Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Aki Halmesmäki

Älykäs ilmastointiratkaisu teollisuuden toimistoihin

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Talotekniikka
Insinöörityö
26.04.2019

Tekijä Otsikko Sivumäärä Aika	Aki Halmesmäki Älykäs ilmastointiratkaisu teollisuuden toimistoihin 141 sivua + 33 liitettä 26.04.2019
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	talotekniikka
Ammatillinen pääaine	LVI-suunnittelu
Ohjaajat	ryhmäpäällikkö TkK Juhani Suihkonen automaatioinsinööri ins. Teemu Holopainen lehtori Jarmo Tapio

Opinnäytetyössä keskityttiin langattomien ilmanvaihtoratkaisutoimittajien kartoittamiseen Suomen markkinoilla sekä tarpeenmukaisen ilmanvaihdon soveltuvuutta teollisuuden eri tiloihin. Keskeiseksi ilmanvaihtojärjestelmäksi opinnäytetyössä nousi Swegonin uuden sukupolven Wise-järjestelmä, johon opinnäytetyössä keskityttiin tarkemmin.

Swegonin uuden sukupolven Wise-järjestelmän soveltuvuusarvioinnissa keskeiseksi arviointikriteeriksi nousi esiin järjestelmään liittyvä langaton tiedonsiirto, antureiden ja toimilaitteiden IoT-tekniikka, tieto- ja kyberturvallisuus sekä Wise-järjestelmään liittyvä integrointi teollisuuden ohjausjärjestelmään. Swegonin uuden sukupolven Wise-järjestelmä on ensimmäisiä Suomessa markkinoitavia sekä tarpeenmukaista ilmanvaihtoa että esineiden internetiä hyödyntävä ratkaisu.

Lisäksi työssä käsiteltiin sisäilmastoon liittyviä kriteereitä, koska Swegon toi ensimmäisenä ilmanvaihtojärjestelmien kokonaistoimittajana VOC-anturit sisäilman laatua mittaaviksi antureiksi normaaleihin toimisto- ja toimitilakiinteistöihin. Myös järjestelmään liittyviä ohjaustoimintoja, energiansäästö ja kustannusetuja käsiteltiin tässä insinöörityössä selvittämään järjestelmän liittyviä kokonaisetuja.

Insinöörityössä laadittiin myös ohjeet automaatiosuunnittelijalle Swegonin Wise-järjestelmään liittyen. Ohjeet laadittiin pääosin automaation kyberturvastandardia 62443 noudattaen sekä yrityksen (Pöyry) tietoturvaohjeita, joita on tarkoitus päivittää myöhemmin uudelleen, kun kyseistä standardisarjaa ja automaation tietoturvaa koskevia standardeja päivitetään Seskon ja Suomen standardoimisliiton toimesta.

Avainsanat	tarpeenmukainen ilmanvaihto, langaton tiedonsiirto, kyberturva

Author Title Number of Pages Date	Aki Halmesmäki Intelligent air conditioning solution for industrial offices 141 pages + 33 appendices 26 April 2019
Degree	Bachelor of Engineering
Degree Programme	Building Services
Professional Major	HVAC engineering
Instructors	Group Manager B.Sc. Juhani Suihkonen Automation engineer eng. Teemu Holopainen Senior lecturer Jarmo Tapio

The thesis focused on mapping wireless ventilation solution providers in the Finnish market and the suitability of demand-controlled ventilation for various industrial premises. The central ventilation system in the thesis was the Swegon New Generation Wise system, which was more closely focused on in the thesis.

The Swegon New Generation Wise system's suitability assessment was based on the introduction of system-related wireless communication, IoT technology for sensors and actuators, cybersecurity, and Wise integration with the industrial control system. Swegon's next-generation Wise system is the first solution in Finland that utilizes both need-based ventilation and the Internet of Things.

In addition, the work focused on indoor climate criteria, as Swegon was the first supplier of ventilation systems to deliver VOC sensors for indoor air quality sensors in normal office and commercial properties. System-related control functions, energy saving, and cost benefits were also addressed in this engineering work to determine the overall benefits of the system.

In the bachelor's thesis, there were also instructions for the automation designer Swegon Wise. The instructions were mainly drafted in accordance with the automation cyber security standard 62443 and the company (Pöyry) security guidelines, which are to be updated later when the standards and automation security standards are updated by Sesko and the Finnish Standardization Association.

Keywords	Demand Controlled Ventilation, Wireless, Cyber Security

Sisällys

Liitteet 33 sivua

Liite 1. Standardien SFS-EN 62443-3-3 ja 62443-4-1 mukaiset automaation verkkoympäristön suojaustasovaatimukset

Liite 2. IoT-laitteita koskevan tietoturvan parhaat käytännöt tehdasympäristössä

Liite 3. Simuloinnilla apua IoT-verkkojen tietoturvaan

Liite 4. Eri hakupalveluilla tehty tietoturvakartoitus Wise-järjestelmään liittyen

Liite 5. Ohjeet automaatiosuunnittelijalle

Liite 6. Esimerkki tarpeenmukaisen ilmanvaihtojärjestelmän kannattavuuslaskennasta DFC-menetelmällä

Liite 7. VOC-yhdisteiden vaikutus toimistojen sisäilman laatuun

Lyhenteet

6LoWPAN	Lyhenne: 6th low energy WPAN. Langaton tietoverkkoprotokolla, joka pohjautuu teknisen standardin IEEE 802.15.4 mukaiseen alhaisen tason langattoman PAN-verkkomääritykseen. Yleinen verkkoprotokolla IoT-laiteverkoissa. Kts. WPAN.
CO_2	Lyhenne: Carbon dioxide, hiilidioksidi (hiilihapon anhydridi); ilmaa raskaampi kaasu, jota muodostuu palamisen yhteydessä.
DCS	Lyhenne: Distributed Control System. Automaatiojärjestelmä, jolla kuvataan yleisesti järjestelmää, jossa on suuri määrä ohjaussilmukoita.
DCSV	Lyhenne: Demand Controlled. Tarpeenmukaiset sisäilmasto-olosuhteet. Ottaa huomioon ilmanvaihdon lisäksi tarpeenmukaisen lämmityksen, jäähdytyksen, valaistuksen ja ääniolosuhteet.
DCV	Lyhenne: Demand Controlled Ventilation. Tarpeenmukainen ilmanvaihto.
DDS	Lyhenne: Data Distribution Service. Tiedon avoimeen välitykseen keskittyvä automaatiojärjestelmä. Automaatiojärjestelmä, jolla kuvataan yleisesti järjestelmää, joka on tarkoitettu tiedon välityspalveluna esim. SCADA-järjestelmä.
DMZ	Lyhenne: DeMilitarized Zone. Ei kenenkään maa, tietoliikennetekniikassa käytetty malli, jolla kuvataan palomuurein eristettyä verkonosaa, joihin voidaan myös eristää esim. erilaisia kriittisiä historia- ja palautusservereitä.
Edge-palvelu	Lyhenne: Edge Computing Service. Pilvipalvelusovellus reunapalveluna, joka on tarkoitettu tiedon nopeampaa laskentaprosessointia varten ja voi toimia sumupalvelun tavoin ajantasaisen tiedon siirtäjänä ja varastoijana pilvipalvelun ja käyttäjän välillä.

IaaS	Lyhenne: Infrastucture as a Service. Infrastruktuuri palveluna tarkoittaa yleistä pilvipalvelutyyppiä ns. konttipalveluna, jossa asiakas itse vastaa pilvipalvelusovellusten rakentamisesta, päivityksistä, tietoturvasta ja hallinnoinnista täysin itse ja saa palveluna ainoastaan infrastruktuurin, kuten serverit pilvipalvelun toteuttamiseksi.
ICS	Lyhenne: Industrial Control System. Yleinen nimitys erityyppisille teollisuuden ohjausjärjestelmille.
IIoT	Lyhenne: Industrial Internet of Things. Teollinen esineiden internet, jolla kuvataan älykästä anturiteknologiaa hyödyntäviä verkkoja teollisuudessa, joissa kulkee suuri määrä tietoa eri sovellusten käsiteltäväksi. Usein yhteydessä erilaisiin pilvipalveluihin, joissa suoritetaan pilvilaskentaa tiedon analysointiin.
IMS	Lyhenne: Ilmamäärän säädin. Säädin jolla pyritään muuttuvailmavirtaisessa ilmanvaihtojärjestelmässä aikaansaamaan muuttuva ilmavirta tietyssä tilassa.
VAV/MIV	Lyhenne: Variable Air Volume. Muuttuva ilmavirta. Lyhenne, jolla kuvataan yleisesti muuttuvailmavirtajärjestelmiä.
IoT	Lyhenne: Internet of Things. Esineiden internet, jolla kuvataan älykästä anturiteknologiaa hyödyntäviä verkkoja, joissa kulkee suuri määrä tietoa eri sovellusten käsiteltäväksi. Usein yhteydessä erilaisiin pilvipalveluihin, joissa suoritetaan pilvilaskentaa tiedon analysointiin.
IPSec	Lyhenne: Internet Protocol Security. Tietoturvaprotokolla, joka on käytössä IPv6-protokollan yhteydessä suojaamaan yhteyksiä laitteiden ja reitittimien välillä.
LAN	Lyhenne: Local Area Network. Langallinen verkkoprotokolla, jolla kuvataan rajoitetulla maantieteellisellä alueella, usein kiinteistön sisällä, toimivaa tietoliikenneverkkoa.

MESH-verkko	Fyysinen verkkotopologia, joka voi olla toteutettu *ad hoc* tai yhdistettynä tähti-puu-topologiana. Usein puhutaan myös peer-to-peer-verkosta, jolla tarkoitetaan *ad hoc* -tyyppistä topologiaa, jossa kaikki laitteet toimivat reitittiminä ja välittävät tiedon toistensa välillä tietoverkossa.
Modbus	Modiconin vuonna 1979 julkaisema sarjaliikenneprotokolla, joka oli tarkoitettu käytettäväksi Modiconin ohjelmoitavien logiikkojen (PLC) kanssa. Protokollasta on muodostunut *de facto* -standardi teollisuudessa, ja on nyt yleisesti käytössä elektroniikkalaitteiden välisessä kommunikoinnissa.
openVPN	Lyhenne: open Virtual Private Network. Avoimeen lähdekoodiin perustuva yksityiseen virtuaaliseen verkkoon perustuva protokolla, jonka tarkoitus on lisätä tietoturvaa VPN-protokollan haavoittuvuuksia.
PaaS	Lyhenne: Platform as a Service. Yleinen pilvipalvelutyyppi, jossa asiakas saa ohjelmistoalustan ja asiakkaan vastuulle jää valmiin ohjelmistoalustan hallinnointi ja tietoturva. Toimittaja vastaa laitetason servereiden hallinnoinnista ja tietoturvasta.
Palomuuri	Fyysinen laite tai ohjelmistopohjainen sovellus, joka suodattaa liikennettä verkosta sisään ja ulkosuuntaan. Työasemapohjainen palomuuri suojaa yksittäistä työasemaa haitalliselta tietoliikenteeltä ja verkkopalomuuri suojelee koko verkkoa haitalliselta liikenteeltä.
Pilvilaskenta	Pilvilaskennalla (cloud computing) tarkoitetaan tietoteknisten palveluiden hajautusta ja ulkoistusta. Pilvilaskenta liittyy internetissä tapahtuvaan tietotekniikan kehitykseen, josta käytetään usein nimitystä laskenta, ja tiedon käyttöön hajautetuissa ympäristöissä.
Pilvipalvelu	Cloud Service. Pilvipalvelua käytetään yleisesti kielikuvana erillisten tietokoneiden tai virtuaalikoneiden muodostamasta hajautetusta pilvilaskentapalvelusta. Palveluiden toteutus perustuu laajalti API (Application Programming Interface, ohjelmointirajapinta) -toteutuksiin ja palvelun käyttämä verkko voi olla joko julkinen pilvi, yksityinen pilvi tai luotettu pilvi perustuen eri palvelutyyppeihin ks. SaaS, PaaS ja IaaS.

Reititin	Reititin on laite tai tietokone, jonka tarkoitus on yhdistää eri verkkosegmentit toisiinsa, esimerkiksi kodin LAN-verkon reititys Internet-verkkoon. Reitittimiä on nykyään saatavilla myös reititin-palomuuriyhdistelminä.
SaaS	Lyhenne: Software as a Service. Yleinen pilvipalvelutyyppi, jossa asiakas saa koko pilvipalveluun liittyvän valmiin ohjelmiston. Toimittaja vastaa koko pilvipalveluun liittyvän ohjelmistoalustan ja infrastruktuuritason servereiden hallinnoinnista ja tietoturvasta ja asiakkaan vastuulle jää ainoastaan ohjelmistotason päivityksistä.
SNMP	Lyhenne Simple Network Management Protocol, yksinkertainen verkon hallinnointi protokolla. Yleisesti IoT-verkoissa käytössä oleva ja TCP/IP-verkkojen hallinnoinnissa käytettävä tietoliikenneprotokolla. Protokollan avulla voidaan kysellä verkossa olevan laitteen tilaa tai laite voi itsenäisesti antaa hälytyksiä.
Sumupalvelu	Fog Computing. Palvelutyyppi, jota käytetään erilaisten teollisuuden IoT-verkkojen Big Datan hallinnointiin ja laskentaan sumulaskennan avulla. Sumulaskennassa käytetyt menetelmät voivat erota pilvilaskennassa käytetyistä menetelmistä. Sumupalvelu toimii yleisesti ns. etäisen esim. yritystason pilvipalvelun tiedon siirtäjänä lähemmäksi käyttäjää. Edge-palvelun tavoin sumupalvelu on tarkoitettu myös tiedon nopeampaa laskentaprosessointia varten.
TCP/IP	Lyhenne: Transmission Control Protocol / Internet Protocol. TCP/IP on usean Internet-liikennöinnissä käytettävän tietoliikenneprotokollan yhdistelmä. ISOn OSI-mallin mukaisesti IP-protokolla on alemman tason protokolla, joka vastaa päätelaitteiden osoitteistamisesta ja pakettien reitittämisestä verkossa.
UDP	Lyhenne: User Datagram Protocol. UDP on ns. yhteydetön protokolla, joka ei vaadi yhteyttä laitteiden välille, mutta mahdollistaa tiedostojen siirron. UDP eroaa TCP:stä monin tavoin. Muun muassa paketin perillemenoa ei varmisteta päästä päähän ja alempi verkkokerrostaso varmistaa

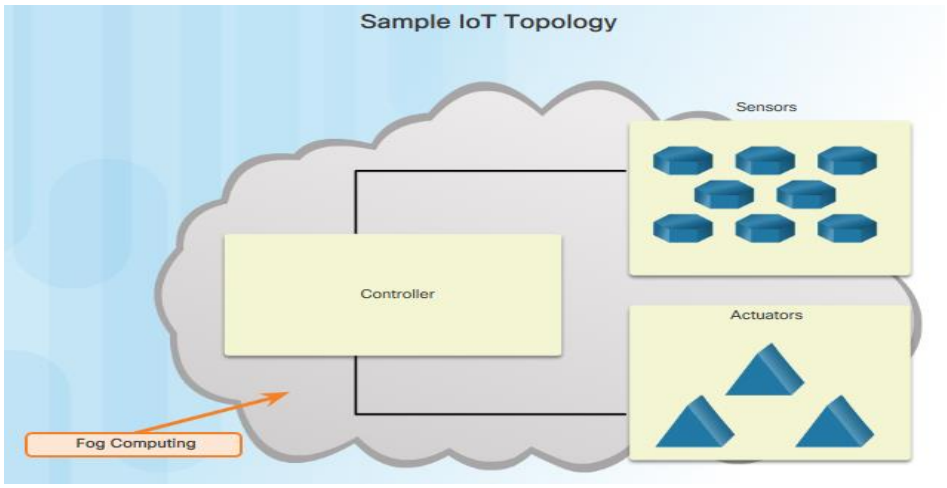
	pakettien lähetyksen seuraavaan solmuun asti. UDP:tä käytetään esimerkiksi DNS-pyyntöjen lähettämiseen. UDP:n yleisrasite on pienempi kuin TCP:n, siinä ei suoriteta alkukättelyä, pakettien kuittausta eikä yhteyden lopettamista. UDP-protokollaa käytetään nykyään useissa kodin IoT-verkkolaitteissa, joka tekee siitä erityisen haastavan tietoturvan kannalta.
WLAN	Lyhenne. Wireless LAN. Langatonta tiedonsiirtoa hyödyntävä verkkoprotokolla, joka on yleisesti käytössä langattomassa tiedonsiirrossa. Verkon kantomatka ja maksimiyhteysnopeudet vaihtelevat riippuen mihin WLAN-standardin IEEE 802.11 versioon kyseinen verkkototeutus kuuluu.
WPAN	Lyhenne (Wireless Personal Area Network) tarkoittaa langatonta lähiverkkoa, joka on kantomatkaltaan lyhyempi kuin WLAN.
VOC	Lyhenne: Volatile Organic Compounds. Haitallisten orgaanisten yhdisteiden määrä, jonka avulla mitataan eri tiloissa olevien haitallisten orgaanisteiden esiintymispitoisuutta. Mittaus voidaan suorittaa kokonaisarvoina eli TVOC-arvoina tai yksittäisten yhdisteiden huippuarvoina (VOC-arvoina) tietyn mittausjakson aikana.
VPN	Lyhenne: Virtual Private Network. Yksityinen verkkoprotokolla, joka on yleisesti käytössä teollisessa internetissä, jossa ehkäistään verkon pakettien skannaamista julkisesta verkosta. VPN protokollan mukaisissa verkkoarkkitehtuureissa IP-paketteja kuljetetaan toisten IP-pakettien sisällä tiedon salaamiseksi.

1 Johdanto

Tämä insinöörityö toteutettiin Pöyry Finland Oy:n toimesta ja tämän insinöörityön tarkoituksena oli tehdä kartoitusta Suomen markkinoilla olevista älykkäistä tarpeenmukaisista ilmanvaihtoratkaisuista. Älykkäällä teknologialla toteutetut laitteet ja ohjelmat hyödyntävät langattomien antureiden avulla älykästä teknologiaa talotekniikan prosessien automatisointiin. Nämä prosessit tarjoavat energiatehokkaita valaistus, lämmitys, ilmanvaihto ja turvallisuusratkaisuja. Esimerkkinä älykästä teknologiaa hyödyntävät rakennukset voivat vähentää energiakustannuksia käyttämällä antureita, jotka tunnistavat kuinka monta ihmistä on huoneessa ja säätävät lämmitystä ja ilmastointia tarpeen mukaisesti. Tekoälyyn- ja koneoppimiseen perustuvat laitteet ja ohjelmat ovat älykkäitä laitteita monimutkaisempia ja hyödyntävät eri tilanteeseen mukautuvaa ohjelmointia, jota kutsutaan yleisesti keinoälyksi. Tekoälyyn- ja koneoppimiseen perustuvat laitteet ja ohjelmat eivät tarvitse toimiakseen ympäristöstä tulevia signaaleja, joihin älykkäät järjestelmät nojautuvat erilaisilla älykkäillä antureilla toteutetuilla laitteilla ja ohjaimilla. [1]

Tässä insinöörityössä keskityttiin älykkäitä IoT-antureita ja -laitteita hyödyntävään Swegonin uuden sukupolven Wise -järjestelmään. IoT (Internet of Things) eli esineiden internet tarkoittaa yleisesti miljoonia älykkäitä laitteita ja antureita, jotka ovat kytkettynä Internettiin ja jotka keräävät ja jakavat tietoa verkon laitteille ja antureille käyttöä ja arviointia varten. IoT-verkoissa olevat anturit ja laitteet muodostavat verkkotopologian eli verkon fyysisen rakenteen, josta on esitetty esimerkki kuvassa 1. Kuvassa 1 anturit (sensors) ovat kytkeytyneenä verkkoon tiedonkeruuta ja tiedonjakamista varten. Tämä vaatii laitteiston kytkentää Internettiin langallisesti tai kytkentää langattomasti ohjainyksikölle. Laitteiston ohjaimet ovat vastuussa tiedon keräämisestä antureilta ja verkon tarjoamisesta tai Internetiin kytkeytymisestä. Älykkäissä järjestelmissä ohjaimilla on kyky tehdä välittömiä päätöksiä tai ne voivat lähettää tiedon tehokkaamman tietokoneyksikön käsiteltäväksi, joka on samaan verkkoon kytkeytynyt kuin ohjainlaite tai sillä voi olla ainoastaan pääsy Internetin kautta ohjaimeen. Anturiverkossa on älykkäissä järjestelmissä usein kytkeytyneenä toimilaitteita, jotka muuttavat sähköisen panoksen (Input) fyysiseksi tuotokseksi (Output). Esimerkkinä anturin havaittua alilämpöä huoneessa, se lähettää

lämpötilalukeman ohjaimen mikrokontrollerille, joka lähettää ohjauskäskyn toimilaitteelle ilmastoinnin sisään puhalluslämpötilan nostamiseksi. [1]



Kuva 1. Esimerkki IoT:n fyysisestä verkkorakenteesta [1]

Nykyisin suurin osa uusista IoT-laitteista vaativat langatonta tekniikkaa ja koska monet anturit ovat ulkona tai fyysisesti hankalissa paikoissa, niin anturit ovat paristokäyttöisiä tai aurinkoenergialla toimivia ja tällöin harkintaa joudutaan käyttämään arvioitaessa antureiden energiankulutusta. Alhaisen energiakulutuksen vaativia antureita tulee käyttää optimoitaessa ja laajennettaessa antureiden mahdollisuutta toimia ja olla saatavilla hankalissakin ympäristöissä. [1]

Viitekehyksenä tässä insinöörityössä toimi kaavion 1 mukainen malli, jossa insinöörityön lähestymistapaa lähdetään ensin avaamaan tarpeenmukaisen ilmanvaihdon ja älykkään teknologian, josta käytetään myös nimitystä IoT-teknologia avulla. Toisessa osassa arvioidaan älykkään tarpeenmukaisen ilmanvaihtojärjestelmän soveltuvuutta teollisuuden tuotanto-, toimisto- ja laboratorioympäristöön, jossa vertailua pyritään tekemään tarpeenmukaista ilmanvaihtoa soveltaen. Työn kolmannessa osassa tehdään vertailua eri laitetoimittajien välillä, jotka hyödyntävät tarpeenmukaista ilmanvaihtoa. Keskeiseksi lähtökohdaksi vertailulähtökohdaksi työssä asetettiin langattomuus, johtuen tarpeesta

asennuskustannuksien minimoimiseksi. Insinöörityön neljännessä osassa keskitytään juuri langattomaan tiedonsiirtoon, jota pohdittiin ensin langattomien tiedonsiirtotekniikoiden avulla sekä valitun älykkään tarpeenmukaisen ilmanvaihtojärjestelmän avulla. Viidennessä osassa selitetään mitä uhkakuvia langatonta älykästä tiedonsiirtoa toteuttava järjestelmä voi luoda teollisessa ympäristössä ja miten automaatioon liittyvä kyberturvallisuustandardi IEC 62443 asian ilmaisee ja miten konkreettisilla suojautumiskeinoja voidaan ennaltaehkäistä uhkakuvilta suojautuminen. Insinöörityön kuudennessa osassa pohditaan mahdollista integrointia teollisuuden automaatioverkkoon, josta käytetään nimitystä ICS (Industrial Control System). Seitsemännessä osiossa käsitellään langattomien antureihin olennaisesti liittyviä sisäilman epäpuhtaus- ja laatutekijöitä toimisto- ja teollisuusympäristöissä. Seitsemännessä osiossa pohditaan millä tavoin sisäilman laatutekijöihin voidaan vaikuttaa tarpeenmukaisen ilmanvaihdon avulla ja millä tavoin valitun älykkään ilmanvaihtoratkaisun avulla voidaan vaikuttaa sisäilman laatutekijöihin. Osiossa kahdeksan pohditaan millä tavoin mittaukset vaikuttavat järjestelmän ohjaukseen. Viimeisessä osiossa pohditaan valitun älykkään ilmanvaihtoratkaisun energiansäästö- ja kannattavuusvaikutuksia yleisesti saatavilla olleiden raporttien perusteella.

Kaavio 1: Viitekehysmalli

2 Tarpeenmukainen ilmanvaihto ja älykkäät ilmanvaihtoratkaisut

Tarpeenmukainen ilmanvaihto määritellään standardin SFS-EN 15251 mukaan ilmanvaihtojärjestelmäksi, jossa ilmanvaihtoa säädetään tietyn sisätilassa olevan ilman epäpuhtauden tai henkilöiden läsnäolon perusteella. [2]

2.1 Periaate

Älykäs ilmanvaihto voidaan määritellä kahdella eri tavalla. Ensimmäinen tapa on määritellä järjestelmä säätöstrategioiden mukaisesti. Älykäs ilmanvaihto toteuttaa säätöstrategiana tarpeenmukaista CCV-strategiaa eli suljettua silmukkaohjausta (Closed Loop Control), jossa parametritietoa saadaan anturilta signaalin muodossa ja sen perusteella säädetään ilmanvaihtoa eri tiloissa. Kuvassa 2 on esitetty erot eri säätö strategioiden ja tekniikoiden osalta vakioilmavirtaisessa ja muuttuvailmavirtaisessa ilmanvaihtojärjestelmässä. [3, s. 17]

Kuva 2. Ilmanvaihdon säätöstrategiat ja tekniikat [3, s. 17].

Swegonin mukaisesti kysyntälähtöinen älykäs ilmanvaihto voidaan katsoa edustavan viidennen sukupolven ilmanvaihtotekniikkaa. Alla on esitetty lista, josta selviää erot eri ilmanvaihtotekniikoiden välillä:

1. Painovoimainen ilmanvaihto

2. Koneellinen tulo- ja poistoilmanvaihto tasailmavirtaperiaatteella

3. Koneellinen tulo- ja poistoilmanvaihto muuttuvailmavirtaperiaatteella

4. Koneellinen tulo- ja poistoilmanvaihto tarpeenmukaisen ilmanvaihdon periaatteella (Demand Controlled Ventilation - DCV)

5. Älykäs tarpeenmukainen sisäilmaston ohjaus älykkäiden anturiteknologioiden periaatteella (Demand Controlled Indoor Climate - DCIC) [4]

Hybridi-ilmanvaihto ei suoranaisesti ole oma ilmanvaihtotekniikkansa ja usein puhutaan painovoimaisen ja koneellisen poiston yhdistelmästä varsinkin vanhoista 80-luvun omakotitalokiinteistöistä. Hybridi-ilmanvaihto useimmiten liittyy talotekniikkaremontteihin vanhoissa kiinteistöissä, joissa painovoimainen ilmanvaihto halutaan korvata koneellisella ilmanvaihdolla kiinteistön yleisissä tiloissa, kuten kellari-, varasto-, pesu- ja mahdollisissa toimistotiloissa. Hybridi-ilmanvaihto tosiasiassa voi olla minkä tahansa edellä olevan yhdistelmä, kunhan lait, rakennusmääräykset ja vaatimukset täyttyvät.

Kysyntälähtöisestä älykkäästä sisäilmastosta käytetään usein lyhennettä DCIC eli yhtä kuin Demand Controlled Indoor Climate, koska suomenkielistä lyhennettä ei ole vielä esitetty yleisesti käytettäväksi. Muuttuvailmavirtajärjestelmästä on yleisesti käytetty suomenkielessä lyhennettä IMS eli ilmamääräsäädin vaikka tämä lyhenne suoranaisesti viittaa ilmamäärän säätöpelteihin, joista on arkikielessä puhuttu IMS-pelleistä. DCV-tekniikassa nämä säätöpellit ovat samalla tavoin mukana, mutta huomattavana erona DCIC-tekniikkaan on, että ilmamäärän säätöpelleissä on mukana äly, jolla järjestelmä pyrkii tasapainottamaan itse itsensä. Säätö kyseisissä säätöpelleissä perustuu kyseissä sijaitsevien mittausantureilta saatavaan tietoon ja järjestelmä pyrkii itse tasapainottaamaan säätöpeltien, mittaus- ja paine-eroantureiden avulla eri vyöhykkeet tai huoneyksiköt. Huomattavana erona DCIC- DCV-tekniikassa on myös, että DCIC-tekniikassa järjestelmän älykkyys perustuu itseohjautuvuuteen ja kaikkien sisäilmastotekijöiden kokonaisvaltaiseen hallintaan huone/vyöhyke säätimien integroinnilla toistensa kanssa, niin että lämmityksen jäähdytyksen ja ilmanvaihdon yksikkösäätimet keskustelevat rakennusautomaation keskusyksiköllä toistensa kanssa yhteisessä sulautetussa rakennusautomaatiojärjestelmässä. DCIC-tekniikkaan kuuluu myös mukaan muut sisäilmastolliset tekijät,

kuten lämmitys- ja jäähdytysratkaisut tietyn tilan tai vyöhykkeen sisällä. Tässä insinöörityössä keskitytään pääsääntöisesti ilmanvaihtotekniikkaan sisältäen rakennusautomaation ja tietoliikenteen mukanaan tuoman älyllisen kehityksen ja osittain sivutaan myös muita sisäilmastollisia tekijöitä, kuten lämmitys- ja jäähdytystekniikan ratkaisuja. [4]

2.2 Paineesta riippuvat, paineesta riippumattomat ja paineoptimoidut järjestelmät

Kaikki muuttuvailmavirtaiset järjestelmät, kuten VAV, DCV ja DCIC, voidaan jaotella paineesta riippuviin, paineesta riippumattomiin ja paineoptimoituihin ilmavirranhallintajärjestelmiin. Paineesta riippumatossa järjestelmässä ilmavirran virtaussäädin ohjaa säätöpeltiä mittausanturin painevaihteluiden perusteella ja mittausanturi voi sijaita yhdistettynä virtaussäätöpeltiin tai erillisenä anturiyksikkönä esim. poistokanavassa. Paineesta riippuvaisessa järjestelmässä kanavistossa tapahtuvia paine-eroja ei huomioida eli virtaussäätimissä ei ole sisäistä älyä, jolla kanaviston paine-erot voidaan tasapainottaa. Lisäksi paineesta riippumattomat järjestelmät tarvitsevat erilliset virtaussäätöpellit, jotka sijaitsevat usein haarakanavissa. [5, s. 24]

Paineoptimoiduissa järjestelmissä puhaltimien kierrosnopeudet säätyvät eri kerroksien haarakanavien alkuun asennetuilla vakiopainesäätimien, säätöpeltiyksiköiden ja mittausantureiden avulla ja tällöin eri kerrosten välillä kulkevassa runkokanavistoissa ei ylläpidetä vakiopainetta. Yleensä poistokanavaan asennetut mittausanturit lähettävät tiedon samassa laitteessa sijaitsevalle vakiopainesäädin ja säätöpeltiyksikölle vakiopaineen ylläpitämiseksi. Paineoptimoidut järjestelmät ovat nykyisin tyypillisesti yhden järjestelmätoimittajan kokonaisuuksia, joihin kuuluu ilmamääräsäätimet, paineanturit, tarvittavat kerros ja/tai vyöhykekohtaiset painesäätimet sekä ilmanvaihtokoneen puhaltimien kierroslukua säätävä keskusyksikkö. Esimerkkeinä paineoptimoiduista järjestelmäkokonaisuuksista on Fläkt Woodsin IPSUM-, Swegonin Super Wise- ja Lindabin Pascal-järjestelmät. [6, s. 32-33]

2.3 Muuttuvailmavirtaisten järjestelmien haasteet

Muuttuvailmavirtaisen järjestelmien, kuten VAV, DCV ja DCIC, haasteina voidaan katsoa olevan seuraavat tekijät:

- Ilmavirtauksien hallinta
- Epäviihtyvyystekijät
- Äänihaitat
- Kanavistojen epäpuhtauksista johtuvat ongelmat

2.3.1 Ilmavirtauksien hallinta

Ilmavirtauksien hallinta koetaan ongelmaksi tilanteissa, joissa ilmavirran nopeus kasvaa liian suureksi tai jää liian pieneksi. Tällöin ilmavirran vaikutus heittokuvioon on merkittävä, jolloin liian suurilla nopeuksilla ilmavirta törmää lattiaan ja muodostaa epäsymmetrisen heittokuvion. Liian alhaisilla ilmavirran nopeuksilla heittokuvio jää vajaaksi, jolloin puhdas ilma jää kattoon eikä puhdas ilma vaihdu kyseisessä tilassa tai vyöhykkeellä tarpeeksi.

2.3.2 Epäviihtyvyystekijät

Epäviihtyvyystekijät koituvat järjestelmän osalta ongelmaksi erityisesti tilanteissa, kun päätelaitteiden otsapintanopeudet kasvavat ilmavirran osalta hallitsemattomasti. Tällöin tulee usein esiin ongelmia, mitkä liittyvät esim. suoraan niskaan puhalluksen vaikutuksiin tai vedon tunteeseen. Vedon tunne aiheutuu usein päätelaitteiden liian suurista otsapintanopeuksista, kun tuntuva lämpötila (ihmisen tuntema lämpötila) eroaa huomattavasti huonelämpötilan arvosta ja pahimmassa tapauksessa huonelämpötilaa lisäämällä ilmalämmityksen avulla päätelaitteen otsapintanopeus vain kasvaa. Vedon aiheuttamat epäviihtyvyystekijät ovat yksi keskeisimmistä sisäilmastotekijöihin, kuten ilmanvaihtoon, lämmitykseen ja jäähdytykseen liittyvistä ongelmista. [7]

2.3.3 Äänihaitat

Äänihaitat korostuvat tilanteissa, joissa tietyn päätelaitteen maksimi otsapintanopeus ylittyy ja kanavistossa ilmavirran nopeus ylittää sallitun. Tällöin kyseiseen tilaan tai vyöhykkeelle alkaa muodostumaan äänihaittoja, jotka ylittävät äänenvaimentimien, päätelaitteiden sekä kyseiseen tilan tai vyöhykkeen pinta-alalle ominaisen Sabine äänenvaimennusarvon. Tällöin kanavistosta muodostuvat ja päätelaitteella usein moninkertaistuvat meluhaitat ovat haitaksi sisäilmatekijöille. [8]

2.3.4 Kanavistojen epäpuhtauksista johtuvat ongelmat

Kanavistoissa esiintyvät epäpuhtausongelmat on ilmanvaihdon osalta todellinen ongelma tilanteissa, joissa ei ole suoritettu asianmukaisia huoltotoimenpiteitä. Ilmanvaihtokanavistojen ongelmat voivat levitä laajalle aina sisäilmaongelmiin asti. Keskeistä kuitenkin muuttuvailmavirtaisten järjestelmien säätöpeltien osalta on, että virtaus- ja paine-eroanturit eivät mittaa virtaus- tai paine-eroja oikein, jos kanavistoissa kulkee pölyistä (pienhiukkasmaista) ilmaa. Tällä hetkellä ainoastaan ultraääniantureilla toteutetut IMS-säätöpellit pystyvät mittaamaan kanavistoissa kulkevan ilmavirran tarkasti myös pölyisissä kanavistoissa. Kuvassa 3 on esitetty FläktWoodsin ultraäänitekniikalla varustettu IMS-säädin. Lisäksi IMS-säätöpeltien huolto ja testaus tulisi suorittaa asiantunteva henkilö, koska usein toimimoottoreilla varustettujen säätöpeltien rikkoontumisriski on suurempi esim. kanavapuhdistusten yhteydessä ja toimimattomuus voi johtua myös säätöpellin eteen kerääntyneistä epäpuhtauksista. [9]

Kuva 3. Fläkt Woodsin Optivent Ultra IMS -säädin [10].

2.4 Älykkään ilmanvaihdon vaikutus sisäilmastotekijöihin

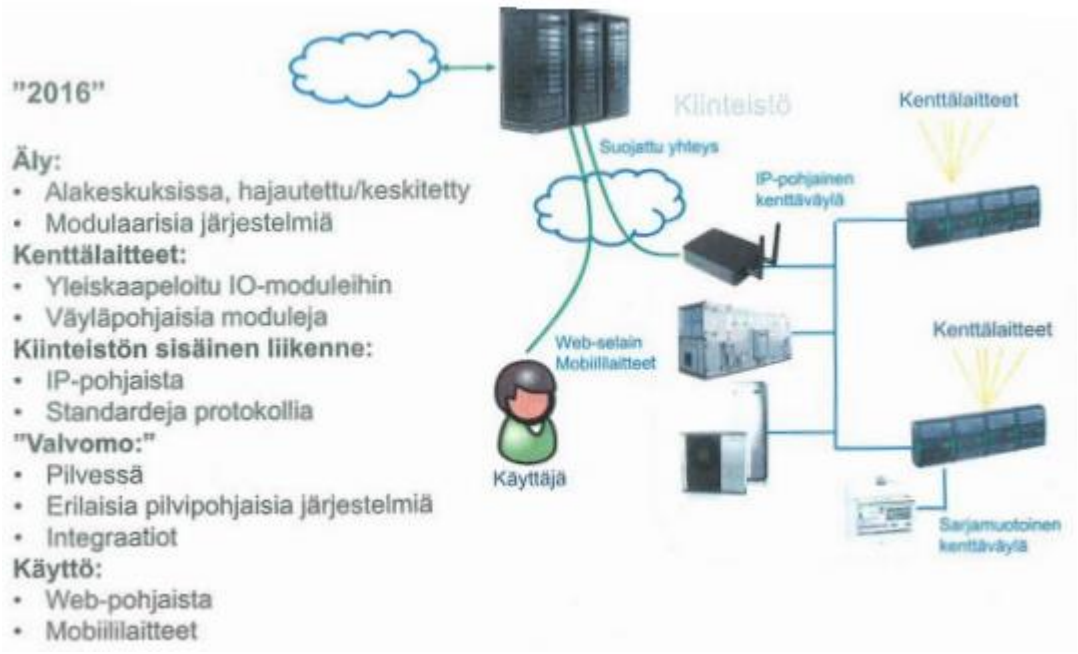
2.4.1 Epäpuhtauksien hallinta

Sisäilmastotekijät koituvat ongelmaksi tilanteissa, joissa orgaaniset epäpuhtaudet eli VOC:it (Volatile Organic Compounds) ja/tai hiilidioksidipitoisuus kohoaa liian suureksi. Epäpuhtauksien mittaamisen avulla tarpeenmukainen ilmanvaihto pyrkii reagoimaan ennen kuin epäpuhtauspitoisuudet kohoavat liian suuriksi. Ilmanvaihtoa lisäämällä järjestelmä pyrkii työntämään, syrjäyttämään ja/tai sekoittamaan epäpuhtaudet sisäilmassa, jotta niiden pitoisuus sisäilmassa pienenisi. Epäpuhtauspitoisuuksien raja-arvoja on esitetty kappaleessa kahdeksan.

2.4.2 Viihtyvyystekijät

Viihtyvyystekijät ovat olleet olennainen seikka älykkäiden kodin IoT-ratkaisujen yleistymisessä. Viihtyvyystekijöihin vaikuttaa ilmanvaihdon osalta erityisesti huoneen nopea lämpötilan ohjaus ilmanvaihdon avulla. Myös lämpötilan vaihtelut vaikuttavat sisäilmastotekijöihin ja ovat suorassa yhteydessä ihmisten terveysvaikutuksiin. Lisäksi ilman liiallinen tai liian alhainen kosteuspitoisuus koituu ongelmaksi, ja sillä on merkittävä yhteys sekä ihmisten terveyteen että rakennusterveyteen liittyvissä asioissa. Riippuen ilmanvaihtokoneesta ja sen ympärille rakennetusta älykkäästä järjestelmästä, myös ilmankosteusarvoja voidaan muuttaa tiettyjen raja-arvojen puitteissa.

2.5 Älykkäät IoT-ratkaisut

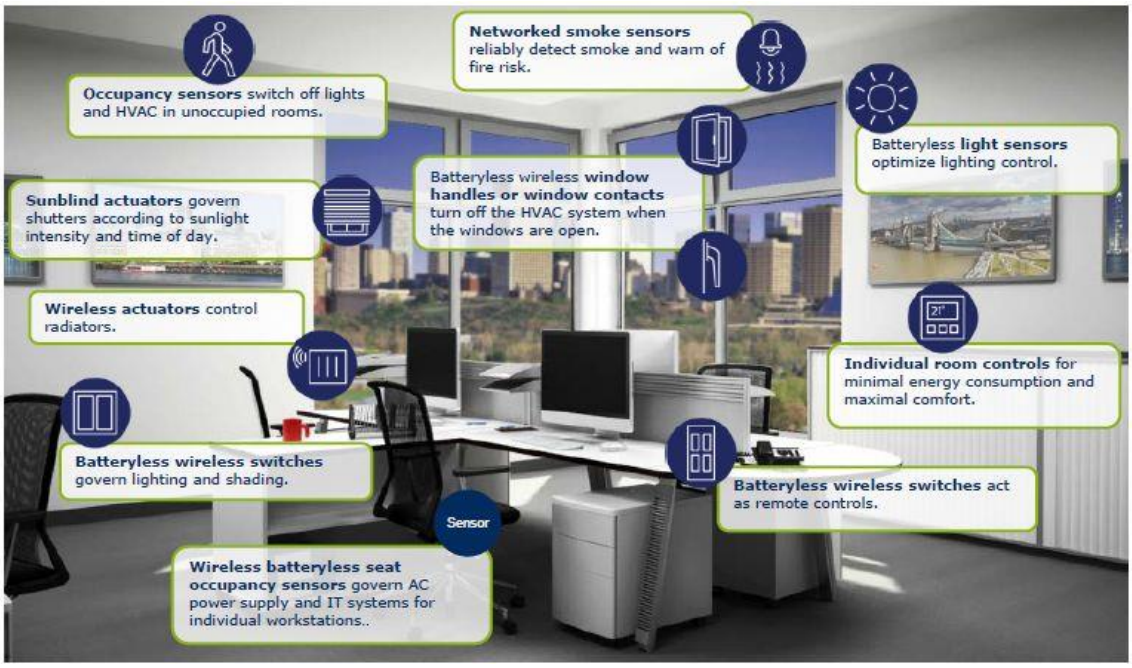


Kuva 4. Pilvipohjainen rakennusautomaatiojärjestelmä [9, s. 10].

Kuvassa 4 on esitetty havainnemalli nykyaikaisesta pilvipohjaisesta rakennusautomaatiojärjestelmästä, jossa järjestelmän käyttö on siirtynyt kokonaan pilveen ja järjestelmän muuntojoustavuutta lisäävät modulaariset järjestelmät ja ylätason pilvipohjaisten järjestelmien integraatio. Erityisesti omakotitalojen IoT-ratkaisujen kasvaneeseen suosioon on vaikuttanut energiankulutuksen reaaliaikainen seuranta, energiansäästömahdollisuudet sekä integrointi eri laitteiden ja järjestelmien välillä. IoT-ratkaisujen toteutuksen osalta on muistettava erilaisilta antureilta saatavan suuren tietomäärän (Big Data) hallinta. Kodin IoT-laitteet voivat tuottaa dataa jopa gigabittien verran viikossa.

Nykyään älykkäitä ratkaisuja on tarjolla hyvin kattava määrä ja ongelmaksi on alkanut tulemaan eri verkkotekniikoiden yhteen liittäminen. Parhaimpaan luotettavuuteen päästään, kun tilataan kaikki kohteen älylaitteet samalta toimittajalta, mutta myöhemmin ongelmaksi voi tulla yhden laitetoimittajaan sisältyvä riski tekniikan kehityksen osalta. Ku-

vassa 5 on esitetty nykyisin hyvin tunnetun EnOceanin valmis ratkaisu toimistojen älykkäistä antureista. EnOceanin standardin kehitystä tukee EnOceanin perustama EnOcean Alliance, joka toimii eräänlaisena kattojärjestönä, ja se toimii yhteistyössä myös muiden älyverkkostandardien (ZigBee), väyläratkaisutoimittajien (BACnet, Modbus, KNX) ja laitetoimittajien (Schneider Electric) välillä.



Kuva 5. EnOceanin valmis älyratkaisu toimistotiloihin [11].

Älyratkaisumarkkinoiden kehitystä on edesauttanut merkittävästi viisi eri tekijää, jotka ovat antureiden langattomuus, laaja valikoima erilaisia antureita, energian kulutuksen seuranta, ohjelmoitavat I/O-säädinyksiköt sekä Internetin yli mahdollistuva päätelaitteiden hallinta. Kuvassa 6 on esitetty Schneider Electricin toimittama VAV-ohjainyksikkö muuttuvailmavirtaiseen ilmanvaihtojärjestelmään, joka toimii langattomasti EnOcean- ja Zigbee-verkoissa. Samanlaisia langattomia säätöpeltien ohjausyksiköitä ei ole markkinoilla muilla toimittajilla ja kyseinen ohjausyksikkö mahdollistaa rakennusautomaation kannalta esim. toimistohuoneiden täysin langattoman ohjauksen ja säätöympäristön.

Kuva 6. Schneider-Electricin toimittama täysin ohjelmoitava VA2 – VAV säädinyksikkö [12].

3 Soveltuvuus teollisuus-, toimisto- ja laboratorioympäristöön

3.1 Ilmanvaihdon ohjausta koskevat asetukset muissa kuin asuinrakennuksissa

Rakennuksen ohjausta koskevat asetukset löytyvät ympäristöministeriön asetuksesta 1009/2017, jossa määritellään, että muiden kuin asuintilojen ilmanvaihtojärjestelmien ohjaus suunnitellaan niin, että ilmavirtoja voidaan säätää tila- tai vyöhykekohtaisesti tilojen kuormituksen tai sisäilman laadun mukaan. Todetaan myös, että yksinkertaisimmillaan ilmanvaihdon tehostus voi perustua lisäaikapainikkeisiin, tehostuskytkimiin tai läsnäolotunnistimiin. Lisäksi todetaan, että tarpeenmukainen ohjaus ja energiatehokkuus voivat perustua myös ilmanvaihdon ohjaamiseen esimerkiksi huonelämpötilan tai epäpuhtauspitoisuusmittausten perusteella. Lähtökohtaisesti määräyksissä ohjeistetaan, että muiden kuin asuinrakennuksien ilmanvaihdon suunnittelussa ja rakentamisessa ilmanvaihtokertoimen tulee olla vähintään 0,2 1/h ja ulkoilmavirran vähintään 15 (dm³/s) /m² koko rakennuksen lattiapinta-alaa kohden. Lisäksi ilmanvaihdon ohjaukseen vaikuttavat hyvin olennaisena seikkana myös HTP-arvot ja muut sisäilmastossa esiintyvät haitalliset aineet, joista on kerrottu tarkemmin kappaleessa 8. [13, s. 18; 14]

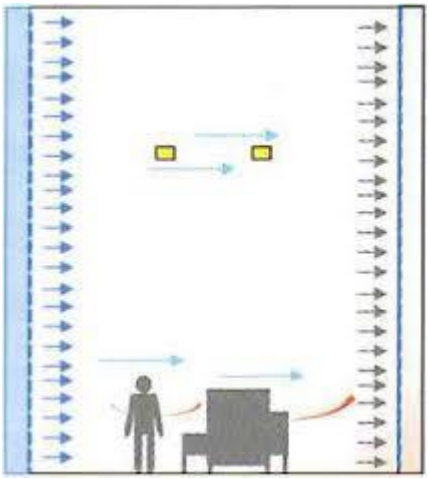
3.2 Älykkään ilmanvaihdon soveltuminen eri ilmanvaihtoperiaatteisiin

Tilailmastoinnin periaate, josta usein englanninkielellä puhutaan myös tilailmastointi strategiasta, on eräänlainen tavoitteenasettelu, jolla pyritään huonetilassa tiettyyn lämpötila-, epäpuhtaus- ja kosteusjakaumaan. Tilailmastoinnin periaatteet jakautuvat yleensä seuraavasti:

- Mäntäperiaate
- Kerrostumaperiaate
- Vyöhykeperiaate
- Sekoitusperiaate

3.2.1 Mäntäperiaate

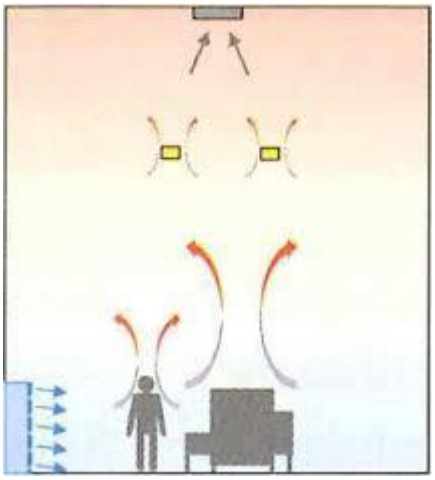
Mäntäperiaatteessa pyritään tasaisesti muuttuvaan jakautumaan ilmavirran suuntaisesti ja huoneilmavirtaukset hallitaan yhdensuuntaisella työntävällä mäntäperiaatteella sekä pienen nopeuden omaavalla tuloilmanjaolla. Mäntäperiaatteen kannalta tärkeintä on suunnitella pientä nopeutta noudattava tuloilmanjako, joka on kuitenkin oltava riittävän voimakas syrjäyttämään häiriövirtaukset. Kuvassa 7 on esitetty vasemmalla mäntäperiaatteen tyypillinen ilmanvaihdon sovelluskuvaus. Mäntäperiaatteelle on tyypillistä hyvin pienet otsapintanopeudet päätelaitteissa, useita päätelaitteita samassa tilassa, laminaariset ilmavirtaukset sekä kohdetilan vaatima erittäin puhdas sisäilmavaatimus. Tyypillinen esimerkki kohteesta on sairaaloiden leikkaussalit, joihin muuttuvailmavirtaiset järjestelmät eivät sovellu, johtuen leikkaussalien kontaminaatioriskistä, joka aiheutuu usein ilman liikkeestä leikkauspöydällä. [15, s. 398]



Kuva 7. Mäntäperiaate [15, s. 398]

3.2.2 Kerrostumaperiaate

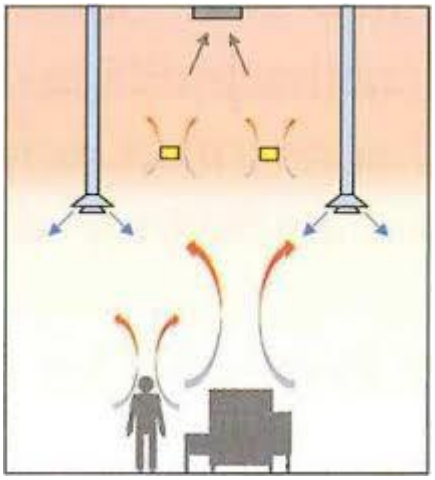
Kerrostumaperiaate on tyypillinen ilmanvaihtoratkaisu usein tehtaissa, prosessitiloissa, ja tuotantotiloissa, joissa on paljon lämmönlähteitä ja halutaan hyödyntää alhaisella ilmavirralla ja pienellä alilämpöisyydellä aikaansaatuja nostevoimien konvektiovirtauksia eli pluumeja. Esimerkkinä on seinille asennettujen konvektoreiden ja lämminilmapuhaltimien sekä ikkunan alle asennettujen ikkunapenkkipuhaltimien avulla aikaansaatu ja ilman tiheyserojen johdosta kerrostuvaan lämpötila ja epäpuhtauskuormaan. Muuttuvailmavirtaisien järjestelmien soveltaminen kerrostumaperiaatteellisiin tiloihin on usein mahdotonta, johtuen konvektoreiden ja lämminilmapuhaltimien sekä ikkunapenkkipuhaltimien soveltumattomuudesta. Jos kerrostuvan ilmanvaihdon tila aiotaan toteuttaa tarpeenmukaisella ilmanvaihdolla, on suunnittelussa kiinnitettävä erityistä huomiota CFD simulointityökalun, kuten Ansys CFX, avulla saataviin tilakohtaisiin virtaus- ja lämpöolomuutoksiin. CFD simulointityökalun avulla on pystyttävä arvioimaan tarpeenmukaisen ilmanvaihdon ilmavirtojen ja lämpötilamuutoksien maksimi ja minimi säätöarvot, joiden ulkopuolella kerrostumaperiaatteella toimivan ilmanvaihtoprosessi häiriintyy eikä kerrostumaperiaate enää toteudu. Kuvassa 8 on esitetty periaatekuvaus täydellisestä kerrostumaperiaatteesta, jossa tiheydeltään ohuempi ja kevyempi lämminilma on katossa ja viileämpi ja painavampi ilma alempana. [15, s. 398]



Kuva 8. Kerrostumisperiaate [15, s. 398]

3.2.3 Vyöhykeperiaate

Vyöhykeperiaatetta sovellettavissa tiloissa ilmavirtauksia pyritään hallitsemaan sekä tuloilmajaolla että konvektion avulla, joilla saavutetaan vyöhykejako, jossa ylempi epäpuhtaampi ja lämpimämpi ilma sijaitsee kontrolloimattomalla vyöhykkeellä ja alempi eli viileämpi ja puhtaampi ilma sijaitsee alemmalla kontrolloidulla vyöhykkeellä. Kerrostumisperiaatetta sovelletaan tehtaissa, tuotantotiloissa, julkisissa rakennuksissa ja muissa tiloissa, joiden tilat ovat riittävän korkeita vyöhykeperiaatteen soveltamiseen. Vyöhykeperiaatetta voidaan tehostaa riittävän alhaisella lämpötilalla oleskeluvyöhykkeen lämpötilaan nähden. Muuttuvailmavirtaisen järjestelmän käyttö soveltuu vyöhykeperiaatteeseen ainoastaan alemman eli kontrolloidun vyöhykkeen ilmavirran ohjaukseen. Suunnittelussa on kuitenkin tapauskohtaisesti varmistettava soveltuvuus erilaisissa tuotanto- ja prosessitiloissa esim. CFD-simulointityökalua apuna käyttäen. Näin voidaan varmistua tuloilman lämpötilojen, kosteusvaihteluiden sekä ilmavirtojen vaikutuksesta minimi ja maksimi ilmavirroilla älykkään ilmanvaihtojärjestelmän rakennusautomaation tueksi. Kuvassa 9 on esitetty vyöhykeperiaatteella toimivan ilmanvaihdon sovelluskuvauksesta. [15, s. 398.]



Kuva 9. Vyöhykeperiaate [11, s. 398]

3.2.4 Sekoitusperiaate

Sekoitusperiaate on yleisin ilmanvaihtoperiaate asuinrakennus- ja toimistotilojen koneellisissa ilmanvaihtojärjestelmissä. Huonetilat eivät ole liian korkeita vyöhykeperiaatteen toteutumiseksi ja ilmavirtaukset ovat liian turbulenttisia ja tuloilman alilämpöisyys suurta kerrostumaperiaatteen toteutumiseksi. Tarpeenmukainen ilmanvaihto soveltuu näihin tiloihin erityisen hyvin, koska ilmavirran tehostukselle ei ole muita kuin äänenpainetta ja ilmankosteutta koskevia rajoitteita. Lisäksi älykkäällä IoT-ratkaisulla varustetun tarpeenmukaisen järjestelmän tehtävä on pitää yllä tarvittavaa ilmanvaihtoa, jos lämpötila ja emissiopitoisuudet alkavat kerrostumaan liian alhaisella ilmavirtauksella. Kuvassa 10 on esitetty sovelluskuvaus sekoitusilmanvaihdon periaatteesta. [15, s. 398]

Kuva 10. Sekoitusilmanvaihto [11, s. 398]

3.3 Soveltuvuus teollisuusympäristön tuotanto- ja prosessitiloihin

Eri teollisuuden alat ja niiden prosessitilat eroavat hyvin paljon toisistaan. Näissä tiloissa hyvin usein itse prosessi asettaa vaatimukset näiden tilojen sisäilmastotekijöille. Entisessä rakennusmääräyskokoelmassa oli esitetty sisälämpötilan suositusarvoja eri teollisuustöihin, mutta tosiasiassa lämpötilat määräytyvät hyvin pitkälti eri teollisuustilojen käyttötarkoituksesta. Tarpeenmukaista ilmanvaihtoa suositaan tänä päivänä energiataloudellisuuden perusteella, esim. yö tuuletuksen avulla, mutta tosiasiassa yö tuuletus suurissa teollisuuslaitoksissa voidaan järjestää myös muulla tavoin. Esimerkiksi savunpoiston ja rakennusautomaation avulla voidaan savunpoistojärjestelmän testausohjelma suunnitella niin, että se toimii samalla yö tuuletuksen mahdollistavana järjestelmänä tiettyinä kellonaikoina. Savunpoistojärjestelmien toimittajat markkinoivat tehokkaita savunpoistopuhaltimia, joita voidaan käyttää päivittäisilmanvaihdon tarpeisiin käyttämällä niitä esimerkiksi ylilämmön poistoon tai yö tuuletukseen. [16]

3.3.1 Tarpeenmukainen ilmanvaihto teollisuuden tuotantotiloissa

Keskeistä on, että teollisuuden prosessitiloja ei voida ohjata läsnäoloanturien eikä välttämättä VOC anturien perusteella. Tämä siksi, koska läsnäoloanturit eivät tunnista pros-

sin toimintaa eikä VOC-anturit välttämättä sovellu teollisuustiloihin, joissa pölyn ja hajujen määrä on merkittävää, esim. konepaja- ja varastokiinteistöissä (pienhiukkasten määrä jopa 500–1 000-kertainen). Tämä voi aiheuttaa tarpeenmukaisen järjestelmän kannalta sen, että energian kulutus kasvaa ilmavirran tehostuksen jälkeen ja eikä välttämättä likaisten tilojen sisäilman laadussa tapahdu merkittäviä muutoksia. Viihtyvyyden kannalta tilanne voi tuntua paremmalta, mutta energiankulutuksen kannalta järjestelmä voi aiheuttaa lisäkustannuksia tiloissa, joissa epäpuhtauksien määrä voi olla suuri ja järjestelmä voi toimia pahimmillaan vain näiden epäpuhtauksien siirtäjänä. Pahimmillaan painesuhteiden liiallinen muutos voi aiheuttaa sen, että lämminilma pyrkii vain rakennuksen vaipasta ulos, mutta epäpuhtaudet ja kosteus jäävät sisätilaan. Eräs turha energiankulutustilanne voi olla esim. se, että tuotantotilassa, joissa esiintyy huomattava määrä pölyä ja epäpuhtauksia pyritään ilmanvaihdon jatkuvalla tehostuksella saada epäpuhtauksista aiheutuvien orgaanisten hajuhaittojen eliminointi, mutta itse hajuhaittojen lähdettä ei saada poistettua, koska ilmanvaihdon teho ei riitä poistamaan ympäristössä esiintyviä orgaanisia kiinteitä epäpuhtauksia.

