SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

AUTOMAATIOJÄRJESTELMÄN TASOT JA KYBERTURVALLISUUS

TEKIJÄ: Markus Pitkänen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Sähkötekniikan tutkinto-ohjelma	
Työn tekijä(t) Markus Pitkänen	
Työn nimi Automaatiojärjestelmän tasot ja kyberturvallisuus	
Päiväys 9.8.2018	Sivumäärä/Liitteet 33/13
Ohjaaja(t) lehtori Pasi Lepistö, lehtori Jari Ijäs	
Toimeksiantaja/Yhteistyökumppani(t) Honeywell Oy, Jari Hämäläinen, pääsuunnittelija	

Tiivistelmä

Opinnäytetyön tavoitteena oli avata IEC 62443-standardia ja tehdä selkokielinen selitys siitä, miksi automaatiojärjestelmän rakenteeseen tehdään tietyt tasot sekä mikä kunkin tason tehtävä on. Lisäksi tavoitteena oli osoittaa, kuinka rakenteen ja tasojen toteutus tapahtuu käytännössä. Tarve opinnäytetyölle syntyi, kun Honeywell Oy tarvitsi lisää tietoa aiheesta dokumentoituna.

Opinnäytetyö oli pääasiassa tutkimuksellista työtä. Työn päälähteenä on käytetty IEC 62443-standardisarjaa, mutta myös muuta kirjallisuutta sekä artikkeleita ja raportteja on hyödynnetty tiedon lähteenä. Työn alussa tuotiin esille automaatiojärjestelmien kyberturvallisuusongelmia, koska pääsyy järjestelmän osiointiin on sen luoma turvallisuus kyberuhkia vastaan. Teoriaosuudessa tutustuttiin IEC 62443-standardisarjaan ja käytiin läpi järjestelmän rakenteen sekä tietoturvavyöhykkeiden muodostuminen standardin mukaisesti. Työvaiheessa osoitettiin, kuinka standardin mukainen järjestelmän rakenne ja vyöhykkeet toteutuisivat käytännössä. Työn pohjana käytettiin Honeywell Oy:n automaatiojärjestelmän rakennetta.

Lopputuloksena saatiin kattavasti tietoa automaatiojärjestelmän rakenteen muodostumisen syistä, ja lisäksi rakenteen muodostamiseen käytettyjä menetelmiä havainnollistettiin käytännön esimerkillä. Tätä työtä voidaan käyttää jatkossa pohjana muille dokumenteille, joita Honeywell Oy tarvitsee aiheesta.

Avainsanat
ISA99, IEC 62443, Automaatio, Kyberturvallisuus

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Electrical Engineering			
Author(s) Markus Pitkänen			
Title of Thesis Levels and Cybersecurity of an Automation System			
Date	9 August 2018	Pages/Appendices	33/13
Supervisor(s) Mr. Pasi Lepistö, Senior Lecturer, Mr. Jari Ijäs, Senior Lecturer			
Client Organisation /Partners Honeywell Oy, Jari Hämäläinen, Lead engineer			

Abstract

The aim of this thesis was to study the structure of an automation system according to the IEC 62443 standard series and the reasons why the structure is done in a certain way. In addition, the aim was to demonstrate how the structure and levels are implemented in practice. The need for this thesis originated because of Honeywell Oy's need for more information on the subject in a documented form.

The thesis was mainly research work. The main source for the thesis was the IEC 62443 standard series, but other literature, articles and reports were also used as a source of information. At the beginning of the thesis, cybersecurity problems of automation systems were highlighted, because the main reason for segmenting the system is the cybersecurity it creates. The theoretical part focused on the structure of an automation system and the formation of security zones and conduits based on the IEC 62443 standard series. In the work phase a real-world example on implementing the zone & conduit strategy was presented. The work was based on the structure of Honeywell Oy's automation system.

As a result, the thesis produced a comprehensive guide on the structure of an automation system. In addition, the methods for creating the structure of an automation system were illustrated by a practical example. The thesis can be used in the future as a basis for other documents that Honeywell Oy needs on the subject.

Keywords
ISA99, IEC 62443, Automation, Cybersecurity

ESIPUHE

Kiitän Honeywell Oy:tä kiinnostavasta opinnäytetyöaiheesta. Opin työn aikana paljon automaatiojärjestelmän rakenteesta sekä sen kyberturvallisuudesta. Haluan kiittää opinnäytetyön ohjaavia opettajia lehtori Jari Ijästä ja lehtori Pasi Lepistöä sekä Honeywell Oy:n Jari Hämäläistä saadusta ohjauksesta. Haluan kiittää myös Honeywell Oy:n Jorma Tyrväistä saaduista neuvoista ja ohjeista.

Standardien lainaukset on tehty Suomen Standardisoimisliitto SFS ry:n luvalla.

Varkaudessa 8.8.2018
Markus Pitkänen

SISÄLTÖ

1 JOHDANTO

Opinnäytetyö sai alkunsa, kun Honeywell Oy tarvitsi lisää tietoa dokumentoituna siitä, miksi automaatiojärjestelmän rakenne on toteutettu tietyllä tavalla. Opinnäytetyön tavoitteena oli avata IEC 62443-standardia ja tehdä selkokielinen selitys siitä, miksi automaatiojärjestelmän rakenteeseen tehdään tietyt tasot sekä mikä kunkin tason tehtävä on. Opinnäytetyö keskittyy pääasiassa standardin osioihin 62443-1-1, 62443-2-1 ja 62443-3-3, sillä ne käsittelevät rakenteeseen liittyviä asioita.

Työssä käydään ensin läpi automaatiojärjestelmien kyberturvallisuushaasteita, koska järjestelmän rakenteen segmentointi johtuu pääasiallisesti kyberturvallisuudesta. Tämän jälkeen käydään läpi IEC 62443-standardisarjaa yleisesti sekä järjestelmän rakenteen muodostumista standardin mukaan. Myös järjestelmän fyysiseen suojaukseen otetaan kantaa, sillä se on tärkeä osa järjestelmän suojausta. Lopuksi osoitetaan, miten järjestelmän segmentointi tasoihin ja vyöhykkeisiin tapahtuisi käytännössä käyttäen pohjana Honeywell Oy:n järjestelmän rakennetta.

Työtä on jatkossa tarkoitus käyttää pohjana muille mahdollisille dokumenteille, joita Honeywell Oy tarvitsee aiheesta. Työstä jalostettuja dokumentteja on tarkoitus käyttää, kun perustellaan automaatiojärjestelmän rakenteen muodostumiseen käytettyjä ratkaisuita.

1.1 Opinnäytetyössä käytetyt lyhenteet ja määritelmät

DMZ	Demilitarized zone
HMI	Human Machine Interface
HPS	Honeywell Process Solutions
ICS	Industrial Control System
IEC	International Electrotechnical Comission
IIoT	Industrial Internet of Things
IP	Internet Protocol
ISA	Internal Society for Automation
IT	Information Technology
NTP	Network Time Protocol
OSI	Open Systems Interconnection
PCN	Process Control Network
RDP	Remote Desktop Protocol

2 HONEYWELL OY

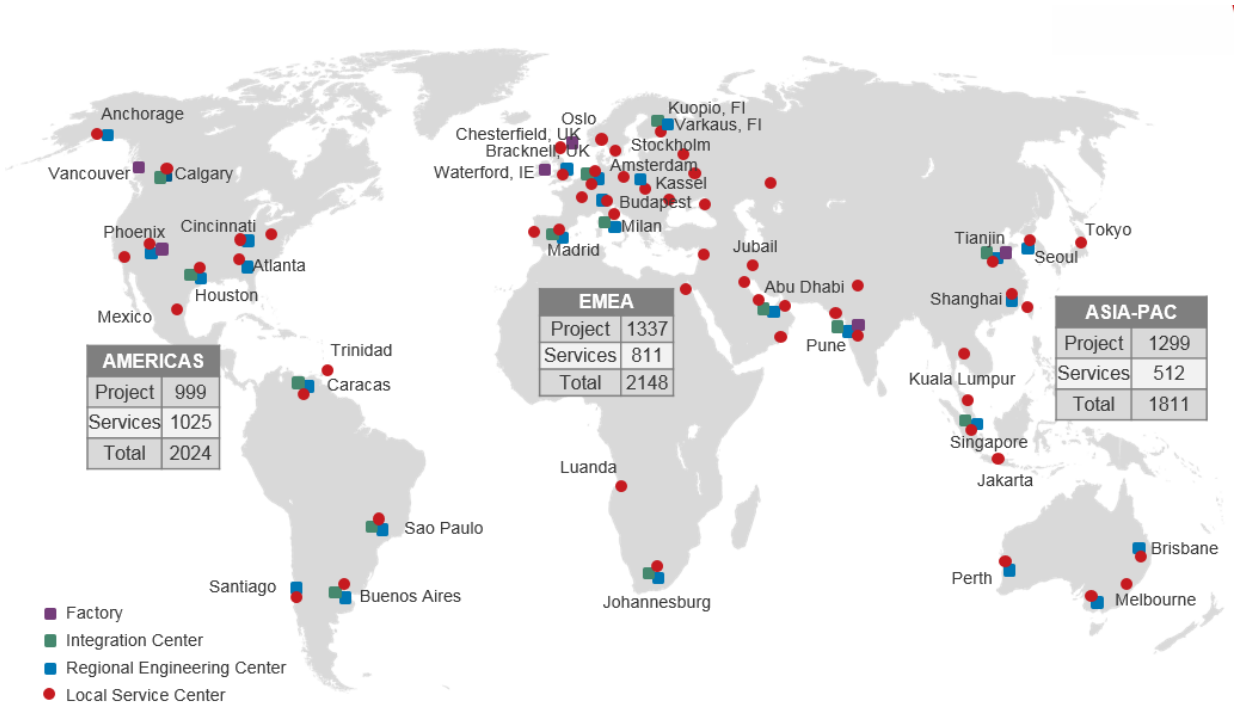
Honeywell Process Solutions (HPS) eli Honeywellin toimiala, joka vastaa automaatiojärjestelmistä sijaitsee Suomessa Varkaudessa sekä Kuopiossa. Kuvassa yksi on Kuopion toimipiste ja kuvassa kaksi on Varkauden toimipiste.

Kuva 1. Honeywell Oy Kuopion toimipiste. (Pitkänen, 2018)

Automaatiojärjestelmät kootaan ja testataan Varkauden toimipisteellä, josta ne lähtevät asiakkaille. Varkaudessa sijaitsee myös tuotemarkkinointi, tuotetuki sekä koulutustoiminnot. Kuopion toimipisteellä sijaitsee tuotekehitystä, projektiliiketoimintaa sekä palveluliiketoimintaa.

Kuva 2. Honeywell Oy Varkauden toimipiste. (Pitkänen, 2018)

Varkauden ja Kuopion toimipisteiden lisäksi HPS:n toimipisteitä on ympäri maailmaa. Kuvassa kolme on kuvattu kaikki HPS:n toimipisteet.



Kuva 3. Honeywell Process solutions toimipisteet (Honeywell Oy, 2018).

Honeywell toimii automaation lisäksi myös mm. ilmailun, koti- ja rakennusteknologian sekä turvallisuus- ja tuottavuusratkaisuiden aloilla. Liiketoimintoja, jotka sijaitsevat Suomessa automaatioratkaisuiden lisäksi on mm. kiinteistöratkaisut, muut teollisuusratkaisut, hälytysjärjestelmät ja turvajärjestelmät. Vuonna 2017 Honeywellin liikevaihto oli n. 40,5 miljardia Yhdysvaltain dollaria.

3 AUTOMAATIOJÄRJESTELMIEN KYBERTURVALLISUUS

Monesti termejä ”kyberturvallisuus” ja ”tietoturvallisuus” käytetään kuin synonyymejä, vaikka termit tarkoittavat eri asioita. Kyberturvallisuus on laajempi käsite, kuin tietoturvallisuus. ”Tietoturvallisuus”-käsitteellä tarkoitetaan tiedon suojaamista. Kyberturvallisuudella tarkoitetaan tiedon suojaamisen lisäksi datan suojaamista, verkkojen kautta tehtävien hyökkäyksien estämistä sekä tietojärjestelmien varassa toimivien rakenteiden suojaamista. (Buchy, 2016) Tässä työssä keskitytään automaatiojärjestelmien kyberturvallisuuteen, eikä pelkästään tietoturvallisuuteen.

3.1 Haasteet

Ennen automaatiojärjestelmät eivät olleet yhteydessä internettiin tai tehtaan toimistoverkkoon. Laitteet olivat eristettynä omassa fyysisessä tehtaan osassa ja erotettuna yleisistä tietokoneverkoista. Täten tehtaiden tuli panostaa eniten järjestelmien fyysiseen suojaukseen kuten kulunvalvontaan varmistaakseen, että laitteisiin pääsy oli vain siihen sallituilla henkilöillä. (Obregon, 2014, s. 2)
Nykyään laitteissa Ethernet-tekniikan käyttö on yleistynyt ja myös järjestelmän toimittajat haluavat etäyhteyksiä laitteistoihin, joten järjestelmiä joudutaan kytkemään internettiin. Järjestelmät alkavatkin

muistuttaa pikkuhiljaa Information Technology (IT)-järjestelmiä. Tämän takia joudutaankin keskittymään myös kyberturvallisuuteen, eikä pelkkä fyysinen suojaus enää riitä.

Kun automaatiojärjestelmät alkavat muistuttaa entistä enemmän IT-järjestelmiä täytyy huomioida, että ne eivät kuitenkaan käyttäydy täysin samoin kuin IT-järjestelmät kyberuhan uhatessa. Mikäli IT-järjestelmässä on tietomurto tai järjestelmään hyökätään, hyökkääjä saa haltuunsa yleensä henkilötietoja tai luottokorttitietoja yms. rahan arvoista tietoa. Jos Industrial Control System (ICS)-järjestelmään hyökätään vaarassa voi olla jopa ihmishenkiä, kun ohjausta muutetaan siten että se on vaaraksi. Yritys voi myös kokea suuria tappioita, mikäli koko tuotantolaitos pysähtyy. (Stouffer;Pillitteri;Lightman;Abrams;& Hahn, 2015)

Puhtaasti IT-puolen ratkaisut eivät välttämättä käy suoraan automaatiopuolelle. Esimerkiksi normaalin virustorjunta-ohjelman asennus tietokoneelle jolla ohjataan prosessilaitteistoa, saattaa estää kommunikoinnin prosessin ohjaimelle ja täten tehdä laitteen operoimisen mahdottomaksi. Kun virustorjuntaohjelmisto asennetaan koneelle, täytyy varmistaa, että se varmasti käy kyseiselle laitteelle. Automaation laitteita ei voi kohdella kuten normaaleita toimistotietokoneita. (Byres, The Industrial Cybersecurity Problem, 2013)

Suuri osa nykyaikaisista järjestelmistä käyttää esimerkiksi Windows-pohjaisia ratkaisuita, joihin täytyy asentaa tietoturvapäivityksiä. Automaatiojärjestelmän täytyy olla toiminnassa lähes jatkuvasti, mikä vaikeuttaa päivitysten asentamista. Lisäksi päivitykset täytyy tarkastaa toimiviksi laitteissa ennen niiden käyttöönottoa, että ne eivät vahingossa estä laitteiden toimintaa halutulla tavalla. Tämä hidastaa vielä entisestään laitteiston päivitystä. Vaikka koneet saataisiin päivitettyä, ne päivitetään kuitenkin lähes aina jäljessä verrattuna peruskäytössä oleviin tietokoneisiin. (Homeland Security, 2016)

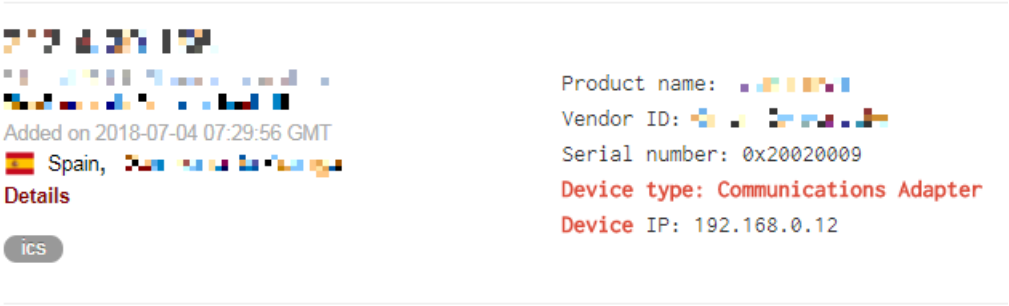
Myös automaatiossa käytettävät protokollat kuten Modbus TCP tai EtherNet/IP eivät ole salattuja, vaan kommunikointi näkyy suoraan datapaketeista, jos niitä tutkii tarkemmin. Mikäli joku osaava henkilö pääsee käsiksi dataan, hän pystyy muokkaamaan ja lukemaan sitä melko vapaasti. Pahimmassa tapauksessa tunkeutuja manipuloi dataa niin, että valvomosta katsottuna kaikki näyttää normaalilta, vaikka tosiasiassa jotain kriittistä on jo tapahtumassa. Protokollissa ei myöskään ole minkäänlaista käyttäjän todennusta. (Ackerman, 2017)

Heikkojen protokollien lisäksi logiikat ja kontrollerit ovat myös huonoja puolustautumaan itse hyökkäyksiä vastaan, koska esimerkiksi virustorjuntaohjelmistoa tai ohjelmistopohjaista palomuuria ei pysty asentamaan logiikkaan, kuten esimerkiksi normaalille Windows-pohjaiselle tietokoneelle pystyy. (Mackenzie, 2012)

On olemassa automaatiojärjestelmiä, jotka on suunniteltu tai toteutettu kyberturvallisuuden kannalta huonosti. Turvallisuudesta on voitu tinkiä koska toisella tapaa asian teko on ollut helpompaa, nopeampaa tai se on säästänyt rahaa. Esimerkkinä siitä, miten monta laitetta tälläkin hetkellä on välttävästi asennettuna, tutkitaan tällä hetkellä internetissä olevia laitteita apuna käyttäen Shodan-sivustoa.

