Antero Natunen

VIRTUALISOITUJEN AUTOMAATIOJÄRJESTELMIEN AUDITOINTI

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Sähkö- ja automaatiotekniikan tutkinto

2023

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä/Tekijät	Antero Natunen
Työn nimi	Virtualisoitujen automaatiojärjestelmien auditointi
Toimeksiantaja	Honeywell Oy
Vuosi	2023
Sivut	52 sivua, liitteitä 0 sivua
Työn ohjaaja(t)	Kalle Pesonen

TIIVISTELMÄ

Honeywell-automaatiojärjestelmien toimitusketjuissa on havaittu kehitettävää, jolloin tarve sisäiselle auditoinnille on konkretisoitunut. Tässä opinnäytetyössä tuodaan esille havaintoja Honeywell Oy:n virtualisoiduista automaatiojärjestelmistä projektien loppuvaiheissa, ennen varsinaista FAT-testausta sisäisen auditoinnin avulla. Esille tulleita löydöksiä tutkittiin tätä varten perustetussa asiantuntijatyöryhmässä ns. projektinhäntien perusteella. Osa-alueet, joita tässä työssä tutkitaan, ovat virtualisointi, verkko/FTE, palvelimet, PMD-tarkastukset, varmuuskopiot sekä erilaiset projektikohtaiset asiat. Jokaiselle osa-alueelle nimettiin vastuuhenkilöt, joiden kanssa läpikäytiin auditoinnin tuloksia ja tehtiin havaintoja. Automaatiojärjestelmän auditoinnin pohjana käytettiin osa-alueittain luotuja tarkistuslistoja. Auditoinnin tavoitteena on lyhentää FAT-testaukseen kuluvaa aikaa tulevissa projekteissa.

Opinnäytetyössä läpikäydään myös Honeywell Experion PMD-automaatiojärjestelmän rakenne ja sen yhdistäminen virtuaaliseen ympäristöön. Työtä on tarkoitus hyödyntää tukena projekteissa sekä uusien työntekijöiden koulutusmateriaalina virtualisoitujen automaatiojärjestelmien kanssa työskenneltäessä Honeywell Oy:ssä. Työssä esiintyviä tuloksia vertaillaan seuraavan automaatiojärjestelmän auditoinnin yhteydessä. Lopuksi työssä pohditaan lyhyesti virtualisoitujen automaatiojärjestelmien tulevaisuudennäkymiä Honeywell Oy:ssä.

Auditointi tehtiin tutkittavaan automaatiojärjestelmään viikolla 39 Honeywellin tuotantotiloissa. Tutkittavan järjestelmän laajuudesta johtuen tähän varattu aika ei riittänyt kaikkien osa-alueiden tutkimuksiin, ja Experion PKS server client osioon liittyvät tarkastukset jäi pois tästä työstä. Auditoinnilla saavutettiin sille asetetut tavoitteet.

Asiasanat: DCS, automaatiojärjestelmä, virtualisointi, auditointi

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author (authors)	Antero Natunen
Thesis title	Virtualization automation system auditing
Commissioned by	Honeywell Oy
Time	2023
Pages	52 pages, 0 pages of appendices
Supervisor	Kalle Pesonen

ABSTRACT

In the supply chains of Honeywell automation systems, improvements have been found and the need for internal auditing has become concrete. In this thesis, findings from Honeywell Oy's virtualized automation systems in the final stages of projects, before the actual FAT testing with the help of internal auditing, are brought to the fore. The findings that came up were examined in the expert working group established for this purpose. Areas explored in this work included virtualization, network/FTE, servers, PMD-checks, backups, and all project-specific issues. Persons in charge were named for each sub-area, the audit results were reviewed and observations were made. The audit of the automation system was based on checklists created by each sub-area. The purpose of the audit was to shorten the time required for FAT testing in future projects.

The thesis also reviewed the structure of the Honeywell Experion PMD automation system and its connection to the virtual environment. The work is intended to be utilized in projects as training material for new employees with virtualized automation systems while working at Honeywell Oy. The results of the work will be compared in connection with the next automation system audit. Finally, the thesis briefly considered the future visions of virtualized automation systems at Honeywell Oy.

The audit was performed on the automation system under investigation in week 39 at Honeywell's production facilities. Due to the scope of the system to be examined, the time allotted for this did not allow for examinations of sub-areas, and inspections related to the Experion PKS server client section were left out of this work. The goals set for the audit were achieved.

Keywords: DCS, automation system, virtualization, auditing

SISÄLLYS

Lyhenteet ja määritelmät

AD1, AD2 Active directory, Windows-toimialueen verkko-ohjaimet

Anti Virus Server Honeywell virustorjunnan jakelijapalvelin

API Application programming interfaces, palvelusopimus käyttöliittymien ja sovellusliittymien välillä

CIM Common Information Model, avoin standardi, joka määrittelee, kuinka laskentaresurssit ovat edustettuna

DCOM Distributed component object model, Microsoftin patentoima tekniikka viestintään ohjelmistojen välillä

DCS Distributed control system, hajautettu ohjausjärjestelmä

DCUI Direct console user interface**,** käyttöliittymä, joka mahdollistaa isäntäkoneen kanssa kommunikoinnin tekstipohjaisten valikoiden avulla

DM Design module Honeywell sovellusasema

DMZ Demilitarized zone, demilitarisoitu taso

Domain Toimialue

EBR Experion backup and restore, Honeywell Experion varmuuskopiointijärjestelmä

ESXi Host Esxi-isäntäkone

FAT Factory acceptance test, automaatiojärjestelmään liittyvien laitteiden ja toimintojen testaus asiakkaan kanssa ennen toimitusta

FCE/FC Honeywell-prosessinohjaimet

FTE Fault tolerant ethernet, kahdennettu vikasietoinen-Ethernet verkko

GTAC Global technical assistance center, Honeywellin asiantuntijatyöryhmä teknisille ongelmille

HM Human machine interface, Honeywell-käyttöliittymä prosessinohjaukseen

HTML Hypertext markup language, hypertekstimerkintäkieli, joka mahdollistaa internetistä haetun materiaalin näyttämisen

I/O Input/output, järjestelmän lähettämä ja vastaanotettava data

IP Internet protocol, internet-protokolla, joka identifioi laitteen tai verkon internetissä

IP Multicast IP-monilähetysmuoto

ISA/IEC 62443 Kyberturvallisuutta käsittelevä kansainvälinen standardi

Management Host Hallintapalvelin

MES Manufacturing execution systems, reaaliaikainen tuotannonseurantajärjestelmä

NAS Network-attached storage, ulkoinen tiedontallennuspalvelin

NTP Network time protocol, verkkoprotokolla ajan synkronointiin

OPC-UA OPC Unified architecture**,** OPC Foundationin kehittämä viestintäprotokolla

PMD Honeywellin lanseeraama automaatiojärjestelmä

PHD Honeywell prosessihistoriadatan keräyspalvelin

PC Personal computer, henkilökohtainen tietokone

RDP Remote desktop protocol, Microsoftin kehittämä etätyöpöytäprotokolla

Relay Node Honeywell etäpalvelukeskuksen välityspalvelin

RHS Honeywell-etäyhteyspalvelin

SAT Site acceptance test, laitteiden testaus toimituksen ja asennusten jälkeen tehtaalla

Service Node Honeywell-käyttöjärjestelmäpäivityspalvelin

TCP/IP Transmission control protocol/internet protocol, viestintäprotokolla verkkolaitteiden yhdistämiseen internetissä

UDP/IP User datagram protocol/internet protocol, yhteydetön tietoprotokollla

UPLINK portti Portti joka yhdistää virtuaalisen kytkimen fyysiseen kytkimeen

vCenter Vmwaren hallintaohjelma virtuaalikoneille

vSphere Vmwaren pilvipalveluiden virtualisointialusta

WAN Wide-area network**,** teknologia joka yhdistää datakeskuksen, pilvisovellukset ja pilvitallennustilan

VMM Virtual machine monitor, Virtuaalikoneen toteutusympäristö

VPN Virtual private network, Suojattu verkkoyhteys

WLAN Wireless LAN, langaton verkko

WSUS Windows server update services, Windows-käyttöjärjestelmäpäivitys

1 JOHDANTO

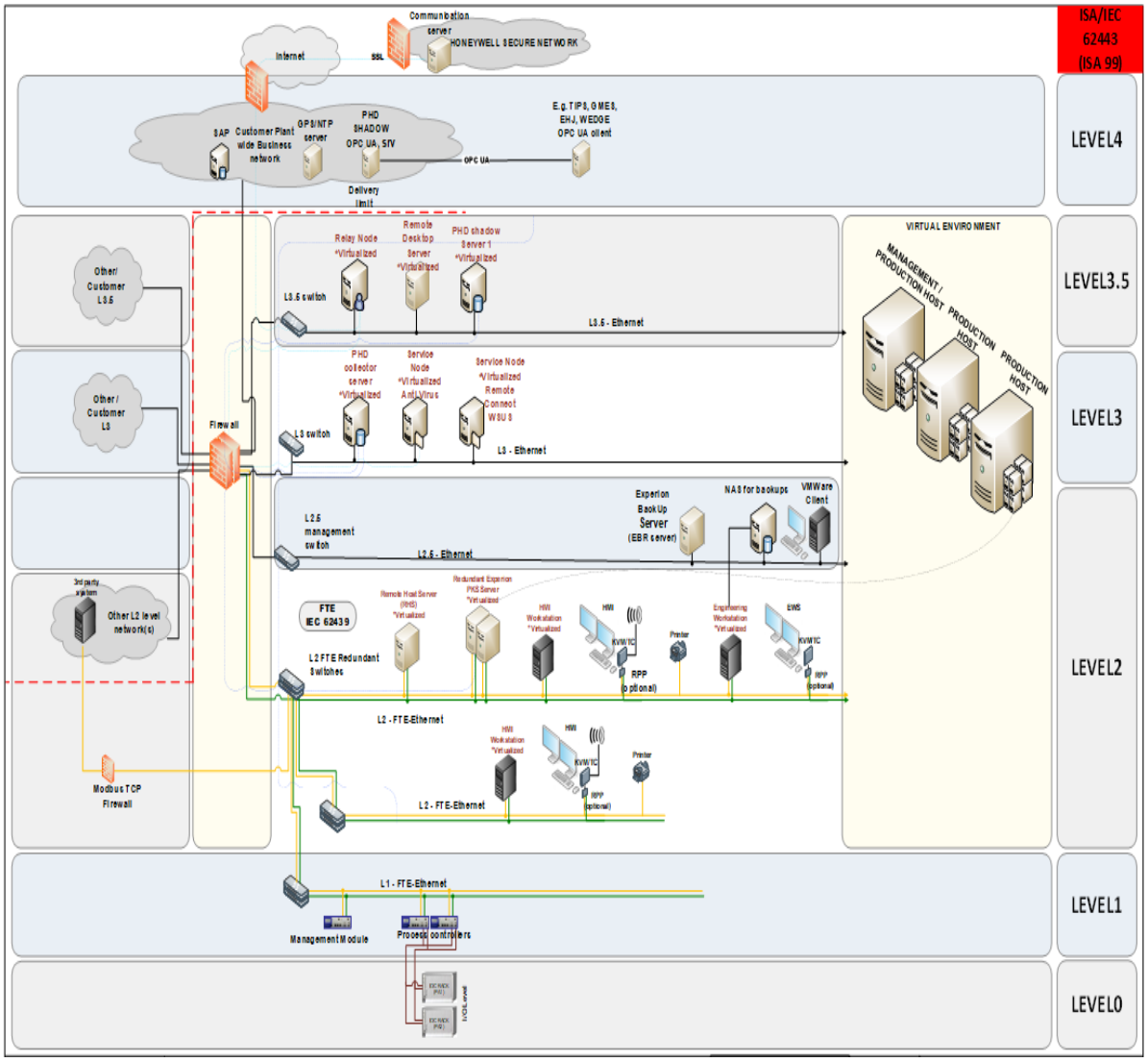
Viimeisten kolmen vuosikymmenen aikana DCS- (Distributed control system) järjestelmät ovat siirtyneet vähitellen myyjien omistuksesta ohjelmistoihin ja laitteisiin, jotka ovat jo olemassa ja ne ovat saatavilla kaupallisista lähteistä. Tähän syynä ovat kustannuksien pienentäminen, joustavuuden lisääminen, ylläpidon helpottuminen sekä suorituskyvyn parantaminen. Perinteisillä hajautetuilla DCS-järjestelmillä on omat verkot ja näin ollen rajoitettu yhteys ulkoisiin järjestelmiin. Kaupallisiin lähteisiin siirtyminen mahdollistaa DCS-järjestelmän liikuttaa tietoa ulkoisiin järjestelmiin yleensä ilman räätälöintiä tai ohjelmointia. Ainoastaan ohjainlaitteet käyttävät omistusoikeudellista teknologiaa niiden redundanssi- ja aikatarpeeseen. Ylläluetun aikaikkunan suuntauksena oli yhdistää kaikki laitteet internetissä, riippuen siitä oliko laitteet toimistotasolla vai yritystasolla. Tästä johtuen ei muodostu vyöhykkeitä tai erillisiä verkkotasoja ja verkon turvallisuudesta tulee kriittinen. (Experion PMD Network & Cyber Security 2020, 4.)

Kyberturvallisuus onkin nykyaikaisissa DCS-järjestelmissä merkittävässä roolissa niin kuin järjestelmän luotettavuus, eheys ja turvallisuuskin. Kyberhyökkäyksen seuraukset DCS-järjestelmässä voivat olla vaaraksi terveydelle, ympäristölle ja tuotteelle. Näistä voi aiheutua suuria taloudellisia menetyksiä yritykselle ja infralle. Honeywell Experion PMD -verkkoympäristö onkin jaettu useammalle vyöhyketasolle mitä perinteinen DCS-järjestelmä. Näistä tasoista jokaiselle on omat turvallisuusvaatimukset. Honeywellin Experion PMD-järjestelmä on suunniteltu kattamaan kaikki nykypäivän haasteet ja samalla järjestelmän toimintaa tukevat helpot huolto- ja päivityspolut. (Experion PMD Network & Cyber Security 2020, 4.)

Työssä havainnoidaan Honeywellin virtuaalisen automaatiojärjestelmän ongelmakohtia laitteiston toimituksen yhteydessä, siinä ilmenneiden parannettavien löydösten osalta sisäisen auditoinnin avulla sekä analysoidaan, korjataan ja esitetään parannusehdotuksia. Lisäksi tässä työssä käydään läpi Honeywell Experion PMD-järjestelmän rakenne I/O-tasolta yritystasolle sekä pohditaan yleisesti virtuaalisten automaatiojärjestelmien tulevaisuudennäkymiä ja niihin liittyviä haasteita.

2 EXPERION PMD-VERKKOYMPÄRISTÖN TASOT

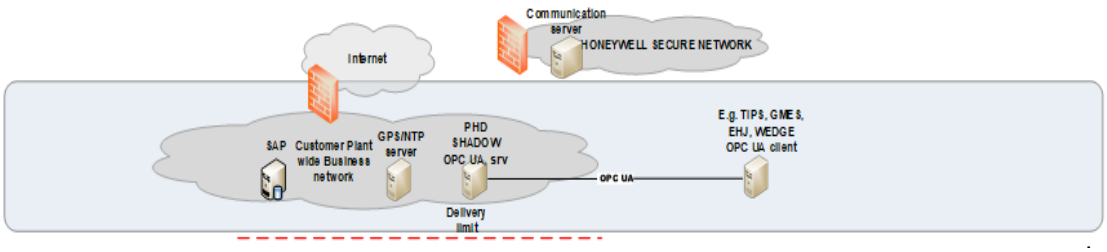
Automaatiojärjestelmissä käytetään yleisesti ISA/IEC 62443 -standardia *(Zurfluh, 2020)*. Tähän standardiin pohjautuen Honeywell PMD -automaatiojärjestelmä sisältää myös lisätasoja, jotka lisäävät tietoturvaa. Nämä tasot ovat 2.1, 2.5 ja 3.5. Kaikki PMD-verkkoympäristöön kuuluvat tasot erotetaan toisistaan palomuuurin avulla joka kuitenkaan ei ole suoraan yhteydessä internetiin. Tässä osiossa esitellään Honeywell Experion PMD -järjestelmä toimistotasolta I/O-tasolle (Kuva 1). Osiossa myös läpikäydään järjestelmän toimintaan oleellisesti vaikuttavia komponentteja sekä toimintaa yleisellä tasolla. (Experion PMD Network & Cyber Security 2020, 8.)



Kuva 1. PMD Experion -verkkoympäristön vyöhyketasot (Experion PMD Network & Cyper Security 2020, 9)

2.1 Taso 4, Yritys- ja toimistotaso

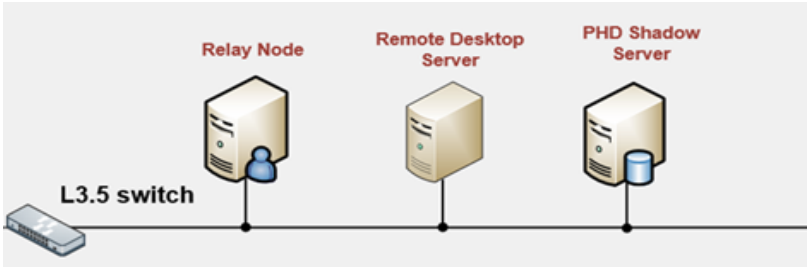
Tasolla sijaitsevat Honeywellin MES (Manufacturing execution systems)-palvelimet ja PHD(Process history data) Shadow-palvelin 2 (Kuva 2). MES-palvelimia käytetään tuotannonhallinnan seuraamiseen ja optimointiin. PHD Shadow palvelin mahdollistaa toimistotason autentikoitujen käyttäjien päästä katsomaan DCS-järjestelmän dataa DMZ (Demilitarized)-tason 3.5 läpi sekä siirtämään sitä pilvipalveluihin. Tason 4 laitteiden ei tarvitse tietää alempien tasojen IP-osoitteita tai käyttäjänimiä. Tasolla tuetaan NTP-protokollaa, ja se on yhdistetty internetiin erillisen palomuurin kautta. (Experion PMD Network & Cyber Security 2020, 9–10.)



