalla tulisi olla riittävä levytila, ja levytilan täyttymistä ja lokien kirjoittamisen häiriöitä tulee valvoa.
- Lokien perusteella tulisi voida selvittää, kuka henkilö on tehnyt tietyn toiminnan
- Järjestelmän kellot tulee synkronoida siten, että keskitetyn lokienhallinnan lokien järjestys on oikein

Lokit suositellaan kerättäväksi keskitetysti hallittuun järjestelmän laajuiseen lokienhallintaan. Sieltä ne voidaan esimerkiksi välittää organisaation Security Operations Center (SOC) -tiimin valvontajärjestelmään (Security Information and Event Management, SIEM), jolloin lokien pohjalta voidaan tehdä myös varsinaista valvontaa. Tässä oleelliseksi nousee oleellisen tiedon tunnistaminen ja siihen reagointi – kumpaakin on syytä harjoitella, ettei jää tiukan paikan tullen sormi suuhun.

## 3.5 Jatkuvuuden hallinta

Saatavilla olo on automaatiojärjestelmien tärkein kyberturvallisuuden tavoite. Saatavilla oloon liittyvät hallintakeinot yrittävät pienentää palveluneston seurauksia ja helpottaa ja nopeuttaa järjestelmän palautumista katkoksen jälkeen. IEC 62443 -standardin osassa 3-3 käsitellään jatkuvuuden hallintaa luvussa 11: *FR 7 – Resource availability*.

Jatkuvuuden ja saatavilla olon hallinnan kannalta keskeisiä keinoja ovat:

- Laitteiden sisäänrakennetut suojaukset verkkomyrskyjä ja palvelunestotilanteita varten
- Varmistetaan laitteiden mitoituksella ja testauksella, että kyberturvallisuuden hallintakeinot eivät kuluta liikaa järjestelmän resursseja
- Varmuuskopioinnin suunnittelu ja toteuttaminen säännöllisesti. Varmuuskopioinnin valvonta ja palauttamisen testaus.
- Varavirran varmistaminen sähkökatkosten varalta
- Verkko- ja tietoturva-asetusten hallinta
- Pienimmän tarvittavan toiminnallisuuden periaate: poistetaan tai estetään kaikki tarpeeton toiminnallisuus järjestelmästä

- Ajantasaisen komponentti-inventaarion ylläpitäminen. Inventaarioluetteloa voidaan hyödyntää poikkeustilanteiden hallinnassa ja ohjelmistopäivitysten hallinnassa.

Tärkeä keino jatkuvuuden turvaamisessa on myös keskeisten komponenttien kahdentaminen.

# 4. VAIHEITTAINEN TOTEUTTAMINEN

Kyberturvallisuuden hallinta on erittäin laaja alue, johon liittyy suuri joukko vaatimuksia erilaisilta osa-alueilta. Käytännössä kyberturvallisuuden hallintaa on pakko rakentaa vaiheittain – muuten oma organisaatio ja toimittajat tukehtuvat uusiin sääntöihin ja käytäntöihin. Myös standardeja ja ohjeistuksia kannattaa ottaa käyttöön vähitellen. Esimerkiksi IEC 62443-standardin suojaustasoissa kannattaa huomioida, että korkeammat suojaustasot voivat olla hyvin vaativia ja kalliita, joten niiden soveltaminen on järkevää vain, jos tunnistetut riskit niitä edellyttävät.

## 4.1 Vaiheittaisen toteuttamisen edut

Usein ketterällä kehittämisellä haetaan kykyä reagoida muuttuviin olosuhteisiin ja vaatimuksiin. Vaikka automaatiojärjestelmän kyberturvallisuusvaatimukset eivät muutu kovin nopeasti, on vaiheittaisella tai ketterällä toteuttamisella useita etuja:

- Kyberturvallisuuden hallinta rakentuu ihmisten toiminnan varaan. Ihmisten on mahdotonta muuttaa käyttäytymistään äkillisesti.
- Vaiheittaisen muutoksen etenemistä voidaan seurata ja mitata
- Muutoksen kustannukset pysyvät hallinnassa ja myös niitä voidaan helpommin seurata.
- On mahdollista tunnistaa pullonkauloja ja parantaa huonommin toimivia osia
- On mahdollista aloittaa kriittisimmistä ja tärkeimmistä kohdista
- Pystytään pitämään myös toimittajat ja kumppanit mukana muutoksessa

Näin ollen onkin viisasta aloittaa muutamista kyberturvallisuuden ydinkohdista ja ottaa lisäkohtia mukaan sitä mukaa, kun aiemmat asiat on saatu valmiiksi.

