Vladimir Pöyhönen

Automaatiojärjestelmän virtualisointi

Korkean käytettävyyden klusteri

Metropolia Ammattikorkeakoulu

Insinööri (ylempi AMK)

Automaatioteknologia

Opinnäytetyö

19.5.2014

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Vladimir Pöyhönen Automaatiojärjestelmän virtuaalisointi 35 sivua + 2 liitettä 19.5.2014
Tutkinto	Insinööri (ylempi AMK)
Koulutusohjelma	Automaatioteknologia
Suuntautumisvaihtoehto	Automaatiojärjestelmän virtualisointi
Ohjaaja(t)	automaatioasiantuntija Jaakko Järvinen Lehtori Jukka-Pekka Pirinen

Tämän työn tarkoitus oli tutkia nykyisen ICT-virtualisoinnin käyttöä hajautetussa automaatiojärjestelmässä. Tutkimuksen aikana on pohdittu mahdollisimman helppokäyttöinen ja varma ratkaisu, jonka jälkeen tämän ratkaisun peruskokeet suoritettiin koelaitteistolla.

Tutkimus ja kokeet osoittavat, että nykytietotekniikan virtuaalisoinnin käyttö teollisuusprosessiohjausjärjestelmissä on mahdollista ja tehokkaasta, mutta esiintyy myös rajoitteita ja estoja.

Nykyisin virtualisoinnin käyttö DCS:ssa on riippuvainen automaatiotoimittajalta. Automaatiotoimittaja määrittelee missä oman DCS:n osa-alueissa virtualisointia käytetään ja minkälaista virtualisointiominaisuuksia kyseisissä osa-alueissa ovat sallittuja. Jotkut automaatiotoimittajat ovat tuotteistaneet hyvin DCS-tuoteita, jotka on perustettu virtualisointiin. Monet automaatiotoimittajat eivät ole halukkaita muuttaa vakiintunutta DCS:n ICT:n toteutusta eikä käytetä virtualisointia lainkaan.

Avainsanat	virtualisointi, automaatio, korkean käytettävyyden klusteri

Author(s) Title Number of Pages Date	Vladimir Pöyhönen DCS Virtualization 35 pages + 2 appendices 19 May 2014
Degree	Master of Engineering
Degree Programme	Automation Technology
Specialisation option	DCS Virtualization
Instructor(s)	Jaakko Järvinen, Automation Specialist Jukka-Pekka Pirinen, Senior Lecturer

The purpose of this project was to investigate the current use of ICT virtualization in a distributed control system. During the study, the easiest to use and reliable solution was considered, after which the solution to the basic experiments were performed on the test equipment.

Research and experiments indicate that the current use of ICT virtualization in the industrial process control system is feasible and effective, but also confronted with constraints and inhibitions.

Nowaday, virtualization use of DCS is dependent on the automation supplier. Automation supplier determines in which DCS sub-areas virtualization is implemented and what kind of virtualization features in these sub-areas are allowed. Some of the suppliers of automation products are the very DCS-shape the goods that have been established for virtualization. Many automation suppliers are not willing to change the well-established DCS ICT implementation and use virtualization at all.

Keywords	virtualization, DCS, high availability cluster

Sisällys

Lyhenteet

AD	Active Directory	Windows-hakemistopalvelu
DCS	Distributed Control System	Hajautettu ohjausjärjestelmä
DNS	Domain Name System	Nimipalvelujärjestelmä
FT	Fault Tolerance	Vikasietoisuus
HA	High Availability	Korkea käytettävyys
ICS	Industrial Process System	Teollisuusprosessisysteemi
KVM	Keyboard Video Mouse	Näppäimistö Näyttö Hiiri
PLC	Programmable Logic Controller	Ohjelmoitava logiikka
Remote I/O	Remote Input/Output	Hajautetut tulot/lähdöt
RDP	Remote Desktop Protocol	Etätyöpöytäprotokolla
RSTP	Rapid Spanning Tree Protocol	Nopea STP-protokolla
RTD	Real Time Device	Reaaliajan laite
RTU	Remote Terminal Unit	Etäterminaaliyksikkö
UTM	Unified Thread Management	Yhtenäinen havoittavuushallinta
VM	Virtual Machine	Virtuaalikone
WSUS	Windows Server Update Services	Windows-päivityspalvelun palvelin

1 Johdanto

Teollisuuden automaatiojärjestelmät kehittyvät koko ajan ja tietotekniikan käyttö prosessiohjauksessa on lisääntynyt merkittävästi. Tänä päivänä tyypillinen DCS (hajautettu automaatiojärjestelmä) sisältää useita sovellus-, tiedonkeruu- ja integrointipalvelimia sekä operointi-, sovellus- ja ylläpitotietokoneita. Nämä ATK-laitteet on yhdistetty ethernet-verkkoon, joka toimi teollisuusväylänä. Koska I/O- ja ristikytkentäkaappien lisäksi DCS-huoneessa on verkko- ja tietokonekaapit, DCS-huone alkaa muistuttaa pientä serverikeskusta, jolle on ominaista ison tilan tarve, jäähdytys ja riittävä virran syöttö. Toimiston ATK-laitteiden, erityisesti työasemien, elinkaari on aika lyhyt verrattuna koko DCS:n elinkaareen. Kaikki nämä asiat pakottavat tarkistamaan DCS-laitteiston elinkaarta ja varautumaan nopean ATK-laitteiden kiertoon tai etsimään muita keinoja, jotta vältettäisiin liian tiheät järjestelmäpäivitykset.

Yksi tällaisista keinoista on virtualisointi, jota voidaan hyödyntää tehokkaasti nykyaikaisessa DCS:ssä ATK:n osalta. Tietotekniikan virtualisointia on käytetty jo vuosia toimistoympäristössä, jossa palveluviive ja itse palvelu usein ei ole niin kriittisiä kuin prosessiohjauksessa. Virtualisointi on kuitenkin mielenkiintoinen tekniikka, koska se tarjoaa merkittäviä etuja, kuten virta-, laitteisto- ja tilasäästöjä, sekä joustoa ja säästöjä syntyy myös elinkaaren hallinnassa.

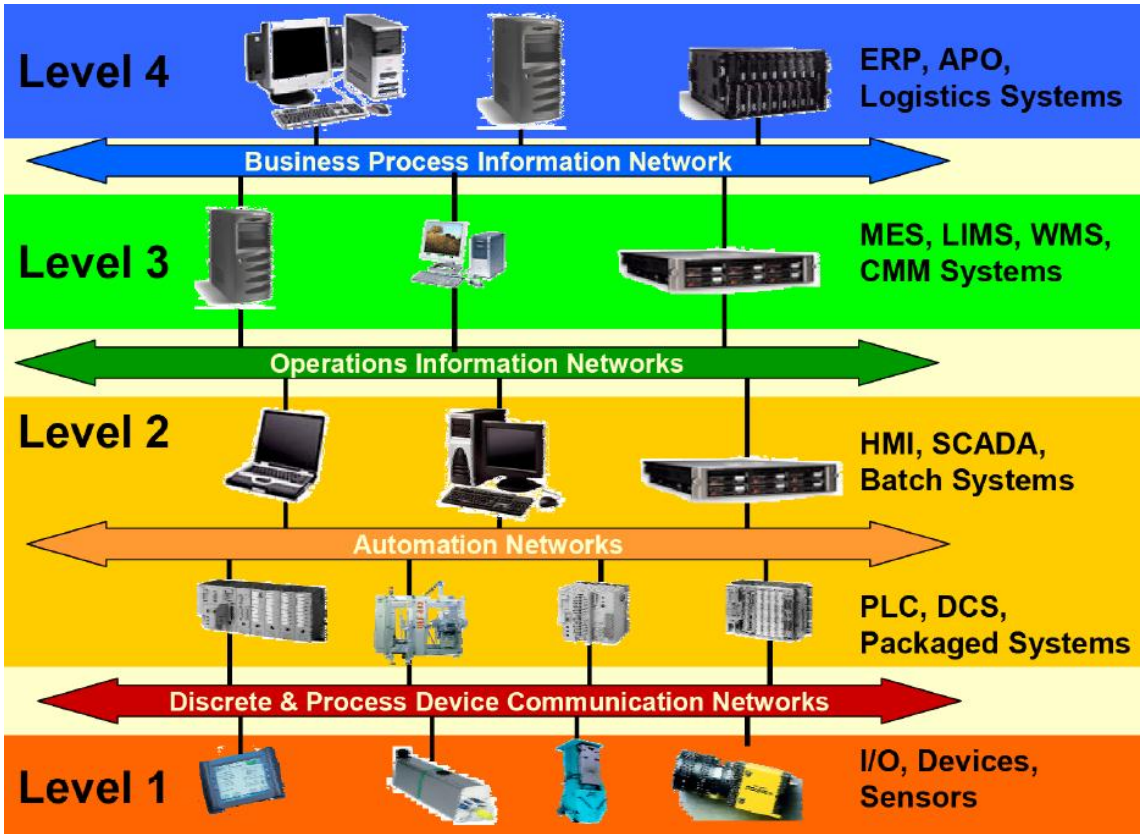
2 Nykyaikainen DCS

2.1 Rakenne

Nykyaikainen keski- tai isokokoinen DCS koostuu neljästä tasosta (kuvio 1, kuvio 13): kenttä- (0, ei kuvioissa), prosessiohjaus- (1, 2), tuotannon- (3) ja toiminnan taso (4). Kaikissa tasoissa, 0-tason lukuun ottamatta, esiintyy ATK-laitteet ja integrointiverkkona toimii Ethernet. Tyypillisesti Ethernetin nopeus on 100 mbps tai 1 Gbps.

Kenttätasolla (0, osittain 1) ovat automaation erikoiset laitteet, kuten prosessiasemat, PLC, ja niiden lisäksi mittaus- ja toimilaitteet, jotka on liitetty järjestelmään perinteisillä diskreetti- tai analogiasignaaleilla tai kenttäväylillä. Kenttätason laitteet ovat eri auto-

maatioyritysten toimittamia erikoislaitteita. Esimerkiksi lämpötilalähettimille tai venttiileille ei ole muita vaihtoehtoja kuin eri toimittajien kyseiset laitteet.