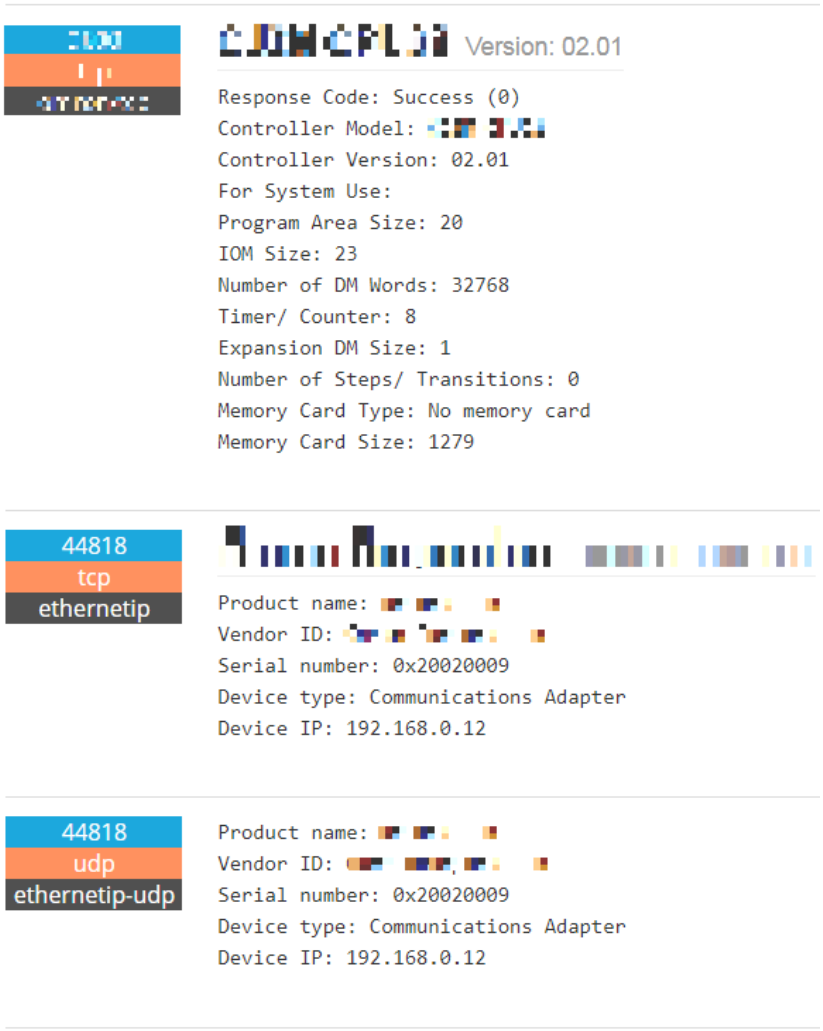
Shodan on Googlen tapainen hakukone, mutta nettisivujen sijaan se etsii laitteita, jotka ovat yhdistetty internettiin. Kun suodatetaan hakua ja tutkitaan laitteita, jotka löytyvät esimerkiksi porttien TCP 102 (Siemensin logiikka (Siemens, 2007)), TCP 502 (Modbus TCP (Speed Guide, 2014)) ja UDP/TCP 44818 (EtherNet/IP (Speed Guide, 2018)) alta, löysi skanneri yhteensä kymmeniä tuhansia laitteita, jotka kuuntelevat tällä hetkellä kyseisiä portteja. Eli siis laitteita, jotka ovat suorassa yhteydessä internettiin. Toki kaikki näistä laitteista ei ohjaa kriittistä prosessia tai ole tehtaalla käytössä, mutta osa luultavastikin on.

Tarkastellaan tarkemmin Shodanin löytämiä laitteita, jotka kuuntelevat EtherNet/IP protokollan portia. Kuvassa 4 on esimerkki löydetystä logiikasta. Kuvasta on sumennettu julkinen Internet Protocol (IP)-osoite sekä laitteen tarkemmat tiedot.



Kuva 4. Logiikka (Shodan, 2018)

Laitteesta nähdään tarkat tiedot, kuten sen sarjanumero, versionumero, malli ja portit joita laite kuuntelee. Laite kuuntelee mm. TCP ja UDP 44818 portteja (Kuva 5). Kuvasta on sensuroitu tiedot, joilla laitteen valmistaja tai malli voitaisiin tunnistaa. Mahdollinen hyökkääjä pystyisi nyt etsimään kyseisen logiikan version 02.01 haavoittuvaisuuksia ja niiden löytyessä käyttämään niitä hyväksi. Mikäli tämä logiikka ohjaa tällä hetkellä jotain prosessia, siihen pääsee aivan liian helposti käsiksi kolmannen osapuolen henkilöt.



Kuva 5. Laitteen tarkemmat tiedot (Shodan, 2018)

Väärin kytkettyjen tai konfiguroitujen laitteiden suuri määrä osoittaa jo, miten tärkeää on suojata sekä konfiguroida laitteistot oikein. Missään tapauksessa ei haluta, että jonkin tehtaan logiikat tai muut säätölaitteet ovat suoraan yhteydessä internettiin ja täten alttiita hyökkäyksille tai väärinkäytölle. Mikäli laitteisto on suoraan yhteydessä internettiin, ne huomataan hyvin pian varsinkin, kun Shodanin kaltaisia työkaluja on olemassa.

3.2 Vastatoimenpiteet

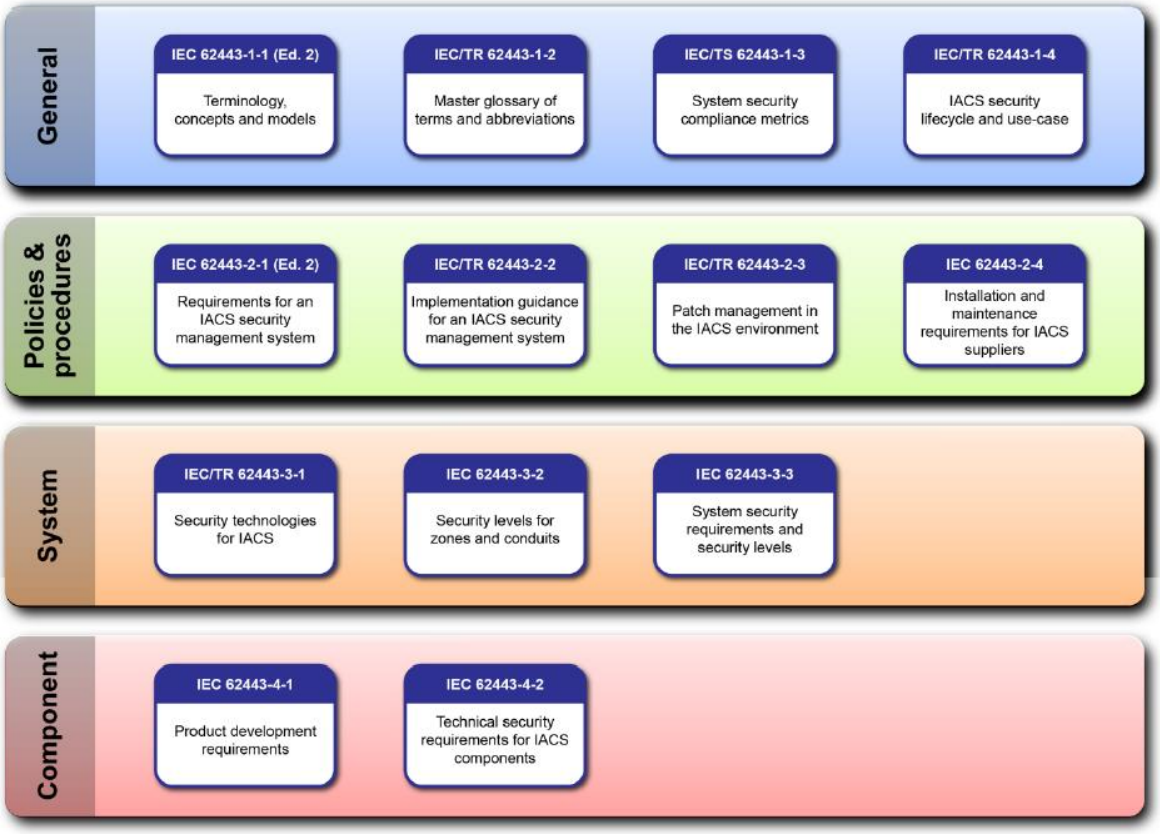
Järjestelmä täytyy suunnitella jo alusta asti kyberturvallisuus huomioon ottaen. Yksi tärkeä asia on järjestelmän rakenteen suunnittelu oikein, jotta mahdolliset tunkeutujat tai haittaohjelmat eivät pääse käsiksi ainakaan automaatioon asti. Tarkoitus on pysäyttää tunkeutujat jo aikaisemmin, tai havaita tunkeutuminen ennen kuin mitään vahinkoa ehtii tapahtua. Rakenne tulee kerrostaa siten, että kaikkein riskialttiimpia laitteita suojataan eniten, eikä automaation laitteet saa olla suoraan yhteydessä julkiseen verkkoon. Automaatiojärjestelmän kyberturvallisuutta koskien on kehitetty standardisarja International Electrotechnical Comission (IEC) 62443. Standardi suosittelee verkon segmentointia tärkeänä osana automaatiojärjestelmän tietoturvallisuutta.

”Verkon segmentointiin kuuluu tärkeimpien teollisuusautomaatio- ja ohjausjärjestelmän suojattavien kohteiden erottaminen vyöhykkeisiin, joilla on yhteiset tietoturvatasot, tietoturvariskien hallitsemiseksi ja halutun tietoturvan tavoitetason saavuttamiseksi vyöhykkeelle. Verkon segmentointi on tärkeä tietoturvallisuusvastatoimenpide, jota käytetään yhdessä muiden puolustuskerrosten kanssa pienentämään teollisuusautomaatio- ja ohjausjärjestelmään mahdollisesti liittyvää riskiä.” (SFS-IEC 62443-2-1, 2013, s. 83)

Yleisenä ideana on, että järjestelmä jaetaan tasoihin laitteiden toimintojen perusteella. Tämän jälkeen laitteet jaotellaan tietoturvavyöhykkeisiin sekä niiden välisiin tietoväyliin laitteiden tietoturvakyvyn, halutun tietoturvatason sekä tietoturvan murtumisesta aiheutuvien riskien perusteella.

3.3 IEC 62443

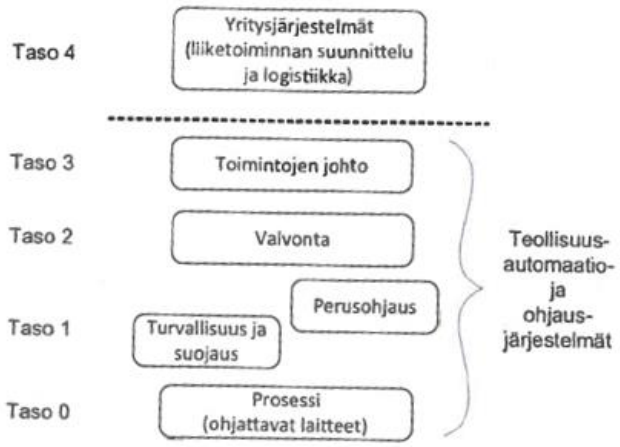
IEC 62443 (ennen ISA (Internal Society for Automation) 99 - standardit) on joukko standardeja ja teknisiä raportteja, jotka koskevat automaatiojärjestelmien kyberturvallisuutta. Standardit jaotellaan osioihin Yleistä (General), Politiikat ja menettelyt (Policies & Procedures), Järjestelmä (System) ja Komponentti (Component). Kuvassa 6 standardiryhmät on kuvattu tarkemmin. Tässä opinnäytetyössä keskitytään osioihin 62443-1-1, 62443-2-1 ja 62443-3-3, sillä ne koskevat järjestelmän rakennetta ja segmentointia.



Kuva 6. IEC 62443-standardisarja (IEC 62443-3-3, 2013, s. 13)

4 JÄRJESTELMÄN REFERENSSIMALLLI

Automaatiojärjestelmille on määritelty standardissa IEC 62264-1 referenssimalli, joka kertoo kuinka järjestelmän laitteet tulisi ryhmitellä erilaisiin toiminnallisiin tasoihin laitteiden tehtävän tai aktiviteetin perusteella. Myös IEC 62443-standardisarja käyttää tätä samaa mallia. Referenssimalli antaa hyvän pohjan järjestelmän rakenteelle sekä se helpottaa ymmärtämään järjestelmän tietoturvatarpeita. Tämä referenssimalli on esitetty kuvassa 7.



Kuva 7. Referenssimalli (IEC/TS 62443-1-1:fi, 2012, s. 58)

Referenssimallin tasoista puhuessa eri alan toimijoiden kesken on tärkeää, että niitä ei sekoiteta jonkin muun referenssimallin tasoihin. Esimerkiksi IT-puolella yleisessä käytössä on Open Systems Interconnection (OSI)-malli, joka kuvaa tiedonsiirtoprotokollien toimintaa seitsemällä eri tasolla (kuva 8). Se on määritelty standardissa ISO/IEC 7498-1.

Kuva 8. OSI-malli (Wikimedia, 2005)

OSI-malli on hyvin yleisesti käytössä tietoliikennepuolella, joten se on painunut IT-henkilöille hyvin mieleen. Täten automaatioväen ja IT-väen keskustellessa tasoista, menee nämä kaksi mallia helposti sekaisin.

Verkkolaitteet toimivat OSI-mallin tasolla kaksi tai tasolla kolme. Esimerkiksi kytkimet toimivat yleensä OSI-mallin tasolla kaksi ja reitittimet OSI-mallin tasolla kolme. Täten puhuttaessa tason kaksi laitteistosta, voidaan puhua OSI-mallin tasolla kaksi toimivasta laitteesta tai automaatiojärjestelmän tasolla kaksi olevasta laitteesta. Esimerkiksi OSI-mallin tasolla kaksi toimiva laite voi fyysisesti sijaita automaatiojärjestelmän referenssimallin tasolla kolme. IT-puolen henkilö saattaa silti puhua tason kaksi laitteesta ja automaatiopuolen henkilö tason kolme laitteesta, vaikka kyseessä on sama fyysinen laite, joka sijaitsee automaatiojärjestelmän tasolla kolme.

5 REFERENSSIMALLIN TASOT

Kohdissa 5.1 - 5.6 käydään läpi kuvassa seitsemän esitetyn referenssimallin tasot tarkemmin.

5.1 Taso 4 – ”Yritysjärjestelmät”

Tasolla neljä sijaitsee tehtaan yritysjärjestelmät, eli tehtaan toimistoverkko. Verkko muistuttaa tyypillistä toimistoverkkoa, jollaisia on tavallisissa toimistojärjestelmissä.

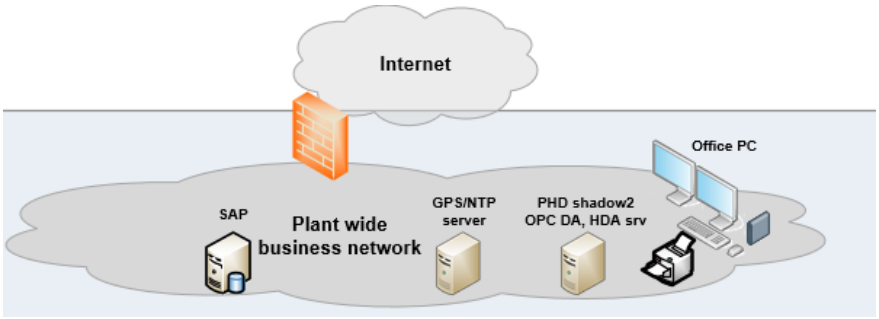
”Tämä taso, jota kuvaillaan liiketoiminnan suunnittelu- ja logistiikkatasoksi standardissa IEC 62264-1, määritellään siten, että se sisältää ne toiminnot, jotka ovat mukana liiketoimintaan liittyvissä aktiviteeteissa, joita tarvitaan valmistusorganisaation johtamiseen. Toimintoihin kuuluvat yrityksenlaajuiset tai alueelliset talousjärjestelmät ja muut yrityksen infrastruktuurikomponentit, kuten tuotannon aikataulutus, toiminnallinen johtaminen ja ylläpidon johtaminen yksittäiselle tehtaalle tai toimipaikalle yrityksessä.” (IEC/TS 62443-1-1:fi, 2012, s. 59)

Tason aktiviteetteihin kuuluu mm. laadunvalvontatiedostojen, prosessissa olevien materiaalien määrää kuvaavien tiedostojen ja kokonaisenergiankulutuksen kerääminen ja ylläpitäminen sekä tehtaan perustuotantosuunnitelman laatiminen. (IEC/TS 62443-1-1:fi, 2012, s. 59 - 60)

Tasolta neljä on pääsy internettiin ja normaaleiden internetpalveluiden kuten sähköpostin käyttömahdollisuus. Tasoa neljä pidetäänkin yleensä kyberuhkien ja automaatiojärjestelmän häiriöiden lähteenä. Tason toiminnot eivät ole automaatiojärjestelmän toiminnan kannalta kriittisiä tai tärkeitä, mutta tason neljä käyttäjät tarvitsevat kuitenkin dataa automaatiojärjestelmästä eli tasoilta 0-3, jotta he voivat esimerkiksi tutkia tuotantolaitoksen tehokkuutta. Tehtaan toimistoverkko (taso 4) tulee erottaa omaksi segmentikseen tehtaan automaatioverkosta (tasot 0 - 3), koska automaatioverkko on kriittinen tehtaan toiminnan kannalta. Tällä tavoin verkkojen segmentointi suojaa automaatiojärjestelmän toimintaa. (Cisco, Rockwell Automation, 2011) Referenssimallissa (kuva 7) on tässä kohtaa myös katkoviiva kuvaamassa erotusta.