## 4.2 Kyberturvallisuuden ydinkohdat

Tämä raportti ja siihen liittyvä tarkastuslista keskittyvät kokonaisuudessaan perusasioihin. Tarkastuslistassa on kuitenkin merkitty erikseen aivan keskeisimmät ydinkohdat.

Jos kyberturvallisuuden hallinta on vielä alkuvaiheessa, voidaan muutoshanke aloittaa seuraavista ydinkohdista:

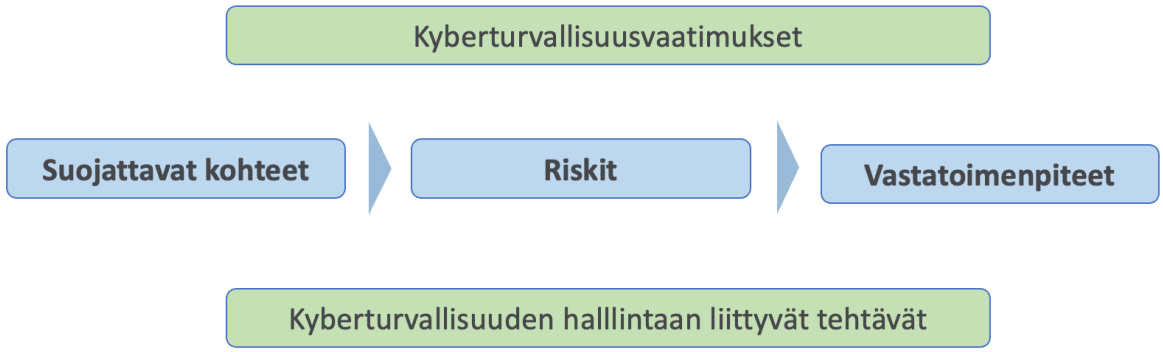
- Kartoita järjestelmät ja kriittisin tuotanto-omaisuus. Tunnista näihin liittyvät riskit. Seuraavat neuvot perustuvat tälle inventaarioluettelolle ja tunnistetuille riskeille. Inventaario ja riskirekisteri voivat aluksi olla yksinkertaisia ja karkealla tasolla tehtyjä esimerkiksi käyttämällä tämän raportin liitteenä olevaa Excel-taulukkoa.
- Tunnista kyberturvallisuuteen liittyvät roolit ja vastuut organisaatiossa. Tähän kuuluu ainakin järjestelmän omistajan IT-organisaatio, automaatio-organisaatio ja tärkeimmät toimittajat. Paranna yhteistyötä eli tarjoa kahvit ja osta pullat. Varmista riittävä osaaminen eli järjestä koulutusta.
- Ota käyttäjätilit ja salasanat hallintaan sekä sellutehtaan omalle henkilökunnalle että toimittajille. Kaikkia tilejä ei voida kytkeä keskitettyyn käyttäjänhallintaan, joten käytä salasanojen hallintaohjelmaa, johon on vahva tunnistautuminen. Vaihda aina oletussalasanat.