Kuva 2. Tason 4 rakenne (Experion PMD Network & Cyper security 2020, 9)

2.2 Taso 3.5, DMZ

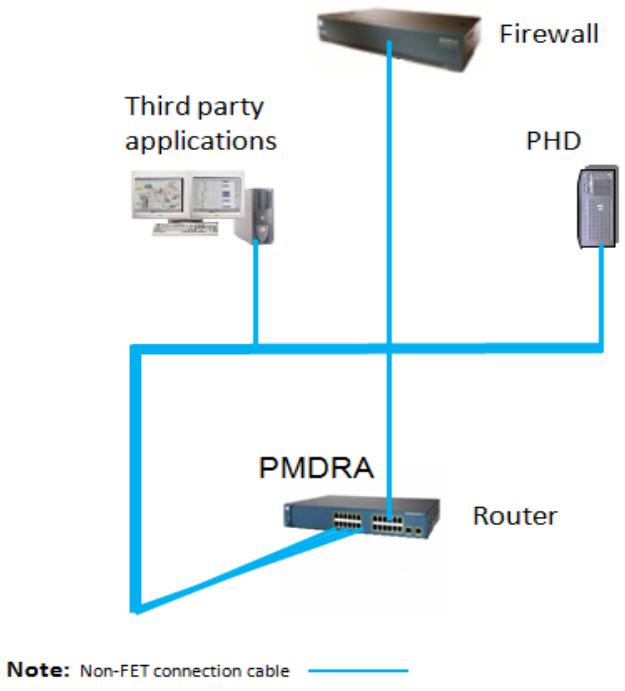
Tasolla 3.5 sijaitsee internetistä erotettu demilitarisoitu taso. Käytetään aliverkkona ja ylimääräisenä tasona, joka parantaa verkkoympäristön turvallisuutta. Tämä taso voidaankin ajatella fyysisenä erottimena tasojen 3 ja 4 välissä. Automaatioverkko eristetään toimistoverkosta tällä tasolla, jolloin näiden välillä ei ole suoraa yhteyttä. Tällä tasolla sijaitsee myös Relay Node -välityspalvelin ja PHD Shadow -palvelin (Kuva 3) . Välityspalvelinta tarvitaan, jotta saadaan yhteys Honeywellin etäpalvelukeskukseen, jonka kautta saadaan viimeisimmät testatut WSUS –(Windows server update services) ja antiviruspäivitykset järjestelmään. (Experion PMD Network & Cyber Security 2020, 10.)



Kuva 3. Tason 3.5 rakenne (Experion PMD Network & Cyper security 2020, 10).

2.3 Taso 3, Raportointi ja tiedonkeruu

Sisältää PHD-palvelimen, joka kerää DCS-järjestelmän prosessidataa tason 2 alapuolelta. PHD-palvelin välittää prosessidatan määritellyltä aikaväliltä valituilta laitteilta toimistotasolle 4. Tällä tasolla ylläpidetään Honeywellin Experion PMD-järjestelmän tärkeitä toimintoja. Anti Virus -palvelin ja Service Node WSUS -palvelin jakavat Relay Node -välityspalvelimelta saatuja testattuja ja hyväksyttyjä virus- ja käyttöjärjestelmäpäivityksiä. Kuvassa 4 näkyvä tason 3 reititin on kytketty tason 4 reitittimeen oman palomuurin kautta. (Experion PMD Network & Cyber Security 2020, 11.)



Kuva 4. Verkkotason 3 rakenne (Experion PKS with PMD controller network planning and design guide 2018)

2.4 Taso 2.5, Virtuaalikoneen hallinta ja varmuuskopiot

Tasolla 2.5 löytyvillä laitteilla ja ratkaisuilla tuetaan virtualisoidun järjestelmän hallintaa ja varmuuskopiointia. EBR (Experion backup and restore) Management -palvelin ja NAS (Network attached storage) -palvelin sijaitsevat tällä tasolla (Kuva 5). NAS-palvelimien tulee olla fyysisesti eri paikassa Esxi Host -isäntäkoneista, jotta tulipalon tai muun onnettomuuden sattuessa ei menetetä kumpiakin. Kaikki tällä tasolla olevat virtuaalikoneet ja isäntäkoneet ovat PMD Experion Domainissa, johon ei kuulu koneita muilta tasoilta. Tasolta löytyvän VMWare vCenter -palvelimen avulla hallitaan järjestelmän EsXi-palvelimen toimintaa. Redundanttiset virtuaalipalvelimet AD1 (Active directory) ja AD2 (Active directory) sijaitsevat myös tällä tasolla, joista kerrotaan lisää opinnäytetyön virtualisointiosiossa. (Experion PMD Network & Cyber Security 2020, 12.)

Kuva 5. Verkkotason 2.5 laitteita (Experion PMD Network & Cyper security 2020, 12)

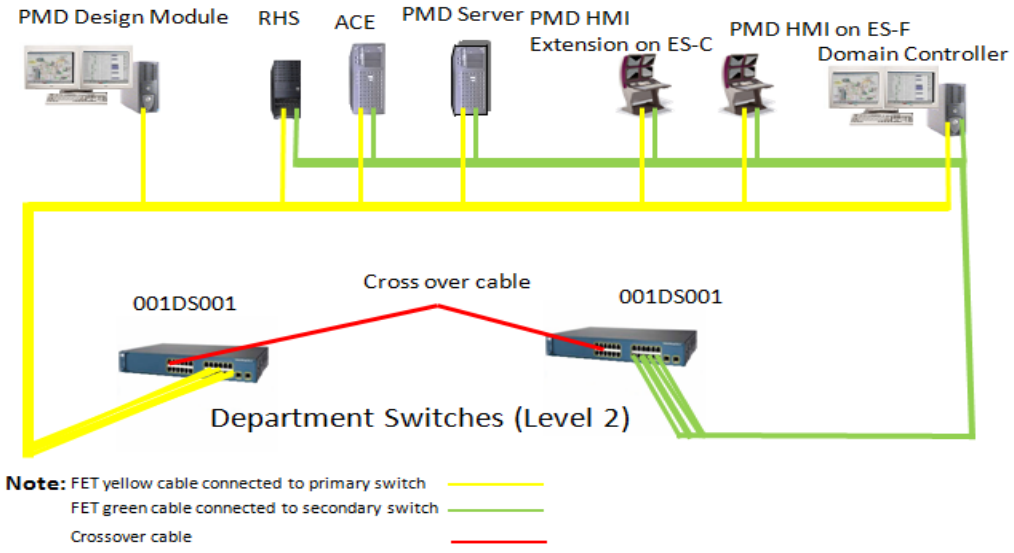
2.5 Taso 2.1, Valvomotaso

Tasolta löytyvät Thin Clientit (Kuva 6), joilla on yhteys useisiin Experion PMD -osastoihin joissain tapauksissa jopa tasolle 3.5, joskin Thin Clienteilla ei ole yhteyttä internetiin. Thin Clientit välittävät kuvan ja datan valvomossa oleville käyttöliittymäkoneille, joilla ohjataan prosessia. Lisätietoa Thin Clienteista löytyy opinnäytetyön virtualisointiosiossa. (Describe basics and configuration thin client 2021, 6.)

Kuva 6. DELL Wyse Thin Client (Describe basics and configuration thin client virtualisointi-kurssi 2021, 6)

2.6 Taso 2, DCS-palvelimet ja käyttöliittymä

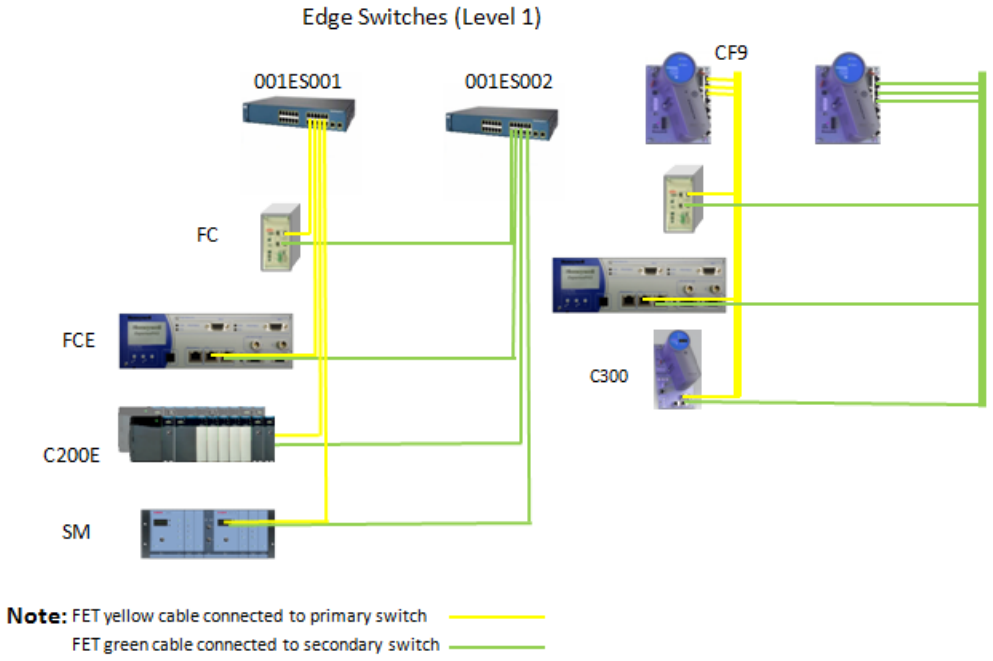
Taso 2 on automaatiojärjestelmän prosessinohjauksen kannalta kriittinen taso. Tästä syystä pääosa tason laitteista onkin redundanttisia(Kuva 7). Honeywell FTE (Fault Tolerant Ethernet) Ethernet-verkko on kahdennettu tällä tasolla. Experion PMD -järjestelmässä jokaisella osastolla on oma aliverkko, joka yhdistyy tasojen 1 ja 2 välillä omaan palomuuriin. HMI-käyttöliittymät on toteutettu Thin Clienteilla, jotka käyttävät kahdennettua yhteyttä. Tasolla sijitsee myös RHS-palvelin ja DM-sovellusasema. (Experion PMD Network & Cyper security 2020, 13.)



Kuva 7. Verkkotaso 2 rakenne sekä laitteiden kaapelointi runkokytkimille (Experion PKS with PMD controller network planning and design guide 2018, 14)

2.7 Taso 1, DCS-ohjaimet(controllerit)

Taso 1 on automaatiojärjestelmän prosessinohjauksen kannalta kriittisin taso. Tältä tasolta yhdistetään automaatiojärjestelmä prosessiin ja ohjataan sitä reaaliajassa. Prosessinohjain suorittaa ohjaustoimintoja itsenäisesti ja generoi tietoja sekä hälytyksiä prosessista PMD-palvelimelle. Yksiköt on kytketty FTE-verkkoon ja prosessinohjaimet ovat yleensä kahdennettuja (Kuva 8). Honeywell Experion PMD -järjestelmässä käytetään kahta eri prosessinohjainta FC ja FCE. Prosessinohjain FC tukee Profibus-protokollaa ja prosessinohjain FCE Profibus- sekä Profinet-protokollaa. (Experion PMD Network & Cyper security 2020, 14.)



Kuva 8. Verkkotaso 1 rakenne sekä laitteiden kaapelointi reunakytkimille (Experion PKS with PMD controller network planning and design guide 2018, 13)

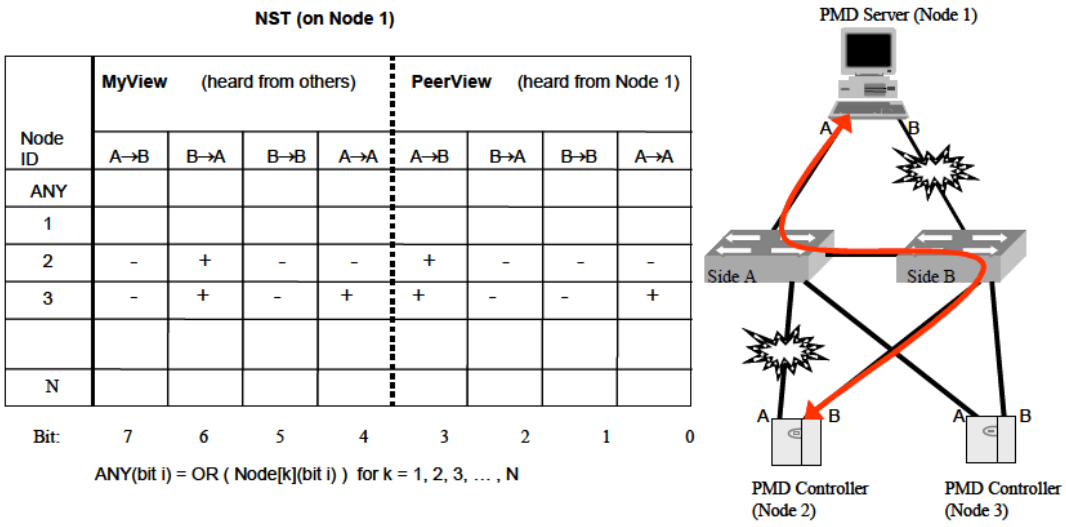
2.8 Taso 0, Prosessitaso

Tällä tasolta löytyvät teollisuuden instrumentointiin käytetyt anturit, mittalaitteet, toimilaitteet ja I/O, joiden datan pohjalta ohjataan prosessia. Tasolta 0 muodostetaan yhteys tason 1 FCE/FC-prosessinohjaimiin, jotka kommunikoivat reaaliajassa kentällä olevien instrumenttilaitteiden kanssa (Experion PMD Network & Cyper security 2020, 14). Teollisuuden instrumentoinnissa käytetään pääosin 4-20mA virtaviestiä häiriöherkkyyden minimoimiseksi.

Kuva 9. Prosessitason IOC-kehikot (Experion PMD Network & Cyper security 2020)

2.9 FTE

FTE-verkko ohjaa Honeywellin PMD Experion-automaatiojärjestelmiä. Se on suunniteltu parantamaan suorituskykyä, turvallisuutta ja vikasietoisuutta teollisuuden automaatiojärjestelmissä (Kuva 10). FTE:n redundanssisuus saavutetaan Honeywellin FTE-ajurin sekä yleisesti markkinoilla olevien komponenttien yhteensopivuudella. Tästä johtuen saavutetaan hyvä vikasietoisuus. FTE tukee TCP/IP- (Transmission control protocol/internet protocol), UDP/IP- (User datagram protocol/internet protocol) ja IP Multicast -protokollia verkkoliikenteessä. FTE:n kaapelit kytketään ja määritetään kytkimille oletuksella keltainen primääri ja vihreä sekundääri. Punainen yhdyskaapeli on vain kahdennetun verkon ylimmällä tasolla olevien kytkimien välillä. FTE on kytketty Ethernet-kaapelilla myös palomuurin kanssa. (Experion PMD Network & Cyper security 2020, 15–16.)



Kuva 10. Esimerkki FTE:n toiminnan jatkumisesta vikatilanteessa (Experion PKS with PMD controller network planning and design guide 2020, 42)

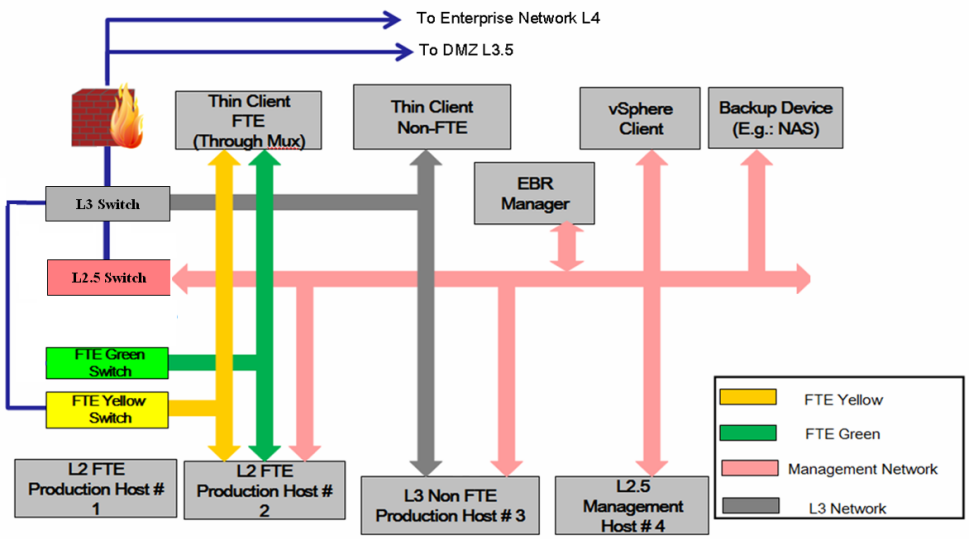
3 EXPERION PMD-JÄRJESTELMÄN PALOMUURI JA LIITETTÄVYYS

Experion PMD-järjestelmässä on Honeywellin hyväksymä palomuuri, joka erottaa verkkotasot toisistaan. Palomuurilla valvotaan verkkoliikennettä kahden verkon välillä ennalta määritettyjen turvallisuussääntöjen mukaisesti, jolloin voidaan kontrolloida sekä ohjata lähtevää ja tulevaa liikennettä. Tasojen aliverkot eivät voi muodostaa yhteyttä suoraan toisille tasoille. Experion PMD palomuuri ei ole koskaan suorassa yhteydessä internettiin.

Experion PMD-järjestelmä tukee ulkoisia yhteyksiä, ja näin ollen se voidaan liittää kolmansien osapuolien verkkoihin ja laitteisiin kiinni (Experion PMD Network & Cyper security 2020, 21).

3.1 Verkkotasojen välinen liikenne

Tasolla 4 on oma palomuurinsa, joka on yhdistetty internetiin joko suoraan tai useamman palomuuritason kautta. Tasojen 2 ja 1 välillä ei sallita WLAN-yhteyksiä, eli kaikki näiden tasojen välillä oleva liikenne kulkee redundanttisia Ethernet-kaapeleita pitkin. Kaikki palomuurissa olevat verkot ovat epäluotettavia, ja verkkoliikenne sekä portit on tarkkaan määritelty. Taso 2.5 kytkeytyy ainoastaan tasolle 3. (Experion PMD Network & Cyper security 2020, 21.)