Kuvio 1. Automaation tasot ICT näkökulmalta [2].

2.2 ATK-laitteisto

2.2.1 Serverit ja työasemat

Laitteisto tasoilla 2 ja 3 koostuu yleensä peruspalvelimista ja -pöytäkoneista (kuvio 2), ja laitteisto kuuluu automaatio-osaston vastuulle. Laitteet tasolla 4 ovat yrityksen ICT-osaston vastuulla. DCS:n laitteiston ylläpito ja elinkaari voivat olla erilaisia riippuen automaation toimittajan roolista, joka on yleensä aika vahva ja määräävä. Huoltosopimus voi pakottaa käyttäjä hankimaan ATK-varaosat suoraan automaation toimittajalta, jolloin hintataso on varsin korkea. Vastaavasti toimittaja joutuu sitoutumaan pidempiin huolto- ja toimitussopimuksiin kuin normaalit ATK-laitteiden toimittajat.

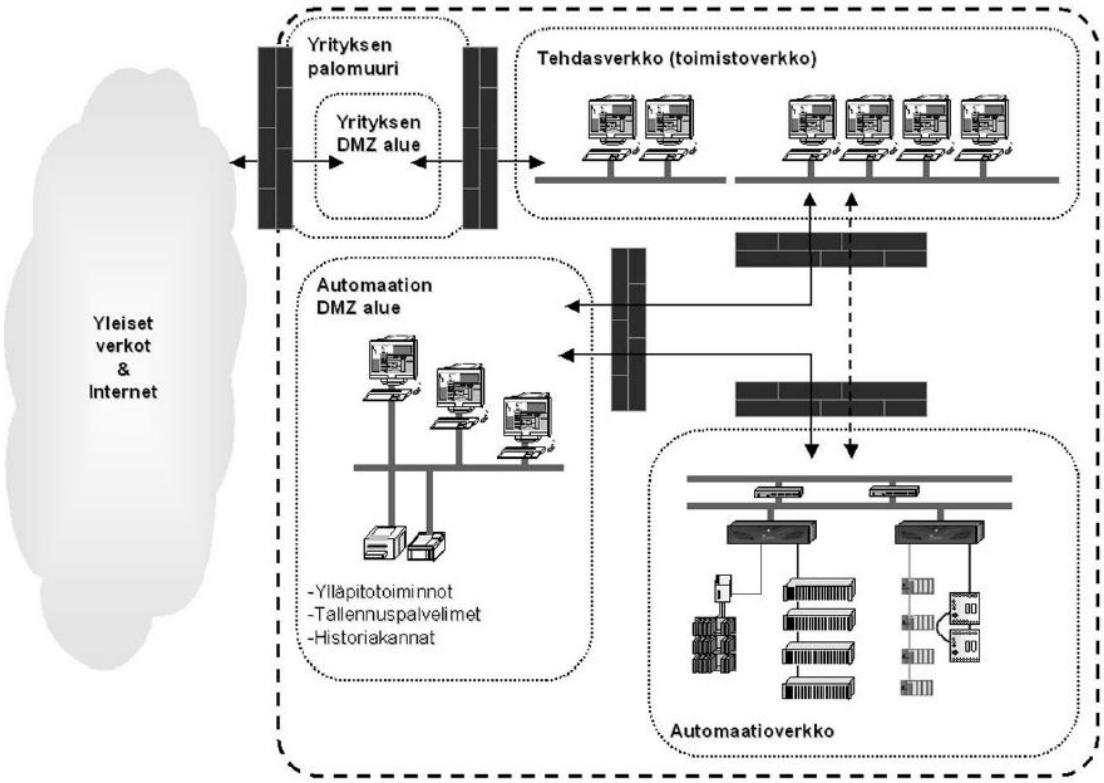
Kuvio 2. DCS:n operointiasemat, perinteinen toteutus. Näytöt ja input-laitteet ovat kytketty KVM-adaptereilla

Fyysisesti ATK-laitteet yleensä eivät erottu ATK-valmistajan laitteista, ellei siihen lisätty erikoiskomponentteja tai OS- tai BIOS-ohjelmistoa ole räätälöity. Näin automaatiotoimittaja suojaa omaa myyntiä ja varaosaliiketoimintaa.

2.2.2 Automaatioverkko

Verkon laitteisto koostuu L2- ja L3-tason kytkimistä, reitittimistä ja palomuureista ja/tai UTM-laitteista sekä erilaisista protokolla- ja mediamuuntimista. Koska palvelun katkeamattomuus ja vasteviive on ratkaiseva, laitteisto pitää tukea muun muuassa RSTP-protokolla, LAG. Monilla komponenttivalmistajilla on tarjolla teollisuudelle tarkoitettuja malleja, jotka voidaan asentaa DIN-kiskolle tai niiden suojakotelointi on sellainen, että laitteisto kestäisi aggressiivisessa toimintaympäristössä.

Turvallisuussyistä tehtaan ohjausverkon pitäisi erotettu muilta verkoista loogisesti fyysisillä laitteilla (ks. 4.3.4). Jaottelu toteutetaan reitittimillä ja palomuureilla tai VLAN-tekniikalla (kuvio 3).

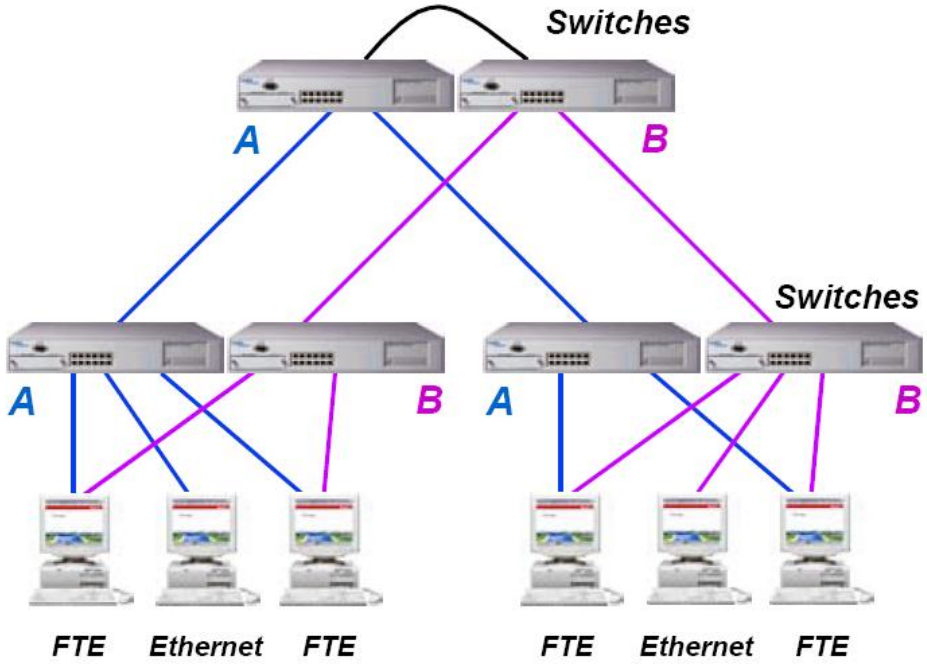


Kuvio 3. Esimerkki tehtaan verkkojaosta [4, sivu 80]

Tänä päivänä tasoilla 2…4 on käytetty Ethernet-tekniikkaa. Tasolla 2 esiintyvät myös muut kuin toimistoverkon laitteet, esimerkiksi eri valmistajien PLC, DCS:n prosessiohjaimet, remote I/O-laitteet (kuvio 4). Tällaiset laitteet käyttävät yleensä Industrial Ethernet -väylän tai vastaavaa, joka on teollisuustarkoituksekseen tarkoitettu Ethernetin muoto.

Kuvio 4. Automaatioverkko [2]. Erityyppiset laitteet on samassa Ethernet verkossa.

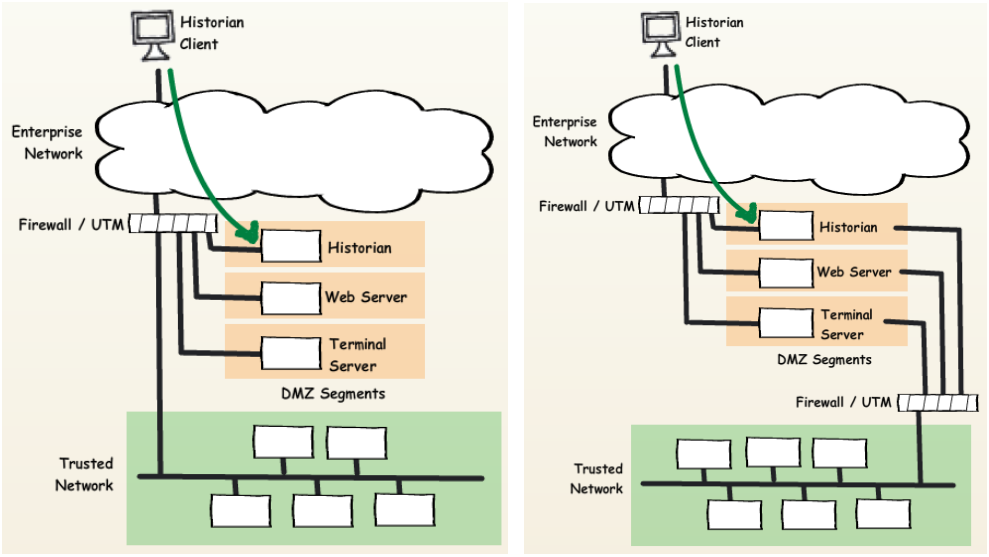
Silloin samaan verkkoon on liitetty ATK-laitteet ja prosessiohjaimet. Verkon topologia voi olla kirjava. Tasojen 2 ja joskus 3 topologiaan vaikuttavat automaatiotoimittajien laitteiden liityntävaatimukset. Esimerkiksi Honeywellin Experion PKS® -järjestelmä vaatii kahdennetun, tähtimäisen Ethernet-verkon (kuvio 5). Muut vaihtoehdot ovat rengasverkko ja sekoitus tähti- ja rengasverkoista.