- Erota automaatiojärjestelmän verkko toimistoverkosta ja rakenna siihen vähintään DMZ-alue, jossa on vain ulkopuolelle kommunikoivia laitteita. Suunnittele ja aikatauluta myös muu verkon segmentointi.
- Käy läpi varmuuskopiointi ja sen testaaminen. Harjoittele palauttamista yhdessä toimittajien kanssa.
- Aloita ohjelmistopäivitysten hallinta kriittisimmille komponenteille. Seuraa toimittajien tietoturvaan liittyvää viestintää. Mieti, voiko ohjelmistopäivityksiä testata ennen jakelua.
- Rakenna perusratkaisu konfiguraation- ja muutostenhallintaan. Järjestelmän tila ja kuinka siihen tehdään muutoksia, on hyvä tietää. Tässä tavoitteena on, että kukaan ei voi tehdä muutoksia ilman valtuuksia tai ilman että muutoksista jää jälki.

Myös näiden ydinkohtien osalta on hyvä muistaa, että kohtuullinen ratkaisu tänään on parempi kuin täydellinen kahden vuoden päästä. Eikä yhden osa-alueen täydellinen suojaaminen ei ole tietoturvassa järkevä lähestymistapa, vaan suojaustasoa tulee pyrkiä nostamaan vaiheittain mahdollisimman laaja-alaisesti. Hyökkääjä ei todennäköisesti tule sisään panssaroidusta ovesta, jos vieressä on avonainen ikkuna.

## 4.3 Tavoitteiden asettaminen, toteuttaminen ja seuraaminen

Tavoitteiden asettaminen, toteuttaminen ja seuraaminen on tärkeä askel muutoshankkeessa onnistumisessa – sitä saat mitä mittaat. Tämän vuoksi mittareita ei kannata lähteä rakentamaan summamutikassa vaan ensin olisi hyvä hahmottaa kokonaisuuteen liittyvät keskeiset käsitteet ja niiden väliset yhteydet eli rakentaa niin kutsuttu informaatiomalli. Yksinkertaistetuimmillaan tässä työssä esitellyt asiat voidaan luokitella seuraavan Kuvan 14 mukaisesti.




*Kuva 14: Kyberturvallisuuden hallinnan yksinkertaistettu informaatiomalli.*

Modulaarisen lähestymistavan mukaisesti ensimmäisiksi vaatimuksiksi voi ottaa vaikkapa tarkistuslistan ydinkohdat ja tehtäviksi edellisessä luvussa esitellyt tehtävät. Kun tehtävien hallintaan käytetään sopivaa työkalua, tästä saadaan näppärästi ensimmäinen mittari, jonka perusteella edistymistä voidaan seurata säännöllisissä tapaamisissa tai ylläpitää jopa reaaliaikaista tilannekuvaa edistymisestä. Tässä on hyvä muistaa, kyberturvallisuuden hallinnan tavoitteena ei ole saada kaikkea valmiiksi vaan löytää riskien hallinnan kautta aina seuraavaksi tärkeimmät vastatoimeenpiteet ja tehtävät, jotka vievät kyberturvallisuutta eteenpäin. Näin ollen säännöllinen seuranta ja jatkuva parantaminen nousevat keskiöön.

# 5. YHTEENVETO

Tässä työssä on käsitelty automaatiojärjestelmien suojaamiseen liittyviä keskeisiä asioita IEC 62443 standardiin ja kirjoittajien kokemuksiin nojautuen. On tärkeää huomata, että lähtökohtana tässä työssä ei ole ollut kaikenkattavuus vaan tärkeimpien perusasioiden esitteleminen. Näillä ohjeilla kyberturvallisuuden hallinnassa pääsee hyvään alkuun matkalla, jonka ei ole tarkoituskaan tulla koskaan päätökseen. Tärkeintä on lähteä matkaan ja pysyä liikkeellä oikeaan suuntaan kulkien. Siihen tässä työssä on annettu hyvät eväät.