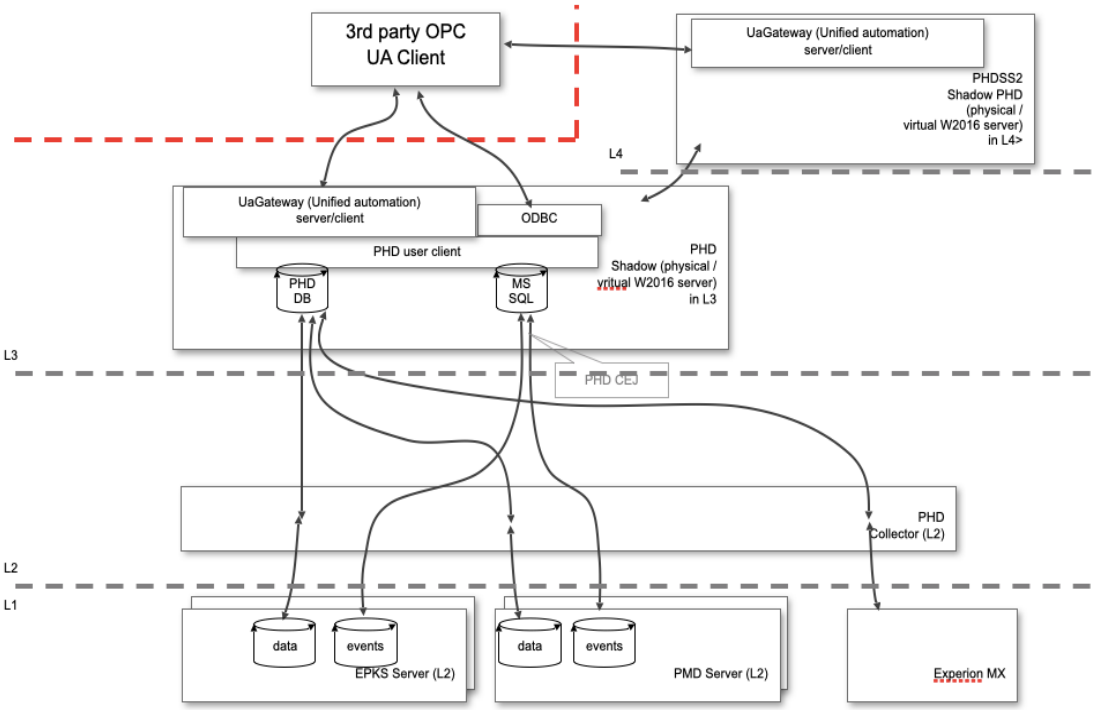
Kuva 11.Honeywell Experion PMD verkkotasojen välinen liikenne (Describe the process to create template 2022, 78)

3.2 Palomuurin konfigurointi

Kommunikaatioprotokollat ja porttien lukumäärät minimoidaan tasojen välillä. Yritystason kommunikointi ohjausvyöhykkeeseen estetään. Palomuuriin määritettävät asiat ovat aliverkot, WLAN-verkot, WAN (Wide-area network) -verkon reititin, UPLINK-portit ja reitittimen suodatus. (Experion PMD Network & Cyper security 2020, 21.)

3.3 Ulkoiset liitännät

OPC (Open Platform Communications) on teollisuuden tiedonsiirtoon määritelty viestintästandardi. Alkuperäinen OPC-standardi perustui OLE-,COM-, ja DCOM-teknologiaan Windows-käyttöjärjestelmissä. Palvelukeskeisten toimintojen ottaessa suurempaa roolia automaatiojärjestelmissä loi nämä uusia haasteita turvallisuuden ja datamallinnuksen kannalta. Tätä varten kehitettiin OPC-UA (Unified Architecture) standardi, joka vastasi näihin haasteisiin. OPC-yhteyden avulla eri valmistajien ohjauslaitteet saadaan kommunikoimaan keskenään reaaliaikaisesti. Uusimmissa Honeywell Experion PMD järjestelmissä käytetään OPC-UA:ta, kun halutaan yhteys kolmansien osapuolien laitteisiin (Kuva 12). (Experion PMD Network & Cyper security 2020, 46.)



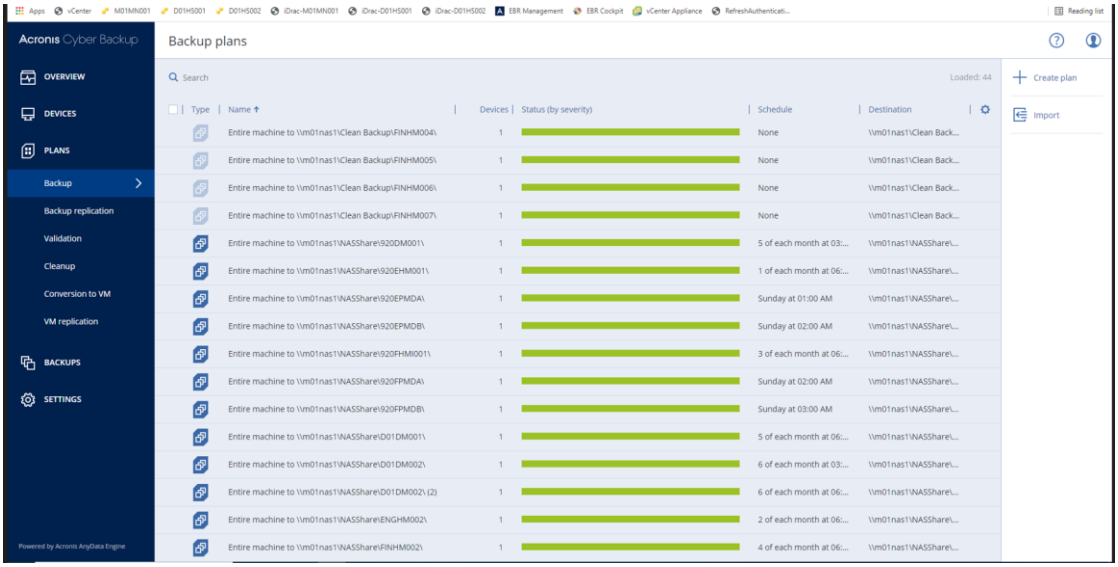
Kuva 12.Yhteys kolmansien osapuolien laitteisiin (Experion PMD Network & Cyper security 2020, 47)

4 EBR

Honeywellin Experion PMD käyttää varmuuskopiointi- ja palautusjärjestelmää, jota kutsutaan nimellä EBR (Experion backup and storage). EBR:ää hallinnoidaan Acronis Backup ohjelmalla (Kuva 13), joka on asennettuna järjestelmän Management-koneelle. EBR on tärkeä työkalu, joka parantaa huomattavasti PMD- järjestelmän turvallisuutta ja mahdollistaa tiedostojen kopioinnin järjestelmän ollessa toiminnassa. EBR tarjoaa suojaa inhimillisiltä erehdyksiltä poistettaessa tietoja, epäonnistuneilta sovelluksilta, kovalevyvioilta, luonnollisilta onnettomuuksilta tai muista laitteistojen sekä ohjelmistojen sammumisilta vaikka sähkökatkossa. EBR varmuuskopioi ennaltamäärätyn aikataulun mukaisesti käyttöjärjestelmän, sovellukset,palvelupaketit sekä kaikki konfigurointitiedostot. Honeywell suosittaa EBR-varmuuskopioitujen tiedostojen siirtämistä NAS-palvelimelle. Onnettomuuden sattuessa asiakas saa laitteet nopeasti toimintakuntoon varmuuskopioiden avulla.

EBR voi replikoida myös itse kokonaisen virtuaalikoneen, jolloin se luo tarkat kopiot lähdekoneesta ja vie ne oikealle VMware ESXi isäntäkoneelle. Aina kun replikointi suoritetaan, myös kopioidut koneet päivittyvät. Replikakoneet

ovatkin täydellisiä kopioita virtuaalikoneista, jolloin ne voidaan jättää virtuaalipakkaan ”varaosiksi”. Nämä koneet ovat kuitenkin sammutettu, joten ne eivät kuluta laskentaresursseja, mutta vievät levytilaa. (Experion PMD Network & Cyper security 2020, 23.)

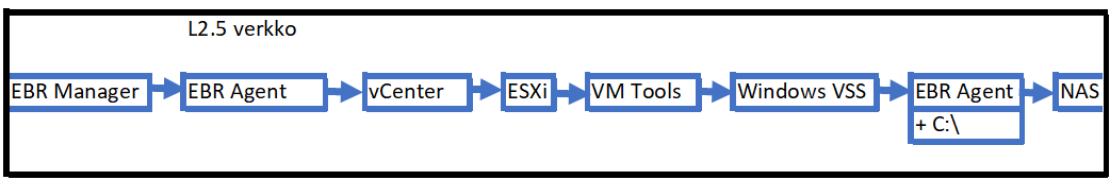


Kuva 13. Backup-suunnitelman tarkastelua Acronis Backup -ohjelmalla (Honeywell 2023)

4.1 EBR Management palvelin

EBR Management palvelin toimii keskitettynä palvelimena varmuuskoipiointitoimintoja varten. Palvelimella määritellään tarkat suunnitelmat jokaiselle ESXi-Hostille. Näissä suunnitelmissa käydään läpi, mitkä tiedostot kopioidaan, milloin ne kopioidaan ja mihin kopioidut tiedostot tallennetaan.

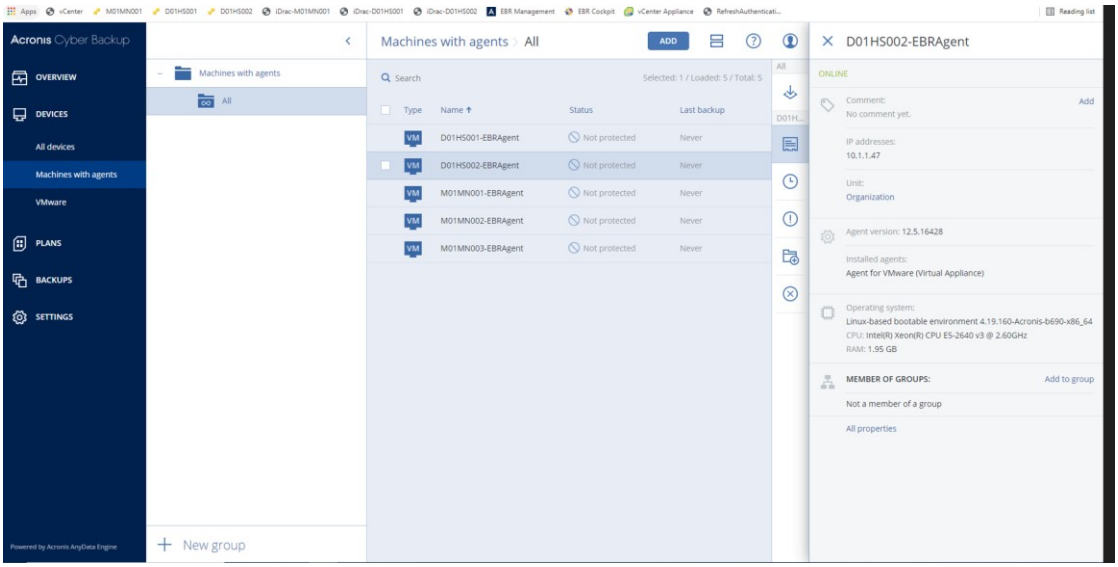
Palvelin vaatii toimiakseen Windows domainin, joka on tasolla 2.5. Palvelin toimii koko yrityksen laajuisena seuranta- ja raportointityökaluna. Palvelimella mahdollistetaan kokonaisvaltainen keskitetty varastointitila varmuuskopioiden arkistointia varten. (Describe the process to create template 2022, 82.)



Kuva 14.Virtuaalikoneen varmuuskopioinnin yksinkertaistettu prosessikaavio (Honeywell, 2023)

4.2 EBR-agentti

Jokaisella ESXi-isäntäkoneelle on asennettu EBR-agentti, joka kytkeytyy hallintaverkkoon(Kuva 15). Management-hallintapalvelin on yleensä asennettu järjestelmässä ensimmäiselle isäntäkoneelle. Uusimmissa järjestelmäversioissa on kuitenkin aiottu laittaa vain yksi EBR-agentti koko virtuaalijärjestelmään. EBR-agentti hoitaa varsinaisen työn varmuuskopiointiprosessissa sekä keskustelee EBR-palvelimen, NAS:in ja vCenter-hallintaohjelman kanssa. (Describe the process to create template-dokumentti 2022, 81–82.)



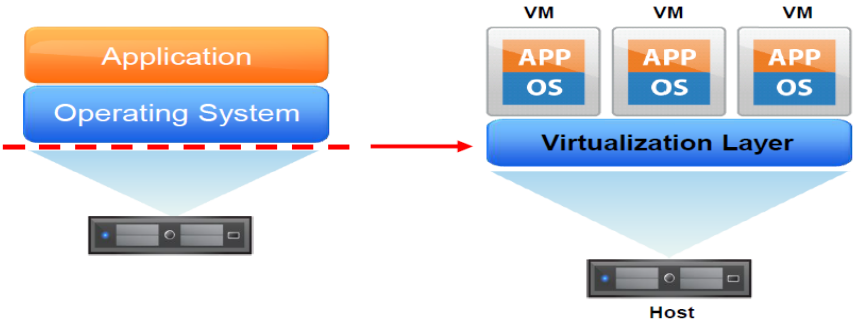
Kuva 15. Isäntäkoneille asennetut EBR-agentit (Honeywell 2023)

5 PMD-JÄRJESTELMÄN VIRTUALISOINTI JA PROJEKTOINTI

Tässä osiossa käydään läpi virtualisoinnin perustoimintoja ja rakennetta sekä avataan lyhyesti Honeywellin projektien etenemistä.

Honeywell Experion PMD-järjestelmä tukee virtualisointia. Virtualisointi toteutetaan Vmware vSphere virtualisointialustalla, jonka ohjelmistoversiot 6.0, 6.5, 6.7 ja 7.0 ovat yhteensopivia PMD-järjestelmän kanssa. Vvmware vSphere virtualisointialustan pääkomponentit ovat VMware ESXi palvelin, VMware vCenter palvelin sekä VMware vCenter Update Manager laiteohjelmisto. (Describe the VMware products used for virtualization 2022,

19,33). VMware vSphere sisältää myös VMKernel-käyttöjärjestelmän, joka hallitsee suurinta osaa laitteison fyysisistä resursseista. Näihin resursseihin luetaan muisti, prosessorit, tallennustila sekä verkko-ohjaimet.
Honeywell käyttää virtualisoinnissaan Vmfare vSpheren Platform Virtualization menetelmää(Kuva 16), jolloin itse käyttöjärjestelmä on erillään fyysisestä laitteistosta ja useat fyysiset koneet on rakennettu yhden tietokoneen sisälle. Tämän menetelmän etuna ovat laitteistoriippumattomuus, vikojen eristäminen virtuaalikoneeseen, vähemmän fyysisten osien vaihtoa ja dynaaminen hallintamahdollisuus prosesorille, muistille sekä verkkoresursseille. (Describe an overview of virtualization technology 2022, 8–9,11.)

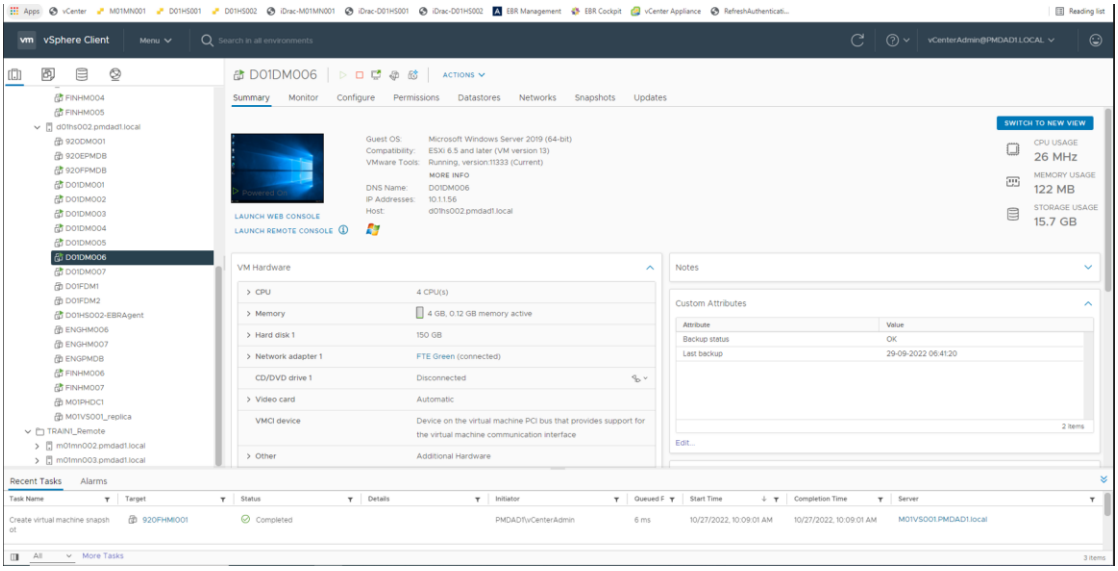


Kuva 16. VMware vSphere Platform Virtualization menetelmä (Describe an overview of virtualization technology 2022, 9)

Honeywellin projektit käynnistyvät asiakkaan tarpeesta päivittää tai parantaa automaatiojärjestelmän laitteita sekä niihin liittyviä toimintoja. Yleensä myyjä, huoltohenkilöstö, palvelupäällikkö sekä työmaakohtainen vastaava ovat olleet asiakkaaseen tiiviisti yhteydessä ennen projektitarpeen tunnistamista ja käynnistämistä. (Honeywell 2022.)