Prosessitiloille on usein ominaista niiden lämpö- ja kosteustaseajattelu. Prosessitiloissa itse tuotantoprosessit voivat aiheuttaa tiloissa huomattavia lämpö- ja kosteuskuormia, jotka lämpötase ajattelun ja termodynamiikan toisen pääsäännön mukaisesti siirtyvät lämpimistä tiloista kylmiin tiloihin, kunnes lämpötilaerot ovat tasapainossa. Sisäilmassa oleva kosteus taas rakennusfysiikan ja termodynamiikan oppien mukaan usein tiivistyy seinärakenteisiin lämpötilan muuttuessa kylmän seinän pinnalla, jollei seinärakenteita ole suojattu, kuten märkätiloissa. Prosessitiloille on ominaista, että prosessien lämpötilaeroista johtuva ilmankosteus ja prosessista syntyvä kosteus pyrkii tasapainottumaan eri lämpötiloissa, jolloin kylmiin pintoihin muodostuu vesipisaroita, jotka diffuusion ja kapillaari-ilmiön seurauksena imeytyvät rakenteisiin ja eri materiaaleihin, joilla on hyvä kosteuden imukyky. Prosessitiloille voi olla ominaista mitata varsinkin ilman suhteellista kosteutta ja lisätä mahdollisesti kuivaa ilmaa siinä suhteessa kuinka paljon ilman suhteellinen kosteus kasvoi jonkin prosessivaiheen seurauksena (esim. valssaus), mutta ongelmaksi saattaisi syntyä prosessin häiriintyminen ja suuri epäpuhtauskertymä. Teollisuudessa kohdepoistot toimivat suurten epäpuhtauslähteiden erillispoistoina, joiden mitoituksessa käytetään kyseisestä prosessista aiheutuvia epäpuhtaus, kosteus ja lämpötilamuutoksia. Eri teollisuuslaitoksissa erillispoistot voivat sijaita täysin eristetyssä tilassa, joita usein nimitetään erityistiloiksi.

Tuotantotilojen ilmanvaihdon kannalta on aluksi mietittävä, että kuinka tarpeenmukainen ilmanvaihto vaikuttaa prosessien ilmanvaihtoon. Tuotantotiloissa yleisilmanvaihto ja prosessi-ilmanvaihto jaotellaan usein erillisiksi toiminnoiksi. Usein vanhoissa ja korjattavissa teollisuuskiinteistöissä halutaan yleisilmanvaihtoa parantaa, jos kyseessä on aiemmin ollut painovoimainen yleisilmanvaihto. Tällöin yleisilmanvaihtoa halutaan parantaa niissä tiloissa, joissa ei aiemmin ole ollut koneellista ilmanvaihtoa. Tällöin keskeistä on, että asiakas päättää esim. kuinka suurella ilmanvaihtokertoimella (1/h) lähdetään yleisilmanvaihtoa toteuttamaan ja miten tulevaisuudessa yleisilmanvaihto tulee vaikuttamaan esim. tilarajauksien suhteen prosessi-ilmanvaihtoon. Lisäksi keskeisesti yleisilmanvaihtoon tuotantotiloissa vaikuttaa poistoilmanvaihdon järjestäminen, esim. prosessien kohdepoistot, siirtoilman ja korvausilman käyttö tuotantotilassa ja sen läheisyydessä olevissa tiloissa. Tarpeenmukaisen ilmanvaihdon kannalta minimi-ilmamäärä tulee suunnitella niin että se riittää myös poistamaan epäpuhtauksia tiloista, joissa käytetään siirtoilmaa.

Swegonin uuden sukupolven Wise-järjestelmää suunniteltaessa tuotantotiloihin ensimmäisenä tulee mieleen, että soveltuvatko langattomat anturit tuotantotiloihin, joissa voi olla riski esim. radiosignaalien heikkenemisen takia. Luvussa 5.2.1 on esitetty antureiden langattomaan tiedonsiirtoon liittyviä olennaisia tekijöitä ja kerrottu tekniikasta lähemmin. Keskeistä on kuitenkin antureiden elektroniikkakomponenttien kosteussuojaus sekä haitallisilta aineilta, kuten pölyltä suojaaminen, jota voidaan arvioida kansainvälisellä kotelointiluokituksella (IP). Uuden sukupolven Wise-järjestelmän anturit noudattavat IP-luokitusta IP20 ja lämpötila-anturin (RTSa) sekä ikkuna- ja ovikoskettimen (WCSa) osalta IP-luokitusta IP31. Täten suurin osa uuden sukupolven antureista ovat sormisuojattuja esineiltä ja pölyltä 12,5 millimetrin halkaisijaan asti, mutta ei ole kosteussuojattuja lainkaan. Lämpötila-anturi (RTSa) ja ikkuna- ja ovikosketin anturit (WCSa) ovat sormisuojattuja esineiltä ja pölyltä 2,5 millimetrin halkaisijaan asti ja kosteussuojattuja pystysuoraan tippuvalta vedeltä. Kaikki sähköasennukset Suomessa kuuluvat SFS 6000 -standardin mukaisten sähköasennustandardien piirin ja tehtaissa ja tuotantotiloissa usein käytetään erityisvalmisteisia teollisuuteen tarkoitettuja antureita, joissa IP-luokitukset ovat aivan eri luokkaa mitä kotitalouksissa ja muissa toimitiloissa (esim. IP65). Tästä syystä uuden sukupolven anturit eivät sovellu normaaleihin tuotantotiloihin. Vaihtoehtona on käyttää tehdastiloihin soveltuvia antureita, joissa on analoginen tai digitaalinen virtaviestiyhteys, ja liittää ne digitaalisella tai analogisella virtaviestijohdolla (0–10 V)

Wise IREa -radiokommunikaatiosiltaan. Tällöin ainoastaan Wise IREa -laitteiden IP-luokitusta pitää parantaa lisäkoteloinnin avulla. [17; 18; 19; 20; 21; 22; 23; 24; 25]

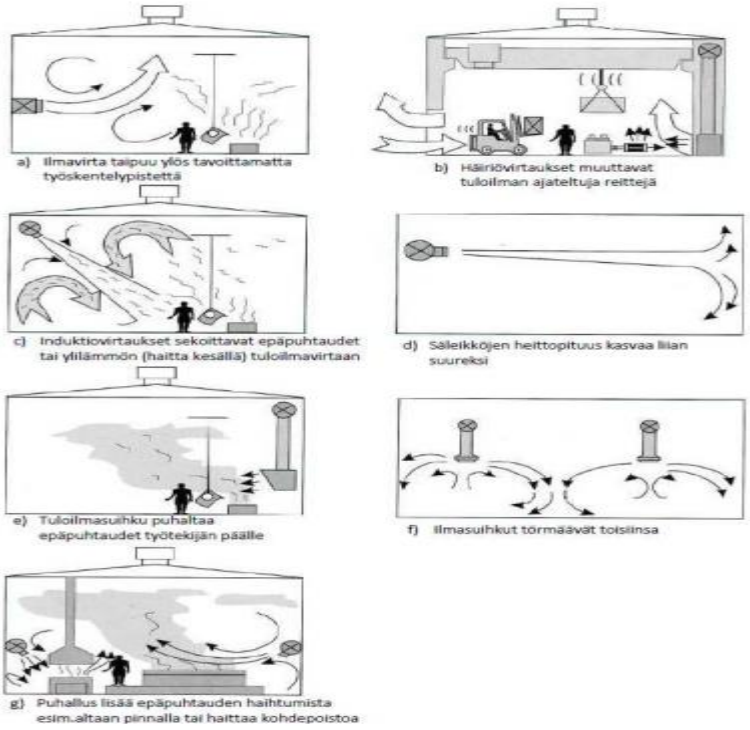
3.3.2 Rakenteellisesti eristetyt erityistilat

Teollisuudessa esiintyy joukko eri laisia toimialalle ominaisia erityistiloja. Erityistiloille on usein ominaista epäpuhtauspitoisuuksien ero verrattuna muihin työtiloihin. Teollisuudessa esiintyy toimialasta riippuen erityistiloja, kuten ATEX I, ATEX II, EMC ja lukuisa joukko muunlaisia erityislaatuisia tiloja, joissa esiintyy jokin huomattava riskitekijä ja tällöin muuttuvailmavirtainen järjestelmä voi aiheuttaa merkittävän riskilisän, koska ilmavirtojen painesuhteiden ja ilmavirtojen muutokset voivat aiheuttaa ongelmia näissä tiloissa, joita ei ole osattu aiemmin ottaa huomioon riskisuojautumisen kannalta. Rakenteellisesti eristettyjen erityistilojen osalta tarpeenmukainen ilmanvaihto on sekä teknisesti että energiataloudellisesti haastavaa toteuttaa, ja usein samaan, ellei parempaan lopputulokseen päästä automaatiojärjestelmän ja kellokytkimen avulla toteutetulla vakioilmanvaihtokoneella (CAV).

3.3.3 Ei rakenteellisesti eristetyt erityistilat

Teollisuuden prosessitiloissa esiintyy usein myös tiloja, joissa on huomattava epäpuhtauskertymä verrattuna muuhun tilaan, mutta tila ei välttämättä ole eristetty muusta tuotantotilasta. Tämmöisiä tiloja voi olla esim. hitsaussolu tai hitsaustyöpiste, joihin määräysten mukaisesti asennetaan kohdepoisto. Kohdepoiston eräs merkittävin ongelma on pluumi eli kohdepoiston ulkopuolelta tuleva häiriöilmavirtaus, joka heikentää kohdepoiston tehokkuutta. Ilmanjaon keskeisinä periaatteina voidaan pitää ilmavirtojen hallintaa halutuissa kohteissa tai vyöhykkeissä, ilmavirtojen nopeuksien hallintaa, epäpuhtaus emissioihin vaikuttaminen (esim. rakenteista irtoavat emissiot), kohdepoistojen vakaa toiminta ilman häiriövirtauksia ja liiallisen pienhiukkaspölyn nostevirtaukset. Ei rakenteellisesti eristetyissä erityistiloissa on teollisuudessa usein erilaisia kohdeilmanvaihtokohteita, kuten hitsauspisteet, korkeapainevesileikkuri, peittausallas ja ilmaverhot. Keskeistä näissä kohdeilmanvaihtokohteissa on, että ne sijaitsevat usein samassa tilassa, jossa on käytössä myös normaali yleisilmanvaihto. [26, s. 2-9, 18-25]

Kohdepoiston läheisyyteen ei saisi asentaa yleisilmanvaihtoon liittyviä tulo- ja poistoilmalaitteita, koska tällöin riski kohdepoiston erillispoistettavien kaasujen leviämiseen kasvaa. Pluumin merkitystä voidaan tarkastella oviaukkojen läheisyydessä esim. oviaukkovirtauksien perusteella, jos oviaukkovirtaukset ovat suunniteltu oikein, ei tilaan pääse ulkoilmavirtauksia. Esimerkiksi oviaukkovirtauksissa häiriövirtauksia pyritään poistamaan rakentamalla erilaisia liepeitä ja seinämiä sekä ilmaverhoja, mitkä auttavat ilmavirtojen oikeanlaista suuntausta ja ilmavirtauksien nopeuden hallintaa sekä estävät kylmien ilmavirtauksien sisäänpääsyä. Kuvassa 11 on esitetty teollisuustilojen tyypillisiä yleisilmanvaihtoon liittyviä ilmavirtojen häiriötekijöitä. Tarpeenmukaista ilmanvaihtojärjestelmää, kuten Swegon uuden sukupolven Wise-järjestelmää suunniteltaessa teollisuuskohteisiin, joissa tuotanto- ja prosessitilat ovat yhdessä, on ensin selvitettävä, millä tavoin prosessit vaikuttavat yleisilmanvaihtoon ja onko olemassa häiriövirtausten riskiä ja onko tällöin tarpeenmukainen ilmanvaihto edes soveltuva kohteisiin, joissa häiriövirtauksien riski on suuri sekä prosessi asettaa omat tarpeensa yleisilmanvaihdon osalta eri ilmanvaihtoperiaatteisiin liittyvien ilmanvaihtotekniikoiden ja tehokkuuden osalta, kuten pieninopeuksinen syrjäytys- ja suurinopeuksinen sekoitusilmanvaihto sekä terminen ilmanvaihto.



Kuva 11. Tyypillisiä teollisuustilojen yleisilmanvaihdon häiriövirtauksia [27]

3.4 Soveltuvuus teollisuuden puhdas- ja laboratoriotiloihin

Usein erilaiset puhdas- ja laboratoriotilat toteutetaan normaalilla ilmanvaihdolla (CAV) automaatiojärjestelmän, kellokytkimien ja tehostuskytkimien avulla ohjattuina. Eräs tyypillinen esimerkki on toteuttaa laboratorion ilmanvaihto kellokytkimen avulla. Esimerkiksi niin, että yleisilmanvaihto toimii normaalin käyttöajan ulkopuolella 50 %:n ilmavirralla, käyttöaikaa edeltävän tunnin aikajakson aikana 125 %:n tehostuksella ja käyttöaikana 100 %:n ilmavirralla. Laboratoriotilat teollisuudessa muodostavat oman spesifisen erikoistilan, jossa usein tilojen väliset painesuhteet saattavat erota toisistaan hyvinkin merkittävästi. Keskeiseen asemaan laboratoriotilojen suunnittelussa huomio kiinnittyy seuraaviin asioihin: terveellisyys ja turvallisuus, viihtyisyys ja motivaatio, tehokkuus ja tuottavuus, hyvä ergonomia, yksilöllisyys ja vaikutusmahdollisuus sekä valaistuksen merkitys. Laboratoriotiloissa erityisesti vetokaapit ja muut erikoispoistot tuovat oman spesifisen haastavuuden ilmanvaihdon suunnitteluun. Laboratorioilmanvaihto jaetaan, kuten muissakin teollisuuskiinteistöissä, yleisilmanvaihtoon (sekoitusilmanvaihto, syrjäytysilmanvaihto ja piennopeusilmanvaihto) ja paikallisilmanvaihtoon (kohdeilmanvaihto ja kohdepoistot). Tarpeenmukainen ilmanvaihto, kuten uuden sukupolven Wise-järjestelmässä, soveltuu laboratoriokohteisiin, joissa ilmanvaihto noudattaa piennopeusilmanjakoa, ja jolla säästetään energiaa sekä tuloilmalla voidaan tarvittaessa suojata työntekijää tai prosessia. Vanhassa rakentamismääräyskokoelmassa (D2 2003) todetaan seuraavaa:

> ”Laboratorioiden ilmavirrat suunniteltavatapauskohtaisesti ja ilmanvaihdon tarpeenmukainen käyttö on oltava mahdollista (liite 1 taulukko 9). Ilmavirtoja on voitava ohjata kuormituksen ja ilman laadun mukaan käyttötilannetta vastaavaksi (kohta 3.2.3). Ilmanvaihtojärjestelmän toimintaa on voitava ohjata ja valvoa (kohta 3.1.3)”.

Kuten rakentamismääräyskokoelman kohdista voidaan päätellä, soveltuu tarpeenmukainen ilmanvaihto tapauskohtaisesti myös laboratoriotilojen ilmanvaihtoratkaisuksi. [28]

3.5 Soveltuvuus teollisuusympäristön valvomoihin

Teollisuusympäristöstä riippuen valvomot sijaitsevat usein tuotanto- ja prosessitilojen välittömässä läheisyydessä ja usein näissä tiloissa on jatkuva päivystys tai lähes jatkuva

päivystys. Se mikä tekee näissä työskentelevien ihmisten riskialttiiksi sisäilmatekijöille, on se, että hyvin usein nämä tilat sijaitsevat tuotanto- ja prosessitilojen välittömässä läheisyydessä. Valvomotyöntekijät viettävät usein samassa tilassa 6-10 tuntia, joten riski sisäilmasairauksille kasvaa, jos ilman epäpuhtaudet eivät ole hallinnassa ja tuotantotilojen kemialliset kaasut pääsevät vapaasti tai lähes vapaasti kulkeutumaan näihin valvomotiloihin. Usein myös ihmiset toimivat näiden vaarallisten kemikaalien ja hajujen kuljettajina ja usein näissä valvomoissa ihmiset kulkevat toistuvasti tuotanto- ja valvomotilojen välillä, jolloin ihmisiin kontaminoidut hajut ja epäpuhtaudet usein kulkeutuvat heidän mukanaan tiloista toiseen. Erona on kuitenkin hyvin stabiili ilmanvaihto verrattuna teollisuus- ja tuotantotilojen häiriövirtauksiin, minkä johdosta tarpeenmukainen ilmanvaihto on hyvä vaihtoehto, lisää viihtyvyyttä ja voi vähentää sairaspoissaoloja hyvän sisäilmaston johdosta. Energiataloudellisesti tarpeenmukainen ilmanvaihto on kuitenkin kannattavinta tiloissa, joissa käytön kuormitusaste vaihtelee. Teollisuuden valvomot eroavat yleisilmanvaihdon osalta eri standardien mukaan hyvinkin paljon ja kansallisissa standardeissa voi olla hyvinkin paljon eroavaisuuksia. Esim. Ruotsin SSG 3700 -standardissa on hyvin tarkat määräykset tuotantotilojen valvomoiden yleisilmanvaihdolle.

3.6 Soveltuvuus teollisuuden toimistoihin

Teollisuuden toimistot ovat usein samalla tapaa kuin valvomot erotettu itse tuotantoprosessista erillisiin tiloihin. Riippuen toimitiloista, teollisuuden toimistot voivat sijaita aivan tuotannon välittömässä läheisyydessä, esim. vanerikuituväliseinällä eroteltu tuotannosta tai ne voivat sijaita kokonaan eri rakennuksessa. Erona valvomotiloihin toimistoissa ei useinkaan ole jatkuvaa päivystystä vaan normaali käyttöaika on toimistotyöaika. Samalla tavoin, kuin valvomotilojen osalta erona on hyvin stabiili ilmanvaihto verrattuna teollisuus- ja tuotantotilojen kohdeilmavaihdon häiriövirtauksiin, minkä johdosta tarpeenmukainen ilmanvaihto on hyvä vaihtoehto ja energiataloudellisesti kannattavaa erityisesti silloin kun käytön kuormitusaste vaihtelee suuresti.

4 Vertailu eri toimittajien välillä

Seuraavassa esitetään eri vertailunäkökohtia ilmanvaihtojärjestelmien kokonaistoimittajien ja ilmanvaihtoon liittyvien automaatiolaitetoimittajien välillä.

4.1 Vertailu langattomien ilmanvaihtojärjestelmätoimittajien välillä

Langattomiin IV-kokonaisratkaisutoimittajiin kuuluivat ainoastaan laitetoimittajat, joilta löytyivät valmispaketit, jotka sisältävät IV-koneen, ohjausjärjestelmän, säädinyksiköt ja langattomat anturit, joissa käytetään IoT-tekniikkaa ilmastointilaitteiden ohjaamiseen.

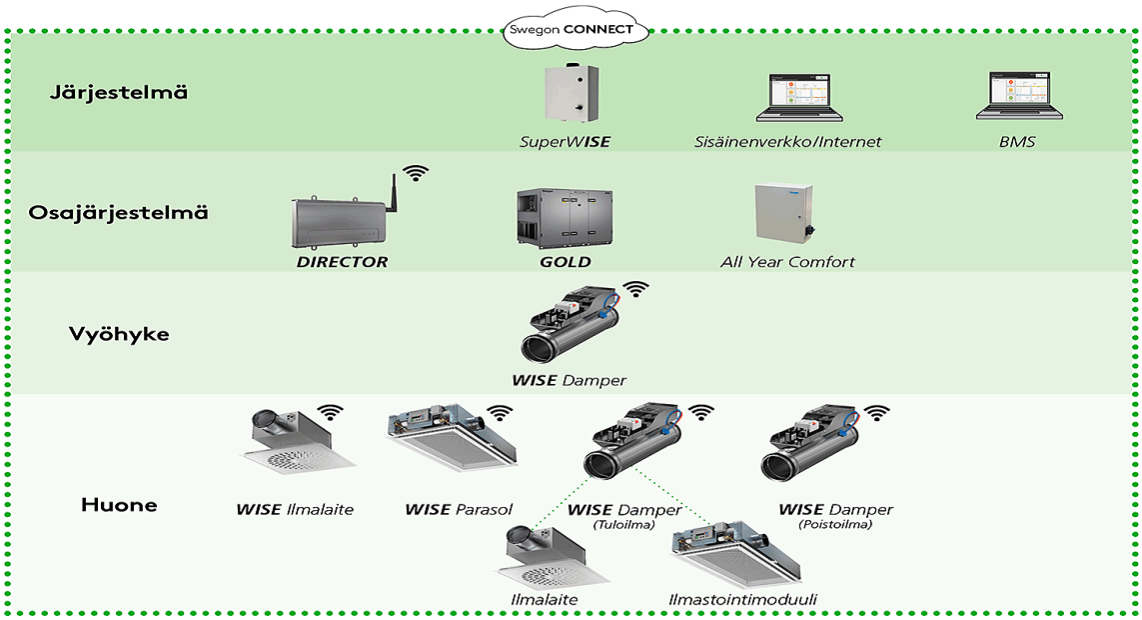
4.1.1 Swegon Gold -ilmanvaihtokone + Wise-ilmanvaihtojärjestelmä

4.1.1.1 Ilmanvaihtokone

Swegon tarjoaa yhdessä Wise-ilmanvaihtojärjestelmän kanssa yhteensopivana Gold-ilmanvaihtokonetta pakettina, jossa suurin ilmamäärä on 9 m^3/s. Swegon Gold-ilmanvaihtokone ei ole pakollinen Wise-järjestelmän osalta, mutta Swegon suosittelee käytettäväksi Swegon Gold-ilmanvaihtokonetta. [29]

4.1.1.2 Ohjausjärjestelmä

Kuvassa 12 on esitetty koko Wise-järjestelmän rakenne. Wise-järjestelmän ohjausyksikkö, koostuu uuden sukupolven Super Wise II -tiedonsiirtoyksiköstä. Super Wise II -tiedonsiirtoyksiköitä on olemassa kahta eri mallia, joista SC-malli (Swegon Connect) pitää sisällään mobiiliverkkoon kytkettävän reitittimen. Lisäksi Super Wise II -tiedonsiirtoyksikkö mahdollistaa Swegon Connect -pilvipalvelun avulla suoran kytkeytymisen rakennusautomaatiojärjestelmään. Lisäksi keskeinen osa uuden sukupolven Wise-järjestelmää on Director-keskusohjausyksikkö, joka toimii järjestelmän tukiasemana IV-koneelle ja langattomille antureille. Director lähettää, vastaanottaa ja käsittelee ohjauskäskyt Super Wisen, kenttälaitteiden ja antureiden välillä. [30]



Kuva 12. Swegon Wise-järjestelmärakenne [30]

4.1.1.3 Kenttälaitteet (= päätelaitteet ja säätimet)

Wise-järjestelmän kenttälaitteet pitävät sisällään laajan kirjon erilaisia päätelaitteita, kuten tulo- ja poistoilmahajoittajia, ilmastointipalkkeja ja säädinyksiköitä. Päätelaitteita on mahdollista saada älykkäällä langattomalla ohjauksella tai ilman. Kun halutaan päätelaitteisiin tuoda äly mukaan, pystytään jokaista päätelaitetta ohjaamaan yksitellen ja tällöin vaaditaan ainoastaan yksi säädinyksikkö huoneen haarakanavaan. Kustannuksia voidaan säästää, kun valitaan päätelaitteet ilman älyä ja yhden säädinyksikön huoneen haarakanavaan. [30]

4.1.1.4 Kenttäväylät ja TCP/IP-yhteydet

Kenttäväyläyhteytenä uuden sukupolven Wise-järjestelmä mahdollistaa Modbus- ja BACnet -parikaapeliyhteydet sekä RJ45 Ethernet -kaapeliyhteyden, jossa valittavana on https (salattu) tai http (salaamaton) -portit. Wise-järjestelmässä kaapeliyhteydet kytketään Super Wise II -tiedonsiirtoyksikön, Director-keskusohjausyksikön ja Gold-ilmanvaihtokoneen välillä. Kaikille kolmelta laitteelle on määritelty Swegonin toimesta oma staattinen IP-osoite, jos muuta käyttöverkkoa ei ole. Swegon uuden sukupolven Wise-järjes-

telmä voidaan asentaa myös kiinteistöihin, joissa ei ole nykyaikaista automaatiojärjestelmää, kuten DCS, ja tällöin Swegonin uuden sukupolven Wise-järjestelmän tietoliikenne toimii ainoastaan anturiverkon, Director-keskusohjausyksikön, Gold-ilmanvaihtokoneen ja Super Wise II -tiedonsiirtoyksikön välillä. Tällöin laitteen etäyhteys tapahtuu Swegon Connect -pilvipalvelun tai kiinteistön oman pilvipalvelun kautta. [30]

4.1.1.5 Anturit

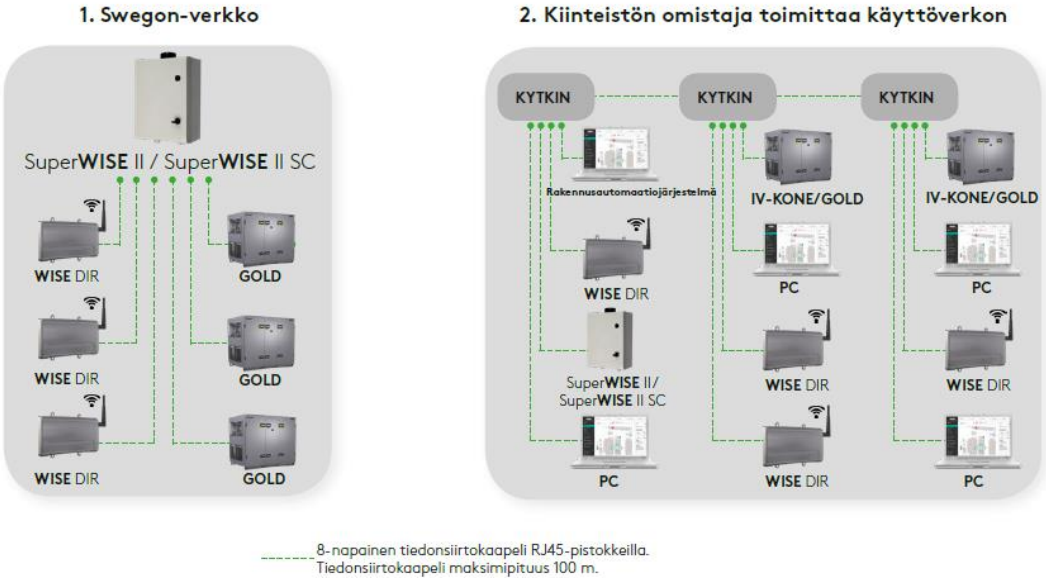
Kaikki Swegonin Wise-järjestelmän anturit myydään lisävarusteena. Swegonin Wise-järjestelmään on saatavilla seuraavia antureita:

- Wise IAQ MULTI-ilmanlaatuanturi: VOC, CO_2 ja RH% ja °C mittaukset
- Wise IAQ CO_2-ilmanlaatuanturi: CO_2 ja RH% ja °C mittaukset
- Wise IAQ VOC-ilmanlaatuanturi: VOC ja RH% ja °C mittaukset
- Wise IORE: verkon vahvistinanturi
    - voi ohjata Swegonin WISE-sisäilmastojärjestelmässä tuotteita, joilla ei ole omaa tiedonsiirtoa
    - käytetään kondenssianturin lukemiseen sekä toimilaitteiden ja muiden valmistajien tuotteiden ohjaukseen
    - mahdollistaa vesikiertoisien tuotteiden integroinnin WISE-järjestelmään
    - toimii samalla järjestelmän vahvistimena muille antureille.
- Wise IRT-huonelämpötila-anturi, joka mittaa samalla lattian pintalämpötilaa
- Wise IRE: analoginen ja digitaalinen kommunikaatiosilta antureille, joilla ei ole omaa tiedonsiirtoa
- Wise OCS: yhdistetty läsnäolo-, kosteus- ja lämpötila-anturi
- Wise RTA: lämpötilan mittaus ja asetusarvosäädin yhdellä digitaalitulolla
- Wise RTS: lämpötila-anturi
- Wise WCS: yhdistetty ikkuna- ja ovi kosketin. [30]

Lisäksi järjestelmän antureihin kuuluu TuneWise-käsipääte, jota käytetään tuotteiden toiminnan testaukseen ja Scanner TuneWise, jota käytetään yhdessä TuneWisen kanssa kunkin tuotteen tunnistamiseen ja pariliittämiseen Wise-järjestelmän toimintojen kanssa. Huomionarvoista on, että Swegon Wise -antureiden käyttöönoton saa tehdä TuneWisellä ainoastaan valtuutettu ja koulutettu Wise-huoltoteknikko. Lisäksi antureiden

puhdistuksen saa tehdä ainoastaan kuivalla liinalla, eikä vettä, puhdistusaineita tai pölynimuria saa käyttää puhdistukseen, ja lisäksi antureita ei saa sijoittaa auringonvalolle tai vedolle altistuviin paikkoihin. [30]

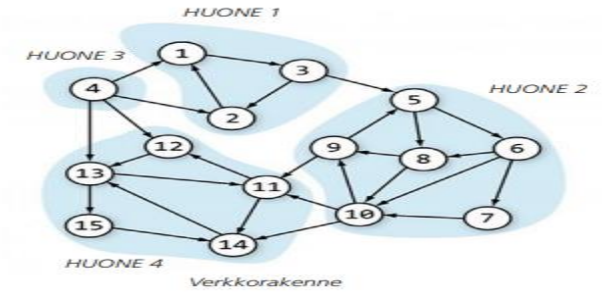
4.1.1.6 Käyttöverkko ja radioverkko



Kuva 13. Kaksi eri tapaa liittää laitteisto verkkoon [30]

Kuvassa 13 on esitetty kaksi eri tapaa Swegon Wisen kytkemiseksi verkkoon. Ensimmäinen tapa tarkoittaa laitteiston kytkemistä laitteiston Swegonin verkkoon ensin kiinteästi kiinteistöverkon kautta esim. LAN-yhteydellä Super Wise II -tiedonsiirtoyksiköltä tai Super Wise II SC -tiedonsiirtoyksiköltä suoraan Swegonin pilvipalveluun sisäänrakennetun 4G-reitittimen avulla. Toinen tapa koskee kiinteistönomistajan halua kytkeä Wise-järjestelmän ilmanvaihtokoneet ja niiden Director-keskusohjausyksiköt suoraan rakennusautomaatiojärjestelmään, jolloin kiinteistön omistaja vastaa käyttöverkon toimituksesta. [30]

Kuvassa 14 on esitetty Swegonin Mesh-radioverkon rakenne, josta on kerrottu lisää luvussa 5. Mesh-radioverkolle on tyypillistä kaikkien antureiden ja päätelaitteiden toimiminen reitittiminä radiosignaalin siirtämisessä.



Kuva 14. Swegonin Mesh-verkkorakenne [30]

4.1.2 Climecon MyAir -ilmanvaihtojärjestelmä

Climeconin MyAir-järjestelmä on suunniteltu erityisesti painovoimaisien kerros- ja asuintilojen ilmanvaihtoon. Järjestelmä pitää sisällään huippuimurin ja/tai kammiopuhaltimen, keskusyksikön, paine-eromittarin, käyttöliittymän, 100mm ja 125mm venttiilit sekä tehostuspainikkeet. Kuvassa 15 on esitetty MyAirilla saavutettavia hyötyjä ja keskeisenä hyötynä korostetaan juuri tarpeenmukaisuutta erityisesti kerrostaloasunnoissa, joissa poistoilmanvaihto on vain osan vuorokauden kellonaikoina päällä. [31]

Kuva 15. Climeconin MyAir-järjestelmän hyödyt [31]

4.1.2.1 Ilmanvaihtokone

Järjestelmä pitää sisällään Climeconin huippuimurin ja mahdollisesti kammiopuhaltimen tapauskohtaisesti suunniteltuna ja asennettuna [31].

4.1.2.2 Ohjausjärjestelmä

Climeconin MyAir-järjestelmä on suunniteltu kerros- ja asuintilojen erillispoistoilmanvaihtoon. Climacon MyAir-järjestelmä hyödyntää IoT-tekniikkaa ja sen keskusyksikkönä toimii pilvipalvelu ja näyttöpaneeli. Järjestelmän ohjaus perustuu tehostuspainikkeiden toimintaan sekä automaattiseen säätöön, joka perustuu tilan kosteuteen ja/tai lämpötilaan. Kuvassa 16 on esitetty yksinkertainen kuvaus Climeconin MyAir-pilvipalveluratkaisusta. [31]

Kuva 16. Climecon MyAir -järjestelmäkuvaus [31]

4.1.2.3 Kenttälaitteet (= päätelaitteet ja säätimet)

Climeconin MyAir koostuu kolmentyyppisistä kenttälaitteista, jotka ovat venttiili, tehostuskytkin ja paine-eromittari. Kummatkin kenttälaitteet sisältävät prosessoriin tallennetun älyn ja langattoman radiolähettimen ja vastaanottimen. [31]

4.1.2.4 TCP/IP

Climecon MyAir voi olla yhteydessä RJ45-kaapelilla rakennusautomaatioon tai pilvipalvelun avulla [31].

4.1.2.5 Anturit

Climecon MyAir -paine-eromittari toimii järjestelmän ainoana mittausanturina, ja se mittaa tilan lämpötilaa, kosteutta ja staattista painetta ja paine-eroa [31].

4.1.2.6 Käyttöverkko ja radioverkko

Käyttöverkkona Climeconin MyAir-järjestelmässä käytetään internetpohjaista pilvipalvelua ja 4G-, 3G- tai 2G-mobiilidataverkkoja, joissa tieto on mittaustietoa, joka voidaan tallentaa tai siirtää rakennusautomaatioon. Radioverkkona antureiden ja ohjausjärjestelmän välillä käytetään Lora-radioverkkoyhteyttä 868 Hz:in taajuudella. [31]

4.2 Vertailu ei-langattomien ilmanvaihtojärjestelmätoimittajien välillä

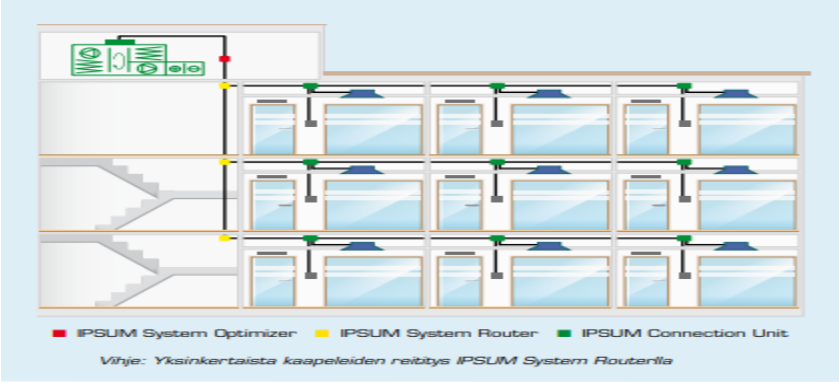
Ei-langattomiin IV-kokonaisratkaisutoimittajiin kuuluivat ainoastaan laitetoimittajat, joilla on valikoimassa valmispaketti, joka sisältää IV-koneen, ohjausjärjestelmän, säädinyksiköt ja tavalliset kenttäväyläyhteydellä tai analogisella/digitaalisella virtaviestillä toimivat anturit.

4.2.1 FläktWoods eQ/eQL -ilmanvaihtokone + IPSUM-ilmanvaihtojärjestelmä

4.2.1.1 Ilmanvaihtokone

Fläktwoods IPSUM-ilmanvaihtojärjestelmää suositellaan käytettävän eQ-sarjan paketti- tai eQ/eQL-sarjan moduuli-ilmanvaihtokoneiden kanssa, joissa suurin ilmamäärä voidaan kasvattaa moduulirakenteisilla eQL-sarjan koneilla jopa 30 m^3/s, mutta yli 20 m^3/s ilmavirroilla ylittyy määräysten mukainen SFP-luku 1,8 kWh/(m3/s). [32]

4.2.1.2 Ohjausjärjestelmä



Kuva 17. Järjestelmäkuvaus Ipsum-ilmanvaihtojärjestelmästä [32]

FläktWoodsin ohjausjärjestelmän keskeisen ytimen muodostavat kuvassa 17 esitetyt Ipsum-järjestelmän optimoija-ohjauskeskus – järjestelmän älykkyys tiedon prosessointiin –, Ipsum järjestelmä reititin – tiedon siirtämiseen oikeaan tilaan ja oikealle säätimelle – ja Ipsum huoneisto tai vyöhykekohtainen liitäntäyksikkö käyttöpaneeleille, säätöpelleille ja päätelaitteille. Ipsum-järjestelmäohjauskeskukset ovat ilmanvaihtokonekohtaisia ja voidaan linkittää FläktWoodsin eQ Smart Web -pilvipalveluun ilmanvaihtokoneen Climatix-paneeliohjauslaitteen avulla. Yhtä ilmanvaihtokonetta kohden voi Ipsum-järjestelmä sisältää yhden Ipsum-järjestelmäoptimoijan, max 30 Ipsum-järjestelmäreititintä ja max 300 Ipsum-järjestelmän huoneisto/vyöhykekohtaista liitäntäyksikköä sekä teoreettisesti max 3,000 tuloilmahajoittajaa tai 4,600 aktiivista jäähdytyspalkkia. [32]

4.2.1.3 Kenttälaitteet (= päätelaitteet ja säätimet)

Kuva 18. Esimerkki Fläkt Woods Ipsum-järjestelmän laitteista [32]

Ipsum-ilmanvaihtojärjestelmään kuuluu olennaisesti erilaisia päätelaitteita ja säätimiä. Kuvassa 18 on esitetty esimerkki Fläkt Woodsin Ipsum-järjestelmän laitteista, jossa keskeiset kenttälaitteet ovat EMSS-virtaussäädin, huonesäädin, aktiivinen Optimix-tuloilmalaite sekä lämmityksen toimilaite. Kaikki kenttälaitteet ja anturit kytketään Ipsum-liitäntäyksikköön. Lämmitystä ja jäähdytystä ohjataan sekvenssiohjauksella, joka tarkoittaa Ipsum-järjestelmässä sitä, että ensin lämmitetään tai jäähdytetään ilmalla ja vasta sitten vedellä nopeamman vasteajan saavuttamiseksi. [32]

4.2.1.4 Kenttäväylät ja TCP/IP

Ipsum -järjestelmä tukee Modbus- ja BACnet-kenttäväyläprotokollia sekä 0-10 VDC:n analogista ja digitaalista viestintää. Ipsum-järjestelmäoptimoijassa on lisäksi ethernet-verkkoa tukeva avoin Modbus- ja BACnet-tietoliikenneväylä. Lisäksi jotkin kenttälaitteet, kuten lämmityksen toimilaite toimii ainoastaan digitaalisella/analogisella virtaviestillä. [32]

4.2.1.5 Anturit

Keskeiset anturit Ipsum-järjestelmässä ovat ulkoinen ja ilmanvaihtokoneen sisäinen lämpötila-anturi, läsnäolotunnistin, CO_2-anturi, ikkunakosketin. Yhteys antureiden ja liitäntäyksikön välillä toimii ainoastaa digitaalisella/analogisella virtaviestillä. [32]

4.2.1.6 Käyttöverkko

Ipsum-järjestelmä optimoijat ja Ipsum-järjestelmäreitittimet on varustettu Internet-palvelimilla ja sisäänrakennetulla Internet-käyttöliittymällä, jossa esim. energiansäästöt näytetään reaaliaikaisesti. Käyttöverkon käyttöönotto vaatii ilmanvaihtokoneen kytkemisen Ipsum-järjestelmä optimoijaan ja ilmanvaihtokoneen puhaltimen ohjausmahdollisuuden. Internet-käyttöliittymä helpottaa järjestelmän käyttöönottoa, kun järjestelmän älykkäisiin ja tasapainotusta helpottaviin toimintoihin pääsee käsiksi Internet-palvelimen kautta, joka näyttää järjestelmään kytketyt laitteet tikapuukaavion muodossa [32].

4.2.2 Lindab Pascal -ilmanvaihtojärjestelmä

Lindabin tuotevalikoimaan eivät kuulu ilmanvaihtokoneet, mutta valikoimassa on kattavasti erilaisia ilmanvaihdon päätelaitteita ja ilmanjakolaitteita sekä Lindab Pascal -järjestelmä. Ilmanvaihtokoneen liittäminen Lindab Pascal -järjestelmään onnistuu ainoastaan 0–10 V:n virtaviestillä. [33]

4.2.2.1 Ohjausjärjestelmä

Lindab Pascal -järjestelmä muistuttaa hyvin paljon Fläkt Woodsin järjestelmää ja on samalla tavoin optimoitu järjestelmä. Erona muihin järjestelmiin on kuitenkin Internet-palvelimen, -kenttäväylän ja pilvipalvelusovelluksen puuttuminen järjestelmästä, jolloin järjestelmä voidaan liittää suoraan ainoastaan rakennusautomaatioon. Pascal-järjestelmän ohjauksen muodostaa päätason Regula-master-ohjauskeskus ja vyöhyketason Regula-

master-ohjauskeskus. Päätason ohjauskeskus kerää tietoa vyöhyketason ohjauskeskukselta ja säätää puhallinnopeutta tarpeenmukaisesti. Vyöhyketason ohjauskeskus kerää tietoa tuloilmasäätimiltä tuloilmavirroista ja säätöpeltien asennoista, ohjaa poistoilmasäätimiä tuloilmasäätimien arvojen mukaisesti, lähettää tiedot päätason ohjauskeskukselle ja suorittaa toimintavarmuuden testauksen. [33]

4.2.2.2 Kenttälaitteet (= päätelaitteet ja säätimet)

Lindab Pascalin päätelaitteet eroavat muista toimittajista siinä, että Pascalin kaikki päätelaitteet ovat ei-älykkäitä hajottajia ja päätelaitteiden tarpeenmukaista ilmanvaihtoa ohjataan paineenalennuslaatikoiden avulla. Paineenalennuslaatikot ovat matalan tuloilmavirran aktiivinen paineenalennuslaatikko integroidulla ilmavirtasäätimellä sekä poistoilman passiivinen paineenalennuslaatikko. Muita säätimiä Pascal-järjestelmässä ovat erilliset tulo- ja poistoilma säätimet, itsenäinen säädinlaite (voi toimia päätason ohjauslaitteena) ja ilmavirtasäätimet. [33]

4.2.2.3 Kenttäväylät

Kenttäväyläyhteytenä järjestelmässä Exoline- tai Modbus väylä päätason ohjauskeskukselta paineenalennuslaatikoille ja huonesäätimille asti. Tulo- ja poistoilmasäätimien ja säätimien ja paineenalennuslaatikoiden välisenä yhteytenä käytetään 0–10 V:n analogista/digitaalista virtaviestiä. [33]

4.2.2.4 Anturit

Lindab Pascal -järjestelmän läsnäoloanturit on integroitu päätelaitteisiin ja lämpötila-anturi on integroitu paneenalennuslaatikon tuloilmakanavaan. Tuloilmasäädinlaitteeseen on myös integroitu hiilidioksidianturi ja valittavana on säädinlaite, johon on integroitu kosteusanturi. [33]

4.2.2.5 Käyttöverkko

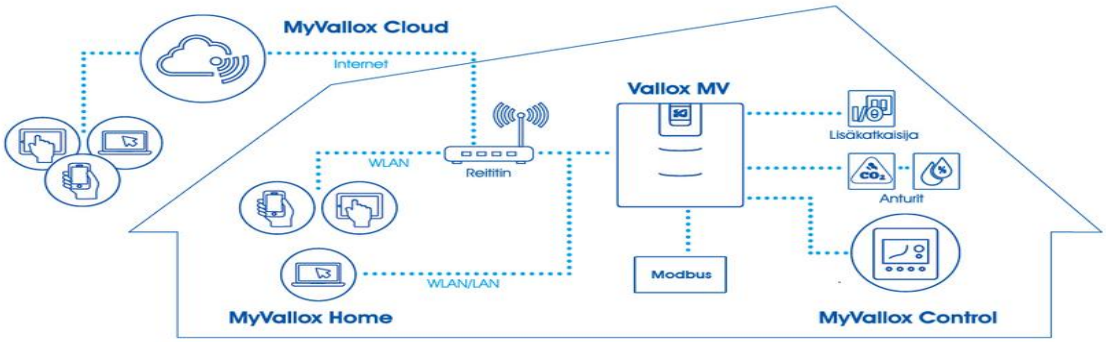
Omaa käyttöverkkoa Lindab Pascalissa ei ole, vaan vaihtoehtona on ainoastaan liittää rakennusautomaatioon Modbus- tai Exoline kenttäväylän avulla [33].

4.2.3 MyVallox-ilmanvaihtojärjestelmä

4.2.3.1 Ilmanvaihtokone

MyVallox-tuoteperheen ilmanvaihtokoneet ovat kaikki MV-luokan koneita, joista isoin 245 MV on tarkoitettu isojen omakotitalojen ja toimistojen ilmanvaihtokoneeksi. Koneen maksimi-ilmavirrat ovat tulolle 245 l/s ja poistolle 265 l/s, ja sen ominaissähköteho eli SFP-luku on ainoastaan 0,7 kWh/(m³/s). [34]

4.2.3.2 Ohjausjärjestelmä



Kuva 19. Kuvaus MyVallox-ilmanvaihtojärjestelmästä [34]

Kuvassa 19 on esitetty MyVallox-ilmanvaihtojärjestelmästä, jossa ohjausjärjestelmä on toteutettu MyVallox Control -ohjausyksiköllä, joka toimii järjestelmän älynä eli siirtää, vastaanottaa ja prosessoi tietoa. Ohjausjärjestelmään kuuluu myös Vallox MV -tiedonsiirtoyksikkö, joka yhdistää pilvipalvelun, käyttöliittymän, anturit ja katkaisijat sekä kenttäväyläyhteyden rakennusautomaatiojärjestelmään. MyValloxin ohjaus perustuu neljään

eri tilavalintaan (kotona, poissa, tehostus ja takkatoiminto), lämpötilaohjaukseen ja automaattisiin – erikseen ohjelmoitavissa oleviin – hiilidioksidi- ja kosteusohjauksiin. [34]

4.2.3.3 Kenttälaitteet (= päätelaitteet ja säätimet)

MyVallox-järjestelmään ei kuuluu päätelaitteita, mutta yhdistettäessä MyVallox-ilmanvaihtojärjestelmä samaan kokonaisuuteen esim. Vallox BlueSky -ilmanjakojärjestelmän kanssa saadaan venttiilit ja ilmanjakolaatikot mukaan. Venttiileissä ei ole älyä eli mikroprosessoreita mukana. Järjestelmän säätölaitteina toimivat MyVallox Control -ohjauskeskus sekä lisäkatkaisija eli poissaolokytkin, jotka säätävät suoraan koneen ilmavirtoja eikä järjestelmässä ole erillisiä säätöpeltejä. [34]

4.2.3.4 Kenttäväylät

Kenttäväyläprotokollana MyVallox-järjestelmässä on Modbus-yhteys IV-koneelle, MyControl-ohjausyksikölle sekä antureille. Lisäksi järjestelmä hyödyntää TCP/IP-verkkoyhteyttä RJ45-kaapelilla reitittimelle MyVallox-pilvipalveluun tai MyVallox Home -kotiverkkoon. [34]

4.2.3.5 Anturit

MyVallox-järjestelmään on saatavilla erilliset hiilidioksidi- ja huoneen kosteusanturit. Ilmanvaihtokoneisiin on integroitu ilmankosteusanturi. Anturit yhdistetään Modbus-parikaapeliyhteydellä tai analogisella/digitaalisella 24 voltin virtaviestijohdoilla Vallox MV -yksikköön. [34]

4.2.3.6 Käyttöverkko

Käyttöverkkona MyVallox-laitteessa toimii WLAN- tai LAN-yhteys kotiverkkoon sekä pilvipalveluyhteys kodin ulkopuolella. MyVallox-pilvipalvelun käyttö edellyttää ilmanvaihtokoneen kytkemistä LAN-kaapelilla reitittimeen. [34]

4.3 Vertailu langattomien automaatiojärjestelmätoimittajien välillä

Seuraavassa on esitetty suppeaa vertailua eri automaatiojärjestelmätoimittajien välillä, joilta löytyy valikoimasta erilaisia langattomia antureita, kenttälaitteita ja pilvipohjaisia ohjausjärjestelmiä, mutta ilmastointituotteet, kuten päätelaitteet, ilmanvaihtokoneet ja säätöpellit puuttuvat valikoimasta.

4.3.1 Schneider Electric

4.3.1.1 Kiinteistöhallintajärjestelmät

Shneider Electric toimittaa sekä laajamittaisia EcoStruxure Building Operation -pilvipalveluita usean kiinteistön kattavaksi integroiduksi ohjelmistoksi kiinteistöjen suorituskyvyn optimointiin että Ecostruxure Building Expert -pilvipalveluita pienten ja keskisuurten kiinteistöjen hallintaohjelmiksi. Keskeisen integraatiorajapinnan muodostaa kuvassa 20 oleva SpaceLYnk -logiikkaohjain, jolla voidaan yhdistää kiinteistöautomaation ja energiamittauksen standardeja ja protokollia sekä hallita kaikkia rakennuksen keskeisiä ohjauksia. Käyttöliittymänä toimii PC, kiinteät kosketusnäytöt tai mobiililaitteet. SpaceLYnk tukee BACnet-, Modbus-, KNX-kenttäväyläprotokollia sekä Internet-protokollaa, joilla eri osajärjestelmät, kuten ilmanvaihto, valaistus, kulunvalvonta, lämmitys ja jäähdytys, lisäksi logiikkaohjain voidaan integroida kiinteistöautomaatioon esim. Shneiderin EcoStruxure -pilvipalveluun. [35]

Kuva 20. Schneiderin logiikkakontrolleri [35]

4.3.1.2 Langattomat kenttälaitteet ja anturit sekä tuetut radioverkot

Langattomien antureiden osalta Schneider luottaa yksinomaan EnOcean- ja ZigBee- radioverkon standardeihin. Kuvassa 21 on esitetty vasemmalla Schneiderin Multi-purpose Manager, jossa on sisäänrakennettuna Schneiderin EcoStruxure Building Expert- lisenssivapaa verkkokäyttöliittymä, joka tukee EnOcean- ja ZigBee-standardeja ja useita MPM-UN-laitteita voidaan yhdistää toisiinsa IP/Ethernetin (BACnet) tai langattoman ZigBee Mesh-verkon avulla ketjutettuna väylänä. Kuvassa 21 on keskellä Zigbee- ja EnOcean-verkon muuttuvailmavirtainen säätölaite ja oikealla langattoman Zigbee- ja EnOcean-verkon tukiasema. Kaikki kuvan MPM-laitteet tukevat myös Zigbee- ja EnOcean-verkon lisäksi Modbus-, CANbus- ja analogisia virtaviestejä. [36]

Kuva 21. Scheinerin toimittamat EnOcean- ja ZigBee- radioverkkostandardien langattomat hallinta, säätö ja tukiasemalaitteet [36]

4.3.2 Ouman

4.3.2.1 Pilvipalvelut ja ohjausjärjestelmät

Ouman toimittaa langattomia Ounet-nettivalvomoita yhdessä kaikkien olemassa olevien yksikkösäätimien kanssa pois lukien EH-800-yksikkösäädin. Kaikki oumanin yksikkösäätimet tukevat Modbus-protokollaa ja 0-10 voltin virtaviestejä. Lisäksi saatavilla on vapaasti ohjelmoitavan Ouflex-järjestelmä. Nykyään monissa asuinkerrostalokiinteistöissä järjestelmät ovat Ouman-yksikkösäätimien avulla liitetty joko kiinteistön omaan rakennusautomaatiovalvomoon tai Ouman-nettivalvomoon. Omasta kiinteistöhuoltokokemuksesta voin todeta, että trendi on sekä monissa pienissä toimitila- että asuinkerrostalokiinteistöissä ollut ajaa vanhoja valvomoita alas ja liittää Ouman-yksikkösäätimellä nettivalvomosovellukseen. [37]

4.3.2.2 Langattomat kenttälaitteet ja anturit sekä tuetut radioverkot

Ouman Wireless on langaton mittausjärjestelmä, johon kuuluu tukiasema, reitittäviä lämpötila-antureita ja tavallisia lämpötila-antureita. Järjestelmään kuuluu siis ainoastaan lämpötila-antureita lämpötila- ja kosteusmittausominaisuudella, ja ne muodostavat itsereitittävän mesh-verkon reitittävien antureiden osalta. Tukiasema voidaan liittää modbus-protokollalla vain tietyn tyyppisille säätimille. Radioverkkona Wireless-mittausjärjestelmä käyttää tukiaseman ja antureiden välillä 6Lowpan radioverkkoteknologiaa ja anturit toimivat paristoilla. Ouman itse mainostaa, että järjestelmä on asennettavissa yhdessä päivässä, minkä ansiosta ei ainoastaan asennusjohtojen asennuskustannukset pienentyisi vaan myös aikaa säästyisi huomattavasti. [38]

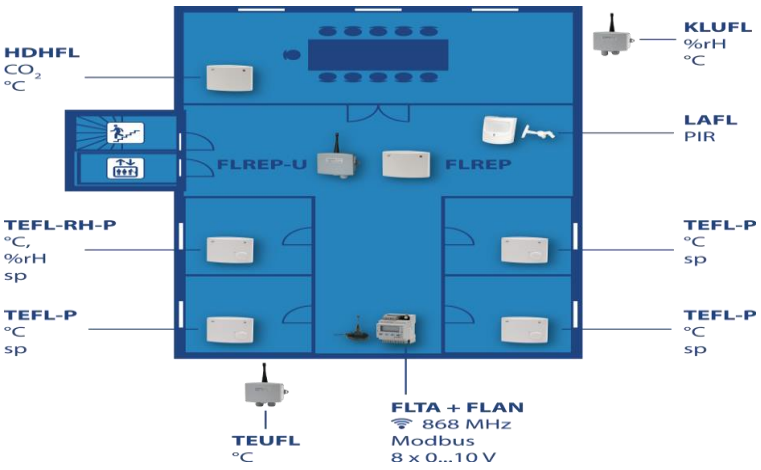
4.3.3 Produal

4.3.3.1 Pilvipalvelut ja ohjausjärjestelmät

Produal on vastikään tullut vasta mukaan langattomien IoT-ratkaisujen markkinoille. Tällä hetkellä Produalilta löytyy langattomia toimistoratkaisuja, ja ohjausjärjestelmänä toimii MyTool-kännykkäsovellus yhdistettynä Produalin MyCloud-pilvipalveluun. [39]

4.3.3.2 Langattomat kenttälaitteet ja anturit sekä tuetut radioverkot

Produalilla on langaton toimistoratkaisu, johon kuuluu tukiasema, vahvistin, säädinlaitteet ja langattomat anturit. Radioverkkona Produalin langattomassa verkossa käytetään BLE-Mesh-tyyppistä verkkoa, joka perustuu Bluetooth low energy verkkostandardiin. Kuvassa 22 on esitetty Produalin langaton toimistoratkaisu. [39; 40.]