Koska tason verkko muistuttaa normaalia toimistoverkkoa ja laitteet ovat lähinnä normaaleja toimistotietokoneita, palvelimia tai tulostimia, liikennöinti laitteiden välillä tapahtuu käyttäen Ethernet-tekniikkaa ja TCP/IP protokollaa, joko langallisesti tai langattomasti. Tämän takia tasoa myös hallinnoi yleensä tuotantolaitoksen IT-organisaatio. IEC 62264-1 antaa tasolle neljä nimen ”yritysjärjestelmät”.

Kuvassa yhdeksän on kuvattu tyypillisiä tason neljä laitteita, kuten toimistokoneita, tulostimia ja erilaisia palvelimia.



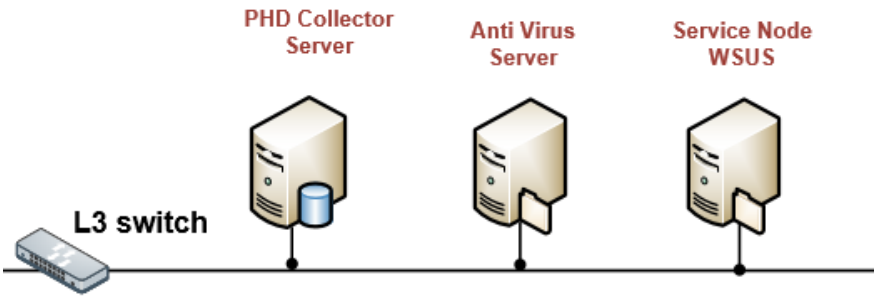
Kuva 9. Tason neljä laitteita (Honeywell Oy, 2018)

5.2 Taso 3 – ”Toimintojen johtaminen”

Taso kolme sisältää toimintoja, jotka liittyvät työnkulun hallintaan sekä luotettavuuden varmistaminen. Tason kolme aktiviteetteihin kuuluu mm. raportointi alueen tuotannosta, tietojen keruu ja ylläpito tuotannosta, varastosta, työvoimasta, raaka-aineista, varaosista ja energiankulutuksesta sekä suunnittelutoimintojen tarvitsemien tietojen kerääminen ja erillinen analyysi. (IEC/TS 62443-1-1:fi, 2012, s. 60)

Tasolla kolme sijaitsee esimerkiksi historiankeruupalvelimet ja erilaiset Windowsin tai virustorjunnan päivitystenjakelupalvelimet. Laitteisto kommunikoi esimerkiksi tason yksi prosessinohjauslaitteille sekä yritystason järjestelmiin tasolle neljä. Tason kolme laitteisto on pääasiassa normaalia tietotekniikkalaitteistoa, ja täten yleensä kommunikoi Ethernet ja TCP/IP tekniikkaa käyttäen. Laitteistoa voi hoitaa IT-taitoja osaavat henkilöt. (Cisco, Rockwell Automation, 2011)
IEC 62443-1-1 antaa tasolle kolme nimen ”toimintojen johtaminen”.

Kuvassa kymmenen on kuvattu tyypillisiä laitteita, jotka sijaitsevat tasolla kolme. PHD Collector-palvelin on historiadatan kerääjä, joka on Honeywell Oy:n tuote. Lisäksi tasolla on mm. virustorjunnan päivitysten ja Windowsin päivitysten jakelijat.



Kuva 10. Tason kolme laitteita (Honeywell Oy, 2018)

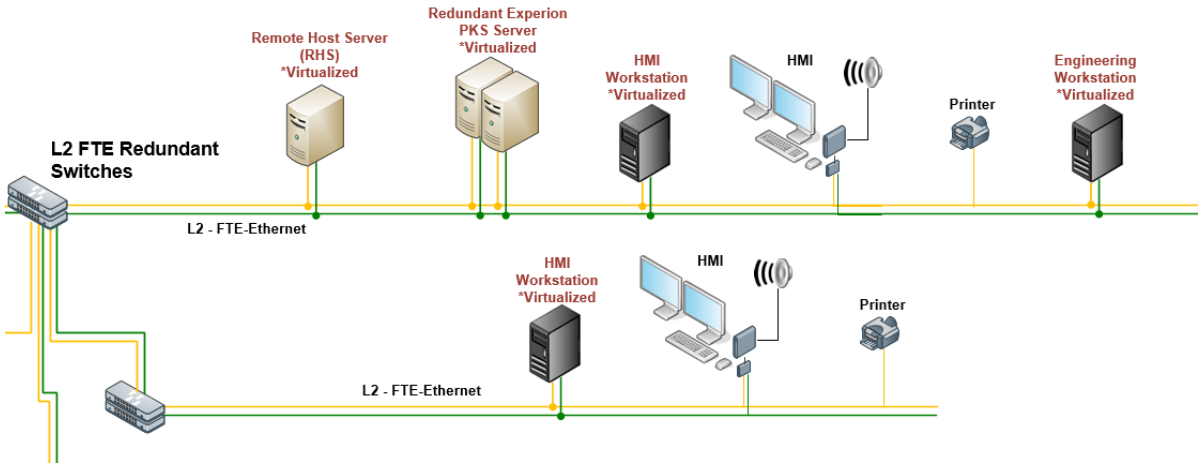
5.3 Taso 2 – ”Valvonta”

Taso kaksi sisältää toimintoja, jotka liittyvät fyysisen prosessin ohjaamiseen ja tarkkailuun. Tason toimintoihin kuuluu mm. operaattorin käyttöliittymä ja siihen liittyvät varoitukset ja valvomotoiminnot. (IEC/TS 62443-1-1:fi, 2012, s. 60)

Tason laitteet kommunikoivat mm. tason yksi prosessinohjauslaitteistolle, ja jakavat dataa ylemmille tasoille mm. historiankeruupalvelimille. Laitteet ovat suurimmaksi osaksi tietokoneita ja erilaisia palvelimia, joten kommunikointi tapahtuu yleensä Ethernet ja TCP/IP tekniikalla. Laitteistoa voi hoitaa IT-taitoja osaavat henkilöt. (Cisco, Rockwell Automation, 2011)

IEC 62264-1 antaa tasolle kaksi nimen ”Valvonta”.

Kuvassa 11 on kuvattu tyypillisiä tason kaksi laitteita, joita ovat mm. Human Machine Interface (HMI)-koneet, sovellusasemat, etäyhteyspalvelimet sekä kokonaista järjestelmää varten olevat palvelimet kuten Honeywell Oy:n Experion PKS-palvelimet.



Kuva 11. Tason kaksi laitteita (Honeywell Oy, 2018)

5.4 Taso 1 – ”Perussäätö”

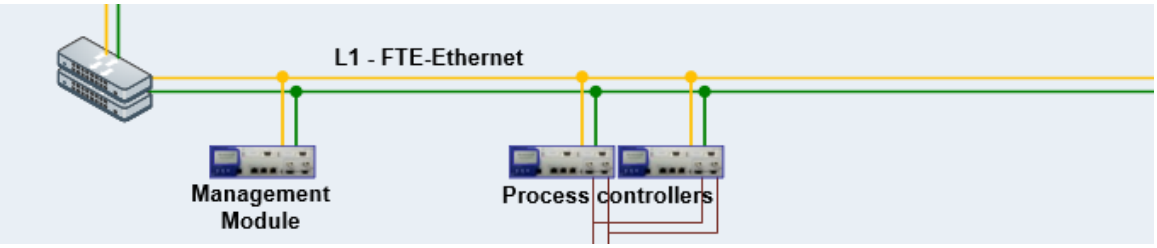
IEC 62264-1 antaa tasolle yksi nimen ”Paikallinen ohjaus tai perusohjaus (perussäätö)”

”Tasoon 1 kuuluvat toiminnot, jotka ovat mukana tunnistamassa fyysistä prosessia ja vaikuttamassa siihen” (IEC/TS 62443-1-1:fi, 2012, s. 61)

Tasolla yksi sijaitsee siis prosessin ohjaus- ja säätölaitteisto. Laitteet ohjaavat prosessia lukemalla dataa tason nolla antureilta ja ohjaamalla tason nolla toimilaitteita luetun datan ja laitteeseen ohjelmoidun ohjelman perusteella. Laite myös monitoroi prosessia ja sen raja-arvoja, jonka perusteella saadaan tason kaksi valvomoihin esimerkiksi hälytykset. (IEC/TS 62443-1-1:fi, 2012, s. 61)

Säätölaitteisto koostuu yleensä ohjelmoitavista logiikoista ja/tai älykkäistä hajautetuista kenttälaitteista. Kommunikointi tapahtuu reaaliajassa. (Cisco, Rockwell Automation, 2011)

Kuvassa 12 on kuvattu tason yksi tyypillistä laitteistoa. Kuvassa on Honeywellillä yleisesti käytössä olevia Field Controller Express ohjaimia, jotka ovat älykkäitä prosessinohjaimia.

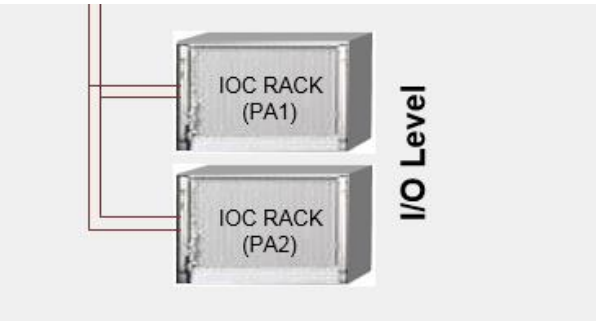


Kuva 12. Tason 1 laitteita (Honeywell Oy, 2018)

5.5 Taso 0 – ”Prosessi”

Tasolla 0 on itse prosessi. Laitteistoon kuuluu erilaisia sensoreita, antureita ja toimilaitteita jotka kytkeytyvät suoraan prosessilaitteistoon. IEC 62264-1 antaa tasolle nolla nimen ”Prosessi”. (IEC/TS 62443-1-1:fi, 2012, s. 61)

Tason nolla laitteet kommunikoivat reaaliajassa pääasiassa tason yksi säätölaitteille. Laitteiston määrä riippuu tehtaan koosta (montako I/O liityntää tarvitaan) ja laitteisto sijaitsee ympäristöllisesti haastavissa paikoissa tehtaalla (kuumuus, kosteus). Laitteistolla on melko pitkä elinikä, eikä laitteita korvata tai vaihdeta kovin usein. Tyypillinen laitteiston elinikä on yli viisi vuotta. Tason nolla laitteisto kommunikoi yleensä tarkoitukseen tehdyillä tai Ethernet-tekniikkaan perustuvilla kenttäväylillä, kuten Modbusilla tai Profinetillä. Pelkkä Ethernet-tekniikka ei täytä laitteiston vaatimia vaatimuksia. (Cisco, Rockwell Automation, 2011) Kuvassa 13 on kuvattu tason I/O laitteistoa.



Kuva 13. Tason nolla laitteita (Honeywell Oy, 2018)

5.6 Taso 3.5 – ”DMZ”

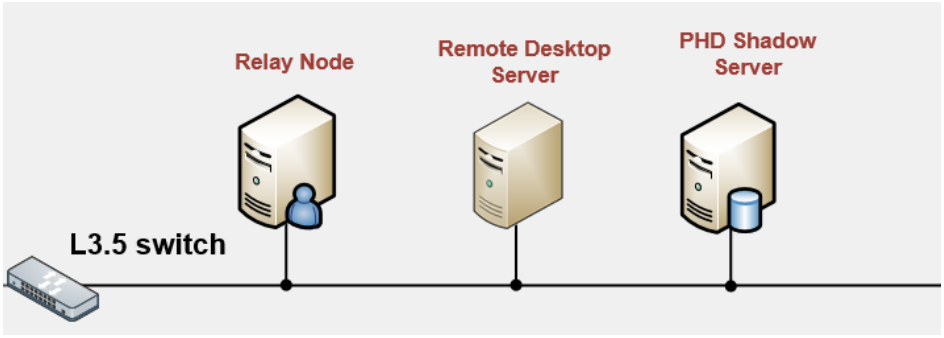
Automaatioverkko (tasot 0-3) on erotettava omaksi verkkosegmentiksi tehtaan toimistoverkosta (taso 4), kuten kohdassa 5.1 mainittiin. Tasojen välillä täytyy kuitenkin kommunikoida, jotta laitteiden toimittajat saavat järjestelmään esimerkiksi etäyhteyksiä ja jotta toimistoverkkoon saadaan sen toimintojen toimimiseen tarvitsema data. Automaatioverkon ja tehtaan verkon välistä kommunikointia varten

tähän väliin muodostetaan yleensä taso 3.5 eli Demilitarized Zone (DMZ). Tasoa ei kuitenkaan ole varsinaisesti merkitty referenssimalliin kuin katkoviivana.

IEC 62443-2-1 suosittelee ottamaan DMZ-tason käyttöön suuren riskin teollisuusautomaatio- ja ohjausjärjestelmissä, sillä se tarjoaa lisämahdollisuuksia riskien pienentämiseen yritysjärjestelmien ja ohjausjärjestelmien välillä tapahtuvassa kommunikoinnissa. (SFS-IEC 62443-2-1, 2013, s. 85)

Tason 3.5 ideana on, että kaikki kommunikointi tuotantolaitoksen verkon ja automaatioverkon välillä päättyy tai alkaa DMZ-tasolta. Minkäänlaista toista kommunikointireittiä tällä välillä ei saa olla. Tasolle sijoitetaan erilaisia palvelimia kuten esimerkiksi historiadata- tai etäyhteyspalvelimia. Jos toimistoverkosta tarvitsee katsoa esimerkiksi prosessin historiadataa, yhdistetään DMZ-tasolla olevalle palvelimelle jolle automaatiojärjestelmässä olevat palvelimet ovat ”työntäneet” datan tarjolle. Täten toimistoverkosta ei ikinä tarvitse ottaa suoria yhteyksiä automaatioon. Tason liikennettä tarkkaillaan ja rajoitetaan palomuurien avulla. (Homeland Security, 2016)

Kuvassa 14 on kuvattu tason 3.5 tyypillisiä laitteita. Honeywell Oy:llä tällä tasolla sijaitsee mm. PHD Shadow-palvelin joka välittää prosessihistoriadatan tehtaan verkkoon, Relay node-palvelin joka välittää Windowsin ja virustorjunnan päivityksiä ja Remote Desktop-palvelin joka on etäyhteyksiä varten.

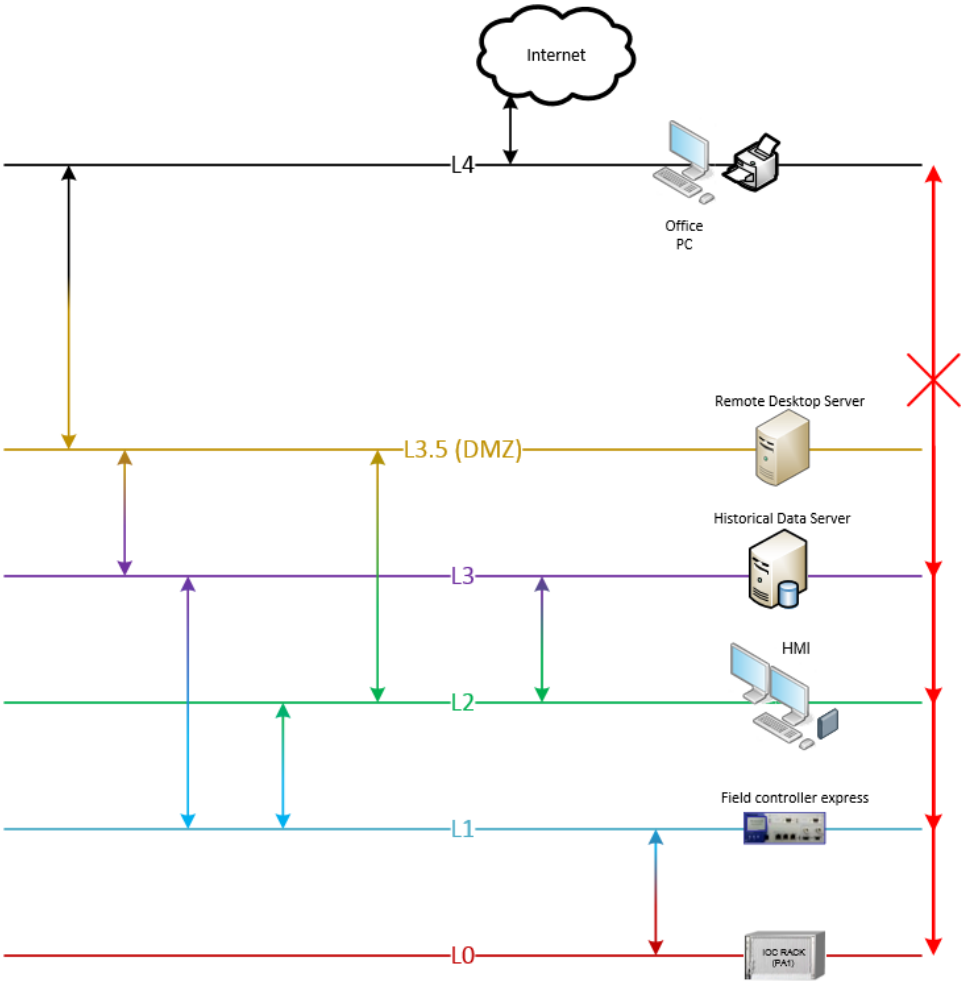


Kuva 14. Tason 3.5 laitteita (Honeywell Oy, 2018)

DMZ-tasosta saatavia hyötyjä on mm. suoraan ohjauslaitteisiin pääsevien henkilöiden lukumäärän minimointi ja täten paremman turvallisuuden tarjoaminen tärkeille teollisuusautomaatio- ja ohjausjärjestelmän laitteille (SFS-IEC 62443-2-1, 2013, s. 85).