Kuvio 5. Honeywell:in FTE (Fault Tolerant Ethernet) verkkototeutus prosessiohjaustasolla (Level 2)

Rengasmaista topologia on suosittu Siemensilla, joka tarjoaa omalla tuotemerkillä tehtyjä verkkolaiteita, kuten kytkimiä ja reitittimiä.

Tason 4-verkko on tyypillisesti perinteistä toimistoverkkoa, joka on erotettu automaatioverkosta palomuureilla tai UTM-laitteilla (kuvio 6). ERP ja MES (automaatio) välistä tiedonvaihtoa toteutetaan DMZ:n avulla, jolloin sen määrittely ja ylläpito on tehtaan ja ICT osastojen yhteinen asia.



a) Yksi palomuuri / UTM b) Kaksi palomuuria / UTM:a

Kuvio 6. DMZ:n käyttö teollisuusohjausverkossa [14].

3 Virtualisoinnin käyttö automaatiossa nykypäivänä

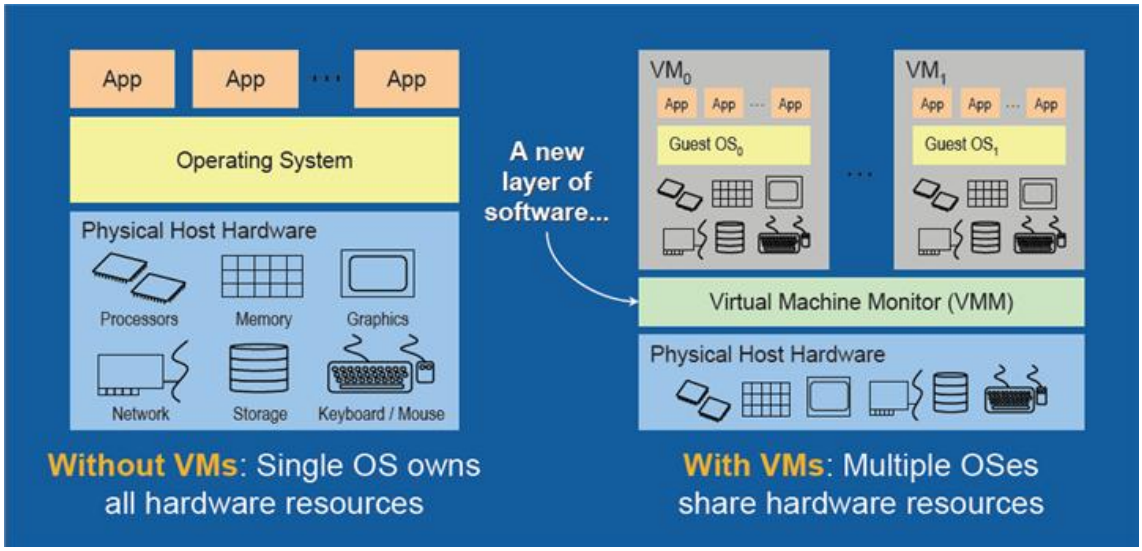
3.1 Virtualisoinnista

Tänä päivänä virtualisointialustan johtajat ovat VMWare, Microsoft ja Citrix (kuvio 7). Kaikki kyseiset toimittajat tähtäävät palvelemaan isot ICT-organisaatiot, esimerkiksi toimisto- tai kouluverkot. Perusideana on korvata iso määrä pöytäkoneita ja palvelimia datakeskuksilla ja päätteillä. Datakeskuksessa toimivat virtuaalikoneet, joita käytetään päätteillä. Silloin hankinta- ja ylläpitokustannukset alenevat sekä käytettävyys paranee huomattavasti. VMWare määrittelee [1] asiaan niin, että virtualisointi jakautuu useaksi kohteiksi:

- palvelimet (ESXi, vSphere)
- verkko (NCX)
- pöytäkoneet (View, Horizon)
- sovellukset (vFabric)
- levy / tallennusasemat (Virtual SAN).

Käyttämällä virtualisointia jokaisella osa-alueella syntyisi merkittäviä säästöjä verrattuna toteutukseen, jossa on käytetty perinteitä ATK-tekniikka. Automaatiotoimitus sisäl-

tää pienempää määrä tietokoneita ja servereitä kuin toimiston ATK-toimitus. Tämän takia automaatiotoimitus voi luokitella pieni- tai keskikokoiseksi ATK-järjestelmäksi virtualisointitoimittajan näkökulmalta. Silloin lisensioinnin merkitys kasvaa, koska lisenssien kustannukset jakautuisivat pienempään määrään terminaaleja ja/tai käyttäjiä.



Kuvio 7. Inteliin esitys virtualisoinnista

Sovellustoimittajien lisäksi laitevalmistaja, kuten Intel tukevat, virtualisointia [3]. Nykyään jopa kannettavissa tietokoneissa virtualisointituki on vakiovaruste laitetasolla.

3.2 Automaation toimittajien virtualisointivalinta

3.2.1 Alusta ja infrastruktuuri

Tänä päivänä melkein kaikki isommat automaatiotoimittajat käyttävät VMWaren tuotteita – alustana vSphere- tai ESXi -palvelin, ja VDI:nä VMWare Horizon -ohjelmisto. Koska tuotekehitys on pitkä, perusteellinen prosessi, automaation virtualisoinnissa ei ole käytetty viimeisintä tekniikkaa. Esimerkiksi, ABB käyttää VMWare vSphere 4.1 Standard -ohjelmistoa vaikka tällä hetkellä tarjolla on 5.5 (tilanne 4.12.2013). Samoilla linjoilla ovat olleet Honeywell ja Siemens. Sen lisäksi toimittajat pyrkivät käyttämään sellaisia ohjelmistoja, jotka ovat yksinkertaisia toiminnan näkökulmalta tai testattu perusteellisesti teollisuusympäristössä.

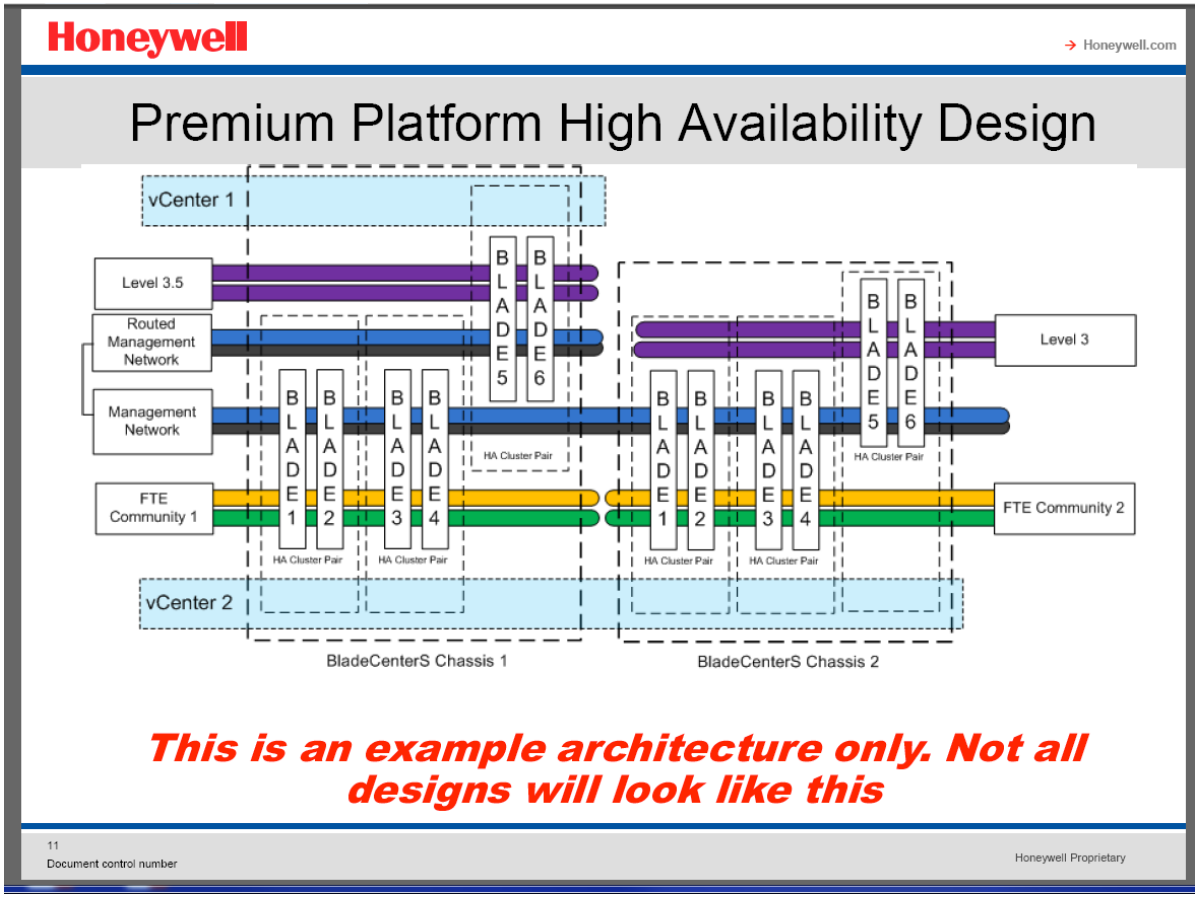
Cluster-tekniikkaa vältetään ilmeisesti mutkikkuuden ja lisenssihinnoittelun takia. Toisin sanoen fyysiset koneet paketoidaan tietokeskukseen, jossa ne toimivat itsenäisinä, ei-kahdennettuna.

Mielenkiintoinen uutinen Honeywellilta tarkoittaa, että kyseinen toimittaja on laajentamassa virtualisointituotteiden tarjontaa ottamalla käyttöön cluster-tekniikan [9]. Vertailutaulukossa (Taulukko 1) toiseksi viimeinen rivi, solmujen automaattinen toipuminen vioista, viittaa VMWare:n vSphere:n HA-ominaisuuteen.