5.1 Virtuaaliympäristön hallinnointi Honeywell PMD-järjestelmässä

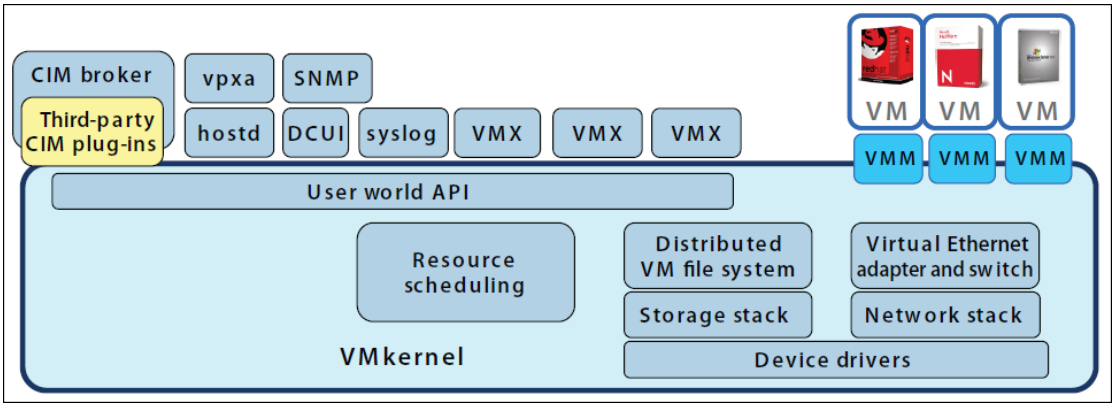
Virtuaaliympäristön koneita hallinnoidaan Linux-pohjaisen VmWare vCenter palvelimen kautta (Kuva 17), joka voidaan konfiguroida myös virtuaalikoneeksi. Palvelin hallinnoi kaikkia Esxi-koneita, jotka on yhdistetty verkkoon sekä valvoo järjestelmän tilaa. Palvelin operoi jatkuvasti, vaikka Vmfare Vsphere Clientit ei olisikaan yhdistetty tai kirjautuneet sisään. Palvelin itsessään tarvitsee erillisen tietokannan tietojen tallentamiseen. (Describe the VMware products used for virtualization 2022, 23.)



Kuva 17. Honeywell koulutusjärjestelmän virtuaalikoneidenhalllinta (Honeywell 2023)

5.2 VMKERNEL

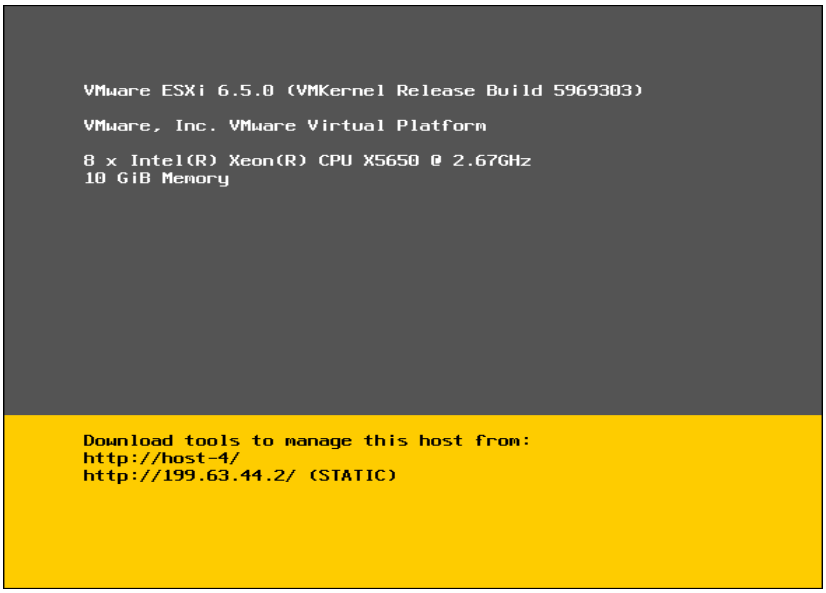
VMKernel on Vmwaren kehittämä POSIX (Portable Operating System Interface) -tyyppinen korkean suorituskyvyn käyttöjärjestelmä. Se toimii suoraan ESXi-isäntäkoneella. Itse ESXi-isäntäkonetta ei ole kytketty Windows -käyttöjärjestelmään. VMKernel -käyttöjärjestelmän toiminnot voidaan eritellä lyhyesti resurssienhallintaan, verkkoympäristön hallintaan sekä tallennustilan hallintaan. (Describe the VMware products used for virtualization 2022, 33–35.)



Kuva 18. VMKernel-käyttöjärjestelmän toiminnot (Describe the VMware product used for virtualization 2022, 33)

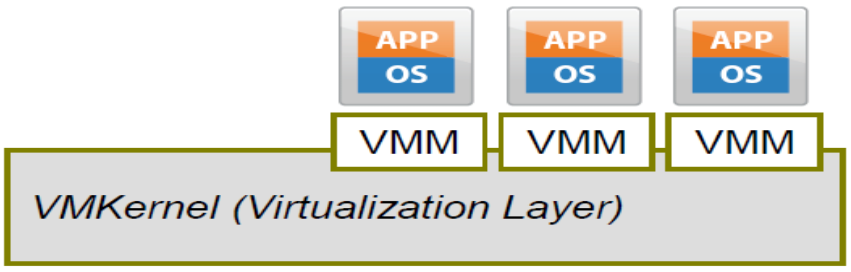
VMKernel-käyttöjärjestelmässä toimii erilaisia prosesseja (Kuva 18), joita käydään läpi seuraavaksi. Yksi näistä prosesseista on DCUI (Direct Console Unit Interface), jonka kautta voidaan olla vuorovaikutuksessa ESXi-

palvelimeen tekstipohjaisten valikoiden avulla. DCUI:ta voidaan verrata BIOS:iin. (Describe the VMware products used for virtualization 2022, 34.)



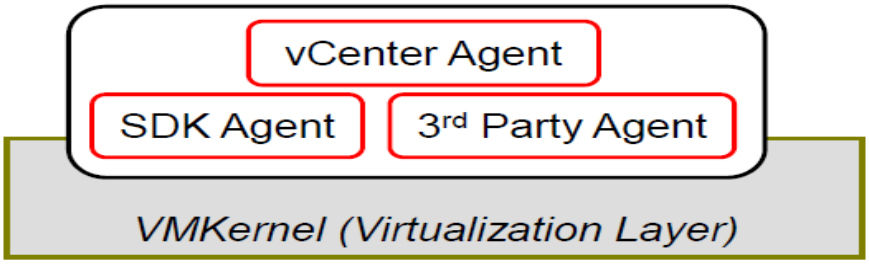
Kuva 19. VMKernel käyttöjärjestelmä (Describe the VMware product used for virtualization 2022, 34)

Jokaiselta virtuaalikoneella löytyy oma VMM (Virtual Machine Monitor), jonka tehtäviin kuuluu hallita virtuaaliympäristössä olevaa isäntäkonetta(Kuva 20). (Describe the VMware products used for virtualization 2022, 34.)



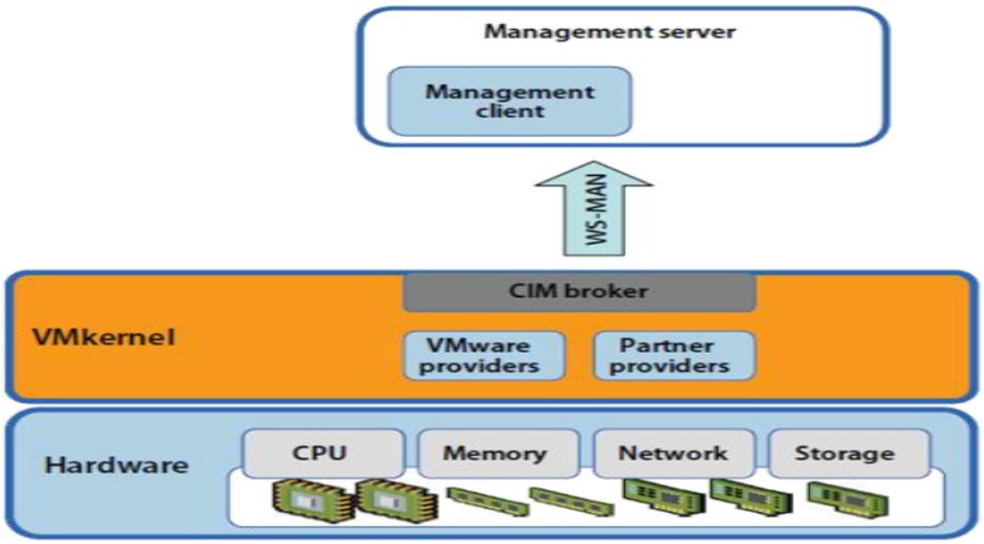
Kuva 20. VMM-periaatekuva (Describe the VMware product used for virtualization 2022, 34)

Agenttivirtuaalikone on kone, joka suorittaa tietyn toiminnon virtuaaliselle infrastruktuurille. VMKernelissä toimivat agentit mahdollistavat korkean infrastruktuurin hallinnan etäsovelluksille(Kuva 21). (Describe the VMware products used for virtualization, 2022, 34.)



Kuva 21.VMKernelin agenttikoneet (Describe the VMware product used for virtualization 2022, 35)

VMKernelin prosesseihin kuuluu myös CIM (Common Information Model). CIM on avoin standardi, joka määrittelee koneen laskkentaresursseja sekä määrittelee, kuinka nämä voivat olla edustettuna ja johdettuna(Kuva 22). CIM mahdollistaa laitteistonhallinnan etäsovelluksista sekä API (Application Programming Interfaces) ohjelmointirajapinnasta. (Describe the VMware products used for virtualization 2022, 35.)



Kuva 22.CIM ((Describe the VMware product used for virtualization 2022, 35)

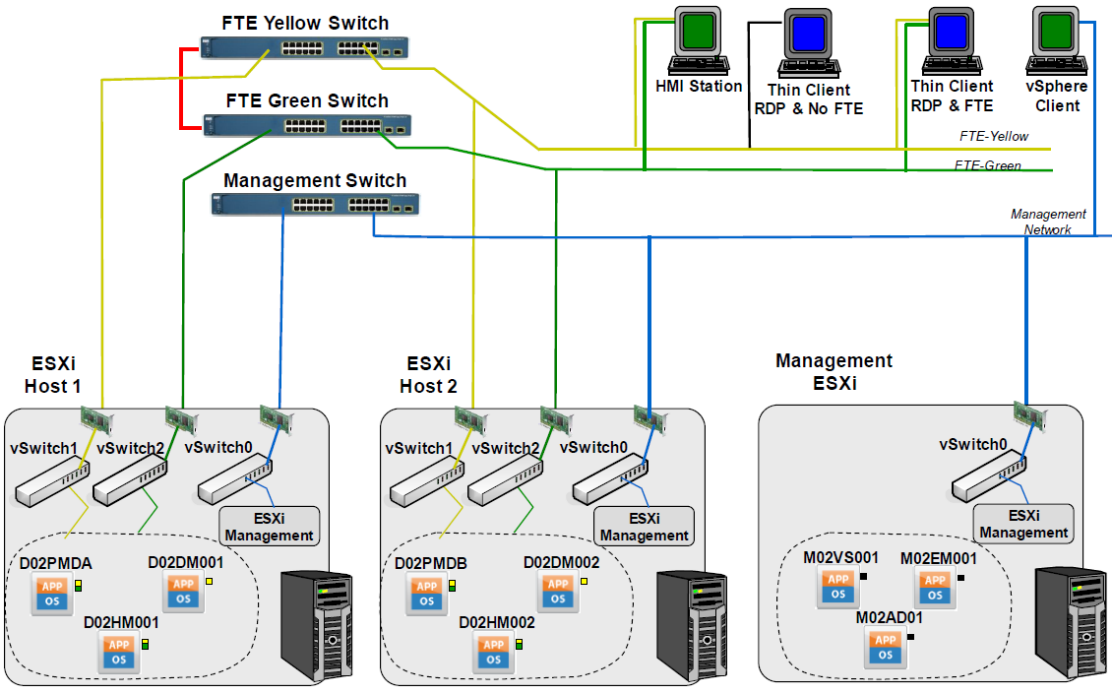
5.3 Isäntäkoneet ja kytkimet

Jokainen virtualisoitu Honeywell Experion PMD-järjestelmä sisältää vähintään kolme kappaletta Hosteja eli isäntäkoneita. Isäntäkone 1 sisältää kaksi redundanttista verkkoalueohjainta AD1 sekä AD2. Nämä verkko-ohjaimet yhdistävät virtuaalikoneet sekä isäntäkoneet tasolle 2.5. Kaikki tasolla 2.5 olevat laitteet yhdistyvät Experion PMD Domainiin(PMDAD1). Isäntäkoneelta löytyy kaksi Linux-virtuaalikonetta, jotka ovat EBR Management-palvelin varmuuskopioiden hallintaan sekä vCenter-palvelin ESXi-hallintaan.

Isäntäkoneilta löytyy myös EBR Agent, ESXi sekä iDRAC. Isäntäkone sisältää yleensä myös Service Noden tasolla 3 ja Relay Noden, PHD-palvelimen sekä RDS-palvelimen(Remote Desktop Server) tasolla 3.5. (Experion PMD Network & Cyper security 2020, 25–27.)

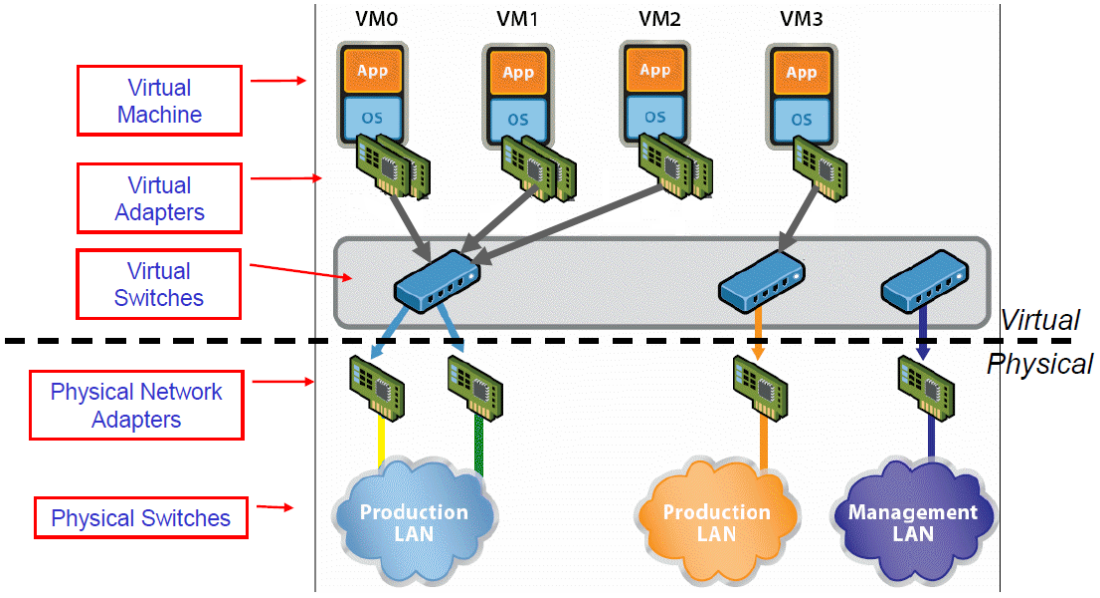
Isäntäkone 2 ja isäntäkone 3 sisältävät redundanttiset PMD-palvelimet tasolla 2 (A-palvelin ja B-palvelin). Samalla tasolla toimivat itse operatiiviset käyttöliittymät eli HMi:t sekä sovellusasema DM. Honeywell Experion PMD-järjestelmään on mahdollista integroida myös QCS-laadunhallintajärjestelmä, joka sijaitsee tasolla 2 (Experion PMD Network & Cyper security 2020, 37). QCS-palvelin on asennettuna yhdelle virtualisoidun PMD-järjestelmän isäntäkoneista, ja tästä otettu replica on asennettu jollekin toiselle isäntäkoneelle sammutetuksi virtuaalikoneeksi, näin ollen mahdollisen vian tullessa isäntäkoneelle voidaan QCS-laadunhallintajärjestelmä nopeasti palauttaa tuotannon tueksi. (Experion PMD Network & Cyper securit 2020, 25–27.)

Virtualisoidussa Experion PMD-järjestelmässä on vähintään kolme kappaletta Honeywellin hyväksymiä verkkokytkimiä(Kuva 23). Kaksi kytkimistä välittää FTE-verkon verkkoliikennettä ja yksi kytkin tasojen 2.5, 3 ja 3.5 sekä mahdollisen QCS-laadunhallintajärjestelmän verkkoliikennettä. (Experion PMD Network & Cyper security 2020, 29.)