Koska ainut kommunikointiväylä tehtaan toimistoverkon ja automaatioverkon välillä on DMZ-taso, voidaan yhteys myös tarvittaessa katkaista. Jos toimistoverkossa havaitaan jokin uhka kuten virus tai tunkeutuja, voidaan yhteys katkaista ja automaatio jatkaa toimintaansa ilman yhteyttä toimistoverkkoon. Kun uhka on saatu poistettua toimistoverkon puolelta, voidaan yhteys automaatioverkkoon jälleen avata. (Suomen Automaatioseura ry, 2010, s. 79)

Kuvassa 15 on esitetty DMZ-tason toiminta, sekä havainnollistettu myös kaikkien tasojen välistä yleistä liikennettä, joka on välttämätöntä laitteiden toiminnan kannalta.



Kuva 15. Tasojen välinen liikenne (Pitkänen, 2018)

6 JÄRJESTELMÄN TIETOTURVAVYÖHYKKEET

Referenssimallin lajittelua osalti hyväksi käyttäen järjestelmä jaetaan tietoturvavyöhykkeisiin. Lajiteltaessa laitteet referenssimallin mukaan, on tietyn vyöhykkeen haluttu tietoturvataso ja laitteiden tietoturvakyky helpompi määritellä, koska samantyyliset laitteet ovat jo valmiiksi samalla ”tasolla”. Tietoturvavyöhykkeistä tulee tyypillisesti yhdenmukaisia järjestelmän fyysisten segmenttien kanssa nykyisten tietoturvaan liittyvien vastatoimenpidetekniikoiden vuoksi (SFS-IEC 62443-2-1, 2013, s. 104).

Tietoturvavyöhykkeiden ideana on ajatella tiettyjen laitteiden tietoturvaa kokonaisena joukkona, eikä vain pelkästään yhden laitteen tietoturvallisuutta. Tietoturvavyöhykkeet helpottavat tietoliikenteen seuraamista ja rajoittamista sekä uhkien havaitsemista ja torjumista. Vyöhykkeet auttavat myös yleisen kyberturvallisuusohjelman teossa. IEC 62443-2-1 asettaakin vaatimukseksi tietoturvavyöhykkeiden perustamisen ja verkon segmentoinnin. (IEC/TS 62443-1-1:fi, 2012; SFS-IEC 62443-2-1, 2013) Taulukossa 1 on esitetty standardin asettamat vaatimukset.

Taulukko 1. Verkon segmentointi: Vaatimukset (SFS-IEC 62443-2-1, 2013, s. 26)

Kuvaus	Vaatimus
4.3.3.4.1 Kehitetään verkon segmentointiarkkitehtuuri	Verkon segmentointiin perustuva vastatoimenpidestrategia, joka käyttää tietoturvavyöhykkeitä, on kehitettävä teollisuusautomaatio- ja ohjausjärjestelmille riskitasosta riippuen.
4.3.3.4.2 Käytetään eristämistä tai segmentointia korkean riskitason teollisuusautomaatio-ja ohjausjärjestelmissä	Korkean riskitason teollisuusautomaatio- ja ohjausjärjestelmä on eristettävä muista vyöhykkeistä, joilla on erilaiset tietoturvatasot tai riskit, tai on käytettävä verkonerotuslaitetta erottamaan se niistä.
4.3.3.4.3 Estetään tarpeeton tietoliikenne verkonerotuslaitteiden avulla	Verkonerotuslaitteiden on estettävä kaikki tarpeeton tietoliikenne kriittisiä ohjauslaitteita sisältävään tietoturvavyöhykkeeseen tai niitä sisältävästä tietoturvavyöhykkeestä.

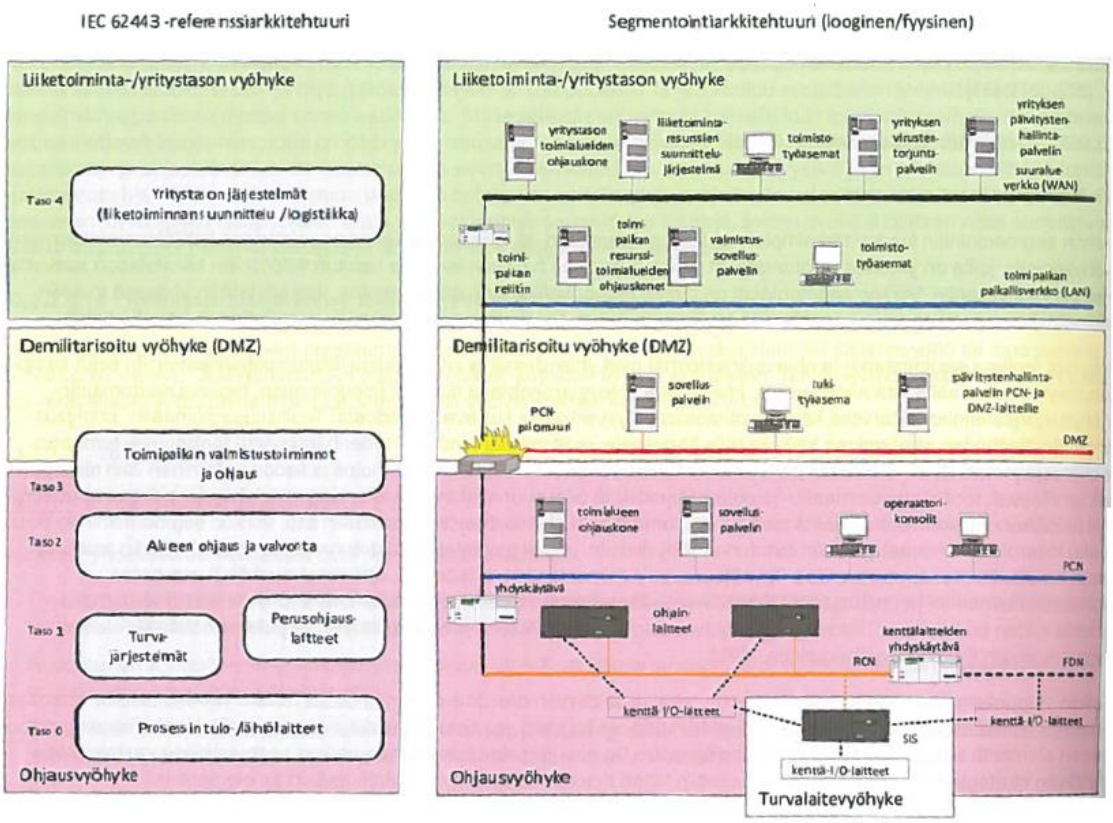
Referenssimallin lajittelun lisäksi vyöhykkeiden perustamiseen käytetään hyödyksi vyöhykkeen sisältämien laitteiden tietoturvakykyä sekä vyöhykkeen sisältämiä riskejä. Vyöhykkeen tietoturvakyvyllä tarkoitetaan sitä, mikä on paras mahdollinen tietoturvataso mihin vyöhykkeen laitteet kykenevät. Esimerkiksi logiikat eivät kykene korkeaan tietoturvatasoon, sillä niissä ei ole käyttäjän autentikointia ja niiden käyttämät protokollat eivät ole suojattuja, kun taas esimerkiksi ”ajan tasalla” oleva Windows-pohjainen tietokone kykenee korkeampaan tietoturvatasoon (Byres, 2014). Vyöhykkeen riskeillä tarkoitetaan sitä, mitä seuraa, jos joku pääsee laitteisiin luvattomasti käsiksi. Riskien arvioinnissa tulisi ottaa huomioon vyöhykkeen tietoturvan vaarantumisen seurauksien lisäksi sen tapahtumisen todennäköisyys.

Vyöhykkeen tietoturvakyvyn sekä riskiarvion perusteella vyöhykkeille määritellään haluttu tietoturvataso. Tietoturvatasoja tulisi olla käytössä minimissään kolme: alhainen, keskinkertainen ja korkea. Tietoturvataso kuvaa siis vyöhykkeen riskiarvioon perustuvaa vastatoimenpidetekniikoilta vaadittavaa tehokkuutta ja laitteiden luontaisia tietoturvaominaisuuksia. Jokaisen organisaation tulee itse määritellä, kuinka vyöhykkeen tietoturvatasoa mitataan. (IEC/TS 62443-1-1:fi, 2012, s. 50) Esimerkiksi vyöhykkeelle, joka sisältää tuotantolaitoksen prosessinohjauslaitteistoa, voitaisiin määritellä korkein haluttu tietoturvataso, sillä laitteisiin liittyy suuri riski ja laitteilla on huonot luontaiset tietoturvaominaisuudet.

Jotta vyöhykkeiden tietoturvatasoa voidaan ylläpitää, jokaisella vyöhykkeellä on kolme tietoturvatasoa: saavutettu tietoturvataso, tavoitteena oleva tietoturvataso sekä tietoturvataso mihin vyöhykkeen laitteet kykenevät. Vyöhykkeen tämänhetkinen saavutettu tietoturvataso riippuu vastatoimenpiteistä, jotka ovat jo käytössä. Tarkoituksena on iteroida vyöhykkeen tämän hetkinen tietoturvataso tavoitteena olevan tietoturvatason tasolle tai korkeammalle. Vyöhykkeen tietoturvatason nostamiseen voidaan käyttää esimerkiksi teknisiä toimenpiteitä, kuten palomuureja ja virustorjuntaohjelmia tai fyysisiä vastatoimenpiteitä kuten lukittuja ovia. (IEC/TS 62443-1-1:fi, 2012)

Jokaiselle luodulle tietoturvavyöhykkeelle tulee määritellä ominaisuuksia, kuten tietoturvapolitiikat, luettelo suojattavista kohteista, pääsyvaatimukset ja valvontamenetelmät, uhat ja haavoittuvuudet, tietoturvan murtumisen seuraukset, valtuutettu teknologia ja muutostenhallintaprosessi (IEC/TS 62443-1-1:fi, 2012, s. 70). Yksi vyöhyke voi myös koostua pelkästään alivyöhykkeistä joissa itse laitteet sijaitsevat. Mikäli vyöhykkeen sisässä on alivyöhykkeitä, alivyöhykkeiden täytyy täyttää kaikki ylemmälle vyöhykkeelle määritellyt vaatimukset. Vyöhykkeillä tulee myös olla selkeä raja mihin vyöhyke loppuu. (IEC/TS 62443-1-1:fi, 2012, s. 66)

Suosituksena on, että perustetaan minimissään kolme tietoturvavyöhykettä: ohjaustason vyöhyke jossa sijaitsee referenssimallin tasot 0-3, DMZ-vyöhyke eli referenssimallin taso 3.5 sekä yritystason vyöhyke eli referenssimallin taso 4 (Collantes & Padilla, 2015, s. 9). Kuvassa 16 on havainnollistettu nämä kolme vyöhykettä sekä referenssimallin tasojen 0-4 sijoittuminen vyöhykkeille. Mikäli yksi fyysinen laite kuitenkin suorittaa monen eri tason tehtäviä tai aktiviteettejä, voidaan sille luoda oma tietoturvavyöhyke, jonka tietoturvapolitiikka on sekoitus näiden vyöhykkeiden politiikkoja (IEC/TS 62443-1-1:fi, 2012 s. 65 - 66).

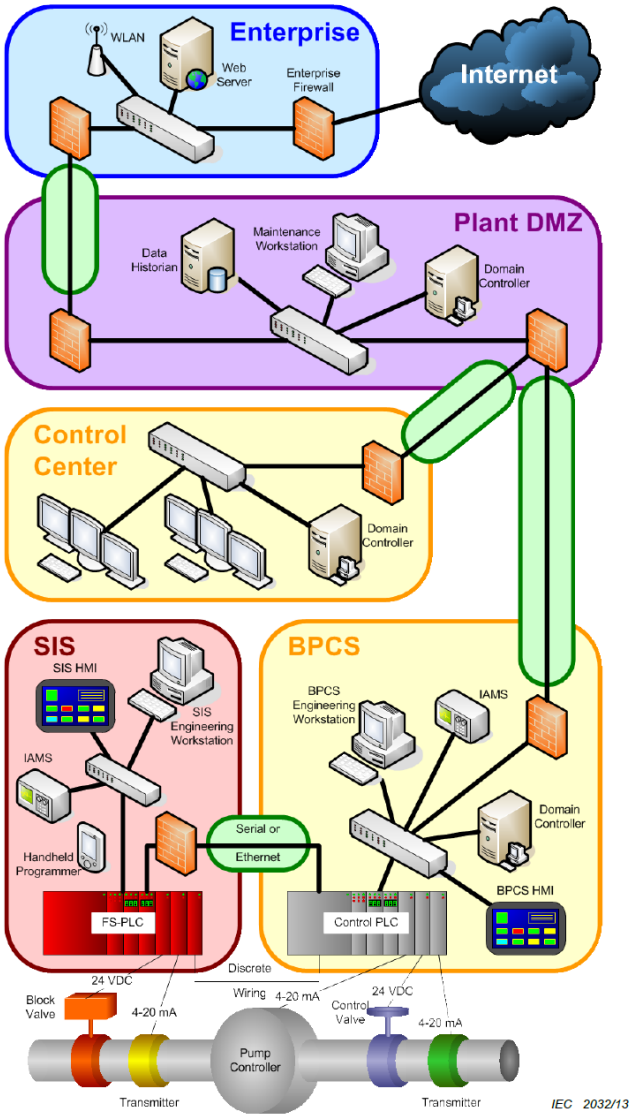


Kuva 16. Referenssiarkkitehtuuri (SFS-IEC 62443-2-1, 2013, s. 84)

Eri tietoturvavyöhykkeiden välinen kommunikointi tapahtuu vain siihen määritettyjä tietoväyliä pitkin, jotka ovat myös eräänlaisia vyöhykkeitä. Tietoväylävyöhykkeessä laitteiden sijaan suojattavana on tieto. Fyysisesti tietoväylä muodostuu vyöhykkeiden välisistä tietoliikennelaitteista, kuten kaapeleista ja kytkimistä. Tietoväylä määritetään jokaisen vyöhykkeen välille, ja sen tehtävänä on taata vyöhykkeiden välinen turvallinen kommunikointi. Tietoväylä on vyöhyketyyppi, jolla ei voi olla alivyöhykkeitä, eli siis tietoväylä ei koostu alitietoväylistä. (IEC/TS 62443-1-1:fi, 2012; SFS-IEC 62443-2-1, 2013)

Jokaiselle tietoväylälle tulee määritellä ne tietoturvavyöhykkeet jotka se yhdistää, sen käyttämät teknologiat ja protokollat jotka on sallittu liikkumaan sen sisässä sekä sen tietoturvaominaisuudet (Byres, 2014, s. 6)

Kuvassa 17 on havainnollistettu tietoväylien muodostumista. Tietoväylät on merkattu kuvassa vihreällä värillä. Jokainen tietoväylä kulkee palomuurin läpi, jotta liikennettä voidaan seurata ja rajoittaa. Huomioitavaa on myös se, että tässä kuvassa myös vyöhykkeitä on enemmän kuin vain ne kolme, jotka ovat minimi suositus.



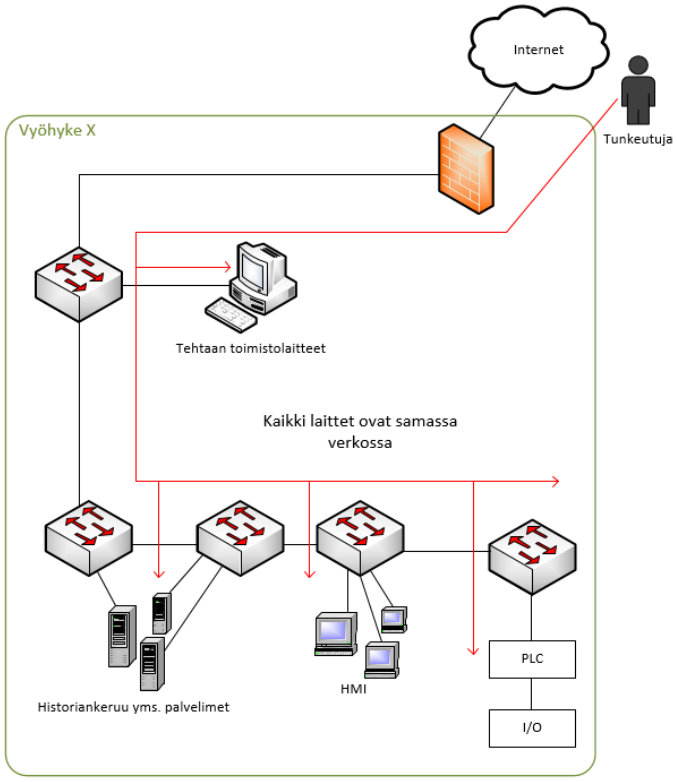
Kuva 17. Esimerkki vyöhykkeistä, (IEC 62443-3-3, 2013, s. 69)

7 HYÖDYT

Kun järjestelmän rakenne on suunniteltu referenssimallin mukaan, saadaan tietoturvavyöhykkeet määriteltyä tehokkaasti sekä järjestelmän sisäistä tietoliikennettä saadaan seurattua. Segmentointi luo suojaa mahdollista hyökkääjää vastaan ja yleisesti se luo suuren tietoturvan. Vyöhykkeet auttavat kehittämään laitteiden tietoturvaa kokonaisuutena, koska se ei huomioi pelkästään yksittäisiä laitteita.

Vertaillaan esimerkiksi kahta erilaista järjestelmän rakennetta, toisessa ei ole harjoitettu minkäänlaista verkon segmentointia, ja toinen järjestelmä on suunniteltu standardin suosituksen mukaan. Esitetyt kuvat ovat karrikoituja esimerkkejä ja niissä on korkea abstraktin taso.

