

Toni Saviahde

# PROSESSIAUTOMAATION KOKONAIS- TURVALLISUUDEN ARVIOINTI ETÄYH- TEYDEN KANNALTA

Diplomityö  
Automaatiotekniikan tiedekunta  
Jari Seppälä  
Mikko Salmenperä  
Toukokuu 2023

# TIIVISTELMÄ

Toni Saviahde: Prosessiautomaation kokonaisturvallisuuden arviointi etäyhteyden kannalta  
Diplomityö  
Tampereen yliopisto  
Automaatiotekniikan koulutusohjelma  
Toukokuu 2023

---

Työssä luodaan kirjallisuuden pohjalta arvioinnille viitekehys ja sitä sovelletaan automaatiotekniikanlaitoksella olevaan tislautusautomaatiojärjestelmään. Tehdään turvallisuuden arviointi etäkäytön aikana prosessin kokonaisturvallisuudesta. Turvallisuus arvioinnin yhteydessä tulleiden ongelmien ja uhkien perusteella tehdään parannus ehdotuksia sekä perustelut miksi juuri ehdotetulla tavalla kannattaisi parantaa prosessin kokonaisturvallisuutta. Teoria osiossa käsitellään myös mitä eroja yritysverkolla ja automaatioverkolla on sekä niiden yhdistymisen riskejä. Nyky päivänä yhä enemmän on yritysverkkojen ja automaatioverkkojen integroitumista.

Työssä toteutetaan etäyhteyden kannalta riskianalyysi käyttämällä rusettimallista riskianalyysia, jolla tunnistetaan mahdollisia riskejä ja uhkia prosessille ja prosessiympäristölle. Tämän analyysin pohjalta kehitetään prosessin turvallisuutta parantavia ehdotuksia. Parannus- ja kehitysehdotukset annetaan perustuen tutkittuun materiaaliin automaatio prosessin kokonaisturvallisuudesta.

Dokumentin lopussa on taulukkomuotoon tehtynä ennaltaehkäisevät toiminnot erilaisten uhkien torjumiseksi sekä lieventäviä toimintoja seurausten minimoimiseksi. Näistä myös jäännös riskit kirjoitetaan taulukkoihin. Taulukossa 1 on ennaltaehkäisevät toiminnot uhille, joita rusettimalleissa on tullut esille. Taulukossa 2 on esitetty lieventävät toiminnot rusettimalleissa esiintyvälle seurauksille.

Avainsanat: Tietoturva, Kokonaisturvallisuus, Prosessiturvallisuus, Riskianalyysi, Rusettimalli, Oppimisympäristö.

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

# ABSTRACT

Toni Saviahde: Evaluation of the overall safety of process automation in terms of remote connection

Master of Science Thesis

Tampere University

Master's Degree Programme in Automation Technology

May 2023

---

On the job based on the literature, a reference framework is created for the evaluation, and it is applied to the distillation automation system at the Department of Automation technology. A safety assessment will be made during remote use of the overall safety of the process. Based on the problems and threats that came up during the safety evaluation, suggestions for improvement are made, as well as justifications for why it would be worthwhile to improve the overall safety of the process in the way that was proposed. In the theory part, the architecture of industrial automation and secure industrial control systems architecture in terms of cyber security are reviewed. In theory part differences between a business network and an automation network becomes familiar as well as the risks of combining them. Nowadays there is more and more integration of business networks and automation networks.

In terms of remote connection, the work implements a risk analysis using a bowtie model risk analysis which identifies possible risks and threats to the process and the process environment. Based on this analysis, proposals are developed to improve the safety of the process. Suggestions for improvement and development are given based on the studied material about the overall safety of the automation process.

At the end of the document there is two tables which includes preventive actions for different kinds of threats and mitigating actions to alleviate the consequences. The residual risks are also written to the tables. Table 1 shows the preventive actions for the threats that have emerged in the bowtie models. Table 2 shows mitigating actions for the consequences occurring in the bowtie models.

Keywords: Information security, Total security, Process safety, Risk analysis, Bowtie model, Learning environment.

The originality of this thesis has been checked using the Turnitin OriginalityCheck service.

# ALKUSANAT

Tämä diplomityö on tehty Tampereen Yliopiston automaatiotekniikan laitokselle etäyhteyksien- ja automaation kokonaisturvallisuuteen liittyen. Haluan kiittää mahdollisuudesta tehdä tämä mielenkiintoinen projekti automaatiotekniikan laitokselle. Kiitän diplomityöni ohjaajia Jari Seppälää ja Mikko Salmenperää hyvästä ohjauksesta työssäni.

Suurimmat kiitokset kuuluvat perheelleni sekä avopuolisolleni. He ovat tukeneet ja kannustaneet minua opintojeni ajan. Haluan myös kiittää avopuolisoni perhettä saamastani tuesta opintoihin.

Porissa, 25.5.2023

Toni Saviahde

# SISÄLLYSLUETTELO

1.	JOHDANTO .....	1
1.1	Ongelma .....	1
1.2	Ratkaisumetodit .....	1
1.3	Diplomityön rakenne .....	2
2.	PROSESSIAUTOMAATION KOKONAISTURVALLISUUS ETÄYHTEYDEN AIKANA .....	3
2.1	Teollisuuden automaatio- ja ohjausjärjestelmät.....	3
2.1.1	Teollisuuden automaatio- ja ohjausjärjestelmien arkkitehtuuri.....	4
2.1.2	Automaatioverkko .....	6
2.2	Turvallinen teollisuuden ohjausjärjestelmien tietoturva arkkitehtuuri.....	7
2.2.1	Palomuurit.....	10
2.2.2	Demilitarisoitu alue.....	11
2.2.3	Välityspalvelin .....	11
2.2.4	Turvavyöhykemallit .....	12
2.3	Etäyhteys .....	13
2.3.1	Verkko- ja järjestelmärajaukset .....	14
2.3.2	Etäyhteyden todennus .....	15
2.3.3	Etäyhteyksien keskitetyt kontrollipisteet .....	15
2.3.4	Etäyhteyksien seuranta.....	15
2.4	Prosessiautomaation turvallisuutta parantavia keinoja .....	16
2.4.1	Prosessi turvallisuus .....	16
2.4.2	Toiminnallinen turvallisuus .....	19
2.4.3	Turva-automaatio.....	19
2.4.4	Riskinpienennys keinoja.....	25
2.5	Riskianalyysi tapoja.....	27
2.5.1	Rusettimalli .....	27
2.5.2	Hyökkäyspuu analyysi .....	28
3.	KOLONNIAUTOMAATIO .....	30
3.1	Tislausautomaatiojärjestelmä.....	30
3.2	Mihin tislausautomaatiojärjestelmää käytetään yliopistolla .....	31
3.3	Työn tavoitteet .....	32
4.	HYBRIDIOPETUKSEN RISKIANALYYSI KÄYTTÄEN RUSSETTIMALLIA.....	34
4.1	Riskianalyysi syöttöpumpun päälle jäämisestä.....	34
4.2	Riskianalyysi tislauskolonnin ylivuodolle.....	35
4.3	Riskianalyysi lämmitysyksikön ylikuumenemisesta tai ylipaineistumisesta.....	37
4.4	Riskianalyysi tuotannon vaarantumisesta.....	39
4.5	Riskianalyysi paikalla olevan henkilön tapaturmasta .....	40
5.	TULOKSET.....	42
5.1	Syöttöpumpun päälle jääminen .....	42

5.2	Tislauskolonnin ylivuoto .....	45
5.3	Lämmitysyksikön ylikuumentuminen ja ylipaineistuminen .....	48
5.4	Tuotannon vaarantuminen .....	52
5.5	Paikalla olevan henkilön tapaturma .....	57
5.6	Tulosten yhteenveto.....	59
6.	YHTEENVETO.....	65
	LÄHTEET .....	66

# LYHENTEET JA MERKINNÄT

ICS	Teollisuuden automaatio- ja ohjausjärjestelmä (Industrial Control System)
IT	Informaatio teknologia (Information Technology)
OT	Operatiivinen teknologia (Operative Technology)
VPN	Virtuaalinen erillisverkko (Virtual Private Net)
FAT	Tehdastesti (Factory Acceptance Test)
SAT	Hyväksymistesti (Site Acceptance Test)
DMZ	Demilitarisoitu alue (Demilitarized Zone)
IDMZ	Teollisuuden demilitarisoitu alue (Industrial Demilitarized Zone)
PLC	Ohjelmoitava logiikka (Programmable Logic Controller)
PAC	Ohjelmoitava automaatio ohjain (Programmable Automation Controller)
SCADA	Valvomo ohjelmisto (Supervisory Control and Data Acquisition)
MES	Tuotannonohjaus järjestelmä (Manufacturing Execution System)
ERP	Toiminnanohjaus järjestelmä (Enterprise Resource Planning)
PID-säädin	suhteellinen, integroiva ja derivoiva säädin (Proportional, Integrative and Derivative controller)
PCS	Prosessin ohjausjärjestelmä (Process Control System)
DCS	Hajautettu ohjausjärjestelmä (Distributed Control System)

# 1. JOHDANTO

Teknologian kehittyessä sekä parantuessa, teollisuusautomaation laitteet vaativat yhä enemmän kriittistä huomiota toiminnallisen turvallisuuden kannalta. Toiminnallinen turvallisuus on yhä tärkeämmässä roolissa ja sillä pystytään ehkäisemään laitteiden virheistä aiheutuvia haittavaikutuksia sekä onnettomuuksia. [5]

Tässä dokumentissa tehdään kirjallisuuskatsaus prosessiautomaation kokonaisturvallisuuden kannalta sekä perehdytään valittuihin riskianalyysi tapoihin, joita voi käyttää kokonaisturvallisuuden arvioinnissa. Kirjallisuuskatsauksessa opittuja asioita sovelletaan tislusautomaatio ympäristöön ja sen perusteella tehdään parannus ehdotuksia turvallisen etäyhteyden parantamiseksi tislusautomaatiojärjestelmään. Tislusautomaatiojärjestelmän liiketoimintana ja tuotantona ovat opintopisteet ja tämä vaikuttaa moniin asioihin tässä dokumentissa kuten turvallisuusmenetelmiin prosessissa.

## 1.1 Ongelma

Järjestelmään pitää pystyä ottamaan opetus- tai koulutuskäytössä useampi henkilö samaan aikaan etäyhteyden ja nyt pohditaan kuinka taataan turvallinen järjestelmä sekä automaatiojärjestelmän toiminnallinen eheystaso, kun käytetään etäyhteyttä järjestelmässä? Tällä tarkoitetaan monen eri henkilön samanaikaista etäyhteyttä prosessiin, jotka haluavat tehdä muutoksia ohjelmallisesti prosessin logiikkaan. Tämä ei saisi vaarantaa prosessin turvallisuutta. Millaisia riskejä tämä tuo järjestelmän fyysiseen ympäristöön sekä ohjelmalliseen ympäristöön? Kartoitus tehdään pohjautuen tutkittuihin dokumentteihin prosessiautomaation kokonaisturvallisuudesta ja näitä tietoja mukaillen tehdään parannus ehdotuksia järjestelmään, jotka parantaisivat prosessin kokonaisturvallisuutta sekä suojaisi prosessin ympäristöä sekä laitteistoa vahingoilta.

## 1.2 Ratkaisumetodit

Kirjallisuuden pohjalta luodaan arvioinnille viitekehys ja sitä sovelletaan automaatiotekniikanlaitoksella olevaan tislusautomaatiojärjestelmään. Tehdään turvallisuuden arviointi etäkäytön aikana prosessin kokonaisturvallisuudesta. Turvallisuus arvioinnin yhteydessä tulleiden ongelmien ja uhkien perusteella tehdään parannus ehdotuksia sekä

perustelut miksi juuri ehdotetulla tavalla kannattaisi parantaa prosessin kokonaisturvallisuutta. Tutkitaan prosessin osia ja komponentteja sekä mahdollisia riskejä, joita monen henkilön etäyhteys aiheuttaa. Riskianalyysiä soveltaen saadaan nostettua esille kriittisimmät riskit.

### **1.3 Diplomityön rakenne**

Luvussa kaksi kerätään taustatietoa diplomityön kannalta keskeisiin asioihin. Luvussa käydään yleisesti läpi prosessiautomaation kokonaisturvallisuuden kannalta keskeisiä asioita. Näihin liittyy teollisuuden automaatio- ja ohjausjärjestelmät sekä niiden arkkitehtuuri, automaatioverkon arkkitehtuuri, turvallinen teollisuuden ohjausjärjestelmien tietoturva arkkitehtuuri, etäyhteys ja siihen liittyvät turvallisuus asiat, prosessiautomaation turvallisuutta parantavat keinot sekä riski analyysi malli.

Luvussa kolme esitellään tislusautomaatiojärjestelmä, johon tämä diplomityö kohdistuu. Tässä luvussa ensiksi kerrotaan lyhyesti mikä on tislusautomaatio johon, riskianalyysit tehdään ja miten se pääpiirteittäin toimii. Sen jälkeen käydään läpi tisluskolonnin käyttötapoja yliopistolla. Viimeisenä kerrotaan mikä on tislusautomaation tutkimuksen tarkoitus ja mitä tutkimuksessa otetaan huomioon.

Luvussa neljä tehdään riski analyysi diplomityön kohteesta liittyen prosessin kokonaisturvallisuuteen etäyhteyden muodostamisessa. Riskianalyysi tehdään rusettimallilla, josta kerrotaan kappaleessa 2.5.

Luvussa viisi esitellään työn tulokset ja mitä tehtiin sekä kuinka tehdyt muutokset parantaisivat automaatiojärjestelmän kokonaisturvallisuutta. Luvussa sovelletaan luvussa kaksi tutkittua aineistoa sekä kappaleessa neljä tehtyjä riskianalyysyjä.

Luvussa kuusi kirjoitetaan yhteenveto diplomityöstä. Tiivistetään saadut tulokset luvusta viisi. Miten diplomityö onnistui kokonaisuudessaan ja päästiinkö asetettuihin tavoitteisiin. Tuliko diplomityön aikana jatkotutkimuskohteita.

## 2. PROSESSIAUTOMAATION KOKONAISTURVALLISUUS ETÄYHTEYDEN AIKANA

Tässä luvussa tutkitaan yleisesti prosessiautomaation kokonaisturvallisuutta sekä etäyhteyttä. Tähän sisältyy teollisuuden automaatio- ja ohjausjärjestelmät sekä niiden arkkitehtuuri, automaatioverkon arkkitehtuuri, turvallinen teollisuuden ohjausjärjestelmien tietoturva arkkitehtuuri, etäyhteys ja siihen liittyvät turvallisuus asiat, prosessiautomaation turvallisuutta parantavat keinot sekä riski analyysi malli. Luvun alussa käydään läpi teollisuuden automaatio- ja ohjausjärjestelmiin liittyviä asioita. Tässä kappaleessa käydään myös läpi automaatiojärjestelmän arkkitehtuuria kuten, mitä eri tasot automaatiojärjestelmässä sisältävät. Seuraavaksi käydään yleisesti etäyhteyksistä asiaa. Sen jälkeen käydään läpi prosessi automaation turvallisuutta parantavia keinoja, johon sisältyy turva-automaatio ja erilaiset muut tavat parantaa prosessin turvallisuutta sekä riskin pienennyskeinoja ja viimeisenä kerrotaan rusettimallisesta riskianalyyseistä ja hyökkäyspuu riskianalyyseistä ja niiden käyttämisestä riskianalyysin tekemiseen.

### 2.1 Teollisuuden automaatio- ja ohjausjärjestelmät

Tässä kappaleessa tutkitaan teollisuuden automaatio- ja ohjausjärjestelmien arkkitehtuuria sekä automaatio verkon arkkitehtuuria. Arkkitehtuuri kappaleessa käydään läpi teollisuuden automaatio- ja ohjausjärjestelmien eri tasoja ja mitä laitteita sekä toimintoja kyseiset tasot sisältävät. Automaatio verkko kappaleessa käydään läpi automaatioverkossa olevat tasot sekä asioita, jotka ovat tärkeitä automaatioverkon näkökannalta.

Kriittistä infrastruktuuria sisältävissä teollisissa ympäristöissä käytetään teollisuuden automaatio- ja ohjausjärjestelmiä (Industrial Control System, ICS). ICS mahdollistaa teollisten prosessien kontrolloimisen sekä valvomisen operaattoreille sekä tukee päivittäisiä tuotannon toimintoja. Tämän kaltaisissa järjestelmissä turvallisuus on suurimpia huolenaiheita ja riippuen laitoksen kriittisyydestä, hyökkäys laitokseen aiheuttaisi pahimmassa tapauksessa haitallisia vaikutuksia maan turvallisuuteen sekä talouteen. Tästä syystä on tärkeää suunnitella nämä järjestelmät alusta alkaen luotettaviksi [36]. Tyypilliseen teollisuuden automaatio- ja ohjausjärjestelmään on rakennettu ylläpitotyökaluja useiden verkkoprotokollien kerroksellisten verkkoarkkitehtuurien avulla sekä lukuisia ohjaussilmukoita, ihmisrajapintoja ja etädiagnostiikkaa [27].

### 2.1.1 Teollisuuden automaatio- ja ohjausjärjestelmien arkkitehtuuri

Teollisuuden automaatio- ja ohjausjärjestelmien arkkitehtuurissa on viisi eri tasoa [46]. Kuvasta 4 nähdään eri tasot ja mitä ne sisältävät.

**Tasoa 0** kutsutaan kenttätasoksi, joka on ohjaushierarkian alimmainen taso. Taso 0 sisältää kenttälaitteet kuten pumput, moottorit, sensorit, venttiilit ja monia muita kenttälaitteita, jotka ovat suoraan yhteydessä laitokseen tai laitteistoon. Nämä kenttälaitteet tuottavat tietoja, joita muut tasot käyttävät prosessin valvomiseen sekä ohjaamiseen [13][39].

**Tasolla 1** on PLC:t eli ohjelmoitavat logiikat ja PAC:t eli ohjelmoitavat automaatio ohjaimet. Tätä tasoa kutsutaan ohjaustasoksi. Ohjelmoitavalla logiikalla ohjataan valmistus- ja tuotantoprosesseja. Viestintäverkkoa käyttäen on ohjelmoitava logiikka yhdistetty kenttälaitteisiin sekä teollisuuden käytönohjaus- ja valvontajärjestelmän isäntäohjelmistoon [13][39]. PLC:n käytön lisäksi teollisuuden käytönohjaus- ja valvontajärjestelmissä niitä käytetään myös pienempien ohjausjärjestelmäkokonaisuuksien ensisijaisina ohjaimina. Ne mahdollistavat erillisten prosessien ohjaamisen kuten autojen kokoonpanolinjat sekä voimalaitosten noenpuhaltimien säätämisen. Edellä mainitut topologiat eroavat teollisuuden käytönohjaus- ja valvontajärjestelmistä sen takia, koska niissä ei ole keskusohjauspalvelua eikä ihmisen ja koneenvälisestä käyttöliittymää. Näiden asioiden puuttumisen vuoksi, nämä pienemmät ohjausjärjestelmäkokonaisuudet tarjoavat ensisijaisesti suljetun silmukan ohjauksen ilman ihmisen suoraa osallistumista prosessiin. Ohjelmoitavissa logiikoissa on ohjelmoitava muisti, johon käyttäjä voi tallettaa tiettyjä toimintoja. Tallennettavia toimintoja ovat I/O-ohjauslogiikan toiminta, ajoitus toiminto, laskenta toiminto, PID-säätimen eli suhteellisen, integroivan ja derivoivan säätimen toiminta sekä datan ja tiedostojen käsittelyt [27].

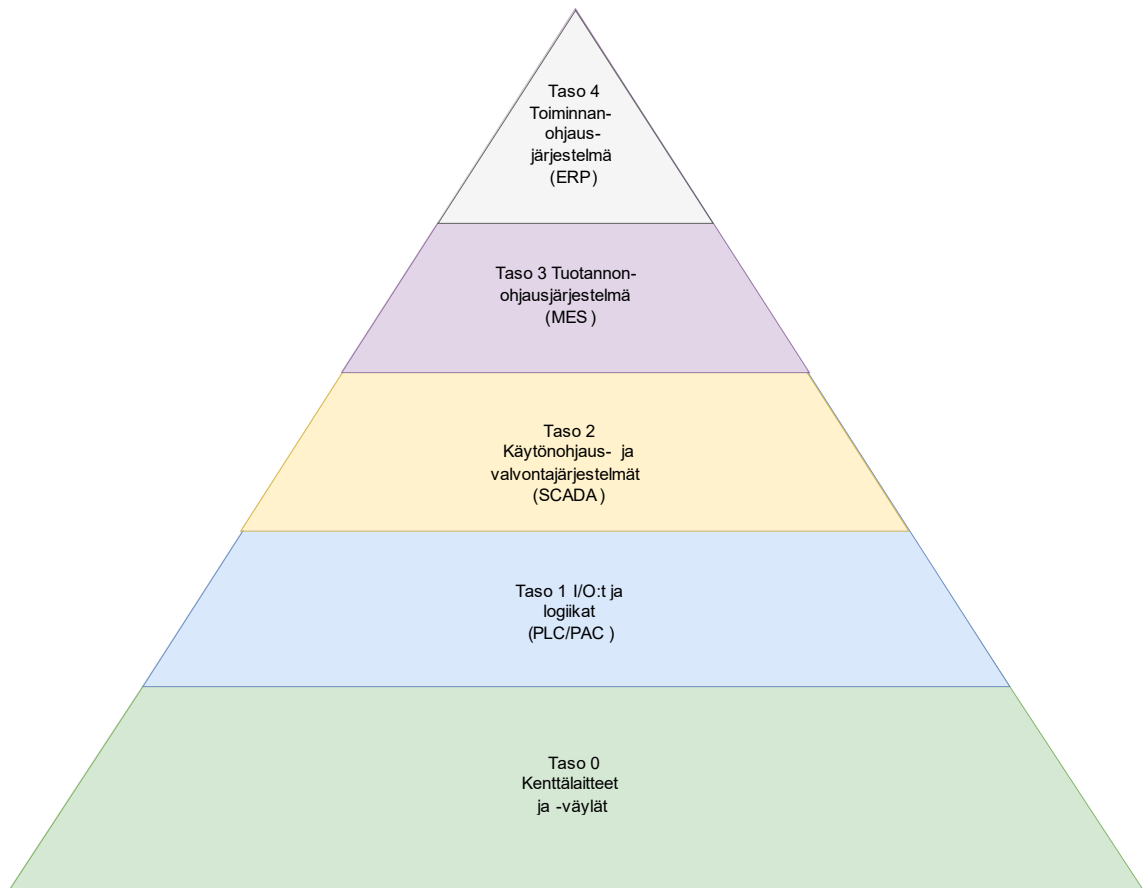
**Taso 2** on teollisuuden käytönohjaus- ja valvontajärjestelmä taso (SCADA, Distributed Control System, DCS, Process Control System, PCS). Nämä järjestelmät valvovat sekä ohjaavat prosessia tai prosessin osia ja prosessin järjestelmiä, jotka on levitetty rajatulle tai suurelle alueelle maantieteellisesti. Tason tärkein ja pääasiällisin tehtävä on kerätä tietoja kenttätason toimilaitteilta sekä välittää kyseisten laitteiden hallinta käyttäen isäntäohjelmistoa. Prosessia seurataan etäyhteys menetelmää käyttäen tietojen ja hälytyksien tallentamiseksi. Tällä tavalla voidaan myös laitteita säätää sekä laittaa pois päältä tai päälle oikeaan aikaan. SCADA-järjestelmä tarjoaa myös lisää toimintoja kuten erilaisten grafiikoiden esittämisen, erilaisia hälytyksiä sekä mahdollistaa tietojen tallentamisen [13][39]. SCADA-järjestelmät integroivat tiedonkeruujärjestelmät tie-

donsiirtojärjestelmien sekä ihmisten ja koneiden välisten käyttöjärjestelmä ohjelmistojen kanssa yhteen. Tällä tavoin saadaan tarjottua keskitetty valvonta- ja ohjausjärjestelmä lukuisille prosessissa oleville tuloille ja lähdoille. Nämä järjestelmät on suunniteltu keräämään kenttälaitteilta tietoja, siirtämään tiedot keskustietokoneelle ja esittämään graafisesti tai tekstimuotoisesti operaattorille kerätyt tiedot, joiden perusteella operaattori pystyy valvomaan ja ohjaamaan koko järjestelmää valvomosta melkein tosiaikaisesti. Melkein tosiaikaisella tarkoitetaan sitä, että yhteyksissä laitteiden ja järjestelmien välillä on pienimuotoinen viive, joka johtuu yhteyksien nopeuksista. SCADA-järjestelmille tyypillisiä laitteita ovat ohjauskeskukseen laitettu ohjauspalvelin, viestintälaitteet kuten puhelinlinja, kaapeli tai radio sekä maantieteellisesti hajautetut kenttäpaikat, jotka koostuvat ohjelmoitavista logiikoista, joilla ohjataan toimilaitteita ja valvotaan antureita sekä etäpääteyksiköitä. Yleisesti ottaen SCADA-järjestelmät on suunniteltu vikasietoisiksi järjestelmiksi. Järjestelmiin on tehty redundanssi mutta se ei ole välttämättä riittävä, jos järjestelmään kohdistuu haitallinen hyökkäys [27]. Lisää tietoa SCADA-järjestelmistä löytyy esimerkiksi lähteen [27] kappaleesta 2.3.2 SCADA systems.

**Taso 3** on tuotannonohjaus taso (MES). Tämä taso on vastuussa prosessin aikatauluksesta, materiaalien käsittelemisestä, kunnossapidosta, inventaarioista ja monista muista asioista [13][39]. Tämä taso pienentää kuilua toiminnanohjausjärjestelmän ja ohjausjärjestelmien välillä ja käyttää tuotannon valmistustietoja kuten tilauksia, laitteita ja resursseja tuotantoprosessien tukemiseksi. Ajan myötä myös MES on kehittynyt integroimaan useita laajennuksia erilaisten tuotannontoimintojen suorittamiseksi käyttäen tietotekniikan kehityksen edistysaskelia [38].

**Taso 4** on toiminnanohjausjärjestelmä taso (ERP). Tämä taso on teollisuusautomaation korkein taso ja se hallinnoi koko ohjaus- tai automaatiojärjestelmää. Tällä tasolla käsitellään kaupallista toimintaa, joka sisältää mm. tuotannon suunnittelua, tilauksia, myyntiä sekä markkina- ja asiakasanalyysjä [13][39].

Kuvassa 1 on esitetty eri teollisuusautomaatiojärjestelmän tasot pyramidimuodossa.



**Kuva 1 Prosessiautomaation tasot esitettynä pyramidi muodossa. Muokattu lähteestä [13]**

### 2.1.2 Automaatioverkko

Teollisuusautomaatioverkon ensisijainen tehtävä on kommunikaatio erilaisten laitteiden välillä kuten ohjelmoitavien logiikoiden ja kenttälaitteiden välillä [37]. Automaatioverkossa tietoturvan toteutus on erittäin tärkeää, koska tässä verkossa on automaatiojärjestelmän kaikki toimilaitteet sekä valvomot ja ohjainyksiköt. Jos automaatioverkkoon pääsee kolmansiä osapuolia käsiksi, voivat he aiheuttaa suurtakin tuhoa järjestelmässä. Valvomatonta tietoliikennettä ei saa koskaan sallia tehdasverkoissa, vaikka niiden tietoturva olisikin toteutettu oikealla tavalla. Valvoton tietoliikenne on aina tietoturvariski. On myös hyvä muistaa, että automaatiojärjestelmän sisäverkossa voi toimia ihmisiä, jotka omaavat taidot sekä motiivin automaatiojärjestelmän häiriöiden aiheuttamiseen. Tästä syystä toimistoverkkoja ja automaatioverkkoja on pidettävä yhtä epäluotettavina kuin internet-verkkoa automaation näkökannalta. Myös automaatioverkkoa on pidettävä yhtä epäluotettavana kuin internet-verkkoa sisäverkon näkökannalta, koska automaatioverkosta pystytään tunkeutumaan sisäverkkoon, jos näiden verkkojen välinen tietoturva ei ole kunnossa. Sisäverkon ja automaatioverkon hallinta pitää olla samassa tietoturvaorganisaatiossa, kuitenkin yksi ihminen/taho ei voi ottaa vastuuta

molemmista ja tästä syystä näiden verkkojen tietoturvavastuut on pidettävä erillään toisistaan [20]. Automaatioverkossa on yleensä kolme erilaista tasoa kuten hallintotaso, automaatiotaso ja kenttätaso [6].