Kuva 23. PMD-virtualisoidun järjestelmän verkkotaso 2 (Describe the network planning 2021, 39)

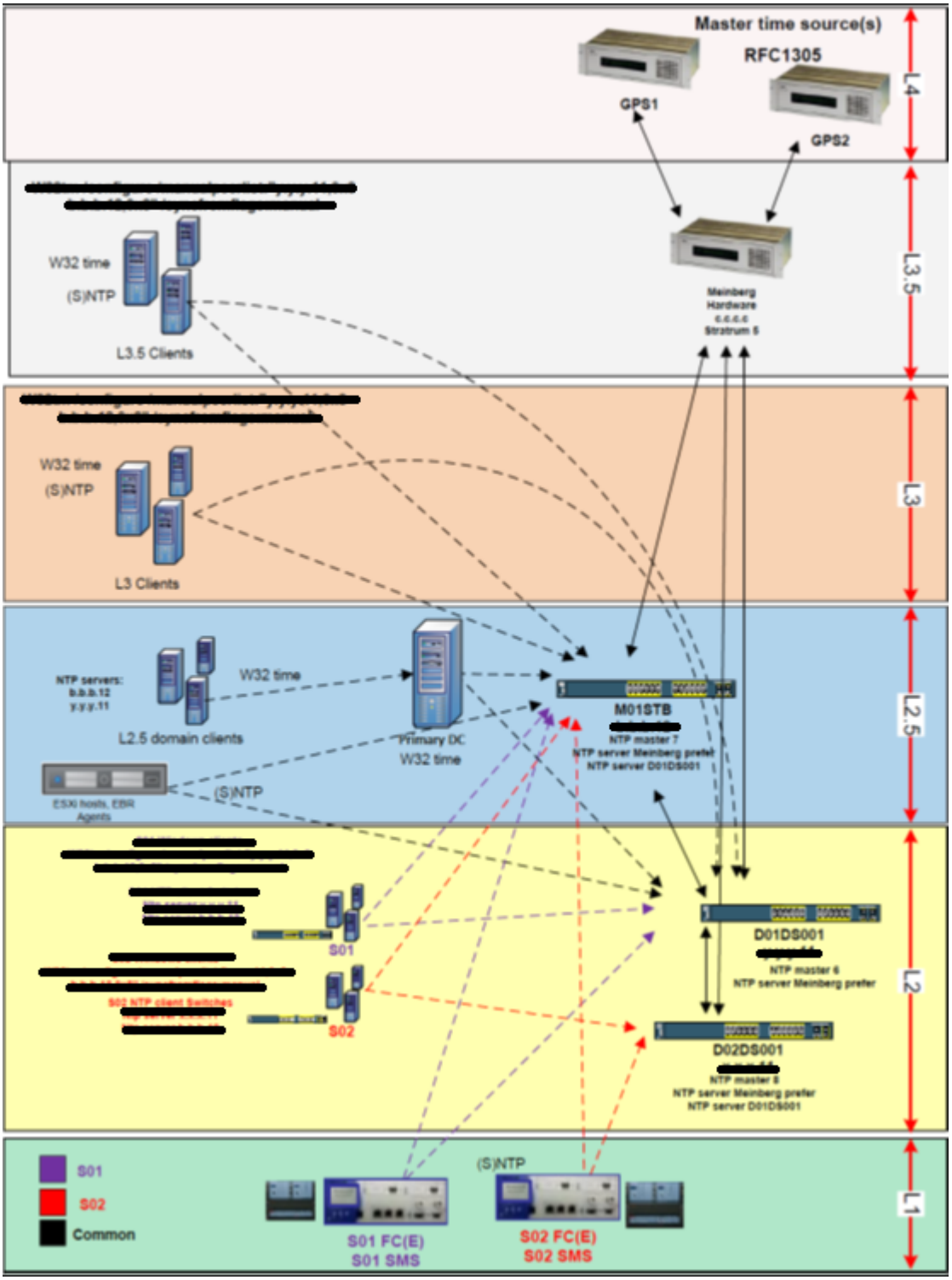
Jokainen PMD-virtuaalikone pitää sisällään vähintään kaksi kappaletta virtuaalisia verkkosovittimia(Virtual Adapters)(Kuva 24). Pääosin sovittimien nopeudet on asetettu toimimaan nopeudella 100Mbps/Full Duplex, jotka on kytketty virtuaalisesti FTE-keltainen sekä FTE-vihreä kytkimille.



Kuva 24. Virtualikoneet yhdistettynä ulkoiseen verkkoon (Describe the network planning 2021, 35)

5.4 Honeywell Experion PMD ajanjakelu virtuaalisessa järjestelmässä

Ajanjakelu on tärkeä osa Honeywellin virtuaalisen PMD-järjestelmän toimintaa. Honeywellin ajanjakelussa käytetyään standardoitua RFC 1305 NTP protokollaa. Ajanjakelun on perustuttava fyysiseen laitteeseen, jotta järjestelmän laitteet toimivat oikein(Kuva 25). Ajanjakelu ei voi perustua virtuaalikoneeseen, koska tällöin järjestelmästä tulee kelluva ajan suhteen eikä järjestelmän toiminnoilla näin ollen ole ankkuria, johon se tukeutuu. Kaikilla järjestelmään kytkeytyvillä laitteilla täytyy olla määriteltynä samat NTP-serverit. Järjestelmässä FTE-keltainen kytkin toimii ensisijaisena NTP-jakelijana tasoille L1,L2 ja L2,5. Toissijaisena jakelijana näille samoille tasoille käytetään Management-kytkintä. Tasolta L3 löytyvä asiakkaan hallinnoima Meinbergin NTP-serveri jakaa aikaa yllämainituille tasoille. Tason 4 aika haetaan joko asiakkaan palvelimelta tai GPS-satelliitin kautta. (Virtuaalijärjestelmä rakenne ja komponentit, virtualisointikoulutus materiaali 2023, 3.)

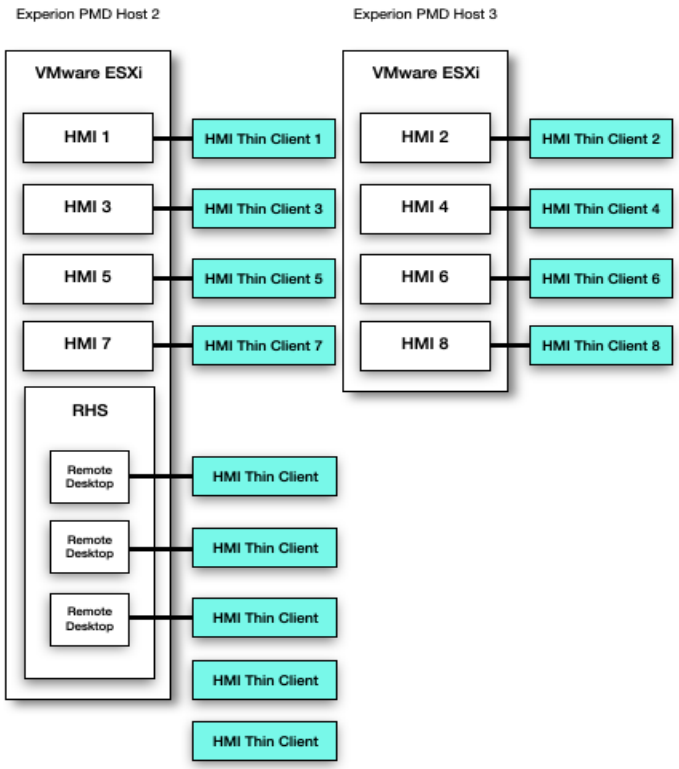


Kuva 25. Ajanjakelun toteutus virtualisoidussa PMD-järjestelmässä (Virtuaalijärjestelmä rakenne ja komponentit, Honeywell 2023)

5.5 HMi-käyttöliitttymä ja DM-sovellusasema

Honeywell Experion PMD-järjestelmä tukee useita HMi- (Human Machine Interface) käyttöliittymiä samanaikaisesti. Käyttöliittymän tehtävänä on kerätä dataa ohjattavasta prosessista ja välittää se käyttäjälle valvomoon tai tuotantotiloihin. Näytön tiedostomuotona on HTML (Hypertext markup

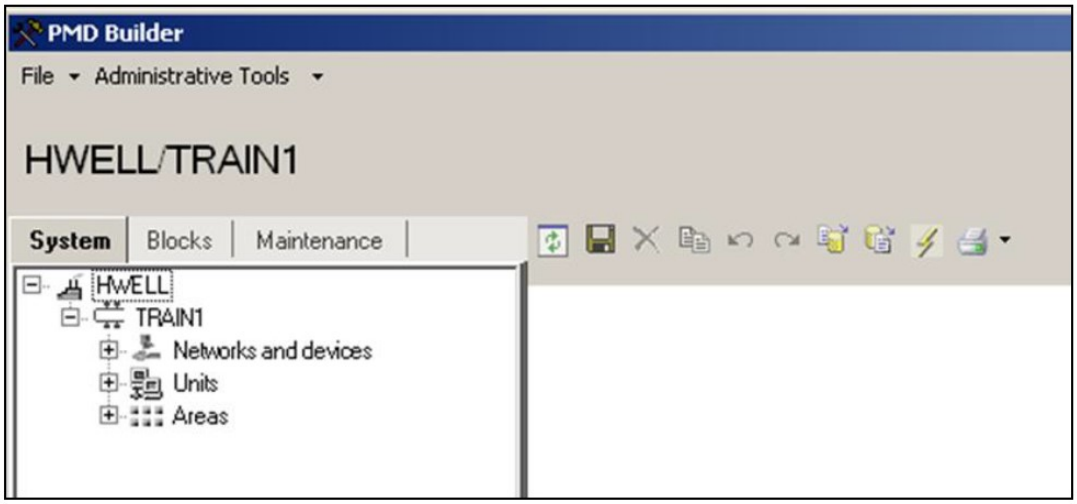
language), ja käyttöliittymiä on kahdentyyppisiä. Toiset käyttöliittymät ovat kiinteitä käyttöliittymiä, jolloin yhdellä HMi-virtuaalikoneella on yksi Thin Client. Toiset käyttöliittymät ovat monipuolisempia, jolloin useampi käyttäjä pystyy operoimaan tai tarkastelemaan prosessia samanaikaisesti RHS-palvelimen (Remote Host Server) kautta(Kuva 26). Virtualisoidussa ympäristössä HMi perustuu Windows 2016- tai Windows 2019 käyttöjärjestelmiin. (Experion PMD Network & Cyper security 2020, 32.)



Kuva 26.Esimerkki, jossa HMi-virtuaalikoneet sijaitsevat isäntäkoneilla 2 ja 3 (Experion PMD Network & Cyper security 2020, 32)

DM (Design Module)- sovellusasemaa käytetään järjestelmän tietojen luomiseen sekä ylläpitoon PMD Builder-ohjelman avulla, joka mahdollistaa järjestelmän toiminnan vaaditulla tavalla sovelluksen sisällä. PMD-Builder sisältää järjestelmäeditorin, lohkoeditorin ja huolto-osion. Huolto-osiosta löytyy Honeywellin Daxmon-työkalu, jonka avulla voidaan tarkastella järjestelmän tilaa ja tehdä huoltotoimenpiteitä. DM-sovellusaseman toimintoihin kuuluvat järjestelmä- ja I/O-määritykset(Kuva 27), sovellus, sovelluksen lataus järjestelmään, sovelluksen toimintojen valvonta, simulointi, kenttäväylämääritelmät ja sovelluksen etähallinta verkossa. Virtualisoidussa ympäristössä DM-sovellusasema perustuu R900.xx Windows 7-tai Windows

2008 käyttöjärjestelmään ja Windows 2019 käyttöjärjestelmään. (Describe system architecture 2021, 6,14.)

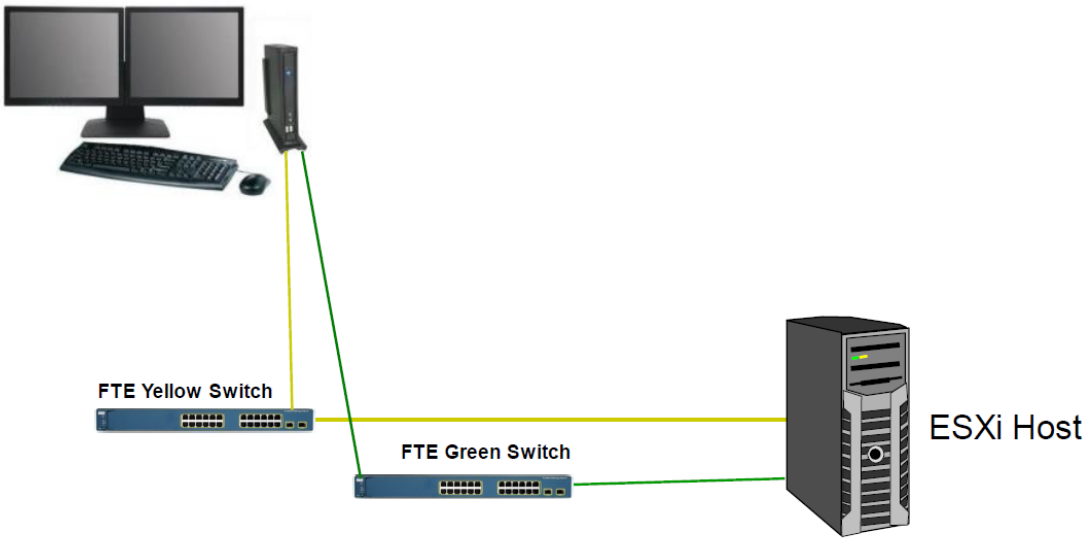


Kuva 27 Esimerkkinäkymä sovellusaseman system-välilehdeltä (Describe design module editor 2019, 5)

5.6 Thin Client

Thin Client on laite, jonka toiminnot ovat verrattavissa normaaliin työasemakoneeseen sillä erotuksella, että Thin Client ei suorita minkäänlaisia prosesseja tai laskentatoimenpiteitä, vaan nämä toiminnot suoritetaan virtuaalisella etähallintakoneella. Thin Clientin tehtävänä on välittää ääni, kuva ja USB-signaaleja verkkokaapeliliitännän kautta prosessoitavaksi. Thin Client mahdollistaa käyttöliittymän näytön, näppäimistön, hiiren ja äänilaitteiden erottamisen virtuaalikoneen prosessorista ja kiintolevyistä menettämättä signaalin eheyttä.

Thin Client konfiguroidaan sallimaan ainoastaan Windows RDP- (Remote desktop protocol) yhteydet, ja sillä on mahdollisuus toimia yhdessä Honeywell FTE-verkon kanssa, jolloin siitä saadaan redundanttinen. Thin Client tukee USB-ELO sekä EETI SAW kosketusnäyttöjä. Yksinkertaisen verkko-, ja näyttökonfiguraation vuoksi laitteiston asentaminen on käytännössä plug and play. (Describe basics and configuration of thin client 2021, 4–6.)

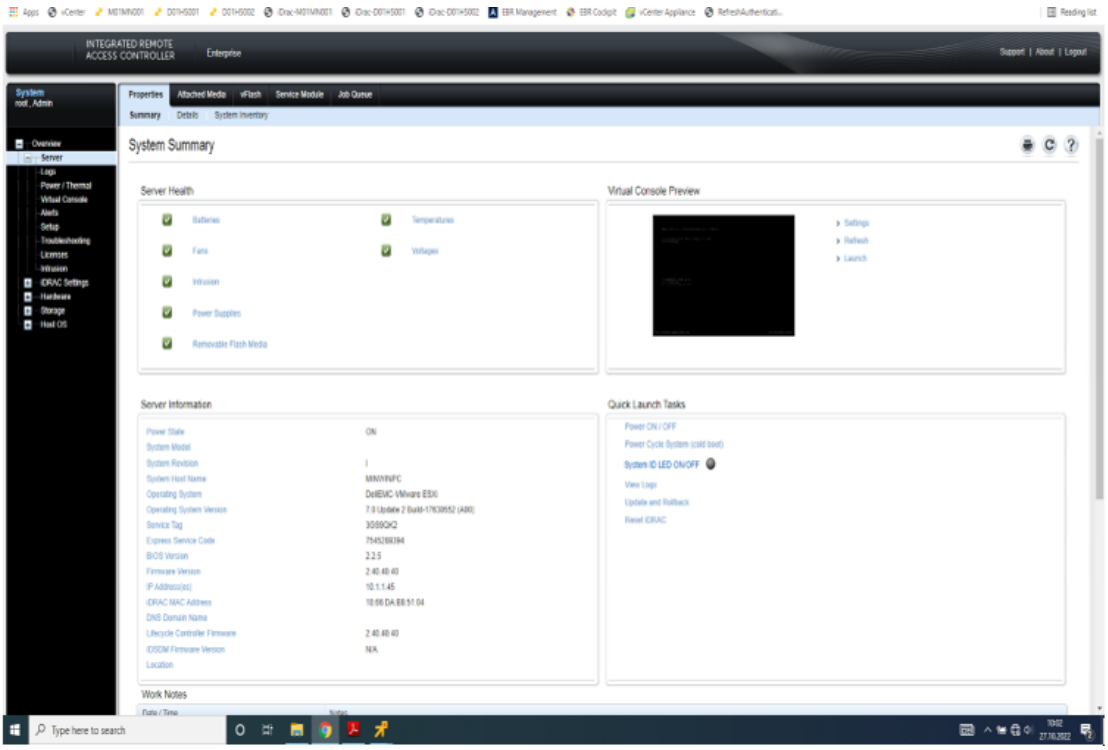


Kuva 28.Thin Clientin kytkentä isäntäkoneelle (Describe basics and configuration of Thin Client 2021, 10)

5.7 iDRAC

Virtualisoidussa järjestelmässä toimivat DELL-palvelimet sisältävät hallinta-alustan jota kutsutaan nimellä iDRAC(Integrated Dell Remote Access Controller). iDRAC on suoraan palvelimen emolevylle asennettu laitteisto, joka valvoo palvelimen tilaa, käynnistää tai sammuttaa palvelin ja antaa käyttäjälle mahdollisuuden hallita palvelinta etänä (DELL 2022). Etähallinta onnistuu myös siinä tapauksessa, vaikka palvelimen ydintoiminnot olisivat häiriintyneet. DELL iDRAC on yhdistetty tasolle 2.5 ja sillä on oma IP-osoitteensa. Sitä hallitaan Vcenter-serverin kautta Vsphere-clientin avulla (Experion PMD Network & Cyper security 2020, 33). Hallinta-alustalta käyttäjä saa paljon erilaista tietoa DELL-palvelimen kunnosta sekä sen sisältämien laitteiden toiminnasta(Kuva 29). Properties System summary välilehti avaa käyttäjälle näkymän, josta löytyy akkujen, tuulettimien, jännitteiden, lämpötilojen, virtalähteiden sekä palvelimen muiden laitteiden yleistila(Kuva 29) (Experion PMD Network & Cyper security 2020, 33.)