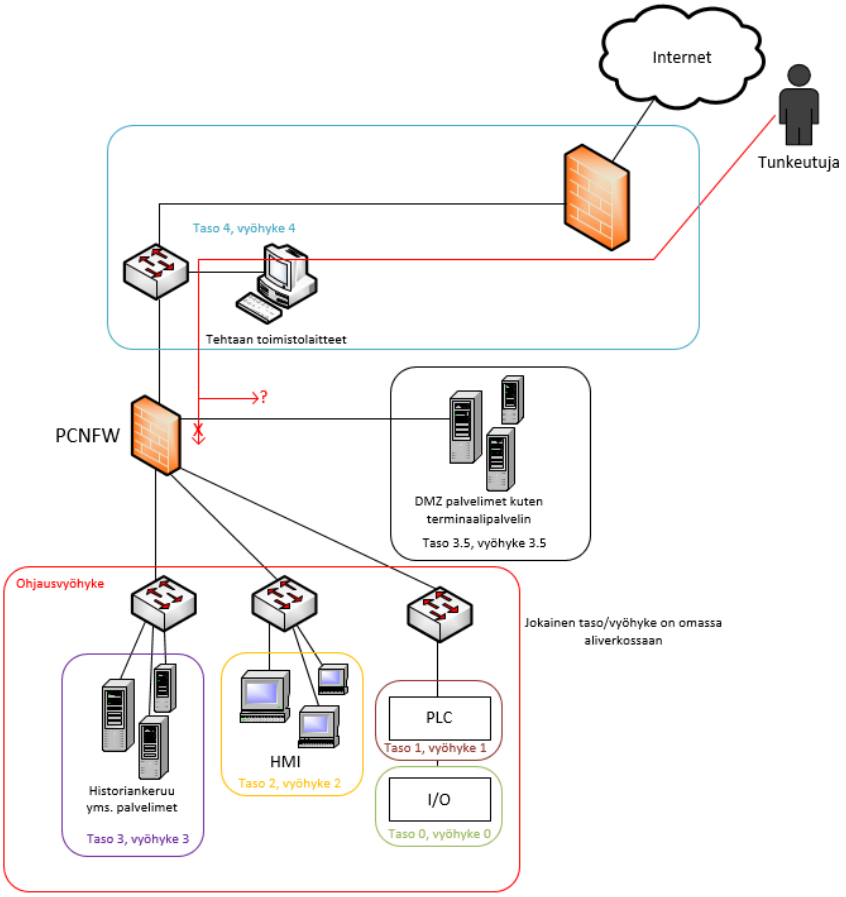
Ensimmäisessä kuvassa (kuva 18) verkkoa ei ole jaoteltu mitenkään. Kaikki laitteet ovat samassa verkossa ja vyöhykkeessä, ja ainoa suoja rakenteen kannalta hyökkääjää vastaan on yksi palomuuri. Mikäli tunkeutuja löytää palomuurin läpi jonkun heikkouden, hänellä on pääsy koko verkkoon. Kuvitellaan, että hän pystyy luvatta etäkäyttämään tehtaan toimistoverkossa olevaa tietokonetta. Koska tietokone on samassa verkossa muiden automaatiolaitteiden kanssa, hänellä on pääsy myös kaikkiin muihin verkon osiin, varsinkaan kun verkon rakenteessa ei ole DMZ-tasoa, eikä minkäänlaisia tietoliikennettä seuraavia tai rajoittavia laitteita kuten toista palomuuria. Käytännössä tunkeutuja pystyisi käyttämään tehtaan toimistokonetta ”hyppypalvelimena” ja ottamaan sitä kautta etäyhteyksiä vaikkapa valvomon HMI-koneille, ja tekemään niillä mitä hän haluaa. Hän voisi ohjata prosessia ja vaikka aiheuttaa koko tehtaan pysähdyksen. Jos jokin haittaohjelma kuten virus pääsee leviämään tehtaalle, se pystyy saastuttamaan kaikki laitteet kerralla, koska tehtaan sisässä ei ole minkäänlaista liikenteen estoa tai seurantaa. Myös laitteiden tämänhetkisen tietoturvakyvyn seuraaminen on hyvin haasteellista.



Kuva 18. Ei segmentointia (Pitkänen, 2018)

Kuvassa 19 verkon jaottelu on toteutettu käyttäen IEC 62443-standardia, sekä tietoturvavyöhykkeet on samalla täsmätty referenssimallin kerrosten mukaan. Myös DMZ-taso on käytössä. Vaikka tunkeutuja pääsisi murtautumaan ensimmäisen palomuurin läpi tehtaan verkkoon, hänen on hyvin vaikea päästä jatkamaan automaatioon asti, eli täten järjestelmässä ei ole vain yhtä pistettä jonka murtuessa koko järjestelmä on uhattuna. Hyökkääjän eteneminen toimistoverkosta eteenpäin on hyvin hankalaa. Koska kaikki liikenne kulkee automaatioon DMZ-tason kautta, tunkeutujan täytyy ensin päästä sinne.

Mikäli DMZ-tasolle päästään tunkeutumaan, kaikki alemman tason laitteistot on segmentoitu erilleen, ja tunkeutujan täytyy ”valloittaa” kaikki tasot erikseen. Lisäksi Process Control Network (PCN)-palomuuri tarkkailee ja suodattaa jokaisen tietoturvavyöhykkeiden välistä liikennettä, mikä hankaloittaa hyökkääjän etenemistä entisestään. Parhaassa tapauksessa tunkeutuja tai haittaohjelma huomataan jo toimistoverkon puolella, ja ne eivät ikinä pääse etenemään edes DMZ-tasolle asti. Laitteiden tietoturvaa on myös helppo ylläpitää vyöhykkeiden ansiosta, koska ne on selkeästi dokumentoitu ja vyöhykkeillä on selkeät vaaditut tietoturvatasot sekä vyöhykkeiden riskit ovat tiedossa.



Kuva 19. Segmentoitu verkko (Pitkänen, 2018)

Tiivistetysti voisi sanoa, että tietyt laitteet täytyy olla tietyillä tasoilla ja eri segmenteissä siksi, koska laitteilla on erilaiset toiminnalliset tehtävät, tietoturvakyvyt, tietoturvan murtumisesta aiheutuvat riskit, sekä kommunikointitarpeet jotka vaikuttavat laitteilta vaadittuun tietoturvatasoon. Ilman segmentointia ja vyöhykkeiden luontia laitteiden erilaisten tarpeiden huomioonottaminen ei ole mahdollista. Eri vyöhykkeet myös hidastavat tai torjuvat ongelmien kuten virusten leviämistä koko verkkoon. Koko verkkoa ei menetetä ainakaan heti vaan luultavasti vain yksi vyöhyke. Mikäli laitteet eivät ole oikeissa segmenteissä tai vyöhykkeissä tai segmentointia ei ole toteutettu ollenkaan, on järjestelmän tietoturvaa hyvin vaikea, ellei jopa mahdotonta seurata ja ylläpitää. Standardin mukainen rakenteen toteutus ei pelkästään paranna tietoturvaa, vaan siitä on myös muita hyötyjä. Kun järjestelmän rakenne on vakioitu, se helpottaa uusien projektien järjestelmän rakenteen suunnittelua.

8 FYYSINEN SUOJAUS

Kun puhutaan kyberturvallisuudesta, yleensä keskitytään enemmän teknologisiin vastatoimiin, kuten tässäkin opinnäytetyössä on keskitytty. Fyysinen suojaus on kuitenkin tärkeä osa kyberturvallisuutta. Mikäli kuka tahansa pääsisi kävelemään suoraan tehtaalle ja laitteiden ohjausjärjestelmille, koko järjestelmän segmentointi ja palomuurien ja muiden tietoturvalaitteiden konfigurointi olisi täysin turhaa. Haittaohjelmat ja tieto kulkevat helposti tuotantolaitokselle ja sieltä pois USB-tikuilla, kannettavilla tietokoneilla tai älypuhelimilla.

IEC 62443-2-1 määritteleekin vaatimuksia myös järjestelmän fyysiseen suojaukseen. Vaatimuksiin kuuluu mm. kulunvalvonnan toteuttaminen, työntekijöiden vaatimus noudattaa fyysisiä tietoturvamenettelyitä, tarkkailua ja hälytystä varten määriteltävät menettelyt ja fyysisen tietoturvan ulkorajojen perustaminen. (SFS-IEC 62443-2-1, 2013 s. 110 - 111).

Fyysisen suojauksen suunnittelu alkaa jo tuotantolaitoksen paikan valitsemisella, eli laitoksen tulisi olla sijainniltaan häiriöttömässä paikassa, eli ei esimerkiksi lentokenttien tai vankiloiden läheisyydessä. Tehtaan ympäristöön tulisi olla hyvä näkyvyys ja se olisi hyvä olla aidattu. Ihmisten sekä autojen kulkua tehtaalle sekä tehtaalta pois tulisi valvoa ainakin tehtaan porteilla. Porteilla voi olla vartija ja/tai tunnistuskortti millä pääsee portista sisään ja ulos. Kaikkia tiloja tulisi valvoa valvontakameroilla. ICS- ja IT-laitteisiin kuten palvelimiin, kytkimiin ja logiikkoihin ei tulisi olla suoraa pääsyä, vaan ne tulisi olla lukitussa tilassa ja vain tiettyjen henkilöiden tulisi päästä tilaan. Turhien Ethernet-porttien ja USB-porttien käyttö laitteissa tulisi estää joko fyysisesti tai ohjelmallisesti. (Ackerman, 2017)

Myös fyysisessä suojauksessa olisi hyvä käyttää montaa turvakerrosta. Monet turvakerrokset vaikeuttavat tunkeutujan luvatonta pääsyä tärkeimpiin tuotantolaitoksen osiin, kuten logiikoille tai palvelimille. Esimerkiksi, että henkilö pääsisi fyysisesti käsiksi jollekin tärkeälle laitteelle, hänen täytyisi tunnistautua ainakin tehtaan portilla sekä muutamalla muulla pisteellä, kuten konehuoneen ovella. (Ackerman, 2017)

9 TOTEUTUS KÄYTÄNNÖSSÄ

9.1 Toteutus yleisesti

Uutta järjestelmää suunnitellessa tulisi järjestelmän rakenne suunnitella kappaleessa 5 esitellyn referenssimallin mukaisesti. Järjestelmään valittavat laitteet tulisi asetella niille kuuluville tasoille riippuen laitteiden käyttötarkoituksesta sekä niiden tehtävistä.

Mikäli on vaikea päättää, kuuluuko jokin laite automaatiopuolelle vai tuotantolaitoksen toimistopuolelle, on hyvä miettiä myös vastausta kysymykseen: ”Jatkuuko tuotanto tai prosessin toiminta, jos yhteys laitteeseen menetetään.” (Ackerman, 2017)

Kun laitteistot on sijoiteltu oikeille tasoille, luodaan tietoturvavyöhykkeet referenssimallin ryhmittelyn, laitteiden tietoturvakyvyn sekä halutun tietoturvatason perusteella. Jotta vyöhykkeet voidaan muodostaa tarkasti, tulee kullekin vyöhykkeelle määritellä niille kappaleessa 6 mainitut ominaisuudet: tietoturvapolitiikat, luettelo suojattavista kohteista, pääsyvaatimukset ja valvontamenetelmät, uhat ja haavoittuvuudet, tietoturvan murtumisen seuraukset (riskianalyysi), valtuutettu teknologia ja muutostenhallintaprosessi. Myös vyöhykkeiden väliset tietoväylät tulee määritellä sekä määritellä tietoväylille kappaleessa 6 mainitut ominaisuudet: vyöhykkeet jotka tietoväylä yhdistää, tietoväylän käyttämät teknologiat ja protokollat jotka on sallittu liikkumaan sen sisässä sekä tietoväylän tietoturvaominaisuudet.

Käytännössä jokainen vyöhyke on oma aliverkkonsa, jotta vyöhykettä voidaan käsitellä omana segmenttinään, ja jotta se oikeasti on erillinen vyöhyke muista verkoista tai vyöhykkeistä. Jotta palomuuri voi suodattaa vyöhykkeiden välistä liikennettä, tulee vyöhykkeestä lähtevä ja tuleva liikennöinti kulkea palomuurin kautta. Verkon rakenne täytyy suunnitella siten, että nämä toteutuvat. Toki poikkeuksia voi olla, mikäli muita tarpeita joudutaan ottamaan huomioon.

Laitteiden asettelun, verkon rakenteen suunnittelun ja tietoturvavyöhykkeiden muodostamisen jälkeen konfiguroidaan palomuurit seuraamaan ja hallinnoimaan vyöhykkeiden välistä liikennettä vyöhykkeiden ominaisuuksien perusteella. Palomuurin määrittelyyn tarvitaan ammattihenkilö, joka tuntee jokaisen laitteen käyttämät protokollat. Kun tietoturvavyöhykkeitä määritellessä on jokaiselle vyöhykkeelle määritelty ominaisuudet, helpottuu palomuurisääntöjen teko. Kappaleessa 9.2 on yleisiä ohjeita palomuurin konfiguroimiseen. Yksi pahin virhe muodostaessa järjestelmää on palomuurin huono konfigurointi, josta johtuen järjestelmän segmentointi on lähes yhtä tyhjän kanssa.

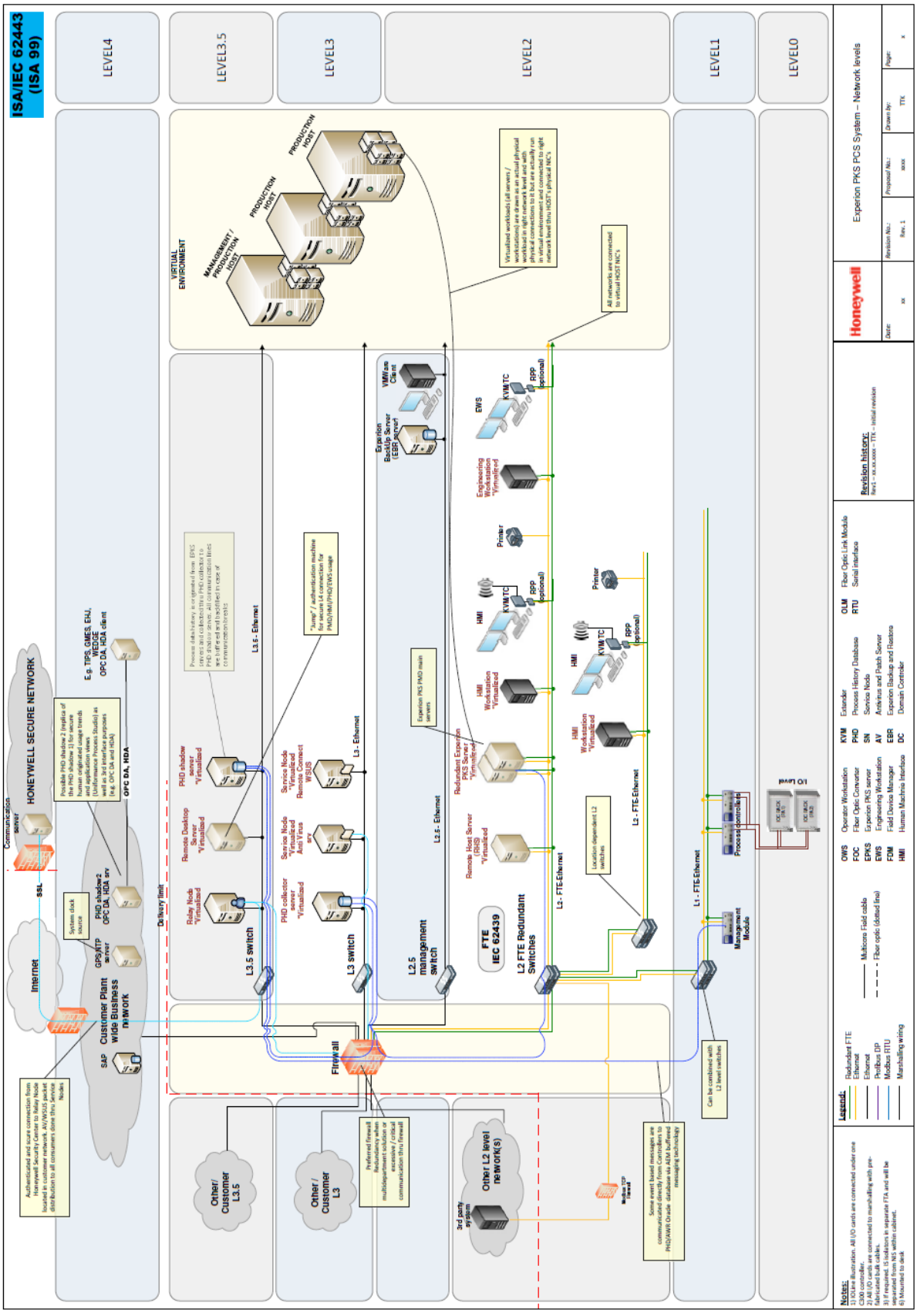
9.2 Palomuurin konfigurointi

Palomuurin perusideana pitäisi olla kaiken liikenteen esto paitsi sen, mikä on erikseen sallittu. Liikenne yritystason vyöhykkeestä ohjausvyöhykkeeseen tulisi estää ja kaikki ohjausvyöhykkeen sekä yritystason vyöhykkeen liikenne tulisi loppua viimeistään DMZ-vyöhykkeelle. Mikään ohjausvyöhykkeessä oleva laite ei saa olla suoraan yhdistetty internettiin, vaikka ne olisivatkin palomuurin takana. (Collantes & Padilla, 2015)

Liikenne tulisi suodattaa kohde ja lähde IP-osoitteiden perusteella sekä porteittain mikäli mahdollista. Palveluita ja portteja joita käytetään yleensä hyökkäykseen ei tulisi avata ollenkaan, ja tietoliikennetekniikoita, jotka käyttävät suurta määrää portteja tulisi välttää. Mikäli näitä tekniikoita joudutaan käyttämään, tulisi ylimääräisiä vastatoimenpiteitä käyttää. (SFS-IEC 62443-2-1, 2013, s. 84)

9.3 Esimerkki: Honeywell Oy:n järjestelmä

Tavoitteena on tutkia, miten laitteet asettuvat referenssimallin tasoille Honeywell Oy:n järjestelmässä sekä muodostaa tietoturvavyöhykkeet sekä tehdä vaaditut määritelmät vyöhykkeille. Pohjana on käytetty Honeywell Oy:n yleistä automaatiojärjestelmän pohjaa.