**Hallintotasolla** sijaitsee valvomot kuten paikalliset valvomot ja etävalvomot. Tällä tasolla on käyttäjä rajapinnat, joista ohjataan järjestelmää ja saadaan yhteys käyttäjän ja järjestelmän välille. Yhteyden muodostamiseen käytetään yleensä järjestelmän lähiverkkoa, mutta yhteyksien muodostamiseen käytetään myös TCP-IP protokollaa. Nykyään useita järjestelmiä voidaan käyttää etänä, mutta etäkäyttöön sisältyy kaikenlaisia tietoturvariskejä [6].

**Automaatiotasolla** on erilaisia ohjainyksiköitä, säätimiä ja I/O moduuleita, jotka ovat alakeskuksissa. Ohjelmat prosessin ohjaukseen I/O moduulien välillä sijaitsevat alakeskuksissa ja prosessia ohjataan yleensä lähiverkossa [6][37].

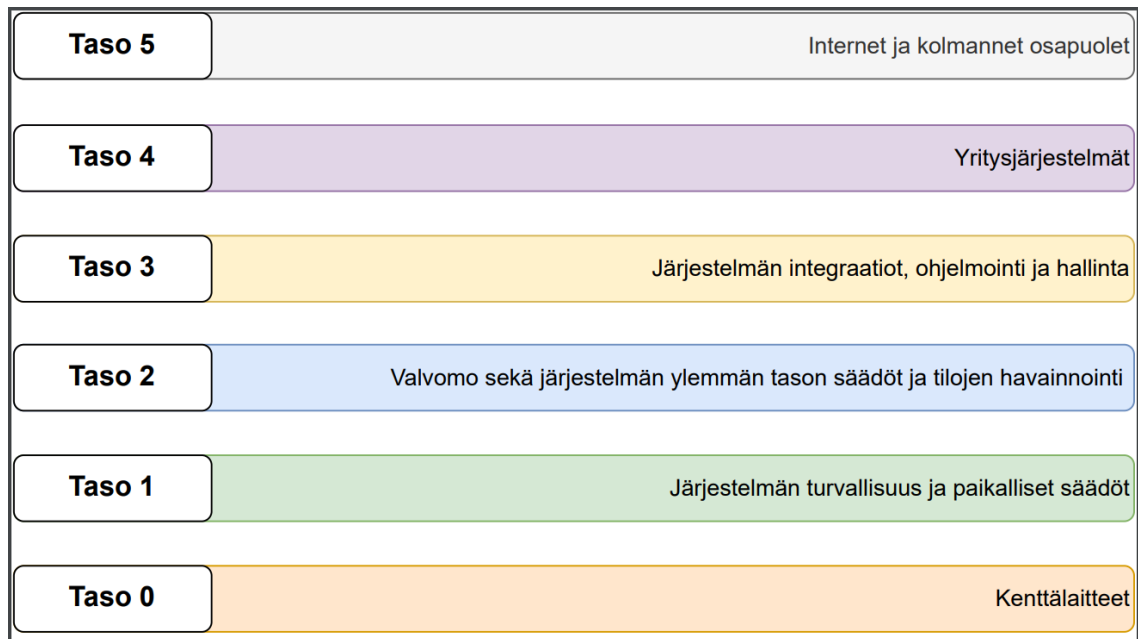
**Kenttätasolla** taas on erilaiset säätö- ja mittalaitteet kuten esimerkiksi anturit, venttiilit, pumput ja moottorit. Mittalaitteet mittaavat prosessissa tapahtuvia asioita ja säätölaitteet säätelevät prosessia automaatiotasolta tulleiden ohjaustietojen mukaan. Mitattavia suureita prosessissa ovat lämpötila, virtaus, paine-ero, tilavuus sekä monien aineiden pitoisuudet [6].

## 2.2 Turvallinen teollisuuden ohjausjärjestelmien tietoturva arkkitehtuuri

Tuotantolaitokselle ja prosessille kyberturvallisuuden kannalta katsottuna paras suunnittelu tapa on pitää automaatioverkko (Operative Technology network, OT verkko) ja yritysverkko (Information Technology network, IT verkko) erillään toisistaan fyysisesti ja loogisesti sekä varmistaa ettei internetistä ole pääsyä OT verkkoon. Tällä teollisuuden ohjausjärjestelmien tietoturva arkkitehtuuri mallilla saadaan pienennettyä riskiä etänä tehdyistä hyökkäyksistä OT verkkoon IT verkon kautta [1]. OT verkko pidetään erillään IT verkosta koska OT verkot ovat yleisesti ottaen huomattavasti haavoittuvaisempia kyberturvallisuuden kannalta johtuen siitä, ettei niihin ole suunniteltu kyberturvallisuutta. [40][41].

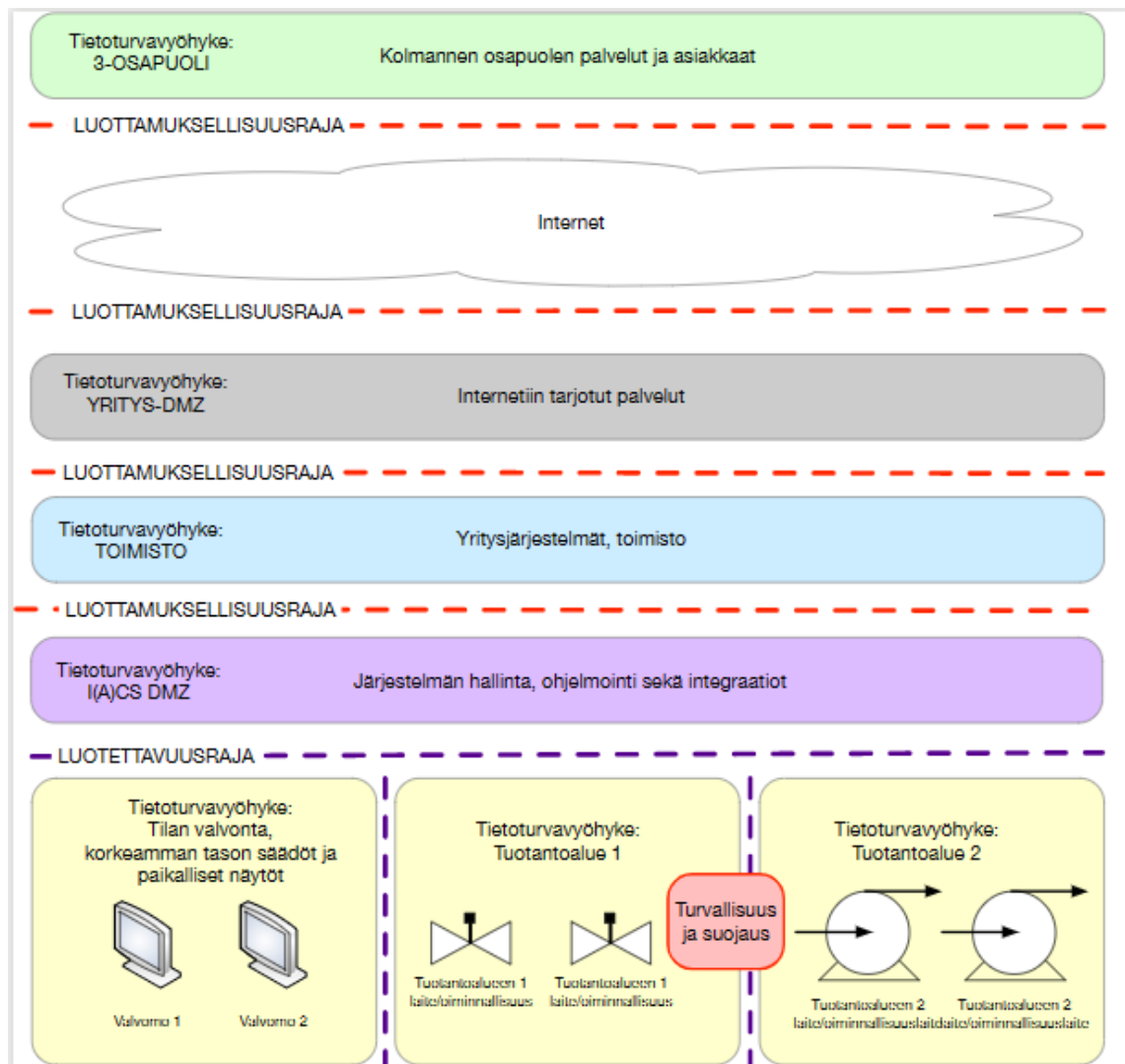
Eristetty prosessin hallintaverkko on suhteellisen turvallinen verkkoympäristö, johon kohdistuvat yleisimmät uhat ovat fyysinen pääsy verkkoon, luonnon tai ihmisen aiheuttama onnettomuus ja tyytymättömien työntekijöiden aiheuttamat haitalliset toimet verkossa eli sabotaasi. Eristetyt prosessin hallintaverkot eivät yleensä ole yhteydessä internettiin, koska internetissä on niin monia potentiaalisia uhkia prosessille. Kun tarvi-

taan yhteys OT verkon ja IT verkon välille nousee riski taso OT verkkoa kohden merkittävästi [1]. Tällaisessa tapauksessa paras vaihtoehto turvallisuuden kannalta on käyttää näiden verkkojen erottamiseen automaatiojärjestelmän arkkitehtuurissa olevaa automaation eteisverkkoa, joka sisältää palomuurin. Verkkojen välillä kulkevat tiedot pitää mennä tämän eteisverkon välityspalvelimien kautta. Suoraa yhteyttä yritysverkon ja automaatioverkon välillä ei hyväksytä, koska suora yhteys aiheuttaisi suuria riskejä automaatioverkkoon [2]. Kuvassa 2 on esitetty tietoturvallinen automaatiojärjestelmän verkkoarkkitehtuuri tasoittain ja mitä kyseiset tasot sisältävät.



**Kuva 2 Automaatiojärjestelmän verkkoarkkitehtuurin tasoista muokattu lähteestä [16].**

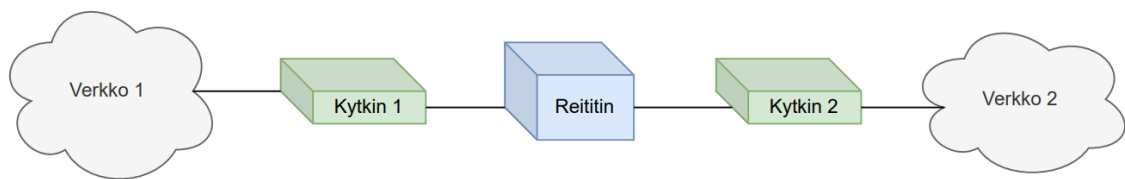
IT/OT yhteydet lisääntyvät koko ajan teollisuudessa, jonka johdosta on huolehdittava tarpeellisista kyberturvallisuus toiminnoista molempien verkkojen suojaamiseksi. Tästä syystä usein tavoitteena on tehdä rajasuojaus näiden kahden verkon välille, joka antaa luvan halutulle informaatiolle kulkea näiden verkkojen välillä samalla kun se suojaa OT verkkoa IT verkon uhilta. Rajasuojaus toteutetaan asentamalla rajasuojauslaite, jonka avulla pystytään ohjaamaan tietoa turvattujen alueiden välillä, joilla on erilaiset turvallisuusvaatimukset. Rajasuojauslaitteiksi sisällytetään mm. palomureja, virustorjunta ohjelmistoja, reitittimiä, salattuja tunneleita, välityspalvelimia ja monia muita [1][27]. Kuvassa 3 esitetään automaatio järjestelmän tietoturvavyöhykkeitä.



**Kuva 3 tietoturvyöhykkeet haettu lähteestä [16].**

Kuten kuvan 3 alareunasta nähdään niin OT verkko on osioitu useampaan pienempään verkkoon eli OT verkko on verkkosegmentoitu. Jokainen pienempi verkkosegmentti on osioitu erilaisten tekijöiden takia. Tekijöitä voivat olla esimerkiksi laitteet, jotka vaativat tiukempaa tietoturvaa, jolloin näiden laitteiden tuotantoalue segmentoidaan omaan pienempään OT verkkoon vaadittavan luotettavuuden saavuttamiseksi. Verkkosegmentointi on yksi tehokkaimmista tietoturvatavoista verkkoarkkitehtuurillisesti, jonka organisaatio voi toteuttaa OT verkonsuojaamiseksi. Segmentointi tekee kyberhyökkäjästä päämäärän saavuttamisen huomattavasti vaikeammaksi. Verkon segmentoinnilla ja erotteulla pyritään minimoimaan arkaluonteisiin tietoihin pääsy järjestelmiltä ja ihmisiltä, jotka eivät sitä tarvitse, samalla varmistetaan, että organisaatio voi jatkaa toimintaansa tehokkaasti. Erilaisia tekniikoita ja teknologioita käyttäen riippuen verkon arkkitehtuurista sekä kokoonpanosta pystytään saavuttamaan arkaluonteisiin tietoihin pääsyn minimointi sekä organisaation tehokas toiminta samanaikaisesti [27]. On olemassa kahdenlaisia seg-

mentointi tapoja, fyysinen ja looginen segmentointitapa. On tärkeää erottaa näiden kahden tyyppisen segmentoinnin eroavaisuudet toisistaan. Fyysisellä segmentoinnilla tarkoitetaan kahden toisistaan erillään olevan fyysisen verkkolaitteen käyttämistä kahden verkon välisen eristyksen toteuttamiseen. Esimerkkinä kahdella kytkimellä tehty eristys eli kytkin yksi tukisi verkkoa yksi ja kytkin kaksi tukisi verkkoa kaksi reitittimellä, joka hallitsee tietoliikennettä näiden kahden verkon välillä. Kun taas loogisella segmentoinnilla tarkoitetaan yhden verkkolaitteen sisällä käytettyjä loogisia toimintoja saavuttaakseen saman tuloksen kuin edellä mainitulla fyysisellä segmentoinnilla [28]. Kuvassa 4 on esitetty fyysinen segmentointi käyttäen kahta kytkintä sekä yhtä reititintä kahden verkon eristämiseen.



**Kuva 4 fyysinen segmentointi. Muokattu lähteestä [47]**

### 2.2.1 Palomuurit

Palomuri hallitsee verkkoliikennettä, joka kulkee sen läpi suojelemaan verkkoa ulkopuolisilta uhilta ja tästä syystä sitä voidaan kutsua tietoverkon portiksi ja portinvartijaksi. Palomuurit asetetaan yleensä suojelemaan lähiverkkoa kuten esimerkiksi kodin tai yrityksen verkkoa. Yleensä Palomuri asetetaan tietoverkon laidalle, jolloin verkkoliikenne kulkee sen lävitse. Tällä tavoin saadaan paras mahdollinen hyöty tietoturvan kannalta [8][31][37][39]. Ulkopuoliset uhat voivat päästä vain tiettyjen yhdyspisteiden kautta lähiverkkoon. Yhdyspisteillä tarkoitetaan portteja [21]. Palomuri suodattaa verkkoliikennettä eikä päästä muuta kuin haluttua liikennettä verkossa eteenpäin. Suodattamiseen on asetettu tietyt säännöt, joiden perusteella palomuri päästää liikennettä eteenpäin [8][30][31][39]. Asetettuja sääntöjä erilaisten yhteydenottoopyyntöjen pois sulkemiseksi voivat olla esimerkiksi IP-osoitteeseen, porttiin, protokollaan, domain-nimeen, ohjelmaan tai avainsanaan perustuvat pyynnöt [21]. On hyvä kuitenkin muistaa, ettei palomuri yksinään tuo tarvittavaa suojaa verkon uhkia vastaan, tästä syystä tarvitaan anti-virus ohjelma palomuurin tueksi [7]. Palomureja on monia erilaisia kuten verkkoa suojelevat palomuurit, fyysiset palomuurit ja ohjelmalliset palomuurit [8].

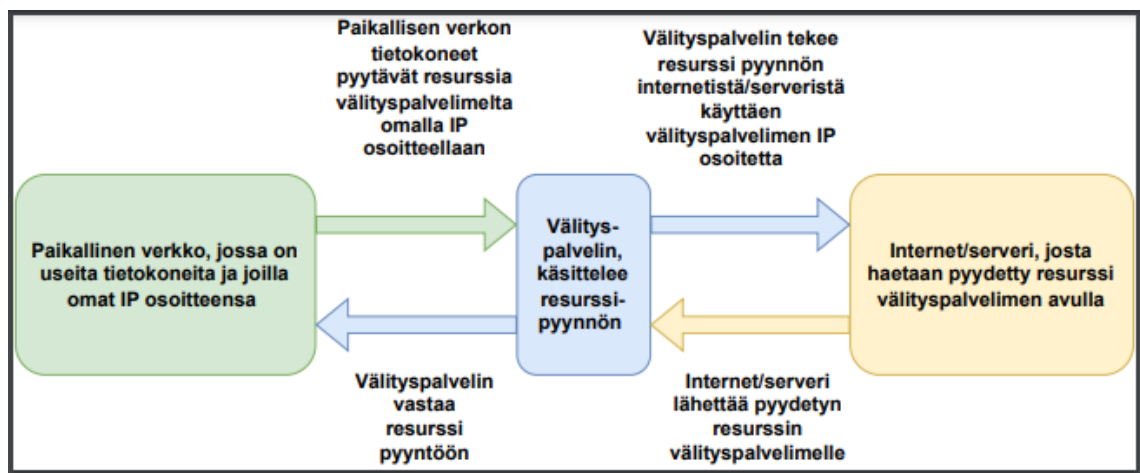
## 2.2.2 Demilitarisoitu alue

Jotkut organisaatiot ja yritykset asettavat osan tietoverkostaan demilitarisoidulle alueelle (DMZ, demilitarized zone), joka on suojarakenne erottaen verkon toisesta verkosta. Tällä tavalla mahdollistetaan demilitarisoidun verkkoalueen tiedon siirto ulospäin tarvittaville resursseille [1][37]. DMZ:lla tehdään suojamuuri yritysverkon ja teollisuusautomaatio verkon välille. Tämä tapa on normaali käytäntö perinteisissä IT verkoissa, mutta uusi teollisuusautomaatioyhteisössä. DMZ on alaverkko kahden palomuurin välissä. Kyseiset palomuurit ovat automaatio- ja yritysverkon välissä. Verkkoliikenne ei koskaan liiku suoraan DMZ:n läpi, joten suoraa yhteyttä yritysverkosta automaatioverkkoon ei saada. Jos DMZ on suunniteltu oikealla tavalla. Pitää se saada irroitettua järjestelmästä siinä tapauksessa, että se on saastunut. Kun DMZ on irrotettu järjestelmästä antaa se silti automaatioverkon toimia ilman häiriöitä. Nyt kun kyberhyökkäyksiä on enemmän kuin koskaan maailmanlaajuisesti, on kiinnitettävä erityistä huomiota siihen, miten teollisuusautomaation prosessit saadaan parhaiten tehtyä turvalliseksi [17]. DMZ:n sisälle voidaan myös valita halutut serverit ja muut resurssit, jotka halutaan erottaa jostain toisesta verkosta. Resurssi voi olla esimerkiksi reititin, serveri, palomuuuri tai monta tietokonetta sisältävä ryhmä. Demilitarisoituja alueita käytetään yleensä eristämään automaatioverkko ja yritysverkko toisistaan. Sillä luodaan kahden verkon välille niin kutsuttu neutraali alue, jolla rajoitetaan ulkoista tiedonvälitystä yrityksen kanssa organisaation tietoturvapoliitiikan määrittelyn perusteella. Mikä tahansa teollisuuden ohjausjärjestelmä, johon yritysverkko vaatii pääsyn pitäisi laittaa OT/IT demilitarisoituun alueeseen ja ainoastaan niihin servereihin, jotka sijaitsevat demilitarisoidulla alueella tulisi olla pääsy yritys verkosta. Yhdellä tai useammalla palomuurilla hallitaan pääsyä demilitarisoidulle alueelle ja ainoastaan ne tietoliikenne portit, jotka on aivan pakko olla auki yritysverkon kommunikoinnin muodostamiseen, avataan palomuurista [1][32].

## 2.2.3 Välityspalvelin

Välityspalvelin (Proxy) estää ulkopuolisia pääsemään paikalliseen verkkoon käsiksi ja estää paikallisesta verkosta suoran yhteyden ulkopuolisiin resursseihin kuten internet. Välityspalvelin antaa paikallisverkossa olevien laitteiden ottaa epäsuoran yhteyden verkkoon, joka on reititetty välityspalvelimen kautta. Paikallisverkossa oleva laite ottaa yhteyden välityspalvelimen serveriin tunnistautumalla tai ilmantunnistautumista ja pyytää tarvitsemaansa resurssia eriserveriltä. Resurssi pyyntöä käsitellessä välityspalvelin joko palauttaa pyydetyn resurssin omasta välimuistista kopiona tai lähettää pyynnön toiselle serverille. Resurssin pyytämiseen käytetään vain välityspalvelimen IP-osoitetta, jolloin ulkopuolisen tunkeutujan on mahdotonta päästä käsiksi paikalliseen isäntään (lo-

cal host) koska sen osoitetiedot eivät näy internetiin. Välityspalvelimen tekemässä suodatus prosessissa jokainen paketti puretaan, arvioidaan ja kootaan uudelleen. Tästä syystä tämän kaltainen yhteys on huomattavasti hitaampi kuin monilla muilla palomuurityypeillä. Välityspalvelimella olevat suodattavat palomuurit ovat konfiguroitu tarkastelemaan kokonaisia paketteja johdonmukaisuuden, sovellustyypin ja sopivien porttien takia. Välityspalvelimen palomuurin oletama tieto pitää sopia yhteen tiedon kanssa, joka pyrkii pääsemään välityspalvelimen porttien läpi paikallisverkossa olevalle laitteelle. Jos ne eivät sovi yhteen tuntematon paketti pudotetaan ja yhteys katkaistaan kohteeseen [1]. Kuvassa 5 on esitetty välityspalvelimen toiminta.



**Kuva 5** esitetty välityspalvelimen toiminta. Muokattu lähteestä [1]

## 2.2.4 Turvavyöhykemallit

Verkossa olevien resurssien ja tiedon suojaamista varten tehdään turvavyöhykkeitä, jotka ovat verkon lohkoja. Nämä lohkot tehdään tietynlaisille turvallisuus tasoille riippuen tiedon sekä resurssien kriittisyydestä sekä haavoittuvuudesta. Käytännössä ideana on laittaa arvokkaimmat sekä kriittisimmät tiedot ja resurssit hyvin suojaaville turvarakenteille [1]. Esimerkiksi automaatioverkko on erotettava turvallisesti ja tehokkaasti omaksi lohkokseen muista yritysverkoista kuten toimistoverkosta. Yleisesti erilaiset ja erilliset palomuurit ovat hyviä tapoja erilaisten verkkojen erottamiseen toisistaan. Myös automaatioverkkojen osajärjestelmät tulisi erotella toisistaan omiin lohkoihinsa [20]. Monikerroksisten luottamusvyöhykkeiden kaavoitusmallit ovat loogisimmat kaavoitusmallit IT verkkojen vyöhykkeiden luomiseen. Sisäisin vyöhyke sisältää arkaluontoisimmat tiedot ja resurssit, joita suojaavat vyöhykkeet niiden ympärillä. Myös jokainen seuraava vyöhyke antaa suojaa viereisille vyöhykkeille [1].

## 2.3 Etäyhteys

Suunniteltaessa turvallista teollisuusverkkoa tai automaatioverkkoa pitää ottaa huomioon etäyhteys järjestelmään. Etäyhteys on välttämätön paha nykyaikana automaatiojärjestelmissä. Organisaatio tarvitsee etäyhteyttä ja etäkäyttöä moniin eri tarpeisiin kuten esimerkiksi käyttönotetun teollisuusautomaation ohjausjärjestelmä yleensä sisältää kolmansien osapuolien kanssa tehtyjä sopimuksia. Esimerkiksi yhteydenotto järjestelmään etänä kaikkina ajankohtina pitää olla mahdollista ongelmien korjaamiseksi. Teollisuuden automaatio ohjausjärjestelmän toimittajan tukihenkilöt saattavat työskennellä eri aikavyöhykkeillä eri puolilla maailmaa edellä mainittujen tiukkojen palveluvaatimusten täyttämiseksi. Myös teknikot tarvitsevat mahdollisuuden etäyhteyden ottamiseen automaatiojärjestelmään diagnostiikan ja ongelmien ratkaisemista varten [28].

Automaatiojärjestelmässä on useita käyttötasoja. Tästä syystä suositellaan henkilökohtaisten tunnusten käyttämistä varsinkin ylemmällä käyttötasolla, josta päästään kriittisiin tietoihin ja resursseihin kiinni. Alemmalla käyttötasolla voi olla yhteiset käyttäjätunnukset, joilla pääsee rajattuihin ominaisuuksiin käsiksi. Henkilökohtaisia tunnuksia suositellaan mm. siksi, että ylemmän tason järjestelmälokeista kuten VPN-palvelusta saadaan selvitettyä takautuvasti millä tunnuksilla etäyhteys oli järjestelmään muodostettu. Etäyhteyden muodostamista varten suositellaan, ettei yhteys ole koko ajan käytettävissä vaan se pitäisi erikseen hyväksyä jokaisella etäyhteydenotto kerralla. Tällaisten toimintojen tekemiseen on useita ratkaisuja. Ratkaisuja, joita voidaan käyttää ovat ohjelmistopohjaisia ratkaisuja, kertakäyttöisten koodien käyttö, jotka vaihtuvat jokaisen kerran jälkeen. On myös työläämpiä vaihtoehtoja kuten verkkoliitynnän kytkeminen manuaalisesti automaatiolaitteeseen tarvittaessa sekä mekaanisia kytkimiä, jotka käydään manuaalisesti laittamassa päälle tarvittaessa. Työläämmissä vaihtoehtoissa riskeinä on, ettei yhteyttä muisteta poistaa [2]. Kuten lähteessä [2] on kerrottu, turvallisuutta etäyhteyksien ottamiseen saadaan parannettua teknisesti rajaamalla verkko- ja järjestelmätasojä, todennetaan etäyhteyden ottaja turvallisesti, seurataan etäyhteyksiä keskittämällä etäyhteyksien kontrollipisteet sekä luomalla varayhteydet.

Turvallisen etäyhteyden saavuttamiseksi käytetään erilaisia etäyhteyden salausmenetelmiä. Salausmenetelmiä on monia erilaisia kuten AES, DES ja RSA. Näillä menetelmillä pyritään takaamaan tietojen kiistämättömyys, eheys sekä luotettavuus. Salausmenetelmän pitäisi olla tarpeeksi vahva, ettei sen salausta pystytä purkamaan liian lyhyessä ajassa eikä liian pienillä resursseilla. Ajan ja resurssien määrittäminen ovat riippuvaisia siitä mitä tietoja halutaan salata sekä kuinka tärkeitä kyseiset tiedot ovat. Etäyh-

teyden salausmenetelmien tarkoituksena on estää ulkopuolisia pääsemästä hyväksikäyttämään etäyhteyttä. Salausmenetelmät voidaan jakaa kahteen eri ryhmään, symmetrisiin salausalgoritmeihin ja epäsymmetrisiin salausalgoritmeihin [18].