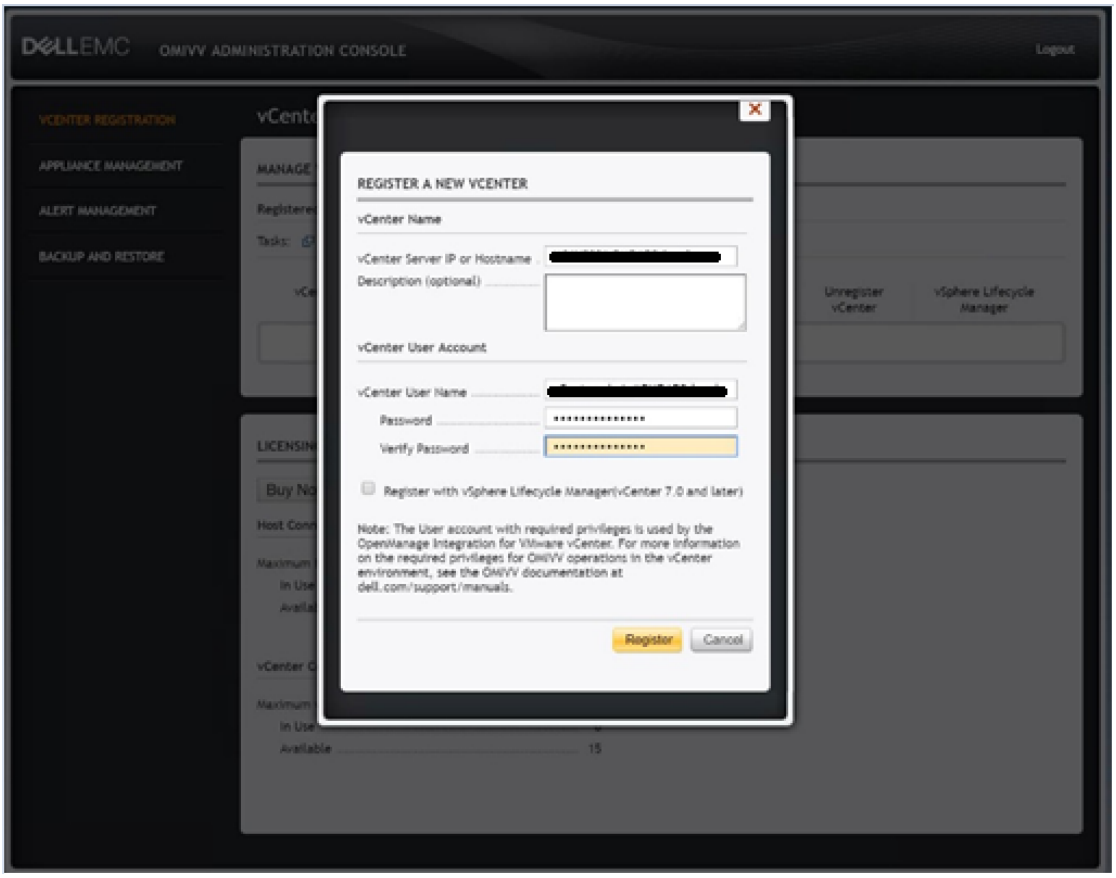
Käyttäjä saakin erilaista tietoa kirjautumalla iDRAC:iin, mutta vian sattuessa hälytykset ei generoidu vCenteriin ja sieltä edelleen PMD-järjestelmään ilman OMIVV-konetta.



Kuva 29. Honeywellin virtuaalisen koulutusjärjestelmän iDRAC näkymä

5.8 OMIVV

OMIVV(Open Manage Integration for VMWare vCenter) virtuaalikoneella tuodaan iDRAC:n hälytykset käyttäjien näkyville PMD-järjestelmän järjestelmähälytysnäytölle, jolloin automaatiojärjestelmän operaattorit saavat hälytyksen palvelimien häiriötilanteista ja näihin osataan reagoida välittömästi. OMIVV:n avulla voidaan myös inventoida palvelinlaitteistoa sekä päivittää BIOS- ja laiteohjelmistot vCenteristä. Kone on yhdistetty hallintaverkkoon tasolle 2.5. OMIVV on lisensoitu tuote. OMIVV-koneella on oma IP-osoite. (OMIVV installation and configuration 2021, 1).

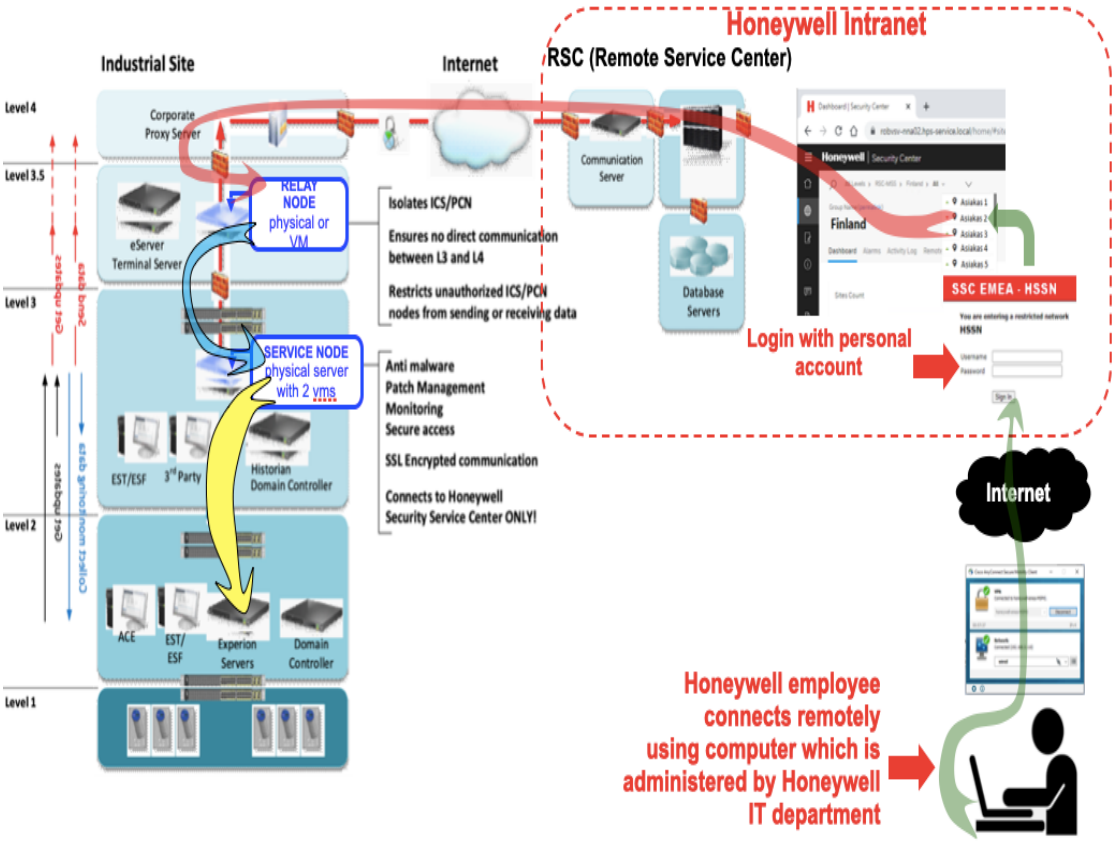


Kuva 30. OMIVV-koneen rekisteröinti vCenteriin(OMIVV installation and configuration 2021, 9)

5.9 Honeywellin etäyhteys

Asiakkaan virtualisoituun Experion PMD järjestelmään on mahdollista ottaa etäyhteys huolto- tai tukitoimia varten Honeywell Remote Service Centerin kautta. Etäyhteyden mahdollisuus tarjoaa laajan skaalan toimintojen suorittamista järjestelmälle ilman, että henkilöstön tarvitsee mennä paikan päälle. Tästä johtuen saadaan säästöjä niin asiakkaan näkökulmasta kuin työnsuorittajankin näkökulmasta. Erityisen hyödyn etäyhteys tarjoaa myöskin vikapäivystyksen osalta. Etäyhteyttä käytettäessä tarvitaan asiakkaalta erikseen pyydetty lupa. Jokaisella käyttäjällä on erilliset tunnukset, joiden avulla pystytään kirjautumaan Relay Node välityspalvelimelle ja tätä kautta itse Experion-järjestelmän palvelimille(Kuva 31). Etäyhteys käyttää SSL salattua kommunikointia.

Joillakin asiakkailla on käytössään myös omia VPN (Virtual private network) tai etäyhteyssovelluksia, joiden avulla on mahdollista ottaa yhteys järjestelmään.



Kuva 31.Etäyhteyden muodostaminen asiakkaalle (Honeywell 2020.)

5.10 Honeywell projektitoimintojen esittely

Honeywellilla eri projekteja hoitaa projektipäällikkö, jonka ensisijainen tehtävä on vastata toimitusprojektikokonaisuudesta, sen taloudesta, aikataulusta, toiminnasta ja laadullisesta tuloksesta. Projektipäällikkö on ensi sijassa organisoija, joka huolehtii projektin kaikkien alueiden toimeksiannoista, valvonnasta ja projektiryhmän yhteispelin sujuvuudesta sekä sisäisesti että tilaajalle projektin saattamiseksi toivottuun tulokseen. (Honeywell 2020.)

Myyntitapahtuman varmistuessa järjestetään Honeywellin sisäinen palaveri projektipäällikön ja myyjien kesken, jossa läpikäydään projekti. Excel-pohjainen järjestelmän kokonaisuuden määrittävä suunnittelu- ja konfigurointityökalu antaa tietoa järjestelmään liittyvistä lisensseistä ja komponenteista. Tätä työkalua hyödynnetään tarjousvaiheessa. Automaatiojärjestelmän päivtysprojekteissa asiakkaalta pyydetyissä lähtötiedoissa läpikäydään järjestelmäkonfiguraatio, sovellus, kuvat, lähdekoodit, PI-kaaviot, ohjelmaluettelo, I/O-listat ja piiriluettelot, toimintakuvaukset, piirikaaviot sekä lisättävät tai poistettavat piirit.

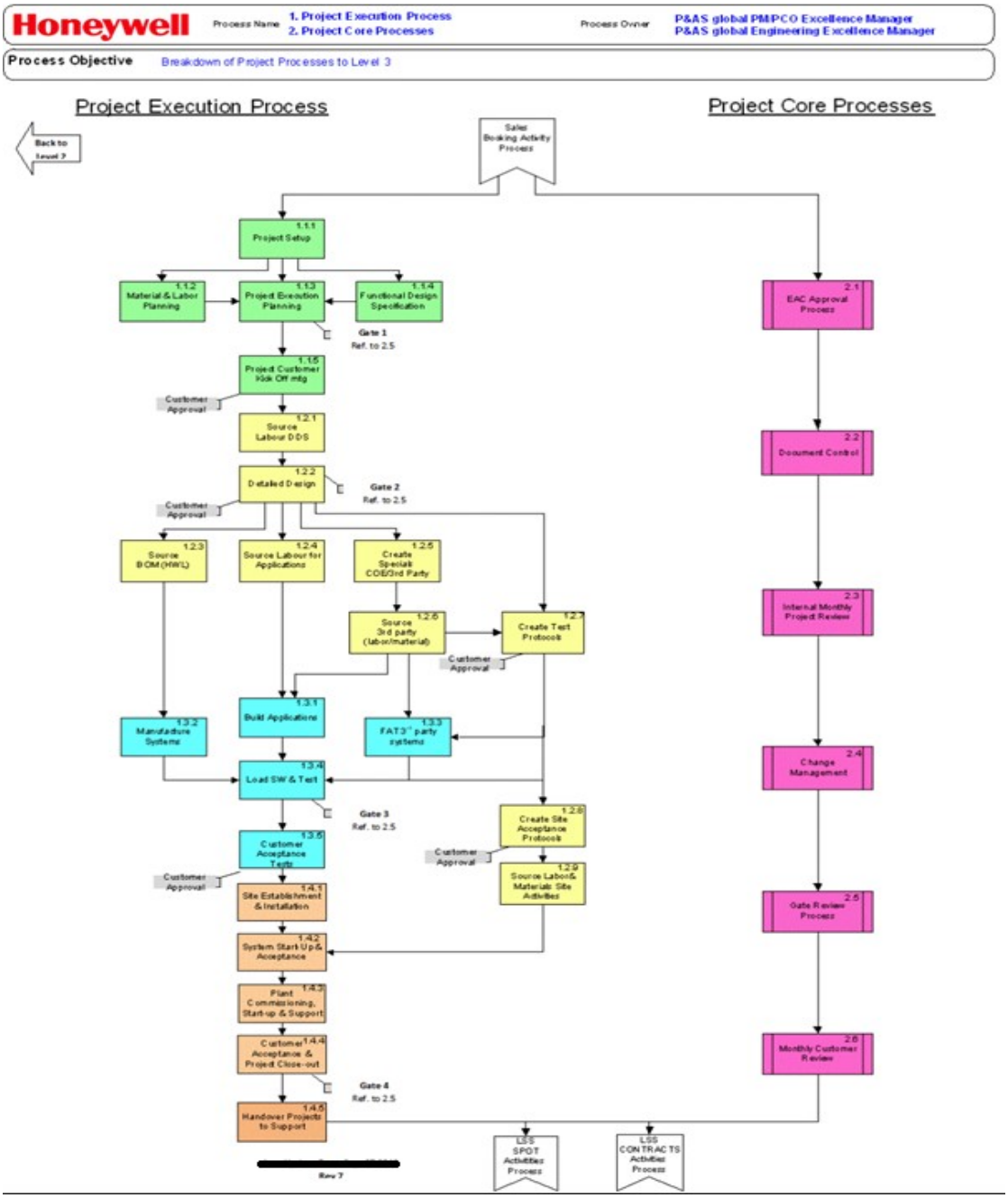
Myyntitapahtuman jälkeen sovellussuunnittelu voidaan aloittaa ilman loppuasiakkaalle tulevia lopullisia laitteita esimerkiksi erillisillä virtuaalijärjestelmillä. (Honeywell 2020.)

Seuraavassa vaiheessa tyypillisesti tilataan projektiin tarvittavat lisenssit ja komponentit Honeywellin hyväksymiltä toimittajilta. Samalla aloitetaan tekemään laitteistosuunnittelua ja järjestelmämäärittelyjä. Ennaltamääritellyn laitteiston saapuessa Honeywellin tiloihin ja yllämainittujen osa-alueiden ollessa kunnossa, tiloissa pidetään tuotannon aloituspalaveri. Palaveriin osallistuu projektipäällikkö, laitteistosuunnittelija, pääsuunnittelija, verkkosuunnittelijat ja varsinainen tuotannon väki, joka lopulta ajaa järjestelmät ylös. (Honeywell 2020.)

Järjestelmäkokonaisuuteen liittyvien ohjelmistojen ja laitteistojen asennuksen, integroinnin ja konfiguroinin jälkeen kokonaisuus siirtyy sovellusuunnitteluun tai sovelluksen käännösvaiheeseen. Käännösvaihe tarvitaan, mikäli asiakkaan sovellus siirretään uudempaan järjestelmäversioon. Sovellusuunnitteluvaiheessa automatiosovellus toteutetaan kokonaan, mikäli kyseessä on kokonaan uusi prosessiyksikkö. Mikäli kyseessä on jo olemassa olevan sovelluksen muuttaminen uudempaan järjestelmään, sovellussuunnittelussa voidaan tehdä sovellukseen muutoksia asiakkaan määrittelyjen ja toiveiden mukaisesti käännösvaiheen yhteydessä. (Honeywell 2020.)

Projektitoimitukseen kuuluu yleensä laitteiden ja järjestelmäkokonaisuuden testaus ennen varsinaista käyttöönottoa itse asiakkaalla. Tätä tapahtumaa kutsutaan yleisesti FAT-testaukseksi(Factory Acceptance Test). FAT-testauksessa käydään läpi sovellus, turvatoiminnot, laitekokoonpano, määrittelyt, kytkennät sekä muut sopimuksessa olevat asiat, jotta laitteisto vastaa sille asetettuja vaatimuksia. Ennen koronapandemiaa FAT-testausta tehtiin myös etänä. Koronarajoitusten aktivoituessa FAT-testaus on siirtynyt arkipäiväisemmäksi toimintamalliksi.FAT-testauksen jälkeen laitteistolle tehdään erilaisia lopputöitä, joihin sisältyy varmuuskopioiden ottaminen, FAT:ssa esiintulleet mahdolliset löydökset, jotka esimerkiksi asiakas haluaa toimivan eri tavalla, virusturva, erilaiset raportit Honeywellin työkaluilla sekä mahdolliset Microsoft Windowsin paikot.

Lopputöiden jälkeen järjestelmä on valmis pakattavaksi ja lähettettäväksi asiakkaalle. Asiakkaalle toimitettu Honeywell PMD-järjestelmä asennetaan heidän erikseeen määritellyihin automaatiotiloihin ja aloitetaan mahdollinen SAT-testaus(Site Acceptance Test). Järjestelmä kirjataan Honeywellin omaan tuotannonseurantajärjestelmään, johon päivitetään toimitetun järjestelmän kaikki laitetiedot sekä muutokset. (Honeywell 2020.)



Kuva 32. Honeywell projektien toteutuskaavio (Honeywell 2020)

6 AUDITOINNIN TULOKSET

Auditoinnissa arvioitiin Honeywell Experion PMD-järjestelmän eri osa-alueiden haasteita ja näiden parantamista virtuaalisen automaatiojärjestelmän osalta ennen FAT-testausta. Yhtenä lähtökohtana oli keskittyä järjestelmäkokonaisuuden yhdenmukaistamiseen ennen FAT-testausta, mikä lyhentää FAT-testauksen aikaa, työmäärää ja resursseja. Auditoinnin varsinainen tarkoitus oli minimoida FAT-testauksessa mahdollisesti ilmenneitä löydöksiä. Auditointi suoritettin Honeywellin toimipisteessä suomessa asiakkaan järjestelmään, ennen siihen tehtävää FAT-testausta viikolla 39. Auditointiprosessissa käytettiin asiantuntijaryhmän aikaisemmin räätälöityjä tarkastuslistoja. Näiden listauksien osalta työ aloitettiin alkuvuodesta 2022 ja asioita käytiin läpi säännöllisissä palavereissa. Jokaisella asiantuntijalla oli oma osa-alueensa, josta he olivat koostaneet materiaalia varsinaista auditointia varten. Allaolevissa luvuissa läpileikataan näitä osa-alueita ja niistä löytyneitä parannettavia kohteita.Työssä auditoitava projekti oli migraatioprojekti TP-Alcontista virtuaaliseen R920 PMD-järjestelmään.

6.1 EBR

Auditoinnin ensimmäisessä osiossa tutkittiin Acronis ohjelman toimintaa sekä varmuuskopiointiin vaikuttavia asetuksia. Osiossa myös katselmoitiin koneiden varmuuskopioiden aikataulutusta,varmuuskopiointisuunnitelmia, resursseja sekä varmuuskopioiden tilannetta yleisesti. Lisäksi ajettiin erillinen varmuuskopiointitesti jokaiselle konetyypille isäntäkoneilla oleville virtuaalikoneille.