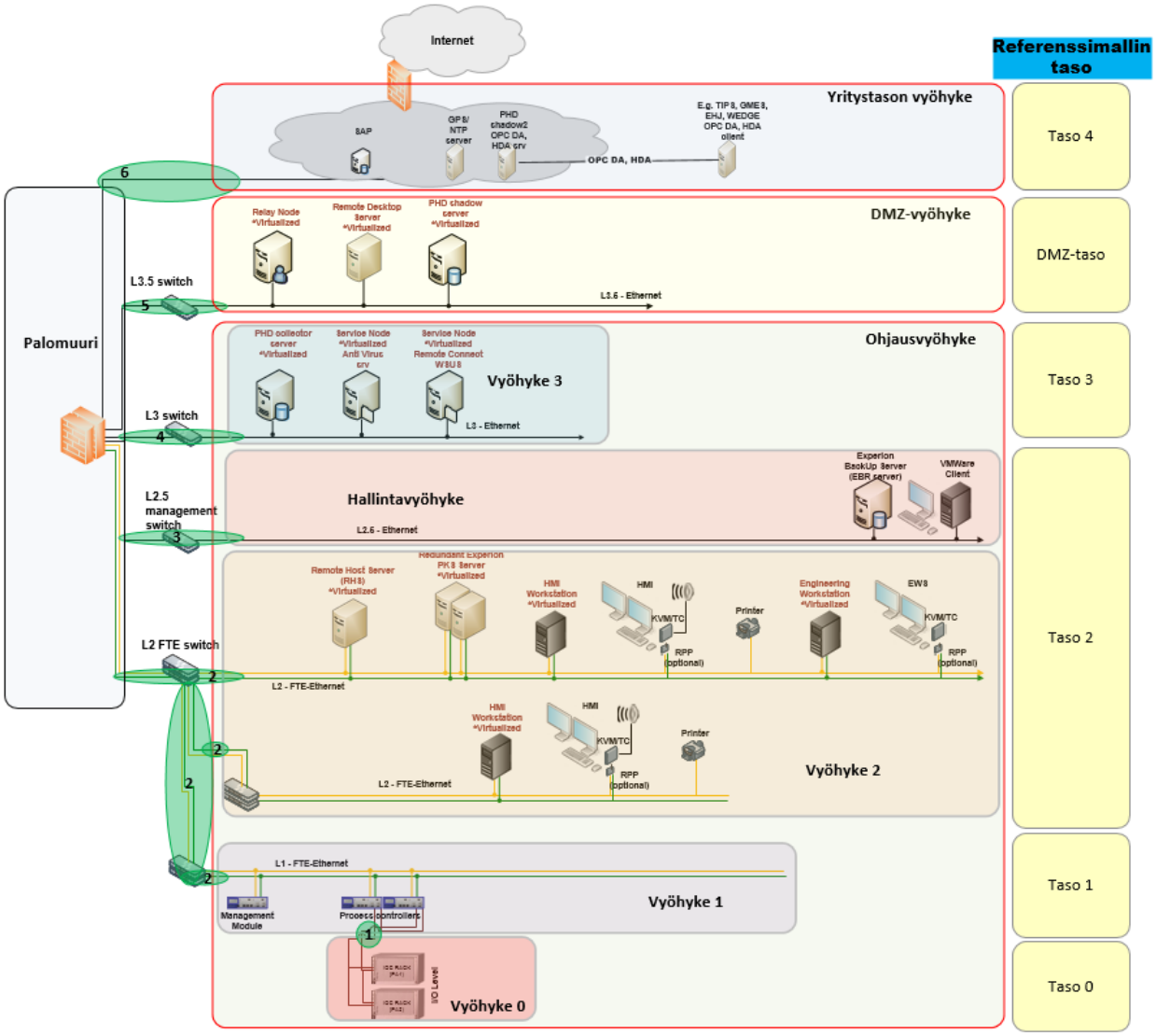


Kuva 20. Honeywell Oy:n tyypillinen järjestelmärakenne (Honeywell Oy, 2018)

Honeywell pohjustaa järjestelmänsä standardin suositteleman referenssimallin mukaisesti. Järjestelmään on luotu tasot 0 – 4 laitteiden toimintojen perusteella ja tasojen välistä liikennettä tarkkaillaan palomuurilla. Kuvassa 20 on esitetty geneerinen järjestelmän rakenne. Koska laitteet, jotka suorittavat

samantyylisiä tehtäviä ja joilla on samantyyliset tietoturvatarpeet ovat jo valmiiksi samoilla tasoilla, tulee tietoturvavyöhykkeistä yhdenmukaisia referenssimallin tasojen kanssa. Ainut poikkeus on referenssimallin tasolla kaksi oleva ”L2.5” joka on tason kaksi laitteiston hallinnointia varten. Sille täytyy tehdä oma vyöhykkeensä, koska laitteilla on erilaiset tietoturvatarpeet verrattuna muuhun referenssimallin tason kaksi laitteistoon.

Kuvassa 21 on esitetty mahdollinen toteutus tietoturvavyöhykkeille sekä niiden välisille tietoväylille. Tietoväylät on merkattu vihreällä sekä referenssimallin tasot on merkattu keltaisella värillä oikeassa laidassa. Tietoturvavyöhykkeitä on merkattu erivärisillä suorakaiteilla.



Kuva 21. Yksi mahdollinen vyöhykeratkaisu (Pitkänen, 2018)

Seuraavat kuvaukset perustuvat kuvaan 21:

Ohjausvyöhyke:

Automaatiojärjestelmän referenssimallin tasot 0-3 on yhdistetty yhdeksi isoksi vyöhykkeeksi, joka muodostuu pelkästään alivyöhykkeistä. Tämä on tehty siksi, koska laitteilla on yleiset samantyyliset

tietoturvatarpeet sekä riskit. Vyöhyke helpottaa myös määrittelemään kaikille alivyöhykkeille yleisiä määrityksiä kuten kommunikointia vyöhykkeestä ulos ja sisään. Liitteessä yksi on tämän tietoturva-vyöhykkeen kuvaus.

Vyöhyke nolla:

Vyöhyke nolla muodostuu referenssimallin tasosta nolla. Tasolla nolla sijaitsee siis referenssimallin mukaisesti anturit ja I/O räkit. Oma vyöhyke on muodostettu sen takia, koska vyöhykkeen laitteilla on samanlaiset tietoturvatarpeet, kommunikointitarpeet sekä riskit. Liitteessä kaksi on tämän tietoturva-vyöhykkeen kuvaus.

Vyöhyke yksi:

Vyöhyke yksi muodostuu myös suoraan referenssimallin tasosta yksi, koska laitteilla on samankaltaiset tietoturvatarpeet, toiminnot sekä riskit. Vyöhykkeellä yksi onkin siis referenssimallin mukaisesti prosessin ohjaus ja säätölaitteet. Honeywell Oy:llä on tähän tarkoitukseen laajalti käytössä heidän Field Controller Express. Liitteessä kolme on tämän tietoturvavyöhykkeen kuvaus.

Vyöhyke kaksi:

Vyöhyke kaksi muodostuu referenssimallin tasosta kaksi laitteiden samantyylisten tietoturvatarpeiden ja riskien takia. Vyöhykkeellä kaksi sijaitseekin prosessin valvomolaitteisto. Honeywell Oy:llä on tasolla kaksi mm. EPKS järjestelmän palvelimet, HMI-konsolit ja sovellusasemat. Laitteisto voi olla virtualisoitu tai perinteinen. Vyöhykkeen kuvaus on liitteessä neljä.

Hallintavyöhyke:

Hallintavyöhykkeellä sijaitsee virtualisoidun järjestelmän palvelimien hallinta sekä varmuuskopiointi. Hallintavyöhyke muodostuu siksi omaksi vyöhykkeekseen, koska vyöhykkeen laitteilla on samankaltaiset tietoturva- ja kommunikointitarpeet. Laitteet eivät liity varsinaisesti valvomon operointiin vaan virtualisoitujen automaatiokäytössä olevien palvelimien hallinnointiin, joten riskit ovat hieman pienemmät kuin muilla automaatiojärjestelmän laitteilla. Mikäli vyöhyke olisi kokonaan pois pelistä, kaikki muut laitteet jatkavat silti normaalia operoimista. Vyöhykkeen kuvaus on liitteessä viisi.

Vyöhyke kolme:

Vyöhyke kolme muodostuu myös referenssimallin tasosta kolme laitteiden aktiviteettien, tietoturva- ja kommunikointitarpeiden sekä riskien perusteella. Vyöhykkeellä kolme Honeywell Oy:llä on mm. PHD (Process History Database) Collector-palvelin. PHD Collector on prosessihistoriadatan kerääjä, joka kerää historiatiedot tason kaksi PMD servereiltä sekä tason yksi ohjaimilta. Nämä historiatiedot tuo-

daan myös tarjolle DMZ-vyöhykkeen PHD Shadow-serverille. Tämä onkin vyöhykkeen yksi erityispiirteitä, koska se joutuu siirtämään dataa korkean riskin sisältäviltä ohjauslaitteilta DMZ-tasolle. Vyöhykkeen kuvaus on liitteessä kuusi.

DMZ-vyöhyke:

DMZ-vyöhykkeellä sijaitsee laitteet, jotka toimivat tiedonvälittäjinä yritystason ja ohjaustason vyöhykkeen välillä. Vyöhykkeellä sijaitsevilla laitteilla on myös samanlaiset tietoturvakyvyt, riskit ja tietoturvatarpeet. Vyöhykkeellä sijaitsee Honeywell Oy:n laitteistoa kuten mm. PHD Shadow-palvelin, eli palvelin jolle PHD Collector käy tuomassa datan tarjolle. Näin dataan pääsee käsiksi ilman suoraa yhteyttä automaatioon. Vyöhykkeellä sijaitsee myös esimerkiksi terminaalipalvelin etäyhteyksille. Etäyhteydet alempien vyöhykkeiden järjestelmiin kulkee terminaalipalvelimen kautta, jotta suoria yhteyksiä automaatioon ei ole. Mitään liikennettä ei ole sallittu suoraan DMZ-vyöhykkeen yli. Vyöhykkeen kuvaus on liitteessä seitsemän.

Yritystason vyöhyke:

Yritystason vyöhyke perustuu referenssimallin tasoon neljä, joka on tehtaan toimistoverkkoa. Laitteet eivät ole merkittäviä prosessin toiminnan kannalta, ja niillä on samanlaiset tietoturvatarpeet sekä riskitaso. Vyöhykkeellä neljä voi sijaita toinen PHD Shadow-palvelin jonne DMZ-vyöhykkeen PHD Shadow-palvelin ”työntää” datansa, mikä lisää tietoturvaa entisestään, koska ihmiskäyttäjien ei tarvitse ottaa yhteyttä edes automaation DMZ-vyöhykkeelle päästäkseen käsiksi PHD:n historiadataan, vaan se on saatavilla suoraan toimistoverkon puolelta. Näin datan katselu onnistuu mistä tahansa internetin välityksellä. Vyöhykkeen kuvaus on esitetty liitteessä kahdeksan.

Tietoväylät:

Tietoväylät on määritelty jokaisen vyöhykkeen välille. Tietoväylien kuvaukset on esitetty liitteessä yhdeksän.

9.4 Muut huomioon otettavat asiat

Honeywell ei pysty vaikuttamaan politiikoihin, joita käytetään tehtaan toimistoverkossa, sillä niistä vastaa yleensä esimerkiksi tehtaan IT-organisaatio. Täten tuotantolaitoksien olisi hyvä olla ainakin tietoisia tässä opinnäytetyössä esitetyistä strategioista. Tuotantolaitoksen olisi otettava huomioon myös tuotantolaitoksella sijaitsevat muut mahdolliset laitteet jotka ovat siellä jonkun toisen toimittajan puolesta ja niiden vaikutus kyberturvallisuuteen.

10 YHTEENVETO

Opinnäytetyössä tutustuttiin automaatiojärjestelmän tasoihin ja syihin, miksi automaatiojärjestelmän rakenne on muodostettu tietyllä tavalla. Järjestelmän rakenteen tietyllä tavalla jaottelun syyksi muodostui automaatiojärjestelmien tärkeimpien laitteiden heikko tietoturvakyky. Lisäksi laitteita halutaan suojata mahdollisimman paljon, koska laitteiden vaarantuessa voi uhkana olla pahimmassa tapauksessa ihmishenkien menetys.

Järjestelmä tulee segmentoida siten, että prosessilaitteistoa suojataan kaikista eniten. Lisäksi automaatiolaitteet eivät saa olla suorassa yhteydessä internettiin, ja ne täytyy erottaa tehtaan toimistoverkosta. Järjestelmän segmentointi ja tietoturvavyöhykkeiden luonti mahdollistavat jokaisen laitteen tai laitejoukon tietoturvatarpeiden huomioon ottamisen. Segmentointi luo myös turvaa vähentämällä suoria yhteyksiä automaatioon sekä hidastamalla mahdollisten haittaohjelmien leviämistä.
Tämän työn pohjalta on tarkoitus jalostaa muita dokumentteja, joita voidaan käyttää, kun suunnitellaan ja perustellaan Honeywell Oy:n automaatiojärjestelmän rakenteeseen liittyviä ratkaisuita. Tarkoitus on myös informoida ja kouluttaa muita kollegoita tästä aiheesta, jotta kaikilla olisi tiedossa syyt, jonka takia järjestelmä täytyy tehdä tietyllä tapaa.

Opinnäytetyön aihe tulee korostumaan tulevaisuudessa entisestään, kun automaatiossa otetaan käyttöön esimerkiksi Industrial Internet of Things (IIoT) laitteita. Laitteet myös kehittyvät jatkuvasti enemmän kohti IT-tyylisiä järjestelmiä, ja kehittyvä teknologia tuo jatkuvasti uusia kyberturvallisuushaasteita.

Opin työn aikana huomattavasti automaatiojärjestelmän laitteistosta ja rakenteesta, niiden sijoittelusta järjestelmään, eri protokollista mitä automaatiojärjestelmissä käytetään, kyberturvallisuudesta sekä palomuureista.

11 LAINATUT LÄHTEET

Ackerman, P. (2017). *Industrial Cybersecurity.* Packt Publishing.

Buchy, J. (2016). *Cyber Security vs IT Security: Is There a Difference?* Haettu 20. 8 2018 osoitteesta http://business.gmu.edu/blog/tech/2016/06/30/cyber-securit-it-security-difference/

Byres, E. (2013). *The Industrial Cybersecurity Problem.* ISA. Haettu 28. 6 2018 osoitteesta https://www.isa.org/pdfs/the-industrial-cybersecurity-problem/

Byres, E. (2014). *Using ISA/IEC 62443 Standards to Improve Control System Security.* Tofino Security. Haettu 12. 6 2018 osoitteesta https://www.tofinosecurity.com/sites/default/files/common/white-papers/Using-ISA_IEC-62443-Standards-WP-v1.2%20(May%202014).pdf

Cisco, Rockwell Automation. (2011). *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide*. Haettu 19. 6 2018 osoitteesta http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf

Collantes, M. H.;& Padilla, A. L. (2015). *Protocols and network security in ICS infrastructures.* Spanis National Cybersecurity Institute. Haettu 10. 7 2018 osoitteesta https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_protocol_net_security_ics.pdf

Homeland Security. (2016). Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Haettu 4. 7 2018 osoitteesta https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

Honeywell Oy. (2018).

International Electrotechnical Commission. (2013). *IEC 62443-3-3.*

Mackenzie, H. (2012). *SCADA Security Basics: Why Industrial Networks are Different than IT Networks*. Haettu 24. 7 2018 osoitteesta Tofino Security: https://www.tofinosecurity.com/blog/scada-security-basics-why-industrial-networks-are-different-it-networks

Obregon, L. (2014). *Secure Architecture for Industrial Control Systems.* Haettu 13. 6 2018 osoitteesta https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327

SESKO ry. (2012). *IEC/TS 62443-1-1:fi.* Suomen Standardisoimisliitto SFS ry.

SESKO ry. (2013). *SFS-IEC 62443-2-1.* Suomen Standardisoimisliitto SFS ry.

Shodan. (2018). Haettu 25. 6 2018 osoitteesta https://www.shodan.io

Siemens. (2007). *Industry online support*. Haettu 24. 7 2018 osoitteesta https://support.industry.siemens.com/cs/document/24534065/which-ports-are-used-by-wincc-flexible-?dti=0&lc=en-WW

Speed Guide. (2014). *Port 502 Details*. Haettu 7. 24 2018 osoitteesta Speed Guide: https://www.speedguide.net/port.php?port=502

Speed Guide. (2018). *Port 44818 Details*. Haettu 24. 7 2018 osoitteesta SpeedGuide: https://www.speedguide.net/port.php?port=44818

Stouffer, K.;Pillitteri, V.;Lightman, S.;Abrams, M.;& Hahn, A. (2015). *NIST Special Publication 800-82 - Guide to Control Systems (ICS) Security.* National Institute of Standards. Haettu 2. 7 2018 osoitteesta https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

Suomen Automaatioseura ry. (2010). Teollisuusautomaation tietoturva - verkottumisen riskit ja niiden hallinta. Haettu 3. 7 2018 osoitteesta https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf

Wikimedia. (2005). Haettu 2018 osoitteesta https://upload.wikimedia.org/wikipedia/fi/4/4c/OSI-malli.jpg

LIITE 1: OHJAUSVYÖHYKKEEN KUVAUS

Ohjausvyöhyke kuvaus

Vyöhykkeen nimi: Ohjausvyöhyke

Vyöhykkeen määritelmä: Vyöhyke sisältää tärkeät automaatiojärjestelmän laitteistot. Vyöhyke koostuu pelkästään alivyöhykkeistä.

Vyöhykkeen toiminnot: Vyöhykkeen toimintoihin kuuluu kaikki automaatiojärjestelmän toiminnot, mukaan lukien prosessin ohjauksen, valvonnan sekä historian keruun. Vyöhyke vastaa koko tuotantolaitoksen prosessin toiminnasta.

Vyöhykkeen rajat: Vyöhykkeeseen kuuluu seuraavat vyöhykkeet: Vyöhyke 0, Vyöhyke 1, Vyöhyke 2, Hallintavyöhyke sekä vyöhyke 3.