**Symmetrisillä** salausalgoritmeilla käytetään samaa avainta tietojen vastaanottamiseen sekä lähettämiseen. Salausavaimesta saadaan suoraan johdettua lähetettyjen tai vastaanotettujen tietojen purkamiseen vaadittu avain. Tähän kategoriaan kuuluvat muun muassa AES ja DES salausmenetelmä. Tämä menetelmä on nopea ja tästä syystä sitä käytetään, mutta menetelmän ongelmana on hallita avaimia. Hallinnasta vaikeaa tekee se, että purkamiseen ja salaamiseen käytetään samaa avainta. Tästä syystä käytetään todennustunnusta tai epäsymmetristä salausta kun siirretään avaimia käyttäjältä toiselle. Jonosalaus ja lohkosalaus ovat luokat, joihin symmetriset salausmenetelmät voidaan vielä jakaa [19]. Näitä ei tässä tekstissä käydä sen tarkemmin, joten jos haluat tarkempaa tietoa näistä luokista niitä löytää lähteen [19] luvusta 2.

**Epäsymmetrinen** salausmenetelmä eroaa symmetrisestä salausmenetelmästä siinä, että epäsymmetrisessä salausmenetelmässä käytetään avainparia tietojen salaamiseen. Avainparit sisältävät kaksi avainta, jotka eivät ole identtiset. Toinen avaimista on yksityinen ja toinen taas julkinen. Tähän kategoriaan kuuluu muun muassa RSA salausmenetelmä. Avainparit toimivat seuraavasti, yksityisellä avaimella salatut tiedostot voidaan purkaa tai avata julkisella avaimella ja julkisella avaimella salatut tiedostot voidaan purkaa tai avata yksityisellä avaimella. Toisin kuin symmetrisissä salausmenetelmissä tässä menetelmässä avainten hallinta on helppoa, mutta menetelmän salausavaimet ovat huomattavasti pidempiä kuin symmetrisissä salausmenetelmissä. Siksi niitä on huomattavasti raskaampaa prosessoida. Saavuttaakseen sama turvataso kuin symmetrisillä salausmenetelmillä, tulee avainten olla pidempiä. Epäsymmetristen salausavainten purkaminen on helpompaa jos niillä on jotkin vaaditut matemaattiset ominaisuudet [19].

### 2.3.1 Verkko- ja järjestelmärajaukset

Kohdekoneeseen pääsyä rajoitetaan mahdollisimman paljon esimerkiksi etätyöpöytäprotokollalla ja https-yhteyksillä tai muilla protokollilla, jotka käyttävät VPN-yhteyttä saadakseen yhteyden hyppykoneeseen. Edellä mainituilla tavoilla saadaan rajoitettua etäyhteydellä saavutettavaa hyökkäys pinta-alaa ja mitä enemmän kyseistä pinta-alaa saadaan rajoitettua, sitä turvallisempi järjestelmä on. Suoraa VPN-yhteyttä kohdeverkkoon ei suositella laitteelle, koska haittaohjelmien on helppo päästä sitä kautta laitteeseen käsiksi, siksi suositellaan vaiheittaista yhteyden muodostamista, jonka ansiosta haittaohjelmien on vaikeampaa edetä. Kohdejärjestelmän käyttöoikeudet tulee rajata

minimiin kolmansien osapuolten käyttäjätunnuksille. Tällä tarkoitetaan sitä, jos esimerkiksi joku kolmasosapuoli tarvitsee vain katseluoikeudet työnsä suorittamiseen, tällöin ainoastaan katseluoikeudet annetaan käyttäjälle, jos järjestelmä tukee tällaista toimintoa [2].

### 2.3.2 Etäyhteyden todennus

Etäyhteyden todentamisessa suositellaan käytettäväksi vahvaa tunnistusta, jolla tarkoitetaan lisätunnistusmenetelmää. Tätä tunnistustapaa käytetään käyttäjätunnuksen ja salasanan lisäksi. Edellä mainittu tunnistusmenetelmä saadaan toteutettua sovelluksella tai laitteella, joka tuottaa kertakäyttöisiä koodeja sekä tekstiviestinä tulevalla koodilla tai älykorteilla. Jos käyttäjätunnus ja salasana päätyisi ulkopuolisen käsiin niin vahvan tunnistautumisen avulla kyseinen ulkopuolinen ei pääse suoraan ottamaan yhteyttä, koska yhteyden muodostamisen yhteydessä kysytään vielä jokin koodi tai muu vahvantunnistuksen menetelmistä [2]. Teollisuusautomaation ohjausjärjestelmän etäkäytön todennusta varten kannattaa rakentaa erillinen palvelin valtuutetuille käyttäjille, jotka ovat organisaation ulkopuolelta kuten myyjät ja integraattorit. Tällä tavoin luodaan mahdollisuus toimittajakohtaisten käyttöoikeustasojen luomiseksi ja niille voidaan antaa ohjausmekanismeja, joilla rajoitetaan monia erilaisia tekijöitä, jotka vaihtelevat vuorokaudenajasta liikennemalleihin. Eri rooleille omistetut todennuspalvelimet mahdollistavat kybertapahtuman nopeat lieventämistoimet ja turvallisuus vastatoimet. Tämä antaa järjestelmän omistajalle mahdollisuuden dynaamisesti lukita toimittajan tai integraattorin käyttöoikeudet. Tämä mahdollistaa myös nopean käyttöoikeuksien palauttamisen tarvittaessa [29].

### 2.3.3 Etäyhteyksien keskitetyt kontrollipisteet

Keskitetyn kontrollipisteen teknisten ominaisuuksien ja suorituskyvyn pitäisi riittää etäyhteyksien seurantaan, yhteyslokiin, josta nähdään käyttäjätunnukset, jotka ovat otaneet etäyhteyden järjestelmään ja edellisessä kappaleessa mainittuun vahvaan tunnistusmenetelmään. Kontrollipisteiden tietoturvaa pystytään kehittämään korkeammille tasoille koko ajan [2].

### 2.3.4 Etäyhteyksien seuranta

Etäyhteyksien seuranta tapahtuu keskitetyn kontrollipisteen tasolla, jossa pitäisi ainakin seurata epäonnistuneet ja onnistuneet kirjautumiset, vahvojen tunnistautumisten epäonnistumiset ja onnistumiset, kohdejärjestelmät, johon otetaan yhteys sekä lähdeosoitteet yhteyksistä, milloin yhteydet on muodostettu ja yhteyksien kesto järjestelmässä, siirretyn datan määrä yhteyksien aikana ja komennot, joita on kohdejärjestelmässä

tehty. Tietomurtojen ja hyväksikäyttötapausten selvittäminen jälkikäteen on sitä helpompaa mitä laajemmin saadaan yhteyden toimintaa seurattua ja kirjattua ylös kohdejärjestelmässä tai kontrollipisteessä [2].

## 2.4 Prosessiautomaation turvallisuutta parantavia keinoja

Kokonaisturvallisuudella saadaan paljon vaikutettua prosessin turvallisuuteen ja turva-automaatiolla sitä saadaan vielä tehostettua parempaan suuntaan. Kokonaisturvallisuus koostuu turva-automaatiosta ja muista suojauskerroksista sekä niiden oikeasta toiminnasta [11]. Toiminnallinen turvallisuus on kokonaisturvallisuuden osa. [11][22]

### 2.4.1 Prosessi turvallisuus

Prosessin turvallisuutta saadaan parannettua monilla erilaisilla tavoilla. Tapoja parantaa turvallisuutta ovat laitteiston sijoittaminen, tekniset ratkaisut, henkilöstön osaamisen kehittäminen ja toimintatapojen osaamisen kehittäminen. Prosessiturvallisuudelle parhaan mahdollisen kokonaisuuden luomiseksi vaaditaan monia erilaisia menetelmiä. Prosessiturvallisuutta voidaan mitata erilaisilla mittaristoilla kuten tapaturma tilastoihin perustuvilla tiedoilla, näihin tietoihin sisältyy tapaturmataajuus sekä poissaolot johtuen tapaturmasta. Tapaturmatilastoissa näkyvissä loukkaantumisissa suurin osa liittyy työturvallisuuteen eikä niinkään prosessiturvallisuuteen. Tämän takia yritysten pitäisi myös tehdä omaan toimintaansa liittyviä ja soveltuvia prosessiturvallisuusmittaristoja. Prosessiturvallisuuteen vaikuttaa merkittävästi myös yrityksen selkeiden ääriivojen luominen turvallisuuskulttuurille yrityksessä [10]. Pitää muistaa, että kun tehdään merkittäviä prosessilaitoksen laajennuksia, asettaa se monia haasteita prosessiturvallisuudesta vastaaville ohjelmille. Laitoksen laajennusprojekteja tehdään muun muassa markkinatilanteen muuttuessa. Siihen pyritään vastaamaan laitoksen kapasiteettia kasvattamalla. Tällaisissa tapauksissa prosessiturvallisuus ei ole keskeinen suunnittelunmuuttuja, joten laajennuksia ei tehdä prosessiturvallisuuden takia, mutta tiloja voidaan muokata prosessiturvallisuuden parannuksien toteuttamiseksi. Tästä syystä on välttämätöntä, että prosessiturvallisuus toiminto on alusta alkaen mukana kaikissa suunnittelu- ja toteutusvaiheissa projektissa [34].

Prosessiturvallisuuden mittareita käyttämällä järjestelmällisesti saadaan tietoa siitä, onko laitoksen prosessiturvallisuus riittävällä tasolla vai tarvitaanko toimenpiteitä prosessiturvallisuuden takaamiseksi. Prosessiturvallisuusmittarit tuovat ilmi millä tasolla laitoksen tai järjestelmän turvallisuusjohtamisjärjestelmän tehokkuus on, varoittavat ennakkoon laitoksessa tai järjestelmässä kehittyvistä ongelmista, tehostavat onnetto-

muusvaaran ennakointia ja tästä syystä saadaan pienennettyä onnettomuuksien todennäköisyyksiä sekä pystytään varautumaan mahdollisiin seurauksiin paremmin. Mittareilta saatujen tietojen perusteella voidaan tehdä ennakoivia toimia, jotka parantavat laitteiden luotettavuutta. Mittareilla saadaan kerättyä tietoa systemaattisesti prosessin ja prosessiturvallisuusjohtamisjärjestelmän tilasta sekä niiden avulla pystytään etsimään osa-alueet, joissa laitoksella tai järjestelmällä on parannettavaa. Mittarit myös tuovat esiin laitoksen henkilöstölle prosessiturvallisuuden merkitystä ja tällä tavoin edistävät myös turvallisuuskulttuuria laitoksessa sekä helpottavat jo tehtyjen toimenpiteiden vaikutuksien seuraamista. Muita turvallisuustason seuraus toimenpiteitä ei pystytä korvaamaan prosessiturvallisuusmittareilla, niillä vain täydennetään muita seuraus toimenpiteitä. Riskien arviointi mittarina voidaan käyttää esimerkiksi Bowtie -mallia [10]. Tästä mallista ja sen käyttämisestä löytyy enemmän tietoa tämän dokumentin kappaleesta 2.5.

Prosessiturvallisuusmittarit yleensä jaetaan kahteen kategoriaan, ennakoiviin ja jälkikä-teismittareihin. Ennakoivat mittarit kertovat milloin on tarpeellista toimia, jos asetettujen raja-arvojen sisällä ei pysytä, tuovat esille miksi ei saavutettu määritettyjä turvallisuustavoitteita. Ennakoivia mittareita pidetään myös prosessin eheyden mittareina. Ennakoivia mittareita ovat muun muassa:

- Poikkeamat turvallisista toiminta rajoista. Tällä tarkoitetaan sitä, kun prosesseissa on erilaisia vaiheita kuten järjestelmän ylös- ja alasajot sekä prosessin normaali toiminta ja niille on yleensä määritelty ylä- ja alaraja-arvot. Jos nämä raja-arvot ylitetään, prosessi ajetaan turvalliseen tilaan manuaalisesti tai turva-automaation avulla. Seurattavat parametrien suureet ovat virtausmäärä, paine, lämpötila, pH, konsentraatio ja niin edelleen.
- Aikataulutetut ennakkohoitojen ja tarkastusten toteuttaminen turvallisuuskriittisille laitteille. Turvallisuuskriittisiin laitteisiin kuuluu muun muassa paineastiat, varastosäiliöt, hätäalasajolaitteet, vuodonilmaisimet, putkistot ja pumput.
- Keskeneräisten tehtävien määrä, jos tapana on valmiiksi tehtyjen tehtävien sulkeminen.
- Turvallisuuskoulutusten pitäminen henkilöstölle.
- Turvallisuuden edistämiseksi tehdyt investoinnit.
- Kuinka usein tehdään turvallisuuskierros ja kierroksen pitää myös sisältää prosessiturvallisuutta, jotta niitä voidaan pitää prosessiturvallisuuden yhtenä mittarina.

- Miten usein johtohenkilöt kiertävät laitoksella.
- Palavereissa tulee ottaa huomioon myös prosessiturvallisuus organisaation eritasoilla.
- Turvajärjestelmien testaus, toimiiko turvajärjestelmä oikealla tavalla vikatilanteessa.
- Ohjeiden päivitykset, kuinka usein tehdään ja paljonko aikaa vievät tuntitasolla.
- Henkilökunnalle tehtävät osaamisarviointit.
- Paljonko on tehty aloitteita prosessiturvallisuuteen liittyen.
- Riskinarviointien päivitysten määrä sekä niiden toimenpiteiden tila.
- Onko dokumentit päivitetty kuten esimerkiksi layout-kuvat, PI-kaaviot, pelastussuunnitelma, ajoparametrit, sähkökuvat jne.
- Kun muutostenhallinnalle on määritetty jotkin vaatimukset, muutostenhallinta mittareilla seurataan, miten suuri osa määritetyistä vaatimuksista täytti tavoitteensa.
- Paljonko on tehty ja on tekemättä tilapäisiä korjauksia.
- Työlupien volyyymi, jotka on täytetty ohjeiden mukaisesti [10].

Jälkikäteismittareilla voidaan päätellä, päästiinkö suunniteltuun lopputulokseen jo tehdyillä turvallisuustoimenpiteillä, onko määriteltyyn tilaan päästy vai ei, mutta ei ota kantaa siihen miksi on päästy tai ei ole päästy määriteltyyn tilaan, ennakoivien mittareiden laatua, saadaan tapahtuneiden tapahtumien seurauksena tunnistettua ja korjattua järjestelmien haavoittuvuudet. Jälkikäteismittareita ovat muun muassa:

- Aktivoituvatko turvallisuusjärjestelmät määritetyllä tavalla.
- Prosessi laitteiden vikaantumishistoria.
- Virheiden määrä.
- Turhat varolaitteiden sekä valvontalaitteiden hälytykset sekä virheelliset toiminnot.
- Reaktioiden määrä, joita ei haluta.
- Prosessin komponenttien tai putkistojen vuotojen määrä tai prosessissa tapahtumien syttymisien määrä.
- Järjestelmän alasajot, joita ei ole suunniteltu.

- Järjestelmän virheistä tehtyjen raporttien ja raporttien käsittelyiden määrä.
- Häätäjärjestelmien käyttöä vaativien tilanteiden määrä.

Prosessiturvallisuuden mittareita on vielä useita muitakin, joita ei ole tähän listattuna [10]. Lähteen [10] mukaan kirjasta ”Guidelines for Risk Based Process Safety” löytyy prosessiturvallisuus mittareista lisää esimerkkejä. Prosessiturvallisuus mittarit toimiakseen tehokkaasti vaativat jatkuvaa kehittämistä [10].

### 2.4.2 Toiminnallinen turvallisuus

Toiminnallinen turvallisuus on kokonaisturvallisuuden osa, joka on riippuvainen järjestelmän sekä laitteistojen oikeanlaisista toiminnoista niiden saamien tietojen perusteella. Hyvä esimerkki toiminnallisesta turvallisuudesta nähdään moottorin yllämmöltä suojaavan laitteen käytössä. Yllämmöltä suojaava laite saa tiedon lämpötila-anturilta, joka on sijoitettu moottorin käämeihin ja lämpötilan noustessa liian korkeaksi yllämmötilalta suojaava laite sammuttaa moottorin. Toiminnallisen turvallisuuden saavuttamiseksi on kaksi vaatimusta turvatoiminnan vaatimukset sekä järjestelmän turvallisuuden eheyden vaatimukset. Toiminnallisen turvallisuuden saavuttamisen haasteita. Turvatoimintoja tehdään yhä enemmän elektronisilla, sähköisillä ja ohjelmoitavilla elektronisilla järjestelmissä. Kyseiset elektroniset järjestelmät ovat yleisesti ottaen niin monimutkaisia järjestelmiä, että on mahdotonta määrittää kaikkia vikaantumisen muotoja tai testata kaikkia mahdollisia järjestelmän toimintoja. Tämä on yksi haaste toiminnallisen turvallisuuden saavuttamiseksi. Myös järjestelmän suunnittelu tavalla, jolla estetään vaaraa aiheuttavat vikaantumiset tai niiden hallinta syntyessään on haasteellista [22].

### 2.4.3 Turva-automaatio

Turva-automaatio on käyttöautomaatiosta erillään oleva turva-automaatiojärjestelmä, jossa turvatoimintoja suoritetaan. Teollisuusprosessin käyttöautomaatiossa on lukituksia, hälytyksiä ja suojaustoimintoja. Kyseisiä toimintoja ei kuitenkaan luokitella turva-automaatioksi, silti niiden toiminnasta on huolehdittava, koska nekin ovat osana prosessien riskienhallintaa. Prosessin automaatiojärjestelmässä on tehtävä kaikki tarpeelliset turvatoiminnot, jotta vältetään onnettomuudet. Turva-automaatiota käytetään vain, jos muilla tavoilla ei saada prosessia turvalliseksi. Turva-automaation on toimittava luotettavasti sen koko elinkaaren ajan [3]. Lähteen [3] mukaan seuraavat säädöskohdat koskevat erityisesti prosessiteollisuuden turva-automaatiota:

- ”Kemikaaliturvallisuuslaki 390/2005 10 §: onnettomuuksien ehkäisemiseksi on tehtävä kaikki tarpeelliset toimet ja ne on toteutettava suunnitelmallisella ja järjestelmällisellä tavalla.” [3]

- ”Painelaki 1144/2016 5 §: painelaite on suunniteltava ja valmistettava, sitä on hoidettava ja käytettävä ja se on tarkastettava niin, ettei se vaaranna kenenkään terveyttä, turvallisuutta eikä omaisuutta.” [3]
- ”Valtioneuvoston asetus vaarallisten kemikaalien teollisen käsittelyn ja varastoinnin turvallisuusvaatimuksista 856/2012 50 § (ns. automaatiopykälä) edellyttää, että prosessissa on järjestelmä, jolla vaaratilanne voidaan havaita riittävän ajoissa sekä estää tai rajoittaa tapahtuman seuraukset mahdollisimman vähäisiksi. Pykälässä mainitaan myös turva-automaatio yhtenä turvajärjestelmänä, mutta siinä ei suoraan vaadita sen käyttämistä, jos onnettomuuksien seuraukset voidaan estää tai rajoittaa muilla keinoilla. Turva-automaation suunnittelussa on huomioitava riippumattomuus käyttöautomaatiosta sekä turvatoimintojen luotettavuus. Lisäksi pykälässä vaaditaan, että turva-automaatio tai muut turvajärjestelmät ovat tarvittaessa käytettävissä myös onnettomuustilanteessa. Voi siis olla tarve suojata laitteita tai huomioida onnettomuusvaikutukset järjestelmän sijoituksessa.” [3]

Turva-automaatiossa sovelletaan standardissa IEC 61511-1 esitettyjä turva-automaation elinkaarivaiheisiin sidottuja vaatimuksia. Tällä tavoin saadaan käsiteltyä turva-automaation vaatimuksia ja toimenpiteitä järjestelmällisesti. Elinkaarimallissa olevat vaiheet on tehtävä suunnitellusti annettujen kriteerien mukaisesti pätevien tahojen toimesta [3]. Turva-automaation elinkaarimallin erivaiheissa pitää varmistaa, ettei turva-automaatiolaitteista tai järjestelmistä aiheudu vahinkoja. Tällä tavalla voidaan turva-automaation tekemisen pääasiallisina osa-alueina pitää toiminnallisen turvallisuuden järjestelmällistä hallintaa ja elinkaarimallin noudattamista [4]. Alla esitelty Tukesin verkkosivuilta lähteestä [3] löydetyn turva-automaation elinkaarimallin erivaiheet ja niiden vaatimukset sekä tavoitellut lopputulokset.

### **Vaihe 0. Laitoksen tai järjestelmän suunnittelu ja hankinta:**

Vaiheen 0 vaatimuksia:

Turva-automaation suunnittelun yhdistäminen laitoksen tai järjestelmän muun suunnittelun kanssa huomioon ottaen säädökset, standardit sekä muut tekniset spesifikaatiot. Suunnittelun alussa on tunnistettava merkittävät vaarat järjestelmässä tai laitoksessa. Perussuunnittelu vaiheen pitää edetä tarpeeksi pitkälle ja kun perussuunnittelussa on päätetty riskeihin varautumisesta, voidaan päättää turva-automaation tarpeellisuudesta. Laitoksen tai järjestelmän tilaajalla on vastuullaan asettaa turva-automaatiolle

vaatimukset sekä kehittää järjestelmälliset toimintatavat turva-automaation eri elinkaari-vaiheille. Kyseiset vaatimukset ja järjestelmälliset toimintatavat on tuotava tehokkaasti esille hankinnan eri osapuolille. Tehokkaan ja luotettavan turva-automaatiojärjestelmän luomiselle ehdottomana edellytyksenä on käyttää turva-automaation elinkaarimallia. Jos laitoksessa tai järjestelmässä käytetään vaarallisia kemikaaleja, selvitetään luvitus-tarve sekä lupahakemuksien tekeminen kyseisten kemikaalien käsittelyä ja varastointia varten. Jos järjestelmässä tai laitoksessa on painelaitteita, niihin liittyviä vaatimuksia on toimittajalla oleva turva-automaation laadunhallintajärjestelmä sekä tuntemus perus-standardista IEC 61508 ja tämän standardin tietojen soveltamisesta toimittamisessaan järjestelmissä. Toiminnalliselle turvallisuudelle tekee arvioinnin kolmasosapuoli ja arviointi pitää aloittaa elinkaaren alusta. Turva-automaation osalle, joka suojaa painelaitteita, tekee arvioinnin jokin ilmoitettu laitos [3].

Vaiheen 0 Tavoitellut lopputulokset:

Järjestelmän tai laitoksen sijoituspaikka tiedossa sekä lay-out, virtaus- ja PI-kaaviot, laite- ja toimintakuvaukset tehtynä. Turva-automaatiota varten tehty turvallisuussuunnitelma. Arvioijan valinta toiminnalliselle turvallisuudelle. Erilaiset sopimukset kuten kumppanuus- ja hankinta sopimukset. Kemikaalilaitoksista tehty lupahakemus Tu-kesille [3].

### **Vaihe 1. Mahdollisten vaarojen sekä riskien arvioiminen:**

Vaiheen 1 vaatimuksia:

Onnettomuus skenaarioiden todennäköisyyksien ja seurauksien selvittäminen riskianalyysin avulla. Suositeltavinta olisi käyttää poikkeamatarkastelua tai muuta riskianalysointitapaa mahdollisten prosessihäiriöiden sekä riskienarviointiin. Riskinvähennyskeinoja tarvitaan, jos riskin suuruus ei ole hyväksyttävällä tasolla. Riskejä arvioidessa on tunnistettava mahdolliset haavoittuvuudet verkonkautta sekä lokaalisti tapahtuvat mahdolliset hyökkäykset. On myös arvioitava edellä mainittujen riskien merkitys onnettomuuksien ehkäisyn kannalta. Jos järjestelmässä tai toimitettavassa laitoksessa on painelaitteita, tässä elinkaaren vaiheessa vaaditaan painelaitteiden ja laitekokonaisuuden riskienarviointi. Riskienarviointi tehdään valmistajan ja tilaajan yhteistyönä. Painelaitteiden ja laitekokonaisuuksien riskienarvioinnista vastaa laitteiden valmistaja [3].

Vaiheen 1 tavoitellut lopputulokset:

Varauduttu mahdollisiin onnettomuuksiin, tehty raportit eri riskianalyyseistä, on tunnistettu turva-automaatiossa käytetyt turvatoiminnot [3].

### **Vaihe 2 Riskinvähennyskeinojen kohdistus ja eheystaso:**

Vaiheen 2 vaatimukset:

Kun riskianalyysit on tehty, päätetään mitä skenaarioita tutkitaan tarkemmin ja selvitetään niiden hallitsemiseen suunniteltujen suojakerrosten riippumattomuus toisistaan sekä riskinvähennyskyvyt. Jotta voidaan pienentää riskiä enemmän kuin kymmenkertaisesti silloin tarvitaan turva-automaatiota. Suunniteltujen suojakerrosten tulee olla riippumattomia toisistaan tarkoittaen sitä, etteivät ne saa yhteisvikaantua. Yhteisvikaantumisella tarkoitetaan samasta syystä aiheutuvaa useamman suojakerroksen vikaantumista [3].

Vaiheen 2 tavoitellut lopputulokset:

Onnettomuusskenaarioon suunnitellut suojakerrokset on tehty ja ovat riippumattomia toisistaan. Riskinvähennystarve ja eheystaso on määritetty jokaiselle turvatoiminnoille [3].

### **Vaihe 3 Turvallisuusvaatimukset ja vaatimus määrittelyt turvatoiminnoille:**

Vaiheen 3 vaatimukset:

Turvatoiminnon kuvaus esimerkiksi syy mikä aiheuttaa turvatoiminnon käynnistymisen ja mitä siitä seuraa sekä kriteerit onnistuneelle toiminnalle. Turvallisuusvaatimuksia ja turvatoiminnon määrittelyyn sisältyvät ympäristöolosuhteet, erilaiset poikkeavat tilanteet, koestusväli, lepovirtaperiaate sekä vasteajat ja monia muita. Turvatoiminnot on selitettävä tarkasti ja yksityiskohtaisesti sekä ne on pystyttävä kohdistamaan tunnettuun häiriöön tai onnettomuusskenaarioon [3].

Vaiheen 3 tavoitellut lopputulokset:

Turvatoiminnoista erittäin tarkat vaatimukset sekä hyvä kuvaus. Järjestelmän eheystason todentaminen käyttäen vikaantumistaajuuslaskemia (PFDavg- tai PHF-arvot), systemaattisen kyvykkyyden todentaminen ja arkkitehtuurilliset vaatimukset turvatoiminnoille [3].

### **Vaihe 4 suunnittelu ja toteuttaminen:**

Vaiheen 4 vaatimukset:

Turva-automaatiolle on määritetty vaatimukset määrittelyvaiheessa. Suunnitellaan turva-automaatio kyseisten vaatimusten mukaisesti. Turva-automaatiojärjestelmään liitetään tarvittavat erilaiset laitteet ja ohjelmistot. Turvatoimintojen pitää olla riippumattomia käyttöautomaation suojaustoiminnoista sekä muista suojakerroksista. Yhteisvikaantumisia voi aiheuttaa järjestelmätasolla ulkoiset tekijät kuten laitteisiin kohdistuva

lämpötila, korroosio ja likaantuminen. Myös turva-automaation ja käyttöautomaation yhteiset komponentit, käyttöhyödykkeet, materiaalit, laitteiden sijoituspaikat sekä muut suunnittelusta johtuvat virheet. Kyberturvallisuus on tärkeää huomioida turva-automaatio järjestelmissä. Lopuksi pitää suunnitella kunnossapito- ja käyttökäytännöt sekä otettava huomioon mahdollisuus inhimillisiin virheisiin suunniteltaessa kyseisiä käytäntöjä [3]. Tämän vaiheen painelaitteisiin liittyviä vaatimuksia voi käydä lukemassa lähteen [3] verkkosivuilta.

Vaiheen 4 tavoitellut lopputulokset:

Tehdastestiraportti (FAT-testiraportti) käytyä läpi ja laitteet sekä toiminnot testattu onnistuneesti. Käyttöohjeet sekä kunnossapito-ohjeet tehtynä. Laittevalinnat on tehty laitesertifikaattien perusteella. Lisäanalyysi, josta huomataan, että yhteisvikaantumiset on luotettavasti estetty [3].