## 5.1 Projektissa tuotetun aineiston käyttö

### Suojattavan tuotanto-omaisuuden tunnistaminen

Riskien hallinta lähtee liikkeelle keskeisten suojattavien kohteiden tunnistamisella. Tämä tuotanto-omaisuus luetteloidaan Kyberturvallisuuden riskientunnistuspohja excelin "*Tuotanto-omaisuus*"-välilehdelle, joka esitellään Kuvassa 15.

| SUOJATTAVIEN KOHTEIDEN LUETTELO | | | | | |
|---|---|---|---|---|---|
| ID | Suojattava kohde | Sijainti | Vastuuhenkilö | Täytyykö riskit arvioida? | Lisätietoja |
| Yleiset | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Tieto-omaisuus | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Keskeiset työkalut ja tietojärjestelmät | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Keskeiset prosessit | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Keskeiset teknologiat | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Keskeiset roolit | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| Keskeiset komponentit | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

*Kuva 15: Esimerkki suojattavien kohteiden luettelointiin käytettävästä taulukosta.*

Pohjaa käytettäessä on hyvä huomioida, että harmaalla pohjalla annettuja väliotsikoita kannattaa muokata omassa organisaatiossa käytettävään luokitteluun sopivaksi. Kehitysorganisaatiossa luokittelu voisi noudatella kehitysprosessia, kun taas bisnesyksikössä olisi luontevampaa käyttää bisnesprosessin vaiheita. Vaiheiden otsikointi auttaa tunnistamaan juuri omaan toimintaa liittyvät keskeiset suojattavat kohteet.

Suojattavien kohteiden osalta tulisi aina olla tiedossa, missä kohde sijaitsee (esimerkiksi fyysinen sijainti tai tietty palvelin/pilviympäristö) ja kuka on vastuussa kyseisen kohteen riittävästä suojaamisesta.

Perinteisessä mallissa kaikkia suojattavia kohteita koskevat riskit arvioidaan, mutta koska suojattavia kohteita voi olla valtava määrä, kannattaa käyttää sopivaa luokittelua, jonka pohjalta riskit arvioidaan ainakin aluksi vain kriittisten suojattavien kohteiden osalta. Tähän on mahdollista rakentaa esimerkiksi luottamuksellisuuteen, eheyteen, saatavilla oloon ja vaatimuksen mukaisuuteen liittyviin tasoihin pohjautu luokittelu, mutta tässä pohjassa on päädytty siihen, että kunkin kohteen osalta päätetään ilman erillistä luokittelua, tuleeko riskit arvioida vai ei.

## Riskirekisteri ja toimenpidesuunnitelma

Tärkeimpien suojattavien kohteiden osalta riskit kirjataan riskirekisteriin. Yhtä suojattavaa kohdetta kohden voidaan listata yksi tai useampia riskejä, mutta arvioinnissa tulisi pohtia ainakin:

- **Luottamuksellisuuteen**: sensitiivinen tieto on asianmukaisesti suojattu ja pääsy on rajattu
- **Eheyteen**: tiedon, järjestelmien ja prosessien johdonmukaisuus, tarkkuus ja luotettavuus on turvattu
- **Saatavilla oloon**: tieto, järjestelmät ja prosessi ovat oikea-aikaisesti käytettävissä

liittyviä riskejä. Nämä riskit luetteloidaan ja arvioidaan Kuvan 16 mukaiseen taulukkoon, joka löytyy liitteenä olevan excelin ”*Riskimatriisi*”-välilehdeltä.

| ID | Suojattava kohde | Uhka | Seuraukset | Käytössä olevat vastatoimenpiteet | RISKIARVIO (käytössä olevat vastatoimenpiteet huomioiden) | | | Riskitaso on hyväksyttävä |
|---|---|---|---|---|---|---|---|---|
| | | | | | Vakavuus | Todennäköisyys | Riskitaso | |
| | | | | | 1-5 | 1-5 | 1-25 | |
| | | | | | | | 0 | |
| | | | | | | | 0 | |
| | | | | | | | 0 | |
| | | | | | | | 0 | |
| | | | | | | | 0 | |
| | | | | | | | 0 | |
| | | | | | | | 0 | |
| | | | | | | | 0 | |
| | | | | | | | 0 | |

*Kuva 16: Riskien tunnistaminen ja arviointi.*

Tunnistetut ja arvioidut riskit käydään läpi organisaation määrittelemättä “hyväksyttävän riskitason”-rajaa vasten ja suunnitellaan vastatoimenpiteet niiden riskien osalta, jotka ylittävät hyväksyttävän riskitason. Nämä dokumentoidaan ”Toimenpidesuunnitelma”-välilehdeltä löytyvään taulukkoon, joka on esitetty seuraavassa Kuvassa 17.