EBR osuutta tutkittiin tarkastuslistan mukaisilla toimenpiteillä(Kuva 33). Tarkastuksessa esille tulleita löydöksiä oli viimeisimpien ohjelmistoversioiden osalta Acronis-ohjelmassa, EBR hallintapalvelimen käyttöjärjestelmässä sekä ESXi-koneella. Varmuuskopioinneista ei projektille löytynyt Excel pohjaista schedule dokumenttia, jonka perusteella virtuaalikoneet on aikataulutettu. Joillakin virtuaalikoneista ei näkynyt varmuuskopiointisuunnitelmaa ja osa varmuuskopioinnin tehtävistä näkyi kaksi kertaa, jolloin ilmoittaa virheestä vaikka varmuuskopiointi olisikin onnistunut kyseiselle virtuaalikoneelle. Acronis virtuaalikoneen resurssiasetuksien kohdalla muistia oli varattu vain 2GB vaikka sitä pitäisi ohjeistuksen mukaan olla 6GB. EBR User salasanan ja

käyttäjätunnuksen kanssa oli haasteita eikä näitä löytynyt dokumenteista. Tämän osa-alueen auditoinnista löytyi eniten parannettavaa.

		Mandatory	Mandatory
Check#1	EBR Management Win + ESXi appliance or plain AIO (no appliances) installed with latest version	Y
Check#2	Acronis virtual appliance resource allocation settings 2 vCPU / Memory 6 GB allocated	Y
Check#3	In VMware virtual machine settings, click Options tab > General > Configuration Param eters, and then ensure that the disk.EnableUUID parameter value is true	Y
Check#4	EBR Backup time should not match with windows time synchronization (started at e.g. xx:03, xx:18, xx:33, xx:48)	Y
Check#5	Recommended EBR Schedules for all nodes	Y
Check#6	No overlapping schedules	Y
Check#7	Disable Acronis check for updates functionality	Y
Check#8	Active Protection and Vulnerability assessment disabled in plan settings	Y
Check#9	Make test backup of each type of nodes/transfer modes (SMB/SFTP) on every host	Y
Check#10	Verify EBR recovery media supports your nodes (5820 etc)and matches installed version.	Y
Check#11	Test backup recovery	Y
Check#12	EBR Agent / AIO connection to vcenter	Y

Kuva 33. EBR tarkastuslista

6.2 Experion PKS Server Client

Tähän osioon kuuluvia tarkastuksia ei saatu auditoitua ajanpuutteen vuoksi. Tarkastuslistaan(Kuva 34) on koottu merkittävimmät kohdat Honeywell GTAC:in (Global Technical Assistance Center) auditointimateriaalista.

	A	B
1	Check, open instructions from here	Mandatory
2	Check # 1. Experion OPC Device Read option	Y
3	Check # 5. History Archive search Path should not contain network paths and be added to Antivirus Exclusions	Y
4	Check # 6. History Archive Configuration (siten että poistetaan arkistot tietyn ajan kuluttua)	Y
5	Check # 7. Online Events/ Event Archiving Periods	Y
6	Check # 9. Event Archiving Directory	Y
7	Check # 10. Event Queries and Archive Configuration Timeouts	Y
8	Check # 13. Tuning DSA Subscriber Connections	N
9	Check # 14. Checking that no remote points are assigned to Experion local history	N
10	Check # 15. Display Scripting – Perform Device Read After a Write	Y
11	Check # 17. DSA Alarm Acknowledgement / Shelving Policy Consistent over DSA	N
12	Check # 18. Verifying Share Heap Existence on Disk	Y
13	Check # 19. Making sure no points are assigned to Unassigned Items	Y
14	Check # 20. Checking for Duplicate Points	Y
15	Check # 21. CDA subsystem – Dynamic Cache Settings	Y
16	Check # 23. Server Raid Controller Write Policy	Y
17	Check # 24. Experion Server RAID Consistency Check	Y
18	Check # 29. Verifying that recent Approved Windows Security and Non Security updates are installed	Y
19	Check # 32. SQL Memory Configuration on Experion R410.x, R43x.x, R5xx.	Y
20	Check # 35. Setting Dell Servers to Performance profile in BIOS	N
21	Check # 39. Verify the Station Normal and Fast Update Rate	N
22	Check # 45. Free up hard disk space on Experion node	Y
23	Check # 49. Run the Experion Events SQL Database Maintenance.	Y
24	Check # 53. Check that the Win Tablet Service is Started by scheduled Task or GPO.	N
25	Check # 60. Verify the Fast Key Behaviour – Apply all display elements	N
26	Check # 61. Defrag Experion Server disks	N
27	Check # 63. Check Windows Appearance Configuration on Station or Orion Console	N
28	Check # 65. Check if CDA slow History assignment is configured with Offset	Y
29	Check # 67. System Performance May Degrade When IEC 61850 Is Not Licensed on Experion R5xx	N
30	Check # 72. Enable Enterprise Model Hierarchy on OPC Client Browse	Y
31	Check # 73. Verify the Display Scaling on Client Nodes on Experion R5xx	Y
32	Check # 77. Checking the Windows Power Scheme on Experion nodes	Y
33	Check # 78. Disable Windows Defender on Experion nodes	N
34	Check # 80. Enabling DSA Connection Response Time Alarm	N
35	Check # 82. Optimizing the alarm silencing processing in Experion Station	Y

Kuva 34. Exprion PKS Server Client tarkastuslista

6.3 PMD-verkkoympäristö ja FTE

Osiossa tarkasteltiin palomuurin sekä runko- ja reunakytkimien versioita, lisenssejä sekä konfiguraatioita ja erilaisia asetuksia laitekohtaisesti(Kuva 36). Tarkastus sisälsi viisi kappaletta runkokytkimiä ja kuusi kappaletta reunakytkimiä. Näiden lisäksi läpikäytiin yksi palomuuri. Laitteita tutkittiin PuTTY-sovelluksen avulla (Kuva 35).

```
Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*     1 28    C9200L-24T-4G      17.03.04b         CAT9K_LITE_IOSXE      INSTALL
```

Kuva 35. Kytkimen ohjelmaversion tarkastus PuTTY-ohjelmistolla (Honeywell. 2023)

Ohjelmistoversiot olivat kaikissa kytkimissä uudemmat mitä Honeywell on testannut ja validoinut automaatiojärjestelmiinsä yhteensopiviksi. Järjestelmän toimintavarmuuden kannalta esimerkiksi vikatilanteessa merkittävä puute oli kaikkien laitteiden konfiguraatioiden varmuuskopioiden puuttuminen NAS-palvelimelta. Näiden tiedostojen olisi tärkeä olla saatavilla viimeisillä

päivityksillä, jotta saadaan konfiguroitua uusi laite hajonneen tilalle nopeasti. Nämä konfiguraatiotiedostot otetaan talteen jokaisen määräaikashuollon yhteydessä ja viedään NAS-palvelimelle erilliseen kansioon.

Tarkennettavaa ja parannettavaa löytyi myös useista kuvista ja kytkennöistä. Laitteita oli kytketty vääriin portteihin ja kaikkia kaapeleita ei oltu merkitty asianmukaisilla kaapelitunnuksilla. Näistä on aiheutunut ongelmia kunnossapidollisesti verkkovikojen tutkimisessa. Tämän osa-alueen auditoinnista löytyi kolmanneksi eniten parannettavaa.

5		Mandatory	Mandatory
6	Check#1	Check Versions	Y
7	Check#2	Check Licensing	Y
8	Check#3	Check NTP	Y
9	Check#4	Check that port congifuration matches with hardware documents	Y
10	Check#5	Check spanning tree configuration	Y
11	Check#6	Check that every device is accessable remotely	Y
12	Check#7	Check that configurations are backed up	Y
13	Check#8	Check stacked switches priority and numbering	Y

Kuva 36.Verkkoympäristöön liittyvät tarkastukset

6.4 PMD-tarkastukset

Osiossa tarkasteltiin PMD-järjestelmän ajanjakelua ja Meinbergin NTP konfigurointiasetuksia, järjestelmässä olevien PMD-palvelimien tilaa ja niiden tärkeimpiä asetuksia ja lokitiedostoja järjestelmän toiminnan kannalta (Kuva 36). Prosessinohjauksen osalta käyttöliittymien(HMi) ja RHS-palvelimen tarkastettiin käyttäjäsuojauksia ja hälytysmäärittelyjä sekä operointiin käytettävien käyttöliittymien toimintaa. Osion tarkastuksiin kuuluivat myös FTE-tarkistukset.

	Point	Tarkastus	Dokumenttihakemisto	Pakollinen
1		**PMD järjestelmä:**		
2		Ajanjakelu		**K**
3		**DM:**		
4		Meinberg asetukset	PMD Audit\Time delivery\TimeShare Meinberg.pdf	K
5		Virus skannerin exlude määrittelyt	PMD Audit\Antivirus\anti-virus-software-guidelines.p	E
6		**PMD palvelin:**		
7		PDS ja EPKS serverien tilat		K
8		Testaa serverien kahdennus vaihtamalla ajavaa ja synkronoimalla		E
9		Testaa serverien käynnistyminen ilman kahdennusparia		K
10		Tarkasta kuvat HMIWeb display builderin Validate Displays toolilla		K
11		History assignment Standard offset	PMD Audit\History assignment	K
12		Virus skannerin exlude määrittelyt	PMD Audit\Antivirus\anti-virus-software-guidelines.p	E
13		Serverin tila: avaa Dell Open management ja tarkasta mahdolliset virheet.		K
14		FTE tila *fte_sysmgmt* työkalulla	PMD Audit\FTE sysmgmt\fte checker DCG.pdf	K
15		FTE status		
16		PMD lokit, onko virheitä		K
17		Windows lokit, onko virheitä		K
18		Lokalisointi		E
19		MS Security patchit asennettu		K
20		DCOM/OPC kovennuksen esto rekisteriavaimet		K
21		**HMI / RHS palvelin:**		
22		Station määritykset		K
23		Käyttäjäsuojaukset User-käyttäjällä		K
24		Hälytysvälityksen toiminta		K
25		**Kontrollerit:**		
26		Kahdennetun kontrolleriparin tila		K
27		Käynnistä kaikki järjestelmän kontrollerit testijärjestelmässä		K
28		Sovelluksen ajo		K
29		Käynnistä sovellus		K
30		Mahdolliset ajonaikaiset virheet		K
31		Tarkasta tapahtumapohjaiset prosessit		E
32		Ratkeamattomat viittaukset (ghostit)		K
33		I/O status, jos kytketty		E
34		Tarkasta vaiheistus		K
35		Kontrollerin kuormitus		K
36		Ympäristömuuttujat		K
37		Kontrollereiden asetukset (NTP ym)		K
38		**Builder:**		
39		ECI määrittelyt ladattu?		
40		Kontrollereiden asetukset		
41		STN tiedostot		
42		KAIKKI KONEET		K
43				

Kuva 37.PMD-tarkastuslista

Löydöksien osalta auditoitavassa järjestelmässä ajanjakelu oli toteutettu poikkeuksellisesti väliaikaisratkaisulla komponenttipulan vuoksi, jolloin ajanjakelijaksi oli konfiguroitu virtuaalikone Meinbergin NTP-asetuksissa. Lisäksi projektin ajanjakelusta ei löytynyt dokumentaatiota, vaikka näin ei tässä vaiheessa saisi olla. Yksi huolenaihe oli Microsoftin DCOM kovennuksen esto. Tämän asetuksen muutos puuttui kaikiilta koneilta rekisteriavaimesta, joka voi aiheuttaa Microsoftin maaliskuun Windows päivitysten jälkeen OPC-tiedonsiirron ongelmia ulkoisille laitteille. Tarkastuslistassa oli muutamia kohtia liityen serverien puolenvaihtoihin ja kahdennuksiin joita ei tarkastettu, koska näille osioille on oma erillinen tarkastus FAT-testissä. Listauksessa oli myös prosessinohjaimien tarkistukset Honeywellin DAXMON-työkalulla, mutta nämäkin tarkistetaan FAT-testauksessa. Tämän osa-alueen auditoinnista löytyi vähiten parannettavaa.

6.5 Virtualisointi

Auditoinnin viimeisessä osiossa käytiin läpi virtuaaliympäristön isäntä koneiden fyysisiä resursseja, verkkoasetuksia ja virtuaalijärjestelmään liittyvien komponenttien tärkeimpiä toimintoja sekä laiteohjelmistoversioita(Kuva 38). Kirjautumiseen liittyvät ongelmat olivat esillä salasanadokumenttien arkistointikäytäntöjen takia vCenter hallintakoneelle kirjautuessa. Tarkastuksen jälkimmäisessä osiossa auditointiin käytettiin apuna RVTools-ohjelmistoa, joka kerää tietoa vCenter-palvelimelta

isäntäkoneiden resursseista sekä virtuaalikoneilta luoden näistä suoraan raportin Exceliin.

Resurssointia läpikäydessä järjestelmän useilla isäntäkoneilla oli levytilaa jäljellä alle 20% tai lähellä tätä minimirajaa. Kahden isäntäkoneen osalta myös muistia oli käytössä alle 20% kapasiteetista. Virtuaalikoneiden osalta levynhallinta tarkastuksessa löytyi parannettavaa Service Node-palvelimen sekä Realy Node-palvelimen resursoinnista. Resurssointi Excel:iä ei ollut saatavilla, joista nämä määritykset olisi voitu tarkastaa.

Kiintolevyjen laiteohjelmistot ja osa BIOS versioista olivat ajantasalla, mutta useilta koneilta BIOS versio poikkesi halutusta. Näiden päivittämiseen tarkoitettua viimeisintä DELL Server Update Utility ISO (SUU) tiedostoa ei ollut saatavilla. Viimeisimmät koneiden laiteohjelmistoversiot tarkistettiin iDRAC-hallintapaneelista.

Joiltain koneilta puuttuivat NTP-asetukset tai nämä olivat puutteelliset. Ajanjakeluun liittyvää dokumentaatiota ei ollut saatavilla vielä tässä vaiheessa projektia, vaikka ihannetilanteessa tämän osa-alueen olisi hyvä olla jo valmiina.

			Mandatory
6	Check#1	Domain login works from vSphere Client/virtual client and other domain members when only one DC is online	Y
7	Check#2	Domain replication is working	Y
8	Check#3	DNS test is passed	Y
9	Check#4	DNS has entries for all machines connected to management network	Y
10	Check#5	Domain PDC is getting time from physical machines in L2 /L 2.5 Network (Meinberg servers)	Y
11	Check#6	Domain members are getting time from PDC	Y
12	Check#7	vCenter login with domain vcenteradmin account	Y
13	Check#8	vCenter login with administrator@vsphere.local	Y
14	Check#9	vCenter appliance login with root	Y
15	Check#10	vCenter root password expiration disabled	Y
16	Check#11	vCenter has the same NTP servers as in PDC and time matches	Y
17	Check#12	All ESXi hosts are using the same NTP server as vcenter/PDC and service is running	Y
18	Check#13	All ESXi hosts have RAM / Disk / CPU 20% resources left	Y
19	Check#14	Add additional RAM and Disks space to fullfill resource requirements	Y
20	Check#15	Idrac has NTP and DNS servers configured.	Y
21	Check#16	Idrac virtual console is working	Y
22	Check#17	Latest DELL BIOS / Firmwares are installed	Y
23		Virtual disk consistency check for all hosts	Y
24		Force Write Back configured in iDrac for Virtual disk	Y
25	Check#18	Run RVTOOLS and verify results to :	Y
26	Check#19	*PMD Virtualization Specifications and*	Y
27	Check#20	*Experion VM and Host Performance Assessment Cheat Sheet*	Y
28	Check#21	Test OMIVV alarms from Idrac of each hosts	Y
29	Check#22	VM settings and disk provisioning is set correctly	Y

Kuva 38. Virtualisointitarkastukset osio 1

Allaolevat tehdyt tarkastukset oli koottu erilliselle välilehdelle(Kuva 39). Näissä tarkastuksissa arvioidaan isäntäkoneiden ja vituaalikoneiden suorituskykyä.

Parannettavaa löytyi isäntäkoneiden CPU:n osalta määrittelyistä CPU-socketien määrässä, joita täytyy olla määriteltynä yksi kappale jokaiselle virtuaalikoneelle. Tämä ei koske ainoastaan Experion-virtuaalikoneita vaan kaikkia isäntäkoneella olevia virtuaalikoneita. Tämän osa-alueen auditoinnista löytyi toiseksi eniten parannettavaa.

1	**Check20**	**Experion VM and Host Performance Assessment Cheat Sheet #18**	
2	**RVTOOLS**	vCPU	No limits
3			CPU with 1 Socket
4			Hot Add = Disabled (False)
5			Hot Remove = Disabled (False)
6			Check Reservation
7		vDisk	Thick provisioning
8			No IOP limits
9		vSnapshot	No snapshots
10		vNIC	Check Speed&Duplex
11		vDatastore	At least 30% free space
12		vHost	Checck Current EVC vs Max EVC
13			Check NTP Server is configured
14		vNetwork	Adapter type is Vmxnet3
15		vTools	Check Tools is up to date
16		vMemory	Balloned = 0 , also no swap
17			Hot Add = Disabled (False)
18			Size MB Should be same than Reservation
19		vCD	Connected = False
20			Starts Connected = False
21		vHealth	Check if there are system events
22		CPUReadiness	>1%
23		vHost	Current EVC Configuration:
24		vNetwork	VMs NIC adapter type Vmxnet3
25		vNetwork	Virtual adapters configuration:
26		vTools	VMWare Tools version

Kuva 39. RVTools:lla tehdyt virtualisointitarkastukset osio 2

7 YHTEENVETO JA KEHITTÄMISKOHTEET

Tuloksia analysoitiin asiantuntijatyöryhmän, myyjien, projektihenkilöstön ja tuotannon kanssa käytyjen keskustelujen ja palaverien sekä omien näkemysten perusteella. Osiossa läpikäydään esille tulleita havaintoja ja parannuskohteita virtualisoidun järjestelmän toteutusvaiheissa aina FAT-testausvaiheeseen asti. Lisäksi osiossa annetaan mahdollisia kehittämisehdotuksia ja ideoita.

7.1 Myyntitapahtuma

Myyntityö on oleellinen asia yrityksen liiketoiminnassa. Ilman myyntiä yritykselle ei tule kauppaa, eikä näin ollen yrityksen liiketoiminnasta voi tulla kannattavaa. Honeywell Oy:lla on laaja historia DCS-järjestelmien toimittamisesta Suomeen ja myyjien rooli tuleekin esille vahvana osaamisena

ja erilaisten teollisuudenalojen automaatiojärjestelmien tarpeiden tunnistamisena.