### **Vaihe 5 asennus, testaus ja käyttöönotto:**

Vaiheen 5 vaatimukset:

Laitteiden asentaminen oikeille paikoilleen suunnitelman mukaisesti ja samalla tarkastetaan laitteiden kytkennät sekä mahdolliset vauriot laitteissa. Hyväksytetään laitteisto sekä turvatoimintojen suunniteltu toiminta hyväksymistestin (SAT- testin) avulla. Kentällä olevat laitteet on merkittävä dokumenttien mukaisin merkkauksin, jotta ne voidaan tunnistaa kentällä teknistä dokumentaatiota tai tietokantaa apuna käyttäen. Toiminnallinen arviointi turva-automaatiojärjestelmästä on tehtävä loppuun ennen kuin käyttöönotto alkaa [3].

Vaiheen 5 tavoitellut lopputulokset:

SAT-testiraportti ja käyttöönottopöytäkirjat täytettynä ja tarkastettuna. Laadunvarmistus dokumentaatio. Laittevalmistajilta saadut dokumentaatiot kuten laitteiden manuaalit. Toiminnallisen turvallisuuden arviointi raportti tehtynä [3]. Tämän vaiheen painelaitteisiin liittyviä vaatimuksia voi käydä lukemassa lähteen [3] verkkosivuilta.

### **Vaihe 6 Järjestelmän käyttö ja ylläpito:**

Vaiheen 6 vaatimukset:

Operaattorit on perehdytettävä ja heidän on ymmärrettävä miten turvatoiminnot toimivat sekä millaisiin vaara- ja häiriötilanteisiin ne on suunniteltu. Käyttövaiheessa turvatoiminnoille on tehtävä säännöllisiä testauksia ja tarkastuksia, joilla saadaan ylläpidettyä turvatoimintojen eheystaso. Turva-automaatiojärjestelmän huoltojen ja korjaustoimenpiteiden jälkeen turvatoiminnot on testattava ja niiden toiminta varmistettava.

Turva-automaation toimintaa tarkkaillaan ja samalla kerätään mittausdataa [3].

Vaiheen 6 tavoitellut lopputulokset:

Ohjeet tehtynä hälytys-, vika- ja ohitustilanteita varten. Kunnossapito raportit dokumentoitu sekä määräaikaisraportit dokumentoitu. Kerätty tietoa järjestelmästä prosessiturvallisuusmittareilla sekä dokumentoimalla havainnot turva-automaation toiminnasta [3]. Tämän vaiheen painelaitteisiin liittyviä vaatimuksia voi käydä lukemassa lähteen [3] verkkosivuilta.

### **Vaihe 7 turva-automaation muutosten hallinta:**

Vaiheen 7 vaatimukset:

Turva-automaation muutosten hallinnalla saadaan varmistettua se, että pystytään arvioimaan muutosten vaikutus turva-automaation toimintaan sekä hallittavaan riskiin. Kun muutos tehdään se yleensä aina vaikuttaa riskien arviointiin asti elinkaarimallissa, joten muutoksia tehtäessä pitää palata elinkaarimallissa aikaisimpaan vaiheeseen asti, johon muutos vaikuttaa [3]. Tämän vaiheen painelaitteisiin liittyviä vaatimuksia voi käydä lukemassa lähteen [3] verkkosivuilta. Lähteen [3] verkkosivulla elinkaarivaiheen 7 kohdassa sanotaan että, muutosten hallintaa tarvitaan esimerkiksi seuraavissa muutoksissa, jotka on listattu alle:

- Kun muutetaan turvatoimintoja.
- Turvatoimintoihin vaikuttavan laitetypin vaihtaminen.
- Lukitusarvoja muutettaessa.
- Tehdään muutoksia testaustapoihin ja niiden aikatauluihin.
- Prosessiolosuhteiden muuttuessa.

Vaiheen 7 tavoitellut lopputulokset:

Muutoksenhallinta menettelyn tekeminen ja muutoksenhallintalomakkeiden sekä dokumentaation päivittäminen ajan tasalle [3].

### **Vaihe 8 käytöstä poisto:**

Vaiheen 8 vaatimukset:

Järjestelmään aiheutuvat vaikutukset arvioitava, kun tehdään käytöstä poisto ja on varmistettava jäljelle jääneen turva-automaation toiminta [3].

Vaiheen 8 tavoitellut lopputulokset:

Muutoksenhallinta tehtynä ja testauspöytäkirjat päivitetty [3].

#### 2.4.4 Riskinpienennys keinoja

Riskinpienennys keinot voidaan luokitella neljään eri kategoriaan. Kategoriat ovat luontainen riskinpienennys, passiivinen riskinpienennys, aktiivinen riskinpienennys ja menetelmällinen riskinpienennys [24].

**Luontaisella** riskinpienentämisellä tarkoitetaan vaaran tai riskin poistamista prosessiin soveltuvilla turvallisemmilla materiaaleilla sekä paremmilla ja turvallisemmilla prosessiolosuhteilla. Luontaisen riskinpienentämisen suunnittelu ratkaisulla poistetaan tai lievennetään riskiä tai vaaraa käyttämällä vähemmän vaarallisia materiaaleja sekä prosessiolosuhteita [24].

Esimerkkejä luontaisen riskinpienentämisen ratkaisuista ovat:

- palavan nesteen vaihtaminen veteen ja pienentämällä tai poistamalla vaarallisten välituotteiden varastot.
- Minimoidaan vaarallisten aineiden varastointi ja käyttö. Vaarallisten aineiden varastointi paikka pitäisi olla mahdollisimman kaukana ihmisistä ja laitteista, jotta vahingon sattuessa vaikutus on minimaalinen.
- Kun vaarallista ainetta ei tarvita enempää pitää se poistaa ja hävittää asianmukaisesti, jottei se aiheuta vaaraa ihmisille tai laitokselle.
- Työntekijöiden väsymyksen minimoimiseksi olisi hyvä optimoida työvuorot ja aikataulut.
- Tutki mahdollisuutta kohonneiden käyttöolosuhteiden aiheuttamien vaarojen minimoimisesta. Esimerkiksi pystytäänkö prosessin taloudellista tuottavuutta vaarantamatta käyttämään prosessia ei niin vaarallisissa olosuhteissa?
- Dokumenttien pitää olla selkeitä sekä helposti ymmärrettäviä.
- Tutki virheellisen tai tahattoman toiminnan estämiseksi turvatoimintoja laitteille, yksiköille ja ohjausjärjestelmille.
- Varmista laitteiden ja sähköasennusten asianmukainen eristys ja suojaus [24][26].

Luonnollisen turvallisuuden korkeammille tasoille päästään suunnittelemalla prosessi, joka poistaa syttyvät ilmapiirit, jotka vaativat laitteiston vahvistamista [24]. Varhaisessa suunnitteluvaiheessa luontaisesti turvallisilla suunnittelu vaihtoehdoilla esimerkiksi prosessitoiminnoille ja laitesuunnittelulle, voidaan saavuttaa korkeammat turvallisuusstan-

dardit sekä kustannushyödyt [25]. Luonnostaan turvallisempaa suunnittelua tulisi käyttää kaikissa prosessin suunnittelun sekä kehittämisen vaiheissa, kun luodaan turvallisempaa prosessiympäristöä ja työympäristöä [26].

**Passiivinen** riskinpienennys tarkoittaa vaaran tai riskin minimoimista prosessisuunnittelulla ja laitesuunnittelulla, joilla vähennetään vaaran tai riskin taajuutta eli esiintymistiheyttä tai niiden aiheuttamia seurauksia ilman aktiivisten laitteiden toimintoja. Esimerkkejä passiivisesta riskinpienentämisestä käyttämällä yhteensopimattomia letkujenliittimiä, roiskeen esto täytettä kiinteästi asennettuihin upotusputkiin, kiinteää maadoitusta ja liitosta sähköä johtavaan metallilaitteistoon tai putkeen sen sijaan että käytettäisiin irrotettavaa kaapelia. Aktiivisilla tai menetelmällisillä järjestelmillä saadaan täydennettyä passiivista suunnittelua erityisesti siellä missä ohimenevät olosuhteet ovat rutiininomaisia. Vaikka passiiviset mallit vaativat vähemmän jatkuvaa huoltoa kuin aktiiviset järjestelmät, on se silti erityisen tärkeää, jotta ne toimivat niin kuin on tarkoitettu. Esimerkiksi etäällä oleva allasalue vaarallisten aineiden vuotojen talteenottoa varten ei ole tehokas, jos sen annetaan täytyä sadevedellä tai se rikkoontuu huonojen huoltokäytäntöjen takia [24].

**Aktiivisessa** riskinpienentämisessä käytetään hälytyksiä, ohjaimia, turvajärjestelmiä ja lieventäviä järjestelmiä poikkeavien prosessitoimintojen havaitsemiseen ja niihin reagoimiseen. Aktiiviset ratkaisut usein sisältävät huollettavia- ja prosessikomponentteja. Tästä syystä aktiiviset ratkaisut ovat tyypillisesti vähemmän luotettavia verrattuna luonnollisiin ratkaisuihin sekä passiivisiin ratkaisuihin. Jotta saavutettaisiin tarvittava luotettavuus, käytetään usein redundanssia poistamaan ristiriita tuotannon ja turvallisuusvaatimusten välillä. Esimerkkeinä aktiivisista riskinpienentämismenetelmistä on varoventtiilien käyttö ylipaineen estämiseksi, Tehdään lukitus korkeantason tunnistuslaitteella imuventtiilille ja pumpun moottorille ylitäyttymisen estämiseksi sekä tulva järjestelmän asentaminen. Aktiivisiin ratkaisuihin kuuluu muun muassa paineenalennusventtiilit, räjähdysten estojärjestelmät, nopeatoimiset venttiilit, liekinpoistovenntiilit, säätimet ja takaiskuventtiilit. Kaikki edellä mainitut laitteet joko vaativat huoltoa tai toimivat reagoimalla prosessi muuttuessaan. Voivat myös vaatia molempia [24].

**Menetelmällisen** mallin ratkaisuissa vaaditaan ihmisen toimintaa vaaran välttämiseksi. Menetelmällisessä riskinpienentämisessä käytetään erilaisia käytäntöjä, toimintamenetelmiä, koulutuksia, hätätilanteita, hallinnollisia tarkastuksia ja muita johtamismenetelmiä vaaratilanteiden tai riskien ehkäisemiseen tai niiden vaikutusten minimoimiseen. Menetelmällisiä ratkaisuja käyttäessä pitää ottaa huomioon myös inhimilliset tekijät, koska korjaavien toimenpiteiden suorittamisessa on mukana henkilö. Inhimillisten teki-

jöiden takia menetelmällinen riskinpienentäminen on kaikista neljästä kategoriasta vähiten luotettava kategoria. Esimerkkejä menetelmällisestä riskinpienentämisestä ovat tavallisten toimintamenetelmien noudattaminen, jotta prosessintoiminnot pysyvät laitteille määritettyjen mekaanisten suunnittelurajojen sisällä, tarkastuslistojen viimeistely allekirjoittamalla tietyt toiminnot tarkastetuksi, korkean tason hälytyksen toimesta syötöeristysventtiilin manuaalinen sulkeminen säiliön ylitäytymisen välttämiseksi, ennaltaehkäisevien huoltotoimenpiteiden tekeminen laitteille vikojen estämiseksi ja maadoitusjärjestelmien manuaalinen kiinnittäminen [24].

Nämä kaikki neljä kategoriaa voivat parantaa prosessin kokonaisturvallisuutta. Askeleet riskin analysoimiseksi, vähentämiseksi ja hallinnoimiseksi ajatellaan hierarkkisella tavalla. Luontainen riskinpienentäminen käyttää materiaalien ominaisuuksia tai prosessin ominaisuuksia riskin tai vaaran poistamiseen tai vähentämiseen. Luontaisen riskinpienentämisen ja kolmen muun välinen ero on se, että luontaisella riskinpienentämisellä pyritään poistamaan riski tai vaara suoraan lähteestä toisin kuin hyväksymällä riski tai vaara ja niiden aiheuttamien vaikutuksien pienentäminen [24].

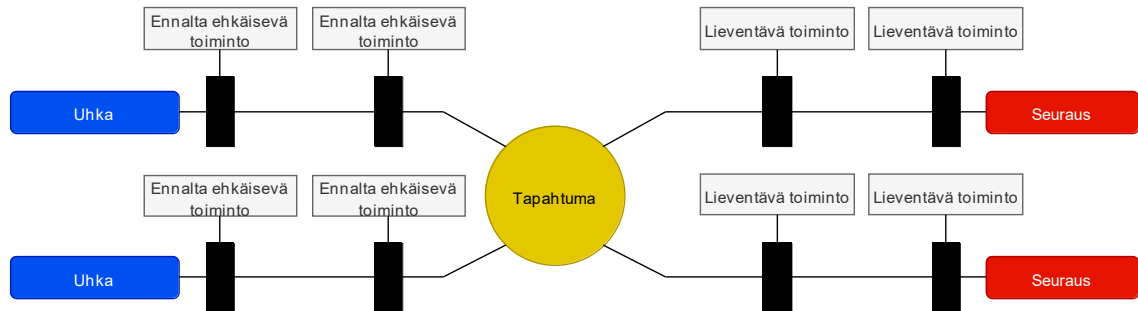
## 2.5 Riskianalyysi tapoja

Riskianalyysi tavaksi valikoitui rusettimallinen riskianalyysi, joka esittää helposti ymmärrettävässä ja visuaalisessa muodossa millaisia uhkia järjestelmässä on sekä millaisia tapahtumia uhat aiheuttavat. Myös tapahtumien seuraukset esitetään rusettimallisissa helposti ymmärrettävällä tavalla. Kappaleessa myös käydään läpi hyökkäyspuumallista riskianalyysiä, joka on tietoturvan kannalta helposti ymmärrettävä ja visuaalinen analyysimalli.

### 2.5.1 Rusettimalli

Rusettimallilla (Bowtie, BT) tarkoitetaan analyysi menetelmää, jossa vasemmalle puolelle mallia määritetään järjestelmälle jokin uhka eli tapahtuman aiheuttaja. Seuraavaksi uhan viereen määritetään mahdolliset toiminnot, joilla pyritään ennalta ehkäisemään aiheuttajasta johtuva tapahtuma kuten esimerkiksi tulipalo. Rusettimallin keskelle tulee tapahtuma, joka tapahtuu malliin määritellyistä uhista, jos uhkia ei saada ennalta ehkäistyä. Mallissa tapahtuman oikealle puolelle määritetään seurauksien lieventävät toimenpiteet, mikäli tapahtuma tapahtuu. Rusettimallin oikeaan reunaan tulee tapahtuman seuraus kuten tulipalon aiheuttamat vahingot. Tiivistettynä rusetti analyysillä analysoidaan ja kuvataan riskin polkua uhasta seuraukseen. Rusettimallia voidaan käyttää riskianalyysien tekemiseen [12][33][35]. Rusettimallinen riskianalyysi voidaan kääntää helposti Bayesian verkkoihin koska siellä voi olla keskinäisiä riippuvuuksia tapahtumien

ja käytettyjen esteiden välillä [35]. Yllä kerrotut mallin elementit vaihtelevat sen mukaan mihin rusettimalia käytetään. Esimerkiksi lentoteollisuudessa oikealle puolelle usein laitetaan tapahtumasta palautumistoiminto eikä lieventävää toimintoa, jota taas käytetään prosessi teollisuudessa. Tapahtumalla tarkoitetaan operaatiota, toimintaa tai materiaalia, joka aiheuttaa henkilövahinkoja, ympäristövahinkoja tai taloudellisia vahinkoja [33]. Kuvasta 6 voidaan nähdä miltä rusettimalilla tehty riskianalyysi voisi näyttää.

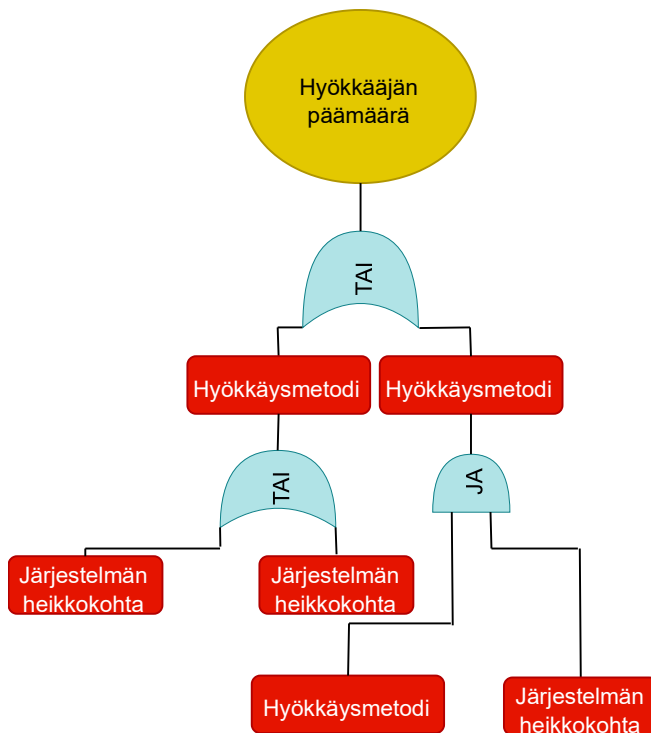


**Kuva 6** Rusettimali on muokattu lähteistä [12] ja [45]

### 2.5.2 Hyökkäyspuu analyysi

Hyökkäyspuu analyysillä (Attack tree, AT) tarkoitetaan mallia, joka visualisoi mahdollisen hyökkäyksen järjestelmään ja on helposti omaksuttava graafinen malli [13]. Samalla se kuvaa järjestelmien ja alijärjestelmien turvallisuutta sekä mallintaa hyökkäysten aiheuttamia mahdollisia vaikutuksia järjestelmässä. Hyökkäyspuun avulla voidaan löytää myös järjestelmän heikkoja kohtia, jolloin se myös auttaa parantamaan järjestelmän turvallisuutta. Hyökkäyspuilla pystytään luokittelemaan järjestelmään kohdistuvia hyökkäyksiä loogisesti [14]. Hyökkäyspuumallin juuressa on hyökkääjän päämäärä. Edellä mainittu juuri on yhdistetty järjestyksessä väli- ja aloitustapahtumiin, jotka demonstroivat erilaisia tapoja onnistuneeseen hyökkäykseen järjestelmää kohtaan, näitä tapahtumia kutsutaan myös lehdiksi [13]. Juuria voi olla useita järjestelmässä ja jokainen juuri mallintaa hyökkääjän eri tavoitteita, tästä syystä jokaisesta eri tavoitteesta tehdään oma hyökkäyspuu. Hyökkäyspuun lehdet sisältävät loogisia operaattoreita kuten JA sekä TAI. TAI operaattoria käytettäessä tuodaan esille monia eri vaihtoehtoisia tapoja, jotka voivat aiheuttaa tapahtuman, kun taas JA operaattoria käytettäessä kuvataan vaadittavat vaiheet päämäärän saavuttamiseksi. Lehdille voidaan asettaa eri arvot, joiden perusteella saadaan karsittua epätodennäköisimmät tapahtumat pois, jos näin halutaan tehdä. Lehtien mahdollisia eriarvoja voi olla esimerkiksi todennäköisyysarvo, totuusarvo, rahallinen arvo tai yhdistelmä kyseisistä arvoista [14]. Kuvassa 7 on esitetty yksi monista mahdollisista hyökkäyspuumalleista. Kyseisessä kuvassa juu-

ressa on hyökkääjän päämäärä ja lehdistä selitetty onko hyökkäys metodista vai järjestelmän heikosta kohdasta kyse ja nämä lehdet on myös yhdistetty JA sekä TAI operaattoreilla.



**Kuva 7 Hyökkäyspuumalli muokattu lähteestä [15]**

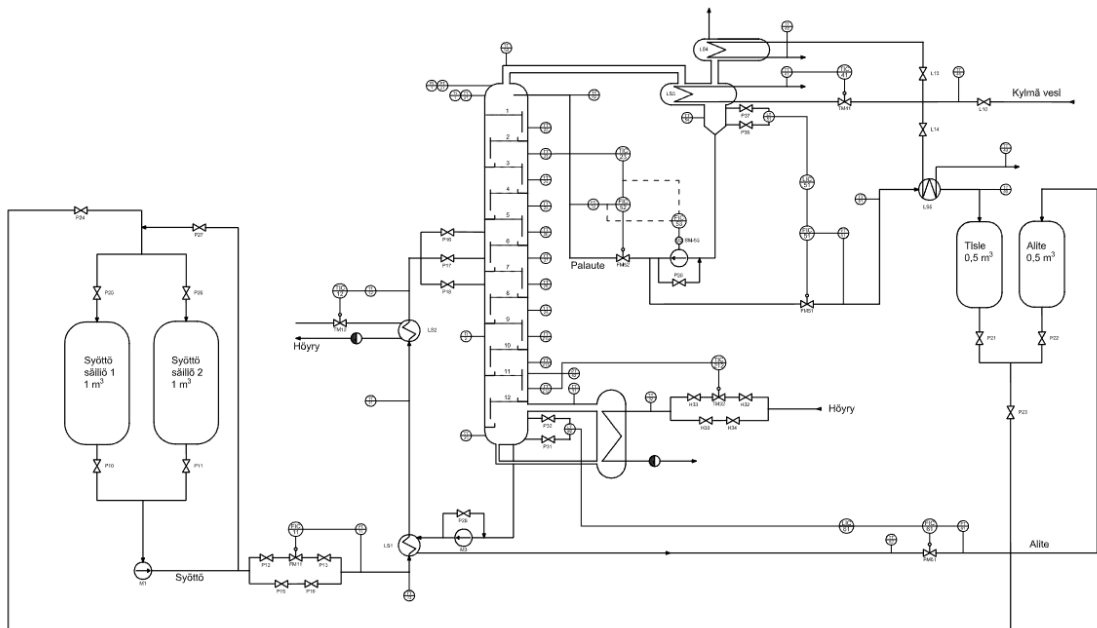
## 3. KOLONNIAUTOMAATIO

Tässä luvussa ensiksi kerrotaan lyhyesti mikä on tislausautomaatiojärjestelmä johon, riskianalyysit tehdään ja miten se pääpiirteittäin toimii. Sen jälkeen käydään läpi tislausautomaatiojärjestelmän käyttötapoja yliopistolla. Viimeisenä kerrotaan mikä on tislausautomaatiojärjestelmään tehtävän tutkimuksen tarkoitus ja mitä otetaan huomioon.

### 3.1 Tislausautomaatiojärjestelmä

Tislausautomaatiojärjestelmä on Tampereen yliopiston automaatiotekniikan osastolla oleva prosessiautomaation opetusympäristö. Opetusympäristöön kuuluu Valmet DNA automaatiojärjestelmä sekä useita erilaisia laitteita ja komponentteja. Opetusympäristöön on opetuskäytössä tarve ottaa etäyhteys ja käyttää prosessia etäyhteydellä sekä ohjelmoida ohjauspiirejä laitteille. Valmet DNA käyttöliittymästä ohjataan prosessin kaikkia osia paitsi lämmitysyksikköä, koska tämä kyseinen yksikkö on manuaalisesti ajettava. Käyttöliittymässä näkyy suurin osa järjestelmässä olevista laitteista ja niiden tiloista.

Tislausautomaatiojärjestelmän laitteistoon kuuluu syöttösäiliöt, tisesäiliö, kolonni, lämmitysyksikkö, pumppuja, putkistot, erilaiset venttiilit, lauhteenpoistimet, höyrykehitin ja lämmönsiirtimet. Tislausprosessissa syöttöneste pumpataan syöttöpumppujen avulla lämmönsiirtimien läpi kolonniin, jolloin osa nesteestä muuttuu höyryksi. Höyry nousee välipohjalta välipohjalle kellojen läpi kolonnia ylöspäin ja neste valuu välipohjalta välipohjalle, kunnes se päättyy kolonnin pohjalle. Pohjalla olevaa nestettä kutsutaan alitteeksi, josta osa menee alitesäiliöön lämmönsiirtimen kautta. Loput pohjalla olevasta nesteestä tuodaan kolonniin takaisin pohjakiehuttimen kautta. Kiehuttimessa neste höyrystyy ja paisuu kolonniin. Kolonnin huipun saavuttanut höyry menee päälauhduttimeen ja siellä höyry tiivistyy lauhdutusputkien ympärille nesteenä, josta se valutetaan tisleakkuun. Osa tisleakkuun valuneesta valmiista nesteestä palautetaan pumpunavulla takaisin kolonnin ylimmälle välipohjalle. Neste, jota ei palauteta kolonniin, ohjataan tisesäiliöön jäähdyttimen kautta [23]. Kolonniautomaation prosessista ja järjestelmästä on selitetty tarkemmin lähteen [23] luvussa 2.



**Kuva 8 PI-Kaavio kolonniautomaatiosta. Haettu lähteestä 16**

### 3.2 Mihin tislauksautomaatiojärjestelmää käytetään yliopistolla

Kolonniautomaatio opetusympäristössä käytetään usealla eri kurssilla. Sitä käytetään myös tutkimusten tekemiseen. Kurssit, joissa kolonnia käytetään ovat automaation turvallisuus, tietoverkkopohjainen automaatio sekä ohjaus- ja automaatiojärjestelmät. Kaikki edellä mainitut kurssit ovat hybridiopettamisen kursseja mikä tarkoittaa sitä, että järjestelmään pitää päästä käsiksi etänä sekä paikan päällä, koska järjestelmässä olevat fyysiset toimilaitteet ovat myös tärkeä osa opetusta ja niitä pitää päästä käyttämään etä- ja läsnäopetus tilanteissa.

**Automaation turvallisuus** kurssilla opetusympäristölle toteutetaan kolmesta eri näkökulmasta riskiarvio. Harjoitukset ovat toiminnallinen turvallisuus ja fyysinen tietoturva, tietoliikenteen tietoturva ja ohjelmistojen tietoturva. Toiminnallisen turvallisuuden ja fyysisen tietoturvan harjoituksessa keskitytään fyysisen prosessiympäristön riskien ja uhkien selvittämiseen sekä niiden korjaustoimenpiteiden ehdottamiseen raporteissa. Kuten myös automaatiojärjestelmässä olevien laitteiden ohjaustapoihin sekä niistä aiheutuviin riskeihin sekä uhkiin. Tietoliikenteen tietoturva harjoituksessa ryhmä selvittää muun muassa prosessin verkon haavoittuvuuksia laitteiden, palomuurien ja reitittimien skannauksen perusteella ja tekevät raportin mahdollisista haavoittuvuuksista sekä antavat toimenpide ehdotuksia haavoittuvuuksien korjaamiseksi. Ohjelmisto turvallisuuden harjoituksessa ryhmät selvittävät millaisia haavoittuvuuksia eri ohjelmistoilla on,

jotka ovat yhteydessä tislusautomaatioon ja tekevät raportin haavoittuvuuksista sekä antavat korjaustoimenpide ehdotuksia haavoittuvuuksien korjaamiseksi [43].

**Tietoverkkopohjaisen automaation** kurssilla oppilaat suorittavat tislusautomaatio ympäristöön erilaisia verkon skannausmenetelmiä, joista saadaan selville millaisia laitteita ympäristö sisältää sekä millaisilla protokollilla laitteet keskustelevat keskenään. Kurssilla opetetaan mitä erilaiset keskustelu protokollat tarkoittavat ja miten ne toimivat sekä verkossa olevien laitteiden tunnistamista skannauksista saaduilla tiedoilla kuten esimerkiksi onko laite ohjelmoitava logiikka vai jokin muu laite [44].

**Ohjaus- ja automaatiojärjestelmät** kurssilla oppilaat suorittavat yhden harjoitustyön tislusautomaatio järjestelmään. Harjoitustyössä tutustutaan tislusautomaatio järjestelmään etsimällä kuviin määritetyt laitteet fyysisestä ympäristöstä sekä tunnistamaan ne prosessikaaviosta. Harjoitustyössä tehdään myös virtauksensäättöpiiri sekä ohjelmoidaan se ja moottorin ohjaus valvomon käyttöliittymään [42].