Kuva 22. Produalin toimistoratkaisukokonaisuus [34]

Kuvassa 22 esitetyt eri anturit vasemmalta ylhäältä alkaen:

- HDHFL – langaton hiilidioksidi ja lämpötilalähetin
- KLUFL – langaton ulkokosteus- ja lämpötilalähetin

- FLREP-U – langaton toistin ulkokäyttöön
- FLREP – langaton toistin sisäkäyttöön
- LAFL – langaton läsnäoloanturi
- TEFL-RH-P – langaton huonelähetin lämpötilan ja kosteuden mittaamiseen
- TEFL-P – langaton huonelähetin lämpötilan mittaamiseen
- TEUFL – langaton ulkolämpötilalähetin
- FLTA+FLAN – langaton tukiasema ja antenni. [40]

4.4 Päätelmät vertailutulosten perusteella

Edellä esitettyjen vertailujen perusteella valittiin kokonaiskustannusvertailua varten Swegonin uuden sukupolven Wise-ilmanvaihtojärjestelmä, koska tämä oli vertailunäkökohdista ainoa toimittaja, joka toteutti sekä langatonta tiedonsiirtoa ja älykkäänä teknologiana pidettäviä IoT-ratkaisuja älykkään anturiteknologian avulla, joilla voidaan asennuskustannuksia saada minimoitua. Kuten edellisistä vertailuista voi todeta, Suomessa älykkäiden ja erityisesti langattomien ilmanvaihtojärjestelmäratkaisujen markkinat ovat vielä hyvin nuoria, mutta erityisesti rakennusautomaation langattomien ratkaisujen kiinnostus ja toteutukset ovat kasvaneet korjausrakentamisessa, jossa halutaan säästää kaapelointikustannuksia. Suomessa ja muuallakin maailmassa langatonta tiedonsiirtoa kiinteistöjen automaatiokehityksessä ovat edesauttaneet mikrokontrollereiden nopea kehitys ja halventuneet hinnat. Kehitys on ollut seurausta elektroniikkakomponenttien ja mikrokontrollereilla (esim. Arduino ja Raspberry Pi) ohjattujen kodinautomaatiolaitteiden kiinnostuksesta kuluttajamarkkinoilla. Kodin automaatioratkaisut erityisesti IoT-tekniikan

avulla ovat ensimmäistä kertaa alkaneet ohittamaan automaatioasteen muodossa toimitilojen rakennusautomaatioon sidoksissa olevat laitteet ja järjestelmät, mutta kuitenkin tämä on aiheuttanut laitteiden tietoturvan osalta merkittäviä ongelmia.

5 Langattomat tiedonsiirtotekniikat

5.1 Langaton tiedonsiirto yleisesti

Langaton tiedonsiirton perustuu eri radiotaajuuksien käyttöön ja radioaaltojen ominaisuuksiin sekä digitaalisen tiedon siirtämiseen. Langaton tiedonsiirto samalla tavoin kuin langallinen tiedonsiirto noudattaa ISO OSI -standardia, mutta ero on erityisesti pakettidatan välityksen ja langattoman puheenvälityksen osalta mobiiliverkkojen avulla. Koska kyseessä on radioliikennettä hyödyntävä tiedon siirto, langaton tiedonsiirto perustuu myös radioliikenteen, ITU-, IEEE- ja ETSI-standardeihin. Langaton tiedonsiirto perustuu keskeisesti tietoliikennetekniikan, radiotekniikan (RF-tekniikka) ja elektroniikan hyödyntämiseen. Langattomassa ja digitaalisessa tiedonsiirrossa signaalikomponenttien välitys perustuu digitaalisignaalikomponenttien moduloimiseen, joka tarkoittaa digitaalisignaalikomponentin muuntamista binäärimuodosta analogiseen (loogiseen) muotoon ja liittämistä radioliikenteen kantoaaltoon ottaen huomioon siirtotien ominaisuudet. Kun analoginen signaali palautetaan takaisin luettavaan digitaaliseen muotoon, puhutaan demoduloimisesta. [41, s.7-9.]

Langattomassa tiedonsiirrossa radioaallot ovat tilassa vapaasti liikkuvia sähkömagneettisia aaltoja, joiden energia esiintyy samanaikaisesti sähköisinä- ja magneettisina kenttinä ja muutos sähkökentässä aiheuttaa vastaavasti muutoksen myös magneettikenttään ja päin vastoin. Langattomassa tiedosiirrossa yhteys syntyy radiotien eli radiotaajuuden käytön välityksellä, jolloin lähettäjän ja vastaanottajan välille syntyy tietty kanavanvaraus. Kanavanvarausperiaate jakatuu radiotekniikassa erilaisiin tekniikoihin, joita ovat esim. FDMA-, TDMA- ja CDMA-tekniikat. [41, s. 21-24.]

Radioliikenteessä radioaallot lähettäjältä vastaanottajalle saapuvat eri teitä ja eri voimakkuuksilla vastaanottajan antennille, jolloin radioaallot summautuvat ja vastaanottaja näkee yhden signaalin ja riippuen lähettäjän ja vastaanottajan signaalikomponenttien vaihe-erosta vastaanottaja voi saada signaalin vahvistettuna, jolloin kahden vierekkäisen antennin vastaanottamat signaalit voivat vaihdella jopa kymmeniä desibelejä toisistaan. [41, s. 10.]

Suomessa radiotaajuuksien käyttöä ohjaa viestintävirasto, koska käytettävissä olevat radiotaajuudet ovat rajoitetut, ja radiotaajuuksia käyttävien laitteiden määrä lisääntyy koko ajan. Kiinteistöissä yleisin vapaa taajuus on 2,4 GHz:ia, ja entistä enemmän otetaan käyttöön myös 5 GHz:in taajuudella toimivia WLAN-verkkoja ja laitemäärän lisääntyessä myös häiriömahdollisuus lisääntyy. [41, s. 1.]

5.1.1 Langattoman tiedonsiirron yleiset ongelmat

Keskeisimmän ongelman radioliikennetekniikassa on aiheuttanut aiemmin kaksi rinnakkain samalla taajuudella olevaa lähetintä, jotka häiritsevät toistensa lähetyksiä. Tämä on pyritty korjaamaan standardoinnin avulla, jonka keskeisenä standardoinnin edelläkävinä ovat olleet ITU-standardit ja suositukset. [41, s. 11.]

Yleiset radioaaltojen ongelmat aiheutuvat radioaaltojen ominaisuuksista, radiolaitteiden haitoista ja radioaaltojen liikkuvuuden ongelmista. Langattomassa tiedonsiirrossa radioaallot saavat aikaan etenemistä, vaimenemista, häipymistä, monitie-etenemistä sekä doppler-ilmiöitä. Radioaallon etenemisestä aiheutuvat ongelmat liittyvät usein kuuluvuusalueen epäsymmetrisyydestä, maastosta, esteistä, radioaallon pituudesta ja katvealueista, ja tällöin vastaanottimen ja lähettimen välillä syntyy ns. kohinaa. Vaimeneminen on radioliikenteessä ongelma, joka johtuu signaalin sisältämän tehon vähentymisen aiheuttamasta signaalin sisältämän resistanssin muuntumisesta lämmöksi, jolloin signaalin amplitudi heikkenee. Signaalin vaimeneminen on hyvin riippuvainen käytetystä siirtotiestä ja käytetystä taajuudesta. Häipyminen on ongelma, joka johtuu joko hitaasta tai nopeasta häipymisestä. Hidas häipyminen tarkoittaa vastaanotetun signaalin keskiarvon muuttumista ja on riippuvainen mm. maaston muutoksista ja näköesteistä. Nopea

häipyminen taas johtuu sekä lähettimen liikkeestä että monitie-etenemisestä. Monitie-eteneminen on ongelma, joka johtuu signaalipulssin leviämisestä ja heijastumisesta ympäristössä olevista esineistä. Monitie-etenemisessä signaalin kulkema matka saattaa kasvaa jopa kaksinkertaiseksi verrattuna lyhimpään, jolloin sen kuljettama energia on aiempaa pienempi ja heijastuva signaali saapuu perille ”väärään aikaan”, jolloin se saa aikaan ns. kaikuilmiön. Doppler-ilmiö aiheutuu signaaliaaltojen lukumäärän poikkeamasta lähettäjän ja vastaanottajan välillä, joka on suoraan riippuvainen lähettäjän ja vastaanottajan etäisyyden muutoksen suuruudesta aikayksikköä kohden. Doppler-ilmiötä esiintyy myös nopean häipymisen ja monitieheijastumisen yhteydessä. [41, s. 11-18.]

Digitaalisessa tiedonsiirrossa edellä esitetyt ongelmat aiheuttavat sen, että mitä enemmän häiriötä on datan siirtotiellä, sitä enemmän vääristyy siirrettyjä bittejä. Virheellisten bittien lukumäärän suhteesta siirrettyjen bittien kokonaismäärään käytetään nimitystä bittivirhesuhde (eng. Bit Error Rate lyh. BER). [41, s. 19.]

5.1.2 Langattomien tiedonsiirtotekniikoiden vertailuja

5.1.2.1 Langattomat laajakaistatekniikat

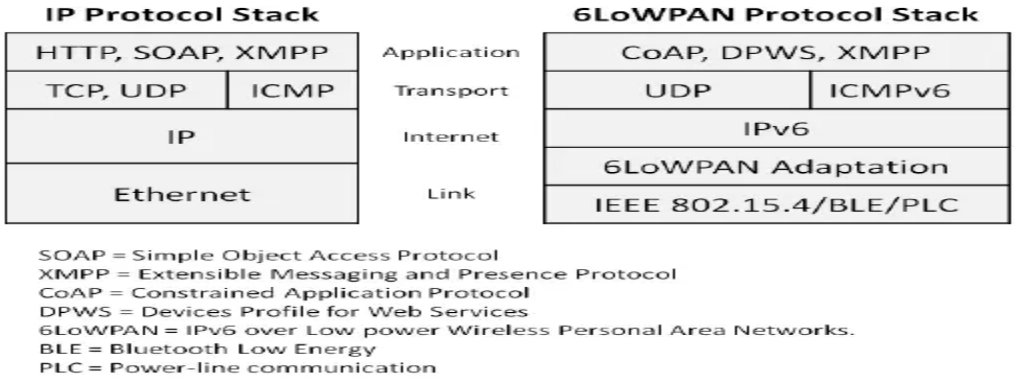
Langattomista laajakaistatekniikoista käytetään usein nimitystä langattomat mobiiliverkkotekniikat. Langattomat laajakaistatekniikat tunnetaan myös yleisnimityksillä 3G- ja 4G-yhteydet. Mobiiliverkkoihin kuuluu näiden lisäksi 2G- ja tekstiviesti eli SMS-tekniikat. Näiden erona on se, että 3G- ja 4G-tekniikat toteutetaan pakettimuodossa, jolloin ne soveltuvat myös normaalissa Internet-verkossa käytettäviksi tekniikoiksi, jolloin ne erotetaan toisistaan käyttämällä nimitystä mobiilidatayhteys ja WLAN-verkossa käytetään nimityksiä 3G- ja 4G-laajakaistayhteydet.

5.1.2.2 Langattomat keskipitkän ja pitkän kantaman lähiverkkotekniikat

Langattomista keskipitkän paikallisista (LAN) ja pitkän kantaman (WAN) langattomista verkoista käytetään usein nimitystä WLAN, joka on tunnetuin langattomien verkkojen nimitys. Langattomasta lähiverkkotekniikasta käytetään usein nimitystä WiFi, joka on puhtaasti kaupallinen markkinointinimitys WLAN-verkkotekniikalle. Viime vuosina WLAN-tekniikan nopeudet ja kantamat ovat kasvaneet huomattavasti, esim. vuonna 2016 julkaistu standardi IEEE 802.11ac kasvatti WLAN-verkon kantaman 1,1 kilometriin, josta voidaan puhua jo pitkän kantaman langattomasta verkosta (Wide Area Network, WAN). Uusimmasta WLAN-tekniikasta (standardi IEEE 802.11ax) kerrotaan lähemmin kappaleessa 5.1.3.1 ja siihen liittyvästä tietoturvasta kappaleessa 6.5.5.8.

5.1.2.3 Langattomat lyhyen kantaman verkkotekniikat

Lyhyen kantaman verkkotekniikoiden suosio ja kehitys on kasvanut viime vuosina huomattavasti, koska niiden käyttöä mahdollistaman M2M-tekniikan (Machine to Machine) kehitys on avannut markkinat IoT-laitteiden (esineiden Internet) yleistymiselle. Samalla tavoin kuin langattomissa laajakaista- ja lähiverkkotekniikoissa niiden viestintätekniikka perustuu viestien siirtämiseen analogisessa radioverkossa, mutta selkeitä eroja on internet-protokollatasoon liittyvän siirtotason ja sovellustason osalta sekä radiosignaalin sovituksen osalta, kuten kuvasta 23 käy ilmi.



Kuva 23. Internet-protokollapinon ja 6LoWPAN-protokollapinon erot [42]

6LowPan-radiotekniikka perustuu IEEE 802.15.4 -standardiin, johon kuuluu suuri joukko muitakin esineiden Internetiä (IoT) hyödyntäviä radiotekniikoita. Taulukossa 1 on esitetty joukko muita yleisimpiä globaalin taajuuskäyttöalueen (2,4 GHz) lyhyen kantaman esineiden Internetiä hyödyntäviä radiotekniikoita ja niiden eroavaisuuksia. Taulukossa 1 älypuhelinintegraatio on vain harvoissa tekniikoissa, kuten bluetooth-tekniikkaan liittyvissä IoT-sovelluksissa. Tietoturvan kannalta tämä tietysti voi olla tietysti hyvä asia, mutta käyttäjäystävällisesti välttämättä ei. Mesh-verkko liittyy fyysiseen verkkotopologiaan eli kuinka eri radioverkkoon liitetyt eri anturit ja laitteet muodostavat yhteyden toisiinsa. Mesh-verkkotopologiaa kuvataan usein, niin että kaikki laitteet ovat toisiinsa yhteydessä, jolloin puhutaan usein peer-to-peer-yhteydestä, joka tarkoittaa sitä, että kaikki anturit ja laitteet Mesh-verkossa ovat itse reitittäviä eli toimivat verkossa samalla lähettäjänä ja vastaanottajana. Taajuushyppely tarkoittaa sitä, että radioverkon laitteet pystyvät vaihtamaan radioverkon signaalin taajuutta 2,4 GHz:in ja 5 GHz:in radiotaajuuskaistojen välillä, joka vähentää radioverkon ja tietoverkon välillä esiintyvien bittivirheiden (BER) määrää. Protokollan kompleksisuus kuvaa kuvassa 23 esiintynyttä protokollapinoon liittyvää rakenteen monimutkaisuutta. Energiankulutus taas viittaa siihen, että IoT-laitteet toimivat usein paristojen varassa, kuten anturit, ja mitä vähäenergisempi laitteiden ja antureiden energiankulutus on, sitä toimintavarmempi ja huoltovapaampi se on jatkossa. Osoitteistus taas taulukossa 1 viittaa eri käytössä oleviin tiedonsiirtotekniikoihin. IoT-laitteiden tiedonsiirtotekniikkana on alettu viime vuosina suosimaan IPv6 tiedonsiirtotekniikkaa, joka perustuu Internetprotokollan version 6 mukaiseen tekniikkaan. [43]

Taulukko 1. Yleisimpiä IoT-verkkojen radiotekniikoita ja niiden eroavaisuuksia [43]

	Älypuhelin-integraatio	MESH-verkko	Taajuus-hyppely	Protokollan kompleksisuus	Energian-kulutus	Osoitteistus
Bluetooth	kaikissa	-	kyllä	*****	*****	Bluetooth
Bluetooth Smart (ent. BLE)	uusissa	lisäkerros	kyllä	**	*	Bluetooth/ IPv6
ANT+	joissakin	jonkinlainen	ei	**	*	ANT
Wireless HART	ei	kyllä	kyllä	***	**	HART
ISA100.11a	ei	kyllä	kyllä	****	**	IPv6
ZigBee	ei	kyllä	ei	**	*	ZigBee / IPv6
WIA-PA	ei	kyllä	kyllä	***	**	IPv6

Kuvassa 24 on esitetty lisää eri esineiden Internetiä (IoT) hyödyntäviä verkkotekniikoita sekä verrattu niitä muihin tekniikoihin, kuten GSM-, SMS-, Wifi- ja langattomiin IoT-tekniikoihin.

Realm	Technology	Typical Application	Reliable Range* (typical) All Highly Environmetally Dependent (walls, etc)	Data Rates (typical)	Power/Batt. Life (typical)	Topology (message hopping)	Cost	Notes
A	Bluetooth Low Energy (BLE)	Personal Device Control Wearables	~ 25 meters		Years	No (Not Typically) Point-to-Point		Everybody's Smartphone has a BLE Radio
A	WiFi	Personal Device Contol "Always On" Home						Everybody's Smartphone has a WiFi Radio!
B	6LoWPAN	Moderate Area Sensor Networks Factory Floors Connected Landscape	~ 250+ meters (depends on "hops")	Low/variable	Years			
C	LoRa/LoRaWAN		multiple kilometers	low depends on range (little "blips" of info e.g. temperature measurements, on/off controls, car engine status, etc.)		LoRaWAN - No Custom LoRa Protocol - Yes		Maturity LoRa (not LoRaWan) can perform message hopping
C	GPRS, ... , LTE, ... (smartphone digital data)	remote installations (near cell towers)	multiple kilometers				HW + Subscription	
C	GSM/SMS (text msg)		multiple kilometers				HW + Subscription	Old, Large installed infrastructure (3rd world, 1st world)
			* Range values are somewhat pessimistic and different from published/more optimistic values					

Kuva 24. Vertailu eri radioverkkojen ulottuvuuksista [44]

5.1.3 Uusimmat langattomat tiedonsiirtotekniikat

5.1.3.1 IEEE 802.11ax Wifi 6 -tekniikka

IEEE 802.11ax -standardista käytetään usein nimitystä WiFi 6, ja se on uusi langattomien verkkojen sertifikaatti, joka ilmestyi lokakuussa 2018. Sertifikaatti on vapaaehtoinen laitevalmistajille ja sen tarkoitus on varmistaa laitteiden yhteensopivuutta laitevalmistajien keskuudessa ja lisätä verkon kapasiteetti-, kattavuus- ja suorituskykyvaatimuksia, jotka ovat nykyään olennaisia korkean luokan sovelluksissa. Wifi 6 -sertifikaatti perustuu IEEE 802.11ax -standardiin, joka on ideaalinen verkkorakennetekniikka langatto-

maan verkkoon, johon on liitetty useita langattoman verkon päätelaitteita. Wifi 6 -tekniikan avulla monet käyttäjät ja laitteet pysyvät yhteydessä toisiinsa samanaikaisesti ja tekevät asioita, kuten korkean luokan teräväpiirtoelokuvien streemaus ja käyttävät kaistanleveyttä vaativia kriittisiä liiketoiminnan sovelluksia. Wifi 6 parantaa sekä 2,4 GHz:in että 5 GHz:in spektristä tehokkuutta, parantaa korkean vaatimustason ympäristöllisiä haasteita ja parantaa WiFi-verkon kapasiteettia nelinkertaisesti edellisestä standardista. [45]

5.1.3.2 5G-mobiiliverkkojen langaton laajakaista

5G-mobiiliverkkojen kehityksen myötä väitetään antureiden määrän kasvavan huomattavasti ja antureiden akunkeston pidentyvän jopa 10 vuoteen sekä tiedonsiirtonopeuden kasvavan kymmenkertaiseksi nykyisestä, joka tarkoittaa samalla kaistanleveyden kasvamista nykyisestään. 5G-mobiiliverkon on tarkoitus tulla kuluttajamarkkinoille 2019-2020, mutta laitteiden valmistus pilotointia ja erilaisia kaupallisia kokeiluja varten on jo alkanut. Uusi tekniikka vaatii täysin uudet laitteet, koska nykyisissä laitteissa ei ole 5G-valmiuksia. Esineiden internetin väitetään myös 5G-tekniikan myötä yleistyvän, ja yhä useammat laitteet ovat yhteydessä Internetiin, joka lisää tarvetta myös verkossa suojautumisen osalta. [46]

5.2 Langaton tiedonsiirto Wise-järjestelmässä

5.2.1 Antureiden langaton tiedonsiirto

Verkkotekniikka uuden sukupolven Wise-järjestelmässä on Lumenradion kehittämä Mira Mesh -tyyppinen käyttöjärjestelmäratkaisu, ja käyttöjärjestelmä perustuu Lumenradion patentoituun vielä tällä hetkellä ainoaan markkinoilla olevaan sulautettuun käyttöjärjestelmään langattomalla Mesh-verkkopinolla, joka toteuttaa kognitiivista rinnakkaiseloa. Radiotekniikkana Mira Mesh -verkko käyttää 6LowPAN-radiotekniikkaa ja IP-protokollana IPv6:sta. Lumenradion kehittämään kognitiiviseen rinnakkaiseloon perustuvaa sulautettua käyttöjärjestelmää suojaa yhdysvaltalainen vuonna 2013 haettu patenttisuoja

(Patent US 8,565,176 B2) ja kognitiivinen rinnakkaiseloon perustuva malli, joka hyödyntää monikäyttäjän havaitsemiseen perustuvaa langatonta viestintätekniikkaa mukautuvalla häiriönsietoisuudella. [47; 48; 49.]

5.2.2 Langattomuus muissa järjestelmän osissa

Swegonin uuden sukupolven Wise-järjestelmän tiedonsiirto esim. automaation DCS-järjestelmään on mahdollista toteuttaa langallisena tai langattomasti esim. pilvipalvelun kautta. Eräs tapa toteuttaa etäyhteys pilvipalveluun on käyttää erillisiä Gateway-laitteita, josta esimerkkinä on Siemensin Industrial IoT2040-Gateway kuvassa 25. Erilaisia langattomia integrointi- ja toteutustapoja tehtaan automaatio-ohjausjärjestelmään on esitetty luvussa 7.2. [50]

Kuva 25. Siemens IoT2040 Gateway [50]

6 Tieto- ja kyberturvallisuus

6.1 Tieto- ja kyberturvallisuus käsitteenä

Yrityksissä on usein tietoteknistä turvallisuutta tarkasteltu tietoturvavallisuuden näkökulmasta, jolloin kohteena on ollut yritysten tietopääoma. Tietoturvan tavoite on ollut yrityksissä turvata tiedon luotettavuus, eheys ja saatavuus. Kyberturvallisuus käsitteenä on tietoturvaa yksityiskohtaisempi näkökulma, joka tuo esiin ihmisten ja datamaailman yh-

dessä muodostaman turvallisuuskokonaisuuden, ja nykyisessä maailmassa kasvava tietoturvallisuus ei enää yksinään riitä kuvaamaan automaatio-ohjauslaitteisiin kohdistuvaa tietoturvallisuus uhkaa, jossa tärkeyskriteerit tiedon osalta ovat eri järjestyksessä kuin talouden ja tietotekniikan osalta. [51, s. 44]

Ensimmäisiä tunnettuja teollisuusautomaatioon kohdistuneita kyberhyökkäyksiä tiedetään tapahtuneen 2000-luvun alussa. Esimerkkinä Hansol Paperilla USA:n Idahossa sattui räjähdys 28.12.2006, joka aiheutti paperikoneiden tuhoutumisen ja puolet koko paperitehtaasta. Tällöin kyberhyökkäystä ei ollut naamioitu tarpeeksi, ja Pt100 lämpötila-anturi aiheutti usein hälytyksen tehtaan automaatiojärjestelmään ylilastauksen takia. Ongelmana oli kuitenkin huoltotiimin tietämättömyys kyberuhkasta, ja tällöin luulona oli pikemminkin lämpötila-anturin viallinen toiminta ja lopulta anturi poistettiin järjestelmästä. Toimintaa jatkettiin keskeytyksettä 6 viikon ajan ajaen paperikonetta ylikuormituksella, kunnes tehtaalla tapahtui räjähdys, johtuen koneen lämpötilasta 1400 °C, vaikka maksimilämpötilaraja oli 110 °C ja hälytysraja 85 °C. [52]

6.1.1 Tietoturva ja IoT

IoT:n tietoturvariskit liittyvät pääsääntöisesti siihen, että IoT-teknologioita käyttävät verkot, ovat joko UDP- tai TCP/IP-verkkoja, ovat useimmiten kytkeytyneenä täysin julkiseen internetiin. Useimmiten IoT:n mahdollistamat tietoturvariskit kohdistuvat järjestelmän tietomurtoihin, datayhteyden riittämättömään suojaukseen, ohjelmistovirheisiin tai haittaohjelmien aiheuttamiin uhkiin. IoT-tekniikoiden laajentuneet järjestelmät tarjoavat lisää ohjelmointirajapintoja, joissa on sekä hyvät että huonot puolet, koska uudet ohjelmointirajapinnat tarjoavat sekä uusia tietoturvauhkia että uusia suojautumiskeinoja. Pelkästään VPN- ja TLS/SSL- pohjaiset ratkaisut ovat hyviä suojautumiseen, mutta tosiasiassa eivät ainoastaan riitä, vaan hyvä keino on lisäksi erilaisten antivirustorjuntaohjelmien hyödyntäminen, joita on tullut markkinoille jo IoT-laitteisiin, esimerkkinä F-Securen tarjoamat palvelut IoT-verkkoihin. Lisäksi IoT-laitteiden aiheuttaman suuren tietomäärän tallentamisen kannalta erilaisten pilvipalveluihin liittyvät riskit, kuten Googlen ”EU Safe Harbor” on hyvä tiedostaa. [53]

6.1.1.1 Tietoturvan merkitys ja periaatteet esineiden internetissä

Esineiden internetiä hyödyntävissä laitteissa keskeistä tietoturvan kannalta on kaikkien verkkoon kytkettyjen laitteiden tunnistus. IoT-laitteet kytkeytyvät tuottamallaan tiedolla taustajärjestelmiin, on siksi olennaisen tärkeää varmistaa tiedon suojaus aina tietoa tuottavan laitteen, kuten anturin, suojauksesta ja yksilöinnistä tietoa välittäviin taustajärjestelmiin ja tiedon varastoinnista vastaaviin pilvipalveluihin. Keskeisinä haasteina IoT-laitteiden tietoturvan kannalta voidaan pitää seuraavia kahdeksaa tekijää:

1. Laitekohtaiset rajoitteet eri suojausmenetelmien osalta.
2. Tietoliikenteen valvontaresurssit eivät välttämättä riitä valvomaan kaikkea dataa.
3. Monet IoT laitteet toimivat suojaamattomissa ympäristöissä.
4. IoT-laitevalmistajat eivät ole luoneet pelisääntöjä verkkojen yhteensovittamiseksi.
5. Eri internetprotokollien (IPv4 ja IPv6) tietoturvaratkaisujen yhteensopimattomuus.
6. Laitteiden tietoturvan varmistaminen on lähtökohtaisesti laitevalmistajilla.
7. IoT-laitteiden osalta ei ole olemassa keskitettyä sertifiointielintä tietoturvaan liittyen.

Cisco ehdottaa IoT-laitteiden tietoturvan takaamiseksi eräänlaista Security Cloudia eli turvapilveä, joka suodattaa ja suojaa laitteiden ja pilvipalvelun välisen liikenteen. Pilvipalvelun alla on Security gateway eli turvattu yhdyskäytävä, jonka avulla estetään ulkopuolisen pääsy käsiksi IoT-laitteiden lähettämään tietoon. Alimmalla tasolla on vielä erinlaiset laitekohtaiset suojaukset ja tiedon suojaaminen taustajärjestelmissä, joista on esitetty seuraavassa listassa tyypillisimmät suojausmenetelmät:

- ECC-suojaus: IoT-laitteissa yleistymässä oleva suojausmenetelmä, joka perustuu julkisen avaimen salausmenetelmään hyödyntäen elliptisiin käyriin liittyviä laskutoimituksia
- AES 256 ja 128: ehkä tunnetuimmat salausmenetelmät, jotka perustuvat lohkosalausmenetelmiin käyttäen 128 bitin lohkoja ja kolmea avainlohkoa 128, 192, 256 bittiä (oikeasti 126, 190, 254 bittiä)
- Triple DES: iteraatioihin perustuva salausmenetelmä, jota ei voi pitää enää turvallisena johtuen siitä, että avoimeen lähdekoodin ohjelmistot eivät tue kyseisiä algoritmejä
- Blowfish: patentoimaton ja ilmainen, mutta erittäin vahva salausalgoritmi (448 bit)

- Twofish: lohkosalausalausalgoritmi, joka muistuttaa AES-algoritmia
- RSA: julkisen avaimen salausalgoritmi, johon perustuvat esim. verkkopankin salasanageneraattorit. [54]

6.1.1.2 IoT:n viestintäprotokollat ja niiden tietoturva

Seuraavassa listassa on esitetty erilaisia IoT-verkkojen viestintäprotokollia ja niihin liittyviä tietoturvaominaisuuksia.

- MQTT: avoimeen lähdekoodiin perustuva viestiprotokolla, vailla lainkaan suojausta, mutta mahdollistaa protokollan ulkopuolisen suojauksen ja kryptauksen.
- CoAP: kiinteistöautomaatioon ja sähkönkulutuksen valvontaan suunniteltu protokolla, joka pitää sisällään erittäin vahvan RSA-pohjaisen suojauksen kommunikointiin.
- XMPP-IoT: eräs turvallisimmista ja käytetyimmistä viestiprotokollista ja se tarjoaa sisäänrakennetun täyden SASL (Simple Authentication and Security Layer) -tuen.
- WebSocket: vaatii http-yhteyttä (http-yhteyden laajennus), koska ei itsessään tarjoa tiedonsiirtoprotokollaa, vaan se on lisättävä erikseen ja tietoliikenteen suojaamiseen voidaan käyttää TLS/SSL suojausta.
- AMQP: tiedonsiirtoprotokolla, joka on suunniteltu erityisesti yritysten palvelinympäristöön ja sisältää vahvan tietoturvan, tiedonvälitysviestien jonotusominaisuuden sekä erittäin suurien tietomäärien luotettavan tiedonvälitysominaisuuden.
- DDS: nopea ja luotettava tiedonvälitysprotokolla, jota käytetään mm. pankkijärjestelmissä ja lennonvalvonnan sovelluksissa ja tietoturvana protokollaan on tarjolla erillinen DDS Security -paketti, joka pitää sisällään lähetettävän viestien salauksen, varmistaa lähetettävän tiedon koskemattomuus sekä suorittaa lähettäjän ja vastaanottajan autentikointi ja auktorisointi.
- Modbus: perinteiseen automaation sarjaliikenneprotokollaan on tarjolla IoT-yhdyskäytäviä Modbus protokollaa tukeviin laitteisiin (TCP/IP), mutta tietoturvan kannalta vaatii erillisiä integroituja ratkaisuja, kuten IconLabsin Floodgate Modbus Protocol Filtering -tuote. [55]

6.1.2 Integrointiin liittyvä riskienhallinta ja kyberturva

Ulkoistettujen pilvipalveluihin liittyy integraation osalta olennainen riskitekijä. Siksi on syytä olla tarkkana laadittaessa sopimuksia pilvipalveluiden tuottajien välillä, koska tiedon omistajuuteen ja tiedon siirtymisessä eri pilvipalveluiden välillä liittyy aina erityinen riskitekijä. [56, s. 6.]

Lähiverkko on yleinen rakennusautomaation tiedonsiirtoväylä, koska se voi toimia siirtotienä kaikille rakennusautomaation integraatiotasoille kenttälaitetasoa (I/O-tasoa) lukuun ottamatta. Verkkosuunnittelun ja toteutuksen kannalta tietoturva on syytä hoitaa, niin että salaamatonta tietoa ei esiinny langattomien taloteknisten järjestelmien osalta. Käytännössä tämä tarkoittaa eri osa-alueiden liikenteen segmentointia eli jakamista omiin verkkoihin, joista ei tule olla pääsyä toisiin osa-alueisiin. Myös verkkoon liittymistä on syytä rajata erilaisilla laitteisiin ja sertifikaatteihin pohjautuvilla mekanismeilla sekä rajata fyysistä pääsyä verkkopisteisiin ja telejakokeskuksiin. [56, s. 6.]

Erilaisten langattomien antureiden, toimilaitteiden ja järjestelmien yleistyessä myös erilaisten langattomien verkkotekniikoiden integraationtarve on kasvanut. Langattomien järjestelmien hyödyntämiseen ja niiden integrointiin liittyy aina hyvin olennainen riskitekijä. Usein taloteknisten järjestelmien tiedonsiirtoprotokollat ovat täysin salaamattomia, jolloin kuka tahansa verkkoon käsiksi päässyt henkilö pystyy vähintään tulkitsemaan verkon sanomaviestintää ja pahimmassa tapauksessa myös ohjaamaan järjestelmän toimintaa tätä kautta. [56, s. 6.]

6.2 SFS/IEC 62443 ja ISO/IEC 27000 -standardien periaatteet ja käsitteet

Standardit SFS/IEC 62443 ja ISO/IEC 27000 kuuluvat teollisuuden automaatio- ja ohjausjärjestelmiin, ja standardoinnista vastaa Seskon komitea SK 65 nimeltään teollisuusprosessien mittaus ja ohjaus, joka on samalla IEC TC 65:n ja CENELEC TC 65:n vastinkomitea Suomessa. SK 65 komitean piiriin kuuluvia standardeja on jo lähes 300 kappaletta. IEC 62443 -standardi koskee teollisuuden tietoliikenneverkkojen ja järjestelmien tietoturvallisuutta, ja se jakautuu neljään eri osaan, jotka ovat:

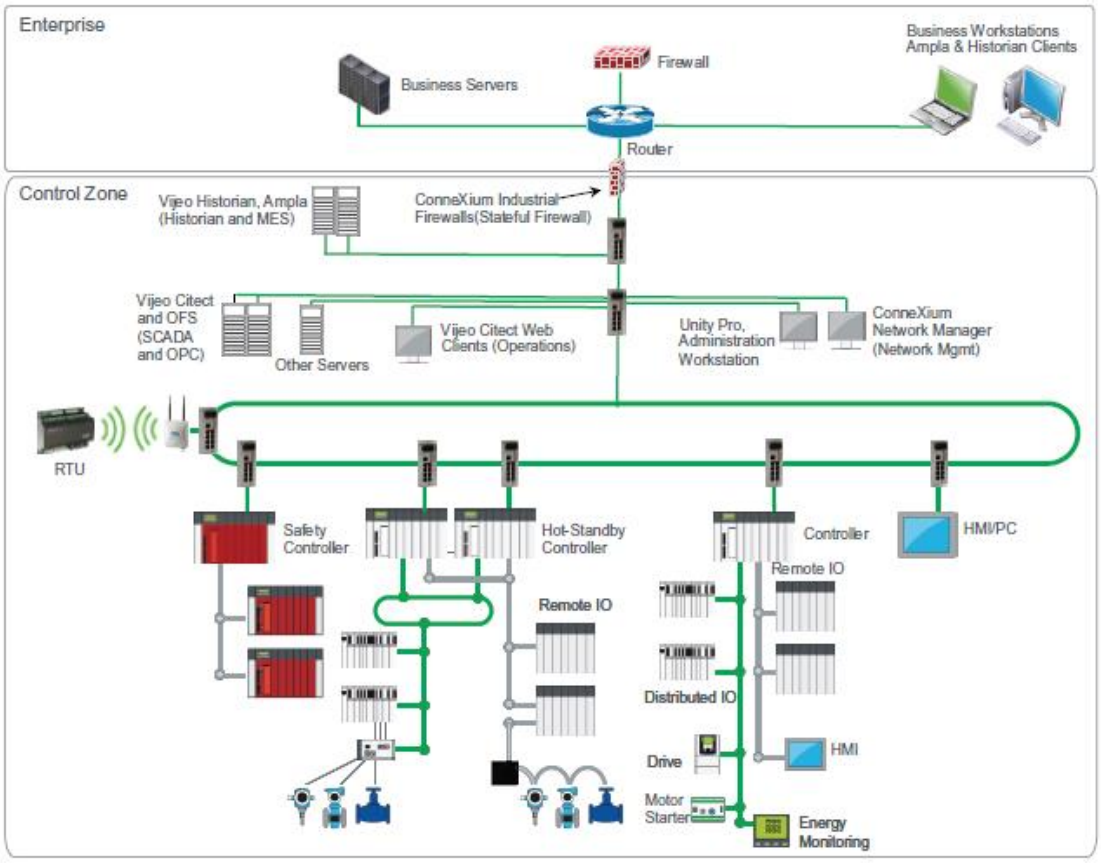
- IEC/TS 62443-1-1, osa 1-1: terminologia, käsitteet ja mallit

- IEC/TS 62443-2-1, osa 2-1: tietoturvallisuusohjelman perustaminen teollisuus-automaatio- ja ohjausjärjestelmiä varten

- IEC/TS 62443-3-1, osa 3-1: tietoturvateknologiat teollisuusautomaatio- ja ohjausjärjestelmille.

IEC 62443 -standardissa teollisuusautomaatio- ja ohjausjärjestelmille (IACS) on asetettu käänteinen prioriteetti verrattuna yleiskäyttöisiin tietotekniikkajärjestelmiin (IT) tiedon saatavuuden ja luottamuksellisuuden osalta. IT-järjestelmien osalta tiedon luottamuksellisuus on tärkeintä, kun taas IACS-järjestelmissä tiedon saatavuus on tärkeintä tiedonsiirron osalta. Tästä syystä useita tietotekniikassa käytettyjä menetelmiä ei voida täysin soveltaa teollisuuden automaatio- ja ohjausjärjestelmiin, vaikka IACS-tieto turva standardissa IEC 62443 viitataan IT-tietoturvastandardiin ISO/IEC 27001. Tietoturvallisuuden tavoitteiden osalta myös mahdolliset terveys-, turvallisuus- ja ympäristövaikutukset korostuvat teollisuuden automaatio- ja ohjausjärjestelmien osalta. [57]

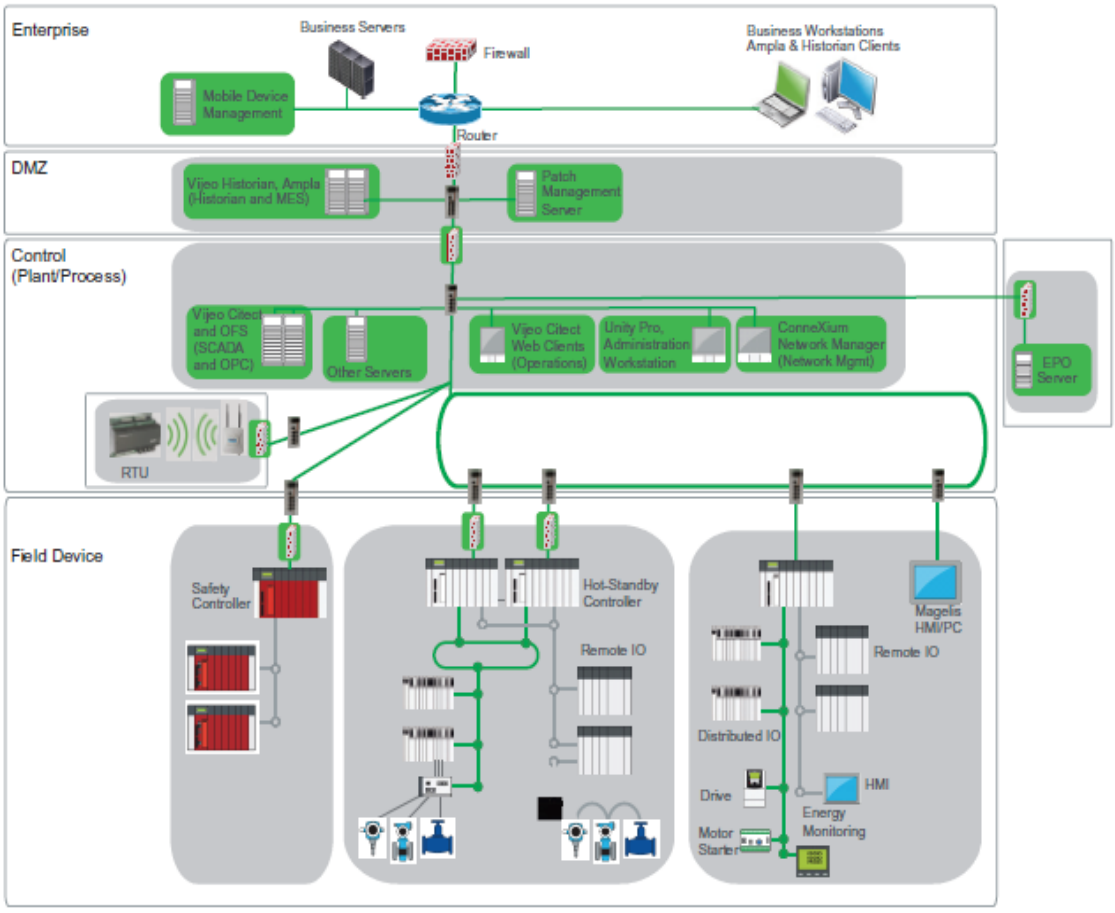
6.2.1 Turvallisuustaso 0 standardin IEC 62443-3-3 mukaisesti esitettynä



Kuva 26. Turvallisuustaso 0 standardin IEC 62443-3-3 mukaisesti esitettynä [59]

Kuvassa 26 on esitetty standardin IEC 62443-3-3 mukainen käytännönläheinen toteutus koskien 0-tason toteutusta. Keskeistä on se, että teollisuuden ohjausjärjestelmän komponentit, kuten ohjaimet, ajurit ja HMI:t (ihmiskone rajapinnat) on otettu käyttöön ympäri teollisuusverkkoa. Taso 0:n avulla estetään ainoastaan sattumanvaraisia ja tahattomia tietoturvauhkia. Esimerkkinä tietoturvauhkasta voisi olla esim. työntekijöiden vahingossa aiheuttama tuotantokatkos, johtuen puutteellisesta perehdytyksestä ja järjestelmien avoin näkymä Internetissä yleisen skannauspalvelun aiheuttamaan katkokseen. [58; 59.]

6.2.2 Turvallisuustaso 1 standardin IEC 62443-3-3 mukaisesti esitettynä



Kuva 27. Turvallisuustaso 1 standardin SFS/IEC 62443-3-3 mukaisesti esitettynä [59]

Kuvassa 27 on esitetty standardin IEC 62443 mukainen käytännönläheinen toteutus koskien 1-tason toteutusta. Kuvassa on merkitty vihreällä erot edelliseen tasoon verrattuna. Kuvassa palomuurien (punaiset pistelaatikot) ja segmentoinnin avulla on saavutettu vähimmäistaso standardin IEC 62443-3-3 mukaiselle tietoturvallisuudelle. IEC 62443-3-3 -standardissa on esitetty 37 erilaista vaatimusta kyseisen vaatimustason toteutukselle, ja nämä vaatimukset on esitetty taulukoissa liitteessä 1. Vaatimustason 1 avulla estetään tietoturvauhkia, joissa käytetään yksinkertaisia keinoja ja yleispäteviä taitoja ja hyökkääjä on aktiivinen ja omaa kohtalaiset resurssit ja matalan motivaation. Esimerkkinä tietoturvauhasta voidaan pitää eräänlaista ”Script kiddietä”, jolla tarkoitetaan henkilöä,

joka käyttää olemassa olevaa koodia tai ohjelmaa hakkeroituakseen tietokoneille ilman että tarvitsee erikoistaitoja ohjelmointitaitojen hallintaan. Vaatimustason toteutus on pilkottu seitsemään pienempään osaan, jotka on merkattu harmaalla. Nämä osat ovat:

1. DMZ (Demilitarized Zone) – aliverkko, joka sisältää ja paljastaa valvonta vyöhykkeen ulkoiset liitäntäpalvelut yritysverkkoon. DMZ:n keskeisenä ajatuksena on, että palvelimet yritysvyöhykkeellä ei pitäisi koskaan olla suorassa yhteydessä valvonnan piiriin kuuluviin elementteihin ohjaus vyöhykkeellä (tehdas/prosessitaso). Yritysten järjestelmät tarvitsevat kuitenkin pääsyn ohjausalueen tietoihin, ja elementit ohjausalueella tarvitsevat pääsyn tiedostoihin epäluotettavista verkkolähteistä (esim. laiteohjelmistopäivitykset). DMZ sisältää järjestelmät, joiden on päästävä sekä ohjaus- että yritystason laitteille.

2. Tehdas/Prosessi-ohjausvyöhyke (Control - Plant/Process) – vyöhyke palvelee tuotteita ja sovelluksia, jotka mahdollistavat tehdas- ja prosessinhallinnan.

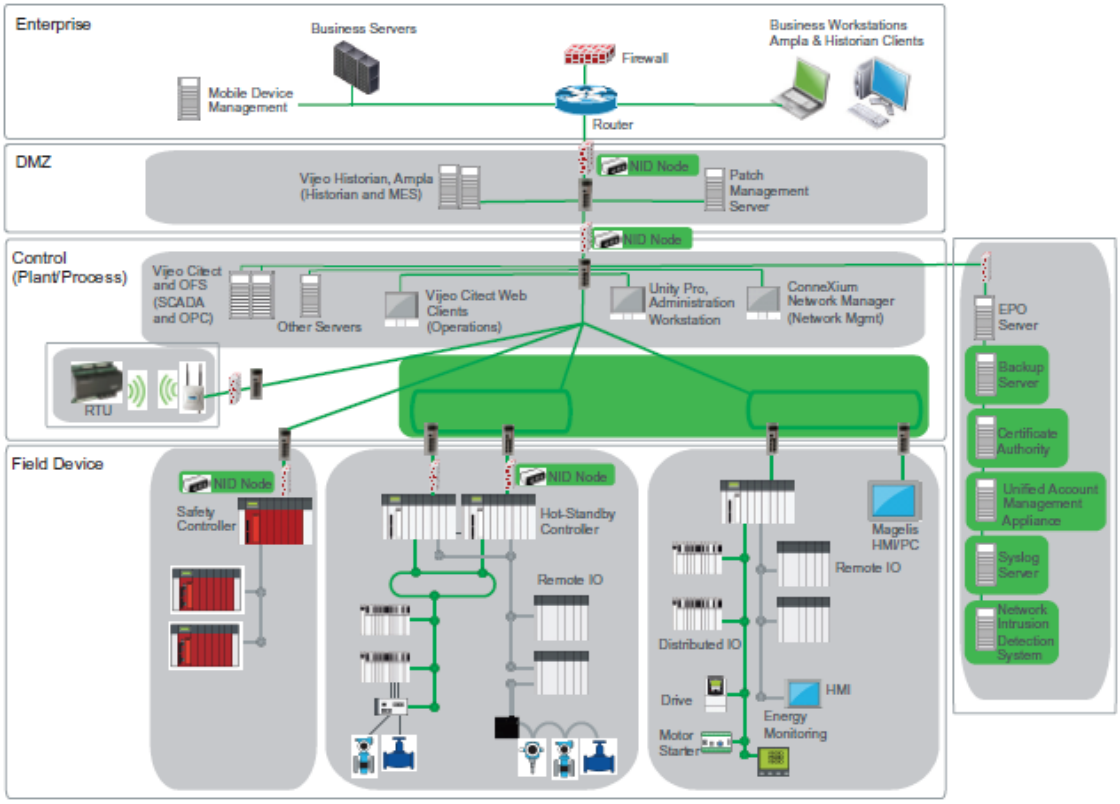
3. Turvallisuuslaitteiden vyöhyke – keskitetty vyöhyke palvelee suuria määriä turvallisuuslaitteita. Esimerkkikuvassa EPO (Ethernet Policy Orchetrator) -palvelin yhdessä sallittujen sovellusten palvelimen kanssa (Aplication Whitelisting Software) toimivat isäntänä tuotannonohjaus järjestelmälle.

4. Langaton vyöhyke – Langaton infrastruktuuri on jaettu erilliseen vyöhykkeeseen.

5. Ohjausvyöhykkeet – Kuvassa kenttälaitealue on hajotettu kolmeen eri vyöhykkeeseen. Kaksi on vakio-ohjausvyöhykkeitä, esim. HMI-ohjausvyöhyke ja vakio-kenttälaitevyöhyke, sekä kolmantena on turvavalvontalohko (Safety controller). Ohjausvyöhykkeen segmentointi on turvasuunnitelmaa koskeva tuote ja vaihtelevuus perustuu käytettävään sovellukseen. [58; 59.]

Lisäksi esimerkkikuvaan on lisätty päätasolle mobiililaitteiden hallintaserveri (yritystasolle), joka sisältää oman autentikoinnin järjestelmään.

6.2.3 Turvallisuustaso 2 standardin IEC 62443-3-3 mukaisesti esitettynä

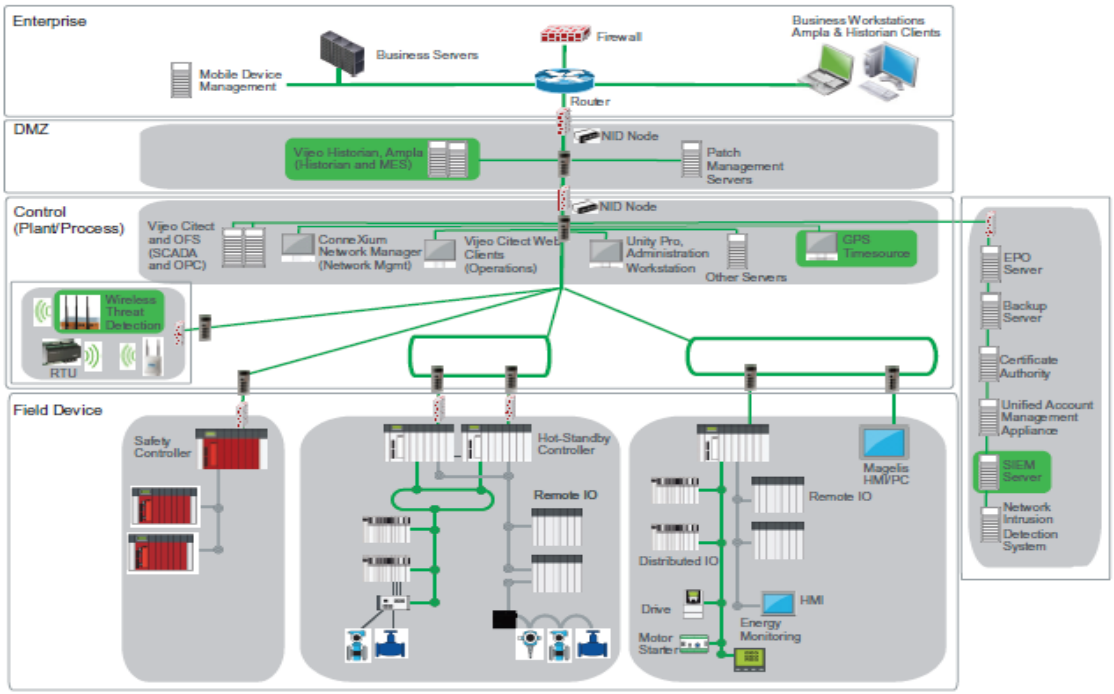


Kuva 28. Turvallisuustaso 2 standardin IEC 62443-3-3 mukaisesti esitettynä [59]

Kuvassa 28 on esitetty standardin IEC 62443-3-3 mukainen käytännönläheinen toteutus koskien 2-tason toteutusta. Kuvassa on merkitty vihreällä erot edelliseen tasoon verrattuna. SFS/IEC 62443-3-3 -standardissa on esitetty 23 erilaista vaatimusta kyseisen vaatimustason toteutukselle, ja nämä vaatimukset on esitetty taulukoissa liitteessä 1. Keskeisenä erona vaatimustaso 1 ja 2 välillä on se, että vaatimustaso 1:ssä järjestelmän on autentikoitava eli tunnistettava ja valtuutettava ihmiskäyttäjät, kun vaatimustaso 2:ssa järjestelmän on myös tunnistettava ja valtuutettava ohjelmistoprosessit ja laitteet. Samoin vaatimustasossa 1 järjestelmän on tunnistettava, raportoitava ja ehkäistävä epäilyttäviä ohjelmia ja samalla tavoin myös vaatimustaso 2:ssa, mutta vaatimustasossa 2 järjestelmän tietoturvareagointi perustuu kaikkien vyöhykkeiden sisään- ja ulostulopisteisiin. Lisäksi joissain tilanteissa vaatimustasoon 2 on lisätty joitakin tarpeita, kuten kyky

tukea tunnistesertifikaatteja. Standardit vaativat tuotteiden lisäämisen verkkoon, kuten yhtenäisen tilinhallintalaitteen, sertifikaattien varmennuslaitteen, varmuuskopiointipalvelimen, tapahtumapalvelimen ja verkon tunkeutumisen havainnointijärjestelmän. Lisäksi osana tietoturvaa palomuurien yhteyteen on asennettava verkonliitäntälaitteen solmut (NID node), joiden avulla tietoturvan reagointi saadaan aikaiseksi kaikkien vyöhykkeiden sisään ja ulostulopisteissä. Ohjausverkko on segmentoitu kahdeksi eri verkoksi, ja kaikki potentiaaliset teollisuusohjausjärjestelmän laitteet (esim. ohjelmoitavat logiikkaohjaimet) on täytynyt päivittää tukemaan uusia vaatimustason 2 mukaisia ominaisuuksia, kuten turvallisuusprotokollia. Vaatimustason 2 avulla estetään tietoturvauhkia, joissa käytetään kehittyneitä keinoja ja teollisuusautomaation tuntemusta edellyttäviä erityistaitoja sekä usein hyökkääjä on aktiivinen ja omaa kohtalaiset resurssit ja kohtalaisen motivaation. Esimerkkinä tietoturvauhasta voidaan pitää eräänlaista aktivistiryhmittymää, joilla on selkeä tavoite ja päämäärä tietoturvahyökkäykselle. [58; 59.]

6.2.4 Turvallisuustaso 3 standardin IEC 62443-3-3 mukaisesti esitettynä



Kuva 29. Turvallisuustaso 3 standardin IEC 62443-3-3 mukaisesti esitettynä [59]

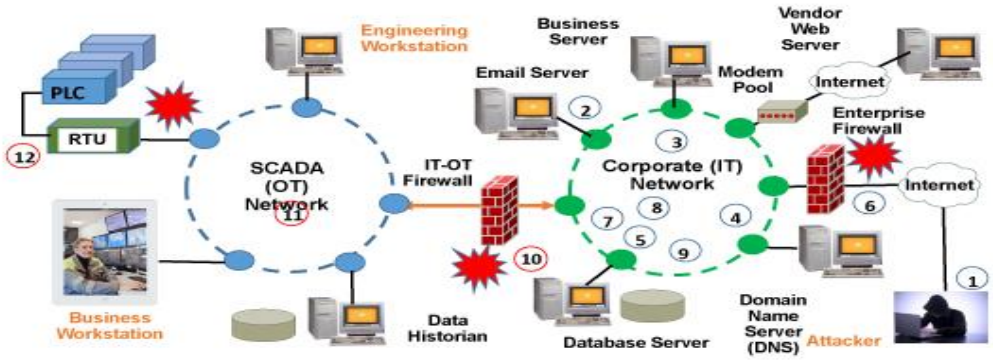
Kuvassa 29 on esitetty standardin IEC 62443 mukainen käytännönläheinen toteutus koskien 3-tason toteutusta. Kuvassa on merkitty vihreällä erot edelliseen tasoon verrattuna. SFS/IEC 62443-3-3 -standardissa on esitetty 30 erilaista vaatimusta kyseisen vaatimustason toteutukselle ja nämä vaatimukset on esitetty taulukoissa liitteessä 1. Erona aikaisempaan vaatimustasoon (vaatimustaso 2) on, että lisää turvallisuusprotokollia ja turvallisten elementtien käyttöä on lisätty salausavainten suojaamiseen. Esimerkiksi vaatimustason 2 vaatimat ominaisuudet voitiin toteuttaa päivittämällä teollisuusohjausjärjestelmän laitteisiin (kuten ohjelmoitaviin logiikkaohjaimiin) uusi ohjelma, mutta vaatimustasossa 3 myös itse laitteet tulee olla vaihdettu tai uusittu. Standardit edellyttävät myös, että vaatimustasossa 3 joitakin laitteita on lisätty verkkoon, kuten tapahtumapalvelimen vaihtuminen SIEM palvelimeksi, joka yhdistää sekä SIM (security information management) turvallisuustiedonhallinnan että SEM (security event management) turvallisuustapahtuman hallinnan. Lisäksi vaatimustaso 3 edellyttää aikaisempaan (vaatimustasoon 2 nähden), että GPS satelliitin asemaan perustuva ajanlähde laitteisto (GPS NTP Server) sekä langattoman verkon tunkeilijan havainnointilaite (IDS) / verkkoliikenneanalysaattori on lisättävä. Esimerkkinä verkon tunkeilijan havainnointilaitteista on esimerkiksi täysimittainen hyökkäyksen havannointijärjestelmä Snort, tietomurron analysointityökalu Bro, verkkoliikenneanalysaattori Silk ja NTOP sekä pakettidatan nauhoitusohjelma Moloch. Tärkeintä on verkon tunkeilijan havannointilaitetta arvioitaessa sen sopivuus organisaation tarpeisiin ja osaamistasoon. Vaatimustaso 3 avulla voidaan katsoa estävän tietoturvauhkia, joissa käytetään kehittyneitä keinoja ja teollisuusautomaation tuntemusta edellyttäviä erityistaitoja. Lisäksi hyökkäävä osapuoli on aktiivinen teoissaan ja omaa kattavat resurssit sekä korkean motivaation, kuten valtiollisen tahon puolesta tehty hyökkäys, joissa resurssit ovat aivan toisenlaisia kuin muissa hyökkäyksissä. [58; 59; 60.]