Taulukko 1. Honeywell DCS:n virtualisointipakettien vertailu

BENEFITS	ESSENTIAL PLATFORM	PREMIUM PLATFORM
Avoid reinstalls for a hardware refresh	✓	✓
Upgrade and patch rapid fallback	✓	✓
Computer Infrastructure reduction	✓	✓
Facility savings (space, power, cooling, weight)	✓	✓
Add new ICSS nodes without requiring additional hardware	✓	✓
Full remote maintenance of hardware	✗	✓
Extended life hardware platform	✗	✓
Automatic recovery from failed nodes	✗	✓
Replace computer hardware transparently	✗	✓

HA-klusterin käyttöä todista myös Honeywellin esitys Premium Platform -toteutuksesta (kuvio 8) [20]. Esimerkissä on DCS:n eritasojen paketointi samalle palvelinpakalle: toisessa palvelimessa on PCN, Management, Level 3.5 (DMZ) -osiot, ja toisessa palvelimessa - PCN, Management, Level 3 (MES). Erilaisten tasojen sijoittaminen samalle levypalvelimelle on mahdollista modulaarisen rakenteen takia.



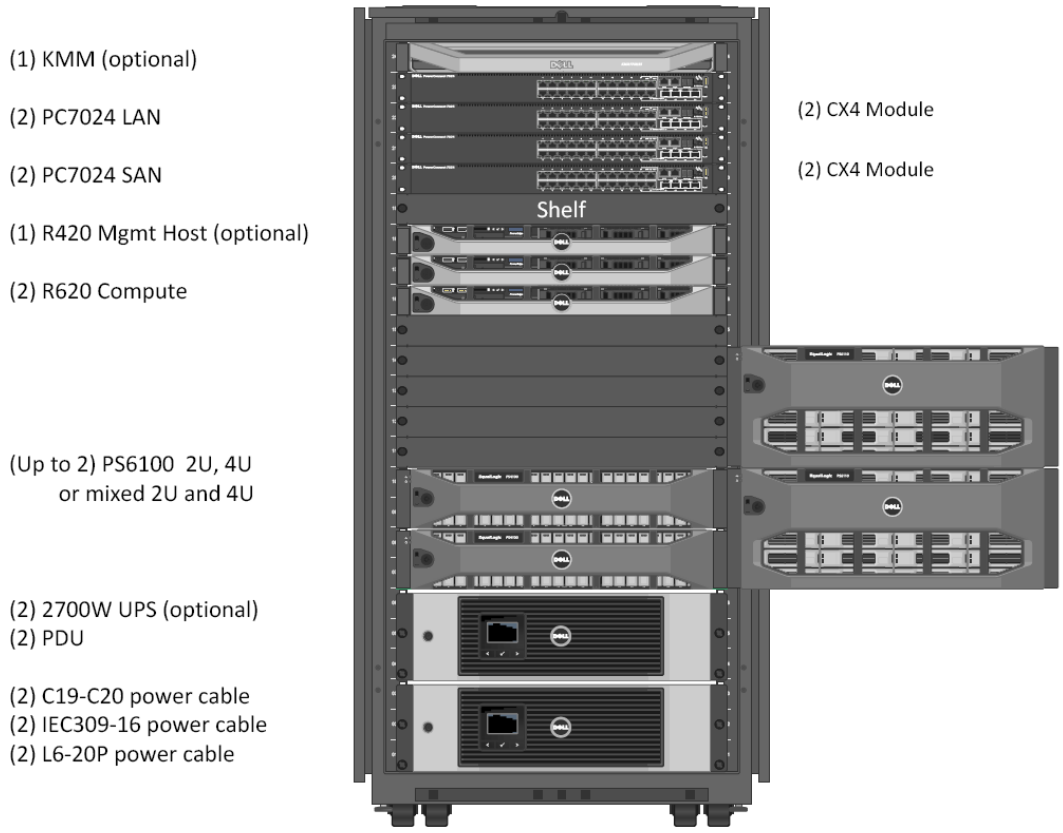
Kuvio 8. Esimerkki levypalvelimen käytöstä DCS virtualisoinnissa, HA-klusteri

3.2.2 Laitteisto

Laitteiston toteutuksessa on kaksi vaihtoehtoa: perinteiset palvelimet ja blade- eli levypalvelimet.
Perinteiset U2…U4 -kokoiset räkkipalvelimet ovat hyvä valinta, kun halutaan sijoittaa laitteet eri tiloihin kahdennussyistä. Levypalvelimet tarjoavat pienempää tilavarausta ja muita kustannussäästöjä.

ICT-toimittajat tarjoavat valmiit paketit tai sopivat tuotteet molemmille tarpeille. Dell on tehnyt kolmesta serveristä, iSCSI-laiteesta ja L3 Ethernet -kytkimistä (kuvio 9) pienen tietokeskuksesta eli Data Center, jotka voi käyttää pienen tai keskisuuren vDCS rakentamisessa [10].

IBM BladeCenter S -datakeskus tarjoaa samat ominaisuudet kuin Active System 50 (vStart 50) kompaktissa koossa (kuvio 10). Molempien ratkaisujen vahva puoli on valmistajien ylläpitotyökalut, joiden avulla voi hallinnoida koko laitteistoa.



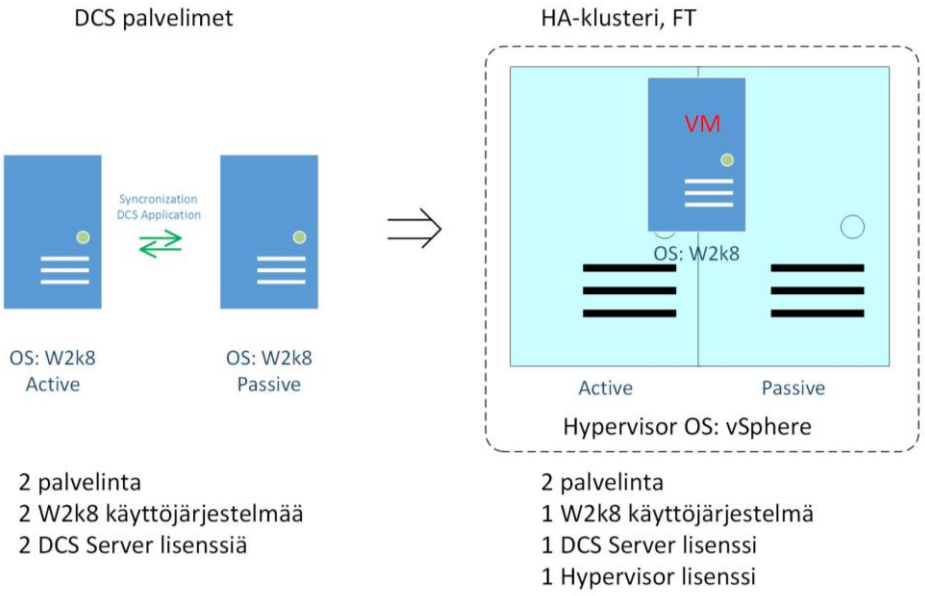
Kuvio 9. Dell Active System 50 (entinen vStart 50) laitteistokokoonpano

Kuvio 10. IBM:n BladeCenter S -tietokeskus käytetään Honeywell:in Experion Virtualization Solution Premium-toteutuksessa. Koko on U7

3.3 Virtualisoinnin haitat automaatiotoimittajalle

Suurin haitta toimittajalle on DCS:n fyysisien osien ja jopa ohjelmiston kannibalisointi eli tässä tapauksessa DCS-osien ja -ohjelmiston korvaaminen muilla osilla ja ohjelmistoilla, joiden yhteenlaskettu arvo on pienempi kuin perinteisen toimituksen toiminnollisuuden kannalta sama arvo. Toisin sanoin, kun useiden ATK-koneiden tilalle toimitetaan huomattavasti pienempää määrä tehokkaita keskuksia, niin saadaan aikaiseksi pienempää myyntiä ja jatkossa huolletaan vain kyseiset keskukset. Tämä tarkoitta, että huolto- ja varaosaliiketoiminta kärsisi. Esimerkiksi tämä voi vähentää Siemensin automaatiotoimituksen ja varaosamyynnin volyymia ja tuottoa, koska Siemens valmistaa omalla tuotemerkillä teollisuustietokoneita ja palvelimia, jotka voidaan korvata tehokkailla peruspalvelimilla. Toinen esimerkki on Honeywellin ja Dellin yhteistyö. Viime vuodet Honeywell on toimittanut DCS infrastruktuuria DELL:in tietokoneilla ja servereillä. DCS infrastruktuurin muutos voi aiheuttaa partnereiden sopimuksen muutoksia ja toimitettavien DCS-osien hintojen muutoksia epäedullisemmaksi automaatiotoimittajalle.

VM korvaa pahimmassa tapauksessa fyysisen koneen lisäksi DCS serverin lisenssin. Näin voi tapahtua, kun käytetään cluster-teknologiaa. Tällöin voi olettaa, että toissijainen VM korvaisi yhtä hyvin redundantista DCS-palvelinta, ja DCS:n voi toteuttaa yhdellä loogisella ohjainpalvelimella. Silloin tarvitaan vain yksi DCS-lisenssi (kuvio 11).



Kuvio 11. Esimerkki kokonpanomuutoksesta perinteisestä virtualisointitoteutuksekseen

Riippuen käytetystä toimittajan teknologiasta (esimerkiksi VMWare, Microsoft), loppukäyttäjä voi joutua maksamaan cluster-lisenssin käytöstä korkeat kustannukset [5]. Silloin vertailussa pitää aina ottaa huomioon hallintaohjelmiston kustannukset. DCS toimittaja joutuisi neuvottelemaan cluster-lisenssin hinnoittelusta ohjelmistotoimittajan kanssa, koska käyttökohteiden määrä on yleensä huomattavasti pienempi kuin isoissa toimisto-organisaatioissa. Nykyinen hinnoittelumalli voi olla kohtuuttoman korkea pienikokoisille virtualisointitoimitukselle.