### 3.3 Työn tavoitteet

Aluksi on tärkeää huomioida, että kolonniautomaatiolla tuotetaan opintopisteitä ja se on liiketoiminta, johon kolonniautomaatiota käytetään tutkimuksien lisäksi yliopistolla. Diplomityön tarkoituksena on selvittää millaisia uhkia ja vaaroja monen etäkäyttäjän yhtäaikainen kolonniautomaation käyttö aiheuttaa sekä millaisia uusia uhkia ja riskejä nousee esille, kun kolonniautomaatioon päästetään käsiksi kolmansia osapuolia joko tutkimustarkoituksessa tai opetustarkoituksessa. Tässä työssä katsellaan edellä mainittuja riskejä ja uhkia prosessin kokonaisturvallisuuden kannalta. Prosessin kokonaisturvallisuuteen kuuluu tietoturva, toiminnallinen turvallisuus, fyysinen turvallisuus etäyhteyden aikana sekä etäyhteyden turvallisuus. Prosessi on hybridiopetuksen mahdollistamisen rajoissa hyvin suojattu, joten työn painotus on prosessin turvamekanismeissa ja niiden tietoturvan tutkimisessa. Nykyisessä prosessissa on useita erilaisia mittalaitteita sekä logiikalla ohjattavia toimilaitteita kuten venttiileitä ja moottoriohjattuja pumppuja. Etäyhteydellä oppilaat pääsevät järjestelmään kiinni ja pystyvät harjoittelemaan ohjauspiirien luomista sekä mittausdatan käyttöä prosessissa. Etäyhteyden kautta voidaan laittaa esimerkiksi pumpun moottoriohjaus päälle ja tämä luo riskin, että pumppu jää fyysisesti päälle, vaikka etäyhteys katkaistaan. Tämän tyyppisiä riskejä pyritään tunnistamaan ja tunnistetuille riskeille pyritään luomaan parannusehdotuksia, jotta järjestelmää olisi turvallista käyttää etänä.

Riskien tunnistamiseen käytettävä metodi on rusettimallinen riskianalyysi (Bowtie-analyysi). Kyseisellä analyysillä tunnistetaan vaarallisia tapahtumia ja uhkia, jotka aiheuttavat edellä mainittuja tapahtumia sekä seurauksia joita tapahtumat aiheuttavat prosessi ympäristössä. Rusettimalliseen riskianalyysiin lisätään myös ennalta ehkäiseviä toimintoja, jotka torjuvat uhat niin ettei tapahtumaa tapahdu kuten myös seurauksille lieventäviä toimintoja. Tällä metodilla saadaan esitettyä visuaalisesti sekä helposti ymmärrettävästi millaisia uhkia, tapahtumia ja seurauksia järjestelmässä mahdollisesti on sekä millaisilla toiminnoilla saadaan ehkäistyä vaarallinen tapahtuma tai millaisilla toiminnoilla saadaan tapahtuman seurauksia lievennettyä.

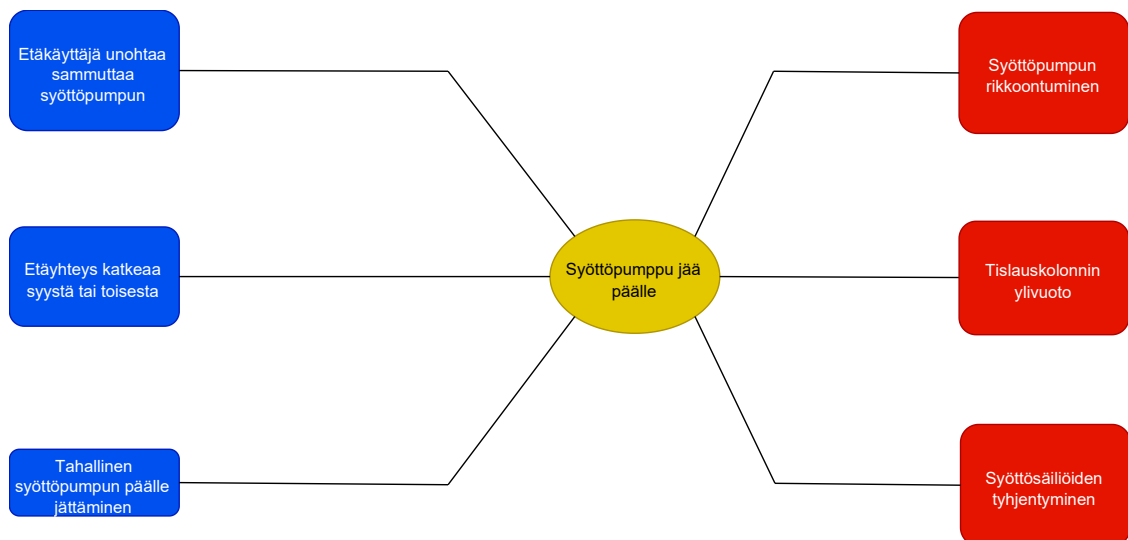
Edellä mainittua metodia sovelletaan tässä projektissa uhkien, tapahtumien ja seurauksien tunnistamiseen sekä ennalta ehkäisevien toimintojen ja lieventävien toimintojen määrittämiseen.

## 4. HYBRIDIOPETUKSEN RISKIANALYYSI KÄYTTÄEN RUSETTI-MALLIA

Tässä luvussa on useita riskianalyysijä rusettimallilla toteutettuna. Rusettimalleissa on uhka tai aiheuttaja sekä keskellä tapahtuma ja jos tapahtuma tapahtuu niin seuraus siitä. Alla muodostetuissa rusettimallisissa riskianalyyseissä on tarkasteltu etäyhteyden aikana tai etäyhteydellä aiheutettuja tapahtumia.

### 4.1 Riskianalyysi syöttöpumpun päälle jäämisestä

Alla olevassa kuvassa 9 tarkastellaan syöttöpumpun päälle jäämisen tapahtumaa, millaisia uhkia tai aiheuttajia tapahtumalle on sekä tapahtuman seuraukset.



**Kuva 9 Riskianalyysi syöttöpumpun päälle jäämisestä**

Tapahtuman aiheuttamia uhkia ovat:

- **Etäkäyttäjää unohtaa sammuttaa syöttöpumpun:** Syöttöpumpulle ei ole määritetty aikaväliä, jolloin se automaattisesti sammutettaisiin eikä syöttöpumpulle ole tehty mittaukseen perustuvia ohjauspiirejä kuten kolonnin pinnanmittaukseen, syöttösäiliön pinnanmittaukseen tai virtausanturia, joka indikoisi tuleeko syöttöpumpulle pumpattavaa nestettä vai ei.
- **Etäyhteys katkeaa:** Etäyhteyden katkeaminen jättää prosessin siihen tilaan missä se yhteyden katkeamisen hetkellä on ollut eli jos on laitettu syöttöpumppu päälle ja yhteys katkeaa niin syöttöpumppu jää päälle eikä sammutta automaattisesti edellä mainitun uhan syiden takia.

- **Tahallinen syöttöpumpun päälle jättäminen:** Syöttöpumpulle ei ole määrätty aikaväliä, jolloin se automaattisesti sammutettaisiin eikä syöttöpumpulle ole tehty mittaukseen perustuvia ohjauspiirejä kuten kolonnin pinnanmittaukseen, syöttösäiliön pinnanmittaukseen tai virtausanturia, joka indikoisi tuleeko syöttöpumpulle pumpattavaa nestettä vai ei.

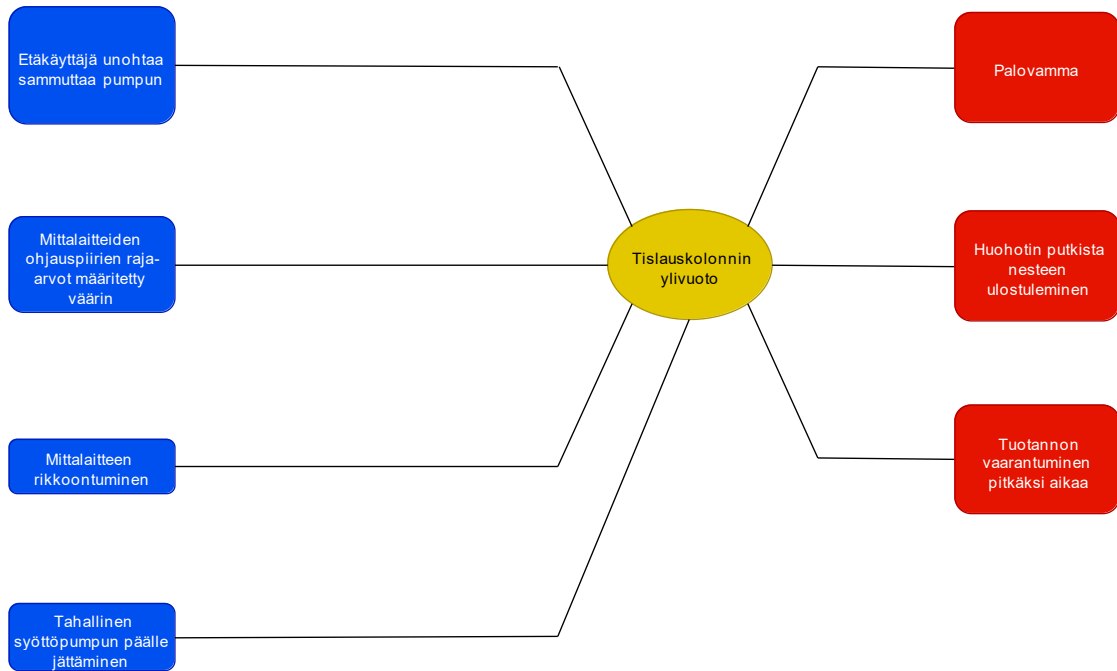
Jos syöttöpumpun päälle jääminen tapahtuu, on sillä tietynlaisia seurauksia prosessille ja sen ympäristölle. Seuraavaksi lueteltuna tapahtuman seurauksia:

- **Syöttöpumpun rikkoontuminen:** Syöttöpumpun pitkäaikainen päällä oleminen voi kuluttaa pumppua, jonka seurauksena on pumpun rikkoontuminen.
- **Tislauskolonnin ylivuoto:** Syöttöpumppu syöttää kolonniin nestettä niin kauan kuin se on päällä ja syöttö säiliöissä on nestettä. Tästä seurauksena kolonnin ylivuoto ja mahdollinen tapaturma tai loukkaantuminen.
- **Syöttösäiliöiden tyhjentyminen:** Kun syöttöpumppu on päällä tyhjentää se syöttösäiliöitä. Tästä seuraa syöttösäiliöiden tyhjentyminen.

On tärkeää löytää mahdollisia ennaltaehkäiseviä tai estäviä toimintoja uhille, jottei tapahtumaa tapahtuisi. Jos tapahtumaa ei pystytä estämään, pitää etsiä mahdollisia lieventäviä toimintoja tapahtuman seurauksille. Näitä toimintoja esitellään tulokset luvussa.

## 4.2 Riskianalyysi tislauskolonnin ylivuodolle

Kuvassa 10 on esitetty rusettimallinen riskianalyysi tapahtumalle tislauskolonnin ylivuoto. Tapahtumalle on määritetty erilaisia uhkia tai aiheuttajia sekä seuraus tapahtumasta.



**Kuva 10 Riskianalyysi tislauskolonnin ylivuodosta**

Tapahtuman aiheuttamia uhkia ovat:

- **Etäkäyttäjää unohtaa sammuttaa syöttöpumpun:** Syöttöpumppu jää päälle, jolloin syöttösäiliössä oleva neste pumpataan kolonniin ja tästä saattaa aiheutua tislauskolonnin ylivuoto.
- **Mittalaitteiden ohjauspiirien raja-arvot määritetty väärin:** Kun mittalaitteiden raja-arvot on määritetty väärin esimerkiksi mittausalueen ulkopuolelle tällöin ei tule hälytystä, jos pinnankorkeus nousee liian korkeaksi tai laskee liian matalaksi, jolloin riski kasvaa tislauskolonnin ylivuodolle.
- **Mittalaitteen rikkoutuminen:** Vaikka raja-arvot olisi määritetty oikein niin mittalaitteen rikkoutuminen aiheuttaa uhan tislauskolonnin ylivuodolle, koska järjestelmässä ei ole mitään lukituspiiriä sille, jos mittalaite rikkoutuu.
- **Syöttöpumpun tahallinen päälle jättäminen:** Aiheuttaa tislauskolonnin ylivuotoriskin, koska tällä hetkellä järjestelmässä ei ole ohjauspiiriä, joka sammuttaisi syöttöpumpun, kun pinnankorkeus nousee tietylle korkeudelle.

Jos ylivuoto tapahtuu, on sillä tietynlaisia seurauksia prosessille ja sen ympäristölle.

Seuraavaksi lueteltuna tapahtuman seurauksia:

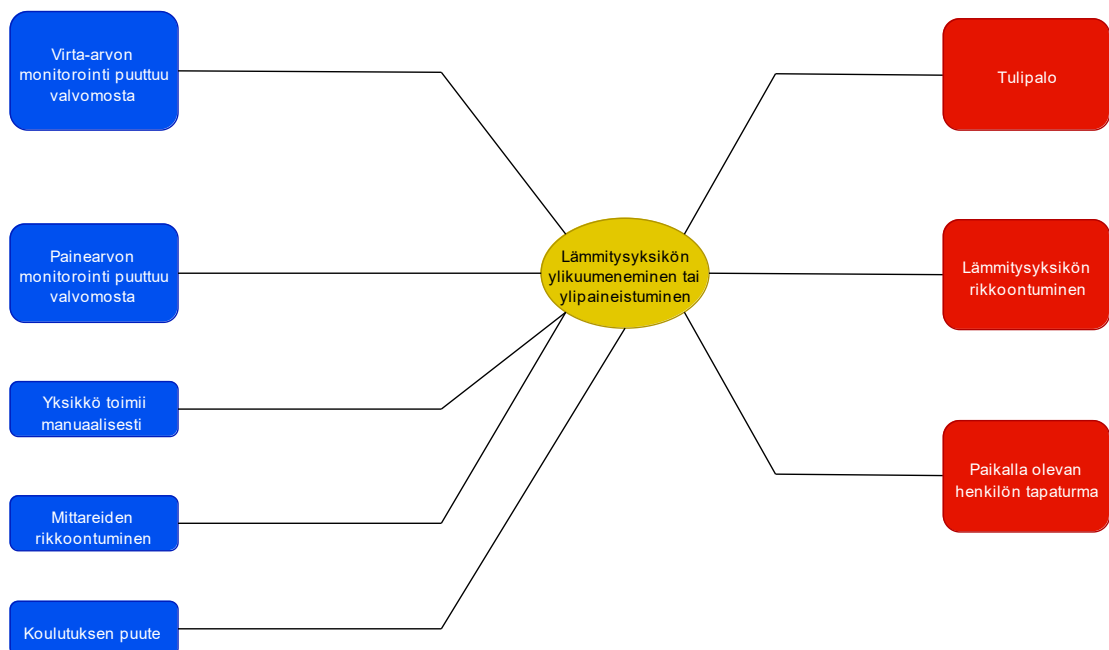
- **Palovamma:** Jos tislauskolonni vuotaa ylitse, kolonniin pumpattu neste vuotaa huohotin putkien kautta ulos. Huohotin putkista ulos kulkeva neste on mahdollisesti kuumaa ja jos ihminen on putkien alapuolella ylivuodon hetkellä saattaa siitä aiheutua palovammoja.

- **Huohotin putkista nesteen ulostuleminen:** Ainoa paikka nesteen ulospääsulle kolonnista, jos kaikki venttiilit ovat suljettuina ylivuodon hetkellä on huohotin putki.
- **Tuotannon vaarantuminen pitkäksi aikaa:** Ylivuodon tapahtuessa kolonni itessään on täynnä nestettä, jolloin sitä ei voida käyttää normaalissa ajossa ennen kuin kolonni on tyhjennetty. Koko kolonnin tyhjentämiseen voi kulua paljon aikaa, jolloin tuotantoa ei pystytä ajamaan eli oppilaat eivät pysty tekemään harjoitustöitensä. Ylivuoto voi myös aiheuttaa laitteiden vikaantumista.

Uhille pitäisi etsiä ennalta ehkäiseviä tai estäviä toiminto ratkaisuja, jolloin tapahtuma vältettäisiin ja jos tapahtumaa ei pystytä välttämään pitäisi etsiä keinoja seurausten lieventämiseksi. Nämä toiminnot tulevat ilmi tulokset luvussa.

### 4.3 Riskianalyysi lämmitysyksikön ylikuumentumisesta tai yli-paineistumisesta

Seuraavaksi tarkastellaan lämmitysyksikön ylikuumentumisen tai yli-paineistumisen uhkia ja aiheuttajia sekä tapahtuman seurauksia kuvassa 11. Lämmitysyksikkö on manuaalisesti käytettävä yksikkö, joka käynnistetään paikan päällä sekä sammutetaan samasta paikasta. Virta-arvo ja painearvo mittaritkin ovat näkyvissä vain yksikön kyljessä paikan päällä.



**Kuva 11 Riskianalyysi lämmitysyksiköstä**

Tapahtuman aiheuttamia uhkia ovat:

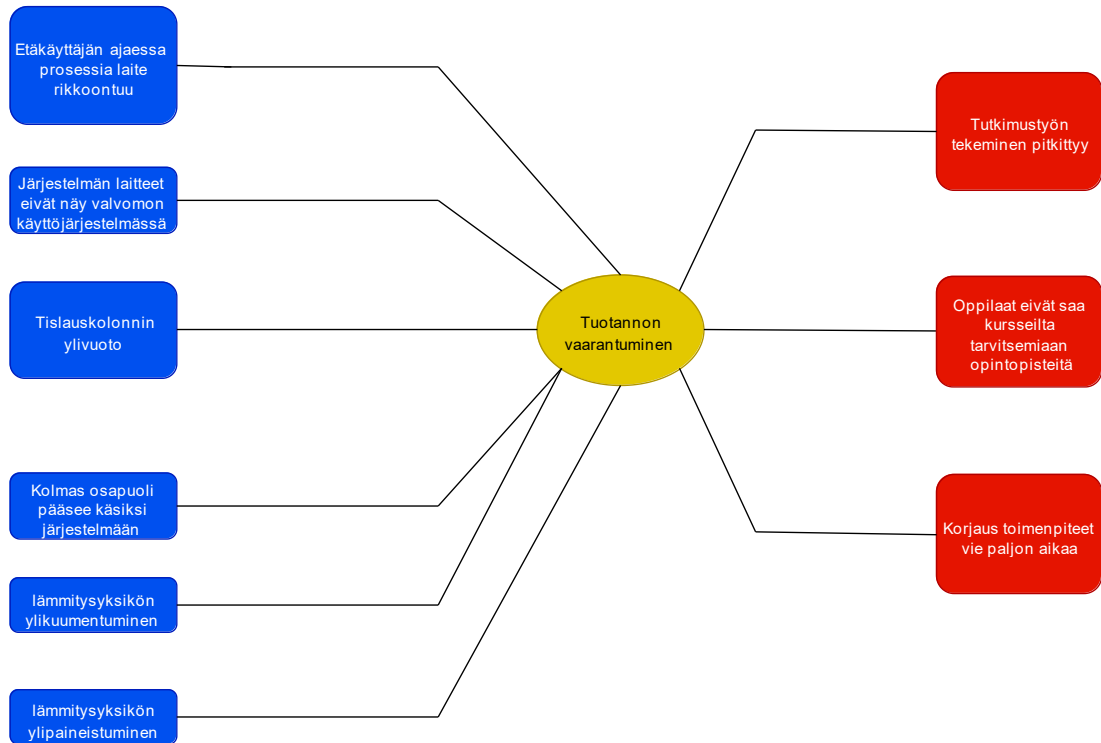
- **Virta-arvon monitoroinnin puuttuminen valvomosta:** Kun tislausautomaatio järjestelmää käytetään etänä, olisi ensiarvoisen tärkeää, että kaikki kriittiset tiedot ovat näkyvissä valvomon käyttöliittymässä, joka nähdään etäyhteydelläkin. Lämmitysyksikön virta-arvoa sieltä ei näe, jolloin etäkäyttäjällä ei ole mitään tietoa siitä mikä reaaliaikainen virta-arvo on ja onko koko yksikkö edes päällä. Kun monitorointi puuttuu, etäkäyttäjä ei pysty tekemään asialle mitään, jos virta-arvo nousee liian korkeisiin lukemiin.
- **Painearvon monitoroinnin puuttuminen valvomosta:** Tislausautomaation valvomon käyttöliittymästä ei myöskään nähdä lämmitysyksikön painearvoa. Etäkäyttäjällä ei ole siis tietoa lämmitysyksikön paineista, eikä etäkäyttäjä pysty tekemään asialle yhtään mitään, jos painearvo nousee liian korkeaksi.
- **Lämmitysyksikkö toimii manuaalisesti paikan päältä:** Lämmitysyksiköstä ei tule minkäänlaisia tietoja valvomon käyttöjärjestelmään, joten etäkäyttäjän on mahdotonta tietää lämmitysyksikön reaaliaikaista tilaa, joka luo riskin ylikuumentumiselle tai ylipaineistumiselle.
- **Mittareiden rikkoontuminen:** Jos valvomon käyttöjärjestelmään saadaan tuotua tieto lämmitysyksikön tilasta sekä virta- ja painearvoista aiheuttaa mittareiden rikkoontuminen riskin ylikuumentumiselle sekä ylipaineistumiselle lämmitysyksikön käynnissä ollessa, jos ei ole ohjauspiiriä, jolla estetään yksikön käyttäminen kun mittalaite on rikkoontunut.
- **Käyttäjien koulutuksen puute:** Tislausautomaation käyttäjien koulutuksen puute lämmitysyksiköstä ja sen toiminnasta.

Jos lämmitysyksikön ylikuumentuminen tai ylipaineistuminen tapahtuisi on sillä seurauksia ympäristölle sekä järjestelmälle itsessään. Seuraavaksi lueteltuna tapahtuman seurauksia:

- **Tulipalo:** Lämmitysyksikön ylikuumentuessa, herkästi syttyvät nesteet tai laitteet saattavat aiheuttaa tulipalon.
- **Lämmitysyksikön rikkoontuminen:** Yksikön ylikuumentuessa tai ylipaineistuksessa yksiköstä voi hajota komponentteja tai laitteita.
- **Paikalla olevan henkilön tapaturma:** Yksikön ylikuumentuessa on mahdollista paikalla olevan henkilön saada palovamma koskiessaan yksikköön tai ylipaineistuksessa jotkin putket saattavat pettää ja roiskaista kuumaa nestettä henkilön päälle.

## 4.4 Riskianalyysi tuotannon vaarantumisesta

Kuvassa 12 tapahtumana tarkastellaan tuotannon vaarantumista sekä sen aiheuttajia ja uhkia. Korostetaan että tässä tuotannolla tarkoitetaan oppilaiden oppimista sekä opintopisteitä, jotka vaaditaan kurssin läpäisyyn.



**Kuva 12 Riskianalyysi tuotannon vaarantumisesta**

Tapahtuman aiheuttamia uhkia:

- **Etäkäyttäjän ajaessa prosessia prosessilaitte rikkoontuu:** Etäkäyttäjä rikkoo prosessilaitteen vahingossa tai koulutuksen puutteen takia, jolloin tuotanto vaarantuu. Riippuen rikkimenneestä laitteesta, korjaamiseen tai uuden laitteen saamiseen voi mennä paljonkin aikaa.
- **Järjestelmän kaikki laitteet eivät näy valvomon käyttöjärjestelmässä:** Lämmitysyksikkö ei näy ollenkaan valvomon käyttöjärjestelmässä ja lauhdutusvesiventtiilin tilakaan ei näy valvomon käyttöjärjestelmässä, koska se on käsikäyttöinen venttiili.
- **Tislauskolonnin ylivuoto:** Ylivuodon tapahtuessa kolonni on täynnä nestettä, jolloin tuotannon ajaminen on mahdotonta. Kolonnin tyhjäksi pumppaamiseen voi kulua paljon aikaa.
- **Kolmas osapuoli pääsee käsiksi järjestelmään:** Kolmas osapuoli tai ulkopuolinen henkilö, joka pääsee käsiksi tislausautomaatioon, pystyy aiheuttamaan tuotannolle ongelmia kuten tahallinen laitteiden väärin ohjelmoiminen, mittaus rajojen vääränlainen määrittäminen yms.

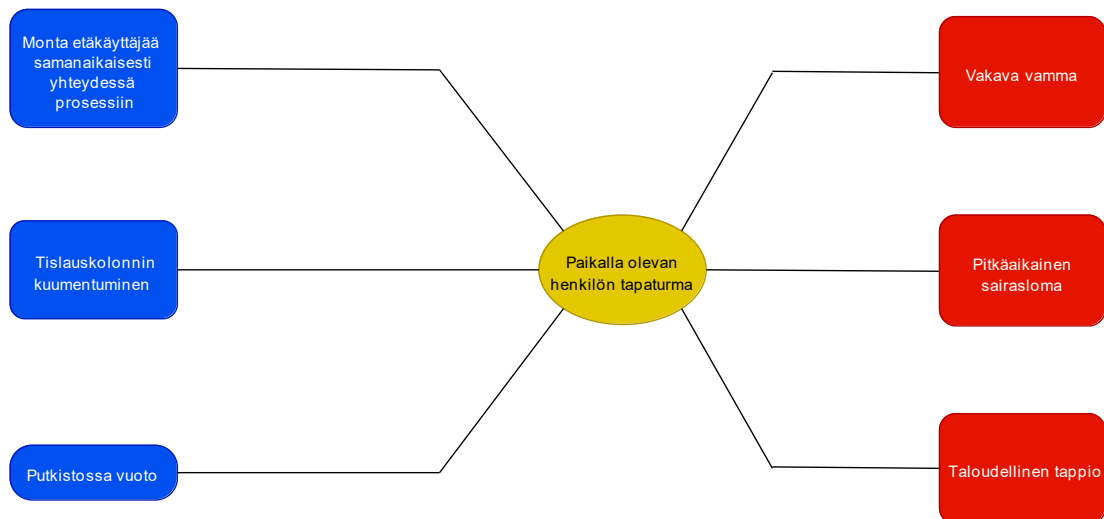
- **Lämmitysyksikön ylikuumentuminen:** Ylikuumentuessa lämmitysyksiköstä voi hajota komponentteja tai laitteita. Tästä syystä tuotanto saattaa vaarantua.
- **Lämmitysyksikön ylipaineistuminen:** Ylipaineistuessa lämmitysyksiköstä voi hajota komponentteja tai laitteita. Tästä syystä tuotanto saattaa vaarantua.

Tuotannon vaarantumisen tapahtuessa on sillä merkittäviä seurauksia opiskelijoille, tutkijoille sekä ympäristölle. Alla lueteltuna mahdollisia tapahtuman seurauksia:

- **Tutkimustyön tekeminen pitkittyy:** Usein tutkimus töillä on tiukat aikataulut ja jos tuotanto vaarantuu eli laitteisto menee esimerkiksi rikki, vaikuttaa se tutkimuksen aikatauluihin.
- **Oppilaat eivät saa kursseilta tarvitsemiaan opintopisteitä:** Pahimmassa tapauksessa jos tislusautomaatio on toimintakyvyttömässä kunnossa pitkään joudutaan siirtämään kurssia toisille periodeille tai suunnittelemaan kurssin sisältö uudelleen.
- **Korjaustoimenpiteet vievät paljon aikaa:** Jos tislusautomaation laitteisto on epäkunnossa voi uusien laitteiden saaminen tai niiden korjaaminen viedä paljon aikaa.

#### 4.5 Riskianalyysi paikalla olevan henkilön tapaturmasta

Kuvassa 13 esitetään rusettimallinen riskianalyysi paikalla olevan henkilön tapaturmasta.