6.3 Teollisuusohjausjärjestelmän kyberturvallisuus

6.3.1 ICS Cyber Kill Chain

ICS Cyber Kill Chain (Industrial Control System Cyber Kill Chain) on alkujaan USA:n aseteollisuusyritys Lockheed Martinin kehittämä teoria teollisuusyritysten kyberhyökkäysten etenemiselle. Nykyään tunnetaan useita tapauksia, joissa kyberiskut ovat kohdistuneet prosessitason automaatio-ohjauslaitteisiin, esimerkkeinä Stuxnet-isku ja Ukrainan energiayhtiöihin kohdistuneet iskut sekä Saksan rautakaivoshyökkäys.

6.3.1.1 12 -askeleen ICS Cyber Kill Chain malli



Kuva 30. Ulkoisen ICS Cyber Kill Chain -prosessin eteneminen [61]

Kuvassa 30 on esitetty havainnollinen kuvaus ICS Cyber Kill Chain -prosessin etenemisestä, ja alla on listattu eri numeroiden avulla kuvassa esiintyvät numerot:

1. Kohteen valinta

2. Uhrin nettikäyttäytymisen oppiminen ja koneen saastuttaminen esim. liitetiedostojen avulla

3. Ensimmäinen yritys päästä IT-verkkoon – liitetiedostojen avaus aiheutti aktivointikoodin, jolla hyökkääjä skannaa IT-verkkoa, tietokoneita, salasanoja, IP-osoitteita, langattomia yhteyksiä, yms.

4. Hyökkääjä avaa käyttäjätilin ja saavuttaa asemaa saastuneessa verkkossa – käyttäjätilin ja sähköpostin avulla hyökkääjä pystyy etsimään verkon administraattorin käsiin

5. Etuoikeutetun käyttäjätilin luonti – hyökkääjän saavutettua verkon administraattorin ja oppimalla administraattorin käyttäjäoikeuksien hallinnan hyökkääjä pystyy päivittämään oman verkko-oikeutensa laajamittaisempaan käyttäjätiliin sekä antaa mahdollisuuden noudattaa turvamenettelyjä, kuten vähiten turvaoikeuksia ja roolipohjaista pääsyä vaativiin turva proseduureihin

6. Palomuurin vaarantaminen yrityksen IT:n ja Internetin välillä – hyökkääjän saavutettua valtuutetun käyttäjätilin hyökkääjä pystyy vaarantamaan koko yrityksen tietoverkon yrityksen ja Internetin välillä. Tämä antaa hänelle vapaan pääsyn siirtää komentorivipohjaista koodia hyökkääjän tietokoneen, Internetin ja uhrin tietoverkon välillä

7. Hyökkäyksen laajentuminen vaakasuoraan (sivuttaissuunteinen eteneminen) läpi koko verkkorakenteen – hyökkääjä voi jatkaa verkon skannaamista kohdistuen automaatioprosesseihin saaden yksityiskohtaista tietoa ohjelmoitavista logiikka ohjaimista (PLC), etäpäätelaitteista (RTU), käytetyistä tietoprotokollista ja ohjauslaitteiden (PLC, RTU) ja IP osoitteista, jotka ovat yhteydessä yritystason IT-verkkoon

8. Näkymättömyyden ylläpitäminen – hyökkääjä kerää enemmän tietoa teollisuuden ohjausjärjestelmien (ICS) arkkitehtuurista vaarantamatta omaa näkyvyyttä verkossa ja mahdollisesti peittämällä oman verkkoidentiteetin ja jäljitettävät yksityiskohdat verkossa

9. Korkeamman tason etuoikeuksien saavuttaminen – hyökkääjän saavutettua riittävät tiedot yrityksen verkossa ja saavutettua tarvittavat valtuutukset, hyökkääjä

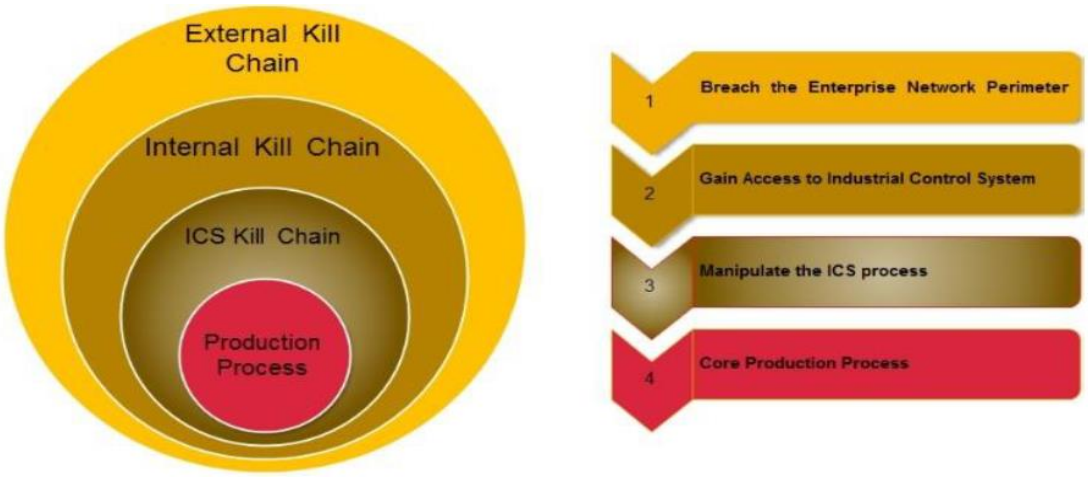
voi luoda korkean luokan järjestelmänvalvojaoikeudet itselleen. Tämä antaa hyökkääjälle oikeuden päästä yrityksen IT-verkkoa ja teollisuuden ohjausjärjestelmä verkkoa (ICS) eristävän palomuurin läpi ja vaarantaa lisäturvatoimenpiteet, jotka voivat normaalisti estää pääsyn teollisuuden ohjausjärjestelmä verkkoon (ICS)

10. Teollisuuden ohjausverkkoa (ICS) suojaavan palomuurin vaarantaminen – hyökkääjä on saavuttanut yrityksen IT-verkon skannauksen kokonaisuudessaan ja on valmis korkean tason järjestelmäoikeuksien avulla vaarantamaan palomuurin teollisuuden ohjausverkon (ICS) ja yrityksen IT-verkon välillä, kun hyökkääjä on saanut palomuurin kaadettua hän voi kaapata tietoa suoraan teollisuusverkosta Internetin ja yritysverkon välityksellä

11. Teollisuuden ohjausverkon (ICS) ja operatiivisten tekniikoiden (OT) oppiminen – etäpäätelaitteiden (RTU) ja ohjelmoitavien logiikkaohjaimien (PLC) avulla tapahtuva ohjausprosessien oppiminen, kuten lämpötila, nopeus, paine, värähtely, virtaama, yms. sekä teollisuuden ohjausverkon (ICS) automaatio palvelimille ja ihmis-konerajapinnassa (HMI) oleville tietokoneille lähtevän tiedon avulla. Ohjausprosessien tunteminen auttaa hyökkääjää muodostamaan väärän kuvan ”oikean tiedon nauhoituksen avulla” ja hyökkääjä voi siirtää HMI-tietokoneille nauhoitettua kuvaa prosessin toiminnasta hyökkäyksen aikana, jolloin hyökkäys pysyy salassa hyökkäyksen aikana. Esimerkkinä Stuxnet- ydinvoimalaprosessien haisteluisku, minkä tarkoituksena oli toimia passiivisena tunnustelijana ja aktivoitua ainoastaan Iranin ydinvoimalaprosessin saavutettua.

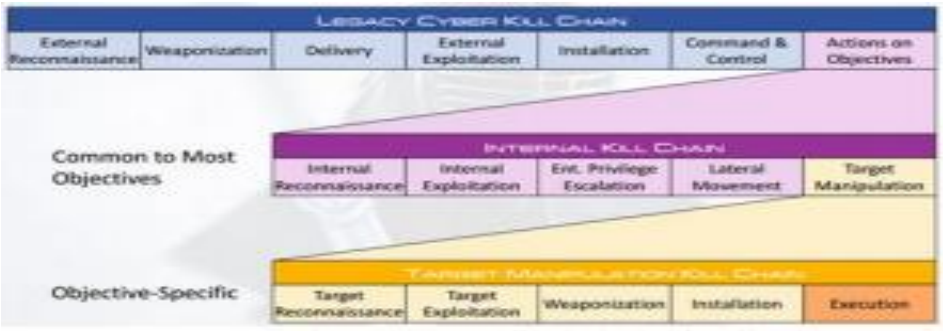
12. Ohjausprosessin manipulointi – hyökkääjä voi manipuloida etäpäätelaitteiden (RTU) ja ohjelmoitavien logiikkaohjaimien (PLC) operatiivisia parametreja, muuttaa ohjausrajoja, muokata ohjaussilmukoita, vaarantaa ohjelmistotason turvaa ja luoda vahinkoja teollisuuden prosessiin ja ihmisiin. Hyökkääjän luodessa väärää kuvaa operatiivisen tason HMI-laitteisiin, kuten valvomokoneille, laitteet näyttävät väärää kuvaa normaalista tilanteesta, kunnes ohjausprosessille kriittiset koneet ja laitteet hajoavat, esimerkkinä Saksan rautakaivosprosessiin kohdistunut isku. [61; 62]

6.3.1.2 Kolmen tason Cyber Kill Chain



Kuva 31. Kolmen tason Cyber Kill Chain [63]

Kuvassa 31 on esitetty kolmen tason Cyber Kill Chain prosessi. Erona aiempaan on se, että tässä mallissa tellisuusohjausjärjestelmän manipulointi on eroteltu koskemaan vain tiettyä teollisuusohjausjärjestelmää, kun koko teollisuuslaitos saattaa sisältää useita ohajusjärjestelmiä. Teollisuusprosessin manipulointi käsittää seuraavat prosessivaiheet: tietyn teollisuusprosessinohjausjärjestelmän ja ohjausohjelmiston havainnointi, ohjausjärjestelmän spesifisen haavoittuvuuden havainnointi, ohjausjärjestelmän haavoittuvuustyökalujen kehittäminen, ohjausjärjestelmän haavoittuvuustyökalujen asentaminen, ohjausjärjestelmään kohdistuvan iskun aloittaminen. Kuvassa 32 on esitetty kolmen tason Cyber Kill Chain prosessikuvaus. [63]



Kuva 32. Kolmen tason Cyber Kill Chain prosessikuvaus [63]

6.3.2 Defence in Depth -arkkitehtuuri ja strategia

Defence in Depth -arkkitehtuuri tarkoittaa yleisesti tarkoin koordinoituja turvallisuus vastatoimia tietopääoman eheyden varmistamiseksi verkossa ja usein siitä käytetään myös nimitystä Defence in Depth -strategia. Seuraavassa esitetään 10 eri askelta Defence in Depth -strategian saavuttamiseksi.

1. Luodaan turvallisuussuunnitelma – kaikkein tärkein askel Defence in Depth -strategian osalta on luoda turvallisuussuunnitelma, joka toimii samalla tietoturvan riskianalyysinä, jossa henkilöstö luo yksityiskohtaisen tarkastuksen kaikista teollisuusohjausverkkoon liitetyistä laitteista. Valmis turvallisuussuunnitelma tarvitaan ennen kuin voidaan siirtyä Defence in Depth -strategiassa eteenpäin. Turvallisuussuunnitelmaan kuuluu kuvaus siitä, miten laitteet ovat kytketty (verkkokartta laitekytkennöillä), katsaus laitteiden suojausasetuksista ja arvioi mahdollisista järjestelmä haavoittuvuuksista. Turvallisuussuunnitelma pitää sisällään myös vaikutuksia koskien tuotteita, verkon arkkitehtuuria, ihmisiä ja yritysprosesseja.

2. Eritytetyt verkot – turvallisuussuunnitelmassa kuvattua verkkokarttaa hyödyntäen verkot voidaan hajauttaa tärkeimpien toimintojen perusteella, esimerkiksi verkkojen jakaminen yritystason, tehdastason, prosessitason ja kenttävyöhyketason verkoiksi ja kaikki vyöhyketason yhteydet tulisi olla tunnistettu ja kuvattu.

3. Kehäsuojaus - kaikki kaapelit ja yhteydet vyöhykkeiden välillä tulee olla asianmukaisesti suojattu ja tärkeimpänä tässä vaiheessa on varmistua etäyhteyden suojaamisesta.

4. Verkon segmentointi – vyöhykkeet, jotka luotiin eriytettyjen verkkojen vaiheessa 2 voidaan jakaa pienempiin vyöhykkeisiin perustuen joko fyysiseen sijaintiin tai toimintoihin, niin että näiden segmentoitujen vyöhykkeiden kehät ovat suojattuja ja suojaustaso näiden eri segmentoitujen vyöhykkeiden välillä voi vaihdella riippuen suojaustarpeesta (esim. turvallisuus ja monitorointilaitteiden välillä).

5. Laitteiden suojastason vahvistaminen – lisäämällä ominaisuuksia teollisuusohjausjärjestelmien laitteisiin voidaan niiden kykyä vastustaa kyberhyökkäyksiä parantaa. Tämä vähentää verkkoelementtien todennäköisyyttä vaaraantua kyberhyökkäyksessä.

6. Verkon analysointi ja monitorointi – verkon monitorointityökalun avulla verkkoliikennettä aktiivisesti seuraamalla voidaan tunnistaa potentiaaliset uhat ja haavoittuvaiset tuotteet, koska uudentyyppiset ohjelmistot ja laiteohjelmistot ovat mahdollistaneet osoittaa haavoittuvuuksia tai lisätä turvallisuusominaisuuksia, jotka saattaavat sisältää tietoturvan kannalta väärennettyjä ominaisuuksia. Tietoturvauhkan tapauksessa verkon analysointi ja jatkuva kehitys mahdollistaa, että verkon takaporttien kautta tapahtunut kyberisku voidaan jatkossa ehkäistä ja mahdollisesti jo saastuneet koneet ja verkot tulee eristää muusta verkkoarkkitehtuurista.

7. Verkon päivitykset – verkon kannalta on tärkeintä, että kriittiset päivitykset ajetaan säännöllisesti ja keskitetysti, joka ehkäisee päivityksiin liittyvät sertikaattiväärennökset ja vanhojen ohjelmistojen haavoittuvuudet. Myös vanhat laitteet ja ohjelmistot, joihin päivityksiä ei ole enää saatavilla, tulee vaihtaa uudempiin, jotka tukevat kyberhyökkäyksiltä suojautumista.

8. Verkon kyberturva asiantuntija – kyberturva asiantuntijan avulla pystytään kyberiskuja ennalta ehkäisemään teollisuusverkoissa, kun on tarkempaa tietotaitoa käytössä mahdollisista haavoittuvuuksista ja kybersuojautumisesta

9. Varajärjestelmä ja varmuuskopioinnit – varajärjestelmän avulla voidaan ennalta-ehkäistä teollisuusohjausjärjestelmän kaatumiseen liittyvät taloudelliset tappiot, mitkä aiheutuvat teollisuusprosessin katkeamisesta. Varmuuskopiontien avulla saadaan palautettua tärkeitä tietoja teollisuusohjausjärjestelmän kannalta, joita tarvitaan koko tuotantoprosessin uudelleen käynnistämiseen.

10. Jatkuvuussuunnitelma – suunnitelma jatkuvuuden varmistamiseksi, joka sisältää yksityiskohtaista tietoa varajärjestelmien, varmuuskopiontien ja todellisten uhkatilanteiden varalle. Sisältää myös eri palvelimien eri maantieteelliset sijannit, joilla

varmistetaan samassa rakennuksessa tai maantieteellisellä alueella sijaitsevien palvelimien uhkatekijöihin liittyvät riskit. [64]

6.3.3 ICS kyberpuolustus

6.3.3.1 Etäyhteyksien ja IoT:n tiedonkeruun tietoturvavaatimukset

IoT-laitteiden suurin ongelma on tietoturvan puuttuminen sekä mobiililaitteiden mahdollistama paritus ilman tietoturvaa (Universal Plug and Play). Suurin syy tähän ovat kustannukset. Teollisessa Internetissä kuitenkin on protokollia kuten Modbus ja SCADA, joilta puuttuu sisäänrakennettu tietoturva. Vaikka teollisuudessa eri protokollia käyttävät laitteet on erotettu Internetistä palomuurilla, niin sisäänrakennetun tietoturvan haavoittuvuusongelmat siiryvät vain astetta ylemmäs olevalle palvelimelle, jolla on oikeus keskustella protokollan kanssa, jolta puuttuu sisäänrakennettu tietoturva. Etäyhteyksien muodostamisessa käytetään usein erinlaisia autentikointiavaimia, joilla varmistetaan etäyhteyksien luotettava toiminta. Eräs autentikointitapa etäyhteyksien muodostamiseen on käyttää geneerisiä salasanageneraattoreita, joita esim. pankeilla on tänäpäivä käytössä verkkopankkiyhteyksien muodostamisessa. IoT-laitteiden autentikointia on teollisten langattomien antureiden osalta pyritty kehittämään jatkuvasti. Eräs autentikointitapa on laitteiden paritus ainoastaan toimittajan markkinoimilla skannauslaitteilla ja ainoastaan toimittajan kouluttaman sekä toimittajan palveluksessa tai alihankintaverkostossa työskentelevän työntekijän toimesta, kuten esimerkiksi Swegonin uuden sukupolven Wise-järjestelmien asennusten osalta tehdään.

6.3.3.2 Yhdeksän yleisintä kyberuhkariskiä ja niiltä suojautuminen

Seuraavassa on esitetty yhdeksän keskeistä kyberuhkariskiä, joita esiintyy teollisuusverkoissa ja lisäksi ranskalaisilla viivoilla on esitetty keskeisiä suojautumiskeinoja kyberuhkariskien varalle. Kyberuhkariskit on esitetty alkaen riskitekijöiltään yleisimmistä ei yleisimpiin riskitekijöihin niiden esiintymistiheyteen perustuen.

1. Henkilöstöön liittyvät riskit (puutteellinen tietoturvapolitiikka ja koulutus)
    - Autentikointi ja avaintenhallinta
    - Salasanojen hallintatyökalut (esim. vaikeiden salasanojen hallinta)

- Tietoturvapolitiikka (esim. ulkoisten kovalevyjen osalta)
- Tietoturvakoulutus (esim. sähköpostien liitetiedostojen avaaminen)

2. Toimittajaan liittyvät riskit (jaetun tiedon ongelmat ja fyysinen pääsy tietokoneille)
   - Toimittajien seulonta ja auditointi
   - Alihankintayrityksien työntekijöiden tietoturvakartoitukset
   - Laitteisto ja ohjelmistotoimittajien maine ja riippumattomuus
3. Etäkäyttöön liittyvät riskit
   - Ainoastaan turvattujen VPN-verkkojen käyttö
   - Automaattisten näppäinlukkojen käyttö
   - Naamioitujen matkapuhelintukiasemien seuranta ja esto kännykkään
   - Kirjoittaviin asemiin liittyvä riski ulkomaanmatkustelussa
4. Laitteistoon liittyvät riskit
   - Ainoastaan laitteiden käyttö, joissa sisäänrakennettu turvajärjestelmä
   - Työntekijöiden omien laitteiden tarkastus ja suojaus
5. Ohjelmistoon liittyvät riskit
   - Teollisuustilojen ohjelmistotuotteiden vaihto päivytyksiä tukeviin ohjelmiin
   - Ohjelmistotuotteiden vaihto pävityksiä tukeviin ohjelmointikieliin
   - Virus- ja haittaohjelmien tarkastus- ja poisto-ohjelmien käyttö
6. Pilvisovellukseen/-laskentaan- ja verkkosovelluksiin liittyvät riskit
   - Proaktiivinen suojausasetusten hallinta ja tunketumisen havainnointi
   - Tietoturvajärjestelmäratkaisu, joka seuraa ja päivittää web-sovelluksia
7. Verkkoon liittyvät riskit
   - Tietoverkon topologian segmentointi ja liittäminen kehittyneillä reititimillä
   - Segmentoitujen verkkotopologioiden liittäminen esim. NATin avulla
   - Reitittimien oletussalasanojen ja WiFi-yhteyden vieralijatilin eliminointi
   - Yrityksen ulkopuolisen henkilön estäminen tietokoneille pääsy
8. Talouteen ja maineeseen liittyvät riskit
   a. Oikeudelliset sopimukset osana yhteistyötä koskien kyberhyökkäyksiä
   b. Kyberhyökkäyksiä koskeva vakuutus mikä kattaa taloudellisia tekijöitä
9. Tulevaisuuteen liittyvät riskit
   a. Ajan tasalla pysyminen nousevien uhkatekijöiden osalta
   b. Toiminnan jatkuvuuden varmistaminen osana nollapävän hyökkäyksiä
   c. Konsultaatio turvallisuuskonsulttien tai turvallisuusvalvojien kanssa

6.3.3.3 IoT-laitteiden liittäminen pilvipalveluihin turvallisesti ja hallitusti

IoT-laitteiden ja erityisesti antureiden liittäminen pilveen tapahtuu sulautetun tietokoneen avulla ja siihen sopivan ohjelmiston avulla. Toinen mahdollinen toteutustapa on käyttämällä sulautetusta tietokoneesta ja ohjelmistosta koostuvaa IoT-yhdyskäytävää (IoT-Gateway) yhdistämään joukon vähemmän älykkyyttä sisältäviä antureita pilveen. Yhdyskäytävälaite voi olla myös fyysisesti erillinen laite tai koteloitu samaan koteloon antureiden kanssa. Kokonaisjärjestelmätoimittajien, kuten Swegon uuden sukupolven Wise-järjestelmätoimittajien kohdalla antureita ei voida suoraan liittää pilveen vaan tarvitaan erillinen yhdyskäytävälaite, joka on yhteydessä Director keskusohjausyksikön ja pilvipalvelun välillä. Keskeistä tietoturvan kannalta on käyttää pilvipalveluissa suojattuja protokollia, kuten MQTT-protokollaa. Alla olevassa taulukossa on esitetty markkinoilla olevista suurimmista pilvipalvelun tarjoajista ja pilvipalveluiden eri ominaisuuksista. [65, s. 28]

Taulukko 2. Taulukko 2: Markkinoilla olevat suurimmat pilvipalvelun tarjoajat [65, s. 25]

Palvelu	AWS IoT	Azure IoT	Google IoT	IBM IoT Bluemix Watson	ThingSpeak	Elisa IoT	GE Predix	MindSphere
Yritys	Amazon	Microsoft	Google	IBM	Mathworks	Elisa	GE	Siemens
Pilvityyppi	IaaS, PaaS	IaaS, PaaS, SaaS	IaaS, PaaS	IaaS, PaaS	PaaS, SaaS	PaaS, SaaS	IaaS, PaaS	Paas
IoT alusta	AWS IoT Core	Azure IoT Hub	Google Cloud IoT Core	IBM Bluemix IBM Watson	ThingSpeak	PTC ThingWorx	Predix	MindSpehre
Tärkeimmät protokollat	MQTT, REST	MQTT, REST	MQTT, REST	MQTT, REST	MQTT, REST	REST, (MQTT)	OPC UA, MQTT	OPC UA, MQTT
Laitteiden asetusten hallinta	AWS IoT Device Management	Azure IoT Hub Device Provisioning, IoT Central	Google Cloud IoT	Watson IoT Platform Device Management service	-	ThingWorx, Remote access and control	Predix Edge Manager	MindConnect, Proximetry
Tiedon tallennus	S3, RDS, Redshift, DynamoDB, Redis, MongoDB	CosmosDB, SQL, MySQL, Redis, MariaDB, MongoDB	CloudSQL, PostgreSQL, MySQL, Bigtable, Cloud Spanner, Redis, MongoDB	DB2, PostgreSQL, MySQL, MongoDB, Redis	ThingSpeak	ThingWorx	PostgreSQL, Blobstore, Time-series	SQL, MongoDB
Analytiikka	Amazon Kinesis, Amazon Redshift, Amazon Athena, Amazon EMR	Azure Stream Analytics, Event Hubs, SQL Data Warehouse, Log Analytics, HDInsights	Google Cloud Dataflow, Google BigQuery	Watson IoT	Matlab	ThingWorx Analytics	Predix Analytics Framework	MindSphere
AI	AWS Machine Learning	Azure Machine Learning Brainwave	Google Cloud Machine Learning Engine	Watson AI	Matlab Neural Network Toolbox	ThingWorx Analytics	Predix AI	MindSphere AI
Tulosten visualisointi	Amazon QuickSight	Power BI, Web App	Google Data Studio, Google Cloud Datalab, Google Cloud BI	Watson IoT Dashboard	ThingSpeak API, MATLAB Visualizations	ThingWorx Analytics Visualization, Virtuaalinen tehdas 3D	GE data visualization, Predix Visualization	Data Visualization , Visual Explorer Mobile SDK
Sovelluskehitysympäristö	AWS Lambda	Azure Functions	Google Cloud Functions	Node-RED, IFTTT	Matlab Trigger	ThingWorx	Predix DevBox	Cloud Foundry
Ohjelmointikielet	Node.js, Java, Python	OoT Edge, Java, .NET, Core 2.0, Node.js, C, Python	Node.js, Java, .NET, PHP, Ruby, Python, Go	C++, C#, C, Java, Mbed++, Node.js, Node-RED	Matlab	ThingWorx graafinen ympäristö	Java, Python, NodeJS, C, C++	Java, Visual Flow Creator
Käyttöjärjestelmät IoT laitteissa	Linux, Amazon Free-RT OS	Windows 10 IoT Core, Azure Sphere OS Android a AndroidThings	AndroidThings, Linux	Linux, Windows 10 IoT Core	Linux, Arduino	Windows, iOS, Android, Linux	Linux, Windows 10 IoT	Windows, Linux
EDGE	AWS Lambda@ Edge, Greengrass	Azure IoT Edge.	Cloud IoT Edge	IBM Bluemix in edge, IBM Watson IoT Platform for edge analytics	Matlab ja Simulink koodia voi ajaa Beckhoffin laitteissa	Thingworx Edge SDK, Thingworx Edge Microserver	Predix Edge	MindSphere Edge Computing
Hintamalli	Käytön mukaan	Käytön mukaan + kk hinta per laite	Käytön mukaan	Käytön mukaan	Etukäteen ostettavat käyttöyksiköt	Tilausmalli	Tilausmalli	Tilausmalli

Taulukon 2 eri pilvipalvelut voidaan jakaa IaaS (Infrastructure as a Service), PaaS (Platform as a Service) ja SaaS (Software as a Service) alustatyyppeihin. Tietoturvan kannalta teollisuusympäristössä tulee valita ainoastaan ne pilvipalvelutoimittajat, jotka ovat erikoistuneet teollisuuden pilvipalveluihin sekä valita alustatyyppi joko PaaS tai IaaS alustana, koska SaaS-pilviratkaisu on täysin pilvitarjoajan hallinnassa, joka aiheuttaa tietoturvariskin teollisuusympäristössä. Yhä useammin pilvialustat tehdään olemassa olevan pilvialustan päälle, jolloin puhutaan sumupilvestä tai reunapilvestä. Edellisen taulukon pilvitoimittajista ainoastaan GE Predixin ja Siemensin pilvialustaratkaisut ovat teollsuusympäristöön tarkoitettuja. Keskeisenä erona näissä kahdessa toimittajassa on se, että GE Predix markkinoi sekä IaaS ja Paas -pilvipalveluja, kun taas Siemens markkinoi ainoastaan PaaS -pilvipalveluja. PaaS -pilvipalveluja myydään OS-palveluna (alustapalvelut), toteutus ympäristöpalveluna tai tietojen tallennus- ja palveluntarjoajapalveluna.

PaaS-pilvipalvelua käytettäessä pilvipalvelun rakentamisessa ongelmana on lukkiutuminen ainoastaan yhteen alustatoimittajaan, mutta hyvänä puolena on kustannustehokkuus, joka syntyy, kun käytetään valmiita komponentteja. IaaS-palvelut ovat pilven infrastruktuuripalveluita ja keskeistä IaaS-pilvipalveluissa on, että toteutusympäristö voi olla tehokkaammin suojattu kuin PaaS-pilvipalveluissa. IaaS-pilvipalveluiden etuna on, että palvelinta ja käyttöjärjestelmää voidaan hallinnoida itse silloin kuin se on tarpeen, joka on merkittävä tekijä esim. teollisuusohjausverkkoon liitettävien pilvipalveluiden yhteydessä. IaaS-pilvipalveluiden toimittajat tarjoavat erilaisia virtuaalikoneita, virtuaaliverkkoja ja virtuaalitallennuspalveluita tai vaihtoehtoisesti kokonaisia ns. IaaS-palvelukontteja. IaaS-pilvipalvelua käytettäessä on virtuaalipalvelimen tai IaaS-palvelukontin siirto ympäristöstä toiseen on helppoa, mutta jos palveluun sisältyy paljon verkko- ja tallennusjärjestelmätekniikkaa voi toteutus uuteen ympäristöön muodostua erittäin haasteelliseksi. [65, s. 22-28.]

6.3.3.4 Datan siirto ja suojaus

Keskeistä datan siirron kannalta on käyttää suojattuja yhteystekniikoita, joita on esim. HTTPS (SSL/TSL), MQTT over HTTPS, VPN (Open VPN), SSH/SCP, WSS (Web Socket Secure). Suojaamattomia yhteystekniikoita on: HTTP, FTP, Telnet, Modbus TCP jne., SCADA- ja automaatioprotokollat ja suurin osa etäsarjaporteista (sarjaliikenne raakana TCP:n yli), Universal Plug and Play (UPnP: UDP + HTTP). Keskeistä on käyttää suojattuja yhteyksiä aina kun se on mahdollista ja päästä päähän suojaus on paras valinta. Lisäksi pelkkä suojaustekniikan valinta ei ratkaise mitään vaan mm. laitteiden tunnistuksen ja avaintenhallinnan pitää olla kunnossa. Transport Layer Security (TLS) on eniten käytetty salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli. Tavallisin käyttötapa on suojata WWW-sivujen siirtoa HTTPS-protokollalla, mutta sillä voidaan suojata myös muita protokollia, kuten: Websocket (wss://), VPN (OpenVPN), SMTP, FTP, NNTP, XMPP ja MQTT -protokollat. Teollisuusverkkojen tehokas suojaus edellyttää, että laitteet toimivat Internetistä erotetussa IP-verkossa ja jokaisessa laitteessa on oltava palomuuri. Teollisuusprotokollat kuljetetaan salattuina VPN-yhteyden läpi ja palomuuri on oltava käytössä myös VPN-yhteyden sisällä sekä ylläpitoyhteyksiin SCP ja SSH -protokollat. Teollisuusverkoissa on oltava keskitetty laitteiden hallinta, joka mahdollistaa konfiguroinnin, avaimet, tunnisteet, IP-osoitteet ja päivitykset verkon sisällä.

Uusi internet protokolla Ipv6 sisältää Internetin tietoturva-arkitehtuuri Ipsec:n, mutta sen haasteina on seuraavat seikat:

- IPv6 tietoturvaosaamisen puutteellisuus
- IPv6-tunnelointitekniikoiden mahdollistamat uudet tietoturvahyökkäykset
- puutteellinen IPv6-tuki laitteissa ja operaattoreilla
- IPv6 -protokollaan sisältyvät bugit vielä löytymättä
- NAT- eli osoitteenmuunnostekniikan puuttuminen osana tietoturvaa
- luulo siitä, että IPv6 internetprotokollan tietoturva olisi samanlainen kuin IPv4 internetprotokollassa
- molempien internetprotokollien vaatima rinnakkainen tuki ja tietoturvahaasteet eri laitteissa
- IoT-laitteiden kasvavaan määrään liittyvä tietoturvauhka
- kiinnostus verkossa olevien laitteiden tietoturva-aukoista
- raudanlujan tietoturvan tarpeen edellyttämä sumulaskenta, niin että sovellus voi pyöriä missä tahansa. [66]

6.3.3.5 Valmistautuminen kyberuhkien torjuntaan

Kasvanut kyberuhkien riski on aiheuttanut niin yritys, valtio ja EU-tasolla valmistautumista kasvaneisiin kyberuhkien torjuntaan. Erityisesti energia-alalla kyberuhkien määrä ja hyökkäysten vaativuustaso on ollut kasvussa. EU-tasolla on laadittu oma NIS-direktiivi kyberhyökkäysten varalle. Suomessa Huoltovarmuuskeskus yhdessä Viestintäviraston ja usean energia-alan- ja teollisuusyrityksen kanssa ovat laatineet KYBER-ENE – ja KYBER-TEO-hankkeet osana KYBER2020-ohjelmaa, jolla on pyrkimys Suomen kriittisten infrastruktuurien suojaamiseen. Yhä useammin kyberhyökkäysten motiivina on Bitcoin virtuaalirahan hankkiminen suurten palvelinkapasiteettien avulla, esimerkkinä on vuonna 2014 tapahtunut kahden teinipojan onnistunut kyberhyökkäys Osuuspankin palvelimiin. Suomessa tehdyn tutkimuksen mukaan yli puolet yrityksistä myöntää puutteet kyberuhkien torjunnassa ja yritykset myös investoivat kyberuhkien torjuntaan. Teollisuusautomaation haasteena on sarjaliikenteisten käytönvalvontaprotokollien, kuten IEC 101, 104 ja 61850 sekä avointen tiedonsiirtostandardien käyttö, kuten OPC DA, joiden hyödyntä-

miseen perustui vuonna 2016 tehty Ukrainan Kiovassa tehty laaja kyberhyökkäys kohdistuen sähköverkkoyhtiöihin, joka aiheutui automaatiolla ohjattavien katkaisijoiden ja erottimien avauksesta sähköasemilla. Viestintävirasto jakaa vuonna 2014 tekemässä raportissa hyökkäysten suojautumisen neljään eri toimenpiteeseen, jotka ovat: ennaltaehkäisevät toimenpiteet, havainnointitoimenpiteet, reagoivat toimenpiteet ja palautustoimenpiteet. Keskeistä kyberhyökkäysten kannalta on rajata ne ohjelmat ja laitteet, jotka ovat kriittisiä esim. teollisuuden automaatiolaitteiden toiminnalle ja varmistaa näiden ohjelmien suojatumiskeinot kyberhyökkäyksien, ohjelmistokatkojen, haittaohjelmien ja tietovuotojen varalle. Jatkuvuussuunnittelun avulla näiden kriittisten tekijöiden osalta on luotava varasuunnitelma (Back Up Plan), kun mahdollinen onnistunut kyberhyökkäys tapahtuu. [67; 68; 69; 70; 71; 72]

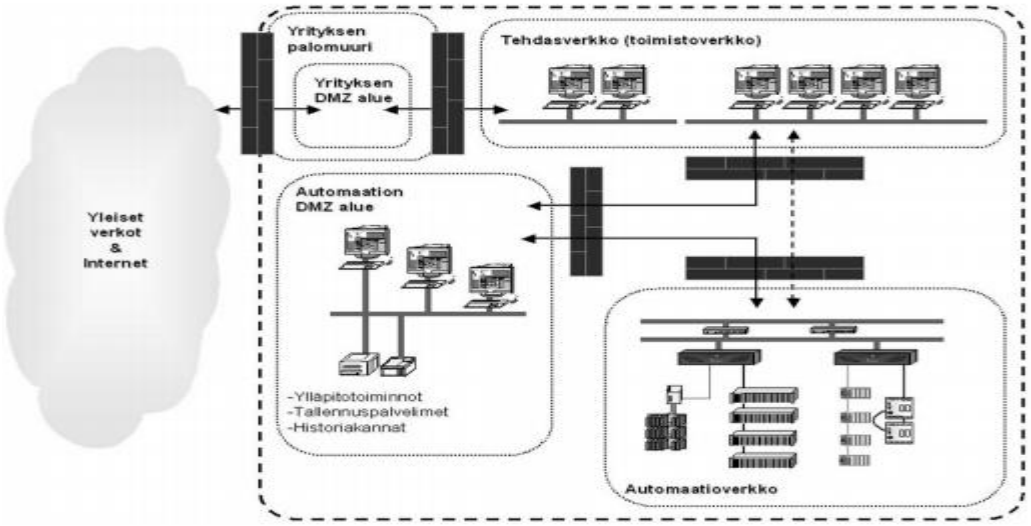
6.3.3.6 Häiriöttömän tuotannon turvaaminen teollisuudessa

Häiriöttömän tuotannon turvaaminen teollisuudessa edellyttää sekä ennakoivan, että jo olemassa olevien häiriöiden turvaamista valmiiden toimintaratkaisujen perusteella. Keskeistä häiriöttömyydelle on standardin IEC 62443 mukaisten vaatimustasojen täyttyminen. On kuitenkin hyvin tärkeää ymmärtää, että mikään yksittäinen ratkaisu ei takaa riittävää suojaa kaikkia erilaisia tietoturva- ja kyberuhkia kohtaan. Alla olevassa listassa on esitetty tapoja, joita noudattamalla pystytään saavuttamaan standardin IEC 63443 mukaista vaativaa 3-tasoa vaativampi suojaustaso, jossa on noudatettu 2-kertaisen DMZ-alueen hallinnointia. Keskeistä on, että yrityksen tietoturva on yhtä vahva kuin sen heikoin lenkki, joten kaikkien käytettävien ratkaisujen on oltava asianmukaisesti suunniteltu, toteutettu ja ylläpidetty.

Teollisuusautomaation luotettavan tietoturvan hallinta edellyttää:

- Verkot erotettu Internetistä palomuurien avulla
- Liikenne palomuurien läpi on tarkoin rajattua
- Verkon autentikoinnin, salasanageneraattoreiden ja salasanaohjelmien käyttö
- Sisäverkossa käytetään virustorjuntaohjelmistoja (päivitettävä säännöllisesti)
- Sisäverkkojen haittaohjelmien seulontatyökalujen käyttö (päivitys säännöllisesti)
- Internet-liikennettä tarkkaillaan (selainliikenteen ja sähköpostiliikenteen tarkkailu)
- Virusten ja roskapostien poistaminen (roskapostisuodattimet ja viruskaranteenit)

- Langattomien verkkojen suojaaminen (Palomuurit, RADIUS ja LEAP-tekniikat)
- Mobiiliverkkojen- ja laitteiden digitaalisen konvergenssin ongelmien ratkaisu
- RFID-lukijoiden mahdollisuus muuttaa sirujen tietoja (voimakkaat RFID-lukijat)
- QR-koodien skannauskielto yrityksen omassa verkossa oleville laitteille
- Etäyhteyksien ja tietoliikenteen salaus (modeemien käyttöön liittyvä tietoturva)
- Syvyyssuuntaisen suojauksen (Defence in Depth) mukainen tasoluokittelu
- Automaatioverkon hallinta (kahdensuuntainen suojaus automaatio-sisäverkko)
- Tarpeettoman suurten tietoturvavyöhykkeiden välttäminen automaatioverkossa
- Automaatiotyöasemien (HMI) suojaaminen (testatut käyttöjärjestelmäversiot)
- Automaatiotyöasemien (HMI) kovennus (Hardening)
- Automaatiotyöasemien (HMI) virustorjunta (antivirus) ja roskapostisuodatus
- Automaatiotyöasemien (HMI) haittaohjelmien seulontatyökalut (spybot)
- Automaatiotyöasemissa (HMI) tarvittavien ohjelmistojen päivitykset
- Automaatiotyöasemien (HMI) käytönhallinnan tunnistus, valtuutus ja seuranta
- Automaatiotyöasemien salasanojen hallinta (salasanaohjelmat – ja generaattorit)
- OPC-tekniikoiden rajoitettu käyttö (DCOM-tekniikan tietoturvaongelmat)
- Automaation 2-kertaisen DMZ-alueen segmentointi (ylläpito, tallennus, historia)
- Anturiverkkojen säätösovellulluksien ongelmien ratkaisu (aikakriittisyys, QoS)
- Automaatioverkon rajoitus ja palomuurit (ei koskaan suoraa Internet yhteyttä)
- Automaation laitetason tietoturvan hallinta (esim. IPSec)
- Automaation etähuoltoyhteydet oletusarvoisesti pois päältä
- Vahva tunnistusmekanismi etähallintayhteyksien varalle (salasanageneraattori)
- Fyysiset menetelmät kyberuhkia vastaan (paikalliset/etä kytkimet)
- Automaatiotyöasemien (HMI) varmuuskopiointien ja palautustestien luonti [69, 73, 74]



Kuva 33. Kaksinkertainen ei-kenenkään-maa (DMZ) suojaus [73]

Kuvassa 33 on esitetty kaksinkertainen ei-kenenkään-maa suojaus (DMZ), jossa automaativerkolle kriittiset ylläpitotoiminnot, tallennuspalvelimet ja historiatietokannat ovat erotettu automaatioverkosta katastrofitilanteiden varalta.

6.4 Tieto- ja kyberturvallisuus Wise-järjestelmän osalta

Seuraavassa esitetään Swegon uuden sukupolven Wise-järjestelmää koskevia tieto- ja kyberturvallisuuteen liittyviä käytäntöjä sekä yleisiä tietoturva ja dokumentointivaatimuksia langattomia automaatiolaitteita koskien. Kappaleessa 7.2 esitetään lisäksi järjestelmän integrointia osaksi teollisuusrakennuksen automaatiojärjestelmää ja siihen liittyvää tietoturvaa.

6.4.1 Järjestelmän käytössä olevat tietoturvaprotokollat

Swegon Director keskusohjausyksikkö, joka toimii samalla langattomien antureiden tukiasemana, on yhdistettävä 8-napaisella kaapeliliitännällä Swegon Super Wise II tiedonsiirtoyksikön välille. Swegonin langattomassa WISE anturiverkossa antureiden ja Director keskusohjausyksikön välillä käytetään AES 128 bittistä salausprotokollaa. AES 128

bittistä salausta pidetään edelleen murtamattomana salausmenetelmänä, vaikka salaus perustuukin oikeasti 126 bittiseen salaukseen. Vaikka salausmenetelmä onkin ns. murtamaton, niin salausmenetelmään liittyvä ohjelmisto ei välttämättä sitä ole, jos salausmenetelmää toteuttava ohjelmisto on toteutettu suljettua lähdekoodia käyttämällä ja ohjelma sisältää ns. takaportteja. Swegon Wise-järjestelmän anturiverkon salausohjelmistoa ei ole haluttu tietoturvasyistä paljastaa julkisuuteen. [75; 76; 77; 78; 79.]

Wise-järjestelmästä siirrettävä langaton 4G-mobiiliverkko alkaa Swegon Super Wise II Swegon Connect tiedonsiirtoyksiköstä. Keskeisen osan tietoturvaa Swegon uuden sukupolven Wise-järjestelmässä on Swegon Connect (TBSC) tiedonsiirtoyksikkö. Swegon Connect sisältää reitittimen (4G LTE ja HSPA+) ja sen maksimi tiedonsiirtonopeus on 100 Mbit/s. Swegon Connect sisältää SIM-korttipaikan mobiililaajakaistaliittymille (4G, 3G, EDGE tai GPRS), Ethernet portin, I/O-portin, USB-portin (host), tuen DHCP-palvelimelle, NAT eli verkko-osoitteen muunnotekniikka (Network Address Translation), NAT-T:n eli verkko-osoitteen muunnostekniikan (NATin) ylläpitotekniikka, Port Forwarding eli NATin sovellusohjelma sekä toiminnot joustavien verkkojen rakentamiseen. Lisäksi myös Swegon uuden sukupolven Wise-järjestelmän kanssa yhteensopiva Gold ilmanvaihtokonetta on mahdollista ohjata Swegon käsipäätteen avulla langattomasti WLAN-verkossa. Tietoturvan ongelmana voi olla juuri ilmanvaihtokoneen WLAN verkossa toimiva käsipääte, koska sitä ei ole palomuurilla suojattu eikä sitä voida segmentoinnin avulla erottaa verkosta tai poistaa toteutukselta, koska käsipäätettä tarvitaan antureiden ja laitteiden pariliitäntään. 4G-mobiiliverkko toteuttaa salausprotokollana WPA2-PSK-protokollaa. Näihin tekniikoihin liittyy nykyisin kuitenkin olennainen riskitekijä. WPA2 salausprotokolla on saatu purettua viime vuonna KRACKattack-välimieshyökkäys menetelmällä ja 4G-verkkojen tukiasemien tietoturvaan liittyy hyvin olennainen riskitekijä, joka tarkoittaa sitä, että Suomessa mobiilioperaattorit eivät salaa LTE-verkkojen liikennettä tukiasemalta eteenpäin. [81; 82; 83; 84.]

6.4.2 Laitteiden ja antureiden pariliitäntään liittyvä tietoturva

Swegon Wise-järjestelmän anturiverkkoon pariliitettävät anturit, päätelaitteet ja säätöpellit luetaan erillisellä skannauslaitteella ainoastaan Wise-järjestelmään koulutuksen saanut huoltohenkilö. Skannauslaite pariliittää eri anturit ja laitteet QR-koodien perusteella.

QR-koodit voivat muodostaa samanlaisen tietoturvauhan kuin kodin Plug and Play -laitteet kotien IoT-verkoissa. On ollut esimerkiksi tapauksia markkinointiyritysten mainosmateriaaleissa olleet QR-koodit ovat sisältäneet linkin pahamaineisille Internet-sivuille, jotka myöhemmin komentorivin aktivoituessaan ovat saastuttaneet käyttäjien laitteet. Swegonin skannauslaitteet toimivat yhteydessä Gold ilmanvaihtokoneen käsipäätteeseen ja suorassa WLAN-yhteydessä asennettavan kohteen sisäiseen verkkoon. Eli pahimmassa tapauksessa hyökkääjällä voisi olla Gold-ilmanvaihtokoneen täysi etähallinta sekä vapaa pääsy asennetun kohteen sisäiseen verkkoon, missä hyökkääjä pystyy tekemään kriittistä tuhoa laajemmassa mittakaavassa. [74; 85; 86; 87.]

6.4.3 Järjestelmän tieto- ja kyberturvallisuuden parantaminen

– järjestelmän koventaminen

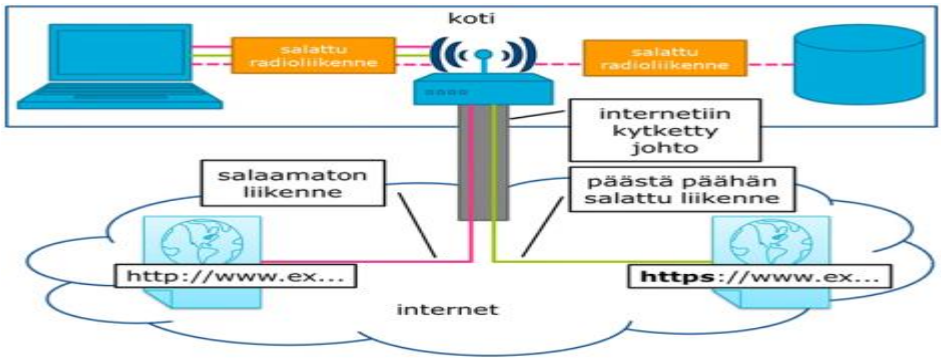
6.4.3.1 4G/VPN-tekniikka

Viestintävirasto suosittelee langattomien yhteyksien käytössä VPN-yhteyden käyttöä, koska langattoman WLAN yhteyden WPA2 suojausprotokolla on pystytty purkamaan välimieshyökkäyksen avulla ja jos käytössä on lisäksi PSK-salaus (TKIP- tai AES-GCMP-salaustekniikat) voi hyökkääjä käyttää hyökkäyksiä myös sisällön muokkaamiseen. Onnistunut hyökkäys edellyttää, että hyökkäys saadaan kulkemaan hyökkääjän hallitseman tukiaseman kautta (haamutukiasema) ja tämä edellyttää, että tukiasemat toimivat verkoissa toistimina ja niissä on standardin IEEE 802.11r mahdollistama ”Fast BSS transition” eli päätelaitteiden liikkuvuuden tukiasemasta toiseen mahdollistava toiminto. Suomessa operaattorit ovat tästä tietoturvauhasta olleet perillä ja pyrkineet uusimaan tukiasemapäivityksiä nopealla tahdilla, mutta ulkomaisiin operaattoreihin ei ole luottamista. [83]

Swegon Connect tiedonsiirtoyksikkö tukee avointa VPN yhteyttä, jonka avulla Swegon Connect voidaan yhdistää esim. tehtaan sisäiseen VPN-verkkoon. Avoin VPN yhteyden avulla mahdollistetaan lähes kaikkien modernien tiedonsiirtoprotokollien siirto VPN-yhteyden välityksellä. Avoin VPN on tietosuojan kannalta merkittävin VPN-ratkaisu, koska se perustuu vapaaseen lähdekoodiin ja se on salaukseltaan tehokkaampi kuin muut vanhemmat teknologiat. [88, 89, 90]

6.4.3.2 Käsi- ja etäkytkimen käyttö

WLAN salaus salaa vain radioliikenteen, kuten alla olevassa kuvassa on esitetty.



Kuva 34. Salattu radioliikenne [91]

Käsi- ja etäkäyttökytkimien käyttöä suosittelevat kyberasiantuntijat. Käytännössä se tarkoittaa, että kyberhyökkäyksen tapahduttua käsi- tai etäkäyttökytkimen avulla voidaan erottaa Swegon uuden sukupolven Wise-järjestelmä ja siihen kytketyt Gold ilmanvaihtokoneet sisäverkosta ilman, että se vaikuttaa niiden toimintaan muuten kuin että niitä ei voida ohjata automaatiojärjestelmän, kuten DCS:n avulla. Muuten järjestelmä toimii normaalisti jollei se ole jo altistunut järjestelmää vaarantavalle komentokoodille. Keskeistä onkin, että järjestelmä erotetaan muusta tietoverkosta, jolloin se erotetaan myös hyökkääjästä ja hyökkääjää viemästä iskua lopulliseen tavoitteeseen eli järjestelmän kaatamiseen tai sabotoimiseen.

Esimerkkinä eräästä käsi- ja etäkäyttökytkimestä, joka on tarkoitettu juuri kyberhyökkäyksiä vastaan, on Siemensin markkinoima RUGGEDCOM kytkin, jossa on etäkäyttömahdollisuus vain sallituille yhteyksille sekä keskitettyjen salasanojen hallintaan ja loogiseen tietoliikenteen eristykseen kytkinporttien avulla. Nimensä mukaisesti RUGGEDCOM laitteet soveltuvatkin juuri teollisuuden vaativiin ympäristöihin, jopa - 40 °C pakkaseen. [92]

6.4.3.3 Verkon segmentointi palomuurein

Tässä insinöörityössä oli tarkoitus miettiä Swegoinin uuden sukupolven Wise-järjestelmän hyödyntämistä teollisuuden toimistoihin. Koska teollisuuskiinteistöt eroavat hyvinpaljon toisistaan esim. toimistot voivat sijaita eri rakennuksessa ja toimistoissa voi olla erillinen rakennusautomaatiojärjestelmä kuin tehdastiloissa, niin tällöin niiden tietoturvavaatimukset eroavat myös huomattavasti toisistaan. Tehdasautomaatiojärjestelmään liityttäessä esim. pilvipalvelun kautta on erityisen tärkeää miettiä standardin SFS/IEC 62443 mukaisia Defence in Depth vaatimustasoluokituksia. Samoin kuin tehtaan omat standardit ja Pöyryn tietoturva säännöt luokittelevat toteutuksille omat vaatimukset tietoturvan ja siihen liittyvän segmentoinnin osalta. Kappaleessa 7.2 esitetään lisäksi järjestelmän integrointia osaksi teollisuusrakennuksen automaatiojärjestelmää ja siihen liittyvää tietoturvaa ja segmentointia.

6.4.3.4 Verkkoliikenneanalysaattori/-monitorointi

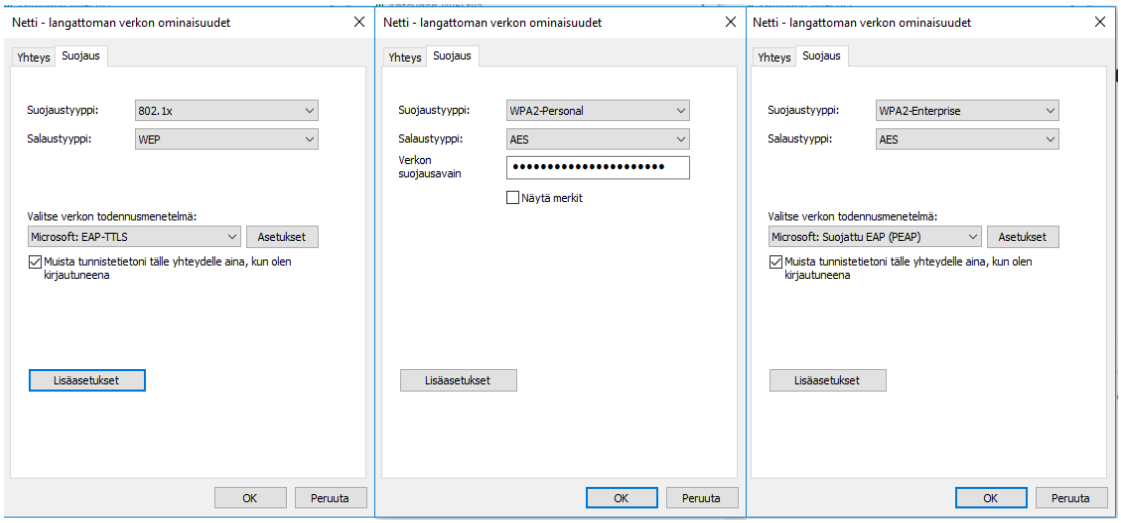
Tehdasympäristössä on tärkeää, että tietoliikennettä seurataan ympäriverkkoa syvyyssuuntaisen (Defence in Depth) mallin vaatimustason 3 mukaisesti langattomalle verkolle tarvitaan oma verkkoliikenteen seurantatyökalu, joka voi olla myös yhdistetty palomuuri- ja verkkoliikenneanalysaattori. Tällä hetkellä vielä lausuntoversiona julkistetussa RIL 268-2017 Kiinteistöä kehittävässä linjasaneerausohjeessakin todetaan, että senroritietojen tekniseen havainnointiin liittyy seuraavien tekijöiden olemassaolo: verkkoliikenneanalysaattorit, tunkeutumisen havaitseminen, palomuurit, lokien hallinta ja valvonta sekä radispektrin valvonta. Eräs kehittyneimmistä ja edistyneimmistä verkkoliikenneanalysaattoreista on Wireshark verkkoliikenneanalysaattori, joka on standardi monilla teollisuudenaloilla, ja mikä on työkalu verkon, palomuurien ja automaation tietoliikenteen analysointiin. Muita verkkoliikenneanalysaattoreita on esim. Ntop verkkoanalysaattori. Verkkoliikenneanalysaattori voi olla verkkoliikenteen seuraamiseen tarkoitettu ohjelma tai teknisesti rakennettu laite. [93, 94].

Verkkoliikennemonitorointi tarkoittaa IT-ammattilaisen sisäisen verkon monitorointia koko laajudessaan usein tehtaan VPN-verkossa. Esimerkkinä teollisuuden hallinnointi-

ja monitorointiohjelmistosta on Beldenin Industrial Hivision Network Management Software teollisuuden Ethernet-verkkojen konfigurointiin ja monitorointiin. Keskeistä verkkojen analysoinnin ja monitoroinnin kannalta onkin juuri tänäpäivänä IT-ammattilaisten kehityksessä mukana pysyminen, kuten uusimpien kyberuhkien tiedostaminen esim. Networkworldin mukaan ARP (Address Resolution Protocol) eli fyysiseen IP-osoitteeseen etsintään liittyvät huijaukset ja haittaohjelmat, Peer to Peer liikenteeseen liittyvät uhat sekä langattomiin verkkoliikenteeseen liittyvät uhat. [95; 96; 97]

6.4.3.5 IPSec-, RADIUS- ja LEAP-suojaustekniikat

IPSec-suojaustekniikka mainittiin aiemmin kappaleessa 6.4.3.4, jossa sen osalta todettiin, että se tukee ainoastaan IPv6 IP-protokollaa. IPSec suojaustekniikka liittyy uude sukupolven Wise-järjestelmän osalta 6LoWPAN radioverkon ja Swegon Director keskusohjausyksikön sekä Super Wise II tiedonsiirtoyksikön välisen tietoliikenteen suojaamiseen. Swegon Connectin langattomassa tiedonsiirtoyksikkössä on myös tuki IPSec-suojaustekniikalle. RADIUS-suojaustekniikka, jonka tarkoituksena on hallinnoida laitteiden salasanoja paikallisesti tai etänä. Aiemmin laitteiden salasanoja ei voinut automaatioverkossa muuttaa, johtuen huollon, nopean palautumisen tai integraation takia, mutta nykyisin eri laitteiden salasanakäytäntö on muuttunut ja RADIUS-serverin avulla pystytään eri automaatiolaitteiden salasanoja hallinnoimaan paikallisesti tai etänä. RADIUS-suojaustekniikka on kuitenkin varsin kallista toteuttaa ja vaihtoehtona on LEAP-suojaustekniikan käyttö. LEAP (Light Extensible Authentication Protocol) perustuu Ciscon luomaan EAP-yhteyskäytäntöön, jossa laillisuustarkistusmekanismi perustuu haaste-vastaus-yhteyskäytäntöön sekä suojausavainten dynaamiseen määrittämiseen. Lisäksi on olemassa muita hyvin tehokkaita suojaustekniikoita, kuten LEAP-tekniikkaa tehokkaampia tunnelointitekniikoita EAP-FAST-, EAP-TTLS- ja PEAP-suojaustekniikat, jotka ovat vielä valmisteilla ja suunniteltu LEAP-tekniikan korvaavaksi suojaustekniikaksi. [98; 99]



Kuva 35. Langattoman 4G-verkon suojaus kotitaloudessa

Kuvassa 33 on esitetty esimerkin omaisesti omassa kotitaloudessani käytettävän 4G-verkon suojauskäytänteestä. Eli vasemmalla on esitetty suojaustekniikka mikä toteuttaa suojaustyyppiä 802.1x ja salaustyyppiä WEP eli on suojaamattomin salaustyyppi. Keskellä on esitetty kotiverkon suojaustyyppi WPA2-Personal salaustyyppinä AES ja verkon suojausavain perustuu 4G-reitittimen oletussalasanaan (default) tai itse määritettävään salasanaan. Kyseisessä näkymässä salasanan voi vaihtaa laittamalla rastin kohtaan näytä merkit tai vaihtoehtoisesti ottamalla yhteyden 4G-reitittimen IP-osoitteeseen ja muuttamalla salasana reitittimen valmistajan asetuksista. Kuvassa oikealla on esitetty yrityskäyttöön tarkoitetun suojaustyypin näkymästä (voidaan käyttää myös kotitaloudessa), jossa suojaustyyppi on WPA2-Enterprise ja salaustyyppi AES. 802.1x ja WPA2-Enterprise suojaustyypeissä voidaan valita, että verkon todennusmenetelmä on älykortti tai muu varmenne, kuten suojattu EAP (PEAP) tai EAP-TTLS. Lisäksi suojaus voidaan kokonaan poistaa käytöstä, jolloin kuka tahansa langattoman kantoalueen sisäpuolella voi ottaa yhteyden kyseiseen reitittimeen ja päästä vapaasti käsiksi langattomaan verkkoon.