| Nro | Riskin ID | Suunniteltu vastatoimenpide | Suunnitellun vastatoimenpiteen tila | Vastuuhenkilö | Tavoite pvm | Lisätietoja |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

*Kuva 17: Vastatoimenpiteiden suunnittelu.*

Vastatoimenpiteiden suunnittelussa on hyvä muistaa kaksisuuntainen linkitys tunnistettuihin riskeihin – yksi vastatoimenpide voi liittyä useampaan riskiin ja vastaavasti yhtä riskiä kohden voi olla tarve useammille

toimenpiteille. Toimenpiteen kannattaa jaotella järkevän kokoisiin palasiin, jotka on mahdollista vastuuttaa ja aikatauluttaa.

Suunnitelmien etenemistä tulee muistaa seurata säännöllisesti ja arvioida myös niiden riittävyyttä jäännösriskien arvioinnin muodossa, mikä tehdään excelin *”Riskirekisteri”*-välilehdelle. Jos toimenpiteet eivät vaikuta riskien vakavuuteen tai todennäköisyyteen, niillä ei ole riskitason kannalta merkitystä. Tavoitteena olisi lopulta saada kaikkien riskien osalta jäännösriskit hyväksyttävälle tasolle.

### Tarkistuslista ja avainsanalista riskien tunnistamisen tukena

Riskien tunnistamisen tukemiseksi excelissä on mukana myös *”Tarkistuslista”*-välilehti, johon on koottu tässä työssä esiteltyihin keskeisiin kyberturvallisuuskäytänteisiin liittyviä kysymyksiä. Kysymykset on ryhmitelty tämän raportin otsikointia mukaillen seuraavasti:

- Kyberturvallisuuden hallinta
- Turvallinen arkkitehtuuri
- Pääsynhallinta
- Järjestelmin eheys
- Verkon ja tietoliikenteen suojaaminen
- Järjestelmän valvonta
- Jatkuvuuden hallinta

Ydinkohdat on merkitty tarkistuslistaan lihavoinnilla. Tarkastuslista on myös mahdollista jakaa pienempiin osiin, kun aloitetaan tunnistamalla kunkin kysymyksen osalta vastuullinen henkilö tai organisaatio. Tämän jälkeen vastauksia voi pohtia yhdessä näiden tahojen kanssa.

Kysymyksiin vastataan asteikolla:

- OK
- Osittain OK
- Ei OK
- En tiedä
- N/A

Jos joku kohta ei ole vielä täysin kunnossa, siihen liittyvät riskit olisi hyvä arvioida ja dokumentoida riskirekisteriin.

Kyberturvallisuuden riskientunnistuspohja-excelissä on mukana myös VTT:n aktiviteetti- ja prosessimallia mukaillen tehty avainsanalista, jossa kyberturvallisuuteen liittyviä asioita on ryhmitelty kyberturvallisuuden hallinnan (ylärivi), tietovoiden (keskirivi) ja elinkaarimallin (alarivi) näkökulmista. Avainsanalistaa voi käyttää riskien tunnistamisen tukena.

## 5.2 Esimerkki riskiarvion tekemisestä

- **Suojattava kohde**: Soodakattilan automaation konfiguraatio.