Tyypilliset laitteet (luettelo suojattavista kohteista): Suojattaviin kohteisiin kuuluu kaikki tämän vyöhykkeen alivyöhykkeet.

Vyöhykkeen sisältämät riskit: Vyöhyke sisältää tärkeät automaatiojärjestelmän ohjaus- ja valvontalaitteet. Tietoturvan murtumisen seuraukset ovat kriittiset tuotantolaitoksen toiminnan kannalta.

-Vyöhykkeen tietoturvakyky
Vyöhykkeessä sijaitsee tietoturvakyvyltään eritasoisia alivyöhykkeitä. Yleinen tietoturvakyky on kohtalainen. Näitä on kuvattu tarkemmin alivyöhykkeiden kuvauksissa.
-Vyöhykkeen uhkat ja haavoittuvuudet
Jokaisella alivyöhykkeellä on määritelty nämä erikseen.
-Tietoturvan murtumisen seuraukset
Mikäli koko vyöhyke ja kaikki alivyöhykkeet menetetään, seuraukset ovat hyvin kriittiset. Seurauksia ovat pahimmassa tapauksessa mm. koko tuotannon pysähtyminen ja laitteiden hajoaminen.
-Tärkeys tuotantolaitoksen toiminnan kannalta
Todella tärkeä
-Vyöhykkeen tavoitteena oleva tietoturvataso
Jos käytetään asteikkoa alhainen, keskinkertainen ja korkea, niin tämän vyöhykkeen tavoite olisi korkea. Tämä tavoite periytyy myös kaikille alivyöhykkeille.

Valtuutettu teknologia: Mikäli vyöhykkeen hyväksyttyihin teknologioihin kuten tietoliikennetekniikoihin tehdään mahdollisia muutoksia liiketoiminnan tarpeen täyttämiseksi, täytyy sen vaikutus vyöhykkeen toimintaan ja riskeihin arvioida. Pääasiassa valtuutettua teknologiaa on vain tässä dokumentissa mainitut tekniikat sekä laitteet, jotka käyttävät näitä tekniikoita.

Pääsyvaatimukset ja valvontamenetelmät: Koska kaikki tietotekninen pääsy vyöhykkeeseen tapahtuu DMZ-vyöhykkeen kautta, ovat pääsyvaatimukset ja valvontamenetelmät DMZ-vyöhykkeen määrittelyssä. Fyysistä pääsyä vyöhykkeen laitteisiin valvotaan tehtaan porteilla.

Tietoturvastrategia: Vyöhykkeeseen menevää ja vyöhykkeestä lähtevää liikennettä valvotaan ja rajataan palomuurilla. Laitteisiin päivitetään aina viimeisimmät tietoturvapäivitykset sekä virustorjuntaohjelmien päivitykset, mikäli mahdollista.

Valvottavat tietoturvatoimenpiteet: Varmistetaan, että kaikki liikenne ohjausvyöhykkeen ja yritystason vyöhykkeen välillä kulkee DMZ-vyöhykkeen kautta. Varmistetaan, että vyöhykkeelle pääsy on rajattu vain tiettyihin IP-osoitealueisiin sekä sallittuihin protokolliin.

Sallitut aktiviteetit: Sallittuja aktiviteettejä ovat toiminnot, jotka liittyvät automaatiojärjestelmän toimimiseen. Esimerkiksi sähköposti tai internetin selaus ei kuulu tälle vyöhykkeelle.

Sallitut tietoliikennetekniikat: Kaikki automaatiolaitteiden välttämättömät protokollat ja tekniikat. Alivyöhykkeiden kuvauksissa ja tietoväylien kuvauksissa näitä on kuvailtu tarkemmin.

Tietoväylät: Tietoväylät on määritelty erillisessä liitteessä.

Muutostenhallintaprosessi: Muutoksista vastaa laitteiden toimittajat heidän kanssaan tehtyjen sopimusten mukaan. Mahdollisissa muutoksissa tulee ottaa huomioon laitteiden muuttuvat tietoturvauhkat. Muutokset eivät saa vaarantaa vyöhykkeen tietoturvaa ja muutokset on dokumentoitava.

LIITE 2: VYÖHYKKEEN NOLLA KUVAUS

Vyöhyke 0 kuvaus

Vyöhykkeen nimi: Vyöhyke nolla

Vyöhykkeen määritelmä: Vyöhyke sisältää I/O laitteistot, joita tarvitaan prosessin ohjauksessa.

Vyöhykkeen toiminnot: Antureiden kautta datan välitys vyöhykkeelle yksi. Prosessilaitteiden ohjaus vyöhykkeen yksi laitteiden perusteella.

Vyöhykkeen rajat: Vyöhykkeeseen kuuluu vain I/O laitteisto.

Vyöhykkeen perimä: Vyöhyke perii ominaisuudet ohjausvyöhykkeeltä, sillä se on vyöhykkeen alivyöhyke. Täten kaikki määritelmät, jotka ovat ohjausvyöhykkeellä ovat myöskin tällä vyöhykkeellä, vaikka niitä ei ole erikseen tässä lueteltu.

Tyypilliset laitteet (luettelo suojattavista kohteista): I/O räkit ja sensorit.

Vyöhykkeen sisältämät riskit: Tason laitteisto on erittäin kriittinen prosessin toiminnan kannalta.

-Vyöhykkeen tietoturvakyky
Vyöhykkeellä on heikko tietoturvakyky. Protokollissa ei ole todennusta eikä salausta.
-Vyöhykkeen uhkat ja haavoittuvuudet
Protokollien heikkoudet.
-Tietoturvan murtumisen seuraukset
Tuotantolaitoksen pysähtyminen, henkilövahingot, suuret tappiot laitokselle.
-Tärkeys tuotantolaitoksen toiminnan kannalta
Erittäin tärkeä.

Pääsyvaatimukset ja valvontamenetelmät: Fyysistä pääsyä vyöhykkeen laitteisiin valvotaan tehtaan porteilla.

Tietoturvastrategia: Varmistetaan kaapeleiden oikeat kytkennät ja laitteiden konfiguraatio. Laitteille tuleva ja laitteilta lähtevä data ei saa päätyä minnekään muualle, kuin prosessia ohjaaville laitteille.

Valvottavat tietoturvatoimenpiteet: Tarkkaillaan että dataa ei pääse minnekään muualle kuin sinne, minne se on tarkoitettu.

Sallitut aktiviteetit: Vain tasolle yksi kommunikointi on sallittu ja prosessidatan tiedonsiirto, muita aktiviteettejä ei ole sallittu.

Sallitut tietoliikennetekniikat: Protokollat joita tarvitaan laitteiden välttämättömään kommunikoimiseen. Kaikki muu on kielletty.

Tietoväylät: Tietoväylät on määritelty erillisessä liitteessä.

Muutostenhallintaprosessi: Laitteiden toimittaja vastaa muutoksista. Mahdollisissa muutoksissa tulee ottaa huomioon laitteiden muuttuvat tietoturvauhkat. Muutokset eivät saa vaarantaa vyöhykkeen tietoturvaa ja muutokset on dokumentoitava tarkasti.

LIITE 3: VYÖHYKKEEN YKSI KUVAUS

Vyöhyke 1 kuvaus

Vyöhykkeen nimi: Vyöhyke yksi

Vyöhykkeen määritelmä: Vyöhykkeellä sijaitsee prosessin ohjauslaitteet.

Vyöhykkeen toiminnot: Prosessin ohjaus vyöhykkeen nolla kautta sekä hälytysten ja ohjauksen mahdollistaminen vyöhykkeelle kaksi.

Vyöhykkeen rajat: Vyöhyke pitää sisällään vain prosessin ohjauslaitteet.

Vyöhykkeen perimä: Vyöhyke perii ominaisuudet ohjausvyöhykkeeltä, sillä se on vyöhykkeen alivyöhyke. Täten kaikki määritelmät, jotka ovat ohjausvyöhykkeellä on myöskin tällä vyöhykkeellä, vaikka niitä ei ole erikseen tässä lueteltu.

Tyypilliset laitteet (luettelo suojattavista kohteista): Field Controller express (FCE), Field Controller (FC) ohjaimet.

Vyöhykkeen sisältämät riskit: Tason laitteisto on erittäin kriittinen prosessin toiminnan kannalta.

-Vyöhykkeen tietoturvakyky
Laitteet eivät osaa itse puolustautua hyökkäyksiä vastaan. Laitteiden luonnollinen tietoturvakyky on heikko.
-Vyöhykkeen uhkat ja haavoittuvuudet
Laitteiden käyttämien tekniikoiden heikkoudet.
-Tietoturvan murtumisen seuraukset
Tuotantolaitoksen pysähtyminen, henkilövahingot, suuret tappiot laitokselle.
-Tärkeys tuotantolaitoksen toiminnan kannalta
Erittäin kriittinen.

Pääsyvaatimukset ja valvontamenetelmät: Pääsy laitteisiin on rajattu palomuurilla tiettyihin portteihin ja IP-osoitteisiin perustuen. Poikkeuksena on vyöhykkeelle kaksi kommunikointi, jonne kaikki liikennöinti on sallittua. Fyysistä pääsyä vyöhykkeen laitteisiin valvotaan tehtaan porteilla.

Tietoturvastrategia: Palomuurit täytyy konfiguroida tarkasti IP-osoitteiden ja porttien osalta, jotta vyöhykkeen laitteita suojataan ja liikenne rajataan vain tiettyihin laitteisiin.

Valvottavat tietoturvatoimenpiteet: Varmistetaan palomuurien oikea konfiguraatio sekä laitteiden kaapeleiden kytkennät. Tarkkaillaan, että data ei pääse minnekään muualle, kuin sinne minne sen on tarkoitus päästä.

Sallitut aktiviteetit: Prosessin ohjaus ja luku vyöhykkeen nolla laitteiden kautta.

Sallitut tietoliikennetekniikat: Kaikki laitteiden toiminnan kannalta välttämättä vaaditut tekniikat ovat sallittu. Kaikki muu on kielletty.

Tietoväylät: Tietoväylät on määritelty erillisessä liitteessä.

Muutostenhallintaprosessi: Laitteiden toimittaja vastaa muutoksista. Mahdollisissa muutoksissa tulee ottaa huomioon laitteiden muuttuvat tietoturvauhkat. Muutokset eivät saa vaarantaa vyöhykkeen tietoturvaa ja muutokset on dokumentoitava tarkasti.

LIITE 4: VYÖHYKKEEN KAKSI KUVAUS

Vyöhyke 2 kuvaus

Vyöhykkeen nimi: Vyöhyke kaksi

Vyöhykkeen määritelmä: Vyöhykkeellä sijaitsee prosessin valvontalaitteisto sekä vyöhykkeen yksi kautta toimiva prosessin ohjaus.

Vyöhykkeen toiminnot: Operaattorin konsolit sekä hälytykset järjestelmästä (järjestelmän valvonta).

Vyöhykkeen rajat: Vyöhykkeen rajat on esitetty kuvassa 20.

Vyöhykkeen perimä: Vyöhyke perii ominaisuudet ohjausvyöhykkeeltä, sillä se on vyöhykkeen alivyöhyke. Täten kaikki määritelmät, jotka ovat ohjausvyöhykkeellä on myöskin tällä vyöhykkeellä, vaikka niitä ei ole erikseen tässä lueteltu.

Tyypilliset laitteet (luettelo suojattavista kohteista): Sovellusasemat, HMI-konsolit, PMD-palvelimet.

Vyöhykkeen sisältämät riskit:

-Vyöhykkeen tietoturvakyky
Vyöhykkeellä on hyvä tietoturvakyky, sillä laitteet pystyvät käyttäjien tunnistautumiseen käyttäjätunnuksen ja salasanan avulla sekä koneisiin voidaan asentaa tietoturvapäivityksiä sekä antivirus-ohjelmistoja.
-Vyöhykkeen uhkat ja haavoittuvuudet
Windowsin sisältämät haavoittuvuudet.
-Tietoturvan murtumisen seuraukset
Prosessin luvaton ohjaus ja muuntelu. Tuotannon katkokset, laitteiston vääränlainen toiminta.
-Tärkeys tuotantolaitoksen toiminnan kannalta
Tärkeä

Pääsyvaatimukset ja valvontamenetelmät: Käyttäjät joutuvat tunnistautumaan käyttäjätunnuksella ja salasanalla. Fyysistä pääsyä vyöhykkeen laitteisiin valvotaan tehtaan porteilla.

Tietoturvastrategia: Tietokoneisiin asennetaan virustorjunta-ohjelmistot sekä liikennettä valvotaan palomuurein. Myös Windows-pohjaiset tietokoneet päivitetään aina viimeisimpiin Honeywell Oy:n tarkistamiin tietoturvapäivityksiin.

Valvottavat tietoturvatoimenpiteet: Valvotaan, että viimeisimmät Honeywell Oy:n hyväksymät päivitykset ovat asennettu Windowsiin sekä antivirukseen. Varmistetaan palomuurin oikea konfiguraatio ja kaapeleiden kytkennät.

Sallitut aktiviteetit: Operaattorin käyttöliittymät ja siihen liittyvät varoitukset ja valvomotoiminnot.

Sallitut tietoliikennetekniikat: Sallitut tietoliikennetekniikat ovat melko laajat laitteiden vaatimien tekniikoiden takia. Sallittua on kaikki tekniikat, jotka liittyvät vyöhykkeen tarvittaviin toimintoihin ja aktiviteetteihin. Kaikki muu on kielletty. Esimerkiksi toimistopuolella olevat tekniikat kuten sähköposti ei ole sallittua tällä vyöhykkeellä.

Tietoväylät: Tietoväylät on määritelty erillisessä liitteessä.

Muutostenhallintaprosessi: Laitteiden toimittaja vastaa muutoksista. Mahdollisissa muutoksissa tulee ottaa huomioon laitteiden muuttuvat tietoturvauhkat. Muutokset eivät saa vaarantaa vyöhykkeen tietoturvaa ja muutokset on dokumentoitava tarkasti.

LIITE 5: HALLINTAVYÖHYKKEEN KUVAUS

Hallintavyöhykkeen kuvaus

Vyöhykkeen nimi: Hallintavyöhyke

Vyöhykkeen määritelmä: Vyöhyke sisältää laitteistot joilla hallinnoidaan vyöhykkeen kaksi laitteistoa sekä otetaan järjestelmästä varmuuskopiot.

Vyöhykkeen toiminnot: Vyöhykkeen kaksi palvelimien hallinnointi ja varmuuskopiointi.

Vyöhykkeen rajat: Vyöhyke sisältää vain vyöhykkeen kaksi hallinnointilaitteet sekä varmuuskopiopalvelimen ja sen ohjaimen.

Vyöhykkeen perimä: Vyöhyke perii ominaisuudet ohjausvyöhykkeeltä, sillä se on vyöhykkeen alivyöhyke. Täten kaikki määritelmät, jotka ovat ohjausvyöhykkeellä on myöskin tällä vyöhykkeellä, vaikka niitä ei ole erikseen tässä lueteltu.

Tyypilliset laitteet (luettelo suojattavista kohteista): Domaincontrolleri, varmuuskopioagentti, VMwaren hallinnointipalvelimet.

Vyöhykkeen sisältämät riskit:

-Vyöhykkeen tietoturvakyky
Vyöhykkeellä on hyvä tietoturvakyky, sillä laitteet ovat Windows- ja Linux-pohjaisia.
-Vyöhykkeen uhkat ja haavoittuvuudet
Windowsin ja Linuxin haavoittuvuudet. Active directoryn haavoittuvuudet.
-Tietoturvan murtumisen seuraukset
VMwaren hallinta päätyy kolmannelle osapuolelle, mikäli ihmiskäyttäjä pääsee tunkeutumaan vyöhykkeelle.
-Tärkeys tuotantolaitoksen toiminnan kannalta
Vyöhyke ei liity suorasti automaation toimintaan. Tuotanto jatkuu, vaikka taso menetettäisiin. Tärkeys on kohtalainen, koska laitteilta pystyy hallinnoimaan VMWaren laitteistoa, ja täten vaikuttamaan vyöhykkeen kaksi laitteistoon.

Pääsyvaatimukset ja valvontamenetelmät: Laitteiden käyttäjien täytyy tunnistautua kirjautumalla sisään käyttäjätunnuksella ja salasanalla. Fyysistä pääsyä vyöhykkeen laitteisiin valvotaan tehtaan porteilla.

Tietoturvastrategia: Asennetaan laitteille antivirus-ohjelmisto sekä päivitetään viimeisimmät Honeywell Oy:n tarkastamat Windowsin tietoturvapäivitykset. Laitteiden turhat käyttäjät ja palvelut poistetaan käytöstä.

Valvottavat tietoturvatoimenpiteet: Valvotaan, että viimeisimmät Honeywell Oy:n hyväksymät päivitykset ovat asennettu Windowsiin sekä antivirukseen.

Sallitut aktiviteetit: Varmuuskopioiden luominen sekä VMWaren hallinnointi.

Sallitut tietoliikennetekniikat: Laitteiden toimintaa edellyttävät tekniikat täytyy sallia kuten Network Time Protocol (ntp) ja etäyhteyksiä varten esimerkiksi Remote Desktop Protocol (rdp). Myös virustorjuntaohjelmistojen käyttämät tekniikat ovat sallittu. Kaikki muu on kielletty.

Tietoväylät: Tietoväylät on määritelty erillisessä liitteessä.

Muutostenhallintaprosessi: Laitteiden toimittaja vastaa muutoksista. Mahdollisissa muutoksissa tulee ottaa huomioon laitteiden muuttuvat tietoturvauhkat. Muutokset eivät saa vaarantaa vyöhykkeen tietoturvaa ja muutokset on dokumentoitava tarkasti.

LIITE 6: VYÖHYKKEEN KOLME KUVAUS

Vyöhyke 3 kuvaus

Vyöhykkeen nimi: Vyöhyke kolme

Vyöhykkeen määritelmä: Vyöhykkeellä sijaitsee laitteita, jotka tarvitsevat kommunikoida monelle eri vyöhykkeelle. Vyöhykkeen tarkoituksena on siirtää ja kerätä erilaista dataa eri vyöhykkeistä toisille.