**Kuva 13 Riskianalyysi paikalla olevan henkilön tapaturmasta**

Tapahtuman aiheuttavia uhkia lueteltu alla:

- **Monta etäkäyttäjää samanaikaisesti yhteydessä prosessiin:** Paikalla oleva henkilö tällä hetkellä ei näe mistään onko järjestelmään joku etänä yhteydessä. Tämä aiheuttaa tapaturma riskin, koska etäkäyttäjäkään ei näe onko ihmisiä

paikan päällä. Esimerkiksi jos järjestelmää huolletaan ja siihen otetaan, etäyhteys pystyy etäkäyttäjä ajamaan prosessia huollon aikana, mikäli huoltohenkilö ei ole tehnyt vaarattomaksi prosessia.

- **Tislauskolonnin kuumentuminen:** Kun prosessia ajetaan, kuumentuu kolonni ja aiheuttaa palovamman riskin, jos paikalla oleva henkilö koskee kolonniin.
- **Putkistossa vuoto:** Prosessille ei tehdä määräaikaisia huoltoja, joten putkiston vuoto saattaa jäädä huomaamatta ja paikan päällä oleva henkilö altistuu tapaturman mahdollisuudelle.

Jos tapahtumaa ei saada estettyä tai ennalta ehkäistyä on sillä tietynlaisia seurauksia ympäristölle ja siellä työskenteleville henkilöille. Alla lueteltuna tapahtuman seurauksia:

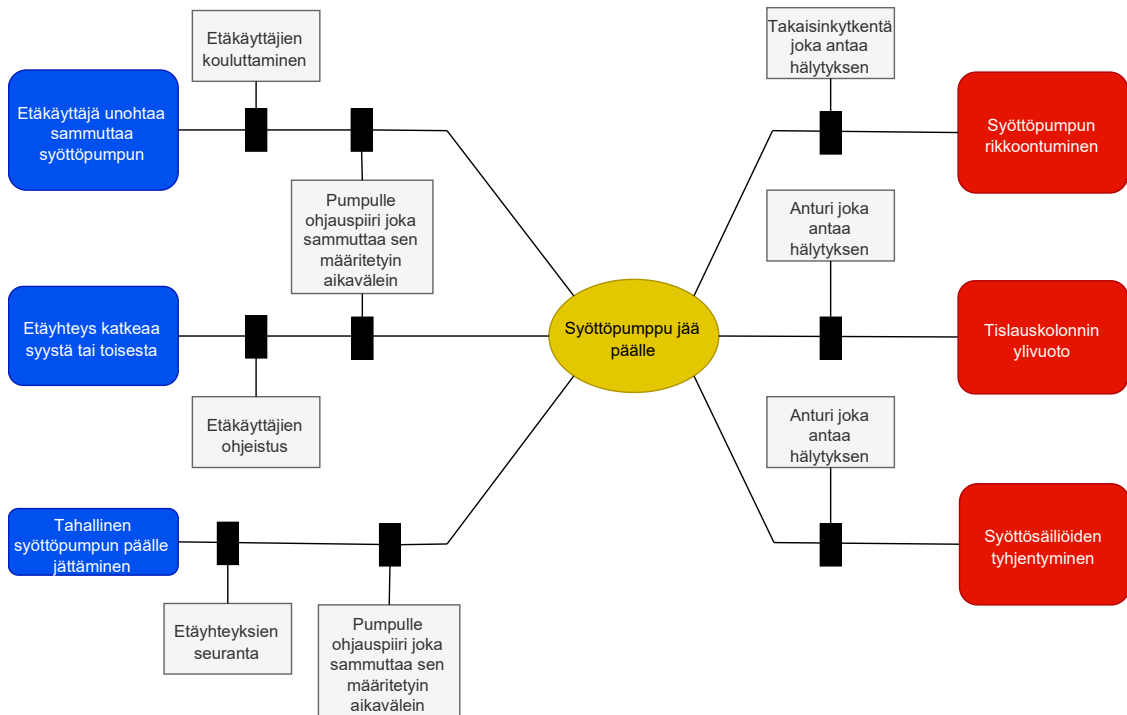
- **Vakava vamma:** Esimerkiksi jos putkistovuodon takia paikalla olevan henkilön päälle roiskuu kuumaa nestettä, aiheuttaa se mahdollisesti vakavat palovammat.
- **Pitkäaikainen sairausloma:** Vakavasta vammasta toipuminen vie paljon aikaa, joten henkilö joutuu olemaan pitkäaikaisella sairauslomalla.
- **Taloudellinen tappio:** Henkilö jolle tapaturma on tapahtunut, joutuu olemaan pitkällä sairauslomalla riippuen tapaturman aiheuttamasta vammasta. Jos henkilö on organisaation työntekijä aiheuttaa se taloudellisia tappioita organisaatiolle koska henkilön tilalle on palkattava tuuraaja sekä henkilön sairauslomaraaha pitää maksaa. Jos henkilö on ulkopuolinen, joudutaan hänelle maksamaan korvauksia mahdollisen vamman tuottamisesta organisaation tiloissa.

## 5. TULOKSET

Tässä luvussa käsitellään luvussa 4 tehtyjä riskianalyyskejä ja täydennetään niihin tuloksina ennaltaehkäiseviä tai estäviä kontrolleja tapahtumalle sekä tapahtuman seurauksien lieventämisen kontrolleja. Tässä luvussa otetaan myös kantaa siihen kuinka tärkeää erilaisten tapahtumien ennaltaehkäiseviä tai estäviä toimintoja on toteutettava.

### 5.1 Syöttöpumpun päälle jääminen

Kuvassa 14 on tehty riskianalyysi rusettimalilla, jonka tapahtuma on ”Syöttöpumppu jää päälle”. Tähän kuvaan on lisätty ennalta ehkäisevät ja estävät toiminnot sekä tapahtuman seurauksia lieventävät toiminnot.



**Kuva 14 Ennaltaehkäisevät tai estävät toiminnot sekä lieventävät toiminnot**

Alla kerrattuna uhat ja uhille ennalta ehkäisevät tai estävät toiminnot lueteltuna:

**Etäkäyttäjän unohtaa sammuttaa syöttöpumpun:** Syöttöpumpulle ei ole määritetty aikaväliä, jolloin se automaattisesti sammutettaisiin eikä syöttöpumpulle ole tehty mitaukseen perustuvia ohjauspiirejä kuten kolonnin pinnanmittaukseen, syöttösäiliön pinnanmittaukseen tai virtausanturia, joka indikoisi tuleeko syöttöpumpulle pumpattavaa nestettä vai ei.

- **Etäkäyttäjien kouluttaminen:** Kun järjestelmään tulee uusia käyttäjiä, olisi tärkeää kouluttaa heidät prosessin eritoimintoihin sekä ilmoittaa millaisia erikoisominaisuuksia prosessissa on kuten se ettei syöttöpumppu pysähdy, ellei sitä manuaalisesti pysäytetä napista.
- **Syöttöpumpulle ohjauspiiri, jolla sammutetaan pumppu määritetyin aikavälein:** Tällä ohjauspiirillä pystytään syöttöpumpulle määrittämään jokin aikaväli kuten esimerkiksi 24 tuntia. Tämä tarkoittaa sitä, että syöttöpumppu sammutetaan 24 tunnin välein. Tälle toiminnolle pitää tehdä myös ohitustoiminto, koska tislautautomaatiota käytetään moneen eri asiaan ja joskus tislautautomaatiota joudutaan ajamaan kauemmin kuin määritetyn aikavälin ajan.

**Etäyhteyden katkeaminen:** Etäyhteyden katkeaminen jättää prosessin siihen tilaan missä se yhteyden katkeamisen hetkellä on ollut eli jos on laitettu esimerkiksi syöttöpumppu päälle ja yhteys katkeaa niin syöttöpumppu jää päälle. Ennalta ehkäiseviä tapoja tapahtumalle ovat etäkäyttäjien ohjeistus ja syöttöpumpulle ohjauspiiri, joka sammuttaa pumpun määritetyin aikavälein.

- **Etäkäyttäjien ohjeistus:** Uudet käyttäjät pitää kouluttaa ennen prosessin käyttöä, jolloin he tietävät miten prosessi toimii ja mitä ominaisuuksia sillä on. Koulutuksessa olisi hyvä ohjeistaa käyttäjiä etäyhteyden katkeamisen tilanteessa. Tilanteessa tulisi yrittää useamman kerran uudelleen yhdistämistä järjestelmään, jotta syöttöpumppu saataisiin sammutettua manuaalisesti. Jos yrityksistä huolimatta ei saada yhteyttä järjestelmään olisi hyvä olla joku yleinen yhteystieto, johon voisi ilmoittaa, että etäyhteys katkennut ja prosessi jäänyt päälle. Tällä tavalla yhteyshenkilö pystyy hoitamaan joko itse manuaalisen sammuttamisen tai etsiä jonkun muun henkilön sen tekemään.
- **Syöttöpumpulle ohjauspiiri, jolla sammutetaan pumppu määritetyin aikavälein:** Tällä ohjauspiirillä pystytään syöttöpumpulle määrittämään jokin aikaväli kuten esimerkiksi 24 tuntia. Tämä tarkoittaa sitä, että syöttöpumppu sammutetaan 24 tunnin välein. Tälle toiminnolle pitää tehdä myös ohitustoiminto, koska tislautautomaatiota käytetään moneen eri asiaan ja joskus tislautautomaatiota joudutaan ajamaan kauemmin kuin määritetyn aikavälin ajan.

**Tahallinen syöttöpumpun päälle jättäminen:** Syöttöpumpulle ei ole määritetty aikaväliä, jolloin se automaattisesti sammutettaisiin eikä syöttöpumpulle ole tehty mittaukseen perustuvia ohjauspiirejä kuten kolonnin pinnanmittaukseen, syöttösäiliön pinnan-

mittaukseen tai virtausanturia, joka indikoisi tuleeko syöttöpumpulle pumpattavaa nestettä vai ei. Tämän uhan ennalta ehkäisy tapoja ovat etäyhteyden seuranta ja syöttöpumpulle ohjauspiiri, joka sammuttaa pumpun määritetyin aikaväleihin.

- **Etäyhteyden seuranta:** Etäyhteyden seurannalla saadaan tietoa siitä, mistä on otettu etäyhteys ja kuka on ottanut etäyhteyden järjestelmään ja tämä tuodaan myös esille koulutus materiaalissa, jolloin etäkäyttäjillä on suurempi kynnys tehdä tahallisia toimia järjestelmässä.
- **Syöttöpumpulle ohjauspiiri, jolla sammutetaan pumppu määritetyin aikaväleihin:** Tällä ohjauspiirillä pystytään syöttöpumpulle määrittämään jokin aikaväli kuten esimerkiksi 24 tuntia. Tämä tarkoittaa sitä, että syöttöpumppu sammutetaan 24 tunnin välein. Tälle toiminnolle pitää tehdä myös ohitustoiminto, koska tislautusautomaatiota käytetään moneen eri asiaan ja joskus tislautusautomaatiota joudutaan ajamaan kauemmin kuin määritetyn aikavälin ajan.

Alla kerrattuna tapahtuman seuraukset sekä lueteltuna seurauksille lieventävät toiminnot.

**Syöttöpumpun rikkoontuminen:** Syöttöpumpun pitkäaikainen päällä oleminen voi kuluttaa pumppua ja sen komponentteja, jonka seurauksena on pumpun rikkoontuminen. Tätä seurausta pystytään lieventämään takaisinkytkennän avulla.

- **Takaisin kytkentä:** Antaa hälytyksen syöttöpumpun vikaantumisesta, jolloin käyttäjä pystyy tekemään nopeammin tarvittavat toimenpiteet pumpunkorjaukseksi tai vaihtamiseksi.

**Tislauskolonnin ylivuoto:** Syöttöpumppu syöttää kolonniin nestettä niin kauan kuin se on päällä ja syöttö säiliöissä on nestettä. Tästä seurauksena kolonnin ylivuoto ja mahdollinen tapaturma tai loukkaantuminen. Seurauksen lieventämisenä voidaan käyttää anturia, joka antaa hälytyksen, kun pinnankorkeus on tietyllä korkeudella.

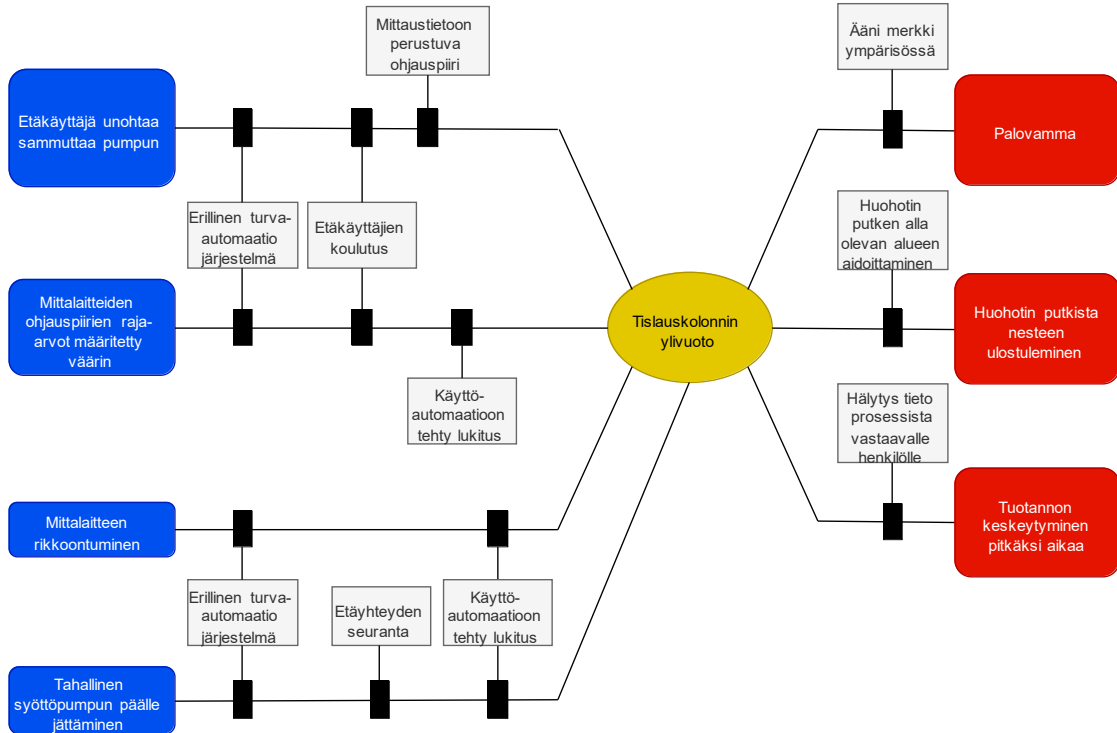
- **Pinnankorkeus anturi:** Kun pinnankorkeus nousee tietylle korkeudelle, annetaan hälytys, jolloin henkilö, joka näkee hälytyksen voi sammuttaa pumpun manuaalisesti.

**Syöttösäiliöiden tyhjentäminen:** Kun syöttöpumppu on päällä tyhjentää se syöttösäiliöt. Tästä seuraa syöttösäiliöiden tyhjentäminen. Seurauksen lieventämiseen voidaan käyttää pinnankorkeusanturia.

- **Pinnan korkeus anturi:** Kun syöttösäiliöiden pinnankorkeus laskee tietylle tasolle, annetaan hälytys syöttösäiliöiden pinnankorkeudesta, jolloin henkilö, joka näkee hälytyksen voi sammuttaa pumpun manuaalisesti.

## 5.2 Tislauskolonnin ylivuoto

Alla olevassa kuvassa 15 on rusettimmallinen riskianalyysi tislauskolonnin ylivuodosta. Tislauskolonnin ylivuoto on tapahtuma, joka pyritään estämään tai siitä aiheutuvat haitat tuotannolle ja ympäristölle minimoimaan.



**Kuva 15 Tislauskolonnin ylivuodon ennaltaehkäisy toiminnot ja seurauksien lieventävät toiminnot**

Alla kerrattuna tapahtuman uhat, tapahtumasta johtuvat seuraukset sekä luetteluna ennaltaehkäiseviä toimintoja ja lieventäviä toimintoja.

**Etäkäyttäjä unohtaa sammuttaa pumpun:** Syöttöpumppu jää päälle, jolloin syöttösäiliössä oleva neste pumpataan kolonniin ja tästä saattaa aiheutua tislauskolonnin ylivuoto. Ennalta ehkäiseviä toimintoja uhalle ovat erillinen turva-automaatio järjestelmä, etäkäyttäjien koulutus ja mittaustietoon perustuva ohjauspiiri.

- **Erillinen turva-automaatio järjestelmä:** Turva-automaatio järjestelmään yhdistettyjen pinnankorkeus antureiden avulla saadaan ohjelmoitua syöttöpumpun sammuttamisen ohjaus perustuen mittaus arvoon. Tarkoittaa sitä, kun pinnankorkeus nousee tietylle korkeudelle turva-automaatio järjestelmä sammuttaa syöttöpumpun ja käynnistää poistopumpun sekä tekee muut tarvittavat toiminnot kolonnin liika nesteen poistamiseksi ja tislausautomaatio järjestelmän ajamisen turvalliseen tilaan.
- **Etäkäyttäjien koulutus:** Uusien etäkäyttäjien kouluttamisen yhteydessä korostetaan syöttöpumpun sammuttamisen tärkeyttä, kun prosessin käyttö lopetetaan.

- **Mittaus tietoon perustuva ohjauspiiri:** Asennetaan pinnankorkeus anturit kolonniin valituille kohdille, jolloin niitä voidaan käyttää syöttöpumpun ohjauspiirissä, jolla sammutetaan syöttöpumppu, kun pinnankorkeus nousee liian korkealle. Tämä eroaa turva-automaatiossa siinä, että tislaukolonniautomaatiossa opiskelijoiden pitää päästä säätämään antureiden toimintoja sekä laitteiden ohjauspiirejä, joten tämä tapa kantaa silti riskin siinä, että pinnankorkeusanturiin ei osata asettaa oikeita raja-arvoja.

**Mittalaitteiden ohjauspiirien raja-arvot määritetty väärin:** Kun mittalaitteiden raja-arvot on määritetty väärin esimerkiksi mittausalueen ulkopuolelle tällöin ei tule hälytystä, jos pinnankorkeus nousee liian korkeaksi, jolloin on riski tislaukolonnin ylivuodolle. Uhan aiheuttama tapahtuma pystytään ennalta ehkäisemään erillisellä turva-automaatio järjestelmällä ja etäkäyttäjien kouluttamisella.

- **Käyttöautomaatioon tehty lukitus:** Käyttöautomaatioon voidaan tehdä salasana ja käyttäjätunnuksella suojattu lukitus mittalaitteiden ohjauspiirien raja-arvoille, jolloin niitä ei pääse muuttamaan kuin määrätty henkilöt.
- **Erillinen turva-automaatiojärjestelmä:** Mittalaitteiden raja-arvojen väärin määrittäminen aiheuttaa riskin ylivuodolle. Mikäli käyttöautomaatioon tehdyillä lukituksilla ei saada luotettavaa ennalta ehkäisyä toteutettua käytetään erillistä turva-automaatio järjestelmää ennalta ehkäisemiseen. Turva-automaatiojärjestelmään on yhdistetty oma pinnankorkeus anturi, jonka raja-arvon ylittyessä turva-automaatio sammuttaa syöttöpumpun ja käynnistää poistopumpun sekä tekee muut tarvittavat toimet ylivuodon ja tapaturmien välttämiseksi.
- **Etäkäyttäjien koulutus:** Uusille etäkäyttäjille pitää koulutuksessa korostaa pinnankorkeuden mittauksen raja-arvojen tärkeyttä, jos syöttöpumpulle on tehty mittausarvoon perustuva ohjaus.

**Mittalaitteen rikkoontuminen:** Vaikka raja-arvot olisi määritetty oikein niin mittalaitteen rikkoontuminen aiheuttaa uhkan ylivuodolle, koska järjestelmässä ei ole mitään ohjauspiiriä sille, jos mittalaite rikkoontuu. Ennalta ehkäiseviä toimintoja uhan aiheuttamalle tapahtumalle on erillinen turva-automaatio järjestelmä.

- **Käyttöautomaatioon tehty lukitus:** Käyttöautomaatioon voidaan tehdä lukitus mittalaitteiden toiminnalle, jolloin mittalaitteen rikkoontuessa käyttöautomaatio pitää järjestelmän turvallisessa tilassa.
- **Erillinen turva-automaatio järjestelmä:** Mikäli käyttöautomaatioon tehdyillä lukituksilla ei saada luotettavaa ennalta ehkäisyä toteutettua käytetään erillistä turva-automaatio järjestelmää ennalta ehkäisemiseen. Turva-automaatio järjes-

telmässä yleensä on oma mittalaite, jota se käyttää, jolloin perus automaatiojärjestelmässä olevan mittalaitteen rikkoontuminen ei vaikuta turva-automaation toimintaan vaan se ohjaa syöttöpumppua oman järjestelmänsä mittalaitteen tiedon perusteella ja pitää tislautusautomaatiojärjestelmän turvallisessa tilassa.

**Tahallinen syöttöpumpun päälle jättäminen:** Syöttöpumpulla ei ole ohjauspiiriä, joka sen sammuttaisi. Tämän uhan ennalta ehkäisy tapoja ovat etäyhteyden seuranta ja erillinen turva-automaatio järjestelmä.

- **Käyttöautomaatioon tehty lukitus:** Käyttöautomaatioon voidaan tehdä salasana ja käyttäjätunnuksella suojattu lukitus syöttöpumpun ohjaukselle, jolloin sitä ei pääse käynnistämään kuin määrätyt henkilöt.
- **Erillinen turva-automaatiojärjestelmä:** Mikäli käyttöautomaatioon tehdyillä lukituksilla ei saada luotettavaa ennalta ehkäisyä toteutettua käytetään erillistä turva-automaatio järjestelmää ennalta ehkäisemiseen. Turva-automaatio järjestelmässä yleensä on oma mittalaite, jota se käyttää syöttöpumpun ohjaamiseen. Tällä tarkoitetaan sitä, että turva-automaatio järjestelmä sammuttaa syöttöpumpun, kun mittalaitteelle määritetty raja-arvo on ylitetty sekä käynnistää poistopumpun ja tekee muita tarvittavia toimintoja kolonnin ylivuodon estämiseksi ja prosessin turvalliseen tilaan ajamiseksi.
- **Etäyhteyden seuranta:** Etäyhteyden seurannalla saadaan tietoa siitä, mistä on otettu etäyhteys ja kuka on ottanut etäyhteyden järjestelmään ja tämä tuodaan myös esille koulutus materiaalissa, jolloin etäkäyttäjillä on suurempi kynnys tehdä tahallisia toimia järjestelmässä.

Alla kerrattuna tapahtuman seuraukset sekä lueteltuna seurauksille lieventävät toiminnot.

**Palovamma:** Jos tislaukskolonni vuotaa ylitse, kolonniin pumpattu neste vuotaa huohotin putkien kautta ulos. Huohotin putkista ulos kulkeva neste on mahdollisesti kuumaa ja jos ihminen on putkien alapuolella ylivuodon hetkellä saattaa siitä aiheutua palovammoja. Tälle seuraukselle lieventävänä tekijänä on äänimerkki prosessi ympäristössä.

- **Äänimerkki prosessi ympäristössä tai valvomo- ohjelmistossa:** Jos ylivuoto tapahtuu, olisi hyvä saada henkilöille, jotka ovat prosessi ympäristön lähellä tieto siitä. Esimerkiksi äänimerkillä voidaan ilmoittaa, että prosessin lähettyvillä ei kannata olla koska jokin on prosessissa vialla.

**Huohotin putkista nesteen ulostuleminen:** Ainoa paikka nesteen ulospääsulle kolonnista, jos kaikki venttiilit ovat suljettuina ylivuodon hetkellä on, huohotin putki. Seurauksen lieventävänä tekijänä on huohotin putken alla olevan alueen aidoittaminen.

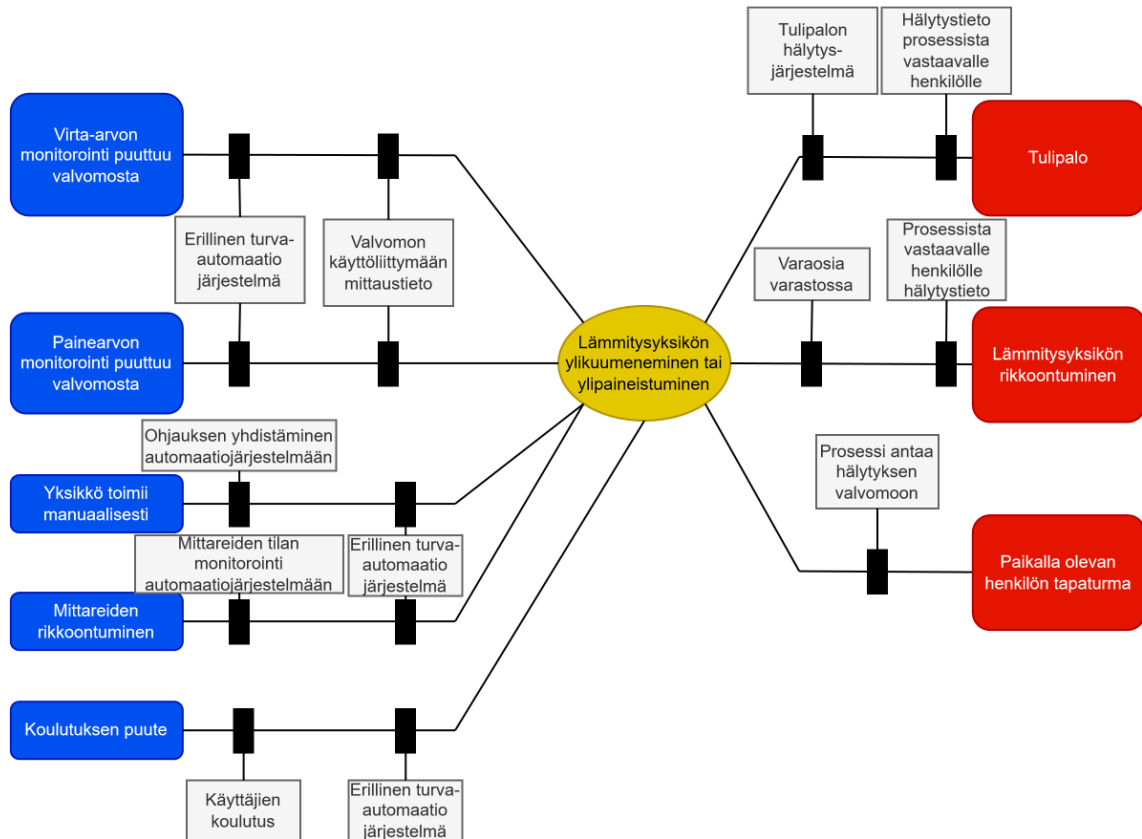
- **Huohotin putken alla olevan alueen aidoittaminen:** Alueen aidoittamisella estettäisiin henkilöiden pääseminen roiske vaaralliselle alueelle, jolloin saataisiin lievennettyä tapaturma riskiä lähettyvillä oleville henkilöille.

**Tuotannon keskeytyminen pitkäksi aikaa:** Ylivuodon tapahtuessa kolonni itsessään on täynnä nestettä, jolloin sitä ei voida käyttää normaalissa ajossa ennen kuin kolonni on tyhjennetty. Koko kolonnin tyhjentämiseen voi kulua paljon aikaa, jolloin tuotantoa ei pystytä ajamaan eli oppilaat eivät pysty tekemään harjoitustöitensä. Ylivuoto voi myös aiheuttaa laitteiden vikaantumista. Lieventävänä toimintona seuraukselle on hälytys tiedon lähettäminen tislusautomaatiojärjestelmästä vastaavalle henkilölle.

- **Hälytystieto tislusautomaatiojärjestelmästä vastaavalle henkilölle:** Yli vuoto tilanteessa on tärkeää toimia nopeasti, jotta saadaan prosessi takaisin normaali tilaan ja tästä syystä hälytys tulisi lähettää prosessista vastaavalle henkilölle, joka voi itse tulla tekemään korjaustoimenpiteet prosessille tai delegoida tehtävän toiselle henkilölle.