- **Uhka**: Ympäristön riittämätön pääsynhallinta ja salasanojen hallinta
- **Seuraukset**: Väärät henkilöt pääsevät muuttamaan järjestelmän konfiguraatiota. Konfiguraation luottamuksellisuus ja eheys varantuvat. Tuotteen tasalaatuisuus vaarantuu ja prosessi saatetaan joutua ajamaan alas korjaustöiden ajaksi.
- **Käytössä olevat vastatoimenpiteet**: Konfiguraation muuttaminen vaatii pääsyn valvomon koneelle, kone sijaitsee lukitussa huoneessa ja kulunvalvonta on asianmukaisesti toteutettu.
- **Vakavuus**: 3 (keskinkertainen). Turva-automaation pitäisi estää henkilö- ja ympäristövahinkojen synty, mutta prosessin häiriintyminen vaikuttaa tuotantoon, joten sillä voi olla vaikutuksia liiketoiminnan jatkuvuuteen.
- **Todennäköisyys**: 4 (todennäköinen). Laadukas kulunvalvonta ei auta, koska valvomon koneelle on mahdollista ottaa suora etäyhteys, jonka suojaustaso ei ole paras mahdollinen.
- **Riskitaso**: 12 (Korkea riski). Riskien hallintatoimenpiteet ovat pakollisia. Niiden toteuttaminen tulee aloittaa mahdollisimman pian ja saattaa loppuun riskienhallintasuunnitelmassa määritellyn ajan kuluessa.

**Suunnitellut vastatoimenpiteet:**

- Dokumentoitu käyttäjätilien ja salasanojen hallintamalli, joka pitää sisällään ainakin pääsy-ja käyttöoikeuksien minimoinnin, oletussalasanojen vaihtamisen sekä vahvan tunnistautumisen konfiguraation hallintaan oikeuttavilla tileillä. Tällä varmistetaan, että konfiguraatiomuutoksia voivat tehdä vain siihen oikeutetut henkilöt.
- Kriittisten järjestelmien pääsy-yritysten logitus ja valvonta. Tämän avulla pystytään puuttumaan murtoyrityksiin nopeasti ja tarvittaessa selvittämään, millä tunnuksilla haitalliset muutokset on tehty.
- Etäyhteyksien suojaus- ja valvontatason nostaminen, joka sisältää suorien etäyhteyksien estämisen, vahvan tunnistautumisen ja riittävän valvonnan. Tämä rajoittaa asiattomien tahojen hyökkäysmahdollisuuksia järjestelmää vastaan merkittävästi.
- Konfiguraatiomuutosten logitus ja valvonta. Tämä mahdollistaa sen, että muutos huomataan nopeasti ja toipuminen päästään aloittamaan mahdollisimman pian.
- Engineering-koneen varmuuskopiointi ja sen testaus. Tämä lyhentää palautumisaikaa, kun vikaantunutta konfiguraatiota ei tarvitse kirjoittaa alusta uudestaan.

**Jäännösriskiarvio:**

- **Vakavuus**: 2 (pieni). Konfiguraatiomuutosten valvonnan avulla mahdolliset ongelmat tunnistetaan nopeasti ja testattujen palautuskäytäntöjen vuoksi oikean konfiguraation palauttaminen on nopeaa, joten vaikutuksia liiketoiminnan jatkuvuuteen ei synny.
- **Todennäköisyys**: 3 (mahdollinen). Hyökkäystä ei ole käytännössä mahdollista tehdä etänä ja sen toteuttaminen vaatii vahvan tunnistautumisen. Valvonnan ansiosta myös hyökkäysyritykset havaitaan nopeasti ja niihin voidaan puuttua.
- **Jäännösriskitaso**: 6 (keskinkertainen). Riskitasoa tulee seurata mahdollisten muutosten varalta.

## 5.3 Hyödyllistä lisämateriaalia

- Suomen Automaatioseuran julkaisema kirja ”Automaation Tietoturva –Kriittisen tuotannon turvaaminen”, https://www.automaatioseura.fi/julkaisut-kirjakauppa/automaation-tietoturva-julkaisut/ Tämän raportin kirjoittajat ovat olleet mukana tämän kirjan kirjoittajina.
- KYBER-TEO “Kyberturvallisuuden kehittäminen ja jalkauttaminen teollisuuteen” –hankkeen tulokset. Insta oli mukana myös tässä hankkeessa, https://www.insta.fi/ajankohtaista/insta-defsec-mukana-kyber-teo-hankkeessa-teollisuuden-kyberturvallisuuden-kehitt%C3%A4miseksi
- Tekesin Turvallisuusohjelman TITAN “Tietoturvaa teollisuusautomaation” -projektin tulokset, VTT https://www.vttresearch.com/sites/default/files/pdf/tiedotteet/2010/T2545.pdf
- IEC 62443 –standardisarja, jonka keskeiset osat ovat saatavilla myös suomeksi
- ISO27000-standardiperhe