PMD-järjestelmän osalta myyjä selvittää nykyisen kokoonpanon yhteistyössä Honeywell huolto- ja projektiasiantuntijoiden sekä asiakkaan kanssa ennen projektin alkamista. Tässä opinnäytetyössä esillä oleva migraatioprojekti on laskettu vuonna 2020 ja myyty vuonna 2021, jolloin resurssien laskentaan tarkoitettu Exel-pohjainen konfiguraattori työkalu ei ole ollut viimeisin versio. Osaksi tästä johtuen koneiden fyysiset resurssit ovat joillakin isäntäkoneilla lähellä minimireserviä.

Myyntihenkilöille mahdollistettava jatkuva koulutus ja tuki, jotta pystytään takaamaan riittävän laaja-alainen järjestelmä- ja versiotuntemus myyntihetkellä asiakkaan tarpeeseen nähden.

7.2 Lähtötiedot, dokumentointi ja versionhallinta

Toimitusketjun sujuvaan etenemiseen vaikuttavat oleellisesti alussa saadut tarkat lähtötiedot pitäen sisällään tavoitteet, tehtävät, projektin rajauksen sekä aikataulutuksen ja dokumentoinnin.
Virtualisoidun PMD- automaatioärjestelmän laajuuudesta ja kokoonpanosta riippuen sen sisältämien komponenttien, laiteohjelmistojen ja versioiden tulee olla Honeywell Oy:n vaatimalla tasolla.

Tuotannossa tuli esille ylösajovaiheessa kytkentäkuvia, joissa oli korjattavaa. Kytkentäkuvia korjataan ja järjestelmään liittyviä muutoksia tehdään projektin edetessä edestakaisin usealta taholta, joka luo haasteita ajankohtaisimpien dokumenttien saatavuudesta. Toisaalta ylösajovaiheessa on joissain tilanteissa mahdoton toteuttaa järjestelmän kytkentää kuvien mukaisesti, kun kyseessä on järjestelmän päivitys yhdistetyistä osastoista, jolloin osa laitteistosta on jo asiakkaan tiloissa tai jotain järjestelmän osaa ei ole saatavilla.

Versionhallinnan näkökulmasta haasteita on esiintynyt isäntäkoneiden ja kytkimien laiteohjelmistojen sekä isäntäkoneiden VMware ja BIOS-versioiden

osalta aiheuttaen ylimääräistä työtä päivitysten muodossa ennen FAT-testausta tai sen aikana.

Lähtötiedot elävät yleensä projektin edetessä, jolloin tiedot kaikista muutoksista tulisi tavoittaa projektissa olevat henkilöt ilman viivettä, jotta asioita ei tarvitse tehdä useaan kertaan. Projektin dokumentaation tulisi löytyä yhdestä paikasta ja päivitysten ollessa ajankohtaisia tehtäisiin muutokset erillisesti sovitun päivitysprosessin mukaan, jotta varmistutaan kuvarevisioiden paikkansapitävyydestä. Laitteiden versionhallintaan tulisi kartoittaa mahdollisuutta henkilöresurssille seuraamaan, vertailemaan ja ylläpitämään kantaa viimeisimmistä ohjelmistoversioista laitevalmistajien ja Honeywell Oy:n sisäisen validoinnin välillä.

7.3 Inhimilliset virheet

Järjestelmien ylösajo pitää sisällään automaatiojärjestelmään kuuluvan laitteiston asentamisen ja kytkemisen tuotantotiloihin sekä järjestelmän vaadittavien määrittelyjen teon. FAT-testauksen jälkeen tuotantohenkilöstö pakkaa valmiin järjestelmän asiakkaalle toimitettavaksi. Tuotantohenkilöillä on omat Honeywellin toimittamat ohjekansiot järjestelmämääritysten tekemiseen, joihin päivitetään mahdollisesti ilmenneet muutokset. Tuotannolla on lisäksi erilliset seurantamonisteet, joihin päivitetään työn kulku.

Tuotannolla on työn alla useita järjestelmiä yhtäaikaa ja eri järjestelmien välillä voi joutua työpäivän aikana käymään jonkun työvaiheen läpi ja sitten palata takaisin edellisen työn pariin. Tuotantotiloissa on paljon ihmisiä töissä järjestelmien eri vaiheissa sekä projekteissa, joten kysymyksiä ja keskeytyksiä tulee aika ajoin. Tälläisissä tapauksissa inhimillisen virheen mahdolisuus korostuu ja joku työvaihe voi jäädä tekemättä tai jäädä kesken. Kiire tai kiireentuntu aiheuttaa myös virheitä tai unohduksia ja lomat sekä muut poissaolot aiheuttaa haasteita, jos seuranta ei ole ajantasalla. Inhmillisiä virheitä ei koskaan täysin voi sulkea pois, oli prosessi kuinka vankalla pohjalla tahansa.

Nykyisellään järjestelmien ylösajossa oleva seurantamoniste on Excel-pohjainen paperituloste. Yhtenä kehitysehdotuksena nykyiselle

seurantamonisteelle voisi olla sähköisen seurannan tekeminen nykyiselle Excel-pohjalle, johon sisällyttäisi jokaisen työvaiheen erikseen tarkastuslistoineen ja seuraavaan vaiheeseen siirtyminen vaatisi kuittauksen tekijältä. Lisäksi jokaisen keskeytyksen tullessa tai tauoille lähdettäessä olisi helppo laittaa merkintä missä kohdassa on menossa. Tähän pohjaan voisi myös linkata ylösajo-ohjeet, jolloin näiden päivittämisestäkin tulisi nopeampaa ja helpompaa.

7.4 Tuotannon tilat

Honeywell OY:n tuotantotilat tuo haasteita ahtaudellaan ja ikääntyneellä tekniikallaan. Tuotantotilojen ahtaus johtuu tällä hetkellä vaikuttavasta globaalista komponenttien saatavuus ongelmista, jotka aiheuttavat pitkiä toimitusaikoja. Tämä osaltaan vaikuttaa myös järjestelmien asennus ja määrittelyvaiheen kestoon. Järjestelmät ovat pidempään tuotantotiloissa, joka tuo lisähaasteita tilantarpeen osalta. Tiloissa on käynnissä useita projekteja näiden eri vaiheissa sekä huollon toimintaa DCS:n kuin QCS:nkin puolelta. Järjestelmien kokoonpanovaiheessa ei välttämättä saada koko järjestelmää ja kaikkia näyttöjä mahtumaan näille suunniteltuihin tiloihin. Tästä johtuen näyttöjä tai laitteita voidaan joutua siirtelemään edestakaisin pakkauksistaan ja järjestelmiä ylösajetaan pienissä pätkissä. Tälläisistä ylimääräisistä vaiheista aiheutuu turhaa työtä vieden resursseja, se myös vaikuttaa työntekijöiden voimavaroihin heikentävästi niin henkisellä kuin fyysiselläkin puolella. Toisinaan järjestelmät voivat olla pitkiäkin aikoja tuotantotiloissa kokoonpantuna odottaen toimitusta tai seuraavan työvaiheen estävää syytä. Tästä aiheutuu välillisesti myös logistisia ongelmia.

Tuotantotiloissa olevat ilmanvaihtokoneet ovat riittämättömät. Tuotantotilat sijaisevat suhteellisen ikääntyneessä rakennuksessa. Toisaalta virtualisoituja automaatiojärjestelmiä voidaan tuottaa pienimmissä tiloissa verrattuna erillisiin PC-pohjaisiin järjestelmiin, jotka vaativat merkittävästi laajemman pinta-alan yhtä järjestelmää kohti. Näin ollen lämmöntuotanto on suurempaa ja tämä yhdistettynä vanhan rakennuksen ilmavaihtolaitteisiin ja niiden kapasiteettiin lämpö ja ilmanlaatu vaikuttavat keskittymiskykyyn sekä jaksamiseen heijastaen sen työn laatuun. Järjestelmien osalta myös sähkönsyöttö on aiheuttanut haasteita, kuitenkin vähemmän nykyisen uuden hallin puolella.

Honeywell Oy on on kartoittanut uusia toimitiloja sekä laajentanut nykyistä tuotantotilaa tämän asian parantamiseksi(Kuva 40). Järjestelmät eivät saisi jäädä lojumaan pitkiksi ajoiksi tuotannon tiloihin, tämä vaatii suunnitelmallisuutta ja ennakointia projektissa olevalta työryhmältä, tosin ulkopuolisiin ongelmiin ja yllätyksiin on hankala varautua.

Kuva 40. Tuotannon lisätilat

7.5 Tiedonkulku

Projektissa olevien osapuolien välistä kommunikaatiota voi aina parantaa eikä sen tärkeyttä voida koskaan liikaa korostaa. Monitahoisen työyhteisön kommunikointi ei saa katketa tai viivästyä, eikä tieto saa matkalla muuttua. Eri osapuolien avoin tiedonkulku edesauttaa projektin sujuvan edistymisen ilman vaivalloisia ja aikaavieviä selvitystöitä, jotka menevät useasti monen eri henkilön kautta. Ajoittaiset useiden projektien päällekäisyydet aiheuttavat tuotantoon kiiretilanteita ja kiireessä työskentely aiheuttaa myös tiedonkulkuun haasteita.

Tuotannossa on ollut tilanteita, joissa järjestelmään on käyty tekemässä muutoksia ja tarvittaville osapuolile on tiedotettu puutteellisesti. Toisinaan järjestelmää koskeviin kysymyksiin ja tiedusteluihin reagoidaan viiveellä, niin projektin puolelta kuin asiakkaan puolelta. Aloituspalaveria lukuunottamatta projektin aikana ei seurata projektin vaiheita ja avoinna olevia kysymyksiä säännöllisesti läpi palavereissa. Asioita selvitellään sähköpostitse, puhelimitse tai paikan päällä tuotantotiloissa. Tiedonkulku on varmistettava ketjun alkupäästä loppupäähän ja toisinpäin. Kokonaisprojektin lopetuspalaverin tietoja ei välttämättä jaeta koko toimitusketjun tietoon ja näin ollen esimerkiksi niitä asioita, joita voidaan parantaa tuotannossa ei tule riittävän usein tiedoksi kokoketjulle.

Sisäistä viestintää tulisi parantaa projektien sisällä. Tämänhetkisessä tilanteessa ei ole olemassa selkeää viestintästrategiaa. Oma näkemykseni olisi, että pääsuunnittelijan ja projektipäällikön kommunikointia olisi parannettava tuotantohenkilöstön sekä suunnittelutoimiston kanssa säännöllisillä palavereilla. Tällä hetkellä pääsuunnittelija sekä projektipäällikkö kommunikoivat asiakkaan edustajan kanssa ja sieltä saatu tieto ei välttämättä tavoita tuotantoa. Palavereissa käytäisiin läpi projektin etenemistä, avoinna olevat kysymykset, projektin muutokset, aikataulut, ongelmat ja dokumenttien päivitykset. Näiden osa-alueiden pohjalta määrättäisiin vastuuhenkilöt ja tehtävät. Mahdollisien toimenpiteiden etenemistä tarkasteltaisiin seuraavissa palavereissa. Lisäksi näkisin, että projektikohtaisesti tarvitaan kaikkien osapuolien tavoittava, nopea ja muusta toiminnasta irti oleva sähköinen viestintäkanava tai sovellus, jonka kautta voidaan jakaa tiedostoja. Tällä mallilla on mahdollista saada vastauksia nopeammin.

7.6 Työtavat

Virtualisoitujen järjestelmien osalta järjestelmän kokonaisvaltaisen määrittelyn ja dokumentoinnin tarve ennen tuotannon aloitusta on korostunut. Aikaisemmissa järjestelmissä ennen virtualisointia toimintamallit mahdollistivat helpommin järjestelmän sovellusvaiheen aloittamisen ja järjestelmän kokoonpanon hallinnan sekä dokumentoinnin samanaikaisuuden ilman ylimääräisiä korjauksia ennen FAT-testauksen alkamista. Virtualisoidun järjestelmän toteuttaminen asettaakin projektin pääsuunnittelijan toimintapojen

terävöittämistä varsinkin järjestelmän kokonaisuuden kannalta projektin alkumetreille. Lisäksi jokainen pääsuunnittelija tekee projektin omalla tavallaan eikä tähän ole päässyt syntymään selvää standardoitua toimintamallia.

Honeywellin henkilöstö on koulutettua ja ammattitaitoista, mutta projekti ei voi nojautua pelkästään henkilöiden ammattitaidon varaan, vaan on kartoitettava paikallisesti mahdollisten projektinhallintaan tarkoitettujen työkalujen käyttöönottoa sekä mahdollisuutta PMD-järjestelmien tuotannon standardointia paikallisesti kirjatuksi toimintamalliksi, tällöin työn vaiheesta, tilanteesta tai tekijästä riippumatta tiedetään tarkasti missä vaiheessa ollaan menossa ja pystytään jatkamaan työtä, jos tekijä vaihtuu. Yhtenä vaihtoehtona olisi kartoitettava mahdollisuutta pilkkoa ja aikatauluttaa PMD-tuotantoprojekti pienempiin kokonaisuuksiin, jolloin sen hallinnasta, henkilöstön resurssoinnista ja seurannasta tulisi helpompaa. Lisäksi eri projekteihin voisi ottaa mukaan henkilön, joka olisi eri projekteissa alusta loppuun ja katselmoisi sekä kehittäisi niiden toimintaa ottaen huomioon eri osapuolien näkökulmat asioihin.

8 POHDINTA

Opinnäytetyössä tutustuin laajasti Honeywell Experion PMD-järjestelmän toimintaan ja laitteisiin I/O-tasolta toimistotasolle sekä näiden virtualisointiin. Työn ohessa tuli myös tutuksi Honeywell Oy:n projektitoiminnot. Auditoiminen käsityksenä ei ollut aikaisemmin minulle tuttu, joten siltäkin osalta opinnäytetyö palveli uusien toimintatapojen ja oppimisen sisäistämistä. Opinnäytetyö palveli erinomaisesti Honeywell Oy:n automaatiojärjestelmän hahmottamisessa ja tukena uusien työtehtävien opettelussa. Suurimpina haasteina opinnäytetyön edetessä oli ajankäytön resursointi varsinaisen työkuorman vaihdellessa ja aiheen laajuudesta huolimatta tuoda Honeywell Oy: virtualisoidun PMD-järjestelmän rakenne esiin mahdollisimman selkeästi kokonaisuuden hahmottamisen kannalta. Toisinaan opinnäytetyön etenemisessä oli jopa yli kuukauden taukoja, jolloin uudelleen kirjoitusrytmiin pääseminen ja asian uudellen sisäistäminen oli hankalaa.

Tämän auditoinnin tuloksia vertaillaan seuraavan järjestelmän auditoinnin tuloksiin, jotta nähdään millainen kehityssuunta toimenpiteillä ja parannuksilla on saavutettu. Tarkoituksena on saada tarkastuslistat ja prosessi mahdollisimman tehokkaaksi ja aukottomaksi, jotta erillisiä auditointeja ei tulevaisuudessa tarvittaisi. Jokaisen toimittettavan järjestelmän kokoonpano on erilainen, mutta laadukas projektin hallinnointi ja työkalut sekä laaja-alainen sitoutuminen antavat mahdollisuuden lyhentää FAT-testaukseen kuluvaa aikaa niin Honeywell Oy:n henkilöstöltä kuin asiakkaalta. Kun meillä on standardoidut prosessit, toimiva projektinhallinta, standardidokumentit, toimivat tarkastuslistat sekä järjestelmien versionhallinta kunnossa, niin auditointien tarve vähenee tai poistuu kokonaan.

Honeywellin tiivis yhteistyö ja pitkät, jopa kymmenien vuosien asiakassuhteet mahdollistavat laajamittaisen kehityksen virtualisoitujen automaatiojärjestelmien osalta nyt ja tulevaisuudessa. Virtualisoitujen automaatiojärjestelmien yleistyessä myös niiden investointikustannukset alkavat tasaantumaan verrattuna perinteisiin automaatiojärjestelmiin. Asiakkaalle jääkin mietittäväksi haluavatko he tulevaisuudessa helpommin ylläpidettävän, paljon mahdollisuuksia ja toimintoja sisältävän virtuaalisen järjestelmän, vai enemmän tilaa vievän perinteisen automaatiojärjestelmän jonka kertainvestointikustannus voi olla pienempi, mutta ylläpitokustannukset suuremmat pidemmässä tarkastelussa.

LÄHTEET

Dell. 2023. Artikkelinumero: 000179517. WWW-dokumentti. Saatavissa: https://www.dell.com/support/kbdoc/en-in/000179517/dell-poweredge-how-to-configure-the-idrac-system-management-options-on-servers [viitattu 02.05.2023].

Describe an overview of virtualization technology. 2022. PDF-dokumentti. Honeywell Oy.

Describe basics and configuration thin client. 2021. PDF-dokumentti. Honeywell Oy.

Describe system architecture. 2021. PDF-dokumentti. Honeywell Oy.

Describe the network planning. 2021. PDF-dokumentti. Honeywell Oy.

Describe the process to create template. 2022. PDF-dokumentti. Honeywell Oy.

Describe the VMware products used for virtualization. 2022. PDF-dokumentti. Honeywell Oy.

Experion PKS with PMD controller network planning and design guide. 2018. PDF-dokumentti. Honeywell Oy.

Experion PMD Network & Cyber Security. 2020. PDF-dokumentti. Honeywell Oy.

Honeywell Oy. 2020. HPS, GPM. Intranet.

Honeywell Oy. 2023. Sisäinen virtualisointikoulutus 8.2.2023.

OMIVV installation and configuration. 2021. Word-dokumentti. Honeywell Oy.

Virtuaalijärjestelmä rakenne ja komponentit. 2023. Sisäinen virtualisointikoulutus materiaali. Honeywell Oy.

Zurfluh R. 2020. IEC62443 – Or How To Implement OT Security in AN Efficient And Reliable Way. Blogiteksti. InfoGuard. 2023. Saatavissa: https://www.infoguard.ch/en/blog/iec-62443-or-how-to-implement-ot-security-in-an-efficient-and-reliable-way [viitattu 27.04.2023].