Vyöhykkeen toiminnot: Historiadatan keruu, päivitysten jakelu.

Vyöhykkeen rajat: Vyöhykkeeseen sisältyy vyöhykkeen toimintoja suorittavat palvelimet, kuten PHD Collector-palvelin.

Vyöhykkeen perimä: Vyöhyke perii ominaisuudet ohjausvyöhykkeeltä, sillä se on vyöhykkeen alivyöhyke. Täten kaikki määritelmät, jotka ovat ohjausvyöhykkeellä on myöskin tällä vyöhykkeellä, vaikka niitä ei ole erikseen tässä lueteltu.

Tyypilliset laitteet (luettelo suojattavista kohteista): PHD Collector-palvelin, Windowsin ja antiviruksen päivitysten jakelupalvelimet.

Vyöhykkeen sisältämät riskit:

-Vyöhykkeen tietoturvakyky
Vyöhykkeellä on hyvä tietoturvakyky, sillä laitteet ovat Windows-pohjaisia palvelimia. Laitteet pystyvät käyttäjien tunnistautumiseen käyttäjätunnuksen ja salasanan avulla sekä koneisiin voidaan asentaa tietoturvapäivityksiä sekä virustorjunta-ohjelmistoja.

-Vyöhykkeen uhkat ja haavoittuvuudet
Windows-käyttöjärjestelmän sisältämät haavoittuvuudet ja uhat. Lisäksi taso joutuu kommunikoimaan laajalti myös suuren riskin sisältäville prosessilaitteistolle ja välittämään sieltä tietoa DMZ-vyöhykkeelle, joka tulee ottaa huomioon.

-Tietoturvan murtumisen seuraukset
Historiadatan joutuminen kolmannen osapuolen käsiin, haittaohjelmien levittäminen palvelimien kautta.

-Tärkeys tuotantolaitoksen toiminnan kannalta
Vyöhykkeen menetys ei keskeytä prosessin toimintaa, mutta joitain toimintoja kuten historiadata ja päivitysten jakelu menetetään, mikäli vyöhyke menetetään. Täten vyöhykkeen tärkeys on kohtalainen toiminnan kannalta.

Pääsyvaatimukset ja valvontamenetelmät: Laitteiden käyttäjien täytyy tunnistautua kirjautumalla sisään käyttäjätunnuksella ja salasanalla. Fyysistä pääsyä vyöhykkeen laitteisiin valvotaan tehtaan porteilla.

Tietoturvastrategia: Tietokoneisiin asennetaan virustorjunta-ohjelmistot sekä liikennettä rajoitetaan ja valvotaan palomuurein. Myös Windows-pohjaiset tietokoneet päivitetään aina viimeisimpiin tietoturvapäivityksiin. Turhat palvelut ja ylimääräiset käyttäjät poistetaan palvelimilta käytöstä.

Valvottavat tietoturvatoimenpiteet: Valvotaan, että palvelimissa on viimeisimmät Honeywell Oy:n hyväksymät Windowsin päivitykset sekä virustorjuntaohjelman päivitykset ovat ajan tasalla.

Sallitut aktiviteetit: Historiadatan keruu, päivitysten jakelu.

Sallitut tietoliikennetekniikat: PHD Collectorin ja päivitysten jakelijoiden tarvitsemat tekniikat. Muut tekniikat ovat kielletty.

Tietoväylät: Tietoväylät on määritelty erillisessä liitteessä.

Muutostenhallintaprosessi: Laitteiden toimittaja vastaa muutoksista. Mahdollisissa muutoksissa tulee ottaa huomioon laitteiden muuttuvat tietoturvauhkat. Muutokset eivät saa vaarantaa vyöhykkeen tietoturvaa ja muutokset on dokumentoitava tarkasti.

LIITE 7: DMZ-VYÖHYKKEEN KUVAUS

DMZ-vyöhyke kuvaus

Vyöhykkeen nimi: DMZ-vyöhyke

Vyöhykkeen määritelmä: Vyöhyke toimii ohjausvyöhykkeen ja yritysvyöhykkeen välisenä vyöhykkeenä, jonka kautta kaikki näiden kahden vyöhykkeen välinen liikenne kulkee.

Vyöhykkeen toiminnot: Vyöhykkeen toimintoihin kuuluu erilaiset hyppypalvelimet sekä mm. historiadatan tarjoaminen yritystason vyöhykkeeseen.

Vyöhykkeen rajat: Vyöhykkeeseen kuuluu vain DMZ-vyöhykkeen palvelimet.

Tyypilliset laitteet (luettelo suojattavista kohteista): PHD Shadow-palvelin (historiadata), RDS-hyppypalvelin (etäyhteydet), erilaisia palvelimia jotka palvelevat vyöhykkeen käyttötarkoitusta.

Vyöhykkeen sisältämät riskit:

-Vyöhykkeen tietoturvakyky
Vyöhykkeellä on hyvä tietoturvakyky, sillä laitteet ovat Windows-pohjaisia palvelimia. Laitteet pystyvät käyttäjien tunnistautumiseen käyttäjätunnuksen ja salasanan avulla sekä koneisiin voidaan asentaa tietoturvapäivityksiä sekä virustorjunta-ohjelmistoja.
-Vyöhykkeen uhkat ja haavoittuvuudet
Taso on osalti avoinna yritystason vyöhykkeen kautta internettiin. Uhkina on Windows-käyttöjärjestelmien haavoittuvuudet.
-Tietoturvan murtumisen seuraukset
Tunkeutujan mahdollinen pääsy syvemmälle automaatioon, yhteyksien menetys ohjausvyöhykkeen ja yritystason vyöhykkeen välillä.
-Tärkeys tuotantolaitoksen toiminnan kannalta
Tästä vyöhykkeestä riippuu esimerkiksi etäyhteydet ja virustorjuntaohjelmistojen määrittelyt. Tärkeys tuotantolaitoksen kannalta on kohtalainen. Vyöhykkeen menetys ei kuitenkaan keskeytä tuotantoa.
-Vyöhykkeen tavoitteena oleva tietoturvataso
Jos käytetään asteikkoa alhainen, keskinkertainen ja korkea, niin tämän vyöhykkeen tavoite olisi keskinkertainen perustuen vyöhykkeen riskeihin sekä toimintoihin.

Valtuutettu teknologia: Mikäli vyöhykkeen hyväksyttyihin teknologioihin kuten tietoliikennetekniikoihin tehdään mahdollisista muutoksia liiketoiminnan tarpeen täyttämiseksi, täytyy sen vaikutus vyöhykkeen toimintaan ja riskeihin arvioida. Pääasiassa valtuutettua teknologiaa on vain tässä dokumentissa mainitut tekniikat sekä laitteet, jotka käyttävät näitä tekniikoita.

Pääsyvaatimukset ja valvontamenetelmät: Vyöhykkeelle päästäkseen täytyy käyttäjän todentaa itsensä käyttäjätunnuksella ja salasanalla. Tehtaan ulkopuolelta tulevat etäyhteydet täytyy kulkea salattua tekniikkaa sekä kaksivaihesta tunnistautumista käyttäen. Fyysistä pääsyä vyöhykkeen laitteisiin valvotaan tehtaan porteilla.

Tietoturvastrategia: Tietokoneisiin asennetaan virustorjunta-ohjelmistot sekä liikennettä valvotaan palomuurein. Myös Windows-pohjaiset tietokoneet päivitetään aina viimeisimpiin tietoturvapäivityksiin. Palvelimien turhat palvelut ja käyttäjät poistetaan käytöstä.

Valvottavat tietoturvatoimenpiteet: Valvotaan, että viimeisimmät päivitykset on asennettu käyttöjärjestelmiin sekä antivirus-ohjelmistoihin.

Sallitut aktiviteetit: Sallittuihin aktiviteetteihin kuuluu vain toiminnot, jotka liittyvät tiedon välitykseen yritysvyöhykkeen ja ohjausvyöhykkeen välillä.

Sallitut tietoliikennetekniikat: Sallittuja tietoliikennetekniikoita on PHD Shadow-palvelimen tarvitsemat portit, RDP-yhteydet sekä virustorjunnan ja Windowsin jakelupäivityksien tarvitsemat portit. Kaikki muu on kielletty. Portteja ja tekniikoita, joita yleensä käytetään hyökkäyksiin ei ole sallittu.

Tietoväylät: Tietoväylät on määritelty erillisessä liitteessä.

Muutostenhallintaprosessi: Laitteiden toimittaja vastaa muutoksista. Mahdollisissa muutoksissa tulee ottaa huomioon laitteiden muuttuvat tietoturvauhkat. Muutokset eivät saa vaarantaa vyöhykkeen tietoturvaa ja muutokset on dokumentoitava tarkasti.

LIITE 8: YRITYSTASON VYÖHYKKEEN KUVAUS

Yritystason vyöhyke kuvaus

Vyöhykkeen nimi: Yritystason vyöhyke

Vyöhykkeen määritelmä: Vyöhykkeellä sijaitsee tuotantolaitoksen yritystason järjestelmät.

Vyöhykkeen toiminnot: Toimintoihin kuuluu normaalit toimistotoiminnot, kuten sähköposti ja tulostus yms.

Vyöhykkeen rajat: Vyöhyke rajoittuu niiden laitteiden mukaan, jotka suorittavat yritystason toimintoja. Laitteet tulee olla omassa verkossa eristettynä automaatiosta, pois lukien DMZ-vyöhykkeen kautta kulkevat yhteydet.

Tyypilliset laitteet (luettelo suojattavista kohteista): Käyttäjien toimistotietokoneita, erilaisia palvelimia sekä tulostimia.

Vyöhykkeen sisältämät riskit:

-Vyöhykkeen tietoturvakyky
Vyöhykkeen sisältämillä laitteilla on yleensä hyvä luontainen tietoturvakyky. Laitteet ovat yleensä Windows-pohjaisia laitteita, ja ne pystyvät käyttäjän tunnistukseen sekä ajamaan esimerkiksi virustorjunta-ohjelmistoja.
-Vyöhykkeen uhkat ja haavoittuvuudet
Windowsin ja tulostimien sisältämät haavoittuvuudet. USB-tikkujen sekä sähköpostin välityksellä kulkeutuvat haittaohjelmistot.
-Tietoturvan murtumisen seuraukset
Toimistoverkon epävakaa toiminta, salasanojen yms. tietojen urkinta, mahdollisesti hyökkääjän pääsy etenemään DMZ-tasolle ja automaatioon.
-Tärkeys tuotantolaitoksen toiminnan kannalta
Mikäli vyöhyke menetetään, osa palveluista menetetään kuten raportointi alueen tuotannosta, mutta tuotanto ei kuitenkaan keskeydy. Täten vyöhykkeen tärkeys ei ole merkittävä tuotantolaitoksen toiminnan kannalta.
-Vyöhykkeen tavoitteena oleva tietoturvataso
Jos käytetään asteikkoa alhainen, keskinkertainen ja korkea, niin tämän vyöhykkeen tavoite olisi alhainen vyöhykkeen riskien ja tärkeyden perusteella.

Valtuutettu teknologia: Mikäli vyöhykkeen hyväksyttyihin teknologioihin kuten tietoliikennetekniikoihin tehdään mahdollisia muutoksia liiketoiminnan tarpeen täyttämiseksi, täytyy sen vaikutus vyöhykkeen toimintaan ja riskeihin arvioida. Pääasiassa valtuutettua teknologiaa on vain tässä dokumentissa mainitut tekniikat sekä laitteet, jotka käyttävät näitä tekniikoita.

Pääsyvaatimukset ja valvontamenetelmät: Pääsy tälle vyöhykkeelle rajoittuu tehtaan työntekijöihin sekä etäyhteyksiin, jotka tulevat vyöhykkeeseen tehtaan ulkopuolelta. Pääsyä tulee valvoa ainakin käyttäjän tunnistautumisella joko fyysisesti tai etäkäyttäjien todennuksella.

Tietoturvastrategia: Tietokoneisiin asennetaan antivirus-ohjelmistot sekä liikennettä DMZ-tasolle sekä internettiin valvotaan palomuurein. Myös Windows-pohjaiset tietokoneet päivitetään aina viimeisimpiin tietoturvapäivityksiin.

Valvottavat tietoturvatoimenpiteet: Valvotaan, ettei vyöhykkeellä esiinny ulkopuolisia tunkeutujia eikä viruksia. Valvotaan, että viimeisimmät tietoturvapäivitykset on aina asennettu.

Sallitut aktiviteetit: Vyöhykkeellä on sallittu toimistokäyttöön liittyviä aktiviteettejä, kuten sähköpostin sekä internetin käyttö. Aktiviteetteihin kuuluu myös mm. prosessissa olevien materiaalien määrää kuvaavien tiedostojen ja kokonaisenergiankulutuksen kerääminen ja ylläpitäminen sekä tehtaan perustuotantosuunnitelman laatiminen. Kaikki muunlainen toiminta on kielletty.

Sallitut tietoliikennetekniikat: Automaatioprotokollia ei ole missään tapauksessa sallittua päästää tälle tasolle. Sallittua on vain normaalit toimistokäyttöön tarvittavat protokollat. Kaikki muu on kielletty.

Tietoväylät: Tietoväylät on määritelty erillisessä liitteessä.

Muutostenhallintaprosessi: Laitteiden toimittaja tai tuotantolaitoksen tähän määrätty organisaatio vastaa muutoksista. Mahdollisissa muutoksissa tulee ottaa huomioon laitteiden muuttuvat tietoturvauhkat. Muutokset eivät saa vaarantaa vyöhykkeen tietoturvaa ja muutokset on dokumentoitava tarkasti.

LIITE 9: TIETOVÄYLIEN KUVAUKSET

Tietoväylien kuvaukset:

”Molempiin suuntiin” meinaa tässä dokumentissa sitä, että jos vyöhyke A saa kommunikoida vyöhykkeelle B, niin myös vyöhyke B saa kommunikoida vyöhykkeelle A.

Tietoväylä 1:

Seuraavien vyöhykkeiden välinen kommunikointi on sallittua käyttäen tätä tietoväylää:

-Vyöhyke yksi saa kommunikoida vyöhykkeelle nolla molempiin suuntiin.

Tietoväylän tietoturvallisuusominaisuudet ovat heikot automaatioprotokollien sekä minkäänlaisen todennuksen tai palomuurin puuttumisen vuoksi.

Tietoväylä 2:

Seuraavien vyöhykkeiden välinen kommunikointi on sallittua käyttäen tätä tietoväylää:

Vyöhyke yksi saa kommunikoida (molempiin suuntiin):
-vyöhykkeelle kaksi ilman rajoituksia
-vyöhykkeelle kolme hyvin rajoitetusti

Vyöhyke kaksi saa kommunikoida (molempiin suuntiin):
-Vyöhykkeelle yksi ilman rajoituksia
-Vyöhykkeelle kolme rajatusti
-DMZ-vyöhykkeelle rajatusti

Tietoväylän tietoturvallisuusominaisuudet ovat kohtalaiset. Vyöhykkeet sisältävät tietoturvaominaisuuksiltaan eritasoisia laitteita, joka vaikuttaa ominaisuuksiin. Rajoitetuissa yhteyksissä sallitut protokollat ovat vain laitteiden käyttämät protokollat, jotka ovat välttämättömiä laitteiden toiminnan kannalta.

Tietoväylä 3:

Seuraavien vyöhykkeiden välinen kommunikointi on sallittua käyttäen tätä tietoväylää:

Hallintavyöhyke saa kommunikoida palomuurin kautta rajatusti (molempiin suuntiin):
-DMZ-vyöhykkeelle
-Vyöhykkeelle numero kolme
-Vyöhykkeelle numero kaksi

Tietoväylän tietoturvataso on hyvä palomuurien ja laitteiden luonnollisen tietoturvakyvyn ansiosta. Sallitut protokollat ovat vain laitteiden käyttämät protokollat, jotka ovat välttämättömiä laitteiden toiminnan kannalta.

Tietoväylä 4:

Seuraavien vyöhykkeiden välinen kommunikointi on sallittua käyttäen tätä tietoväylää:

Vyöhyke numero kolme saa kommunikoida palomuurin kautta rajatusti (molempiin suuntiin):
-Vyöhykkeelle numero yksi
-Vyöhykkeelle numero kaksi
-DMZ-vyöhykkeelle

Tietoväylän tietoturvallisuus on hyvä, sillä laitteet osaavat käyttää todennusta ja liikenne kulkee palomuurin läpi. Sallitut protokollat ovat vain laitteiden käyttämät protokollat, jotka ovat välttämättömiä laitteiden toiminnan kannalta.

Tietoväylä 5:

Seuraavien vyöhykkeiden välinen kommunikointi on sallittua käyttäen tätä tietoväylää:

DMZ-vyöhyke saa kommunikoida palomuurin kautta rajatusti (molempiin suuntiin):

-Yritystason vyöhykkeelle
-Vyöhykkeelle numero kaksi
-Vyöhykkeelle numero kolme
-Hallintavyöhykkeelle

Sallitut protokollat ovat vain laitteiden käyttämät protokollat, jotka ovat välttämättömiä laitteiden toiminnan kannalta. Tietoväylän tietoturvallisuusominaisuudet ovat hyvät laitteiden tietoturvakyvyn sekä palomuurin ansiosta.

Tietoväylä 6:

Seuraavien vyöhykkeiden välinen kommunikointi on sallittua käyttäen tätä tietoväylää:

Yritystason vyöhyke saa kommunikoida palomuurin kautta rajatusti (molempiin suuntiin):

-DMZ-vyöhykkeelle

Tietoväylän tietoturvallisuusominaisuudet ovat hyvät laitteiden tietoturvakyvyn sekä palomuurin ansiosta. Sallitut protokollat ovat vain laitteiden käyttämät protokollat, jotka ovat välttämättömiä niiden toiminnan kannalta. Protokollia tai palveluita, joita käytetään yleensä hyökkäyksiin ei tule sallia missään tapauksessa.