## 5.4 Kiitokset

Haluamme lopuksi esittää vielä kiitokset kaikille työryhmän toimintaan ja työn katselmointiin osallistuneille arvokkaista kommenteista ja kehitysehdotuksista. Kiitokset (etunimen mukaisessa aakkosjärjestyksessä) Arttu Hanhela, Emma Kärkkäinen, Heikki Lappalainen, Ilkka Koivuniemi, Janne Peltonen, Kari Kärki, Matti Raninen, Markku Tyynelä, Petri Kuitikka, Taneli Mutikainen, Tatu Liimatainen, Toni Henriksson ja Ville Hämäläinen. Kiitokset kuuluvat myös Suomen Automaatioseuralle, kun saimme olla mukana tekemässä *Automaation Tietoturva – Kriittisen tuotannon turvaaminen*-kirjaa ja sitä kautta jalostaa omaa ajatteluamme ja työtämme eteenpäin.

SUOMEN SOODAKATTILAYHDISTYS RY, RAPORTTISARJA

1/2021 Suomen Soodakattilayhdistys ry
Soodakattila-alan yhteistoiminta
Vuosikertomus 2020
(16A0913-E0208) 21.4.2021

2/2021 Suomen Soodakattilayhdistys ry
Soodakattila-alan yhteistoiminta
Pöytäkirja. Vuosikokous 21.4.2021, Teams-kokous ja AFRY Finland Oy, Vantaa
(16A0913-E0209) 21.4.2021

3/2021 Suomen Soodakattilayhdistys ry
Soodakattilapäivä 4.11.2021
Sokos hotelli Presidentti, Helsinki
(16A0913-E0210) 4.11.2021

4/2021 Suomen Soodakattilayhdistys ry
Lime Kiln alternative fuels and emissions / Meesauunin päästöt erilaisilla polttoaineilla
Henna Hietanen, Jens Kohlmann, AFRY Finland Oy
(16A0913-E0211) 17.11.2021

5/2021 Suomen Soodakattilayhdistys ry
Ioninvaihto metsäteollisuuden vedentuotannossa – hallinta, seuranta ja toimenpiteet
Karri Aunola, Essi Korhonen, Maija Vidqvist, Anu Kettunen, Teollisuuden Vesi Oy
(16A0913-E0212) 21.12.2021

6/2021 Suomen Soodakattilayhdistys ry
Pulp mill deposit formation and aging – role of intra-deposit alkali chloride transport, Phase 2
Roland Balint, Markus Engblom, Åbo Akademi
(16A0913-E0213) 21.12.2021

7/2021 Suomen Soodakattilayhdistys ry
Recovery Boiler superheater corrosion – Impact of amount of melt at T0
Ebba Malm, Åbo Akademi
(16A0913-E0214) 21.12.2021

SUOMEN SOODAKATTILAYHDISTYS RY, RAPORTTISARJA

1/2022 Suomen Soodakattilayhdistys ry
Konemestaripäivä 7.4.2022, esitelmät
Sokos hotelli Kaarle, Kokkola, UPM-Kymmene Oyj, Pietarsaaren tehtaat
(16A0913-E0215) 7.4.2022

2/2022 Suomen Soodakattilayhdistys ry
Soodakattila-alan yhteistoiminta
Toimintakertomus 2021
(16A0913-E0216) 26.4.2022

3/2022 Suomen Soodakattilayhdistys ry
Soodakattilapäivä 27.10.2022
Lapland hotels Arena, Tampere
(16A0913-E0217) 27.10.2022

4/2022 Suomen Soodakattilayhdistys ry
Kyberturvallisuuden perusteet soodakattiloiden automaatiojärjestelmissä
Suvi Kaartinen ja Henry Haverinen, Insta Advance Oy
(16A0913-E0218) 7.11.2022