3.4 Virtualisoinnin DCS-käyttökohteet

DCS:n ATK-laitteet koostuvat ICT infrastruktuurin servereistä (DNS, RTS, BU, WSUS, AD jne.), operointi- ja sovelluskoneista (pöytäkone, kannettava) ja DCS:n palvelimista, jotka palvelevat prosessiohjaimia ja muita ohjausjärjestelmän osia. Visualisointia käyttäen voi korvata melkein kaikki serverit ja pöytäkoneet, joihin ei ole lisätty erikoislaajennuskortteja. Tällaisille korteille yleensä ei ole kehitetty ajureita virtualisointiympäristöä varten, tai niiden toimintaa ei ole testattu tai se on epävakaa.

Verkko-osat, kuten hallittavat kytkimet, reitittimet ja tietoliikenneturvalaitteet (palomuuri, UTM), ovat osa virtualisointia. Tänä päivänä virtuaalikytkimet ovat vakio-osa virtualisointiratkaisuja. Virtuaalisia UTM-laitteita on tarjolla, mutta ne sopivat paremmin isolle ATK-kokoonpanolle korkeiden kustannuksien takia (esimerkiksi virtuaalikytkin tuoteperhe Cisco Nexus 1000V, jolla on tuvallisuusominaisuudet).

4 Koejärjestelmän rakentaminen

Virtualisointisoveltamista prosessiohjausjärjestelmissä testattiin pienessä laitteistossa, joka koostui muutamasta palvelimista, NAS-levyistä ja terminaaleista. Ohjelmistoalustaksi valittiin VMWare:n vSphere Standard. NAS-asemien käyttöjärjestelmiksi otettiin ilmainen FreeNAS ja Microsoftin Server 2012 Data Center.

4.1 Laajuus

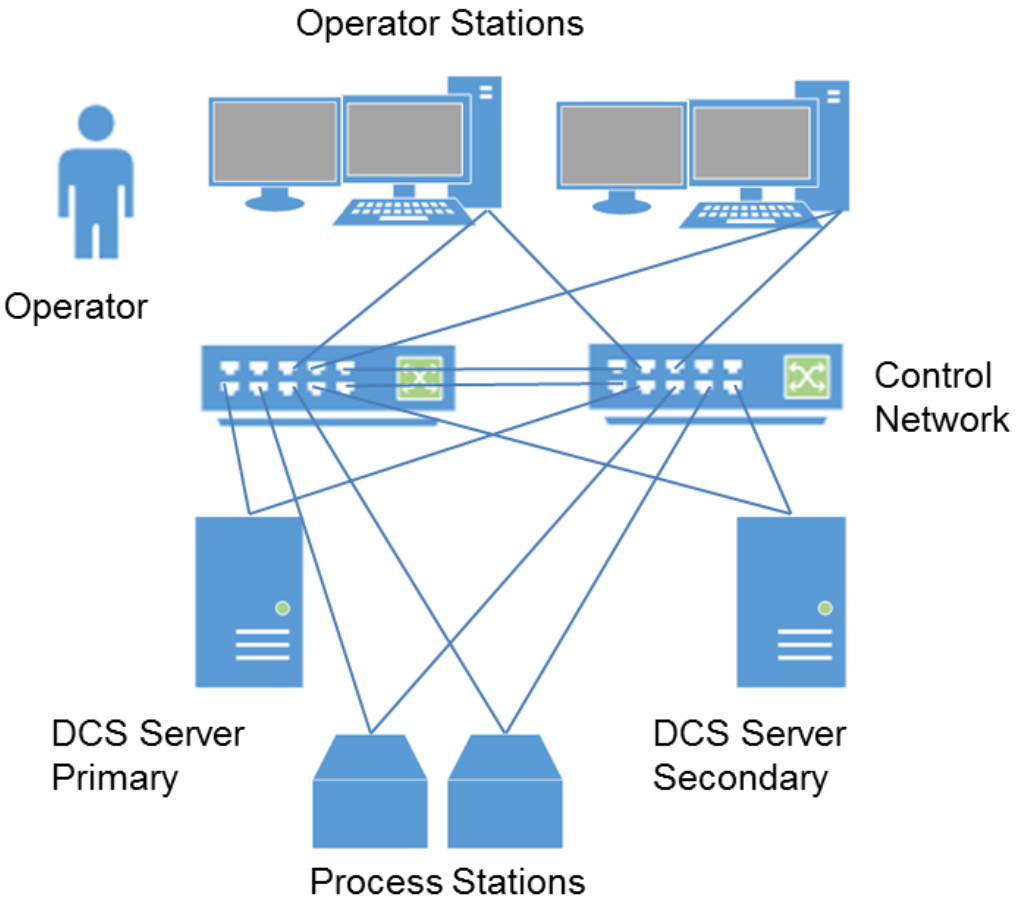
Koelaitteiston testauksen tavoitteena oli rakentaa pienikokoinen DCS ja testata perustoimintaa häiriötilanteissa. Virtualisoidussa järjestelmässä oli käytetty tekniikkaa, joka ei ole vielä yleistynyt automaatiotoimittajien keskuudessa, eli HA-klusteria, jossa on FT-ominaisuus. Koejärjestelmästä tehtiin DCS-ydinkomponentti (kuvio 12), joka palvelee vain prosessiohjausta eli prosessiohjaimien, prosessipalvelimien ja operointipäätteiden yhteistoimintaa.

Taso 4 eli ERP-liitäntä, jäi kokeilun ulkopuolella. Tehtaan tuotanto-ohjausta ja datakeruuta ei myöskään päästy testaamaan sopivien komponenttien puuttuessa.

4.2 Virtualisoidun DCS:n topologia

Koejärjestelmän fyysinen ydin koostuu kolmesta fyysisestä palvelimista, joista kaksi muodostaa HA-klusterin ja kolmas on iSCSI-tallennuslevyasema. Kokonaisuuden tallennuslevyasemana on käytetty myös kaksi tavallista tietokoneetta, joihin oli asennettu FreeNAS-käyttöjärjestelmä (ks. liite 1, kuvio 23). Ne toimivat myös Heart Beat -levyasemina varmistamassa sitä, että yhteydet HA-klusterien palvelimien ja NAS-asemien välillä toimii.

Näyttöpäätteinä kokeissa on käytetty kahta Thin Client -laitetta, joilla otettiin yhteyttä virtualikoneisiin RDP:n avulla. Toinen laitteista toimii langattomasti. Hallinta- ja varmuuskopiointikonsolina oli tavallinen pöytäkone XP-järjestelmällä (ks. liite 2, kuvio 24).



Kuvio 12. Perinteinen DCS topologia, ”ydinosat” ovat järjestelmäpalvelimet, prosessiohjaimet, kytkimet, operaattoriasemat.

Ohjelmistokokonaisuus koostui VMWaren Sphere 4.x Standard alustasta (kuvio 24), VM:den käyttöjärjestelmistä ja Honeywell Experion PKS R400 automaatiotoimittajan DCS demo lisensseistä. Virtuaalikoneiden Microsoftin OS-lisenssit olivat opiskelijan versioita, täysin toimivia.

4.3 Koe DCS:n toiminnan/ominaisuuksien määritteleminen

DCS:n ominaisuudet ovat vaikuttaneet virtualisointitopologiaan, rajana on ollut vain laitteisto- ja lisenssirajoitteet.

4.3.1 Käytettävyys

Tyypillinen DCS käytettävyys on yli 98 %, mikä tarkoittaa sitä, että DCS voisi olla pois päältä muutaman minuutin tai jopa sekunnin vuodessa [11]. Tämä on aivan eri tason vaatimus kuin toimistoverkon järjestelmissä, joka sietää jopa useiden tuntien palvelukatkot useita kertoja vuodessa.

4.3.2 Vikasietoisuus

Nykypäivänä kriittiset ja vaaralliset prosessit ohjataan niin, että prosessiohjaimen vikaantuessa ohjaus siirtyy viallisesta kahdennetulle ohjaimelle. Tällainen vikasietokykytoteutus vaatii varaohjaimen lisäksi Ethernet-verkosta vastaavaa kahdennusta sekä nopeampaa yhteyden reititystä kuin toimistoverkossa vikaantumisen tapauksessa. Silloin käytetään kahden rinnakkaisen kytkimen topologiaa tai rengasmuotoista verkkoa sekä verkon RSTP-ominaisuutta.