### 5.3 Lämmitysyksikön ylikuumentuminen ja ylipaineistuminen

Kuvassa 16 on määritetty rusettimallinen riskianalyysi lämmitysyksikölle. Tapahtumana on lämmitysyksikön ylikuumentuminen tai ylipaineistuminen.



**Kuva 16 Lämmitysyksikön ennaltaehkäisy toiminnot ja seurauksien lieventävät toiminnot**

Alla kerrattuna tapahtuman uhat, tapahtumasta johtuvat seuraukset sekä lueteltuna ennaltaehkäiseviä toimintoja ja lieventäviä toimintoja.

**Virta-arvon monitorointi puuttuu valvomosta:** Kun tislousautomaatiojärjestelmää käytetään etänä, on ensiarvoisen tärkeää, että kaikki kriittiset tiedot ovat näkyvissä valvomon käyttöliittymässä, joka nähdään etäyhteydelläkin. Lämmitysyksikön virta-arvoa sieltä ei näe, jolloin etäkäyttäjällä ei ole mitään tietoa siitä mikä reaaliaikainen virta-arvo on ja onko koko yksikkö edes päällä. Kun monitorointi puuttuu etäkäyttäjä ei pysty tekemään asialle mitään, jos virta-arvo nousee liian korkeisiin lukemiin. Ennalta ehkäiseviä toimintoja uhalle ovat erillinen turva-automaatio järjestelmä ja virta-arvo tiedon tuonti valvomon käyttöliittymään.

- **Erillinen turva-automaatiojärjestelmä:** Turva-automaatiojärjestelmään yhdistetään virta-arvon mittauslaite. Mittaus arvon kohottua korkeammalle kuin määritetty arvo turva-automaatiojärjestelmään, tekee se tarvittavat toiminnot virta-arvon laskemiseksi sallittuihin arvoihin esimerkiksi rajoittamalla virran kulkua yksikköön.
- **Virta-arvon tuonti valvomon käyttöliittymään:** Etäkäyttäjät ovat tietoisia lämmitysyksikön virta-arvon tilasta, jolloin he voivat tehdä tarvittavia toimintoja virta-

arvon pysymiseksi sallituissa rajoissa. Esimerkiksi ilmoittaa paikan päällä olevalle henkilölle arvon noususta, jolloin henkilö voi esimerkiksi sammuttaa lämmitysyksikön. Etäkäyttäjät eivät itse pysty ohjaamaan lämmitysyksikköä automaatio järjestelmällä, koska se on manuaalinen laite, jonka ohjausta ei ole automaatio järjestelmän käyttöliittymässä.

**Painearvon monitorointi puuttuu valvomosta:** Tislausautomaation valvomon käyttöliittymästä ei myöskään nähdä lämmitysyksikön painearvoa. Etäkäyttäjällä ei ole siis tietoa lämmitysyksikön paineista, eikä etäkäyttäjä pysty tekemään asialle yhtään mitään, jos painearvo nousee liian korkeaksi. Ennalta ehkäiseviä toimintoja uhalle ovat erillinen turva-automaatio järjestelmä ja painearvo tiedon tuonti valvomon käyttöliittymään.

- **Erillinen turva-automaatiojärjestelmä:** Turva-automaatiojärjestelmään yhdistetään painearvon mittauslaite. Mittaus arvon kohottua korkeammalle kuin määritetty arvo turva-automaatiojärjestelmään, tekee se tarvittavat toiminnot painearvon laskemiseksi sallittuihin arvoihin esimerkiksi rajoittamalla virran kulkua yksikköön, jolloin lämpötila laskee ja höyrystä johtuva paine alenee.
- **Painearvo tiedon tuonti valvomon käyttöliittymään:** Etäkäyttäjät ovat tietoisia lämmitysyksikön painearvon tilasta, jolloin he voivat tehdä tarvittavia toimintoja painearvon pysymiseksi sallituissa rajoissa. Esimerkiksi ilmoittaa paikan päällä olevalle henkilölle arvon noususta, jolloin henkilö voi esimerkiksi sammuttaa lämmitysyksikön. Etäkäyttäjät eivät itse pysty ohjaamaan lämmitysyksikköä automaatio järjestelmällä, koska se on manuaalinen laite, jonka ohjausta ei ole automaatio järjestelmän käyttöliittymässä.

**Yksikkö toimii manuaalisesti:** Lämmitysyksiköstä ei tule minkäänlaisia tietoja valvomon käyttöjärjestelmään, joten etäkäyttäjän on mahdotonta tietää lämmitysyksikön reaaliaikaista tilaa, joka luo riskin ylikuumentumiselle tai ylipaineistumiselle. Ennalta ehkäisevinä toimintoina uhalle ovat erillinen turva-automaatiojärjestelmä ja ohjauksen yhdistäminen automaatio järjestelmään.

- **Erillinen turva-automaatiojärjestelmä:** Lämmitysyksikköön asennetaan mittauslaitteita, jotka yhdistetään turva-automaatiojärjestelmään. Järjestelmään määritetään raja-arvot paineelle ja virralle, jolloin raja-arvojen ylityttyä järjestelmä tekee toiminnot, joilla saadaan lämmitysyksikkö turvalliseen tilaan kuten esimerkiksi virran katkaisu laitteesta tämä edellyttää, että yksikön ohjaus on myös yhdistettynä turva-automaatiojärjestelmään.
- **Ohjauksen yhdistäminen automaatiojärjestelmään:** Lämmitysyksikön ohjauksen yhdistäminen automaatio järjestelmään antaisi etäkäyttäjille mahdollisuuden ohjata yksikköä etänä. Esimerkiksi jos arvot nousevat liian korkeiksi

pystyy etäkäyttäjä sammuttamaan lämmitysyksikön tai tekemään muita tarvittavia toimenpiteitä yksikön turvallisen tilan saavuttamiseksi. Tämä edellyttää myös sitä, että valvomon käyttöliittymässä on mittaustiedot virrasta ja paineesta näkyvillä.

**Mittalaitteiden rikkoontuminen:** Jos valvomon käyttöjärjestelmään saadaan tuotua tieto lämmitysyksikön tilasta sekä virta- ja painearvoista aiheuttaa mittareiden rikkoontuminen riskin ylikuumentumiselle sekä ylipaineistumiselle lämmitysyksikön käynnissä ollessa, jos ei ole ohjauspiiriä, jolla estetään yksikön käyttö kun mittalaite on rikkoontunut. Ennalta ehkäiseviä toimintoja uhalle ovat erillinen turva-automaatiojärjestelmä ja mittareiden tilojen monitorointi käyttöjärjestelmään.

- **Erillinen turva-automaatiojärjestelmä:** Järjestelmään tehdään ohjaus, joka estää lämmitysyksikön käytön, jos jokin mittalaite on rikki.
- **Mittareiden tilojen monitorointi valvomon käyttöjärjestelmään:** Mittareiden tila tiedot kertovat etäkäyttäjälle onko lämmitysyksikössä mittalaitteet kunnossa.

**Koulutuksen puute:** Tislausautomaation käyttäjien koulutuksen puute lämmitysyksiköstä ja sen toiminnasta. Ennalta ehkäiseviä toimintoja uhalle ovat erillinen turva-automaatiojärjestelmä ja etäkäyttäjien kouluttaminen.

- **Erillinen turva-automaatiojärjestelmä:** Järjestelmä ajaa yksikön turvalliseen tilaan tarvittaessa. Tämä ehkäisee vahinkoja, jotka aiheutuvat etäkäyttäjien tahattomista toimista ja koulutuksen puutteen syystä.
- **Etäkäyttäjien kouluttaminen:** Kouluttamalla käyttäjät järjestelmän toimintoihin ja laitteisiin, joita järjestelmä sisältää. Tällätavalla vältetään vahingoilta ja koulutuksen puutteesta aiheutuvista vahingoista. Pitää kuitenkin muistaa, että etäkäyttäjät ovat ihmisiä ja ihmisille voi tapahtua vahinkoja, vaikka olisi koulutettu tarvittavalla tavalla järjestelmän toimintoihin.

Alla kerrattuna tapahtuman seuraukset sekä lueteltuna seurauksille lieventävät toiminnot.

**Tulipalo:** Lämmitysyksikön ylikuumentuessa, herkästi syttyvät nesteet tai laitteet saattavat aiheuttaa tulipalon. Lieventävinä toimintoina seuraukselle ovat tulipalon hälytysjärjestelmä ja hälytystiedon lähettäminen prosessista vastaavalle henkilölle.

- **Tulipalon hälytysjärjestelmä:** Hälyttää tarvittaessa palokunnan paikalle ja hälytys äänellä ilmoittaa järjestelmän lähistöllä oleville henkilöille palosta.
- **Hälytystiedon lähettäminen prosessista vastaavalle henkilölle:** Tulipalon tapahtuessa samalla kun palokunta hälytetään paikalle, on tärkeää lähettää hälytys ilmoitus prosessista vastaavalle henkilölle, vaikka tekstiviestinä, jolloin hän

tietää tehdä tarvittavat toiminnot tuhojen minimoimiseksi palokunnan kanssa yhteistyönä.

**Lämmitysyksikön rikkoontuminen:** Yksikön ylikuumentuessa tai ylipaineistuessa yksiköstä voi hajota komponentteja tai laitteita. Lieventävinä toimintoina seuraukselle ovat varastoon varastoidut varaosat ja prosessista vastaavalle henkilölle hälytystieto yksiköstä.

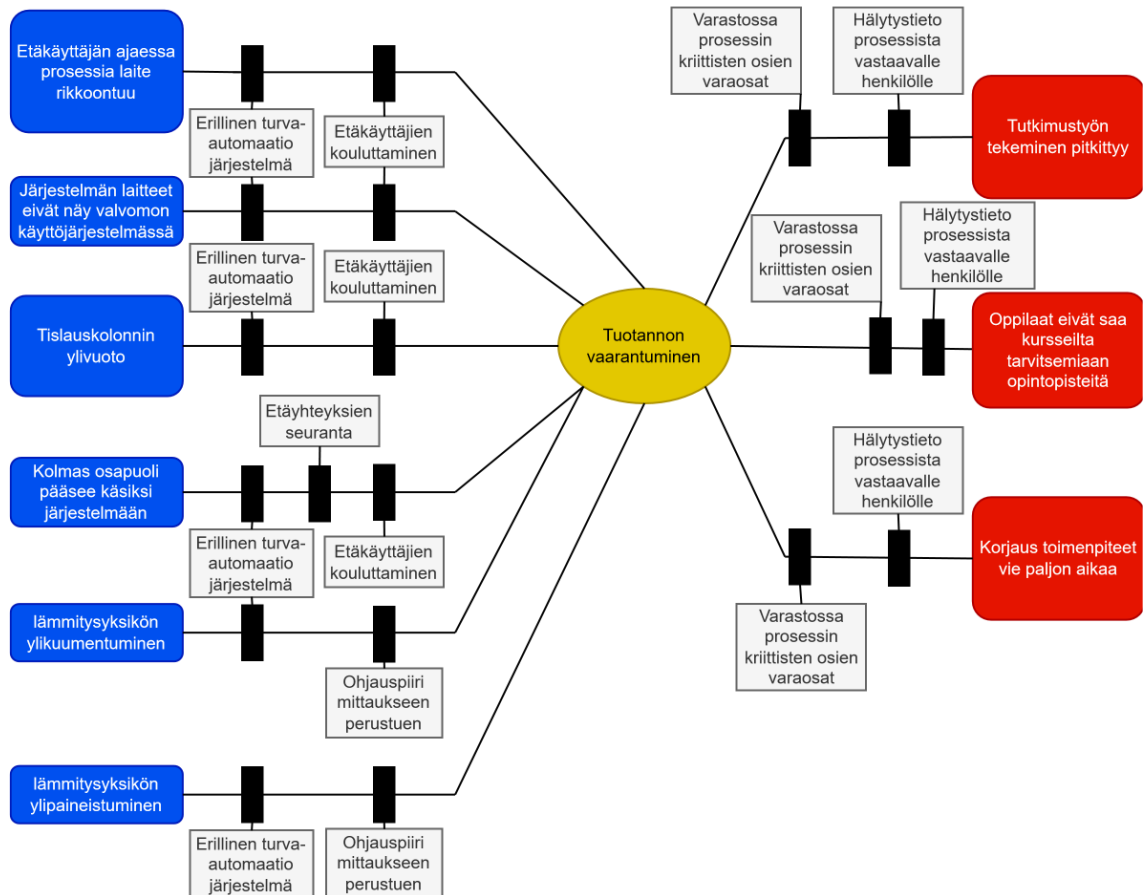
- **Varastoon varastoidut varaosat:** Jos yksiköstä menee komponentteja tai laitteita rikki, on ne nopeaa vaihtaa, kun varaosat ovat valmiina varastossa eikä tarvitse odottaa pitkiä aikoja uusien osien saamiseksi.
- **Prosessista vastaavalle henkilölle hälytystieto:** Yksikön rikkoontumisesta lähetetään hälytys tieto prosessista vastaavalle henkilölle, jolloin henkilö pystyy tekemään korjaustoimenpiteet mahdollisimman nopeasti tuotannon jatkumisen vuoksi tai sitten delegoimalla tehtävän toiselle henkilölle.

**Paikalla olevan henkilön tapaturma:** Yksikön ylikuumentuessa on mahdollista henkilön saada palovamma koskiessaan yksikköön tai ylipaineistuessa jotkin putket saattavat pettää ja roiskaista kuumaa nestettä henkilön päälle. Lieventävänä toimenpiteenä seuraukselle on hälytyksen antaminen valvomon käyttöliittymään.

- **Valvomon käyttöliittymään hälytys:** Paikalla oleva henkilö näkee valvomon käyttöliittymästä, että lämmitysyksiköllä on hälytys ja tiedostaa riskin tapaturmalle, jos menee lähelle lämmitysyksikköä.

## 5.4 Tuotannon vaarantuminen

Kuvassa 17 on esitetty tuotannon vaarantumisesta rusettimallinen riskianalyysi. Tislausautomaatiojärjestelmän tuotannolla tarkoitetaan opintopisteitä ja tämä riskianalyysi on tehty sitä silmällä pitäen.



**Kuva 17 Tuotannon vaarantumisen ennaltaehkäisy toiminnot ja seurauksien lieventävät toiminnot**

Alla kerrattuna tapahtuman uhat tapahtumasta johtuvat seuraukset sekä lueteltuna ennaltaehkäiseviä toimintoja ja lieventäviä toimintoja.

**Etäkäyttäjän ajaessa prosessia prosessilaitte rikkoontuu:** Etäkäyttäjä rikkoo prosessilaitteen vahingossa tai koulutuksen puutteen takia, jolloin tuotanto vaarantuu. Riippuen rikkimenneestä laitteesta, korjaamiseen tai uuden laitteen saamiseen voi mennä paljonkin aikaa. Ennalta ehkäiseviä toimintoja uhalle ovat erillinen turva-automaatio järjestelmä ja etäkäyttäjien kouluttaminen prosessin toimintoihin. Tätä uhkaa ei pystytä täysin estämään, koska laitteet ja komponentit prosessissa kuluu ja näin ollen rikki menemisen riski kasvaa.

- **Erillinen turva-automaatiojärjestelmä:** Turva-automaatiojärjestelmään on ohjelmoitu laitteiden monitorointi. Jos prosessin jokin kriittinen laite menee rikki, estää turva-automaatiojärjestelmä prosessin käytön tai estää se tietyn prosessin toiminnon käyttämisen.
- **Etäkäyttäjien kouluttaminen:** Kouluttamalla etäkäyttäjät ohjaamaan ja käyttämään prosessinlaitteita oikealla tavalla, saadaan ehkäistyä laitteiden käyttäjä virheistä johtuvia rikkoontumisia.

**Järjestelmän laitteet eivät näy valvomon käyttöjärjestelmässä:** Lämmitysyksikkö ei näy ollenkaan valvomon käyttöjärjestelmässä ja lauhdutusvesiventtiin tilakaan ei näy valvomon käyttöjärjestelmässä, koska se on käsikäyttöinen venttiili. Tämä aiheuttaa sen, ettei etäkäyttäjät tiedä näiden laitteiden olemassaolosta eikä sitä kuinka kriittisiä ne ovat onnistuneen tuotannon suhteen. Ennalta ehkäiseviä toimintoja uhalle ovat erillinen turva-automaatiojärjestelmä sekä etäkäyttäjien kouluttaminen.

- **Erillinen turva-automaatiojärjestelmä:** turva-automaatiojärjestelmään tehdään ohjaukset kaikille tuotannolle kriittisille laitteille mittaustietojen perusteella ja vaikka etäkäyttäjä ei tiedä laitteiden olemassaolosta pystyy hän käyttämään prosessia turvallisesti koska turva-automaatiojärjestelmä tarvittaessa yli kirjoittaa kaikki tarvittavat toiminnot omillaan, jos prosessin arvot ylittävät määritetyt raja-arvot tai prosessin laitteita menee rikki.
- **Etäkäyttäjien kouluttaminen:** Kouluttamalla etäkäyttäjät tuntemaan kaikki järjestelmässä olevat laitteet nekin, jotka eivät näy valvomon käyttöliittymässä pystytään ehkäisemään laitteiden rikkoontumisia sekä mahdollisia tapaturmia.

**Tislauskolonnin ylivuoto:** Ylivuodon tapahtuessa kolonni on täynnä nestettä, jolloin tuotannon ajaminen on mahdotonta. Kolonnin tyhjäksi pumppaamiseen voi kulua paljon aikaa. Uhan ennaltaehkäiseviä toimintoja ovat erillinen turva-automaatiojärjestelmä ja etäkäyttäjien kouluttaminen.

- **Erillinen turva-automaatiojärjestelmä:** Turva-automaatiojärjestelmään on asennettuna tarvittavat mittalaitteet, joiden mittaamia arvoja käytetään pumppujen ohjauksissa kuten esimerkiksi pinnanmittauslaitteet. Tällä tavalla saadaan ennaltaehkäistyä tislauskolonnin ylivuoto.
- **Etäkäyttäjien kouluttaminen:** Kouluttamalla etäkäyttäjät prosessin toimintoihin ja ominaisuuksiin kuten esimerkiksi siihen, että syöttöpumppu pysyy päällä niin kauan, kunnes joku sen manuaalisesti napista sammuttaa. Tällä tavalla saadaan ennaltaehkäistyä tislauskolonnin ylivuoto, koska etäkäyttäjät ovat tietoisia prosessin toiminnoista ja ominaisuuksista ja osaavat tehdä tarvittavat toiminnot käyttönsä aikana turvatakseen prosessin.

**Kolmasosapuoli pääsee käsiksi järjestelmään:** Kolmas osapuoli tai ulkopuolinen henkilö, joka pääsee käsiksi tislausautomaatioon, pystyy aiheuttamaan tuotannolle ongelmia kuten tahallinen laitteiden väärin ohjelmoiminen, mittaus rajojen vääränlainen määrittäminen, pumppujen ohjauksien tahallinen väärin määrittäminen ja monia muita asioita. Ennaltaehkäisevinä toimintoina uhalle ovat erillinen turva-automaatiojärjestelmä, etäyhteyksien seuranta ja etäkäyttäjien kouluttaminen.

- **Erillinen turva-automaatiojärjestelmä:** Turva-automaatiojärjestelmään on ohjelmoitu omat ohjaukset kaikille kriittisille toiminnoille ja niillä pystytään ylikirjoittamaan perusautomaatio järjestelmän ohjelmoinnit. Turva-automaatiojärjestelmän toiminnot ovat myös suojattu salasanoin ja käyttäjätunnuksin. Näitä tunnuksia ja salasanoja ei saa luovuttaa muille kuin prosessista vastaaville henkilöille.
- **Etäyhteyksien seuranta:** Seuraamalla etäyhteyksiä pystytään identifioimaan käyttäjä, joka on aiheuttanut tahallisen vahingon sekä paikka, josta on etäyhteyksimuodostettu.
- **Etäkäyttäjien kouluttaminen:** Etäkäyttäjille korostetaan millaisia riskejä se aiheuttaa, jos he antavat etäyhteyden käyttäjätunnukset ja salasanat jollekin ulkopuoliselle ja niiden jakaminen myös kielletään koulutusmateriaalissa.

**Lämmitysyrityksen ylikuumentuminen:** Ylikuumentuessa lämmitysyrityksestä voi hajota komponentteja tai laitteita. Tästä syystä tuotanto saattaa vaarantua. Ennaltaehkäisevinä toimintoina uhalle ovat erillinen turva-automaatiojärjestelmä ja ohjauspiiri mittaukseen perustuen.

- **Erillinen turva-automaatiojärjestelmä:** Saadaan ohjelmoitua ohjauspiiri lämmitysyritykselle, jolla mittausarvoon perustuen voidaan ohjata lämmitysyrityksen virtaa tarvittaessa pienemmälle ehkäistäksemme ylikuumentumisen ja laitteiden sekä komponenttien rikkoontumisen.
- **Ohjauspiiri mittaukseen perustuen:** Toinen tapa välttää ylikuumentuminen on tehdä lämmitysyritykselle ohjauspiiri perusautomaatiojärjestelmään, joka ohjaa mittausarvoon perusteella yksikön virtaa. Tässä on riskinä se kun opiskeluympäristössä pitää oppilaiden päästä tekemään ohjauksia laitteille perusautomaatiojärjestelmässä jolloin myös tätä ohjauspiiriä päästään muokkaamaan.

**Lämmitysyrityksen ylipaineistuminen:** Ylipaineistuessa lämmitysyrityksestä voi hajota komponentteja tai laitteita. Tästä syystä tuotanto saattaa vaarantua. Ennaltaehkäisevinä toimintoina uhalle ovat erillinen turva-automaatiojärjestelmä ja ohjauspiiri mittaukseen perustuen.

- **Erillinen turva-automaatiojärjestelmä:** Saadaan ohjelmoitua ohjauspiiri lämmitysyritykselle, jolla mittausarvoon perustuen voidaan ohjata lämmitysyrityksen virtaa tarvittaessa pienemmälle ehkäistäksemme ylipaineistumisen ja laitteiden sekä komponenttien rikkoontumisen.
- **Ohjauspiiri mittaukseen perustuen:** Toinen tapa välttää ylipaineistuminen on tehdä lämmitysyritykselle ohjauspiiri perusautomaatiojärjestelmään, joka ohjaa

mittaustuloksen perusteella yksikön virtaa. Tässä on riskinä se kun opiskeluym-päristössä pitää oppilaiden päästä tekemään ohjauksia laitteille perusautomaatiojärjestelmässä jolloin myös tätä ohjauspiiriä päästään muokkaamaan.

Alla kerrattuna tapahtuman seuraukset sekä lueteltuna seurauksille lieventävät toiminnot.

**Tutkimustyön tekeminen pitkittyy:** Usein tutkimus töillä on tiukat aikataulut ja jos tuotanto vaarantuu eli laitteisto menee esimerkiksi rikki, vaikuttaa se tutkimuksen aikatauluihin. Lieventävinä toimintoina seuraukselle ovat tuotannolle kriittisten osien varastointi ja hälytystiedon lähettäminen prosessista vastaavalle henkilölle.

- **Tuotannolle kriittisten osien varastointi:** Varastoimalla tuotannon jatkumiseksi kriittiset varaosat lievennetään esimerkiksi rikkimenneen osan korjaukseen kulunutta aikaa. Jos joudutaan tilaamaan uusi osa siinä voi mennä todella kauan, joten varastoimalla kriittiset osat pystytään lieventämään tutkimustyön pitkittymiseen kulunutta aikaa.
- **Hälytystiedon lähettäminen prosessista vastaavalle henkilölle:** Prosessista vastaava henkilö saa tiedon tuotannon vaarantumisesta esimerkiksi osan rikkoontumisen takia, jolloin hän pystyy tekemään nopeita päätöksiä, jotta tuotantoa pystyttäisiin jatkamaan mahdollisimman nopeasti.

**Oppilaat eivät saa kursseiltaan tarvittavia opintopisteitä:** Pahimmassa tapauksessa jos tislusautomaatio on toimintakyvyttömässä kunnossa pitkään joudutaan siirtämään kurssia toisille periodeille tai suunnittelemaan kurssin sisältö uudelleen. Lieventävinä toimintoina seuraukselle ovat tuotannolle kriittisten osien varastointi ja hälytystiedon lähettäminen prosessista vastaavalle henkilölle.

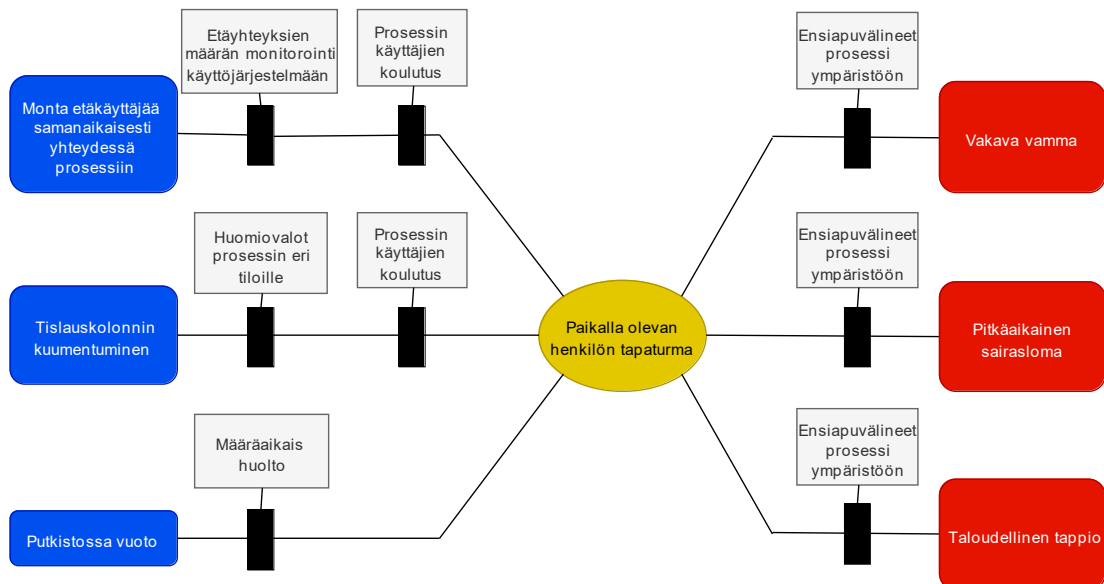
- **Tuotannolle kriittisten osien varastointi:** Varastoimalla tuotannon jatkumiseksi kriittiset varaosat lievennetään esimerkiksi rikkimenneen osan korjaukseen kulunutta aikaa. Jos joudutaan tilaamaan uusi osa siinä voi mennä todella kauan, joten varastoimalla kriittiset osat pystytään lieventämään tutkimustyön pitkittymiseen kulunutta aikaa.
- **Hälytystiedon lähettäminen prosessista vastaavalle henkilölle:** Prosessista vastaava henkilö saa tiedon tuotannon vaarantumisesta esimerkiksi osan rikkoontumisen takia, jolloin hän pystyy tekemään nopeita päätöksiä, jotta tuotantoa pystyttäisiin jatkamaan mahdollisimman nopeasti.

**Korjaustoimenpiteet vievät paljon aikaa:** Jos tislusautomaation laitteisto on epä-kunnossa voi uusien laitteiden saaminen tai niiden korjaaminen viedä aikaa paljon. Lieventävinä toimintoina seuraukselle ovat tuotannolle kriittisten osien varastointi ja hälytystiedon lähettäminen prosessista vastaavalle henkilölle.

- **Tuotannolle kriittisten osien varastointi:** Varastoimalla tuotannon jatkumiseen kriittiset varaosat lievennetään esimerkiksi rikkimenneen osan korjaukseen kulunutta aikaa. Jos joudutaan tilaamaan uusi osa siinä voi mennä todella kauan, joten varastoimalla kriittiset osat pystytään lieventämään tutkimustyön pitkittymiseen kulunutta aikaa.
- **Hälytystiedon lähettäminen prosessista vastaavalle henkilölle:** Prosessista vastaava henkilö saa tiedon tuotannon vaarantumisesta esimerkiksi osan rikkoutumisen takia, jolloin hän pystyy tekemään nopeita päätöksiä, jotta tuotantoa pystyttäisiin jatkamaan mahdollisimman nopeasti.