6.4.3.6 Salasanageneraattoreiden ja salasanapankkien käyttö

Nykyään salasanageneraattoreiden käyttö on suosittua kotitalouksissa esim. verkkopankkiyhteyksien muodostamisessa sekä joissain yrityksissä sitä käytetään myös etäyhteyksien muodostamiseen. Salasanageneraattori voi siis olla erillinen laite, joka on tietoturvallisin tapa toteuttaa verkkoyhteyden muodostaminen esim. automaation HMI-laitteilla tai se voi olla erillinen salasanagenaraattoriohjelma tai salasanapankki. Salasanageneraattorit ovat hyvä tapa suojata esim. pilvipalveluihin kirjautumista, kun monesti tehdas- ja huoltoympäristössä vaativien salasanojen käyttöä ei välttämättä ole totuttu hyödyntämään.

6.4.3.7 Paritustekniikan ja IV-koneen käsipäätteen suojaaminen

Swegon uuden sukupolven Wise-järjestelmässä, niin kuin monessa muussakin järjestelmässä antureiden ja laitteiden paritustekniikkaan liittyvä tietoturva arveluttaa jo siltäkin osalta, jos joku ulkopuolinen henkilö esim. toimistokiinteistössä pystyy lukemaan tarran omalla kännykkäsovelluksellaan ja muodostaa oman kännykän avulla yhteyden langattomiin antureihin ja laitteisiin, esim. tilanteessa, jossa antureiden tai laitteiden päälle on jäänyt QR-kooditarra. Swegon uuden sukupolven Wise-järjestelmän pariliittämisessä käytettyä Tune Wise skannerin, Connect Wise käsipäätteen ja Connect Wise pariliitäntään liittyvissä dokumenteissa sanotaan, että pariliitännän käyttöönoton saa tehdä vain valtuutettu ja koulutettu WISE-huoltoteknikko. Vaikka järjestelmän käyttöönotto on tarkasti rajattu valtuutettujen ja koulutettujen Wise-huoltoteknikkojen vastuulle, niin tietoturvariski on silti olemassa. Skanneri on bluetooth yhteydessä pariliittämisen aikana käsipäätteeseen ja käsipääte on WLAN-yhteydessä käsipäätteeseen asennettavan USB-mokkulan avulla. Tietoturva liittyy siis keskeisesti käsipäätteen WLAN-yhteyden tietoturvaan ja QR-koodien todentamiseen. Markkinoilla on useita QR-koodien lukijasovelluksia, joilla voidaan varmistaa QR-koodien turvallisuus, esimerkkinä Kapersky tietoturvayrityksen markkinoima Kapersky QR-Scanner sovellus. Uuden sukupolven Wise-järjestelmässä pariliitäntään liittyvä QR-koodien lukemisella on pyritty helpottamaan laitteiden liittämistä, mutta tietoturvallisin tapa on edelleenkin lukea ja syöttää tiedot suoraan pää-

telaitteille ja Wise-järjestelmien tuotteiden osalta tämä onnistuu QR-koodien vieressä sijaitsevan RFID-numerosarjan avulla, kuten alla olevassa kuvassa 36 on esitetty. [84; 85; 86; 87; 100]

Kuva 36. Wise IRE anturin QR-koodi ja RFID-numerosarja [21]

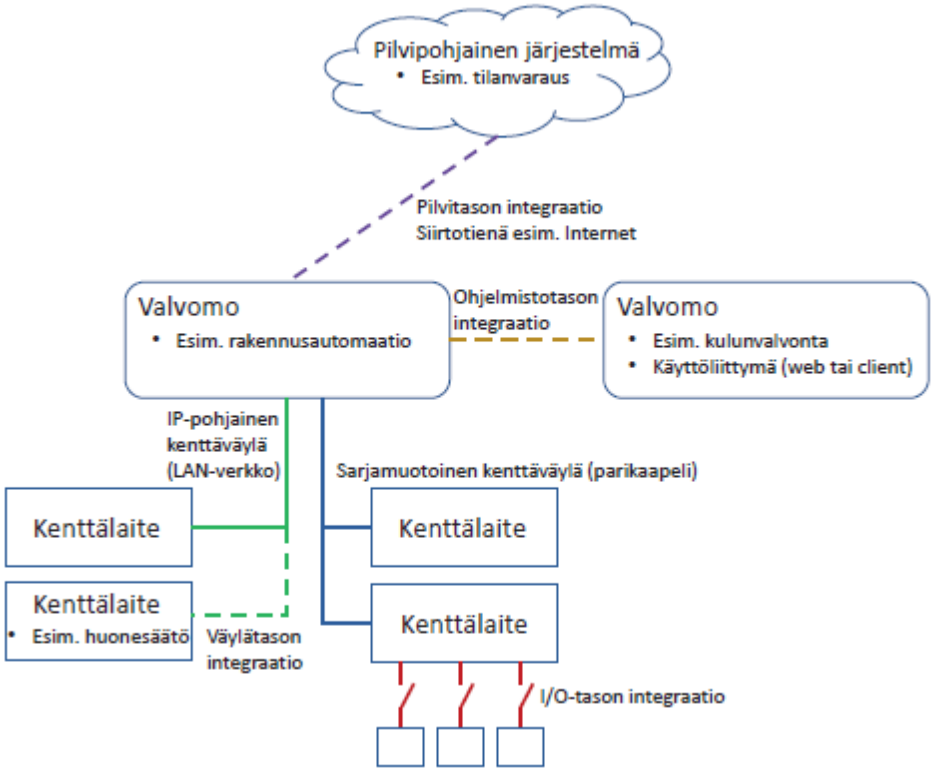
6.4.3.8 IEEE 802.11ax -verkkostandardilla saavutettava tietoturva

WiFi 6 eli 802.11ax standardissa itsessään ei ole määritelty uusia turvallisuusparannuksia tai vaatimuksia, mutta se edellyttää WPA3-suojausta ennakkoehtona. Tämän seurauksena 802.11ax-laitteet sisältävät uusimmat tietoturvaominaisuudet ja -ominaisuudet, jotka eivät olleet olemassa vielä muutama vuosi sitten, kun 802.11ac standardi julkaistiin - puhumattakaan standardeista 802.11n ja 802.11g (julkaistu vuosina 2009 ja 2003). WiFin WPA3 -suojaprotokolla, tuo esiin turvallisuuden parannuksia, tärkeimpänä samanaikainen yhtäläisyyksien todentaminen (SAE) korvaa WPA2-Personalin ennalta jaetun avaimen (PSK). WPA3 -suojausprotokolla vaatii myös suojatut hallintakehykset (PMF), joka tarjoaa tehokkaampaa suojaa korkean tason hyökkäyksiltä. Lisäksi WPA3-suojausprotokolla tarjoaa valinnaisen 192-bittisen salausohjelmiston. [101]

7 Tiedonsiirto automaatiojärjestelmään

7.1 Integrointi käytännössä

Integrointi voidaan toteuttaa käytännössä kenttätason-, kaapelitason-, keskustason- tai käyttöliittymätason integroinnilla. Kuvassa 35 on esitetty eri integrointitasoja, joilla järjestelmät ja kenttälaitteet ovat yhteydessä rakennusautomaatiojärjestelmään. [56, s. 3]



Kuva 37. Erilaisia integrointitasoja rakennusautomaatiojärjestelmään [56, s.8]

Kenttätason integroinnilla tarkoitetaan käytännössä I/O-tason integrointia kosketinohjauksina. Kenttätason integrointi on yleisin ja yksinkertaisin integrointitapa eri järjestelmien ohjauksien välillä. Kenttätason huonot puolet liittyvät laajaan kaapelointitarpeeseen ja vain suppeaan on/off – tyyppisiin tieto-ominaisuuksiin. [56, s. 4]

Fyysinen kaapelitason integrointi tarkoittaa käytännössä väylätason integraatiota eri järjestelmien välillä samaa tiedonsiirtoprotokollaa käyttäen, jolloin puhutaan yleisesti kenttäväylätekniikasta. Etuina väylätason integroinnissa on parikaapelilla toteutettava yksinkertaisuus, tiedonkulun reaaliaikaisuus ja toimintavarmuus. Tiedonsiirtoprotokollia on olemassa useita (esim. Modbus, BACnet, KNX) ja tiedonsiirtoprotokolla voi olla myös valmistajakohtainen. Yleisin kaapelityyppi kaapelitason integroinnissa on parikaapeli, mutta Ethernet kaapeli (IP-verkkokaapeli) on paljon yleistynyt väylätason kaapelityyppinä. IP-pohjaiset kenttäväyläprotokollat ovat alkaneet yleistymään nopeasti, johtuen erilaisista mahdollisuuksista datan siirtämiseen ja IP-pohjaisten protokollamuuntimien yleistymisestä. IP-pohjaisilla protokollamuuntimien etuna on, että sarjamuotoista tietoa voidaan muuntaa esim. IP-verkon yli toimivaksi. Kaapelitason integraation ongelmat liittyvät yleisesti seuraaviin tekijöihin:

- järjestelmävalmistajien asettamat rajoitteet, kuten ohjauspisteiden luenta ja kirjoitustiedon puutteet
- sarjamuotoisen väylän herkkyys signaalin häiriöille
- IP-pohjaisten väyläratkaisujen tietoverkon reititykseen liittyvät puutteet
- IP-pohjaisten väyläratkaisujen tietoturvan puutteet (salaamattomat kenttäväylä-protokollat). [56, s. 4]

Keskustason integraatiolla tarkoitetaan käytännössä valvomo- ja ohjelmistotason integraatiota. Valvomo- ja ohjelmistotason integrointi on voitu toteuttaa valvomotasolla usean erillisjärjestelmän käyttöliittymätason integraationa siten, että ohjaus ja hallinta mahdollistetaan yhdellä graafisella käyttöliittymällä. Usein usean eri talotekniikan järjestelmän integroidusta järjestelmästä käytetään nimitystä kiinteistöhallintajärjestelmä (BMS). Etuna yhden käyttöliittymä yhteissovelluksessa on käytön tehostaminen useiden valvomoiden ja käyttöliittymäjärjestelmien sijaan sekä kattavat ohjelmistotason konfigurointi mahdollisuudet eri tilanteisiin ja käyttäjille kohdennettuina. Kun puhutaan älykkäistä järjestelmistä, niin sillä tarkoitetaan käyttöliittymäintegrointia ohjelmistotasolla, niin että tie-

toa vaihdetaan kahden tai useamman eri järjestelmän välillä pistetasolla, joka mahdollistaa tiedon hyödyntämisen myös automaattisten toimintojen toteutukseen, kuten ilmanvaihdon ohjaaminen kulunvalvontatiedon perusteella. [56, s. 4-5]

Käyttöliittymätason integroinnilla tarkoitetaan laajamittaisesti yleistyneitä pilvipalveluita, jotka on toteutettu Web-käyttöliittymätason integraatiolla. Usein puhutaan SaaS -tyyppisistä palveluista (Software as a Service) eli ohjelmisto palveluna tyyppisistä integrointiratkaisuista, jolloin pilvipalvelu toimii esim. Web-pohjaisella käyttöliittymällä järjestelmään. Nykyään myös pilvipalvelut toimivat useasti myös älypuhelin käyttöliittymien avulla kännykkäverkossa. Pilvipalveluiden avulla toteutettu integraatio koskee eri pilvipohjaisten järjestelmien välistä integraatiota pilvitasolla eli kokonaan kiinteistön ulkopuolella. Erona valvomo- ja ohjelmistotason integrointiin on juuri se, että tieto liikkuu kiinteistön ulkopuolella ja pilvipalvelu on ulkoistetun palveluntarjoajan hallinnassa. Pilvipalvelut mahdollistavat laajamittaisen tiedon hyödyntämisen eri pilvipalveluiden välillä sekä uusien sovellusten ja innovaatioiden nopean hyödyntämisen. Ongelmana on kuitenkin tiedon luottamuksellisuus, tiedon eheys ja tiedon saatavuus. [56, s. 5]

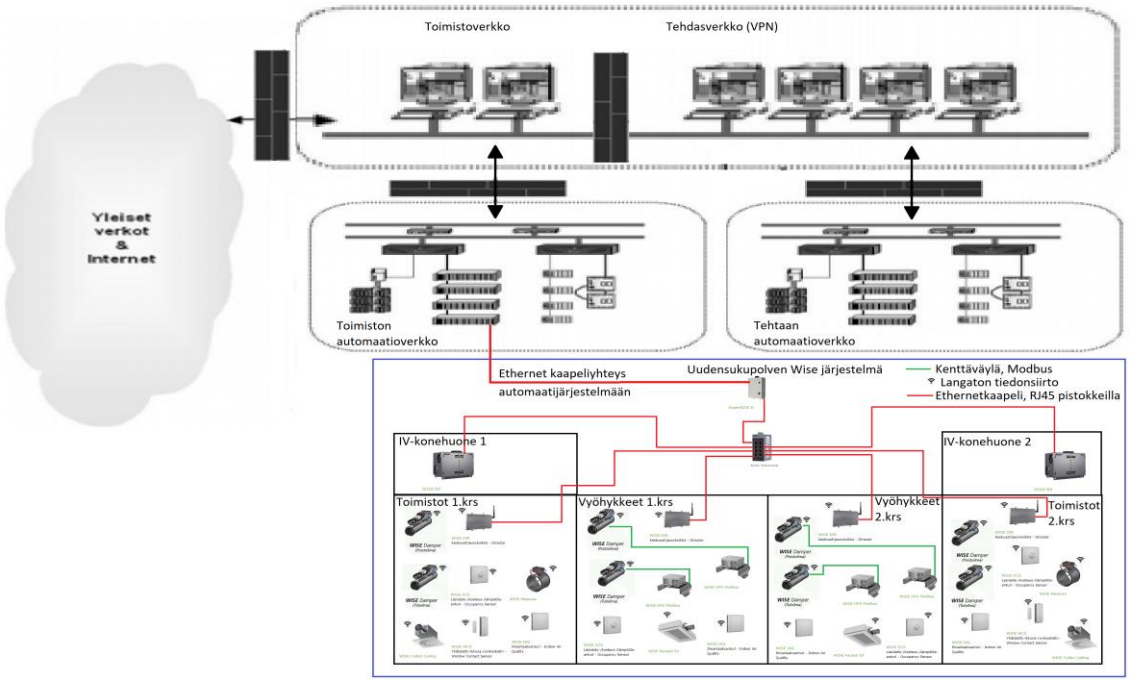
Integrointia suunniteltaessa järjestelmien tekninen yhteensovittaminen on syytä kuvata suunnitelmissa I/O- tai väylätasolla, jolla varmistetaan standardien väyläratkaisujen käytettävyys, urakkarajat ovat selkeät, urakka on helposti jaettavissa ja mahdollistetaan laajempien integroitujen kokonaisratkaisujen tarjoaminen. [56, s.7]

7.2 Toteutusratkaisu - Swegon uuden sukupolven Wise-järjestelmä

7.2.1 Antureiden, toimilaitteiden ja päätelaitteiden tiedonsiirto

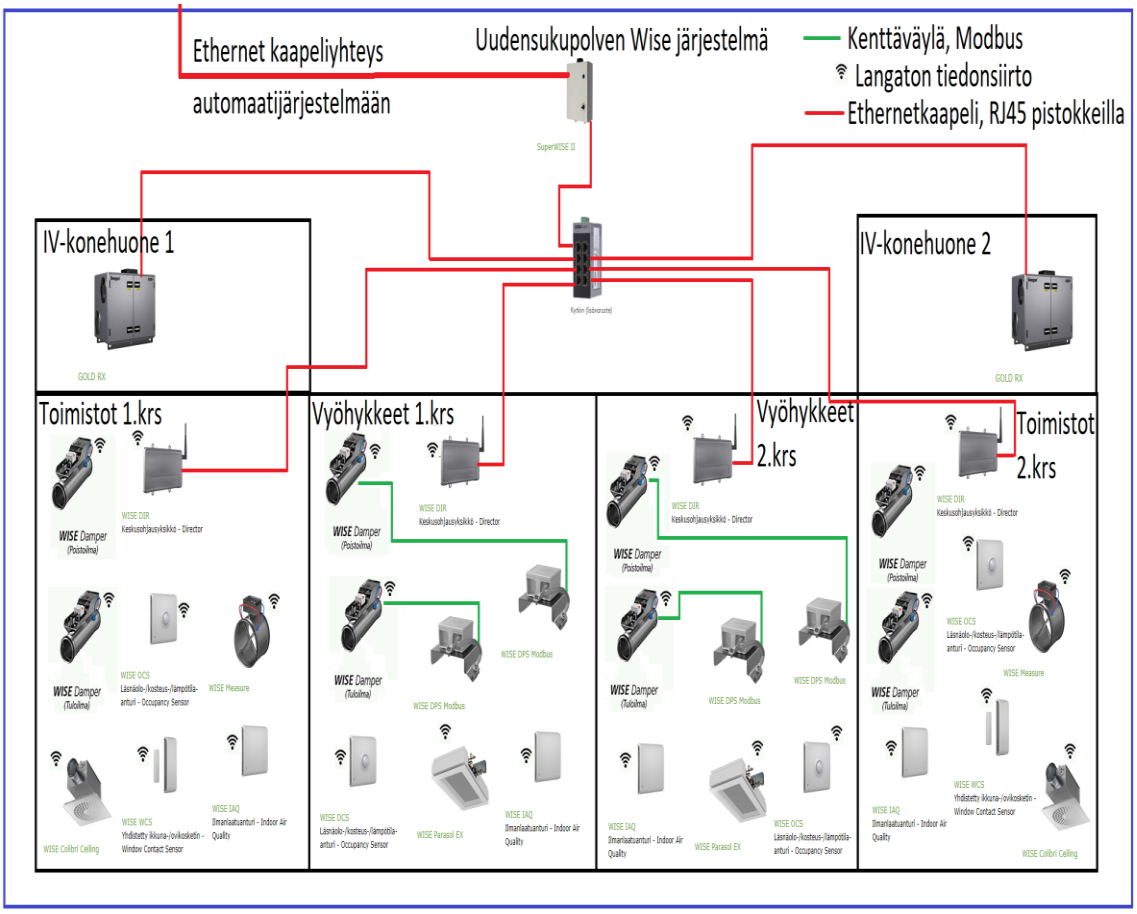
Swegon Wise-järjestelmän anturi, toimilaite ja päätelaitteiden IoT-verkon linkkikerroksessa on käytössä AES 128 bittinen salausalgoritmi ja järjestelmään on mahdollista toteuttaa mikä tahansa IP-perustainen tietoturvaprotokolla/ratkaisu ja olettamuksena IoT-verkossa on täysi Wifi 6 verkon IPv6-tuki. [102]

7.2.2 Integrointi syvyyssuuntaisen suojaustason (Defence in Depth) 0 mukaisesti toimiston rakennusautomaatio-järjestelmään



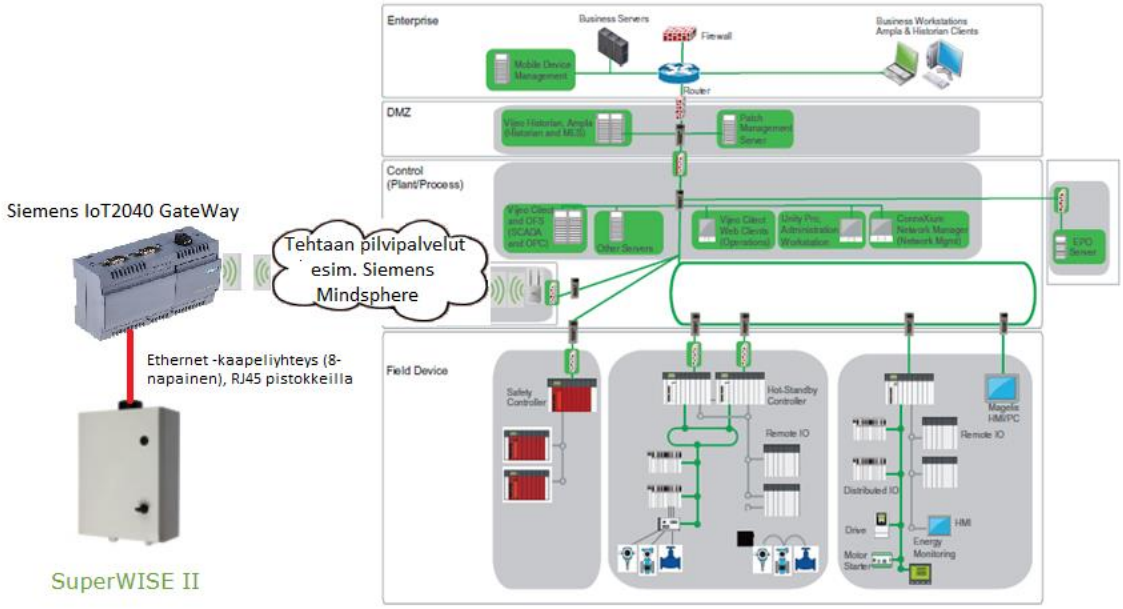
Kuva 38. Syvyyssuuntaisen suojaustason 0 (Defence in Depth) periaatekuvaus [30; 73]

Kuvassa 38 on esitetty syvyyssuuntaisen suojaustason 0 periaatekuvaus. Keskeistä on huomata, että muille suojaustasoille ominainen segmentointi puuttuu kyseisestä mallista. kuvassa 39 on vielä esitetty selkeämmin uuden sukupolven Wise-järjestelmän periaatekuvaus, jossa Super Wise II ohjausyksikön ja toimiston automaatiojärjestelmän yhteys on toteutettu langallisena kenttäväyläyhteytenä eikä ohjausyksikkö tällöin sisällä Swegon Connect langatonta tiedonsiirtoyksikköä.



Kuva 39. Uuden sukupolven Wise -järjestelmän periaatekuvaus [30]

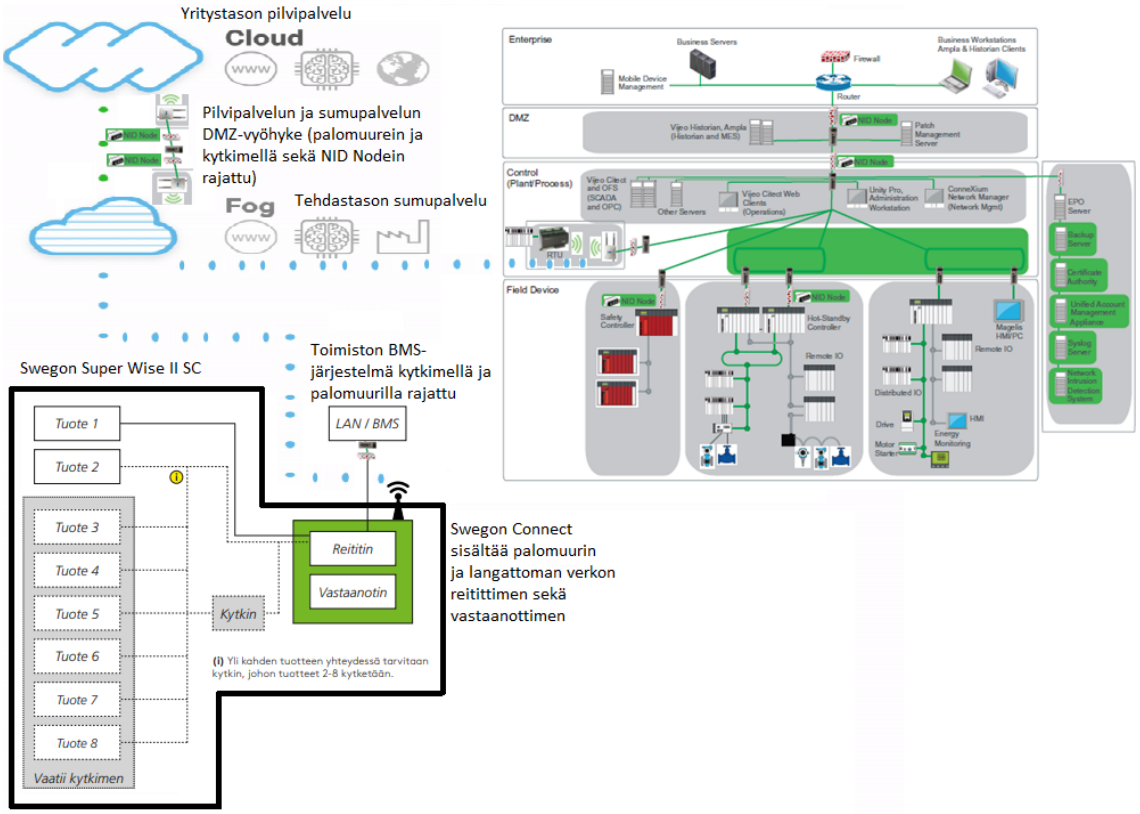
7.2.3 Langaton integrointi tehtaan pilvipalveluun syvyyssuuntaisen suojaustason (Defence in Depth) 1 mukaisesti



Kuva 40. Langaton integrointi syvyyssuuntaisen suojaustason 1 mukaisesti ja toteutus virtuaalisena pilvipalveluna [30; 60; 50]

Kuvassa 40 on esitetty syvyyssuuntaisen suojaustason 1 mukainen kuvaus mahdollisesta toteutuksesta (vrt. kappale 6.2.2), jossa Super Wise II -tiedonsiirtoyksikkö, joka toimii järjestelmän rajapintana muuhun tehdasautomaatiojärjestelmään, on kytketty Siemensin IoT2040-kenttäväylän avulla tehtaan pilvipalveluun.

7.2.4 Langaton integrointi syvyyssuuntaisen suojaustason (Defence in Depth) 2 mukaisesti sumupalvelun avulla tehtaan pilvipalveluun

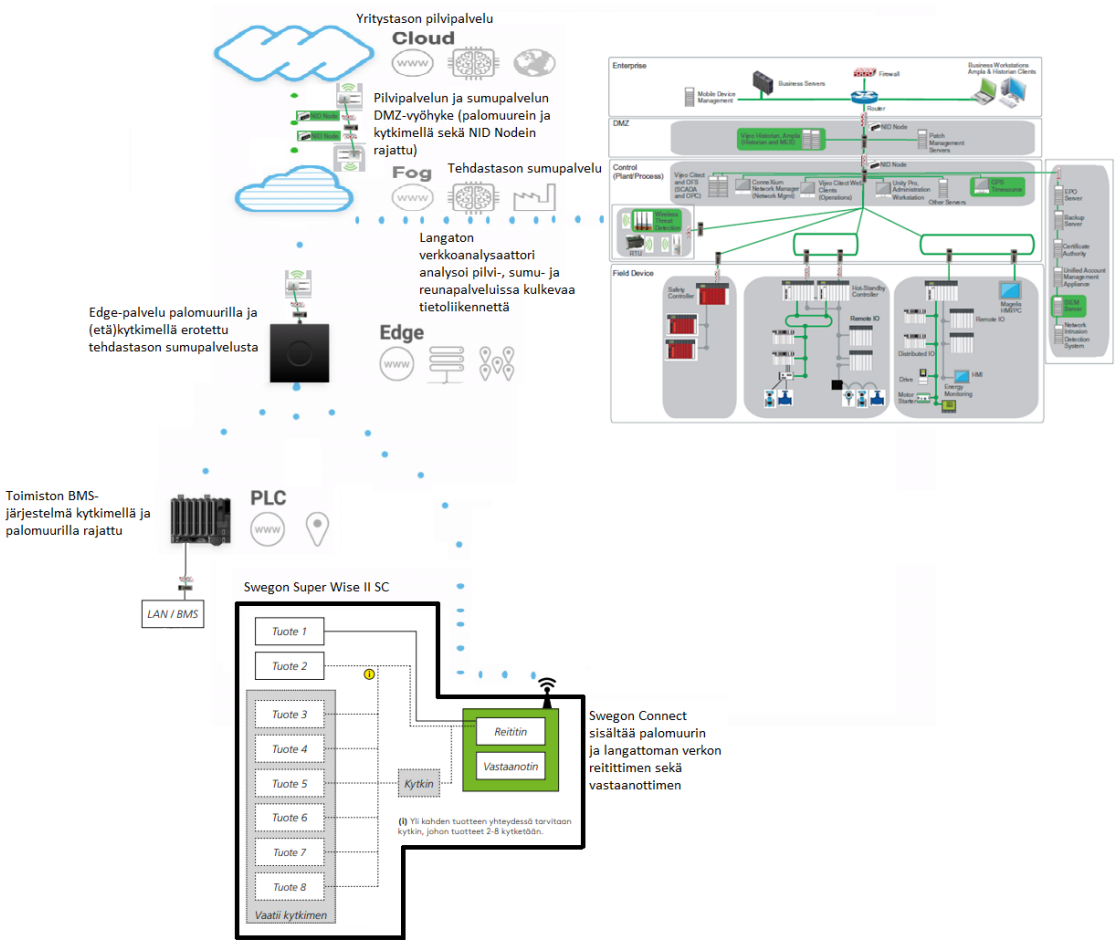


Kuva 41. Langaton integrointi Swegon Connectin avulla tehtaan sumupalveluun syvyyssuuntaisen suojaustason 2 mukaisesti [60; 81]

Kuvassa 41 on esitetty Swegon Super Wise II SC tiedonsiirtoyksikön, sisältäen Swegon Connect tiedonsiirtoyksikön, integroinnin tehdastason sumupalveluun syvyyssuuntaista suojaustasoa 2 mukaillen (vrt. kappale 6.2.3). Keskeistä Swegon Connect tiedonsiirtoyksikön liittämisessä tehdastason sumupalveluun on, että Swegon Connectin mukana tulevaa Swegonin omaa pilvipalvelua ei tietoturva syistä saa ottaa käyttöön. Swegonin pilvipalvelusovellus kuuluu usein toimitukseen ja otetaan käyttöön liittämällä Swegon Connect pilvipalvelun mahdollistava usb-mokkula Swegon Connect usb-porttiin. Tämä asia

pitää tilauksessa huomioida ja yrittää tilauksen yhteydessä sopimuksella velvoittaa toimittajaa tietoturvasyistä jättää usb-mokkula pois tilaukselta tai hän vastaa mahdollisista tietoturva ongelmista esim. sanktiomalliin perustuen.

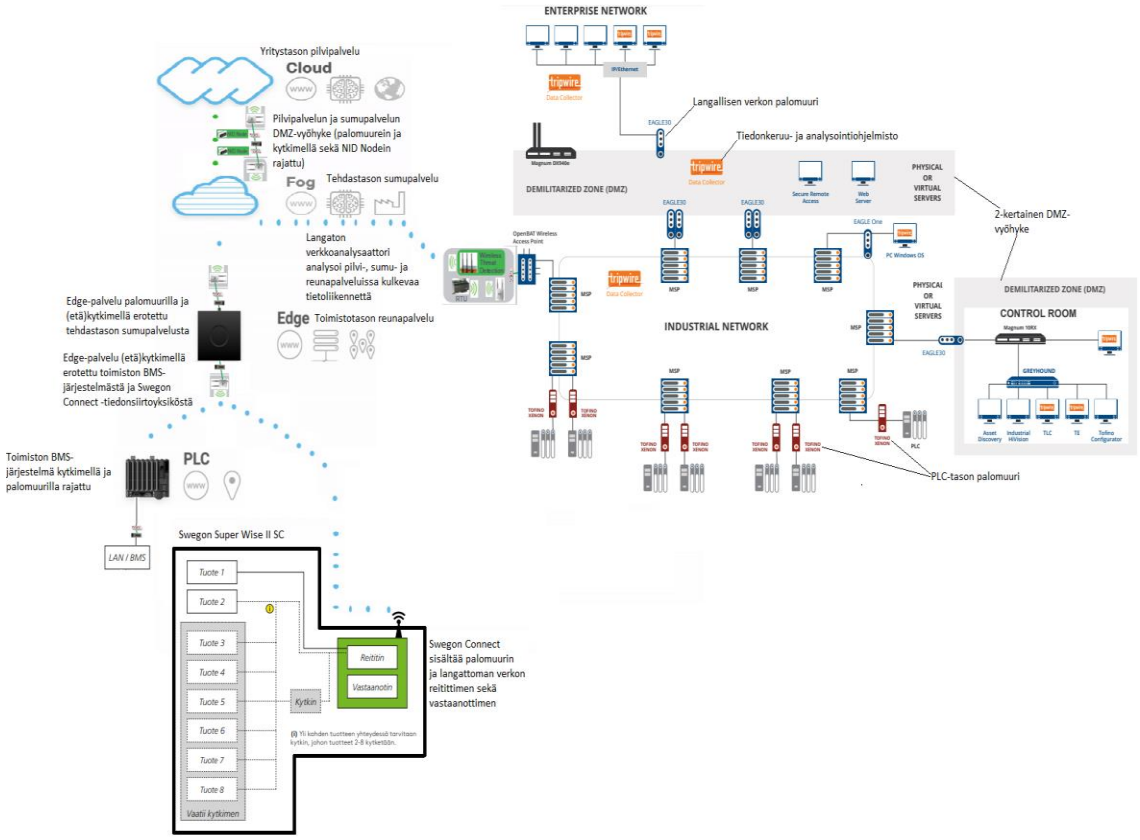
7.2.5 Langaton integrointi syvyyssuuntaisen suojaustason (Defence in Depth) 3 mukaisesti reunapalvelun avulla tehtaan pilvipalveluun



Kuva 42. Langaton integrointi Swegon Connectin avulla toimiston reunapalveluun syvyyssuuntaisen suojaustason 3 mukaisesti [60; 81]

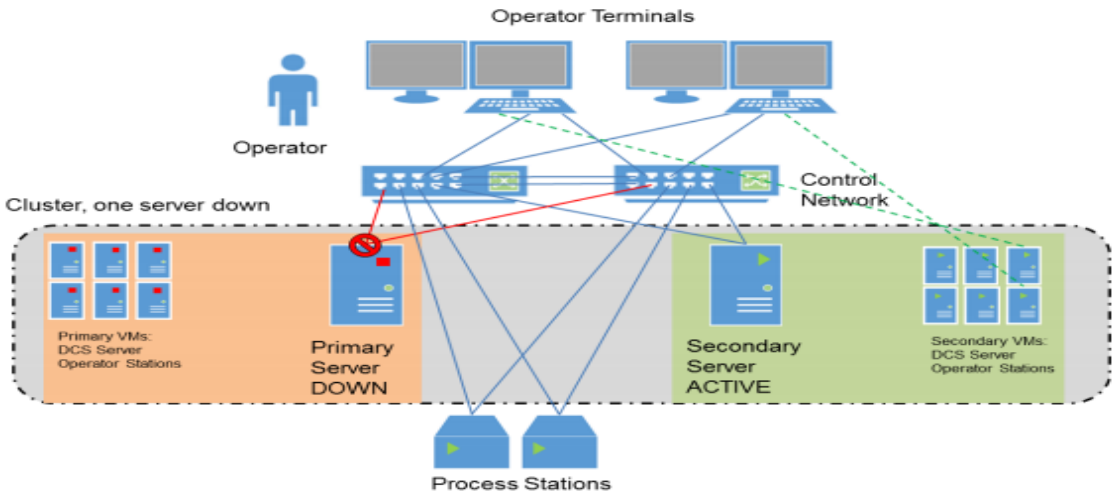
Kuvassa 42 on esitetty Swegon Super Wise II SC -tiedonsiirtoyksikön, sisältäen Swegon Connect tiedonsiirtoyksikön, integroinnin toimiston reunapalveluun syvyyssuuntaista suojaustasoa 3 mukaillen (vrt. luku 6.2.4). Mallissa reunapalvelu (Edge) on erotettu palomuurilla tehdastason pilvipalvelusta eli segmentoitu omaksi toimistotason vyöhykkeeksi. Samoin kuin edellisessä suojaustasossa, Swegon Connectin mukana tulevaa Swegonin omaa pilvipalvelua ei tietoturvasyistä saa ottaa käyttöön.

7.2.6 Langaton integrointi 2-kertaisen ei-kenenkään-maa mallin mukaisesti



Kuva 43. Langaton integrointi 2-kertaisen ei-kenenkään-maa mallin mukaisesti [73; 81; 103]

Kuvassa 43 on esitetty langaton integrointi 2-kertaisen ei-kenenkään-maa mallin mukaisesti. Uutena syvyyssuuntaiseen vaatimustasoon 3 nähden on malliin tullut kaksinkertainen DMZ-vyöhyke langallisessa verkossa (vahvennettu ohjaustason DMZ-vyöhyke), kriittisten prosessien PLC-tason palomuureja, joita löytyy esim. Belbinin valikoimasta ja Tripwire -tiedonkeruu ja analysointiohjelmistoja sekä erilaisia kytkintyyppejä, joissa on mukana tietoliikenteen automaattista seurantaa tukevia toimintoja sekä etäkytkentä ominaisuuksia. 2-kertaista ei-kenenkään-maa mallia voitaisiin katsoa tulevaisuudessa käyttävän ne teollisuusyritykset ja energiantuotantolaitokset, jotka kokevat toimintansa kriittiseksi esim. valtiollisten kyberuhkatekijöiden varalta ja ovat toistuvasti joutuneet kyberhyökkäyksien kohteeksi. Mallia voitaisiin täydentää vielä esim. eri pilvipalveluiden omilla tiedonkeruu- ja analysointiin keskittyvillä monitorointipäätteillä, jolloin eri pilvipalvelusovellusten (Pilvi-, sumu- ja reunapalvelut) erottaminen kriittisessä tilanteessa edesauttaa kyberhyökkäykseltä palautumisessa. Toiseksi DMZ Control Room -vyöhyke voitaisiin vielä jakaa kahteen eri DMZ-vyöhykkeeseen, niin että ohjaustoiminnot ja tiedon varastointi- ja prosessessointipalvelimet olisivat langallisessa automaatioverkossa sijoitettuna eri vyöhykkeille. Samoin edellä esitetyistä malleista puuttuu kokonaan tehdastason varajärjestelmän esittäminen, koska mallit kuvasivat pääsääntöisesti järjestelmäarkkitehtuuria ja Swegon Wise-järjestelmän liittämistä osaksi teollisuuslaitosten automaation tietoliikennearkkitehtuuria. Varajärjestelmän kuvauksesta on esitetty kuvaus esimerkinomaisesti seuraavassa kuvassa, jossa ohjaus siirtyy varalla olevalle palvelimelle. [73; 103; 104.]



Kuva 44. Esimerkki varajärjestelmän käytöstä ESXi-palvelimella [104]

8 Sisäilman laatutekijät ja niiden mittaaminen asuin-, toimisto- ja teollisuuskiinteistöissä

8.1 Sisäilmaston epäpuhtaudet

Ennen kuin voidaan mieltää sisäilman laatutekijöitä, on hyvä käydä hieman läpi sisäilman epäpuhtaus luokittelua. Sisäilman epäpuhtaudet jaetaan yleensä kahteen tai kolmeen kategoriaan – riippuen luokittelusta – hiukkasmaiset- ja kemialliset- sekä biologiset epäpuhtaudet. Erona on tietenkin se, että hiukkaset, jotka ovat kiinteitä pystytään vain harvoin ilmanvaihdolla vaikuttamaan muuten kuin ulkoilman suodatuksella, niin ettei ulkoilmasta pääse kontaminoitumaan hiukkasia sisätiloihin. Kemialliset epäpuhtaudet ovat luonnossa muussa kuin kiinteässä muodossa esiintyviä, usein kaasumaisia epäpuhtauksia. Biologiset epäpuhtaudet esiintyvät kaasumaisessa, kiinteässä tai nestemäisessä muodossa olevia toisten aineiden kanssa reagoivia ainesosia. Seuraavassa listassa on esitetty, mitä eri hiukkasmaisia ja kemiallisia epäpuhtauksia usein huoneilmastossa voi esiintyä.

- Hiukkasmaiset epäpuhtaudet
    - huonepöly, epäorgaaniset kuidut, asbesti, mineraalivillat, PCB, yms.
- Kemialliset epäpuhtaudet
    - hiilidioksidi, radon, tupakansavu, hiilimonoksidi, ammoniakki, VOC-yhdisteet (haihtuvat orgaaniset yhdisteet), PAH-yhdisteet, otsoni, yms. [105, s. 14]
- Biologiset epäpuhtaudet
    - allergeenit, kosteusvauriomikrobit, bakteerit ja virukset [15, s. 66-67]

Sisäympäristöongelmat ovat yleisiä toimistotyöpaikoilla ja teollisuudessa. On arvioitu, että jopa kaksi kolmasosaa Suomen työvoimasta työskentelee toimistoissa tai vastaavissa tiloissa, joissa sisäympäristöön liittyvät ongelmat ja niihin liittyvä oireilu on yleistä. Yleisimpiä sisäilmastolähtöisiä ongelmien aiheuttajia katsotaan olevan ilmanvaihdon ongelmat, liian korkea lämpötila tai ilmanjakoon liittyvät ongelmat, kuten veto, kosteusvaurioiden synnyttämät mikrobiperäiset epäpuhtaudet, materiaalien päästöt sekä teollisten mineraalikuitujen aiheuttamat ongelmat. Yleisiä fysikaalisia, kaasumaisia ja hiukkasmaisia sisäilman laatuun liittyviä tekijöitä on esitetty taulukossa 3. [106, s. 14-15]

Taulukko 3. Yleiset sisäilman laatuun vaikuttavat fysikaaliset, kaasumaiset ja hiukkasmaiset tekijät [106, s.15]

Fysikaaliset tekijät	Kaasut		Hiukkaset
	Orgaaniset kaasumaiset epäpuhteudet	Epäorgaaniset kaasumaiset epäpuhtaudet	
Ilman liike	Hyvin haihtuvat orgaaniset yhdisteet (VVOCs)	Hiilimonoksidi	Huonepöly (sisältäen ihmisten ja eläinten hilseen)
Ilman kosteus	Haihtuvat orgaaniset yhdisteet (VOC)	Rikkidioksidi	Liikenteen ja energiantuotannnon hiukkaspäästöt (esim. ultrapienet hiukkaset)
Lämpötila	Puolihaihtuvat orgaaniset yhdisteet (SVOCs)	Typpidioksidi	Mikrobit (esim. Homesienet ja bakteerit) ja niiden aineenvaihdunta-tuotteet
Säteily (pientaajuiset magneettikentät)	Polysykliset aromaattiset hiilivedyt (PAH-yhdisteet)	Otsoni	Kuidut (esim. asbestikuidut, teolliset mineraalikuidut)
Melu		Ammoniakki	Tupakansavun hiukkasmaiset epäpuhtaudet
Valaistus		Radon	

Taulukossa 3 esitettyjen orgaanisten kaasumaisten yhdisteiden jaotteluna on käytetty neljää eri ryhmää perustuen niiden eri kiehumispisteisiin. VVOC kaasuyhdisteet, eli erittäin haihtuvat yhdisteet (very volatile organic compounds) ovat aineyhdisteitä, joiden kiehumispisteet ovat luokassa <0...50–100 °C, esimerkkinä formaldehydi ja pentaani. VOC kaasuyhdisteet, eli haihtuvat orgaaniset yhdisteet (volatile organic compounds) ovat aineyhdisteitä, joiden kiehumispisteet ovat luokassa 50–100...240–260 °C, esimerkkinä styreeni, tolueeni ja ksyleeni. SVOC kaasuyhdisteet, eli puolihaihtuvat yhdisteet ovat aineyhdisteitä, joiden kiehumispiste on luokassa 240–260...380–400 °C, esimerkkinä flataatit. Lisäksi on olemassa vielä neljäs kaasumainen yhdiste ryhmä, jota kutsutaan POM kaasuiksi eli hiukkasiin sitoutuneet yhdisteet (polysyclic organic matter) joiden kiehumispiste on luokassa >380 °C. [106, s. 15]

8.2 Keskeiset sisäilman laatutekijät toimistokiinteistöissä

Usein sisäilmaongelmat eivät johdu pelkästään ilmanvaihdosta vaan usein sisäilmatekijät ovat monen tekijän summa esimerkiksi sisäilman lämpötila, ilman kosteus pitoisuus, sisätilojen siisteys ja mikrobikasvusto, rakenteet ja kalusteet, ihmisten ja vaatteiden mukanaan kuljettamat epäpuhtaudet, ääni, hiilidioksidi (CO_2), orgaaniset aineyhdisteet (VOC) ja muut haitalliset aineet ja kaasut. [15 s. 66-67]

8.2.1 Hiukkasmaisien epäpuhtauksien esitystavat 2,5 ja 10 ja niiden eroavaisuudet

Hiukkasmaisia epäpuhtauksia mitataan usein hiukkaskokoina, jotka ovat alle 2,5 mikrometriä ja alle 10 mikrometriä. Sisäilmassa esiintyvät pienhiukkaset ovat pääosin peräisin ulkoilmasta, kuten liikenteen, teollisuuden tai naapurikiinteistöistä tulevista pienhiukkasista. Pienhiukkaset jaetaan niiden olemassa olon perusteella orgaanisiin- ja epäorganisiin pienhiukkasiin. Usein alle yhden mikrometrin leijuvia pienhiukkasia pyritään poistamaan ulkoilmasta ilmanvaihdon avulla, kun taas yli yhden mikrometrin hiukkasia poistetaan erilaisin siivousmenetelmin. Ihmisten keuhkoihin leviävät pienhiukkaset ovat

kooltaan alle 5 mikrometriä ja päästessään keuhkoihin ne voivat alveolijakeen avulla päästä ihmisen verenkiertoon. [107]

8.2.2 Keskeiset mitattavat kaasu- ja aineyhdisteet toimistorakennuksissa

Seuraavassa listassa on esitetty keskeisitä sisäilman laatutekijöitä, joita usein mitataan sisäilman terveellisyyden kannalta:

1. Lämpötila

   Lämpötila ilmaisee ilmassa olevan kaasun tilavuuden ja/tai paineen muutosta tiettynä aikana ja lämpötilalla on suora yhteys epäpuhtauksien erityisesti biologisten eli orgaanisten epäpuhtauksien olemassa oloon. [106, s 14-15]

2. Kosteus

   Erityisesti kosteus on useammin pääasiallisena ongelman lähteenä monessa sisäilmaongelma tapauksessa. Kosteuden avulla monet biologiset hiukkaset, kuten kosteusvauriomikrobit ja hiukkasiin sitoutuneet kaasumaiset yhdisteet (POM yhdisteet) pystyvät lisääntymään ja jatkamaan lisääntymistä. Nykyään ei ole vielä tutkimuksin pystytty todistamaan, miten eri biologisperusteiset kosteusvauriomikrobit reagoivat erilaisten rakennusmateriaalien kanssa, kun ympäristöolosuhteet kuten kosteus ja lämpötila edesauttavat niiden olemassa oloa. Useat rakennusaineet kuten betoni ovat arkoja liialliselle kosteuspitoisuudelle ja tällöin erilaisten hiukkasmaisten biologisten ainayhdisteiden leviäminen, lisääntyminen ja jossain tapauksissa myös rakennusmateriaalien heikentyminen voidaan katsoa johtuvan näiden biologisten hiukkasmaisten kosteusvauriomikrobien otollisen elinympäristön laajentumisesta. Erilaiset kosteassa ympäristössä viihtyvät kosteusvauriomikrobit altistavat ihmisen hengitysilman erityisesti niiden aineenvaihduntaan liittyvillä tuotteilla, joissa voi esiintyä muita haitallisia aineyhdisteitä kuten viruksia ja mikrobeja. [106, s 14-15]

3. Hiilidioksidi

Hiilidioksidi on kaasumainen aineyhdiste, jota syntyy ihmisten uloshengityksen yhteydessä ja hiilidioksidi syrjäyttää hapen sisäilmassa. Ihminen tarvitsee puhdasta happea soluhengitykseen ja ihmisen soluhengityksessä syntyvä loppukaasu on hiilidioksidi. Hiilidioksidi sitoo hapen ilmasta, jolloin sisäilman hiilidioksidipitoisuus kasvaa mitä enemmän ihmisiä kyseisessä tilassa on. Hiilidioksidi sisäilman laatua mittaavana tekijänä on ollut olemassa jo kauan ja hiilidioksidin mittaaminen kuvastaa sisäilman happikatoa. Hiilidioksidin sisäilman laatua kuvaavana mittarina on määritelty myös rakennusmääräyskokoelmassa D2.

4. VOC-yhdisteet

VOC-yhdisteillä tarkoitetaan yleisesti haihtuvia orgaanisia yhdisteitä, joilla on katsottu olevan tutkimuksien mukaan yhteys sisäilmaston viihtyisyyteen, kuten hajuvaikutuksiin, ärsytysoireisiin ja sairasrakennusoireyhtymään. VOC-yhdisteiden vaikutuksesta sisäilmanlaatuun on kuitenkin kyseenalaista, koska VOC-yhdisteiden aiheuttamat ärsytykset ovat hyvin riippuvaisia yksilöllisistä eroista reagoida VOC-yhdisteisiin sekä monialtistumisreaktioiden vaikutusmahdollisuudesta. On kuitenkin pystytty tutkimuksin toteamaan, että niissä tiloissa ja rakennuksissa, joissa esiintyy epätavanomaisia VOC-lähteitä, kuten rakennusvirheistä johtuvat lähteet tai vialliset lattiamateriaalit tai vaha-aineet ovat vapauttaneet sisäilmaan ihmiselle ärsyttäviä yhdisteitä, jotka ovat lisänneet riskin ärsytysoireilulle. VOC-yhdisteitä kattavampi näkökohta on ottaa huomioon myös muut orgaaniset yhdisteet, joista käytetään sisäilmaston laatua kuvaavana lyhenteenä OCIA (organic componds in indoor air), joka kuvastaa kaikkia biologisesti merkityksellisiä ilmassa esiityviä aineyhdisteitä. Sisäilman OCIA-yhdisteitä tutkimalla on pystytty toteamaan, että kemiallisesti reaktiivisilla orgaanisilla yhdisteillä, kuten radikaaleilla ja ionisoiduilla yhdisteillä on yhteyttä sisäilman ärsytysoireisiin. Yksi keskeisimmistä orgaanisesta yhdisteestä, jolla on vaikutusta sisäilman laatuun, on nimeltään formaldehydi, joka on luokiteltu aineyhdisteenä ihmiselle karsinogeeniseksi. Formaldehydi imeytyy helposti limakalvoihin ja aiheuttaa silmän sidekalvojen ja ylätiehengitysteiden limakalvojen ärsytystä. Oireina on esimerkiksi jatkuva yskä, nenän tukkoisuus, nuha ja silmien kirvely. Muita oreita voi myös esiintyä, joista yleisinä oireina on huimaus, päänsärky, pahoinvointi ja väsymys. Myös

OCIA-yhdisteiden kohdalla yksilölliset erot voivat olla suuret. Liitteessä 6 on esitetty lisää tietoa VOC- ja OCIA-yhdisteiden taulukkoarvoista. [106, s. 23, 34-35]

5. Radon

Radon on yksi haitallisimmista ja vaarallisimmista sisäilmassa esiintyvistä kaasumaisista ainyhdisteistä. Radon on maaperän alaosissa luonnostaan esiintyvä kaasumainen aineyhdiste, joka syntyy uraanin hajoamisprosessin tuloksena. Vaaralliseksi radonin tekee sen säteilypitoisuus, joka syntyy uraaniatomin puoliintuessa, ja kaasumaisen aineyhdisteen hyvä imeytymiskyky esim. käyttövesivesiverkostoon. Radonin esiintyminen Suomessa on selkeästi voimakkaampaa suurten harjujen ja kallioiden läheisyydessä ja tietyillä alueilla Suomessa vaaditaan radon mittauksia maaperästä ennen rakentamista ja radonpoistoilmaverkostoa raja-arvojen ylittyessä. Myös rakennustekniikalla ja ilmastolla on merkitystä-Radonin esiintyvyyteen. Radon luokitellaan karsinogeeniseksi aineyhdisteeksi ja sen valvontaa ja mittauksia valvoo Suomessa säteilyturvakeskus. Suomessa radonin maksimipitoisuus uudisrakentamisen osalta ei saa ylittää 200 Bq/m³. Asuntojen keskimääräinen radonpitoisuus on Suomessa 96, Ruotsissa 108, Norjassa 106, Tanskassa 77, Saksassa 50, Ranskassa 66 ja Englannissa 20 Bq/m³. [108]

6. Muut keskeiset mitattavat kaasu- ja aineyhdisteet

Muita keskeisiä mitattavia kaasu- ja aineyhdisteitä Suomessa on erilaiset mikrobien aineenvaihdunnan aihettamat kaasumaiset aineyhdisteet, joista usein käytetään nimitystä MVOC-yhdisteet sekä erilaiset teolliset kuitumaiset aineyhdisteet. MVOC-yhdisteitä ilmenee erityisesti vanhemmissa ja vanhoissa rakenteissa sekä rakennuksissa, joissa on todettu kosteus- tai homeongelmia esim. rakennusvirheiden johdosta. Kuitumaisia aineyhdisteitä syntyy ja ilmenee usein uusien teollisesti valmistettujen rakennusaineiden, kuten kuitulevyjen yhteydessä. [106, s. 21, 27]

8.3 Teollisuuskiinteistöjen sisäilman laatuun liittyvät tekijät ja mittaaminen

8.3.1 HTP-arvot teollisuussa

Teollisuusympäristöjen eroavaisuuksia voidaan tarkastella HTP-arvoilla eli haitalliseksi tunnettujen pitoisuuksien raja-arvon perusteella. HTP-arvot kuvaavat teollisuuden raja-arvoja haitallisille pitoisuuksille. Esimerkiksi teollisuudessa leijuvan pölyn haitalliseksi tunnettu pitoisuus on orgaaniselle pölylle 5 mg/m^3 ja epäorgaaniselle pölylle 10 mg/m^3. Verrattuna rakennusmääräyskokoelman osaan D2 (2012) teollisuuden pölyhiukkas arvot ovat noin 500-1000 kertaa suurempia, mitä normaaleissa asuin- ja toimistotiloissa. [15, s. 62]

HTP-arvot ovat arvioita työntekijöiden hengitysilman epäpuhtauksien pienimmistä pitoisuuksista, jotka voivat aiheuttaa haittaa tai vaaraa työntekijöiden turvallisuudelle, terveydelle tai lisääntymisterveydelle. HTP-arvojen määrityksissä perusteena käytetään ihon, silmien ja hengitysteiden ärsyyntymistä sekä altistusaikaa, joka voi olla tapauskohtaisesti määritelty 8 tunnin, 15 minuutin tai hetkelliselle keskipitoisuudelle riippuen mitattavan aineen tai aineryhmän ominaisuuksista. Suomessa HTP-arvoja määrittävät biologiset altistusindikaattoreiden raja-arvot on vahvistettu työturvallisuuslain nojalla annetulla sosiaali ja terveysministeriön asetuksella. HTP-arvoja ilmaistaan yleensä massapitoisuuksina eli milligrammoina per kuutiometri (mg/m^3), mutta kaasujen ja höyryjen osalta on käytössä myös tilavuusosuuksien ilmaisutapa, tilavuuden miljoonasosa (ppm, parts per million), sekä joidenkin aineiden ilmaisutavassa, esim. kuitumaiset pölyt mm. sahanpurupöly, on käytetty ilmaisutapana kuitujen määrää per kuutiosenttimetri (kuitua/cm^3). Teollisuuden haitallisten aineiden mittaamisesta ja tunnistamisesta sekä riskien arvioinneista on annettu määräyksiä valtioneuvoston asetuksessa 715/2001 sekä ohjeita SFS/EN -standardeissa 689, 482 ja 1540. SFS/EN 689 standardi luo pohjan valtioneuvoston asetuksen noudattamiselle, jolla altistuksen arviointi voidaan toteuttaa. HTP-arvot ovat kuitenkin useimmissa tilanteissa puutteellisia suunnittelun kannalta, koska ne perustuvat hyväksyttävän riskin käsitteeseen, niitä uudistetaan tietyin aikavälein, ne määrittelevät mikä on sopimaton pitoisuustaso ottamatta huomioon hyvää ja viihtyisää ilman laatua sekä suomalaisilla teollisuudenaloilla aloilla vallitsevat pitoisuustasot ovat selkeästi HTP-arvojen alapuolella. [108]

HTP-arvoja parempi ja systemaattisempi keino hyvän puhtaan sisäilman laadulle on käyttää tavoitetasoja, jotka ovat dominoivan epäpuhtauden ennalta määrättyjä pitoisuustasoja, ja jotka on tarkoitus saavuttaa. Teollisuudessa HTP-arvojen tavoitetasojen määrittämiseen vaikuttaa yleisesti ilman laatutasolle määritetyt sitovat raja-arvot, kuten kattoarvoihin perustuvat kynnysarvot, tavoitearvot eri ilman laatutasojen perusteella ja benchmarking eri tehtaissa esitettyjen epäorgaanisen pölyn pitoisuuksista. Keskeistä teollisuudessa on huomioida myös fyysisen työn kuormittavuuden vaikutus HTP-arvojen osalta. Fyysisesti raskaampi työ vaikuttaa hengityksen voimakkuuteen, joka johtaa samalla suuremman määrän haitta-aine pitoisuuksien imeytymisen elimistöön, vaikka työympäristön epäpuhtauspitoisuudet eivät ylittäisi HTP-arvoja. HTP-arvot jakautuvat riskianarvion perusteella epäpuhtauksiin, joille on määritelty kynnysarvovaikutus ja epäpuhtauksiin, joille ei ole määritelty kynnysarvovaikutusta. Epäpuhtauden, joille on määritelty kynnysarvovaikutus, on jaettu niiden esittämistavan ja mittaustavan mukaisesti kahteen eri luokkaan. Epäpuhtaudet, joita esitetään ja mitataan NOEL annoksina ja epäpuhtaudet, joita esitetään ja mitataan turvallisuuskertoimien perusteella. Syöpävaarallisia aineita pidetään yleisesti haitallisina aineina, koska ne aiheuttavat vähäiselläkin altistuksella ainakin jossain määrin sairastumisen riskiä. Ne epäpuhtaudet, joille ei ole määritelty kynnysarvovaikutusta ovat annoksia, jonka alapuolelle jäljellä oleva riski on mitätön – vaikutuksien ilmaantumisen todennäköisyys on pieni – tai hatallisuuksien vaikutusta pidetään lievänä tai vaihtoehtoisesti vaikutukset rajoittuvat vain herkkiin – atoopikoihin ja erilaisia sairauksia poteviin - työntekijöihin. Usein riskinarviot matalilla epäpuhtaustasoilla ovat hyvin epätarkkoja ja näiden mitattavuuden toteuttamiskelpoisuutta tulee arvioida lähtökohtaisesti. [108]

8.3.2 VOC-arvot teollisuudessa

VOC-arvot perustuvat teollisuudessa myös HTP-arvojen luokitukseen, jossa työturvallisuuslain nojalla annetulla sosiaali ja terveysministeriön asetuksella otettava haitalliset pitoisuudet huomioon. Haitalliseksi tunnetut pitoisuudet VOC-yhdisteiden osalta on sosiali ja terveysministeriön tekemien arvioita työntekijöiden hengitysilman epäpuhtauksien

pienimmistä pitoisuuksista, jotka voivat aiheuttaa haittaa tai vaaraa työntekijöiden turvallisuudelle tai terveydelle taikka lisääntymisterveydelle. VOC-yhdisteiden taulukkoarvoja on esitetty liitteessä 6. [108]

8.3.3 Muut vaaralliset aineet ja aineyhdisteet teollisuudessa

Muita vaarallisia aineita on teollisuudessa, esimerkiksi taulukossa 4 esitetyt vaaralliset aineet joita on rikkivety (Hydrogen sulphide), rikkidioksidit (Sulphur Oxides SO2, SO3), kloori (Chlorine Cl2), typpioksidit (Nitrogen Oxides NOx), fluorivety (Hydrogen Fluoride HF), ammoniakki (Ammonia NH3) ja otsooni (Ozone O3). Vaaralliset aineyhdisteet määritellään eri kansallisissa standardeissa, kuten taulukossa 4 on noudatettu Ruotsalaista SSG ja yhdysvaltalaista ISA standardeja.