4.3.3 Laajennettavuus ja joustavuus

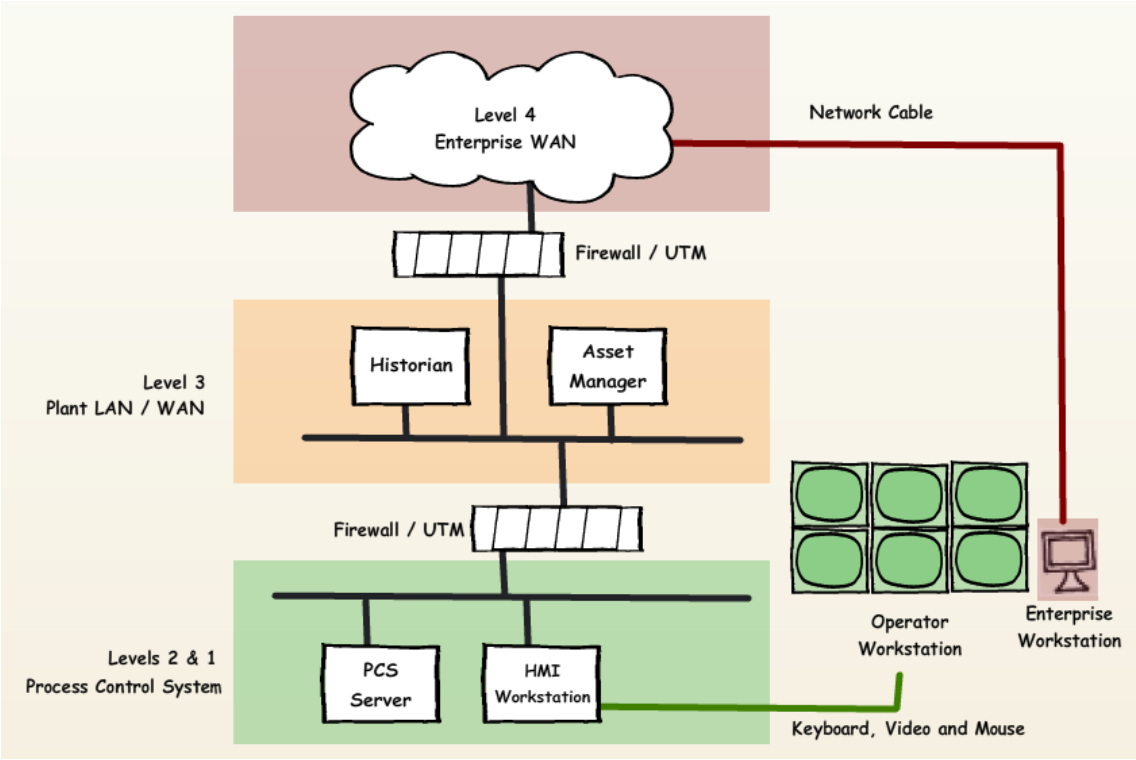
Ethernet-verkko tuo DCS-rakenteeseen joustavuutta ja helpompaa laajennettavuutta. Koska DCS-laitteet ovat kiinni kytkimissä, laitteiden siirto, kytkeminen tai poisto on helppoa. Fyysinen kytkentä yleensä tapahtuu kytkimen portin avulla, ja kytkimen asetus on suhteellisen nopea ja helppo toimenpide ICT-ammattilaiselle, kun taas DCS-järjestelmän muutos on automaatiosovellusinsinöörin vastuulla.

4.3.4 Turvallisuus

NLST:n erikoisjulkaisu numero 800-82 määrittelee yksityiskohtaisesti DCS-turvallisuuden. Tärkeimpiä asioita on verkon arkkitehtuuri [6, chap. 5], muun muassa verkon erottelu (kuvio 13, [15]) ja turvallisuuden hallinta [6, chap. 6]. Turvallisuuden hallinnan rooli on kasvamassa koska uhkia on paljon ja teollisuusvakoilu kaikissa muodoissa on kasvamassa [19].

Virtualisoidussa DCS-toteutuksessa verkon arkkitehtuuri muuttuisi niin, että fyysisien laitteiden määrä pienenee ja jossain tapauksissa topologia muuttuisi niin, että rengasmaista segmenttiä karsitaan. Verkkojen (prosessiohjaus, DMZ, toimistoverkko) erottelu

tapahtuu edelleen palomuurien / UTM laitteiden avulla. Toisin sanoin verkkojen segmentoinninsuhteessa ei tapahtuisi muutoksia. Tietysti voi käyttää virtuaalisia ratkaisuja, mutta kokonaisuus voisi muuttua monimutkaisemmaksi ja vaikeammin hallittavaksi.



Kuvio 13. Tehtaan prosessi-, tuotannon- ja toiminnan -ohjauksien verkojen jako ja erottelu palomuureilla / UTM:illa

NLST:n mukaan [6, chap. 5.3.6] verkon turvallisin ratkaisu sisältäisi yksi tai useampi DMZ alueita. Palomuuri/UMT 3. ja 4. tasojen välillä on kriittinen lisääntyvien uhkien takia.

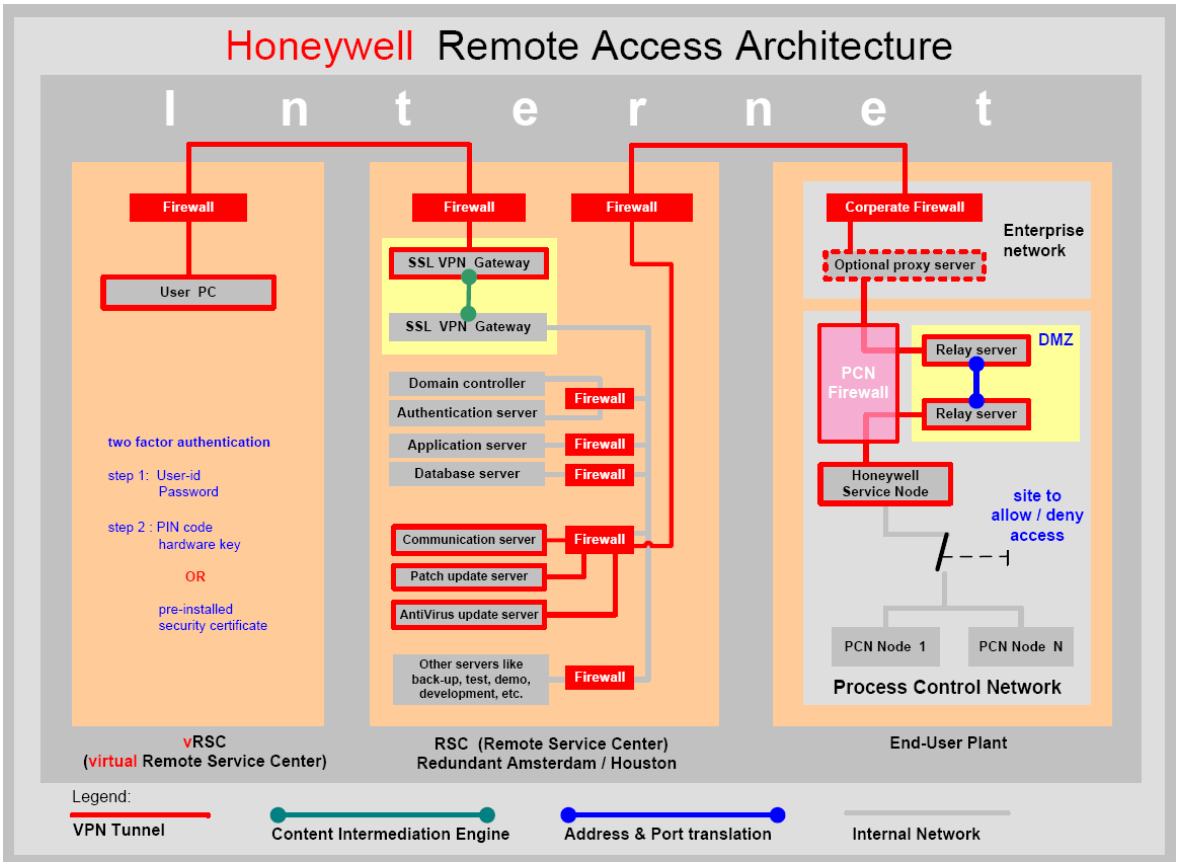
4.3.5 DMZ

Tietokoneet ja palvelimet, jotka palvelevat loppukäyttäjiä toimistoverkossa ja hakevat tietoa prosessiohjausverkosta, kuten historia, datakeruu, ICT:n ylläpito, on yleensä sijoitettu DMZ alueella. Datakeruun kollektorit yleensä sijaitsevat PCN:ssä, tiedon keruu DB-palvelimet DMZ:ssa. Kollektorit saavat olla virtualisoituja PCN:ssa, clustertoteutuksessa ei tarvita kahdennettuja kollektoreiden VM:a, vaan saa olla yksi FT VM-toteutus.

DMZ-alue ei ollut tämän työn tarkastelussa. Voidaan kuitenkin olettaa, että sen osa-alueen koneiden virtualisointi olisi tehtaan ICT- ja automaatio-osastojen yhteinen asia.

4.3.6 Etäyhteydet prosessiohjausverkkoon

Etäyhteydet DMZ- ja PCN-verkkoihin kannattaa toteuttaa harkiten, ja vakoilu-uhkien takia kannattaa käyttää keskitettyä ratkaisua (kuvio 14) ja välttää yksittäisten VPN-etäyhteyksien tekemistä.



Kuvio 14. Honeywell:in Remote Access –ratkaisun rakenne

Kuviossa 14 voi nähdä, että ratkaisu vaatii prosessiohjausverkossa Service Node-komponentin, joka on erillinen tietokone, palvelin tai ohjelmisto. Senkin saa käyttää virtuaalisena, koska voi olettaa, että laitteistopohjaista salaustekniikkaa ei käytäisi.

4.4 Virtualisointialustan valinta

Kahdesta suurimmista virtualisoinnin tuottajasta VMWare ja Microsoft valittiin ensimmäinen käyttöystävällisyyden takia. Valintaan on vaikuttanut opiskelijalisenssien saatavuus ja esikokeiden perustella muodostanut käyttäjäystävällisyyskokemus.

VMWaren Sphere 5.1 Enterprise -ohjelmistoalusta sisältää HA:n lisäksi FT:ta, jonka avulla saa toteuttaa cluster-solmun. FT:n käyttö mahdollistaa korkeatasoisen käytettävyyden ja vikasietoisuuden. Viime tiedon mukaan automaatiojärjestelmien toimittajat, lukuun ottamatta Honeywelliä, eivät tarjoa virtualisoitua DCS:a HA-toteutuksena. Sille on selitys, koska lisenssi maksaa paljon enemmän kuin perusversio, jonka avulla voi luoda yksittäisiä isäntäkoneita. Myös DCS-komponenttien yhteensopivuus HA/TF-clusterissa vaatii perusteellista testausta ja asettaa rajoituksia. Esimerkiksi sarjaporttia ei saa käyttää HA/FT-clusterissa, koska RS232-yhteyden kaapeli on kiinni yhdessä palvelimen liittimessä ja pysyy siellä, kun virtuaalikoneen ajoa siirretään toiselle klusterin palvelimelle. Silloin RS232 yhteys ei ole käytettävissä

4.5 Laitteiston hankinta ja kasaus

Laitteiston hankintaa ja muutoksia on tapahtunut jatkuvasti sopivien laitteiden löytymisen mukaan. Alkuvaiheessa on ollut yksi fyysinen serveri, johon oli asennettu ESXi Server ohjelmisto ja sen päälle kaksi virtuaalikonetta: DCS-serveri (ESV01R400) ja operaattorin asema (ESF01R400).