## 5.5 Paikalla olevan henkilön tapaturma

Kuvassa 18 tarkastellaan paikan päällä olevan henkilön tapaturman tapahtumaa rusettimallilla.



**Kuva 16 Henkilön tapaturman ennaltaehkäisy toiminnot ja seurauksien lieventävät toiminnot**

Alla kerrattuna tapahtuman uhat, tapahtumasta johtuvat seuraukset sekä lueteltuna ennaltaehkäiseviä toimintoja ja lieventäviä toimintoja.

**Monta etäkäyttäjää samanaikaisesti yhteydessä prosessiin:** Paikalla oleva henkilö tällä hetkellä ei näe mistään onko järjestelmään joku etänä yhteydessä. Tämä aiheuttaa tapaturma riskin, koska etäkäyttäjään ei näe onko ihmisiä paikan päällä. Esimerkiksi jos järjestelmää huolletaan ja siihen otetaan etäyhteys, pystyy etäkäyttäjä ajamaan prosessia huollon aikana, mikäli on unohtunut huoltohenkilöiltä tehdä prosessi vaarattomaksi huollon ajaksi. Ennaltaehkäiseviä toimintoja uhalle ovat etäyhteyksien määrän monitorointi valvomon käyttöjärjestelmään ja prosessin käyttäjien kouluttaminen.

- **Etäyhteyksien määrän monitorointi valvomon käyttöjärjestelmään:** Tällä tavalla pystytään paikalla oleville henkilöille näyttämään, että prosessiin on etäyhteys päällä. Tapaturman ehkäisemiseksi riittää, että käyttöjärjestelmässä näkyy tieto etäyhteydestä ei ole väliä montako niitä on samanaikaisesti prosessissa. Kun tieto näkyy ja paikalla olevat henkilöt sen huomaavat, tietävät he, että prosessia saatetaan myös ajaa etänä.
- **Prosessin käyttäjien kouluttaminen:** Käyttäjiin sisällytetään tässä yhteydessä huoltohenkilötkin. Kaikki henkilöt, jotka tekevät prosessille jotain on koulutettava tarpeeksi hyvin ja heille on tuotava esille, että järjestelmää käytetään myös etänä.

**Tislauskolonnin kuumentuminen:** Kun prosessia ajetaan, kuumentuu kolonni ja aiheuttaa palovamman riskin, jos paikalla oleva henkilö koskee kolonniin. Ennaltaehkäisevinä toimintoina uhalle ovat huomiovalot prosessin eri tiloihin ja prosessin käyttäjien koulutus.

- **Huomiovalot prosessin eri tiloihin:** Tiloilla tarkoitetaan prosessin sen hetkistä tilaa eli onko prosessi ajossa, hälytystilassa vai seisonta tilassa. Kun eri tiloista on huomiovalot pystyvät paikalla olevat henkilöt sen perusteella varomaan prosessin eri osia. Esimerkiksi jos prosessi on käynnissä ja vaikka vihreällä valolla indikoidaan käynnissä tilaa niin tietävät paikalla olevat henkilöt, että tislauskolonni voi olla kuuma.
- **Prosessin käyttäjien koulutus:** Käyttäjiin sisällytetään tässä yhteydessä huoltohenkilötkin. Kaikki henkilöt, jotka tekevät prosessille jotain on koulutettava tarpeeksi hyvin ja heille on tuotava esille, että järjestelmää käytetään myös etänä. On myös koulutuksessa tuotava ilmi mitä eriväriset huomiovalot tarkoittavat, jos sellaiset asennetaan prosessi ympäristöön.

**Putkistossa vuoto:** Prosessille ei tehdä määräaikaista huoltoja, joten putkiston vuoto saattaa jäädä huomaamatta ja paikan päällä oleva henkilö altistuu tapaturman mahdollisuudelle. Ennaltaehkäisevänä toimintona uhalle olisi määräaikaishuollot järjestelmälle.

- **Määräaikaishuollot järjestelmälle:** Sisältää kaikkien putkistojen tarkastukset sekä toimilaitteiden kunnan tarkastuksen. Tällä tavalla saadaan ehkäistyä mahdollista tapaturmaa, koska saadaan kiinni heikot ja rikkimenneet osat prosessista.

Alla kerrattuna tapahtuman seuraukset sekä lueteltuna seurauksille lieventävät toiminnot.

**Vakava vamma:** Esimerkiksi jos putkistovuodon takia paikalla olevan henkilön päälle roiskuu kuumaa nestettä, aiheuttaa se mahdollisesti vakavat palovammat. Lieventävänä toimena uhalle on ensiapuvälineiden asettaminen prosessi ympäristöön.

- **Ensiapuvälineiden asettaminen prosessi ympäristöön:** Jos tapaturma tapahtuu niin, lähellä olevilla ensiaputarvikkeilla pystytään hoitamaan nopeasti tapaturmasta aiheutunutta vammaa ja parhaimmassa tapauksessa saadaan lievennettyä vamma niin, pieneksi ettei se tarvitse jatkotoimenpiteitä.

**Pitkäaikainen sairausloma:** Vakavasta vammasta toipuminen vie paljon aikaa, joten henkilö joutuu olemaan pitkäaikaisella sairauslomalla. Lieventävänä toimintona seuraukselle on ensiapuvälineiden asettaminen prosessi ympäristöön.

- **Ensiapuvälineiden asettaminen prosessi ympäristöön:** Jos tapaturma tapahtuu niin, lähellä olevilla ensiaputarvikkeilla pystytään hoitamaan nopeasti tapaturmasta aiheutunutta vammaa ja parhaimmassa tapauksessa saadaan lievennettyä vamma niin, pieneksi ettei se tarvitse jatkotoimenpiteitä. Tällä tavoin saadaan sairausloman pituutta lyhennettyä ja vamman vakavuutta pienennettyä.

**Taloudellinen tappio:** Henkilö jolle tapaturma on tapahtunut, joutuu olemaan pitkällä sairauslomalla riippuen tapaturman aiheuttamasta vammasta. Jos henkilö on organisaation työntekijä aiheuttaa se taloudellisia tappioita organisaatiolle koska henkilön tilalle on palkattava tuuraaja sekä henkilön sairauslomarahaa pitää maksaa. Jos henkilö on ulkopuolinen, joudutaan hänelle maksamaan korvauksia mahdollisen vamman tuottamisesta organisaation tiloissa. Lieventävänä toimintona seuraukselle on ensiapuvälineiden asettaminen prosessi ympäristöön.

- **Ensiapuvälineiden asettaminen prosessi ympäristöön:** Jos tapaturma tapahtuu niin, lähellä olevilla ensiaputarvikkeilla pystytään hoitamaan nopeasti tapaturmasta aiheutunutta vammaa ja parhaimmassa tapauksessa saadaan lievennettyä vamma niin, pieneksi ettei se tarvitse jatkotoimenpiteitä. Tällä tavoin saadaan sairausloman pituutta lyhennettyä ja vamman vakavuutta pienennettyä sekä taloudellinen tappio jää pienemmäksi.

## 5.6 Tulosten yhteenveto

Tuloksia tarkastellessa huomataan, että suurimassa osassa tapahtumissa on ennaltaehkäisevänä tekijänä erillisen turva-automaatiojärjestelmän tai käyttöautomaation lukitusten keinoin toteutettu turvallisuus. Kolonnin pintojenmittaukseen olisi hyvä asentaa anturit turva-automaatiojärjestelmää varten jolloin, anturien tunnistuessa pinnan korkeuden ohjaa turva-automaatiojärjestelmä kolonnin poistopumpun päälle ja syöttöpumpun pois päältä, jolloin saadaan pinnan korkeutta laskettua. Liian korkealle nouseva kolonnin pinta aiheuttaa tapaturma vaaran. Lämmitysyksikölle pitäisi myös asentaa virtamittari sekä painemittari ja näiden pitäisi olla yhteydessä turva-automaatio järjestel-

mään. Tämä pitää tehdä siitä syystä, että tällä hetkellä lämmitysyksikkö on manuaalisesti käytettävä ja jos operaattori tai käyttäjä ei huomaa virta-arvon tai painearvon liiallista nousua aiheutuu siitä mahdollinen vaaratilanne. Kun mittarit ovat yhdistetty turva-automaatio järjestelmään ja arvot nousevat liian korkeiksi tekee turva-automaatio järjestelmä sille ennalta määritetyt toiminnot lämmitysyksikön turvalliseen tilan saavuttamiseksi, kuten virran poispäältä laittaminen tai ylipaineen päästäminen pois säiliöstä. Pumpun päälle jäämisen ehkäisemiseksi turvaututaan toiminnalliseen turvallisuuteen eli tehdään ohjauspiiri, joka sammuttaa pumpun määritetyin aikavälein. Tälle toiminnolle pitää myös laittaa käyttöliittymään ohitus painike, jos halutaan esimerkiksi ajaa prosessia tutkimuskäytössä pitempiä aikoja kuin määritetty sammutus aikaväli. Tarvitaan myös turva-automaatio järjestelmää, johon ohjelmoidaan ohjauspiirejä erilaisten antureiden avulla kuten syöttösäiliön pinnanmittaus anturi, syöttöpumpulle tulevan putken virtausmittari sekä kolonnin pinnankorkeuden mittaamiseen käytetty anturi. Kun jonkun näiden antureiden määritetyistä arvoista ylittyy tai alittuu sammuttaa turva-automaatio järjestelmä syöttöpumpun ja ajaa prosessin turvalliseen tilaan. Järjestelmään pitää tehdä myös lukitus, jos edellä mainittujen antureiden määritetyt arvot ovat ylittyneinä tai alittuneina kun prosessia yritetään ajaa tai käyttää niin se ei ole mahdollista ennen kuin kyseiset arvot ovat sallituissa lukemissa. Paikalla olevan henkilön tai huoltohenkilön tapaturman ennalta ehkäisemiseksi on tärkeää tehdä prosessille määräaikaishuoltoja, joissa tarkastetaan, että putket eivät vuoda tai ole ruostuneet, kriittiset mittalaitteet ovat toimintakunnossa ja näyttävät oikeita arvoja, tehdään testit, että turva-automaatio toimii edelleen niin kuin sen on tarkoituskin, pumput ovat kunnossa ja säiliöissä on nesteitä tarpeeksi. Prosessi ympäristöön laitetaan jonkinlainen valomajakka, jossa eriväriset valot tarkoittavat eriasioita kuten onko prosessi ajossa tai hälytystilassa ja niin edes. Valvomon käyttöjärjestelmään näkyviin etäyhteyksien määrä reaaliajassa järjestelmässä, jolloin paikalla oleva henkilö on tietoinen, että joku etänä oleva henkilö voi yrittää käyttää prosessia. Tähän pitää myös kouluttaa henkilöt, jotka käyttävät prosessia paikan päällä.

Alla on täytettyinä taulukot, johon merkitty uhat yhtä ennalta ehkäisevää toimintoa kohden sekä seuraukset yhtä lieventävää toimintoa kohden ja niiden jäännösriskit. Taulukosta 1 nähdään millä ennalta ehkäisevällä toiminnalla saadaan sille kohdistetut uhat estettyä sekä jäännös riski, jos toiminto toteutetaan. Taulukosta 2 nähdään millä lieventävällä toiminnalla saadaan sille kohdistetut seuraukset lievennettyä ja millainen jäännösriski lieventävän toiminnan toteutuessa on.

**Taulukko 1 Uhille kohdistetut ennalta ehkäisevät toiminnot**

Ennaltaehkäisevä toiminto	Uhat	Jäännösriski
Erillinen turva-automaatiojärjestelmä	Etäkäyttäjä unohtaa sammuttaa syöttöpumpun, Mittalaitteiden ohjauspiirien raja-arvot määritetty väärin, Mittalaitteen rikkoontuminen, Tahallinen syöttöpumpun päälle jättäminen, Virta-arvon monitorointi puuttuu valvomon käyttöliittymästä, Painearvon monitorointi puuttuu valvomon käyttöliittymästä, Lämmitysyksikkö toimii manuaalisesti, Lämmitysyksikön mittalaitteiden rikkoontuminen, Etäkäyttäjien koulutuksen puute, Etäkäyttäjän ajaessa prosessia laite rikkoontuu, Järjestelmän kaikki laitteet eivät näy valvomon käyttöliittymässä, Tislauskolonnin ylivuoto, Ulkopuolinen henkilö pääsee käsiksi järjestelmään, Lämmitysyksikön ylikuumentuminen, Lämmitysyksikön ylipaineistuminen.	Turva-automaatiojärjestelmän käyttäjätunnuksien ja salasanojen vuotaminen väärin käsiin, Turva-automaatiojärjestelmän ohjelmointi tehty huonosti.
Etäkäyttäjien kouluttaminen	Etäkäyttäjä unohtaa sammuttaa syöttöpumpun, Etäyhteys katkeaa, Mittalaitteiden ohjauspiirien	Etäkäyttäjät eivät sisäistä koulutettuja asioita

	<p>raja-arvot määritetty väärin, Koulutuksen puute lämmitysyksiköstä, Etäkäyttäjän ajaessa prosessia laite rikkoontuu, Järjestelmän kaikki laitteet eivät näy valvomon käyttöliittymässä, Tislauskolonnin ylivuoto, Ulkopuolinen henkilö pääsee käsiksi järjestelmään, Monta etäkäyttäjää samanaikaisesti yhteydessä prosessiin, Tislauskolonnin kuumentuminen.</p>	
<p>Syöttöpumpulle ohjauspiiri, joka sammuttaa sen määritetyin aikavälein</p>	<p>Etäkäyttäjä unohtaa sammuttaa syöttöpumpun, Etäyhteys katkeaa, Tahallinen syöttöpumpun päälle jättäminen.</p>	<p>Prosessia käytävillä henkilöillä on valtuudet ohjelmoida sekä tehdä uusia ohjauksia prosessin laitteille, jolloin on riski, että ohjauspiirejä yli kirjoitetaan tai poistetaan.</p>
<p>Käyttöautomaatioon tehty lukitus</p>	<p>Mittalaitteiden ohjauspiirien raja-arvot määritetty väärin, Mittalaitteen rikkoontuminen, Tahallinen syöttöpumpun päälle jättäminen.</p>	<p>Lukituksiin käytetyt salasanat ja käyttäjätunnukset leviävät ulkopuolisten käsiin</p>
<p>Etäyhteyksien seuranta</p>	<p>Tahallinen syöttöpumpun päälle jättäminen, Ulkopuolinen henkilö pääsee käsiksi järjestelmään.</p>	<p>Tekijä ei välitä kiinnijäämisestä.</p>
<p>Mittaustietoon perustuva ohjauspiiri</p>	<p>Etäkäyttäjä unohtaa sammuttaa syöttöpumpun,</p>	<p>Prosessia käytävillä henkilöillä on valtuudet ohjelmoida sekä tehdä uusia</p>

	Lämmitysyksikön ylikuumentuminen, Lämmitysyksikön ylipaineistuminen.	ohjauksia prosessin laitteille, jolloin on riski, että ohjauspiirejä yli kirjoitetaan tai poistetaan.
Valvomon käyttöliittymään lämmitysyksikön mittaus-tiedot.	Virta-arvon monitorointi puuttuu valvomon käyttöliittymästä, Painearvon monitorointi puuttuu valvomon käyttöliittymästä.	Etäkäyttäjät eivät huomaa mitta-arvoja valvomon käyttöliittymässä.
Lämmitysyksikön ohjauksen yhdistäminen automaatiojärjestelmään	Yksikkö toimii manuaalisesti	Jos ei yhdistetä turva-automaatio järjestelmään, on riskinä prosessia käyttävien henkilöiden valtuudet tehdä muutoksia ohjauspiireihin tai yli kirjoittaa niitä sekä poistaa
Lämmitysyksikön mittareiden tilojen monitorointi valvomon käyttöjärjestelmään	Mittareiden rikkoontuminen	Etäkäyttäjä ei huomaa valvomon käyttöliittymässä mittarin tilaa.
Etäyhteyksien määrän monitorointi valvomon käyttöjärjestelmään.	Monta etäkäyttäjää samanaikaisesti yhteydessä prosessiin.	Paikalla oleva henkilö ei huomaa valvomon käyttöliittymässä etäyhteyksien monitorointia.
Huomiovalot prosessin eri tiloille	Tislauskolonnin kuumentuminen.	Huomio valot on väärin ohjelmoitu sekä käyttäjä ei ole koulutettu huomiovalojen erivärien tarkoituksiin.
Määräaikaishuolto	Putkistossa vuoto	Määräaikaishuollolla saadaan pitkälti kaikki rikkoontuneet laitteet ja osat huomioitua, mutta aina jää riski sille, ettei ole huomattu tai jokin osa tai laite rikkoontuu yllättävästi.

**Taulukko 2 Seurauksille kohdistetut lieventävät toiminnot**

Lieventävä toiminto	Seuraukset	Jäännösriski
Takaisin kytkentä antaa hälytyksen	Syöttöpumpun rikkoontuminen	Laitteen korjaukseen tai uuden tilaamiseen voi kulu paljon aikaa.
Anturi antaa hälytyksen	Tislauskolonnin ylivuoto, Syöttösäiliöiden tyhjentäminen.	Anturin rikkoontuminen. Anturin raja-arvojen ohjelmointi tehty väärin
Äänimerkki prosessi ympäristössä	Palovamma	Henkilö ei kuule äänimerkkiä
Huohotin putken alla olevan alueen aidoittaminen	Huohotin putkista nesteen ulostuleminen	Aidatulle alueelle meneminen
Hälytystieto prosessista vastaavalle henkilölle	Tuotannon vaarantuminen pitkäksi aikaa, Tulipalo, Lämmitysyksikön rikkoontuminen, Tutkimustyön tekeminen pitkittyä, Oppilaat eivät saa tarvitsemaansa osaamista kurssilta, Korjaus toimenpiteet vievät paljon aikaa.	Vastaava henkilö ei huomaa lähetettyä hälytystietoa.
Tulipalon hälytysjärjestelmä	Tulipalo	Tulipalon hälytysjärjestelmässä vikaantuminen
Prosessista tulee hälytys valvomoon	Paikalla olevan henkilön tapaturma	Paikalla oleva henkilö ei huomaa valvomoon tulleutta hälytystä.
Varastossa tuotannon varmistamiseksi kriittiset varaosat	Tutkimustyön tekeminen pitkittyä, Oppilaat eivät saa tarvitsemaansa osaamista kurssilta, Korjaus toimenpiteet vievät paljon aikaa.	Varaosat ovat loppuneet varastosta.
Ensiapuvälineet prosessiympäristöön	Vakava vamma, Pitkäaikainen sairausloma, Taloudellinen tappio.	Ensiapuvälineiden käytön koulutuksen puute

## 6. YHTEENVETO

Diplomityö oli alueeltansa todella laaja, kun piti ottaa huomioon prosessin kokonaisturvallisuus, johon sisältyy prosessintietoturva, prosessiturvallisuus sekä etäyhteyksien turvallisuus. Työstä olisi mahdollisesti saatu yksityiskohtaisempi, jos se olisi rajattu pelkästään tietoturvan tai prosessiturvallisuuden näkökannalle kuten millaisia riskejä etäyhteyden muodostaminen aiheuttaa prosessiturvallisuuden tai tietoturvallisuuden kannalta. Tällä tavoin olisi päästy syvemmälle teoriaan yhdestä aiheesta.

Tässä projektissa käytettyä riskianalyysi metodia pidän sopivana tämän kaltaisille projekteille. Tällä tavalla on helppo etsiä uhat, jotka aiheuttavat vaarallisia tapahtumia sekä helppoa pohtia niille mahdollisia ehkäiseviä toimintoja. Rusettimalliseen riskianalyysiin voidaan yhdistää muitakin riskianalyysejä tarvittaessa.

Diplomityö tehtiin siitä syystä, kun yliopisto alkaa antamaan tietyille ulkopuolisille tahoille oikeuden käyttää tislusautomaatiojärjestelmää ja todennäköistä on, että sitä käytetään etäyhteyden yli opetus tai tutkimus käytössä. Tästä syystä tutkittiin millaisia uhkia ja tapaturma vaaroja etäyhteyden yli prosessin käyttöön liittyy tietoturvan kannalta sekä fyysisen prosessiympäristön kannalta ja miten niitä pystyttäisiin ennaltaehkäisemään tai estämään. Riskien ja uhkien analysointiin tässä työssä käytettiin kätevää rusettimallista riskianalyysi tapaa, jolla tunnistettiin tapahtuma, joka aiheutuu monista erilaisista uhista ja millaisia seurauksia tapahtumalla on, jos se tapahtuu. Rusettimalliin laitettiin myös ennaltaehkäiseviä toimintoja tapahtumalle tiettyä uhkaa kohden sekä toimintoja, joilla tapahtuman seurauksia pystyttäisiin lieventämään.

Tässä dokumentissa esitettyjen turvallisuutta parantavien ehdotusten käyttämisestä ja toteuttamisesta päättää tislusautomaatiojärjestelmästä vastuussa oleva henkilö.

## LÄHTEET

- [1] Craig, P. A. & Brooks, C. J. (2022) 'Secure ICS Architecture', in *Practical Industrial Cybersecurity*. United States: John Wiley & Sons, Incorporated. p.
- [2] Ahonen, P. et al. (2021) *Automaation tietoturva: kriittisen tuotannon turvaaminen*. 1. painos. Helsinki: Suomen automaatioseura ry.
- [3] Turvallisuus- ja kemikaalivirasto. (2021) *Turva-automaatio prosessiteollisuudessa*.
- [4] Syrjä, K. (2021) *Turvallisuuden eheystason vaikutus turva-automaatio-sovelluksen arkkitehtuuriin*.
- [5] Renesas (2022). *Functional safety in industrial automation*.
- [6] Kattilakoski, E. Pokela, V. Tuikka, N. (2020) *Automaatioverkkojen tietoturva*.
- [7] F-Secure. (2022) *Mikä on palomuuuri*.
- [8] Rönni, R. (2022) *Nykyaikaiset palomuuritekniikat*.
- [9] Suominen, A. (2019) *Toiminnallinen turvallisuus prosessiteollisuudessa*.
- [10] Turvallisuus- ja kemikaalivirasto. (2016) *Prosessiturvallisuus ja sen mittaaminen*.
- [11] SFS-EN 61511-1:2005. Toiminnallinen turvallisuus. (2017) *Turva-automaatiojärjestelmät prosessiteollisuussektorille. Osa 1: Rakenne, määritelmät, järjestelmän, laitteiston ja sovellusohjelmoinnin vaatimukset*.
- [12] Subagyo, E. et al. (2021) Risk assessment using bowtie analysis: A case study at gas exploration industry PT XYZ Gresik East Java Indonesia. *Process safety progress*. [Online] 40 (2).
- [13] Abdo, H. et al. (2018) A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis. *Computers & security*. [Online] 72175–195.
- [14] Ryynänen, M. (2015) *Turvallisuuden suunnittelu ketterässä järjestelmäkehityksessä*.
- [15] Wideł, W. et al. (2019) Beyond 2014: Formal Methods for Attack Tree--based Security Modeling. *ACM computing surveys*. [Online] 52 (4), 1–36.
- [16] Seppälä, J. Tampereen yliopisto AUT.440 Automaation turvallisuus, kurssimateriaali kevät-2022.
- [17] Mazur, D. C. et al. (2016) Defining the Industrial Demilitarized Zone and Its Benefits for Mining Applications. *IEEE transactions on industry applications*. [Online] 52 (3), 2731–2736.
- [18] Paakanen, M. (2012) Tietokoneen etähallinta yritys- ja kotikäytössä.

- [19] Rantanen, L. (2013) *Kehittyneet salausmenetelmät*. Tampereen ammattikorkeakoulu.
- [20] Suomen automaatioseura RY. (2010) Teollisuusautomaation tietoturva: *Verkotumisen riskit ja niiden hallinta*.
- [21] Klusaité, L. (2020) Mikä on palomuuuri.
- [22] SFS-EN 61508-0:2011 Sähköisten/Elektronisten/Ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. (2011) *Osa 0: Toiminnallinen turvallisuus ja IEC 61508*.
- [23] Virtanen, A. (2015) *Monikäyttöisen oppimisympäristön riskinarviointi ja kehitysuosituks*.
- [24] Anon (2012) *Guidelines for engineering design for process safety*. 2nd ed. New York, N.Y: Center for Chemical Process Safety.
- [25] Khan, F. et al. (2015) Methods and models in process safety and risk management: Past, present and future. *Process safety and environmental protection*. [Online] 98116–147.
- [26] Mannan, S. (2014) *Lees' process safety essentials : hazard identification, assessment and control*. First edition. Oxford, UK: Butterworth-Heinemann.
- [27] Stouffer, K. et al. (2011) 'GUIDE to industrial control systems (ICS) security', in *The Stuxnet Computer Worm and Industrial Control System Security*. pp. 11–158.
- [28] Knapp, E. D. & Langill, J. (2014) *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*.
- [29] National Cyber Security Division. (2011) *Configuring and managing remote access for industrial control systems*.
- [30] Ceragioli, L. et al. (2022) Can my firewall system enforce this policy? *Computers & security*. [Online] 117102683–.
- [31] Salah, K. et al. (2012) Performance Modeling and Analysis of Network Firewalls. *IEEE eTransactions on network and service management*. [Online] 9 (1), 12–21.
- [32] Soewito, B. & Andhika, C. E. (2019) 'Next Generation Firewall for Improving Security in Company and IoT Network', in *2019 International Seminar on Intelligent Technology and Its Applications (ISITIA)*. [Online]. 2019 Piscataway: IEEE. pp. 205–209.
- [33] Anon (2018) *Bow ties in risk management : a concept book for process safety*. Hoboken, NJ: John Wiley & Sons, Inc.
- [34] Anon (2016) *Guidelines for implementing process safety management*. Second edition. Hoboken, New Jersey: Wiley.
- [35] Khān, F. et al. (2022) *Methods to assess and manage process safety in digitalized process system*. Faişal Khān et al. (eds.). Cambridge, Massachusetts: Elsevier.

- [36] Gonzalez, D. et al. (2019) 'Architectural Security Weaknesses in Industrial Control Systems (ICS) an Empirical Study Based on Disclosed Software Vulnerabilities', in *2019 IEEE International Conference on Software Architecture (ICSA)*. [Online]. 2019 IEEE. pp. 31–40.
- [37] Zhou, C. et al. (2021) A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems. *Proceedings of the IEEE*. [Online] 109 (4), 517–541.
- [38] Mantravadi, S. & Møller, C. (2019) 'An overview of next-generation manufacturing execution systems: How important is MES for industry 4.0?', in *Procedia Manufacturing*. [Online]. 2019 pp. 588–595.
- [39] Flaus, J.-M. (2019) 'Methods and Tools to Secure ICS', in *Cybersecurity of Industrial Systems*. [Online]. United States: John Wiley & Sons. pp. 1–1.
- [40] Manninen, J. (2022) *IT and OT cybersecurity practises for Digirail*.
- [41] Bogen, C. (2019) Bridging the Gap Between IT And OT Cybersecurity. *Transmission & Distribution World*.
- [42] Tampereen Yliopisto kurssi materiaali ASE-2170 Automaatiojärjestelmät ja -suunnittelu. AUT.230-2022-2023-1 Ohjaus- ja automaatiojärjestelmät 2023.
- [43] Tampereen Yliopisto kurssi materiaali AUT.440 Automaation turvallisuus aloitus luento. AUT.440-2022-2023-1 Automaation turvallisuus 2023.
- [44] Tampereen Yliopisto kurssi materiaali AUT.410-2021-2022-1 Tietoverkkopohjainen automaatio Johdanto kurssiin. AUT.410-2021-2022-1 Tietoverkkopohjainen automaatio 2022.
- [45] Carlson, J. et al. (2021) Using Bow Tie Risk Modeling for Industrial Cybersecurity.
- [46] SFS-EN 62264:2013 Enterprise-control system integration. (2013) IEC 62264.
- [47] Hartpence, B. (2011) Packet guide to routing and switching. 1st edition. Beijing ;: O'Reilly Media.