Taulukko 4. Vaarallisia aineyhdisteitä teollisuudessa [110]

Design outdoor temperatures	2009ASHRAE, Inc. WMO#022861
Winter outdoor Dry Bulb Temperature	-15,3 °C
Summer outdoor Dry Bulb Temperature (max annual)	+28,6 °C
Water content	13,4 gH_2O/kg d.a.
Enthalpy	54,0 kJ/kg
Mill environment classification according to SSG 3700-2 /2005 The reactive environment is classified according to ISA S71.04-1985 Instrument Society of America	M3/M2 Category GX (severe) pulp mill environment

Hydrogen sulphide	>50 ppb
Sulphur Oxides SO_2, SO_3	>300 ppb
Chlorine Cl_2	>10 ppb
Nitrogen Oxides NOx	>1250 ppb
Hydrogen Fluoride HF	>10 ppb
Ammonia NH_3	>25 000 ppb
Ozone O_3	>100 ppb

8.4 Sisäilman laatutekijöihin vaikuttaminen tarpeenmukaisen ilmanvaihdon avulla

Sisäilman laatutekijöitä, kuten lämpötila, suhteellinen kosteus, hiilidioksidi ja VOC-yhdisteitä on tutkittu aiemmin, kun on vertailtu tarpeenmukaisen- ja vakioilmanvaihdon toimintaa. Selkeä ero tarpeenmukaisen ilmanvaihdon ja jatkuvalla täysteholla toimivan ilmanvaihdon välillä on sisä- ja ulkoilman paine-eromuutoksista aiheutuva huojunta ja vetoriskin kasvaminen sekoittavaa ilmanvaihtoa toteuttavissa tiloissa. Sisäilman laatutekijät eivät välttämättä sinällään parane tarpeenmukaista ilmanvaihtoa toteuttavissa kohteissa, jos ilmanvaihtokanavistojen koot ja maksimi-ilmavirrat ovat suunniteltuja samalla periaatteella kuin normaalissa jatkuvalla täysteholla toimivassa ilmanvaihtojärjestelmässä. Keskeinen ero näiden eri järjestelmien välillä syntyy ohjausautomaatiosta ja energiankulutuksen optimoinnista. Valitettavan usein kuitenkin jatkuvalla täysteholla toimivat ilmanvaihtojärjestelmät sammutetaan käyttöajan ulkopuolella energiansäästösyihin vedoten, jolloin korvausilmaventtiilit ja erillispoistoilmanvaihto eivät yksistään riitä poistamaan rakennuksesta rakenteiden, rakennusmateriaalien, huonekalujen ja varastoiduista tuotteista aiheutuneita emissiopäästöjä. [111]

8.4.1 Sisäilman laatutekijöiden mittaaminen Swegon Wise-järjestelmän avulla

Swegon uuden sukupolven Wise-järjestelmässä sisäilman laatutekijöihin pyritään vaikuttamaan ilmanlaatua mittaavan anturin (WISE IAQ) säätötoimintojen avulla. Swegon myy ja markkinoi ilmanlaadun antureita erillisinä lisävarusteantureina tai tehdasasennettuina tuotteina valmiiksi integroituina huonetuotteisiin. [75]

Swegonin yritysvierailulla todettiin, että pelkkä hiilidioksidin mittaaminen on pelkästään riittämätön mittausperuste sisäilman laatua kuvaavana tekijänä. Perusteena tälle käytettiin Yhdysvaltain ydinsukellusveneiden hiilidioksidiraja-arvoja 5000–7000 ppm, kun Suomessa rakennusmääräyksissä on jo pitkään ollut 1200 ppm tavanomaisissa sääoloissa ja huonetilan käyttöaikana. [112; 113, s. 2.]

9 Mittauksien vaikutus järjestelmän ohjaukseen

9.1 Teoreettiset lähtökohdat

9.1.1 Ilman nopeus ja heittokuvioiden törmääminen

Kun päätelaitteiden otsapintanopeudet kasvavat hallitsemattomiksi, niin ongelmaksi tulee usein hallitsemattomat ilmasuihkujen heittokuviot, jolloin riski ilmasuihkujen törmäämisestä toisiin ilmasuihkuihin tai rakenteisiin kasvaa. Usein ilmasuihkujen törmääminen suurella nopeudella toiseen ilmasuihkuun tai rakenteeseen aiheuttaa vääristyneitä heittokuvioita, vedon tunnetta tilassa, kylmäsiltoja, operatiivisen lämpötilan laskemisen ja kosteusriskejä rakenteissa. Eri päätelaitteiden heittokuviomallinnusta on saatavilla lähes kaikilla toimittajilla, esimerkkina Haltonin Hit mallinnustyökalu. [111]

9.1.2 Vetokriteeri (Draft Rating)

Yhtälössä 1 on esitetty vetokriteerinä tunnetun lausekkeen, joka kuvaa prosentuaalisesti tyytymättömien osuuksia.

Yhtälö 1 $$DR = (0{,}37 * v * Tu + 3{,}14) * (34 - Ti) * (v - 0{,}05)^{0{,}62}$$ [15, s. 48]

Yhtälössä 1 merkinnät: DR = tyytymättömien osuus [%], Ti = ilmavirtauksen lämpötila, Tu = ilmavirtauksen turbulenssiaste (= nopeuden keskihajonnan suhde keskinopeuteen [%]), v = ilman keskinopeus [m/s]

Yhtälössä 2 on esitetty kuinka ilmavirtauksen turbulenssiasteen voi laskea.

Yhtälö 2 $$Tu = S/v$$ [15, s. 74]

Yhtälössä 2 merkinnät: Tu = ilmavirtauksen turbulenssiaste [%], v = ilman keskinopeus [m/s], S = nopeusvaihtelun keskihajonta [m/s].

9.1.3 Huonetilan CO_2-taseen avulla tuloilmavirran määrittäminen

Huonetilan CO_2-pitoisuus määritellään taseyhtälönä seuraavasti: huoneeseen tulevat epäpuhtausvirrat = huoneesta lähtevät epäpuhtausvirrat

Yhtälö 3 $$q_{tulo} * C_{tulo} + G_{CO_2} = q_{poisto} * C_{poisto}$$ [15, s. 101]

Yhtälö 4 $$q_{tulo} = \frac{G_{co_2}}{C_{poisto} - C_{tulo}}$$ [15, s. 101]

Yhtälöissä 3 ja 4 merkinnät: q_{tulo} = tuloilmavirta [m^3/s], G_{CO_2} = ihmisen tuottama hiilidioksidivirta (noin 24 l/h = 6,7 cm^3/s, kevyen työn aktiviteetilla 1,2 met), C_{poisto} = poiston hiilidioksidipitoisuus cm^3/m^3 (= ppm), C_{tulo} = tulon hiilidioksidipitoisuus cm^3/ m^3

Kun tiedetään, että mikä ilmanjako periaate on kyseessä, niin voidaan arvioida poistoilman hiilidioksidipitoisuutta sen mukaan. Jos esim. kyseessä täysin sekoittava ilmanjako ja tuloilman hiilidioksidipitoisuus ei laske ulkoilman keskimääräisestä hiilidioksidipitoisuudesta (C_{ulko} = 400 ppm), on poistoilman hiilidioksidipitoisuus sama kuin huoneilman hiilidioksidipitoisuus. Usein pyritään kuitenkin epäpuhtauksien kerrostumaperiaatteeseen, jolloin C_{poisto}- C_{tulo} on suurempi ja tällöin oleskeluvyöhykkeellä epäpuhtauksien osuus on pienempi mitä se on poistoilmassa. Tästä on esimerkki yhtälössä 5.

Yhtälö 5 $$q_{tulo} = \frac{G_{CO_2}}{C_{oleskelu} - C_{ulko}}$$ [15, s. 101]

Kun kaavaan 5 sijoitetaan ulkoilman keskimääräinen hiilidioksidipitoisuus ja toimistotilojen maksimihiilidioksidipitoisuus suositusarvoksi sisätiloissa (1200 ppm), saadaan tuloilmavirraksi yhtälön 6 mukaisesti.

Yhtälö 6 $$q_{tulo} = \frac{6{,}7\ cm^3/s}{1200\ (\frac{cm^3}{m^3}) - 400\ (\frac{cm^3}{m^3})} = 0{,}008375 \frac{m^3}{s} = 8{,}375\ l/s$$

9.1.4 Huonetilan VOC ja kemikaalitaseidella tuloilmavirran määrittäminen

VOC:a ja muita haitallisia sekä myrkyllisiä kemikaaleja ei usein esiinny suurissa määrin tuloilmassa. Jos halutaan päästä täysin varmuuteen asiasta, niin on syytä käydä paikan päällä suorittamassa mittauksia tai arvioitava, että onko, esim. teollisuustiloja lähettyvillä, joista VOC-päästöt tuloilmaan saattaisivat levitä. Yhtälössä 7 on esitetty VOC ja kemikaalitaseen perusteella tuloilmavirta.

Yhtälö 7 $$q_{tulo} = \frac{G}{C_{oleskelu}}$$ [15, s. 101]

Yhtälössä 7 merkinnät: q_{tulo} = tuloilmavirta [m^3/s], G = epäpuhtauslähteen tuottama epäpuhtausvirta, $C_{oleskelu}$ = tilan epäpuhtausmäärä cm^3/m^3 (= ppm)

9.1.5 Huonetilan kosteuskuormituksen perusteella tuloilmavirran määrittäminen

Yhtälö 8 $$q_{tulo} = \frac{q_h}{\rho_i(x_{poisto} - x_{tulo})}$$ [15, s. 106]

Yhtälössä 8 merkinnät: q_{tulo} = tuloilmavirta [m^3/s], ρ_i = ilman tiheys, x_i = ilman absoluuttinen kosteus [g_{H20}/kg_{ki}]

9.2 Määräyksiin perustuvat lähtökohdat

9.2.1 Veto

Ilmanvaihdon aiheuttaman ilman liikenopeus saa olla huoneen oleskelualueella suunnittelutilanteissa enintään taulukon 5 mukainen. Ilmanvaihdon tehostustilanteessa nopeus voi nousta 0,1 m/s taulukon arvoista, kun tehostus on suoraan käyttäjän säädettävissä ja 0,05 m/s, kun tehostus tapahtuu keskitetysti eikä ole käyttäjän suoraan säädettävissä. [114]

Taulukko 5. Vetokriteerit ilmannopeudelle [114]

Tilan kuvaus	Ilman suurin sallittu keskinopeus (+20 °C) [1)]	Ilman suurin sallittu keskinopeus jäähdytystilanteessa
Kevyt työ tai vastaava Kiinteät työpisteet, toimisto, kevyt liikunta, koululuokka, päiväkoti, aula, paikallan oleva seisomatyö, asuinhuoneet	0,2	0,30
Keskiraskas työ tai liike esim. käytävä, jossa ei oleskella ja/tai istuta	0,25	0,35

Raskas työ tai liike esim. urheiluhallit	0,30	0,40

1) Arvo ympäristöministeriön asetus uuden rakennuksen sisäilmastosta ja ilmavaihdosta.

Varmistusmittaukset tehdään standardin SFS-EN 12599 mukaisesti suuntariippumattomalla nopeusanturilla käyttäen nopeuden kolmen minuutin keskiarvoa, talvella ulkolämpötilan ollessa alle 0 °C, kesällä jäähdytystilanteessa, jos tuloilma on jäähdytetty. Mittauspisteet valitaan oleskeluvyöhykkeeltä siitä kohdasta, jossa on odotettavissa suurimmat virtausnopeudet tai joissa oleskelu on todennäköisesti pitkäaikaisinta. Mittauspisteiden valinnassa voidaan käyttää apuna merkkisavua. [114]

9.2.2 Ilman kosteus

Rakennusmääräyskokoelman osan D2:n (2012) mukaisesti:

> ”Sisäilman kosteus ei saa olla jatkuvasti haitallisen korkea eikä kosteus saa tiivistyä rakenteisiin eikä niiden pinnoille tai ilmanvaihtojärjestelmään siten, että se aiheuttaa kosteusvaurioita, mikrobien tai pieneliöiden kasvua tai muuta terveydellistä haittaa. Lisäksi sisäilman kosteus ylittää arvon7g H_2O/kg kuivaa ilmaa, kostutetaan huoneilmaa vain painavista syistä esimerkiksi prosessin tai varastoinnin niin vaatiessa. Arvo 7 g H2O/kg kuivaa ilmaa vastaa huoneilman tilaa, jossa suhteellinen kosteus on 45 %, kun huonelämpötila on 21 °C ja ilman paine on 101,3 kPa. Alhaisesta sisäilman suhteellisesta kosteudesta aiheutuvien haittojen vähentämiseksi vältetään lämmityskauden aikana tarpeettoman korkeita huonelämpötiloja.” [115, s. 6]

Lisäksi vuonna 2017 ilmestyneessä FINVAC:in oppaassa ilmanvaihdon mitoitukseen muissa kuin asuinrakennuksissa ohjeistetaan, että erityistiloissa kuten uimahalleissa ilmanvaihdon mitoitus tehdään kosteuden tuoton ja poiston perusteella. [114, s. 15]

9.2.3 Minimi-ilmavirta

Lähtökohtaisesti määräyksissä ohjeistetaan, että muiden kuin asuinrakennuksien ilmanvaihdon suunnittelussa ja rakentamisessa ilmanvaihtokertoimen tulee olla vähintään 0,2

1/h ja ulkoilmavirran vähintään 15 (dm³/s) /m² koko rakennuksen lattiapinta-alaa kohden tilassa, jonka vapaa korkeus on 2,5 m. [13, s. 18]

Lisäksi vanhassa rakennusmääräyskokoelman osan D2:n vuoden 2012 versiossa mainittiin minimi-ilmavirran osalta seuraavasti:

> ”Jos ilmanvaihto on asuntokohtaisesti ohjattavissa, voidaan ilmanvaihtojärjestelmä suunnitella ja rakentaa siten, että ilmavirtoja voidaan ohjata myös käyttöajan ilmavirtoja pienemmiksi. Kun asunnossa ei oleskella eikä käyttöajan ilmanvaihdolle ole tarvetta esimerkiksi kosteuden hallitsemiseksi, voidaan ilmanvaihdon ohjaus suunnitella siten, että asunnon ilmavirtaa voidaan pienentää enintään 60 % käyttöajan ilmavirrasta.”

Tämä sääntö koskee pääasiallisesti asuinhuoneistoja, eikä kyseistä ohjetta ole mainittu FINVAC:in oppaassa ilmanvaihdon mitoitukseen muissa kuin asuinrakennuksissa. [114; 115, s. 10]

9.2.4 Minimi- ja maksimilämpötilat

Huonelämpötilan lämmityskauden suunnitteluarvona on käytettävä lämpötilaa 21 °C. Huonelämpötilan hallinnan suunnittelussa huonelämpötila voi olla 20–25 °C lämmityskaudella ja 20–27 °C lämmityskauden ulkopuolella. Erityisestä syystä, kuten tilan erityisiä lämpötiloja edellyttävän toiminnan tai tilan erityisluonteen vuoksi, voidaan huonelämpötilan suunnitteluarvona ja huonelämpötilan hallinnan suunnittelussa käyttää näistä arvoista poikkeavia lämpötiloja. Rakennuksen huonelämpötilan on oltava suunniteltuna käyttöaikana viihtyisä, eivätkä ilman liike, lämpötilasäteily, lämpötilan vaihtelu, lämpötilaerot ja pintalämpötilat saa sitä heikentää. [13, s. 9]

9.3 Swegonin uuden sukupolven Wise-järjestelmän ohjaus

Swegonin mukaan Suomessa on ollut pitkään vallalla käsitys, jonka mukaisesti Suomessa sisäilman laadun tärkein kriteeri on hiilidioksidiin perustuva tulkintatapa. Swego-

nin tuotepäällikön mielestä tämä on väärä kriteeri, koska tutkimus osoittaa, että Yhdysvaltojen ydinsukellusveneissä on asetettu hiilidioksidirajaksi 5000 ppm, joka on yli seitsemän kertaa suurempi kuin Suomen rakentamismääräyskokoelman osan D2 määräys sisätilojen sallitusta hiilidioksidipitoisuudesta. Tästä syystä Swegon on halunnut tuoda markkinoille myös vaihtoehdon sisäilman laadun jatkuvaan seurantaan ja ylläpitämiseen, joka perustuu TVOC-pitoisuuksien mittaamiseen ja säätöön. Swegonin uuden sukupolven Wise-järjestelmässä sisäilman laadun ja lämpötilan mittaaminen ja säätö koostuu seuraavista anturivaihtoehdoista:

1. Erilliset huone-/vyöhykeanturit
    a. Ilman suhteellinen kosteus ja hiilidioksidi (Wise IAQ CO_2)
    b. Ilman suhteellinen kosteus ja TVOC (Wise IAQ VOC)
    c. Ilman suhteellinen kosteus, hiilidioksidi ja TVOC (Wise IAQ Multi)
    d. Ilman suhteellinen kosteus, lämpötila ja läsnäolo (Wise OCS)
    e. Lämpötila (Wise IRT, RTA & RTS)
2. Päätelaitteisiin tehdasasennetut anturit
    a. Wise Parasol EX + ilmanlaatuanturi Wise SMA (lämpötila, RH, TVOC)
    b. Wise Parasol EX + läsnäolo- ja lämpötila-anturi Wise SMB
3. Ohjaus- ja säätöpelteihin tehdasasennetut anturit
    a. Wise Damper + Wise IAQ

9.3.1 CO_2-pitoisuuksien vaikutus ohjaukseen

Hiilidioksidipitoisuuksien perusteella tapahtuva ohjaus voi perustua Wise-järjestelmässä yhdeltä tai useammalta huone- tai vyöhykeanturilta saatavaan ohjausviestiin, joka voi langattomassa IoT-verkossa perustua samalla tapaa esim. 0–10 V virtaviestiin kuin langallisessa kenttäväyläverkossa. Useamman huone- tai vyöhykeanturin tapauksessa säätö voidaan suorittaa huone- tai vyöhykelaitteita palvelevien antureiden minimi-, keski- tai maksimi mittausarvon perusteella. Swegon IAQ-anturin hiilidioksidipitoisuuden mittausalue on välillä 400–2000 ppm, joka yksinkertaisesti tarkoittaa, että anturin toimiessa tilassa tai vyöhykkeellä, jossa on muita tarpeenmukaiseen ilmanvaihtoon ja ilmanlaadun mittaamiseen tarkoitettuja antureita, hiilidioksidianturille on voitu antaa isäntä- tai orjalaitteen luokitus. Esim. Wise-järjestelmässä ilmanlaatua mittaavat anturit ja ilmanvaihtokoneen ilmamäärän säätö toimivat usein orjalaitteena on/off-tyyppisille läsnäolotunnistimille sekä ikkuna- ja ovikoskettimille. [18; 75]

9.3.2 VOC-pitoisuuksien vaikutus ohjaukseen

Uuden sukupolven Wise-järjestelmässä VOC-yhdisteiden mittaus perustuu VOC-yhdisteiden yhteismittausarvoon eli TVOC-arvoon. Mittausalueena TVOC-arvoille on WISE IAQ-anturissa 450 – 2000 ppm. Samalla tapaa kuin hiilidioksidin avulla tehtävässä ilmamääräsäädössä niin myös TVOC-mittauksien tapauksessa useamman huone- tai vyöhykeanturin tapauksessa säätö voidaan suorittaa huone- tai vyöhykelaitteita palvelevien antureiden minimi-, keski- tai maksimi mittausarvon perusteella. Erona hiilidioksidimittauksiin on, että TVOC-pitoisuuksien mittaustulokset voivat muuttua hyvin radikaalisti esim. avatessa ikkunan- tai oven likaiseen tilaan. Tästä oli esimerkkinä Swegonin Kirkkonummen testauslaboratoriossa käytetty testauslaitteisto, joka reagoi nopeasti savukoneen aiheuttamaan TVOC-pitoisuuksien muutokseen Gold-ilmanvaihtokoneen ilmavirtojen säädöllä samoin kuin ikkunakoskettimen avautuessa järjestelmä pyrkii tasapainottamaan ilmavirtoja. Energiansäästösyistä esim. yötuuletuksen tai nopean savunpoisto-/ikkunatuuletuksen aikana järjestelmä kannattaa olla poissaolotilassa tai erillisellä kytkimellä sammutettu, jolloin järjestelmä ei pyri turhaan säätämään ilmavirtoja kyseisessä tilassa. [18; 75; 112]

9.3.3 Läsnäolon vaikutus ohjaukseen

Uuden sukupolven Wise-järjestelmässä läsnäolon tunnistus vaikuttaa järjestelmän ohjaukseen merkittävästi. Uuden sukupolven Wise-järjestelmässä esim. passiivisen infrapunatunnistusanturin avulla järjestelmä muuttaa tilaa läsnäolo- ja poissaoloasetuksien välillä on/off säätöön perustuen. Läsnäoloasetuksiin kuuluu muun muassa huoneen tai vyöhykkeen lämpötilan, ilmanlaadun ja ilmankosteuden sekä valaistuksen ohjaus. Poissaolotilassa järjestelmä sallii käyttötila-asetuksiin perustuen alhaisemman lämpötilan sekä suuremmat arvot ilmanlaadun ja ilmankosteuden osalta. Läsnäolon tunnistus ja eri käyttötilanteet ovat uuden sukupolven Wise-järjestelmässä suurin yksittäinen infrapunaanturin automaattiseen tunnistukseen ja säätöön perustuva energiansäästöjä edesauttava anturi. [75]

9.3.4 Lämpötilan vaikutus ohjaukseen

Lämpötilan ohjaus uuden sukupolven Wise-järjestelmässä perustuu järjestelmän mittausalueen ja lämpötila-asetusten säätöön. Selkeänä erona moniin muihin tarpeenmukaiseen ilmanvaihtojärjestelmään on, että järjestelmä säätää lämpötilaa automaattisesti vain tiettyyn asetusarvoon perustuen ja näin ollen järjestelmä ei sisällä huonekohtaisia säädinlaitteita vaan säätö tehdään esim. kännykkäsovelluksen avulla. Lämpötilan mittausalueena järjestelmässä on 0–50 °C ja virhemarginaalina ± 0,5 °C. Järjestelmän käyttöönoton yhteydessä järjestelmälle määritetään lämpötilan sallittu vaihtelualue sekä läsnäolo, että poissaolotilojen osalta. Lämpötila-anturi on siten suorassa yhteydessä käyttötilanneohjauksiin, kuten läsnäolo, poissaolo, aamulämmitys ja kesäyöjäähdytys. Uuden sukupolven Wise-järjestelmässä voi valita kolme erillistä lämpötilan anturia, joista Wise IRT sisältää sekä passiivisen läsnäoloanturin että lämpötila-anturin. Toimisto- ja asuinrakennuksissa hyvän sisäilman edellytyksiin kuuluu noudattaa eri sisäilmaluokkien ja määräysten mukaisia sisäilman laatukriteereitä myös lämpötilan osalta. [75]

9.3.5 Kosteuspitoisuuksien vaikutus ohjaukseen

Uuden sukupolven Wise-järjestelmässä kosteusmittauksen mittausalueeksi on asetettu kaksi raja-arvoa virhemarginaaleineen, joista ensimmäinen eli RH% 20-80, ± 3% kuvastaa tarkempaa ja sallitulla vaihteluvälillä olevaa rajaa sekä toinen raja-arvo RH% 0 – 100, ± 5%, kuvastaa ei suositeltavaa raja-arvoa, koska yli 80 % suhteellinen ilmankosteus alkaa jo tiivistyä rakenteisiin ja riski rakenteiden altistumisesta homebakteereille kasvaa. Samalla tapaa kuin lämpötilan osalta niin myös kosteuspitoisuus pyritään järjestelmän avulla pitämään läsnäolotilanteessa hyvien sisäilmastoluokituksien mukaisina ja muissa kuin läsnäolotilanteessa voidaan salli hieman poikkeuksia. Wise-järjestelmässä kosteus on todettu merkittäväksi sisäilmastolliseksi tekijäksi ja siksi ilman suhteellisen kosteuden mittaaminen on osana kaikissa lämpötila ja sisäilman laatuantureissa. [18; 75]

9.3.6 Ympäristön kemikaalien vaikutus ohjaukseen

Uuden sukupolven Wise-järjestelmässä ei ole mukana erillisiä ympäristön kemikaalien mittausantureita, kuten teollisuudessa käytettäviä ja hyväksyttyjä vaarallisten aineyhdisteiden kemikaaliantureita. Wise-järjestelmään voidaan kuitenkin liittää mukaan Wise IORE tai Wise IRE -anturit, jotka toimivat järjestelmän yhdyskäytävinä järjestelmään liitettäville ulkopuolisille antureille. Erityisesti valvomotiloissa, jotka usein toimivat teollisuudessa samalla myös vaarallisilta aineyhdisteiltä suojautumistilana, kuten ruotsalaisessa SSG standardissa on mainittu. Tällöin erilaisia prosessille tyypillisiä, tehtaan-, EN- sekä SSG standardien mukaisia kaasutunnistusantureita olisi syytä liittää mukaan järjestelmään näiden valvomotilojen osalta. [75]

9.3.7 Eri käyttötilanteiden vaikutus ohjaukseen

Uuden sukupolven Wise-järjestelmä eri käyttötilanteille on olemassa omat ohjaustavat, joiden perusteella järjestelmä pyrkii reagoimaan eri tilanteisiin tiettyjen ennalta määritel-

tyjen asetusarvojen mukaisesti. Eri käyttötilanteiden avulla järjestelmä pyrkii energiansäästöön, sisäilman laatutekijöiden parantamista ja nopeuttamaan eri käyttötilanteista siirtymistä. Eri käyttötilanteita uuden sukupolven Wise-järjestelmässä on läsnäolo, poissa, sisäänkirjautunut, säätö, loma, aamulämmitys ja kesäyöjäähdytys. Läsnäolo- ja poissaolon käyttötilat järjestelmä tunnistaa läsnäolotunnistimen avulla. Sisäänkirjautumistila on Wise-järjestelmässä määritelty ulkoisena signaalina rakennusautomaatiojärjestelmästä esim. tilavarausjärjestelmän kautta tai sisäänkirjautumistila on aktivoitu Super Wise -ohjausyksiköstä. Sisäänkirjautumistila muistuttaa ohjaukseltaan läsnäolotilaa, mutta erona on se, että tila ei vaadi läsnäoloa kytkeytyäkseen päälle vaan esim. voi olla yhteydessä tilavarausjärjestelmään rakennusautomaation kautta ja huoneen käytön mukainen kalenterivaraus toimii ohjauskäskynä ilmastoinnin tehostukseen. Sisäänkirjautumistila ohjaa Wise-järjestelmässä ilmavirran tehostustoimintoa, minkä tarkoituksena on valmistella kyseinen tila läsnäolotilaa varten ja sisäänkirjautumistilan kestoa ja ilmavirtojen tehostustoimintoa voidaan ohjelmoida Super Wise -yksikköön kirjautumalla. Myös muiden tilatietojen kuten loma, aamulämmitys ja kesäyöjäähdytys Wise-järjestelmä pyrkii lukemaan rakennusautomaatiojärjestelmästä tai erillisestä kalenterijärjestelmästä. Erillisen säätötilan käyttäjä tai usein järjestelmän käyttöönottaja käyttöönoton yhteydessä määritelee Super Wise rajapinnassa eri ilmavirrat ja Wise-järjestelmä pyrkii säätötilan avulla varmistamaan oikeat ilmavirrat ja säätää tarvittaessa ilmavirtoja eri tilakokonaisuuksissa. [75]

9.3.8 Eri käyttötoimintojen vaikutus ohjaukseen

Uuden sukupolven Wise-järjestelmässä on mahdollista 10 eri käyttötoimintoon, joilla on vaikutusta edellä esitettyihin eri käyttötiloihin, energiansäästöön ja ennen kaikkea tarpeenmukaiseen ja parempilaatuiseen sisäilmaan. Eri käyttötoiminnot ja niiden vaikutus Wise-järjestelmässä ovat seuraavanlaisia:

1. Ilmavirtatasapaino

    - Tasapainottaa huoneiden ilmavirrat ali- ja ylipaineiden osalta

2. Valaistusohjaus huoneessa

    - Valojen sytytys valokatkaisimella, Wise-järjestelmän läsnäoloanturilla tai ryhmäsignaalilla Super Wisen tai rakennusautomaatiojärjestelmän kautta

3. Ikkunavedon esto

    - Wise-järjestelmään liitettyjen radiaattoreiden vetosuojaus, joka huolehtii jäähdytettyjen tilojen samanaikaisesta lämmityksestä ehkäisten ikkuna-veto-ongelmat

4. Jäätymissuoja

    - Huoneen vesikiertoisten tuotteiden suojaaminen jäätymiseltä automaattisen lämmitysventtiilin avaamisella

5. Avoin ikkuna

    - Ikkunakosketin lähettää signaalin ikkunan avaamisesta ilmavirtojen- ja vesikiertoisien tuotteiden lämminvesivirtauksien säätämiseksi

6. Puhallinkonvektorin ohjaus

    - Puhallinkonvektorin kahden rinnakkaisen järjestelmän (vesi- ja ilma) yhtaikaisen ohjauksen mahdollistaminen puhallinnopeuden säädön suhteella vesiventtiilin asentoon

7. Lattialämmitys

    - Järjestelmään liitetyn lattialämmitystermostaatin avulla toiminto pitää yllä haluttua lattia- ja huonelämpötilaa

8. Ilmatehostus

- Pakotetun ilmavirran avulla saadaan aikaan nopea huonetuuletus hyvän sisäilmaston mahdollistamiseksi

9. Kondenssi

- Järjestelmän jäähdytysmenoputkien kondensoitumisriskille oleva toiminto sulkee jäähdytysventtiilin välittömästi ja samalla säätää ilmavirran minimi- tai maksimiarvoon riippuen järjestelmän käyttöönoton yhteydessä tehdystä järjestelmäkonfiguroinnista

10. Kanavalämmitin/jäähdytin

- Kanavalämmitys/jäähdytystoiminnolla ilma lämmitetään tai jäähdytetään huone- tai vyöhyketasolla, kun eri huoneilla on erilaiset lämpötilatarpeet muuhun rakennukseen verrattuna tai ihmisistä johtuvat lämpötilakuorma ovat erilaisia eri tiloissa. [75]

Uuden sukupolven Wise-järjestelmässä edellä esitettyjen toimintojen oikeaan ja energiatehokkaaseen toimintaan vaikuttaa hyvin paljon myös asennuksien yhteydessä tehtävä järjestelmän käyttöönottoon liittyvä järjestelmäkonfigurointi. Swegonilla Wise-järjestelmän konfigurointiprosessia on pyritty saamaan virheettömäksi, mutta täysin virheettömäksi sitä ei ole saatu ja siksi komissioinnin yhteydessä erityisesti eri käyttötilojen ja niihin liittyvien käyttötoimintojen läpikäynti virheettömyyden varmistamiseksi on suotavaa. [29]

10 Järjestelmän energiasäästöjen ja kokonaiskustannuksien arviointi

Tässä insinöörityössä ei ollut käytössä valmiita elinkaari- tai kokonaiskustannuslaskelmia liittyen uuden sukupolven Wise-järjestelmään tai saati valmista kustannusarviota järjestelmän toteutukseen liittyen. Koska uuden sukupolven Wise-järjestelmä on verrattain vielä uusi järjestelmä, niin tämän takia tarkkoja elinkaarikustannuksia on mahdotonta arvioida historiatietoon perustuen. Tästä johtuen seuraavassa esitetään vertauksia aiempien opinnäytetöihin perustuen järjestelmään liittyvistä tutkimuksista sekä erityisesti asennus- ja energiakustannusten säästövaikutuksia.

10.1 Tarpeenmukaisen ilmanvaihdon energiansäästö- ja kannattavuusvaikutukset yleisesti

Automaation energiatehokkuus standardin SFS-EN 15232 mukaisesti tarpeenmukaisessa ilmanvaihdossa käytetyt puhaltimet, jotka ovat tarpeenmukaisesti ohjattuja, kuuluvat parhaaseen A luokkaan. Vastaavasti pelkällä läsnäolo-ohjauksella ohjatut puhaltimet kuuluvat luokkaan B, aikaohjauksella (kellokytkin) luokkaan C ja ei automaattisella ohjauksella luokkaan D. Yksinkertaisimmillaan tarpeenmukainen ilmanvaihto voidaan toteuttaa vyöhykesäädöllä ja tilakohtaisesti on/off-säädöllä toteutettava ratkaisu, joka on helpompi huoltaa ja silti toiminnaltaan tehokas vakaamman ja nopeammin muutoksiin reagoivien kaksiasento peltien avulla. [9]

Tarpeenmukaisen ilmanvaihdon energiansäästö- ja kannattavuusvaikutuksia tulee jokaisessa suunnittelukohteessa arvioida erikseen, koska rakennuksien käyttö voi olla erilaista, vaikka rakennus olisi samantyyppinen. Aiempien tutkimuksien ja selvityksien perusteella tarpeenmukaisen järjestelmän energiankulutuksen säästöistä noin puolet johtui siitä, että järjestelmää voidaan käyttää osateholla käyttöajan ulkopuolella. Tarpeenmukaisen järjestelmän eri antureilta saatavien pitoisuusmittausten perusteella voidaan historiatietoon perustuen tehdä analyyseja eri tilojen ilmamäärien tarpeesta eri tiloissa ja

tilojen ilmamääriä muuttamalla saada aikaan lisää energiasäästötoimenpiteitä, kuten myös ultraääni-ilmavirtasäätimien avulla. Tarpeenmukaisen ilmanvaihdon energiasäästöjä syntyy erityisesti ilmanvaihtoilman ja huoneilman lämmittämisestä (Tilojen ja IV-koneiden lämmitysenergian kokonaissäästö) sekä puhaltimien sähkönkulutuksesta (Puhallinsähkö) pienemmillä kokonaisilmavirroilla. Esimerkiksi aiemman opinnäytetyötutkimuksen mukaan vakioilmavirtaisen lämmitysenergiankulutukseltaan noin 100 MWh:n ilmanvaihtojärjestelmän karkeastiarvioitu vuosisäästö on noin 4000 € tarpeenmukaisella ilmanvaihtojärjestelmällä toteutettuna ja takaisinmaksuajaksi arvioituna 16 vuotta. [116]

10.2 Wise-järjestelmän energiansäästöjen ja kannattavuuden arviointi

Uuden sukupolven Wise-järjestelmässä energiansäästö ja kannattavuustekijöiden arvioinnissa tulee ottaa huomioon seuraavia keskeisiä tekijöitä, jotka ovat:

- Langattoman ohjausjärjestelmän etuja ovat joustavuus, ohjausmahdollisuudet, muokkaamisen ja laajentamisen helppous sekä merkittävät säästöt asennuskustannuksissa erityisesti järjestelmän nopean ja sujuvan käyttöönoton osalta
- Yksinkertaistetut kaapeliyhteydet järjestelmän tiedonsiirtoyksiköiden (Wise DIR & Super Wise) ja IV-koneen PCI-keskusyksikön välillä
- Eri antureiden huoltokustannuksiin vaikuttava vaihtoväli (esim. Wise IAQ)
- Toimiston layoutin kustannustehokas muutos järjestelmän osalta langattomilla antureillaan
- Alentuneet energiakustannukset tarpeenmukaisen puhallin ohjauksen ansiosta
- Ilmanvaihtokoneen EC-moottoriin liittyvien energiakustannusten paraneminen verrattuna taajuusmuuttajalla ohjattuun AC-moottoriin tehokkaamman säädön ansiosta

- EC-moottorin elinkaari voi koitua lyhyeksi ja kalliiksi johtuen ei-huollettavasta rakenteesta

- Epäsuorien kustannuksien vaikutus kokonaiselinkaarikustannuksiin esim. toimiston tuottavuuden paraneminen ja sairaspoissaolojen väheneminen

- Huoltokustannusten väheneminen ja etänä mahdollistuva huolto, mutta samalla myös huollon monimutkaistuminen liittyen järjestelmän langattomiin IoT-anturei-hin

- Kiinteistöautomaatiojärjestelmien tehostaminen Wise-järjestelmällä liitettäessä ohjaukset valaistuksen-, lämmityksen-, jäähdytyksen- ja ilmanvaihdon osalta saman Super Wise yksikön alle

- Ultraääniantureilla toimivien säätöpeltien mahdollinen liittäminen (WISE IORE) osaksi järjestelmää tehokkaamman säädön mahdollistamiseksi myös pölyisissä kanavissa vaikuttaen pitkällä tähtäimellä energia- ja huoltokustannuksiin

- Yhteen ja samaan järjestelmätoimittajaan liittyvä riski kustannusten noususta.

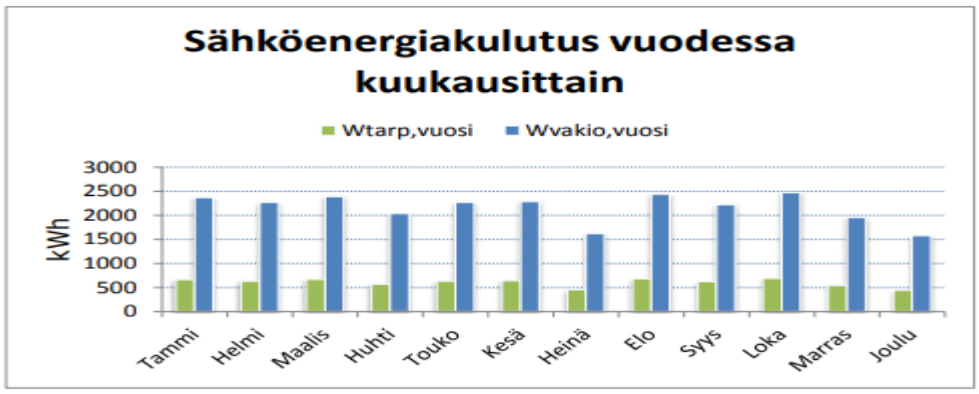
10.2.1 Swegon vanhan sukupolven Wise-järjestelmään liittyvä energiansäästövertailu

Tässä insinöörityössä ei ollut saatavilla Swegonilta tai muista tutkimuksista tai opinnäytetöissä tutkittua ajantaisaista tietoa uuden sukupolven Wise-järjestelmän energiasäästöjen osalta. Seuraavassa esitetään vertailunäkökulmana kahdessa insinöörityötutkimuksessa tehtyjä energiansäästövertailuja, joissa vertaillaan vanhan sukupolven Wise-järjestelmän tarpeenmukaista ilmanvaihtojärjestelmää vakioilmavirtaisen ilmanvaihtojärjestelmän energiakulutukseen. Ensimmäinen insinöörityötutkimus on tehty vuonna 2013 Vaasan ammattioppilaitokselle ja toinen vuonna 2017 tehty insinöritutkimus Keltimäen päiväkotikiinteistöön Jyväskylässä. Erityisesti vuonna 2017 tehtyä insinöörityötutkimusta

voidaan pitää lähimpänä vertailunäkökohtana arvioitaessa uuden sukupolven Wise-järjestelmästä saatuja energiasäästöjä.

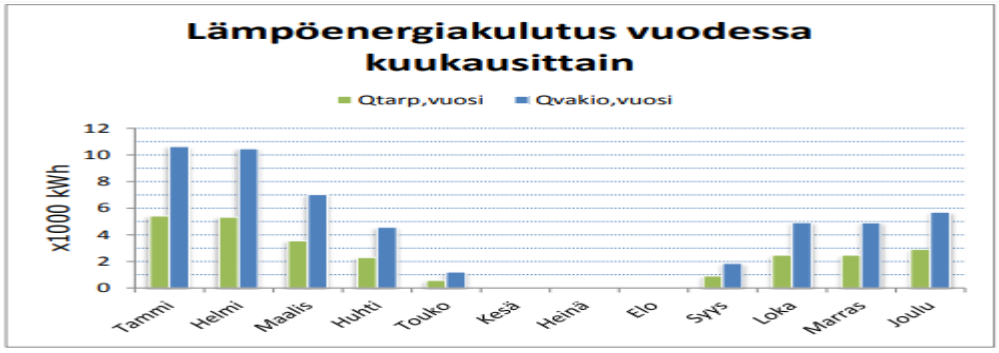
10.2.1.1 Vuoden 2013 insinööritutkimus vanhan sukupolven Wise-järjestelmästä

Swegon Wise-järjestelmä on tunnettu jo aiemman sukupolven aikana, jolloin käytössä ei ollut vielä langattomia antureita, energiaa säästävästä tarpeenmukaisesta ilmanvaihtojärjestelmästään. Swegon Wise-järjestelmä energiansäästö syntyy sekä sähköenergian että lämmitysenergian säätöistä. Vanhan Swegon Wise-järjestelmän laskennallinen vuosittainen sähköenergian säästö oli 72,1 % verrattuna vakioilmavirtaiseen järjestelmään. Kyseinen tutkimus tehtiin Vaasan ammattioppilaitoksella vuonna 2013 kahden luokkatilan, joissa oli Swegon Wise vanhemman sukupolven tarpeenmukainen ilmanvaihtojärjestelmä ja vertauskohteena oli erillisten luokkatilojen vakioilmavirtainen ilmanvaihtojärjestelmä. Kuvassa 45 on esitetty ilmanvaihtokoneiden sähköenergiankulutus suhteutettuna mittauspäivien lukumäärään. [117]



Kuva 45. Ilmanvaihtokoneiden vuosittainen sähköenergiankulutus [117]

Jälkilämmityspatterin energiankulutus oli Vaasan ammattioppilaitoksella tehdyn tutkimuksen mukaan 38,7 % vähemmän vakioilmavirtaiseen ilmanvaihtoon verrattuna, kun huomioituna oli puhaltimen aiheuttama tuloilman lämpötilakorotus. Ilman huomattavaa lämpötilankorotusta tarpeenmukainen ilmanvaihto kulutti 46,8 % vähemmän lämmitysenergiaa vakioilmavirtaiseen verrattuna. Vuositasolla jälkilämmityspatterin vuosisäästö oli 49,4 %, kun laskelmissa käytettiin ilmanvaihtokoneiden näennäisiä käyntiaikoja, johtuen ilmanvaihtokoneiden pitkistä käyntiajoista. Lämmitysenergian säästöä varten tutkimuksessa laskettiin vuosihyötysuhteet ulkolämpötilan pysyvyystaulukon ja lämpötilahyötysuhteen avulla. Kuvassa 46 on esitetty tarpeenmukaisen ja vakioilmavirralla toimivien ilmanvaihtokoneiden jälkilämmityspatterin vuosittainen energiankulutus eri kuukausina. [117]



Kuva 46. Jälkilämmityspatterin vuosittainen lämpöenergiankulutus [117]

10.2.1.2 Vuoden 2017 insinöörityötutkimus vanhan sukupolven Wise-järjestelmästä

Vuonna 2017 tehty insinöörityötutkimus tehtiin Keltinmäen päiväkotikiinteistöön, jossa verrattiin tarpeenmukaisen vanhan sukupolven Wise-järjestelmän ja vakioilmavirtaisen ilmanvaihtojärjestelmän lämmitys- ja sähköenergian säästöjä kyseisen rakennuksen käyttäjäprofiiliin perustuen. Lisäksi tarpeenmukaista ilmanvaihdon ohjaus oli toteutettu läsnäolo- ja VOC-antureiden avulla. Tutkimus perustui uudiskohteeseen ja rakennuksen lämmitys- ja sähköenergian kulutusta tutkittiin IDA ICE simulointiohjelman avulla, jossa

jokaisesta tutkittavasta huoneesta tehtiin tarpeenmukaista ilmanvaihtoa ja vakioilmanvaihtoa simuloivat mallit sekä kaikkien huoneiden osalta tehtiin myös yhteinen simulointimalli. [3]

Tutkimustulosten perusteella todettiin, että yksittäisen huoneen ilmanvaihtokoneen lämmitysenergiassa voidaan säästää jopa 51% ja puhaltimien sähköenergiassa jopa 82 %. Lisäksi kaikkien huoneiden perusteella tehdyn yhteisen simulointimallin perusteella tarpeenmukaisen ilmanvaihtokoneen lämmitysenergiassa voidaan säästää 43 % ja puhaltimien sähköenergiassa 77 %. Tutkimustulokset olivat hyvin linjassa vuonna 2013 tehtyjen tutkimuksen tuloksien kanssa. Lisäksi tutkimuksessa tutkittiin ilmanvaihdon jäähdytyksen vaikutusta lämmitysenergian säästöön, joka vaikutti huomattavasti lämmitysenergiansäästöön, jopa 76 %-yksikön kasvulla aiempaan lämmitysenergiansäästöön. Tutkimustuloksien kerrottiin olevan samassa linjassa myös Swegonin omien tutkimustuloksien kanssa. [3]

10.2.2 Lämmityksen ja valaistuksen ohjausjärjestelmien integrointi ja vaikutus energiansäästöön ja kustannuksiin

Huomattavia energiasäästöjä haettaessa tulee myös eri talotekniikkajärjestelmien sujuva yhteen liittäminen oltava kunnossa. Swegon Wise-järjestelmän Super Wise yksikköön liitettävissä olevat lämmityksen ja valaistuksen ohjausjärjestelmät ovat suositeltavaa liittää yhteen, koska tällöin mahdollistetaan eri järjestelmien sujuva tarpeen mukainen käyttö. Swegon Wise-järjestelmään ei kuulu erillisiä älykkäitä valaistuksenohjausjärjestelmiä, kuten Dali, mutta järjestelmän Super Wise keskusyksikköön on liitettävissä erillisiä valaistuksenohjaus ja lämmityksenohjausjärjestelmiä, koska Wise-järjestelmässä on omat ohjaustoiminnot näitä varten.

Valaistusohjauksen elinkaarikustannushyödyt tulevat esiin erityisesti suuremmissa rakennuskokonaisuuksissa, koska tällöin pyritään usein valaistuksenohjaus toteuttamaan

rakennusautomaatiojärjestelmästä erillisellä valaistuksenohjausjärjestelmällä. Valaistuksen ohjauksen energiatehokkuuteen, kuten myös ilmanvaihdon energiatehokkuuteen, vaikuttaa merkittävästi automaatiostandardin SFS-EN 15232 mukainen luokittelu, jossa läsnäolon automaattinen tunnistus, esim. PIR-anturein, kuuluu luokkaan A eli parhaaseen energiatehokkuusluokkaan. Swegon Wise-järjestelmään liitetystä valaistuksenohjauksesta tehtyjä energialaskentasäästötutkimuksia ei ollut tätä insinöörityötä tehdessä saatavilla, mutta myös valaistuksen osalta langattoman ohjausjärjestelmän etuja ovat joustavuus, ohjausmahdollisuudet, muokkaamisen ja laajentamisen helppous sekä merkittävät säästöt asennuskustannuksissa. Valaistusohjauksella on mahdollista saavuttaa myös valovirran aleneman kompensoitumisesta saavutettava 10-25 prosentin säästö ja tällöin valonlähteen valovirranalenemasta johtuva ylimitoitus on kompensoitavissa vakiovalo-ohjauksella tai älykkäällä vakiovalotoiminnolla varustetulla virtalähteellä. [118]

Lämmityksen ohjausjärjestelmien integrointi on myös mahdollista Super Wise-keskusyksikköön erillisten lattialämmitystermostaattien ja patteritermostaattien osalta. Markkinoille on tullut hyvin paljon erilaisia älykkäitä lattialämmitystermostaatteja ja patterilämmitystermostaatteja, kuten Danfoss Living Eco, joiden liittäminen Swegon Super Wise-keskusyksikköön on mahdollista ja niiden ohjaus tapahtuu Wise-järjestelmän lattialämmitystoiminnolla. Swegon Wise-järjestelmään liitetystä lämmityksenohjauksesta tehtyjä energialaskentasäästötutkimuksia ei ollut tätä insinöörityötä tehdessä saatavilla, mutta yleisesti lämmityksen tarpeenmukaisuutta on tutkittu esimerkiksi Tampereen yliopiston rakennusfysikaalisessa tutkimuksessa, jossa tutkittiin kesämökkien kuivanapitolämmityksen riittävyyttä, joka on selkeä energiakustannuksiin vaikuttava ja lämmityksen tarpeenmukaisuutta edistävä tutkimus. [119]

10.2.3 Kokonaiskustannusten arviointi

Seuraavassa esitetyt kokonaiskustannuksen arviointi perustuu vuonna 2013 Metropolian Myyrmäen yksikköön tehdyn ilmanvaihdon modernisaatiota käsittelevään insinöörityö-

hön, joka perustui Swegonin vanhan sukupolven Wise-järjestelmän avulla tehtyyn pilottihankkeeseen kahteen eri luokkatilaan. Kyseisessä tutkimuksessa todettiin, että Wise-järjestelmän kustannukset osoittautuivat paljon pienemmiksi kuin vastaava toteutettuna vakioilmanvaihdolla, jossa ilmanvaihdon eri osat tulevat eri toimijoilta ja kokonaisuutta hallitaan kiinteistöautomaatiosta. Lisäksi todettiin, että pakettiratkaisu on mahdollista toteuttaa melko yksinkertaisesti esim. saneerauskohteeseen, koska se voidaan liittää osaksi vanhaa järjestelmää ja sen asennus on yksinkertaista. [120]

Tehdyssä insinöörityötutkimuksessa esitetyt kustannusarviot jakautuivat seuraavasti:

- Ilmanvaihtokoneen EC-moottorin hankintakustannus arvio 3000 – 4000 € (ei sisällä asennus- ja hankintakustannuksia)

- EC-moottoriohjausta varten tarvittavat uudet mittaukset antureiden osalta n. 1000 €

- Kiinteistöautomaatiojärjestelmän modernisointikustannukset (ilmanvaihdon muutokset vaativat myös kiinteistöautomaatiojärjestelmän modernisointia) n. 3000 € + työt pitäen sisällään:

    - CPU-yksikkö Atmosware IC1000

    - 2 kpl I/O-kortteja

    - työ (ohjelmointi, tagien lisääminen järjestelmään, valvomografiikan päivitys, kytkentämuutokset ala-asemaan)

- Swegonin tarpeenmukaisen ilmanvaihdon laitteet ja tarvikkeet n. 2900 €

- Ilmanvaihtokoneen ohjelmointi ja muutostyöt n. 3000 €

- Swegon Wise-järjestelmän liitäntä kiinteistöautomaatiojärjestelmään n. 2750 €

- Asennuskustannuksien (työ + tarvikkeet) arvio n. 2000 €

- Kustannusarvio yhteensä 18 150 €. [120]

Kyseisessä insinöörityötutkimuksessa, joka toteutettiin Metropolian Myyrmäen yksikön B-osan luokkatilojen B243 ja B244 osalta päätettiin EC-moottori korvata taajuusmuuttajaohjatuilla AC-moottoreilla, johtuen EC-moottoreiden 10-kertaisesta hankintahinnasta. Taajuusmuuttaja ohjatun AC-moottorin hankintahinnaksi arvioitiin n. 300 – 1000 € ja taajuusmuuttajat n. 900 €. Lopullinen kokonaishinta ilman asennuskustannuksia kahden eri luokkatilan oli seuraavanlainen:

- Swegon Wise-järjestelmä 2864 €
- Schneider Electric (Taajuusmuuttajat, IC1000, anturit) 5750 €
- Lassila&Tikanoja (Asennukset ja tarvikkeet) 2000€. [120]

Kokonaiskustannukseksi saatiin 10 614 € ja 30 % vuosittaisella energiansäästöllä saatiin takaisinmaksuajaksi 27 vuotta, kun huomioon oli otettu käyntiaikamuutokset. Keskeisenä kustannussäästönä voidaan pitää Schneiderin kokonaishintaa, joka piti sisällään Wise-järjestelmän liitännän rakennusautomaatiojärjestelmään, anturit, rakennusautomaation CPU-yksikön, taajuusmuuttajat sekä tarvittavat ohjelmoinnit. Kun arvioidaan ilmanvaihdon vaikutusalueen pinta-alan perusteella, niin hinta alennettuna oli 73,30 €/m^2 ja ilman alennettua hintaa ja EC-moottoreilla 125,35€/m^2 sekä ilman EC-moottoreita 94,28 €/m^2, kun kahden luokkatilan pinta-ala oli yhteensä 144,8 m^2 (60,8 m^2 ja 84 m^2). [120]

Keskeistä mitä kustannusarviosta ei pystytä arvioimaan voisi olla uuden ilmanvaihtokoneen aiheuttama lisäys kokonaiskustannuksiin. Kyseisten luokkatilojen kokonaisilmamäärä oli tuloilman osalta 0,3964 m^3/s ja poiston osalta 0,2129 m^3/s. Tällöin Swegon Wise-järjestelmään suositeltu ja yhteensopiva Swegon Gold ilmanvaihtokoneen kokonaiskustannustenjakautuminen kyseisiin luokkatiloihin tarkoittaa ilmanvaihtokoneen maksimi-ilmamäärän 9 m^3/s jakamista tuloilmamäärällä. Luokkatilojen vaikutus ilman-

vaihtokoneen hankintahintaan on noin 1/22 osaa, joka tarkoittaa esim. 80 000 € ilmanvaihtokoneella n. 3636 €. Kun lasketaan neliöperusteinen kokonaiskustannukselle ilman EC-puhaltimia, koska ilmanvaihtokone pitää ne sisällään, saadaan 119,40 €/m^2. Hinnassa ei tietenkään pystytä arvioimaan Swegonin langattomien antureiden aiheuttamia hankinta-, asennus- ja konfigurointikustannuksia ja muita uuden sukupolven Wise-järjestelmään liittyviä epäsuoria kustannuksia, joita syntyy erilaisten esim. päätelaitteiden, säätöpeltien yms. hankinnasta ja konfiguroinnista osaksi järjestelmää. [120]

11 Yhteenveto

Keskeisenä seikkana tässä insinöörityössä oli tehdä Swegonin yritysvierailun tuloksena alkuselvitys liittyen Swegonin uuden sukupolven Wise-järjestelmän kaltaisiin tarpeenmukaisiin älykkäisiin ilmanvanvaihtoratkaisujen toimittajiin Suomen markkinoilla. Työn lähtökohtana painotettiin erityisesti langatonta tiedonsiirtoa ja sen tuomia mahdollisuuksia, joista esimerkiksi antureiden, toimilaitteiden ja päätelaitteiden kaapelointikustannuksien kustannussäästöt ja asennusaikojen minimointi nähtiin tarpeellisina toteutuksen kannalta. Uhkakuvina työssä nähtiin erityisesti kyberturvallisuus, jota työssä käytiin teoreettisesti läpi, mutta joka vaatii jatkotarkastelua esim. tietotekniikkaan ja kyberturvallisuuteen painottuvassa opinnäytetyössä. Se miksi näitä asioita ei voitu tässä insinöörityössä tarkkaan todeta on, se että työntekijä ei ole tietotekniikkaa lainkaan opiskellut, ja erilaiset IoT-laitteet, jotka hyödyntävät yhteydetöntä protokollaa (UDP) ja/tai yksinkertaisia verkonhallintaprotokollia (SNMP) voivat olla alttiina kyberturvallisuushyökkäyksille. Monesti tarkempi tietoturvallisuuden tarkastelu edellyttää myös laitetason tarkempaa selvitystä, koska on yleisesti tiedossa, että esim. kodinkoneet, jotka ovat hyödyntäneet IoT-verkkoja ja ovat olleet yhteydessä kodin tietoverkkoon, ovat voineet skannata kodin verkkoliikennettä vapaasti. Monesti erityyppiset laitetoimittajat ostavat IoT-verkkoon kytkettävät anturit ja sovellukset alihankkijoilta ilman tarkempaa tietoa kyberturvallisuuteen liittyvistä asioista. Swegonin uuden sukupolven Wise-järjestelmä hyödyntää Lumen radion MiraOS-järjestelmäratkaisua IoT-verkossa ja Lumenradion markkinoima 1500 € maksava testisovellus nähtiin tämän insinöörityön kannalta liian kalliiksi toteutuksen tarkempaa tarkastelua varten.