Jatkossa tavallisesta PC:stä oli tehty iSCSI-verkkolevyasema, ja 1G-kytkimen (PowerConnect 5424) kanssa oli muodostettu virtuaaliympäristö. Myöhemmin toisen sopivan palvelimen hankkimisen jälkeen tietokeskus muutettiin klusteriksi.

Yllämainitut muutokset todistavat, että VMWaren vSphere alustan avulla saa erittäin joustavasti muunnella kokoonpanoa, päivittää alustaohjelmistoa ja muuttaa alustan rakennetta (esim. ESXi-palvelimien muutos klusteriksi).

Fyysisen kokoonpanon esikuvana on ollut testilaitteisto [21]. Kahdesta sopivasta palvelimista tehtiin klusteri, jonka levytila toteutettiin kolmannella iSCSI-serverilla. iSCSI-serverin OS on ollut MS W2k8R2 ja siihen tarvittava iSCSI-ohjelmistolaajennus. Kaikki

Ethernet yhteydet toteutettiin kahdella Dell 5424 Connect-kytkimillä. Kytkimien asetusohjeet iSCSI:n sopivaksi löytyy Dellin tukisivustosta [22].

Toiselle kytkimistä liitettiin Thin Clien-terminaali ja hallintatietokone. Toinen Thin Client langaton terminaali yhdistettiin WIFI-retitimeen, joka oli yhdistetty molempiin kytkimiin. Kytkimien välillä muodostettiin LAG-linkki sillä varalta, että toinen kytkimistä olisi pois toiminnasta. Lopullinen laitteiston kokoonpano on esitetty liitteissä 1 ja 2

4.6 Ohjelmistojen asennus

Ohjelmiston VMwaren alustaohjelmiston asennus tehtiin kun tarvittava palvelin oli hankittu ja käytettävissä. Hallintapalvelin, vSphere Server, toteutettiin virtuaalikoneena ja se oli sijoitettu klusterin toiselle palvelimelle. DCS-palvelimen toteutus tehtiin Stand Along eli yhdellä palvelimella, koska HA/FT-klusterissa on aina kahdennettu virtuaalikone, joka kytkeytyy päälle heti kun aktiivinen VM jostain syystä on pois päältä.

4.7 Klusterin viritys

Klusterin luonti ja muutokset tehtiin vSphere Server CLI:n avulla. VMWaren tukisivuilla löytyy ohjeet ja tarkastuslista ongelmien ratkaisemiseksi. Microsoft iSCSI palvelimeen tarvittaessa otettiin RDP-yhteyttä, FreeNAS iSCSI -asemia hallittiin selaimen kautta. Työllistävin vaihe oli Microsoft Windows 2008 Serverin iSCSI:n asetus. Lopuksi luotiin kahta iSCSI-asemaa, iSCSI_A ja iSCSI_B, mutta Windows 2008 Server hälytti jatkuvasti sitä, että asemien levytila on alhainen. Niiden toiminta kuitenkin jatkui normaalisesti, ja hälytyksien vaikutusta toimintaan ei tutkittu.

Kahta FreeNAS-asemaa käytettiin Heart Beat-asemina varmistamaan, että fyysiset palvelimet on toiminnassa.

5 Laitteiston käynnistys ja testaus

5.1 Laitteiston käynnistys

Johtuen erilaisesta fyysisestä rakenteesta käynnistyksen järjestys oli hieman erilainen kuin perinteisessä DCS-käynnistysrutiinissa. Ensin käynnistettiin iSCSI NAS-asemat, sitten klusterin palvelimet. Virtuaalikoneet oli asetettu käynnistämään tietyn viiveen päästä fyysisien palvelimien käynnistyksien jälkeen. Kun kaikki ATK-laitteet ja virtuaalikoneet oli käynnistetty, laitettiin käyntiin DCS-sovellukset.

Käynnistyksen aikana esiintyi selittämättömiä hetkellisiä ongelmia Microsoft iSCSI NAS-aseman kanssa. Alussa iSCSI NAS ei ollut tunnistettu kluster-palvelimilla vaikka NAS palvelin oli pitkä aika käynnistetty. Lopuksi virtualisointi-infrastruktuuri ja DCS-sovellukset toimivat normaalisesti.

5.2 Laitteiston testaus

Laitteisto testattiin normaaliolo- ja häiriö/vikantumistilassa. Se osoittautunut stabiilina normaalitilassa, jolloin ei tapahtunut merkittäviä häiriöitä. Virtualisoitu DCS-järjestelmä ei aiheuttanut mitään häiriöitä liittyen infrastruktuuriin eli virtuaalikoneiden ajot ja RDP yhteydet ja palvelimien kuormat pysyivät normaaleina. Pääosin testi rajoittui siihen että RDP:n avulla otettiin yhteyttä virtuaalikoneisiin ja käytettiin DCS:n sovellustyökaluja ja operaattoripäätteitä kyseisillä etäyhteyksillä.

Poikkeustilanteita tehtiin kahdella tavalla: hallittu alasajo ja äkilliset sähkön tai yhteyksien katkot. Hallittu alasajo tapahtui sammuttamalla klusterin aktiivista palvelinta hallitusti ja käynnistämällä uudestaan. Tämän toimenpiteen aikana kaikki palvelut ovat siirtyneet varalla olevalle palvelimelle katkon ajaksi ja palautuneet takaisin ensisijaiselle palvelimelle kun se oli taas käytettävissä. RDP-yhteys ei katkennut, eli operointipäätteen virtuaalikone oli käytössä koko ajan. Se oli tärkein testi, josta koelaitteisto selvisi ilman ongelmia.

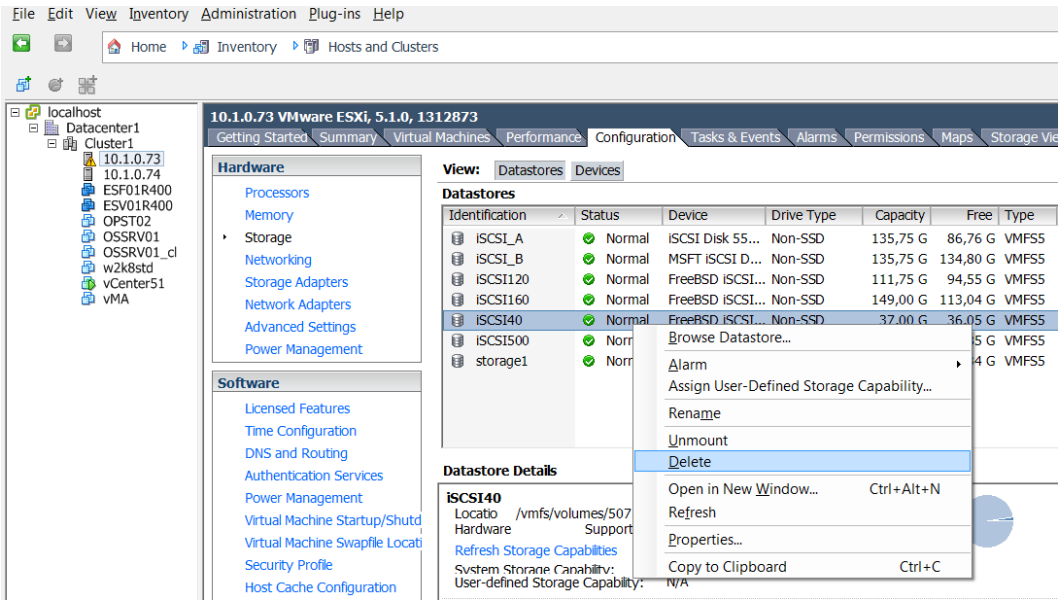
Ylläkuvatut perustestit ei saa missään nimessä pitää riittävänä sanomaan että koelaitteisto ohjelmistoineen voisi korvata kokonaan tai osittain jonkun oikean prosessiautomaatio järjestelmän. Kehitystyötä on jatkettava jotta uudesta automaatiojärjestelmän

rakenteesta tulisi luotettava ja hyväksytty käytettäväksi kriittisessä prosessiohjauksessa.

5.3 Varmuuskopio, migraatio

Tärkeimmät virtualisoidun DCS:n huolto-ominaisuudet kuten varmuuskopiointi ja virtuaalikoneiden siirto eli migraatio testattiin kevyesti. Varmuuskopioinnin ohjelmistona kokeiltiin ilmainen ohjelmisto: Veeam Backup & Replication 6. Perustoiminnot toimivat häiriöttä, VM:n palautus tapahtui huomattavasti nopeammin kuin esimerkiksi palvelimen ohjelmiston perinteinen palautuminen. Koska kyseessä oli virtuaalikone, jonka käyttöjärjestelmä on Microsoft Windows, oli testattu aktivointiseikat varmuuskopioinnin palautumisen ja migraation jälkeen. Virtuaalikoneen levyaseman ja isäntäkoneen sijainnin vaihto ei aiheuttanut mitään aktivointitarpeita. Tämä on tärkeä ominaisuus, koska kriittisessä tapauksessa välttämätön uudelleen aktivointi voi aiheuttaa kohtuuttoman turvallisuusriskin prosessin ohjaukselle koska se pakottaisi varautumaan palvelukatkoon aktivointirutiinin takia..

Virtuaalikoneiden migraatio palvelimesta toiseen ja NAS-levyjen välillä onnistui myös ilman virheitä ja todella nopeasti. NAS iSCSI-asemien lisäys ja poisto on helppo tehdä VCL-kautta kun asema ei ole käytössä (kuvio 15).



Kuvio 15. NAS-levyaseman poisto vSphere:ssä VCL-liittymällä

Verkkoasemien käytön kuorma ei aiheuttanut koko järjestelmälle haitallisia sivuvaikutuksia kuten pitkiä vasteviiveitä, PC-koneiden ja VM:den kaatumista. Myös verkkolaitteet (2 kpl Dell PowerConnect 5424) toimineet ilman häiriöitä. Kuitenkin on huomautettava että koelaitteisto oli pienikokoinen verrattuna ison tehtaan DCS:aan.