Tässä insinöörityössä kuvattiin älykkäiden antureiden ja IoT-verkon mahdollistamaa ilmanvaihtoratkaisua, johon uuden sukupolven Swegon Wise-järjestelmä on keskittynyt. Suomessa älykkäiden antureiden ja IoT-verkkojen hyödyntäminen on vasta kehitysasteella ja suurimmaksi osasyyksi on arveltu tietoturvan puute monissa kuluttajalaitteissa. Seskon IoT-komitea ISO/IEC JTC 1/SC 41 on vuonna 2017 käynnistänyt IoT-verkkojen luottamuksenarvoisuudesta selvityksen, joka on käyttäjälähtöinen järjestelmänsuunnittelukonsepti, johon kuuluvat kaikki ne ominaisuudet, jotka aikaansaavat luottamuksen

järjestelmään. Näihin kuuluvat tietoturvallisuus, saatavuus, jatkuvuus, turvallisuus, toimintavarmuus ja yksityisyys. Selvitystä ei oltu vielä julkistettu vuoden 2019 alussa, eikä myöskään automaatiokyberturvallisuuteen liittyvää laitestandardia IEC 62443-4-2, joka keskittyy pääasiallisesti päätelaitteiden suojaamiseen, ei ollut myöskään julkistettu tätä insinöörityötä tehdessä. [126]

Tässä insinöörityössä verrattiin langallisia ja langattomia älykkäillä antureilla toimivia ilmanvaihtoratkaisuja, joiden tarkoituksena oli sisäilman laadun parantaminen ja tarpeenmukaisen ilmanvaihdon soveltuvuuden arvioiminen eri teollisuuden tiloihin. Tässä insinöörityössä ainoaksi soveltuvaksi tarpeenmukaista ilmanvaihtoa noudattavaksi järjestelmäksi nousi esiin Swegonin uuden sukupolven Wise-ilmanvaihtojärjestelmä. Järjestelmän soveltuvuutta teollisuuden tuotantotiloihin Swegonin myyntipäällikkö Tryggve Leander ei suositellut, mutta teollisuuden toimistotiloihin järjestelmä on mahdollista hyödyntää. Lisäksi järjestelmän radiokuuluvuus ja radioesteet on syytä selvittää ennen laitteen käyttöönottoa.

Insinöörityö oli erityisen haastava, johtuen IoT-verkkojen olemuksesta hyödyntää sekä IT- (Information Technology) että OT- (Operative Technology) järjestelmiä, joka on selkeä tietoturvariski teollisuusohjausjärjestelmään liittyen. Hyvinä puolina langattomien IoT-antureiden hyödyntämisessä nähdään asennuskustannusten alentuminen, nopeampi käyttöönotto, tilamuutoksista johtuvien kustannusten aleneminen, energian säästö monipuolisempien antureiden avulla, energiansäästö vähävirtaisten antureiden avulla sekä huoltokustannusten vähentyminen liittyen etäyhteyksien avulla tapahtuvaan huoltoon sekä sähköjohtoihin liittyvään vianetsintään.

Lähteet

1 IoT essentials verkkokurssi 11.01.2019. Kaakkois-Suomen ammattikorkeakoulu.

2 SFS-EN 15251. 2007. Sisäympäristön lähtötiedot rakennusten energiatehokkuuden suunnitteluun ja arviointiin ottaen huomioon ilman laatu, lämpöolot, valaistus ja äänitekniset ominaisuudet. Helsinki: Suomen Standardisoimisliitto.

3 Rantalainen, Samuel. 2017. Tarpeenmukaisen ilmanvaihtojärjestelmän vertaaminen perinteiseen ilmanvaihtojärjestelmään. Insinöörityö. Kaakkois-Suomen ammattikorkeakoulu.

4 Tarpeenmukainen ilmanvaihto. Verkkoaineisto. Swegon Oy. <www.swegon.com/fi/Tuotteet/Tarpeenmukainen-ilmanvaihto/>. Luettu 1.11.2018.

5 Köykkä, Kai. 2013. Tarpeenmukainen ilmanvaihto koulurakennuksissa. Insinöörityö. Insinöörityö Seinäjoen ammattikorkeakoulu.

6 Löfman, Janne. 2018. Muuttuvailmavirtaisten ilmastointijärjestelmien ohjaus ja säätö toimistorakennuksessa. Insinöörityö. Metropolia ammattikorkeakoulu.

7 Toimistomaisten tilojen ilmastoinnin suunnittelu. Verkkoaineisto. Työterveyslaitos. <www.ttl.fi/tyoymparisto/sisaymparisto/toimiva-ilmanvaihto/toimistomaisten-tilojen-ilmastoinnin-suunnittelu/>. Luettu 1.11.2018.

8 Veijalainen, Tuomas. Lindab Oy. Vierailijaluento 08.10.2018. Metropolia ammattikorkeakoulu, Leppävaaran yksikkö.

9 Holopainen, Esa. 2016. Tarpeenmukainen ilmanvaihto ja automaatio päiväkotihankkeessa. Insinöörityö. Jyväskylän ammattikorkeakoulu.

10 Fläkt Woods Optivent Ultra IMS-säädin. 2015. Verkkoaineisto. VTT. <www.vtt.fi/vaikuttavuus/referenssej%C3%A4/referenssit-%C3%A4lyk%C3%A4s-teollisuus/uusi-mittausj%C3%A4rjestelm%C3%A4-parantaa-sis%C3%A4ilman-laatua-ja-v%C3%A4hent%C3%A4%C3%A4-energiakustannuksia-jopa-50>. Luettu 1.11.2018.

11 EnOceanin ratkaisut toimistotiloihin. 2018. Verkkoaineisto. Enocean alliance. <www.enocean-alliance.org/solutions/building-automation/>. Luettu 14.11.2018.

12 Schneider-Electricin toimittama täysin ohjelmoitava VA2 – VAV säädinyksikkö. 2018. Verkkoaineisto. Enocean alliance. <www.enocean-alliance.org/product/schneider_va2-vav-controller/>. Luettu 14.11.2018.

13 Sisäilmasto ja ilman vaihto-opas. 2018. Verkkoaineisto. Talotekniikkainfo. <www.talotekniikkainfo.fi/sites/default/files/talotekniikkainfo_sisisailmasto_ja_ilmanvaihto_-opas_30.1.2018.pdf>. Luettu 14.11.2018.

14 Teollisuusilmastointi. Verkkoaineisto. Työterveyslaitos. <www.ttl.fi/tyoymparisto/sisaymparisto/toimiva-ilmanvaihto/teollisuusilmastointi/>. Luettu 30.1.2018.

15 Sandberg, Esa (toim.). 2014. Sisäilmasto- ja ilmastointijärjestelmät, Ilmastointitekniikka osa 2. Helsinki. Talotekniikka-julkaisut Oy.

16 Koneelliset savunpoistolaitteet rakennusprojekteihin. Tuotekuvasto 2019. Verkkoaineisto. Sodeca. < https://www.sodeca.com/repository/documentos/FI/SE20_THT_HATCH_2019FI.pdf>. Luettu 27.03.2019.

17 IP-luokitus. 2018. Verkkoaineisto. Sähköturvallisuuden edistämiskeskus STEK ry. <stek.fi/perustietoa-sahkosta/sahkojarjestelmat/ip-luokitus/>. Luettu 22.11.2018.

18 WISE IAQ-anturi. 2017. Verkkoaineisto. Swegon Oy. <www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/WISE_IAQa.pdf>. Luettu 22.11.2018.

19 WISE IORE-anturi. 2017. Verkkoaineisto. Swegon Oy. <www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/WISE_IOREa-m.pdf>. Luettu 22.11.2018.

20 WISE IRT-anturi. 2017. Verkkoaineisto. Swegon Oy. <www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/WISE_IRTa-m.pdf>. Luettu 22.11.2018.

21 WISE IRE-anturi. 2017. Verkkoaineisto. Swegon Oy. <www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/WISE_IREa-m.pdf.> Luettu 22.11.2018.

22 WISE OCS-anturi. 2017. Verkkoaineisto. Swegon Oy. <www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/WISE_OCSa-m.pdf>. Luettu 22.11.2018.

23 WISE RTA-anturi. 2017. Verkkoaineisto. Swegon Oy. <www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/WISE_RTAa-m.pdf>. Luettu 22.11.2018.

24 WISE RTS-anturi. 2017. Verkkoaineisto. Swegon Oy. <www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/WISE_RTSa-m.pdf>. Luettu 22.11.2018.

25 WISE WCS-anturi. 2017. Verkkoaineisto. Swegon Oy. <www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/WISE_WCSa-m.pdf>. Luettu 22.11.2018.

26 Sarhela, Arto. 2010. Ilmastointijärjestelmän perusparannuksen esisuunnitelma teollisuusyrityksessä. Insinöörityö. Mikkelin ammattikorkeakoulu.

27 Takatalo, Tuomas. 2015. Rakennusten yleisilmanvaihto kaivosteollisuudessa. Insinöörityö. Oulun ammattikorkeakoulu.

28 Eloranta, Jouko. Fanison Oy. Vierailijaluento 08.11.2018. Metropolia ammattikorkeakoulu Leppävaaran yksikkö.

29 Leander, Tryggve. Swegon Oy. Vierailijaluento 10.10.2018. Metropolia ammattikorkeakoulu Leppävaaran yksikkö.

30 WISE uusi sukupolvi. 2017. Verkkoaineisto. Swegon Oy. <www.swegon.com/fi/Tuotteet/Tarpeenmukainen-ilmanvaihto/WISE--uusi-sukupolvi/>. Luettu 1.11.2018.

31 Climecon MyAir-ilmanvaihtojärjestelmä. Verkkoaineisto. Climecon Oy. <www.climecon.fi/doc/muut/MyAir-esite.pdf>. Luettu 14.11.2018.

32 IPSUM-ilmanvaihtojärjestelmä. 2014. Verkkoaineisto. FläktWoods Oy. <resources.flaktwoods.com/Perfion/File.aspx?id=e6aad9bc-4925-4632-b239-5fac97b05a1d>. Luettu 14.11.2018.

33 Pascal-järjestelmä. 2014. Verkkoaineisto. Lindab Oy. <www.lindab.com/fi/Documents/Ilmastointi/esitteet%20ja%20dokumentit/Pascal-j%C3%A4rjestelm%C3%A4%20esite.pdf>. Luettu 15.11.2018.

34 MyVallox-järjestelmä. 2018. Verkkoaineisto. Vallox Oy. <https://www.vallox.com/myvallox>. Luettu 15.11.2018.

35 SpaceLYnk logiikkaohjain. 2018. Verkkoaineisto. Schneider Electric Oy. <www.se.com/fi/fi/product/LSS100200/knx-spacelynk-monirajapinta/>. Luettu 15.11.2018.

36 Multi-Purpose Management Devices. 2016. Verkkoaineisto. Schneider Electric Oy. <download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=MPM+Series+-+Installation+Sheet.pdf&p_Doc_Ref=II-SSL-MPM-EN.A4>. Luettu 15.11.2018.

37 Ouman Ounet. 2015. Verkkoaineisto. Ouman Oy. <https://ouman.fi/tuote/ouman-ounet/>. Luettu 15.11.2018.

38 Ouman Wireless. 2018. Verkkoaineisto. Ouman Oy. <ouman.fi/wp-content/uploads/2018/08/OUMAN_WIRELESS__brochure__fi.pdf>. Luettu 15.11.2018.

39 Uuden sukupolven langattomat proxima lähettimet. 2018. Verkkoaineisto. Produal Oy. <www.produal.com/fi/news/uuden-sukupolven-langattomat-produal-proxima-lahettimet-kisaavat-finnbuild-messujen-mielenkiintoisimman-tuotteen-tittelista/>. Luettu 15.11.2018

40 Langattomat toimistosovellukset. 2018. Verkkoaineisto. Produal Oy. <www.produal.com/fi/applications/office-room-applications-2/wireless-business-building-application/>. Luettu 02.11.2018.

41 Granlund, Kaj. 2001. Langaton tiedonsiirto. Docendo Finland Oy.

42 6LoWPAN protokollapinon erot. 2015. Verkkoaineisto. Research Gate. <www.researchgate.net/figure/IP-and-6LoWPAN-protocol-stack-in-reference-to-layers-of-the-TCP-IP-networking-model_fig1_281333084>. Luettu 20.11.2018.

43 Nikunen, Joonas. Bluetooth Smart ja langattoman automaation mahdollisuudet - Metso, Flow Control. 2017. Verkkoaineisto. Suomen automaatioseura Ry. <www.automaatioseura.fi/site/assets/files/1550/f2062.pdf>. Luettu 22.11.2018.

44 IoT:lla toteuttettujen laitteiden radiokattavuus. 2019. Verkkoaineisto. Blue Marble Inc. <http://bluemarbleirrigation.com/iot-basics-three-realms-of-iot-radio-range/>. Luettu 28.11.2018.

45 Wifi 6 verkon hyödyt. Verkkoaineisto. 2018. Belden Inc. <https://www.belden.com/blog/smart-building/the-benefits-of-wi-fi-6-and-what-youll-need-to-support-it>. Luettu 30.11.2018.

46 Mikä muuttuu, kun tulee 5G. 2017. Verkkoaineisto. Elisa Oyj. <https://yksityisille.hub.elisa.fi/mika-muuttuu-kun-tulee-5g/>. Luettu 3.12.2018.

47 Lumenradio MiraOS. 2018. Verkkoaineisto. Lumenradio Ab. <https://docs.lumenrad.io/miraos/>. Luettu 15.12.2018.

48 Patenttihaku, Patentimages. 2013. Verkkoaineisto. USPTO. <https://patentimages.storage.googleapis.com/00/9b/f1/afad55881c5cb9/US8565176.pdf>. Luettu 15.12.2018.

49 Cognitive Coexistence Radios. Verkkoaineisto. MIT TLO. <http://tlo.mit.edu/tech-keywords/cognitive-coexistence-radios>. Luettu 15.12.2018.

50 Siemens IoT2040 älykäs Gateway pilvipalveluihin. Siemens Oy. <http://www.siemens.fi/fi/industry/teollisuus/tuoteuutiset/simatic_iot2040_on_alykas_iot_gateway_pilvipalveluihin.htm>. Luettu. 2.12.2018.

51 Saalamo, Antti. 2018. Siviilitiedustelulainsäädännön vaikutukset yritysten liiketoiminnassa. Tradenomityö. Laurea ammattikorkeakoulu.

52 Remes, Juha. 2018. Seminaariesitys. Vaasa Energy Week, Cooperation between Energy Technology and Cyber Security Actors. Verkkoaineisto. Vaasa Energy Week. <https://www.energyweek.fi/wp-content/uploads/2017/09/CyberDigi_Remes.pdf>. Luettu 22.03.2018.

53 IoT:n tietoturvariskit. 2016. Metropolia verkkoaineisto. <https://wiki.metropolia.fi/display/alykas/IoT%3An+tietoturvariskit>. Luettu 13.01.2018.

54 Tietoturvan merkitys ja periaatteet IoT:ssa. 2016. Metropolia verkkoaineisto. <https://wiki.metropolia.fi/display/alykas/Tietoturvan+merkitys+ja+periaatteet+IoT%3Assa>. Luettu 13.01.2018.

55 IoT:ssä käytettyjä viestiprotokollia. 2016. Metropolia verkkoaineisto. <https://wiki.metropolia.fi/pages/viewpage.action?pageId=138445135>. Luettu 13.01.2018.

56 ST 682.10. Tietotekniset järjestelmät. 2018. Tietoteknisten järjestelmien integrointi. Helsinki: Sähköinfo Oy.

57 Alve, Jukka; Sundqvist, Matti. Standardisarja IEC Teollisuuden tietoliikenneverkot - Verkkojen ja järjestelmien tietoturvallisuus. 2013. Verkkoaineisto. Suomen automaatioseura Ry. <https://www.automaatioseura.fi/site/assets/files/1431/sundquist_matti_standardi_iec_62443_161013_sundcon_sas_asaf_16_10_2013.pdf>. Luettu 17.11.2018.

58 Plant Security Services – Kyberturvakartoitus. Automaatioseuran Turvallisuusjaoston automaation tietoturva. 2017. Verkkoaineisto. Suomen automaatioseura Ry. <https://www.automaatioseura.fi/site/assets/files/1603/sas_asaf-teemapaiva_10-5-2017_jyrki_keinanen_tietoturva-arvio_ja_sen_tekeminen.pdf>. Luettu 17.11.2018.

59 Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications. 2018. Verkkoaineisto. Schneider Electric Oy. <https://www.schneider-electric.com/en/download/document/998-20186845/>. Luettu 20.11.2018.

60 Tietomurtojen havainnointi verkosta open source -työkaluin. 2014. Verkkoaineisto. Nixu Cybersecurity Oy. <https://www.nixu.com/fi/blog/tietomurtojen-havainnointi-verkosta-open-source-tyokaluin>. Luettu 20.11.2018.

61 A Step by Step Analysis of How Your ICS is Compromised through an Externally Generated Cyber Attack. 2018. Verkkoaineisto. Cyber Startup Observatory Inc. <https://cyberstartupobservatory.com/step-by-step-compromising-your-ics-through-externally-generated-cyber-attack/>. Luettu 28.11.2018.

62 German Steel Mill Cyber Attack (Cyber-to-Physical or Process Effects) case study paper. 2018. Verkkoaineisto. ICS CP/PE. <https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf>. Luettu 23.11.2018.

63 Kill Chain for Industrial Control System. 2018. Verkkoaineisto. MATEC Web of Conferences 173. <https://www.matec-conferences.org/articles/matecconf/pdf/2018/32/matecconf_smima2018_01013.pdf>. Luettu 23.11.2018.

64 Is your manufacturing facility vulnerable to cyber-attacks? Verkkoaineisto. Formacpace Inc.<https://formaspace.com/articles/it-computers/manufacturing-facility-cyber-attacks/>. Luettu: 24.11.2018.

65 Näin IoT-järjestelmät menevät pilveen. 2018. Verkkoaineisto. Teknologiamediat Oy <https://www.uusiteknologia.fi/wp-content/uploads-/2018/10/2_2018_low.pdf>. Luettu 27.11.2018.

66 Engdahl, Tomi. Salaus ja tietoturva teollisen internetin ratkaisuissa. 2015. Verkkoaineisto. Teknologiamediat Oy <http://www.uusiteknologia.fi/wp-content/uploads/2015/10/IoT_Tietoturva_Final1.pdf>. Luettu 24.11.2018.

67 Lisää rautaa kyberturvaan: suomalaiset pankit paransivat suojauksiaan iskujen jälkeen. 2017. Verkkoaineisto. Alma Media Oyj. <https://www.tivi.fi/Kaikki_uutiset/lisaa-rautaa-kyberturvaan-suomalaiset-pankit-paransivat-suojauksiaan-iskujen-jalkeen-6613074>. Luettu 13.11.2018.

68 Energia-ala varautuu yhdessä kyberuhkiin. 2018. Verkkoaineisto. VTT. <https://www.vtt.fi/Impulssi/Pages/Energia-ala-varautuu-yhdessa-kyberuhkiin.aspx>. Luettu 13.11.2018.

69 Addressing Cyber Threats in Power Generation and Distribution. 2017. Verkkoaineisto. Vaasa EnergyWeek Oy. <https://www.energyweek.fi/wp-content/uploads/2017/09/CyberDigi_-Tuomela.pdf>. Luettu 13.11.2018.

70 Komission tiedonanto Euroopan Parlamentille, Eurooppa-neuvostolle ja neuvostolle. 2018. Verkkoaineisto. Euroopan komissio. <http://ec.europa.eu/transparency/regdoc/rep/1/2018/FI/COM-2018-211-F1-FI-MAIN-PART-1.PDF>. Luettu 13.11.2018.

71 Yli puolet yrityksistä myöntää puutteet kyberuhkien torjunnassa. Verkkoaineisto. EY. <http://news.cision.com/fi/ey/r/yli-puolet-yrityksista-myontaa-puutteet-kyberuhkien-torjunnassa,c2397321>. Luettu 13.11.2018.

72 Kohdistetut haittaohjelmahyökkäykset uhka otettava vakavasti. 2014. Verkkoaineisto. Traficom. <https://www.viestintavirasto.fi/attachments/tietoturva/Kohdistetut_haittaohjelmahyokkaykset_uhka_otettava_vakavasti_raportti_28082014.pdf>. Luettu 13.11.2018.

73 Teollisuusautomaation tietoturva. Verkkoaineisto. Suomen automaatioseura Ry.<https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf>. Luettu 13.11.2018.

74 Huijarille täysi hallinta puhelimeen - qr-koodien skannauksesta varoitetaan. 2013. Verkkoaineisto. Alma Media Oyj. <https://www.tivi.fi/Uutiset-/2013-08-21/Huijarille-t%C3%A4ysi-hallinta-puhelimeen---qr-koodien-skannauksesta-varoitetaan-3203205.html>. Luettu 13.11.2018.

75 Swegon Wise-järjestelmäopas. 2018. Verkkoaineisto. Swegon Oy <https://www.swegon.com/Global/PDFs/Flow%20control/WISE%-20gen.2/_fi/WISE_Systemguide_gen2.pdf>. Luettu 17.11.2018.

76 Tietojen salaaminen. Yksityisyyden suoja. Verkkoaineisto. 2018. <https://www.yksityisyydensuoja.fi/tietojen-salaaminen>. Luettu 17.11.2018.

77 AES-salaus ei olekaan niin varma kuin luultiin. Verkkoaineisto. 2011. Alma Media Oyj. <https://www.tivi.fi/Arkisto/2011-08-19/AES-salaus-ei-olekaan-niin-varma-kuin-luultiin-3140363.html>. Luettu 17.11.2018.

78 Snowdenin jalanjäljillä. 2015. Verkkoaineisto. Tampereen yliopisto Porin yksikkö. <http://www.poridi.fi/snowdenin-jalanjaljilla/>. Luettu: 17.11.2018.

79 Turvallisempi kirjautuminen on nyt helppoa. 2016. Verkkoaineisto. Alma Media Oy. <https://www.tivi.fi/Vinkit/turvallisempi-kirjautuminen-on-nyt-helppoa-6535036>. Luettu 17.11.2018.

80 Swegon Wise suunnitteluopas. 2018. Verkkoaineisto. Swegon Oy. <https://www.swegon.com/Global/PDFs/Flow%20control/WISE-%20gen.2/_fi/WISE_Suunnitteluopas_S%C3%A4hk%C3%-B6%20ja%20ohjaus.pdf>. Luettu 27.12.2018.

81 Swegon Connect. 2017. Verkkoaineisto. Swegon Oy. <http://www.swegongroup.net/Global/PDFs/System%20Prod-ucts/_fi/SwegonConnect_brochure.pdf>. Luettu 22.12.2018.

82 Langattomien verkkojen salaus murrettu – Viestintävirasto ja Microsoft julkaisivat toimintaohjeet. 2017. Verkkoaineisto. Mareti Media Oy. <https://mobiili.fi/2017/10/16/langattomien-verkkojen-salaus-murrettu-viestintavirasto-ja-microsoft-julkaisivat-toimintaohjeet/>. Luettu 18.11.2018.

83 Suomessa 4g-dataa voi varastaa - "salataan vasta, kun jollakin operaattorilla tapahtuu jotain". 2014. Verkkoaineisto. Alma Media Oyj. <https://www.tivi.fi/Arkisto/2014-04-03/Suomessa-4g-dataa-voi-varastaa---salataan-vasta-kun-jollakin-operaattorilla-tapahtuu-jotain-3076940.html>. Luettu 18.11.2018.

84 Scanner Tune Wise. 2017. Verkkoaineisto. Swegon Oy. <https://www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/Scanner_TuneWISEa.pdf>. Luettu 18.11.2018.

85 Scanner Tune Wise kit. 2017. Verkkoaineisto. Swegon Oy. <https://www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/Scanner_TuneWISEa-KIT-m.pdf>. Luettu 18.11.2018.

86 Connect Wise USB. 2017. Verkkodokumentti. Swegon Oy. <https://www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/Connect_WISE_USBa-m.pdf>. Luettu 18.11.2018.

87 Tune Wise. 2017. Verkkoaineisto. Swegon Oy. <https://www.swegon.com/Global/PDFs/Flow%20control/WISE%20gen.2/_fi/TuneWISEa-m.pdf>. Luettu 18.11.2018.

88 Haavoittuvuus. 2017. Verkkoaineisto. Traficom. <https://www.viestintavirasto.fi/kyberturvallisuus/haavoittuvuudet/2017/haavoittuvuus-2017-033.html>. Luettu 19.11.2018.

89 Turpeinen, Mikko. 2014. Avoimen lähdekoodin ohjelmistopohjaiset VPN-sovellukset. Tradenomityö. Haaga-Helia ammattikorkeakoulu.

90 Virtuaalinen erillisverkko. 2013-2018. Verkkoaineisto. Vesa Viljanen <https://www.yksityisyydensuoja.fi/content/virtuaalinen-erillisverkko>. Luettu 18.11.2018

91 Tietoturva nyt 2014. Verkkoaineisto. Traficom. <https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2014/09/ttn201409091046.html>. Luettu 19.11.2018.

92 Cyber security. Verkkoaineisto. Siemens Oy. <https://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/technology-highlights/pages/cyber-security.aspx#Multi_20Service_20Platform>. Luettu 19.11.2018.

93 RIL 268 2017 Kiinteistöä kehittävä linjasaneeraus lausuntoversio. Verkkoaineisto. Suomen rakennusinsinöörien liitto RIL ry. Linkki: <https://www.ril.fi/media/2017/2017-julkaisut/ril-268-2017-kiinteistoa-kehittava-linjasaneeraus-lausuntoversio.pdf>. Luettu 20.11.2018.

94 Kukkola, Pasi. 2010. Verkkoliikenneanalysaattori Linux-ympäristössä. Insinöörityö. Keskipohjanmaan ammattikorkeakoulu.

95 Industrial HiVision Network Management Software. 2017. Verkkoaineisto. Belden Inc. <https://www.belden.com/products/industrial/networking/software/industrialhivision>. Luettu 21.11.2018.

96 Networkworld. LAN switch security: what the hackers know that you don't. Verkkoainesto. IDG Communications, Inc. <https://www.networkworld.com/article/2288792/lan-wan/lan-switch-security--what-the-hackers-know-that-you-don-t.html>. Luettu 21.11.2018.

97 Industrial Ethernet Switches Enhance Cyber Security at No Cost. 2017. Verkkoaineisto. Belden Inc. <https://www.belden.com/blog/industrial-security/industrial-ethernet-switches-enhance-cyber-security-at-no-cost>. Luettu 21.11.2018.

98 Teollisuusautomaation tietoturva. 2016. Verkkoaineisto. Traficom. <https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf>. Luettu 23.11.2018.

99 Termisanasto. Verkkoaineisto. 2015. Elmark Inc.<http://www.support.elmark.com.pl/rgd/drivery/S15S/WLAN/INTEL/XP_VISTA/XP/Docs/FIN/glossary.htm>. Luettu 24.11.2018.

100 Arveluttaako QR-koodin lukeminen? Näin teet sen turvallisesti. Verkkoaineisto. Alma Media Oyj. <https://www.tivi.fi/Vinkit/arveluttaako-qr-koodin-lukeminen-nain-teet-sen-turvallisesti-6539243>. Luettu 23.11.2018.

101 Coleman, David; C. Miller, Lawrence. 2018. 802.11ax for dummies – Aerohive Special Edition. John Wiley & Sons, Inc., Hoboken, New Jersey 2018.

102 Lindkvist, Peter. Lumenradio AB. Haastattelu koskien Mira IoT-verkkojen tietoturvaa. 17.12.2018

103 Industrial Cyber Security. 2017. Verkkoaineisto. Belden Inc. <https://www.belden.com/hubfs/resources/knowledge/other/belden-tripwire-cyber-security-line-card.pdf?hsLang=en>. Luettu 24.11.2018.

104 Pöyhönen, Vladimir. 2014. Automaatiojärjestelmän virtualisointi - Korkean käytettävyyden klusteri. Insinöörityö. Metropolia ammattikorkeakoulu.

105 Sippola, Maria. 2018. Koulurakennusten sisäilmaongelmat ja rakennustekninen luokittelu. Insinöörityö. Satakunnan ammattikorkeakoulu.

106 Salonen, Heidi; Lappalainen, Sanna; Lahtinen, Marjaana; Holopainen, Rauno; Palomäki, Eero; Koskela, Hannu; Backlund, Peter; Niemelä, Raimo; Pasanen, Anna-Liisa; Reijula, Kari. Toimiston sisäilmaston tutkiminen. Työterveyslaitos. Tampere 2011.

107 Hiukkasmaiset epäpuhtaudet. 2016. Verkkoaineisto. Sisäilmayhdistys Ry. <http://www.sisailmayhdistys.fi/Terveelliset-tilat/Sisailmasto/Hiukkasmaiset-epapuhtaudet>. Luettu 22.11.2018.

108 Radon Suomessa. Verkkoaineisto. Säteilyturvakeskus. <https://www.stuk.fi/aiheet/radon/radon-suomessa>. Luettu 13.01.2019.

109 Innanen, Seppo. Erikoistilojen LVI-tekniikka. Kurssimateriaalit 09-12.2018.

110 Pöyryn Finland Oy. Esimerkkiprojektin lähtötietolomake vaarallisista aineyhdisteistä teollisuudessa.

111 Kemppi, Jarkko. 2017. Tarpeenmukaisen ilmanvaihdon vaikutus sisäilmaolosuhteisiin. Maisterityö. Itä-Suomen yliopisto.

112 Yritysvierailu Swegon Oy:n Kirkkonummen testilaboratoriossa. 13.10.2018.

113 Persson, O; Wadsö L. Indoor air quality in submarines. Verkkoaineisto. <https://www.isiaq.org/docs/papers/4D2p2.pdf>. Luettu 13.01.2019.

114 Opas ilmanvaihdon mitoitukseen muissa kuin asuinrakennuksissa. FINVAC. Verkkoaineisto. <https://asiakas.kotisivukone.com/files/finvac.kotisivukone.com/tiedostot/Opas_ilmanvaihdon_mitoitukseen_muissa_kuin_asuinrakennuksissa.pdf>. Luettu 13.12.2018.

115 D2 Suomen rakentamismääräyskokoelma. 2012. Verkkoaineisto. Finlex. <https://www.finlex.fi/data/normit/37187-D2-2012_Suomi.pdf>. Luettu 16.11.2018.

116 Laakkonen, Henri. 2018. Tarpeenmukaisen ilmanvaihdon kannattavuus päiväkodissa. Insinöörityö. Karelia ammattikorkeakoulu.

117 Pasila, Juha. 2013.Tarpeenmukainen ilmanvaihto oppilaitoksissa – Energiansäästö ja ilmanlaatu. Insinöörityö. Vaasan ammattikorkeakoulu.

118 Valaistuksen ohjaus. Verkkoaineisto. Motiva Oy. <https://valaistustieto.fi/energiatehokas-valaistus/valaistuksen-ohjaus/>. Luettu 09.01.2019.

119 Vaihtoehto kesämökin talvilämmitykselle. 2010. Verkkoaineisto. Tampereen yliopisto. <http://www.tut.fi/rajapinta/artikkelit/2010/3/vaihtoehto-kesamokin-lammitykselle>. Luettu 26.12.2018.

120 Laukkanen, Joni. 2013. Myyrmäen kiinteistöautomaation nykytilan selvitys ja modernisointi. Insinöörityö. Metropolia ammattikorkeakoulu.

121 Pöyryn Finland Oy. Tietoturvaohjeet.

122 Tärkeä opas teollisuuden IoT tietoturvaan. Uusiteknologia. <https://www.uusiteknologia.fi/2018/04/04/tarkea-opas-teollisuuden-iot-tietoturvaan/>. Luettu 11.01.2019.

123 Censys.io palvelussa tehty tietoturvaskannaus. Verkkoaineisto. Censys Inc. <www.censys.io>. Luettu 11.01.2019.

124 Shodan.io palvelussa tehty tietoturvaskannaus. Verkkoaineisto. Shodan.io <www.shodan.io>. Luettu 11.01.2019

125 Tietoturvaan liittyvä ohjevideo. 2018. Verkkoaineisto. Cisco Networking academy. <cisco-netacad.wistia.com/medias/jjnqkypamu>. Luettu 12.01.2019.

126 Kriittisen infrastruktuurin suojaaminen ylimmälle tasolle asti. 2017. Verkkoaineisto. Sesko. <https://www.sesko.fi/sesko-akatemia/artikkelit_ja_kirjoitukset/kriittisen_infrastruktuurin_suojaaminen_ylimmalle_tasolle_asti.1521.news?1519_o=6>. Luettu 12.11.2018.

Standardien SFS-EN 62443-3-3 ja 62443-4-1 mukaiset automaation verkko-ympäristön suojaustasovaatimukset

Seuraavissa taulukoissa 6-12 on esitetty standardien 62443-3-3 ja 62443-4-1 mukaisia tietoturvavaatimuksia.

Taulukko 6. Eri suojaustason selitteet [60]

Suojaus-taso	Kohde	Taidot	Motivaa-tio	Tarkoitukset	Resurssit
1	Satunnaiset tai sattumanvarai-set rikkomukset	Ei hyökkäystai-toja	Ereh-dykset	Ei tarkoituksen-mukainen	Yksilölliset
2	Tietoverkko-ri-kollisuus, hakkeri	Yleiset taidot	Vähäi-nen	Yksinkertainen	Alhaiset (yksittäiset yksilöt)
3	Poliittista tai sosi-aalista edistystä tukeva hakkeri tai terroristi	Teollisuusoh-jaus-järjestel-miin erikoistu-neet taidot	Keskin-kertai-nen	Pitkälle kehitetty (Hyökkäys)	Kohtalai-set (esim. hakkeri ryhmä)
4	Kansallisvaltio tai valtion tu-kema	Teollisuusoh-jaus-järjestel-miin erikoistu-neet taidot	Korkea	Pitkälle kehitetty (Kampanja use-aan kohteeseen)	Laajenne-tut (moni-tietei-set tiimit)

Taulukossa 6 on esitetty eri suojaustason selitteet. Tasot 1-3 liittyvät suoraan standardiin 62443-3 ja taso 4 liittyy Pöyryn tietoliikennetekniikkaosaston tekemään oman spesifi-seen kartoitukseen standardin 62443-3-3 ja 62443-4-1 pohjalta.

Taulukko 7. Suojaustaso 1:n vaatimukset standardin 62443-3-3 mukaisesti [60]

Suojaustaso 1	Yleinen suojaustaso	
Sisältäen myös yleiset standardin 27001 mukaiset tietoturvavaatimukset		
Vaatimus	Vaatimuksen mukainen selite	Vaatimuksen mukainen tekniikka
1	Ohjausjärjestelmä pystyy autentikoimaan ja vahvistaa ihmiskäyttäjät. Käyttäjätilejä voidaan luoda ja hallinnoida. Määriteltävissä oleva salasanojen vahvuusvatimus. Seuraa epäonnistuneita sisäänkirjausyrityksiä.	Loppukäyttäjien tilit luodaan laitteilla tai keskitetyn autentikointiserverin avulla.
2	Ohjausjärjestelmä pystyy autentikoimaan ja vahvistaa langattomat käyttäjät.	Langattomat laitteet tai verkkoinfratruktuuri autentikoi käyttäjät.
3	Ohjausjärjestelmä tulee huolehtia mahdollisuudesta seurata ja ohjata pääsyä ei luotetuista verkoista.	Palomuurit monitoroi tietoliikennettä ei luotetuista verkoista.
4	Ohjausjärjestelmä tulee pystyä rajoittaa upotetuja koodisältöjä sähköpostiviesteissä tai tiedon varastointiin tarkoitetuissa medialaitteissa.	EPO palvelin pystyy rajoittamaan vuorovaikutusta langattomien laitteiden kanssa.
5	Ohjausjärjestelmä tulee huolehtia mahdollisuudesta luoda seurantatietueita.	Laitetason luomat tarkistustietueet / lokit.
6	Ohjausjärjestelmän on suojattava lähetettyjen tietojen eheyttä.	Laitteet tukevat salattuja protokollia, vankkatekoinen summatarkistus/hajautus.
7	Ohjausjärjestelmän on havaittava, estettävä ja raportoitava haittaohjelman vaikutukset.	Sovelluksen sallittujen lähettäjien tarkistusmekanismi (Whitelisting) on käytössä alatason laitteissa.
8	Ohjausjärjestelmän tulee suojata tietojen luottamuksellisuutta sekä tietokannan lepotilassa että siirtotilassa.	Laitteet tukevat kirjautumiseen ja valtuutukseen käytettäviä käyttäjänimiä ja salasanoja.
9	Ohjausjärjestelmä on segmentoitava verkot ja suojella niiden rajoja.	Palomuurit segmentoivat verkot ja suojaavat niiden välisiä rajoja.
10	Ohjausjärjestelmän on kyettävä estämään viestien vastaanottaminen ulkopuolisilta käyttäjiltä tai järjestelmiltä.	Palomuuri voi suodattaa ulkoisten verkkojen viestejä.
11	Ohjausjärjestelmän on tarjottava kykyä tukea kriittiseen tietoon perustuvien tietojen, sovellusten ja palvelujen jakamista vyöhykemallin toteuttamiseksi.	Verkot on segmentoitava käyttäen vyöhyke- ja kanavamallinnusta.
12	Ohjausjärjestelmän on toimittava huonontuneessa tilassa palvelunestopyynnön yhteydessä.	Erilliset verkkoelementit (kytkimet, reitittimet, jne.) tukevat nopeuden rajoittamista.
13	Ohjausjärjestelmään kytkettyjen laitteiden tulee estää tarpeettomat toiminnot, portit, protokollat ja palvelut.	ICS-laitteilla on kyky poistaa tarpeettomat ominaisuudet, kuten suoran yhteyden muodostaminen julkiseen Internettiin.
14	Ohjausjärjestelmän on tehtävä varmuuskopio käyttäjän ja järjestelmän tason tiedoista.	Varmuuskopiotiedostot saatavilla yksittäisten laitteiden avulla.

Taukukossa 7 on esitetty suojaustason 1 minimivaatimukset ja merkitty punaisella ne keskeiset tekijät, joilla katsotaan olevan vaikutusta Wise-järjestelmän ja sen langattomien IoT-verkkojen osalta.

Taulukko 8. Suojaustaso 2:n vaatimukset standardin 62443-3-3 mukaisesti [60]

Suojaustaso 2	Keskinkertainen suojaustaso	
Sisältäen myös edelliset suojaustasot		
Vaatimus	Vaatimuksen mukainen selite	Vaatimuksen mukainen tekniikka
1	Ohjausjärjestelmän tulee todentaa ja hyväksyä ohjelmistoprosessit ja -laitteet.	Ohjelmistot ja laitteet todentavat ohjelmistoprosessit käyttämällä varmenteita/sertifikaatteja.
2	Ohjausjärjestelmän on tunnistettava langattomaan viestintään osallistuvat henkilö- ja ohjelmisto käyttäjät.	Mobiililaitteet ja verkkoinfrastruktuuri todentavat käyttäjät keskitetystä autentikointipalvelimesta.
3	Ohjausjärjestelmän on tuettava vakiomuotoista PKI (Public Key Infrastructure - Julkisen avaimen perusrakenne) - ja sertifikaattipohjaista todennusta, jos sitä käytetään.	Sertifikaattien hallitsija/pääkäyttäjä lisättynä valvontaverkkoon varmenteiden myöntämiseksi.
4	Ohjausjärjestelmän on kyettävä kieltämään epäluotettavien verkkojen käyttöpyynnöt, ellei niille ole annettu valtuutettua roolia.	Ominaisuus on käytössä alatason laitteissa.
5	Ohjausjärjestelmän avulla valtuutetut käyttäjät voivat määritellä ja muokata roolien luvan kartoitusta.	Laitteissa tai yhtenäisessä tilinhallintalaitteessa on käytössä roolit ja oikeudet.
6	Ohjausjärjestelmän on käytettävä haittaohjelmien suojausta kaikissa segmentoiduissa tulo- ja lähtöpisteissä.	Verkon tunkeutumisen havaitsemisjärjestelmä (NID-node ohjelmisto) tukee haittaohjelmien suojausta. Keskitetty palvelin, joka on toteutettu etäsolmuilla, suojaa verkkoja.
7	Ohjausjärjestelmän on suojattava verkkoistuntojen eheys	Laitteet tukevat salattuja protokollia (esim. VPN, Open VPN)
8	Ohjausjärjestelmän on suojattava tarkastustiedot.	Tapahtumapalvelin, jota käytetään keskitettynä tietovarastona. Alatason laitteet välittävät tietueet tapahtumapalvelimeen.
9	Ohjausjärjestelmän on suojattava tiedon luottamuksellisuutta etäkäytössä, mikä kulkee epäluotettavan verkon kautta.	Palomuurin avulla käynnistetty VPN suojaa etäkäyttöyhteyksiä.
10	Ohjausjärjestelmän on pystyttävä fyysisesti segmentoimaan ohjausjärjestelmäverkot ei-ohjausjärjestelmä verkoista.	Viestintä kriittisistä järjestelmistä kuljetetaan eri verkoissa kuin viestintä ei-kriittisten järjestelmien osalta.
11	Ohjausjärjestelmän on raportoitava luettelo asennetuista komponenteista, joihin liittyy komponenttien ominaisuuksia.	Tallennustilaan tallennetut tiedot - valmiudet voidaan toimittaa tunkeutumisen havaitsemisjärjestelmällä (IDS).

Taukukossa 8 on esitetty suojaustason 2 minimivaatimukset ja merkitty punaisella ne keskeiset tekijät, joilla katsotaan olevan vaikutusta Wise-järjestelmän ja sen langattomien IoT-verkkojen osalta.

Taulukko 9. Suojaustaso 3:n vaatimukset standardin 62443-3-3 mukaisesti [60]

Suojaustaso 3	Korkea suojaustaso	
Sisältäen myös edelliset suojaustasot		
Vaatimus	Vaatimuksen mukainen selite	Vaatimuksen mukainen tekniikka
1	Ohjausjärjestelmän on tuettava usean tekijän todentamista epäluotettaville rajapinnoille.	Ominaisuus on otettu käyttöön keskitetyn tilinhallinnan- ja alatason laitteiden avulla.
2	Ohjausjärjestelmän on yksilöitävä ja tunnistettava ohjelmistoprosessit yksiselitteisesti.	Ominaisuus tuetaan sertifiointiviranomaisen kautta. Myös turvallisia protokollia voidaan käyttää.
3	Ohjausjärjestelmän on tuettava yhtenäistä tilinhallintaa.	Yhtenäinen tilinhallinta on käytössä keskitetyn tilinhallintapalvelimen avulla.
4	Ohjausjärjestelmän on suojattava yksityiset avaimet laitteistomekanismien avulla.	Tietoturvallinen elementti ICS-laitteissa.
5	Ohjausjärjestelmän on tunnistettava ja ilmoitettava luvattomista langattomista laitteista.	Luvattomien langattomien laitteiden tunnistaminen lisäämällä langattoman uhkailmaisin/analysointi-laitteen.
6	Ohjausjärjestelmän on tarkistettava mobiilikoodin eheys ennen kuin se sallitaan.	Mobiilikoodin eheys on varmistettu EPO-palvelimen ja sertifikaatin/varmenteen hallitsijalta.
7	Ohjausjärjestelmän on huolehdittava keskitetysti hallinnoidusta järjestelmän laajuisesta jäljitysketjusta.	Alatason laitteet välittävät lokitiedostot SIEM-palvelimelle.
8	Ohjausjärjestelmän on synkronoitava sisäinen järjestelmäkello konfiguroitavalla taajuudella.	GPS-tekniikkaan perustuva kellotoiminto/laite lisätään verkkoon osoittamaan ajan lähdettä.
9	Ohjausjärjestelmän on tuettava salausmekanismeja tunnistamaan tiedonsiirron muutokset viestinnän aikana.	Käytössä suojattuja protokollia käyttäen.
10	Ohjausjärjestelmä hallinnoi keskitetysti haittaohjelmien suojausmekanismeja.	Haitallinen koodi on suojattu EPO-palvelimen ja SIEM-palvelimen kautta. Kaikki havaitut ongelmat välitetään SIEM-palvelimelle.
11	Ohjausjärjestelmän on tuettava automaattista varmuuskopiointia konfiguroitavalla taajuudella.	Automaattinen varmuuskopiointitoiminto on tuettu varmuuskopiointipalvelimessa.
12	Ohjausjärjestelmän on raportoitava alatason laitteiden nykyiset suojausasetukset.	EPO-palvelin yhdistettynä verkonhallintajärjestelmiin raportoi suojausasetuksia.

Taukukossa 9 on esitetty suojaustason 3 minimivaatimukset ja merkitty punaisella ne keskeiset tekijät, joilla katsotaan olevan vaikutusta Wise-järjestelmän ja sen langattomien IoT-verkkojen osalta. Seuraavalla sivuilla taulukoissa 10-12 on esitetty Pöyryn olennaiset tietoturvaohjeistukset, joihin merkitty punaiselle keskeiset ongelmakohdat, kuten kryptografisen AES-salausavaimen pituus 256 bittiä ja Peer-to-Peer IoT-verkko, Wise-järjestelmän ja sen IoT-verkon osalta.

Taulukko 10. Suojaustaso 4:n vaatimukset Pöyryn tietoturvaohjeistuksen mukaisesti (1/3) [121]

Taulukon liite poistettu Pöyry Finland Oy:n salassapitovelvollisuuden johdosta.

Taulukko 11. Suojaustaso 4:n vaatimukset Pöyryn tietoturvaohjeistuksen mukaisesti (2/3) [121]

Taulukon liite poistettu Pöyry Finland Oy:n salassapitovelvollisuuden johdosta.

Taulukko 12. Suojaustaso 4:n vaatimukset Pöyryn tietoturvaohjeistuksen mukaisesti (3/3) [121]

Taulukon liite poistettu Pöyry Finland Oy:n salassapitovelvollisuuden johdosta.

IoT-laitteita koskevan tietoturvan parhaat käytännöt tehdasympäristössä

Koska IEC:n kyberturvallisuus alakomitiean 46 muistio ja standardi 62443-4-2 on vielä julkaisematta, niin seuraavassa esitetään uusiteknologia.fi verkkopalvelussa esitetyn IoT-laitteita koskevan tietoturvan parhaista käytännöistä, jotka on todettu tähän mennessä toimiviksi ja tietoturvallisiksi ratkaisuiksi.

Industrial Internet Consortium (IIC) -yhteisön uusin opas tarkentaa vuonna 2016 julkaistua IIC Industrial Internet Security Frameworkin (IISF) tietoturvamallimallidokumenttia IoT-päätelaitteiden osalta. Laitteiden valmistajat, teollisuusyritykset ja integraattorit voivat käyttää Endpoint Security Best Practices -asiakirjaa ymmärtämään, miten vastatoimia tai valvontatoimenpiteitä voidaan soveltaa tietyn tietoturvatason saavuttamiseksi (perus, tehostettu tai kriittinen). Kirjan on tarkoitus auttaa parantamaan teollisuusinternetin tietoturvaa auttamalla riskimallinnusta ja uhka-analyysia. Lisäksi Endpoint Security Best Practices tarjoaa erityisiä suosituksia eri tietoturvatasoille.

Endpoint Security Practices kirjassa kuvataan parhaita käytäntöjä teollisen turvallisuuden toteuttamiseksi, jotka ovat sopivia sovitulle turvallisuustasolle, joille voidaan antaa teollisen ekosysteemin osallistujille mahdollisuuden määritellä ja pyytää tarvitsemaansa turvallisuutta. Vaikka valkoisessa kirjassa pyritään ensisijaisesti parantamaan uusien päätepisteiden turvallisuutta, käsitteitä voidaan käyttää vanhojen päätepisteiden kanssa käyttämällä yhdyskäytäviä, verkon turvallisuutta ja tietoturvan seurantaa. Lyhyen ja ytimekkään 13-sivuinen dokumenti kokoaa keskeisiä tietoja päätepisteen laitteiden turvallisuudesta teollisuusohjauksesta ja vaatimustenmukaisuuskehyksistä, kuten IEC 62443, NIST SP 800-53 ja IIC IISF. Keskeisenä erona IEC 62443 standardiin on, se että kirjassa määritellään tietoturvatasot luokkina 2-4, koska alhaiset 0-1 tason tietoturvatasot eivät sovellu tehdasympäristöön.

Endpoint Security Best Practices kirja löytyy Internet osoitteesta www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf ja sen vuonna 2016 julkaistu pääteos löytyy Internet osoitteesta https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB.pdf. Lisäksi muita vastaavia IoT-tietoturvaa koskevia vastaavia dokumentteja suunnittelijoiden tueksi on brittihallituksen julkaisema Secure

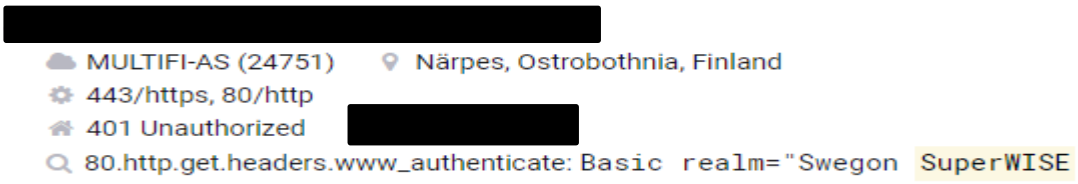
by Design tietosuojaselostus, joka löytyy Internet osoitteesta assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.

Brittihallituksen Secure by Design tietosuojaselostuksessa keskeisiä tietoturvaohjeita on, että siinä kehotetaan siirtämään verkkoturvallisuusvastuu IoT-laitevalmistajille loppukäyttäjien sijaan ja suojelemaan kuluttajien yksityisyyden suojaa. Dokumentissa pyydetään esim. esineiden internet-laitevalmistajia poistamaan oletussalasanoja, lisäämään avoimuutta haavoittuvuuksien paljastamisessa ja tallettamaan käyttäjätunnukset turvallisesti. Tietoturvavastuu siirtäminen ketjussa laitevalmistajien suuntaan on myös keskeinen idea IEC 62443-4 standardin osalta, jonka toinen osa 62443-4-2 on vielä valmisteilla ja tulossa saataville vasta vuosien 2019-2020 aikana.

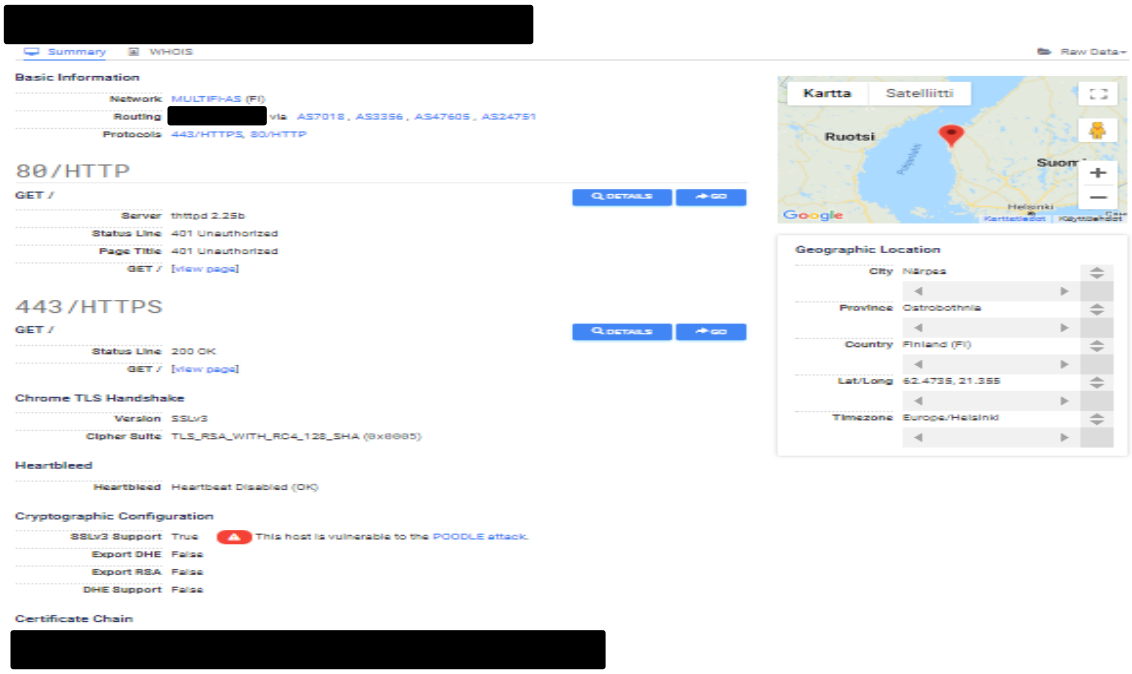
Suomessa keskeisiä avoimia IoT-laitteita selvittää ja valvoo Viestintävirasto, joka päivittää kerran vuodessa kattavan raportin nimellä ”Suojaamattomia automaatiolaitteita suomalaisissa verkoissa” – raportti. Vuoden 2018 raportti on saatavilla verkosta osoitteesta legacy.viestintavirasto.fi/attachments/cert/tietoturvakatsaukset/Erityisraportti_suojaamattomia_automaatiolaitteita_suomalaisissa_verkoissa_2018.pdf.

Eri hakupalveluilla tehty tietoturvakartoitus Wise-järjestelmään liittyen

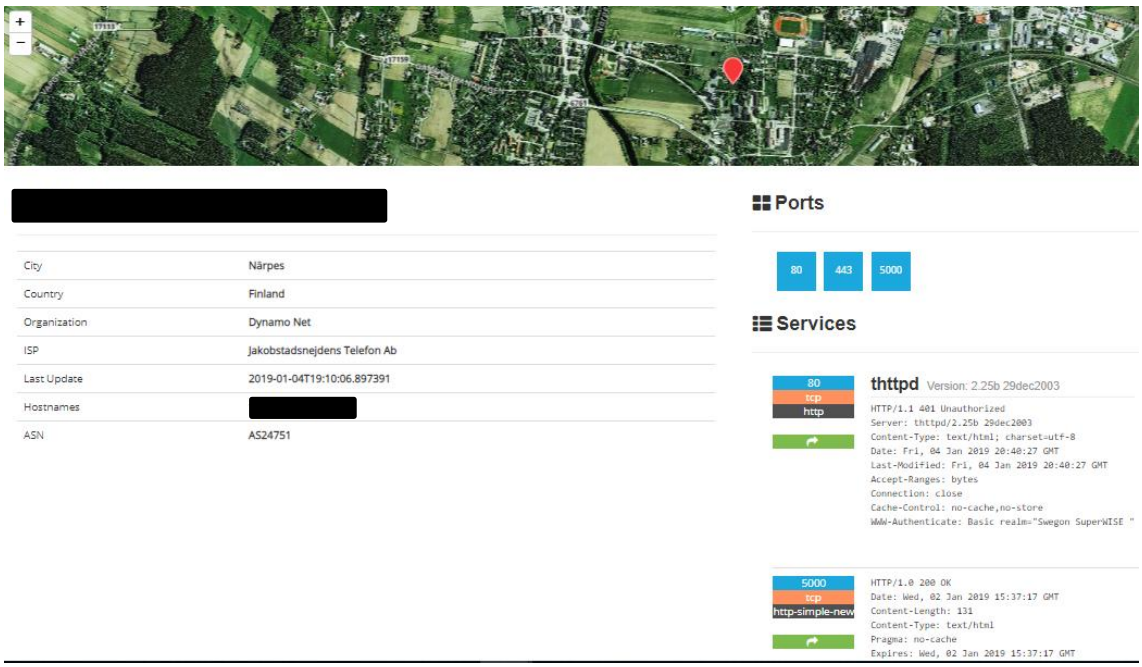
Seuraavissa kuvissa on esitetty kahdella eri verkkohakupalvelulla censys.io ja shodan.io tehdystä verkkoskannauksesta liittyen Wise-järjestelmään. Kuvissa 47-49 on esitetty haavoittuvuus koskien vanhaan Wise-järjestelmään liitetyn Närpiössä sijaitsevan kohteen tietoturvahaavoittuvuudesta, joka selviää kuvasta 47.



Kuva 47. Riskialttiin tietoturvakohteen tiedot censys.io verkkoskannauksen perusteella [123]



Kuva 48. Riskialttiin tietoturvakohteen tiedot censys.io verkkoskannauksen perusteella [123]

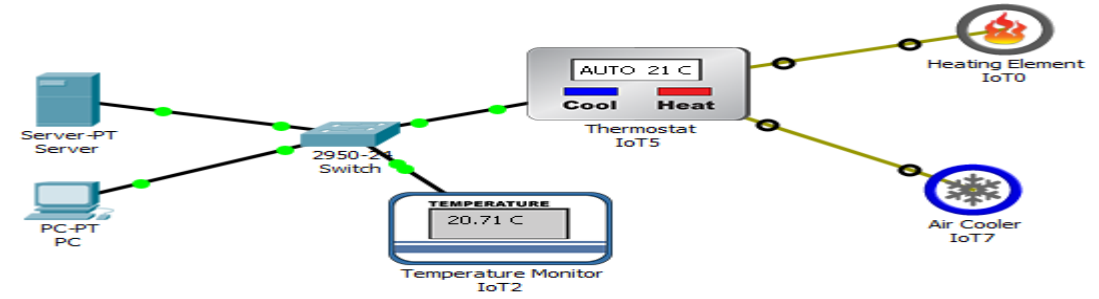


Kuva 49. Riskialttiin tietoturvakohteen tiedot shodan.io verkkoskannauksen perusteella [124]

Verkkoskannauksen perusteella tehty kartoitus osoittaa, että haavoittuvuus, joka liittyy SSLv3 konfiguraation tukemiseen ja mahdolliseen villakoirahyökkäyshaavoittuvuuteen (Poodle Attack). Verkkoskannauksessa ei löytynyt vastaavia merkkejä uuden sukupolven Wise-järjestelmän osalta, joka saattaa oleellisesti johtua IPV6 verkkoteknologian ja OpenVPN:kin käytöstä. Swegonin pilvipalveluun yhdistyviä Swegon Login laitteita pystyi kuitenkin skannaamaan censys.io ja shodan.io verkkoskannauksilla, mutta viitteitä tunnetuista haavoittuvuuksista ei vielä ainakaan löytynyt. Muita tunnettuja verkonskannaustyökaluja on Metasploit, Wireshark ja ShieldUP, jotka ovat hieman pidemmälle kehitettyjä verkonskannaustyökalua ja joiden käyttö vaatii verkkotekniikoiden syvällisempää tuntemusta ja paneutumista ohjelmien käyttöön. Seuraavassa videolinkissä on esitetty IoT-laitteiden tietoturvaa koskeva esimerkki, jossa on hyödynnetty IoT-huoneyksikkönä toimivan termostaatti laitteen valinnaista verkkoon kytkeytymistä, video löytyy osoitteesta: cisco-netacad.wistia.com/medias/jjnqkypamu.

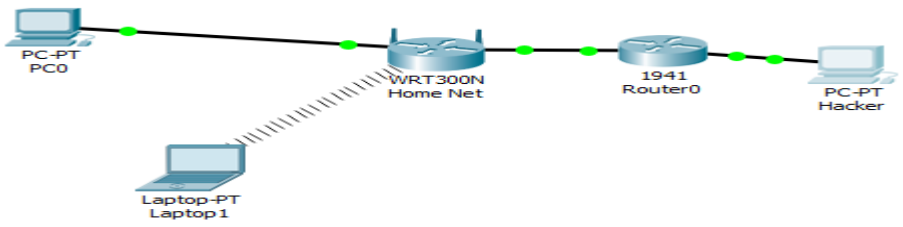
Simuloinnilla apua IoT-verkkojen tietoturvaan

Alla olevassa kuvassa 50 on esitetty Ciscon Packet Tracer simulointiohjelmalla luotu IoT-verkko, jossa lämpötila-anturin ja termostaation avulla ohjataan automaattisesti sekä lämmitysyksikköä (Heating Element IoT) ja jäähdytysyksikköä (Air Cooler). Erilaiset simulointityökalut ovat näppäriä työkaluja juuri IoT-verkkojen toiminnan testaukseen, mutta niillä voidaan testata myös tietoturvaa. Oikean tyyppisen simulointiohjelman löytäminen voi olla haasteellista, mutta simuloinnista voi olla apua myös automaatio-ohjausjärjestelmien tietoturvan ja segmentointivyöhykkeiden testauksessa.



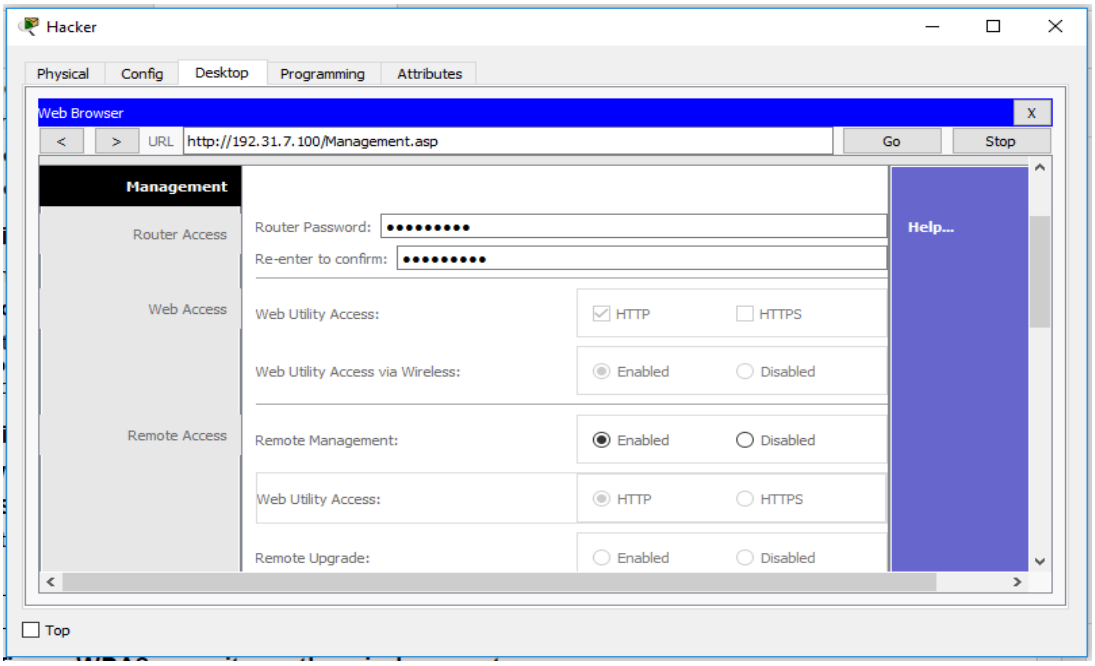
Kuva 50. Lämpötilaohjattu IoT-verkko automaattisella säädöllä [126]

Alla olevassa kuvassa 51 on kuvattu kotiverkkoa, jossa on langaton reititin sekä langallinen pöytäkone ja langattomasti toimiva kannattava tietokone. Kuvassa oikealla on esitetty verkon hakkeri, joka on yhteydessä reitittimen avulla kotiverkkoon.

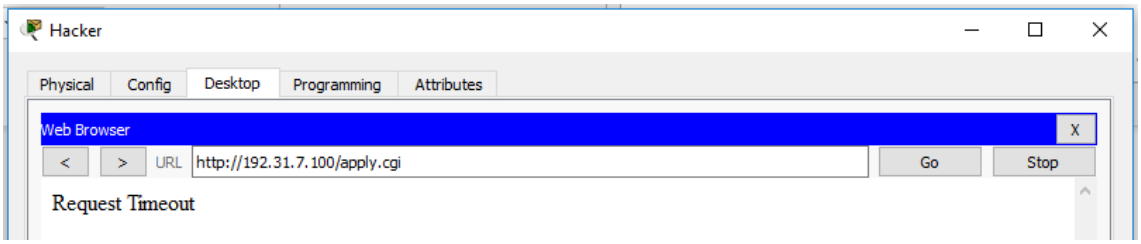


Kuva 51. Kotiverkkoa kuvaava laitehierarkia [126]

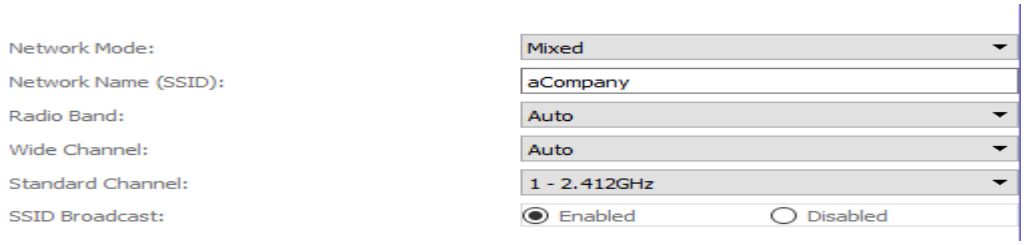
Kuvassa 52 on esitetty hakkerin hyökkäyksen kohteena oleva kuvan 49 langaton WRT300N reititin. Langattomaan reititinpalomuuriin hakkeri oli mahdollista päästä murtautumaan kuvassa 53 esitetyn etäkäyttöhallinnan (Remote Management) ollessa päällä (Enabled) ja tämän etäkäyttöhallinnan avulla hakkeri pystyy tekemään mitä tahansa murtauduttuaan verkoon admin-oikeuksin.



Kuva 52. Hakkerin (vasen ylälaita) murtautumisen kohteena oleva langaton reititin & palomuuri [126]



Kuva 53. Hakkerin muuttaessa etäkäytönhallinnan (Remote Management) [126]



Kuva 54. Verkon nimen lähettämiseen liittyvä toiminto [126]

Kuvassa 54 on esitetty langattoman verkon reitittimen nimen (SSID) lähettämiseen (SSID Broadcast) liittyvä toiminto. Valitsemalla ei käytössä (Disabled) toiminnon, joka mahdollistaa sen, että langaton verkko on piilotettuna verkkoskannausohjelmilta, kuten shodan.io ja censys.io.

Markkinoilla on useita simulointiohjelmia, joilla pystytään IoT-verkkoja simuloimaan. Esimerkkejä erilaisista maksullisista IoT-verkkojen simulointityökaluista on Iotify, MATLAB, Netsim, BevyWise IoT Simulator, Ansys IoT Simulator ja IBM Bluemix. Näiden eri simulointiohjelmien käytössä ja ominaisuuksissa on selkeitä eroja ja siksi niiden kokeiluversioihin kannattaa ensin tutustua ennen kuin harkitsee niiden lisenssien hankintaa.

Ohjeet automaatiosuunnittelijalle

Seuraavassa on esitetty suppeat ohjeet automaatiosuunnittelijan vaatimuksesta. Ohjeiden lisäksi liitteessä 1 esitettyjä taulukoita on tarpeenmukaista käydä läpi tehtäessä kartoitusta tietoturvavaatimuksista.

IoT-antureiden ja Big Dataan liittyvien tietojen tallennus

IoT-anturiverkkojen seurantaa, raportointia ja tietoturvaa varten eri anturiverkkojen ja laitetason luomat tarkistustietueet/lokit oltava mahdollista tallentaa johonkin suureen tietovarastoon, josta tietoturva ekspertit tarvittaessa tekee skannausajoja seuraa sertifikaattien ylläpitoa ja tekee rutiinitarkastuksia tai selvittelee antureihin liittyviä ongelmia.

Kodin IoT-anturit voivat tuottaa jopa yhden gigabitin verran informaatiota viikossa ja turvallisuusanturit kaivosteollisuudessa jopa 2,4 terabitin verran dataa minuutissa. Tästä syystä tiedon varastointia varten on oltava erillisiä palvelimia, jotka toimivat samalla tietovarastoina ja datapalvelimina esim. erityyppiset pilvipalveluratkaisut.

Vaadittava tietoturvataso Wise-järjestelmälle standardin 62443-3-3 ja 62443-4-1 mukaisesti

Seuraavassa esitetyt standardit on esitetty lyhennetyssä muodossa ja käytännönläheisimmin toinen toisiaan täydentäen. Katso tarkemmin liite SFS-EN 62443-3-3 ja 62443-4-1 standardien mukaiset automaation verkkoympäristön suojaustasovaatimukset ja niiden hyödyntäminen.

Taso 0: Ei vaadittua tietoturvatasoa – kytkentä toimiston DDC-järjestelmään, joka ei ole yhteydessä tehtaanohjausjärjestelmään (ICS) – käytännössä ei sallittu tietoturvataso (tai riippuu toimiston automaatiojärjestelmän tietoturvatasosta)

- Kytkentä parikaapelilla (esim. Modbus) suoraan tai Ethernet-kaapelilla (POW) Super Wise keskusyksiköstä toimiston automaatiojärjestelmään tai Swegon Connectin avulla langattomasti.

- Swegon Connect Wise-järjestelmän yhdistäminen toimiston verkkoon (ei suositella Swegonin ylläpitämää Swegon pilvipalvelua käyttöön).

Taso 1: Matala/Alhainen tietoturvataso – kytkentä toimiston DDC-järjestelmään, joka ei ole yhteydessä tehtaanohjausjärjestelmään (ICS)

- Kytkentä parikaapelilla (esim. Modbus) suoraan tai Ethernet-kaapelilla (POW) Super Wise keskusyksiköstä toimiston automaatiojärjestelmään tai Swegon Connectin avulla langattomasti.

- Swegon Connect Wise-järjestelmän yhdistäminen toimiston verkkoon (Swegonin ylläpitämää Swegon pilvipalvelua ei saa käyttöönottaa).

- Kaikkien kyseiseen järjestelmään liitettyjen laitteiden oletussalasanat ja langattoman lähiverkon verkkotunnukset (SSID:t) tulee vaihtaa.

- Vähimmäisvaatimuksena yleiset GDPR (General Data Protection Regulation) -ohjeet, joiden mukaan tietoturvan osalta myönnetään ilmainen ja helppo pääsy henkilötietoihin, jotta jokainen meistä voi helposti nähdä, millaisia henkilötietoja yrityksillä ja julkisilla viranomaisilla on meistä.

- Järjestelmän pystyttävä autentikoimaan langallisen tai langattoman verkon käyttäjät ja vahvistamaan ihmiskäyttäjät sekä salasanan vahvuudelle asetettu vahvuusvaatimus.

- Langattoman verkon tapauksessa järjestelmän tiedonsiirtoyksikkö tulee olla varustettu palomuurilla ja langattomalla reitittimellä.

- Sallittujen lähettäjien tarkastusmekanismi (Whitelisting) on oltava käytössä alatason laitteissa.

- Anturitason ja laitetason luomat tarkistustietueet/lokit oltava mahdollista tallentaa johonkin suuren datamäärän omaavaan tietopankkiin. Myös käyttäjäkohtaiset tiedot oltava mahdollista tallentaa tiedonsiirtoyksiköstä johonkin tietovarastoon.

- Järjestelmään kytköksissä olevat anturit ja laitteet tulee estää tarpeettomat toiminnot, protokollat ja palvelut, jotka saattavat olla oletusarvoisesti avoimena julkiseen Internetiin.

Taso 2: Keskitaso – kytkentä tehtaan pilvipalveluun (tai yhteydessä) tai vaihtoehtoisesti tehtaan ohjausjärjestelmään

- Kytkentä parikaapelilla/ethernet kaapelilla määriteltyyn ja sertifioituun reititin ja palomuuri yksikköön (mieluiten yhdistetty reititin ja palomuuri).

- Palomuurissa oltava käyttäjäryhmät ja salasanojen hallintatyökalu sekä reititimen SSID broadcast-toiminto oltava pois päältä. (SSID Singlecast: yksi yhteys/tietojen luovutusosoite sallittu, SSID Multicast: useampi yhteys/tietojen luovutusosoite sallittu, SSID Broadcast: lähettää tiedot kaikille)

- Kaikkien kyseiseen järjestelmään liittettyjen laitteiden oletussalasanat ja langattoman lähiverkon verkkotunnukset (SSID:t) tulee vaihtaa.

- Reittittimessä ja palomuurissa oltava VPN yhteysmahdollisuus, PSK (Pre Shred Key), RSA (public-key cryptosystem - salasanageneraattori) tai WPA2-AES (tietoturvallisin vaihtoehto) suojaustaso mobiililaitteille, NAT (Network Address Translation) työkalu ja http-etäyhteys on oltava pois käytöstä mahdollisten verkkoskannausten eliminoimiseksi (eli verkkoon liitettävien laitteiden oltava sen mallisia, joissa ei käytössä olevat vapaat etäyhteysportit voidaan poistaa käytöstä).

- Reititin ja palomuuriyhdistelmissä tehdasasetukset tarkistettava erityisesti palomuurin tila voi olla oletuksena pois päältä.

- Varmuuskopionti mahdollistettava.

Taso 3: Korkea – kytkentä tehtaan pilvipalveluun (tai yhteydessä) tai vaihtoehtoisesti tehtaan ohjausjärjestelmään

- Kytkentä parikaapelilla/ethernet kaapelilla määriteltyyn ja sertifioituun reititin ja palomuuri yksikköön (mieluiten yhdistetty reititin ja palomuuriyksikkö).

- Palomuurissa oltava käyttäjäryhmät, salasanojen hallintatyökalu, jossa backlog tiedosto vikatilanteiden varalle ja mahdollisten verkkohyökkäysten analysointiin sekä sertifikaattien hallinta- ja päivitystyökalu. Lisäksi reitittimen SSID broadcast-toiminto oltava pois päältä, ja mielellään myös multicast (jos mahdollista). (SSID Singlecast: yksi yhteys/tietojen luovutusosoite sallittu, SSID Multicast: useampi yhteys/tietojen luovutusosoite sallittu, SSID Broadcast: lähettää tiedot kaikille)

- Kaikkien kyseiseen järjestelmään liittettyjen laitteiden oletussalasanat ja langattoman lähiverkon verkkotunnukset (SSID:t) tulee vaihtaa.

- Verkkoanalysointityökalu järjestelmän suuntaan verkon luotettavuuden seurantaan.

- Reittittimessä ja palomuurissa oltava VPN yhteysmahdollisuus (mielellään OpenVPN), PSK (Pre Shared Key), RSA (public-key cryptosystem - salasanageneraattori) tai WPA2-AES (tietoturvallisin vaihtoehto) suojaustaso mobiililaitteille, NAT (Network Address Translation) työkalu ja http-etäyhteys on oltava pois käytöstä mahdollisten verkkoskannausten eliminoimiseksi (eli verkkoon liitettävien laitteiden oltava sen mallisia, joissa ei käytössä olevat vapaat etäyhteysportit voidaan poistaa käytöstä) sekä erillinen NID node switch (Network Industrial Device node switch) eli etäkäyttökytkin teollisuusverkon suntaan, jossa samassa

verkon automaattinen analysointiohjelma tai työkalu tiedon prosessointiin ja seurantaan.

- Reititin ja palomuuriyhdistelmissä tehdasasetukset tarkistettava erityisesti palomuurin tila, joka voi olla oletuksena pois päältä.

- Varmuuskopiointi ja sertifikaattien todentaminen ja hallinnointi mahdollistettava.

Taso 4: Spesifioitu – Pöyryn tietoturvaohjeita ja asiakkaan vaatimuksia tukeva

- Kaikkien järjestelmään kytkettävien laitteiden kuten Wise-järjestelmän ja järjestelmään kytkettävien laitteiden oletusetäyhteydet ja laitteiden oletussuojausasetukset ja salasanat on poistettava käytöstä ja määritettävä uudelleen vaatimuksien mukaisiksi. Esim. Super Wise II ja Swegon Gold ilmanvaihtokoneen oletusetäyhteydet ja suojausasetukset.

- Teollisuusohjausjärjestelmään liitettäessä palomuurin ja reittimen kryptisen AES suojaustason oltava vähintään 256 bittinen.

- SFS62443-4-1 mukaisten Conformance Certification listaa laitetoimittajien osalta on ensikädessä suosittava. Lista löytyy osoitteesta: isasecure.org/en-US/End-Users/ISASecure-Certified-Devices

- Laitteiden tietoturvallisuusvaatimukset on varmistettava standardin SFS62443-4-2 (valmisteilla) mukaisesti tai jollei saatavilla, niin vähimmäisvaatimuksena on parhaiden käytäntöjen kirja (löytyy osoitteesta www.iiconsortium.org/pdf/Endpoint_Security_Best_Practices_Final_Mar_2018.pdf).

Taso 5: Erityisen riskitekijän tilanteessa – Tiedonsiirtoyksiköt omina järjestelminä

- Jokainen tiedonsiirtoyksikkö (Swegon Wise) ja ilmanvaihtokone (Swegon Gold) muodostaa oman automaatiojärjestelmän, johon voi olla liitettynä esim. valaistuksenohjaus-, verhojenohjaus- ja lämmityksenohjausjärjestelmät. Pois lukien

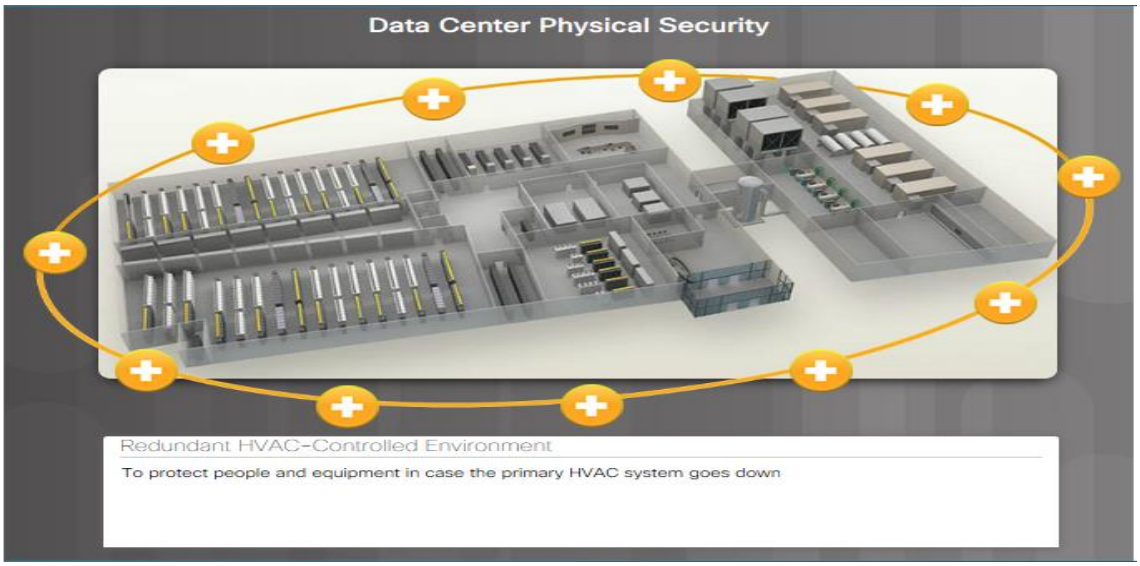
kaikki mitkä liittyvät turvallisuuteen tai teollisuusohjausjärjestelmään ei voi liittää osaksi kyseistä automaatiojärjestelmää.

- Kaikissa erillisissä automaatiojärjestelmissä oltava palomuuri reititin yhdistelmä ja verkon seuranta/analysointi sekä palomuurissa oltava käyttäjäryhmät ja salasanojen hallintatyökalu koskien vain kyseiseen ilmanvaihtokoneen ohjaustilaan liittyviä käyttäjäryhmiä. Erillisillä automaatiojärjestelmillä esim. mobiiliyhteys ja SIM-kortti tai ei verkkoyhteyttä lainkaan ja käsisäädettävät huonetermostaatit.

- Tässä tapauksessa erityisesti antureihin liittyvän Big Datan seurantaan ja tallentamiseen kannattaa kiinnittää huomiota. Eli mihin voidaan tallentaa anturiverkkojen Big Data ilman, että automaatioverkon tietoturva vaarantuu.

- Pienen IoT-anturiverkon tietoturvan analysointi on helpompaa ja nopeampaa, mutta antureiden ja muiden verkkolaitteiden tietoturvapäivitys voi olla haastavampaa ja siksi verkon kaikkien verkkolaitteiden sertifikaatit ja ohjelmistoversiot on dokumentoitava.

- Varajärjestelmän, ks. kuva 55, mahdollistaminen kriittisten toimintojen osalta, kuten valvomoissa sijaitsevien ihmisten suojaus hätätilanteessa valvomon toimiessa turvatilana.



Kuva 55. Palvelinrakennuksen fyysiseen suojaukseen kuuluu myös ihmisten ja laitteiden suojaus [1]

Esimerkkejä teollisuuden etähallintasovelluksista

Seuraavassa on esitetty esimerkit kahden eri valmistajan etähallintalaitteista Tosibox ja MB Connect Line.

Tosibox ratkaisut

Tosibox tarjoaa mm. teollisia 3g modeemeja, Tosibox Lock lukkolaitteita ja Tosibox Key avaimia sekä päätelaitetta/ohjelmistoa mobiililaitteen kautta tehtävää hallintaa varten. Yhteydenotto Tosibox laitteeseen tapahtuu kryptatun VPN yhteyden kautta, Tosibox:n ratkaisuissa käytössä on autentikointia ja hallintaa varten RSA avain sekä TLS, Blowfish 128bit ja AES 256bit suojaus. Suojausta käytetään seuraavasti:

- VPN-kryptoarkkitehtuuri PKI, 1024/2048/3072 bit RSA-avaimilla

- VPN-datasalaus Blowfish 128 bit /AES 128/192/256 bit
- VPN-kontrollikanavan salaus AES 256 bit (symmetrinen, AES-256-CBC)
- Avaintenvaihto TLS/SSL Diffie-Hellman ja asiakassertifikaatti

Sen ansiosta, että kryptaus puretaan ainoastaan lähettävässä ja vastaanottavassa laitteessa, Tosibox:n sovelluksissa verkossa liikkuu ainoastaan kryptattu data. Laitteissa on mahdollista myös kytkeä päälle offline-tila, jolloin yhteys muodostuu suoraan Tosibox latteiden välille, tällöin ulkoinen internet-yhteys ei ole käytössä eikä laitteeseen ole mahdollista muodostaa etäyhteyttä. Tosibox:n etäyhteyden ominaisuudet estävät mm. MAC ja IP osoitteiden väärentämisen ja oikein toteutettuna etäyhteyden salliminen sisäverkkoon ei muodosta tietoturvariskiä.

MB Connect Line ratkaisut

MB Connect Line tarjoaa ratkaisuja etähallintaan puhelinverkon ja internetin yli, teollisia reitittimiä sekä työkaluja ja laitteita tiedon varmuuskopiointiin ja verkon monitorointiin. Kaikkien laitteiden keskeisenä ominaisuutena on suojattu VPN yhteys eli kaikki ylläpitoon liittyvä toiminta tapahtuu VPN yhteyden kautta samaan tapaan kuin myös Tosiboxin tarjoamissa ratkaisuissa. Tämän lisäksi kaikissa laitteissa on sisäänrakennettuna palomuuriratkaisu. MB Connect Linen tuotteita on saatavilla Profibus liitännällä, sarjaporttiliitännöillä sekä tavallisella Ethernet liitännällä, tästä esimerkkinä mm. puhelinverkon yli tapahtuvaan ylläpitoon suunniteltu mbPoint laite; samainen laite voi yhteyslaitteen lisäksi toimia myös reitittimenä. Datan (asetukset yms) varmuuskopiointiin PLC-tasolla MB Connect Line tarjoaa mbSECBOX laitetta, kyseinen laite on tarkoitettu Siemens S7-300 ja S7-400 logiikoiden varmuuskopiointiin. Yhdistäminen laitteeseen etähallintaa varten tapahtuu puhelinverkon yli VPN yhteydellä. Varmuuskopioinnin lisäksi laite toimii virustutkana eli laite kykenee tunnistamaan muutokset komponenteissa ja tarjoaa suojan haittaohjelmia kuten Stuxnet vastaan ilmoittaen muutoksista ennenkuin vahinkoa on tapahtunut.

Yhteenveto

Verrattaessa Tosiboxin ja MB Connect Linen tuotteita, suurin ero toimintatavassa ovat tiedon salausmenetelmät; Tosibox käyttää RSA avaimia, jotka luodaan jokaista käyttökertaa varten uudelleen; yhteyden muodostamiseen käytetään Tosibox Key sovellusta, joten tässä suurin ero. Koska MB Connect Line ei tarjoa teknistä dataa suojauksen rakenteesta, näiden kahden vertaileminen toisiinsa tietoturvan näkökulmasta on hyvin hankalaa. Tosin molemmat laitteista täyttävät kaikki vaaditut tietoturvastandardit, joten oletettavaa on, että kumpikin tarjoaa riittävän tietoturvan.

Esimerkki tarpeenmukaisen ilmanvaihtojärjestelmän kannattavuuslaskennasta DFC- menetelmällä

Seuraavassa esimerkissä on laskettu pääkaupunkiseudulla olevan toimistorakennuksen ilmastoinnin elinkaarilaskennasta DFC-menetelmää hyödyntäen. Kyseinen esimerkki tehtiin kuvaamaan Wise-järjestelmän kannattavuutta. Sinällään ilmanvaihdon kannattavuudenlaskenta on hieman väärä termi kuvaamaan ilmanvaihtoinvestointia, koska nykyaikaiset energiamääräykset eivät salli uusien toimistokiinteistöjen painovoimaista ilmanvaihtoa ja vaihtoehtoisesti vain uusimalla vastaavanlaiseen normaalilla jatkuvalla ilmanvaihdolla toimivaan järjestelmään ei energiasäästöjä ole odotettavissa.

Tarvittavien muutostöiden (mm. kanavamuutokset, ilmanvaihtokone EC-moottorilla, päätelaitteet, anturit ja asennuskustannukset) kustannukset arvioitiin olevan 100 000 € ja automaatiokustannukset (ilmanvaihtokoneen ja EC-moottorien ohjaus, automaatiojärjestelmän uusiminen sekä huoneanturien kytkennät) 20 000 €. Vuotuiset huoltokustannukset, kuten anturien vaihdot, yms., arvioitiin olevan 2 % hankintahinnasta ja viiden vuoden välein pienempi korjaushuolto arvoltaan 5 000 € sekä 10 vuoden välein suurempi korjaushuolto (pitäen sisällään EC-moottorin vaihdon ja päivityksen rakennus automaatioon) arvoltaan 10 000 €.

Muita lähtötietoja ja olettamuksia oli seuraavat tekijät:

- Keskimääräisen ilmanvaihdon arvioidaan pienevän 40 % tarpeenmukaisella ilmanvaihdolla
- Tarkastelujakso 30 vuotta
- Korkokanta 5 %

- Investointikustannus yhteensä 120 000 €
- Lämmitysenergian hinta arvioituna 55 €/MWh ja sähkön hinta 95 €/MWh
- LTO hyötysuhde 85 %
- Käyntiaika normaalilla jatkuvailmavirtaisella järjestelmällä 24h/7vrk per viikko
- Käyntiaika tarpeenmukaisella järjestelmällä 7,5h/5vrk per viikko ja vähennettynä arkijuhlapyhät – Ei käyttöä arkijuhlapyhäpäivinä (Arkijuhlapyhien lukumäärä keskimäärin: Tammikuu 1, Huhtikuu 2, Kesäkuu 1 ja Joulukuu 4)
- Tarpeenmukaisen ilmanvaihdon ajatellaan olevan täysteholla keskimäärin 7,5 h päivässä
- Tulo- ja poistoilmavirrat ajatellaan olevan lähes yhtäsuuria, suuruudeltaan 9 m³/s
- Keskimääräisenä sisälämpötilaksi arvioitiin 22 °C ja sisäänpuhalluslämpötilaksi 20 °C sekä lämpötilannousuksi puhaltimessa 0,5 °C (EC-puhallin)
- Lisäksi ominaissähkötehoa kuvaavana SFP-lukuna pidettiin vuoden 2018 määräysten mukaisesti lukua 1,8 kW/m³.

Taulukossa 13 on kuvattu muuttujat, joita muuttamalla voidaan suorittaa helposti arvio esim. herkkyystarkastelua varten tarpeenmukaisen ilmanvaihdon kannattavuudesta.

Taulukko 13. DFC-laskennan muuttujana toimivat lähtöarvot

Keskimääräisen ilmavirran arvioidaan pienenevän tarpeenmukaisen ilmanvaihdon avulla	40	%
Tarpeenmukaisen ilmanvaihtojärjestelmän käyntiaika päivässä keskimäärin	7,5	h
LTOn hyötysuhde	85	%
Sisäänpuhalluslämpötila	20	°C
Lämpötilan nousu puhaltimessa	0,5	°C
Tuloilmamäärä	9	m³/s
Poistoilmamäärä	9	m³/s
Keskimääräinen sisälämpötila toimistokiinteistössä	22	°C
Korkokanta	5	%
Lämpöenergiahinnan reaalihinnan nousu	2	%
Sähköenergiahinnan reaalihinnan nousu	2	%
SFP-luku	1,8	kW/m³
Vuosittaiset huoltokustannukset	2	%
Korjauskustannukset 5 vuoden välein (sisäläen kanavien puhdistus ja korjauskustannukset sekä anturien ja säätöpeltien vaihtokustannukset	5000	€
Korjauskustannukset 10 vuoden välein (sisältäen EC-puhaltimien vaihdo ja automaatiopäivitykset)	10000	€

Taulukko 14. DFC laskentaa varten tehdyt laskelmat tarpeenmukaisen ja vakioilmavirtaisen ilmanvaihdon lämmitys- ja sähköenergiankulutuksen pienenemisestä

kk	Tammi	Helmi	Maalis	Huhti	Touko	Kesä	Heinä	Elo	Syys	Loka	Marras	Joulu
keskimääräinen ulkolämpötila kuukaudessa [°C]	-3,97	-4,5	-2,58	4,5	10,76	14,23	17,3	16,05	10,53	6,2	0,5	-2,19
normaalikäyntiaika h/kk	744	672	744	720	744	720	744	744	720	744	720	744
IMS normaalikäyttöpäivien lkm per kk (ei sisällä arkipyhäpäiviä)	23	20	23	22	23	22	23	23	22	23	22	23
Arkipyhäpäivien lkm keskimäärin per kuukausi	1	0	0	2	0	1	0	0	0	0	0	4
IMS käyntiaika h/kk	165	150	173	150	173	158	173	173	165	173	165	143
(EI IMS) lämmöntalteenotolla talteenotettu kuukauden keskimääräinen teho [kW]	238	243	226	161	103	71	43	55	105	145	197	222
IMS lämmöntalteenotolla talteenotettu kuukauden keskimääräinen teho [kW]	32	33	31	20	14	9	6	8	14	20	27	26
(EI IMS) lämmöntalteenottolaitteen jälkeinen lämpötila [°C]	18	18	18	19	20	21	21	21	20	20	19	18
IMS lämmöntalteenottolaitteen jälkeinen lämpötila [°C]	18	18	18	19	20	21	21	21	20	20	19	18
(EI IMS) ilmanvaihdon lämmitysenergian nettotarve [kWh]	11213	10705	9538	972	-6541	-10377	-14423	-12917	-6061	-1045	5638	9068
IMS ilmanvaihdon lämmitysenergian nettotarve [kWh]	331	320	308	25	-211	-298	-465	-417	-191	-34	178	200
Ilman lämmitysenergian nettotarpeen pieneminen vaihdettaessa IMS:iin [kWh]	10882	10385	9230	947	0	0	0	0	0	0	5460	8868
(EI IMS) ilmanvaihdon sähköenergian nettotarve [kWh]	4464	4032	4464	4320	4464	4320	4464	4464	4320	4464	4320	4464
IMS ilmanvaihdon sähköenergia nettotarve [kWh]	594	540	621	540	621	567	621	621	594	621	594	513
Sähköenergian pieneminen vaihdettaessa IMS:iin [kWh]	3870	3492	3843	3780	3843	3753	3843	3843	3726	3843	3726	3951

Taulukko 15. Yhteenveto tarpeenmukaisella ilmanvaihdolla saavutettavasta energiansäästöstä verrattuna vakioilmavirtaiseen (aina käynnissä olevaan) ilmanvaihtoon

Ilmanvaihdosta talteenotettu lämpöenergia/a	45,772088	MWh	Muutos	97 %
Sähköenergian pieneneminen/a	45,513	MWh	Muutos	87 %
Energian säästö yhteensä/a	91,285088	MWh	Muutos	92 %

Taulukko 16. DFC laskennan tulokset 30 vuoden ajanjaksolla laskettuna

						Kumulatiiviset arvot						
Vaihtoehto A. DFC-menetelmällä						Energian	Netto	Diskontattu	Lämmitysenergian	Lämmitys	Sähköenergian	Sähkön
						säästö	säästö	nettosäästö	säästö	energian hinta	säästö	hinta
vuosi	Hankinta	huolto	korjaus	automatiikka	purku	€/a	€/a	€/a	MWh/a	€/MWh	MWh/a	€/MWh
0	100000			20000		0	-120000	-120000	0	55		95
1		2000				7 118 €	5118	4874	46	56	46	97
2		2000				7 405 €	5405	4903	46	57	46	99
3		2000				7 704 €	5704	4928	46	58	46	101
4		2000				8 016 €	6016	4949	46	60	46	103
5		2000	5000			8 339 €	1339	1049	46	61	46	105
6		2000				8 676 €	6676	4982	46	62	46	107
7		2000				9 027 €	7027	4994	46	63	46	109
8		2000				9 392 €	7392	5003	46	64	46	111
9		2000				9 771 €	7771	5009	46	66	46	114
10		2000	10000			10 166 €	-1834	-1126	46	67	46	116
11		2000				10 576 €	8576	5014	46	68	46	118
12		2000				11 004 €	9004	5014	46	70	46	120
13		2000				11 448 €	9448	5011	46	71	46	123
14		2000				11 911 €	9911	5006	46	73	46	125
15		2000	5000			12 392 €	5392	2594	46	74	46	128
16		2000				12 893 €	10893	4990	46	76	46	130
17		2000				13 413 €	11413	4980	46	77	46	133
18		2000				13 955 €	11955	4968	46	79	46	136
19		2000				14 519 €	12519	4954	46	80	46	138
20		2000	10000			15 106 €	3106	1170	46	82	46	141
21		2000				15 716 €	13716	4923	46	83	46	144
22		2000				16 351 €	14351	4906	46	85	46	147
23		2000				17 011 €	15011	4887	46	87	46	150
24		2000				17 699 €	15699	4868	46	88	46	153
25		2000	5000			18 414 €	11414	3370	46	90	46	156
26		2000				19 158 €	17158	4825	46	92	46	159
27		2000				19 932 €	17932	4803	46	94	46	162
28		2000				20 737 €	18737	4780	46	96	46	165
29		2000				21 575 €	19575	4756	46	98	46	169
30		2000	10000			22 446 €	10446	2417	46	100	46	172
Yhteensä	100000	60000	45000	20000	0	401 867 €	176867	7799				

Taulukossa 16 on esitetty DFC-laskennalla saavutettu laskelma. Laskelmasta ei näy takaisinmaksuaikaa, koska aikajakso 30 vuotta on liian pitkä, mutta tällä laskentamallilla takaisinmaksuajaksi saatiin 30 vuotta, jonka aikana tarpeenmukainen ilmanvaihto maksaa itsensä takaisin saavutettavien energiansäästökustannuksien avulla. Laskelma on vain karkea malli eikä ota huomioon vakioilmavirtaisen järjestelmän mahdollisia ei käyntiaikoja. Lisäksi karkeasti arvioitu 7,5 h päivittäinen käyttöaika ei todellisuudessa ole pysyvä, mutta ottaa huomioon tavallaan myös mahdolliset huonetilan ei aktiivisen käytön, kuten Swegonin uuden sukupolven Wise-järjestelmä.

VOC-yhdisteiden vaikutus toimistojen sisäilman laatuun

Seuraavissa taulukoissa 17-26 on esitetty Työterveyslaitoksen mittaamia yleisiä VOC aineyhdisteitä ja pitoisuuksia, joita esiintyy yleisimmin toimistokiinteistöissä. VOC arvot ovat yksittäisiä aineyhdistepitoisuuksia ja TVOC arvot ovat kaikkien sisäilmassa esiintyvien VOC aineyhdisteiden keskiarvoa kuvaava luku. Yleisesti ottaen TVOC-arvot perustuvat näennäiseen viitearvoon ja suositusarvoihin, eikä niille ole määritelty tarkkaa yläarajaa.

Taulukko 17. Aromaattisiin hiilivetyihin kuuluvien VOC-yhdisteiden mahdollisia päästölähteitä ja ohje-, viite- ja suositusarvoja [106]

Kemiallinen ryhmä ja yleisimmät VOC-yhdisteet kyseisessä ryhmässä	Esimerkkejä mahdollisista päästölähteistä	Ohjearvo 1: tavoitearvo (yksittäiselle yhdisteelle)	Ohjearvo 2: toimenpidearvo (yksittäiselle yhdisteelle)	Kokonaisviitearvo (TVOC)	Suositusarvo (TVOC)
Aromaattiset hiilivedyt					
Tolueeni	Maalit, lakat, liimat, pakokaasut, bensiini, liottimet, seinäpinnoitteet, polyuretaanit, puhdistusaineet, tietokoneet, tulostimet, kopiokoneet	Ohjearvo 1: 2 µg/m³ (Saksan ympäristöministeriö)	Ohjearvo 2: 20 µg/m³ (Saksan ympäristöministeriö)	> 250 µg/m³ (ISO 16017-2, 16000-6)	300 µg/m³ (European Community 1995)
Ksyleenit (p, m)					
Ksyleeni (o)					
1,2,4-Trimetyylibentseeni					
Bentseeni	Maalit, lakat, liimat, pakokaasut, bensiini, liottimet, seinäpinnoitteet, polyuretaanit, puhdistusaineet, tietokoneet, tulostimet, kopiokoneet, tupakointi, synteettiset kuidut				
Etyylibentseeni	Pakokaasut, bensiini, tupakointi, eristeet, tulostimet, tietokoneet, kopiokoneet, linoleum				

Taulukko 18. Alkoholeihin kuuluvien VOC-yhdisteiden mahdollisia päästölähteitä ja ohje-, viite- ja suositusarvoja [106]

Kemiallinen ryhmä ja yleisimmät VOC-yhdisteet kyseisessä ryhmässä	Esimerkkejä mahdollisista päästölähteistä	Viite-/Suositusarvo (yksittäiselle yhdisteelle)	Ohjearvo (yksittäiselle yhdisteelle)	Kokonaisviitearvo (TVOC)	Suositusarvo (TVOC)
Alkoholit					
1-Butanoli	Liottimet, puhdistusaineet, maalit, liimat, tasoitteet, laastit, kosmetiikkatuotteet, kuitulevyt	Kohonnut > 5 µg/m³ (Salonen 2008)	Ohjearvo 1 (tavoitearvo): 2 µg/m³ ja Ohjearvo 2 (toimenpidearvo): 20 µg/m³ (Saksan ympäristöministeriö)	> 250 µg/m³ (ISO 16017-2, 16000-6)	300 µg/m³ (European Community 1995)
2-Etyyli-1-heksanoli	Muovimatot, liimat, tulostimet, kopiokoneet				
2-Metyyli-1-propanoli	Puun uuteaineet, liuottimet, puhdistusaineet, maalit, liimat, tasoitteet, laastit, pehmitinaineet				
Fenoli	Liuottimet, puhdistusaineet, maalit, liimat, tasoitteet, laastit, tietokoneet, tupakointi, PVC-pohjaiset pinnoitteet				

Taulukko 19. Alifaattisiin hiilivetyihin kuuluvien VOC-yhdisteiden mahdollisia päästölähteitä ja ohje-, viite- ja suositusarvoja [106]

Kemiallinen ryhmä ja yleisimmät VOC-yhdisteet kyseisessä ryhmässä	Esimerkkejä mahdollisista päästölähteistä	Viite-/Suositusarvo (yksittäiselle yhdisteelle)	Ohjearvo (yksittäiselle yhdisteelle)	Kokonaisviitearvo (TVOC)	Suositusarvo (TVOC)
Alifaattiset hiilivedyt					
Tetradekaani	Maalit, liimat, bensiini, palamislähteet, tiivisteet, kopiokoneet, tietokoneet, linoleum, kosmetiikkatuotteet	Kohonnut > 5 µg/m³ (Salonen 2008)	Ohjearvo 1 (tavoitearvo): 2 µg/m³ ja Ohjearvo 2 (toimenpidearvo): 20 µg/m³ (Saksan ympäristöministeriö)	> 250 µg/m³ (ISO 16017-2, 16000-6)	300 µg/m³ (European Community 1995)
Pentadekaani					
Dodekaani					
Nonaani					
Undekaani					
Heksadekaani	Maalit, liimat, bensiini, palamislähteet, tiivisteet, kopiokoneet, tietokoneet,				
Tridekaani					
Dekaani	Maalit, liimat, bensiini, palamislähteet, tiivisteet, kopiokoneet, tietokoneet, linoleum, kosmetiikkatuotteet, puun uuteaineet, tekstiilit				
Heptaani	Liimat, bensiini, pakokaasut, liottimet, polyuretaani, seinä/lattiapäälysteet, kopiokoneet, linoleum				
Oktaani	Liimat, bensiini, pakokaasut, liottimet, polyuretaani, painetut puutuotteet, puhdistusaineet, kopiokoneet, linoleum				
Heksaani	Liimat, bensiini, pakokaasut, liottimet, polyuretaani				

Taulukko 20. Aldehydeihin kuuluvien VOC-yhdisteiden mahdollisia päästölähteitä ja ohje-, viite- ja suositusarvoja [106]

Kemiallinen ryhmä ja yleisimmät VOC-yhdisteet kyseisessä ryhmässä	Esimerkkejä mahdollisista päästölähteistä	Viite-/Suositusarvo (yksittäiselle yhdisteelle)	Ohjearvo (yksittäiselle yhdisteelle)	Kokonaisviitearvo (TVOC)	Suositusarvo (TVOC)
Aldehydit					
Nonanaali	Puutuotteet, lastulevyt, tapetit, lattiavahat, hajusteet, linoleum, kostea mineraalivilla, tietokoneet	Kohonnut > 5 µg/m³ (Salonen 2008)	Ohjearvo 1 (tavoitearvo): 2 µg/m³ ja Ohjearvo 2 (toimenpidearvo): 20 µg/m³ (Saksan ympäristöministeriö)	> 250 µg/m³ (ISO 16017-2, 16000-6)	300 µg/m³ (European Community 1995)
Oktanaali					
Pentanaali					
Bentsaldehydi	Pakokaasut, lastu- ja kuitulevyt, värit, hajusteet, tietokoneet, linoleum				
Dekanaali	Tasoiteaineet, betonit, maalituotteet, lattiapäällysteet (linoleum, PVC-matot), liimat, puupohjaiset rakennusmateriaalit, kuitulevyt, tietokoneet				
Heksanaali	Puutuotteet, lastulevyt, tapetit, lattiavahat, hajusteet, linoleum, kostea mineraalivilla, kopiokoneet, hartsit, vesieristeet				
2-Furfuraali	Tasoiteaineet, betonit, maalituotteet, lattiapäällysteet (linoleum, PVC-matot), liimat, kuitulevyt, mineraalivilla				
Formaldehydi	Puutuotteet, eristemateriaalit, kulutustuotteet, pintakäsittelyaineet, kankaat, tupakointi, toimistolaitteet, otsonin ja terpeenin reaktiot				

Taulukko 21. Glykoli/glykolieettereihin kuuluvien VOC-yhdisteiden mahdollisia päästölähteitä ja ohje-, viite- ja suositusarvoja [106]

Kemiallinen ryhmä ja yleisimmät VOC-yhdisteet kyseisessä ryhmässä	Esimerkkejä mahdollisista päästölähteistä	Viite-/Suositusarvo (yksittäiselle yhdisteelle)	Ohjearvo (yksittäiselle yhdisteelle)	Kokonaisviitearvo (TVOC)	Suositusarvo (TVOC)
Glykoli/glykolieetteri					
1,2-Propanidioli	Vesiohenteiset maalit, lakat, PVC-päällysteiset lattiamateriaalit, liimat, korkkimatot, tasoitteet, vedeneristemassat, laastit, vahat, vahanpoistoaineet, pesuaineet	Kohonnut > 5 µg/m³ (Salonen 2008)	Ohjearvo 1 (tavoitearvo): 2 µg/m³ ja Ohjearvo 2 (toimenpidearvo): 20 µg/m³ (Saksan ympäristöministeriö)	> 250 µg/m³ (ISO 16017-2, 16000-6)	300 µg/m³ (European Community 1995)
2-Fenoksietanoli	Liuotinpesuaineet, hajuvedet, liimat, pehmitinaineet, kittausaineet				
2-(2-Butoksietoksi)etenoli	Puhdistusaineet, pesuaineet, maalit, värit, musteet, kittausaineet				
1-Metoksi-2-propanoli	Lattialiimat, vesiohenteiset maalit ja lakat, pehmitinaineet				
2-(2-Etoksietoksi)etanoli	Mattoliimat, pehmitinaineet, vesiohenteiset maalit, lattiavahat, vahanpoistoaineet, kittausaineet				

Taulukko 22. Terpeeneihin kuuluvien VOC-yhdisteiden mahdollisia päästölähteitä ja ohje-, viite- ja suositusarvoja [106]

Kemiallinen ryhmä ja yleisimmät VOC-yhdisteet kyseisessä ryhmässä	Esimerkkejä mahdollisista päästölähteistä	Viite-/Suositusarvo (yksittäiselle yhdisteelle)	Ohjearvo (yksittäiselle yhdisteelle)	Kokonaisviitearvo (TVOC)	Suositusarvo
Terpeenit					
Alfa-pineeni	Puu- ja puupohjaiset materiaalit, hajusteet, maalit, liuottimet, siivousaineet, kosmetiikkatuotteet, tietokoneet, ilmanraikastimet	Kohonnut > 10 µg/m³ (Salonen 2008)	Ohjearvo 1 (tavoitearvo): 2 µg/m³ ja Ohjearvo 2 (toimenpidearvo): 20 µg/m³ (Saksan ympäristöministeriö)	> 250 µg/m³ (ISO 16017-2, 16000-6)	300 µg/m³ (European Community 1995)
Limoneeni					
3-Kareeni	Puu- ja puupohjaiset materiaalit, hajusteet, maalit, liuottimet, siivousaineet				

Taulukko 23. Pii yhdisteisiin kuuluvien VOC-yhdisteiden mahdollisia päästölähteitä ja ohje-, viite- ja suositusarvoja [106]

Kemiallinen ryhmä ja yleisimmät VOC-yhdisteet kyseisessä ryhmässä	Esimerkkejä mahdollisista päästölähteistä	Viite-/Suositusarvo (yksittäiselle yhdisteelle)	Ohjearvo (yksittäiselle yhdisteelle)	Kokonaisviitearvo (TVOC)	Suositusarvo (TVOC)
Pii yhdisteet					
Dekameetyylisyklo-pentasiloksaani	Kosmetiikkatuotteet, saumausaineet, kosteuseristeet, tekstiilien lianhyljintäpinnoitteet, laastit	Kohonnut > 5 µg/m³ (Salonen 2008)	Ohjearvo 1 (tavoitearvo): 2 µg/m³ ja Ohjearvo 2 (toimenpidearvo): 20 µg/m³ (Saksan ympäristöministeriö)	> 250 µg/m³ (ISO 16017-2, 16000-6)	300 µg/m³ (European Community 1995)
Orgaaniset piiyhdisteet	Rakennusmateriaalit, tiivistemassat, siivousaineet, pintojen käsitelyaineet, hiuslakat				

Taulukko 24. Orgaanisiin happoihin kuuluvien VOC-yhdisteiden mahdollisia päästölähteitä ja ohje-, viite- ja suositusarvoja [106]

Kemiallinen ryhmä ja yleisimmät VOC-yhdisteet kyseisessä ryhmässä	Esimerkkejä mahdollisista päästölähteistä	Viite-/Suositusarvo (yksittäiselle yhdisteelle)	Ohjearvo (yksittäiselle yhdisteelle)	Kokonaisviitearvo (TVOC)	Suositusarvo (TVOC)
Orgaaniset hapot					
Heksaanihappo	Linoleum, hartsit, liotinohenteinen maali (alkydimaali), mäntylauta (puun uuteaineet), lastulevy	Kohonnut > 10 µg/m³ (Salonen 2008)	Ohjearvo 1 (tavoitearvo): 2 µg/m³ ja Ohjearvo 2 (toimenpidearvo): 20 µg/m³ (Saksan ympäristöministeriö)	> 250 µg/m³ (ISO 16017-2, 16000-6)	300 µg/m³ (European Community 1995)
Etikkahappo	Tiivistemassat, kittausaineet, linoleum, liimat				
Pentaanihappo	Linoleum, puun uuteaineet, hartsit				
Propaanihappo	Linoleum				

Taulukko 25. Estereihin kuuluvien VOC-yhdisteiden mahdollisia päästölähteitä ja ohje-, viite- ja suositusarvoja [106]

Kemiallinen ryhmä ja yleisimmät VOC-yhdisteet kyseisessä ryhmässä	Esimerkkejä mahdollisista päästölähteistä	Viite-/Suositusarvo (yksittäiselle yhdisteelle)	Ohjearvo (yksittäiselle yhdisteelle)	Kokonaisviitearvo (TVOC)	Suositusarvo (TVOC)
Esterit					
n-Butyyliasetaatti	Muovit, kuidut, maalit, lakat, liimat (liottimina), kosmetiikkatuotteet, kittausaineet	Kohonnut > 10 µg/m³ (Salonen 2008)	Ohjearvo 1 (tavoitearvo): 2 µg/m³ ja Ohjearvo 2 (toimenpidearvo): 20 µg/m³ (Saksan ympäristöministeriö)	> 250 µg/m³ (ISO 16017-2, 16000-6)	300 µg/m³ (European Community 1995)
2-(2-Butoksietoksi)etyyli-asetaatti					
Etyyliasetaatti	Liimat, korjauskynät, siivousaineet, kosmetiikkatuotteet, homeet, tiivisteaineet, kittausaineet				
2,2,4-Trimetyyli-pentanedioli-isobutyraatti, TXIB	Muovimatot, lattialiimat, pehmitinaineet, apuaineet, tapetit, maalit, keinonahkatuotteet				

Taulukko 26. Ketoneihin kuuluvien VOC-yhdisteiden mahdollisia päästölähteitä ja ohje-, viite- ja suositusarvoja [106]

Kemiallinen ryhmä ja yleisimmät VOC-yhdisteet kyseisessä ryhmässä	Esimerkkejä mahdollisista päästölähteistä	Viite-/Suositusarvo (yksittäiselle yhdisteelle)	Ohjearvo (yksittäiselle yhdisteelle)	Kokonaisviitearvo (TVOC)	Suositusarvo (TVOC)
Ketonit					
2-Butanoli	Liottimet, puun uuteaineet, hartsit, liimat, kuitulevyt	Kohonnut > 5 µg/m³ (Salonen 2008)	Ohjearvo 1 (tavoitearvo): 2 µg/m³ ja Ohjearvo 2 (toimenpidearvo): 20 µg/m³ (Saksan ympäristöministeriö)	> 250 µg/m³ (ISO 16017-2, 16000-6)	300 µg/m³ (European Community 1995)
6-Metyyli-5-hepten-2-oni	Liottimet, puun uuteaineet, hartsit, liimat, kuitulevyt, kittausaineet, mineraalivilla				