Kokonaisuudessa voi sanoa että virtualisointi tuonut joustavuutta ja nopeutta varmuuskopiointitoiminnalle, ja migraatio on sellainen asia, jota ei saa perinteisellä PC ja palvelin -tekniikalla.

5.4 Korkean käytettävyyden klusteri

Higt Availability Cluster eli korkean käytettävyyden klusteritekniikka on ollut pitkään tarjolla ICT-alalla. Se takaa palvelun käytettävyyden yhden tai useamaan palvelinsolmun vikaantuessa.

Koelaitteiston klusteritekniikan valittiin HA, joka sisälsi FT (Fault Tolerance) ominaisuuden. FT:n avulla saa toteuttaa katkeamaton palvelun siirto toiselle. Tänä päivänä FT:n käytöstä prosessiautomaatio-ohjauksesta ei löytynyt tarkkaa tietoa. Ainoastaan Honeywell tarjoaa HA-ratkaisu, mutta FT käytöstä ei ole varmuutta.

Käytettävyystestien aikana aktiivinen palvelin oli käynnistetty uudestaan sammuttamatta päällä olevia virtuaalikoneita kyseisellä palvelimella. Tällä testillä testattiin VM:iden katkeamatonta toiminta HA/FT-klusterilla. Tulos oli rohkaiseva koska käyttäjälle ei tullut mitään huomattava toiminnassa.

6 Koelaitteiston testien kokemus

6.1 Monimutkaisuus ja helppokäytöisyys

Testilaitteiston kokoaminen ja muutokset sujuvat kohtalaisen helposti. Kun sopivat palvelinlaitteet oli hankittu, niiden virtuaalialustan ohjelmiston asennus ja päivitys onnistui ilman suuria ongelmia. Päivityksen jälkeen virtuaalikoneet toimivat kuin ennen. Klusterin luonti ja asetus oli helppo graafisen liittymän avulla, mutta vaatii asiantuntemusta. Virtualisointipätevyys ei välttämättä automaatioasiantuntijan vakio-osaamisalueella.

Ethernet verkko on pienentänyt fyysisesti, mutta sille on kasvanut vaatimukset. Kytkimien nopeus on kasvanut 1 Gb:ksi, iSCSI on tuonut verkon asetuksille monimuotoisuutta. Tällainen osaaminen taas on perinteisen ICT toimisto-osaston tuen asioita.

Toisin sanoin perinteinen automaatioasiantuntija tarvitsee virtualisointi- ja verkkolisäkoulutusta tai asiantuntevaa tukea yrityksen ICT-osastolta. ICT tuen pitää tuntea ja ottaa huomioon prosessiohjausverkon vaatimukset, jotka on poikkeavat verrattuna toimistoverkon vaatimuksiin.

6.2 Joustavuus

Virtuaalikoneiden migraatio ja luonti template:ista on onnistunut VMwaren vSphere 5 -alustalla erittäin hyvin ilman suurempia häiriöitä. Näiden toimenpiteiden kesto oli tyypillisesti alle tunti per tapahtuma. Vertailun vastakohteena olisi DCS IT-laiteiden (palvelin, operaattoriasema PC) puhdas asennus tai varmuuskopiointipalautus, jotka kestäisi useita tunteja. Näin säästyisi runsaasti aikaa, joka voi mitata rahana.

Migraatio on tuonut jousto-ominaisuutta, joka voi tehokkaasti hyödyntää huolto- ja vikatilanteissa. Näiden tilanteiden sattuessa huolto- tai korjaustyötä voi usein suorittaa sammuttamatta DCS:n palvelimia ja koko DCS:aa, eikä prosessiohjauspalvelu katkea.

Tänä päivänä virtualisointiohjelmisto eli Hypervisor käyttää 64 bittistä IT-prosessointitekniikkaa. Koska nykyisissä palvelimissa ja pöytäkoneissa riippumatta valmistajasta käytetään tätä tekniikkaa, syntyy tilanne että virtualisoinnin voisi soveltaa melkein mihin tahansa tietokoneeseen, joka täyttää ohjelmiston vaatimukset. Se antaa valinnanvaraa loppukäyttäjälle laitteiston hankinnan vaiheessa ja mahdollistaa kilpailuttamista ICT toimittajien tai -valmistajien välillä.

6.3 Tehon optimointi

Virtualisointitekniikan tärkein ominaisuus on resurssien optimaalinen käyttö. Silloin prosessoinnin ja muistin kapasiteettia käytetään palvelimen yhteismäärästä niin paljon kun tarvitaan. Tarpeen muukaan resursseja otetaan käyttöön lisää, esimerkiksi kun dataprosessoinnin määrää kasvaa.

Klusterin palvelimien välillä oleva resurssien tasaus tarjoaa uusia mahdollisuuksia DCS järjestelmän tehokkaassa käytössä. Sellainen tekniikka on mm VMWare:n DSR (Distributed Resource Sheduler).

Käynnistettyjen virtuaalikoneiden teho-optimointi eli DPM (Distributed Power Management) ei ole niin tärkeä DCS ympäristössä koska koneiden määrä on pieni ja niiden käyttö tyypillisesti jatkuva. Automaatiojärjestelmän koneiden siirto valmiustilaan ei ole suotava.

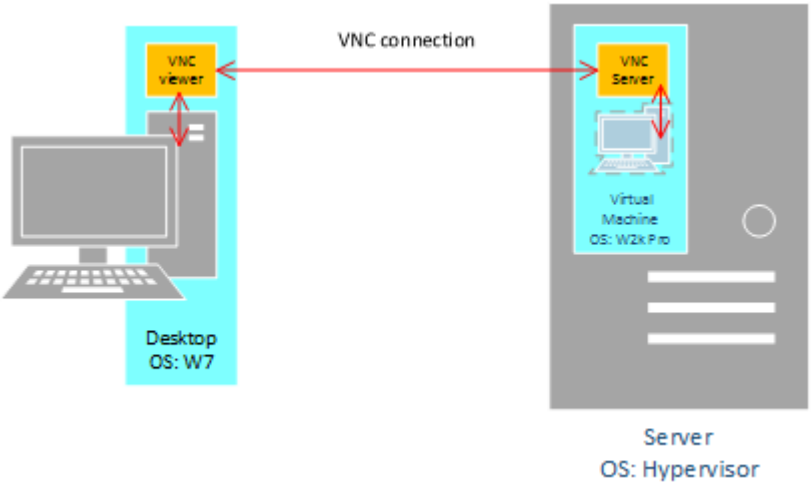
Testilaitteiston käytön aikana ei ilmennyt mitään häiriöitä, jotka viittaisivat resurssien riittämättömyyteen. Kahden palvelimen prosessointiteho oli samantyyppinen kuin tavallisissa DCS-palvelimissa, mutta keskusmuistia oli reilusti enemmän verrattuna perinteiseen automaatiopalvelimeen. Tästä voi päätellä että pienellä laitteiston lisäkustannuksella ja käyttämällä virtualisointia saadaan kokonaisjärjestelmä, joka on kustannuksilta edullisempi, kuluttaa vähemmän virtaa, vaatii vähemmän tilaa ja yhtä tehokas kuin periteisellä tekniikalla toteutettu.

6.4 Laitteiston muunneltavuus

Laitteistotarpeet muuttuvat virtualisoidussa ympäristössä. Fyysisiä palvelimia tarvitaan määrällisesti vähemmän, mutta niiden suorituskyky kasvaa. Myös oltava virtualisointituki ja klusterin vaadittamia prosessointitekniikat.

Tarvittavien palvelimien kokonpanoa joudutaan mitata. Aputyökaluja löytyy virtualisointitoimittajilla ja koko mittaaminen ei pitäisi aiheuttaa mitään vaikeuksia, koska se on puhtaasti IT-osaamista.

Melkein kaikissa tapauksissa pöytäkoneiden tilalle tulee terminaalit (Thin Clien). Kuitenkin tapauksissa, jossa terminaalien RDP tai muita yleisimpiä etäyhteyksien protokollia ei tueta, joudutaan käyttämään pöytäkonetta ja erikoisohjelmistoa. Esimerkiksi Microsoft Windows 200 Pro ei tue RDP:ta, silloin voidaan käyttää VNC tai PCAnywhere -ohjelmistoa (kuvio 16).



Kuvio 16. VNC-etäyhteys pöytäkoneesta virtuaalikoneeseen, jonka käyttöjärjestelmä on Microsoft Windows 2000 Pro

6.5 Haitat

Visualisointi eli VDI (Virtual Desktop Infrastructure) tuo haasteita DCS ympäristössä. Graafisen toteutuksekseen tulee kompromisseja koska laitteistonäytönohjain melkein aina varmempi ja monipuolisempi ratkaisu. Kriittisissä paikoissa Thin Clientin käyttö on mahdoton tai ei ole suositeltu ratkaisu. VDI lisensointi tuo kustannuksia ja hallinta-monimuotoisuutta.

Nykyiset Thin Client näyttöominaisuudet yleensä rajoittuu kahteen näyttöön. Koska jossakin tapauksissa valvomoissa käytetään esimerkiksi neljän näytön operaattori asemia, virtualisointi on näissä paikoissa mahdoton sopivien laitteiden puutteen vuoksi.

Thin Clientin verkkoyhteyden suorituskyky on tärkeä. Virtualisoinnin asiantuntija Vladan Seget väittää että 46% VDI projekteja kohtaavat kustannus- ja suorituskykyongelmia [16]. Kustannukset ovat huomattavia, esimerkiksi VMWaren Horizon View lisensointi on melko kallis pienille kokonaisuudelle (Taulukko 2), koska Connection Server vaatii Microsoft W2k8R2 lisenssiä. Sen lisäksi uusien Thin Clientien laitteiden hankintahinta on aika lähellä tavallisen PC:n kustannuksia. Asetus tuo haasteita, mm Horizon View Connection Server vaatii AD palveluita eli se pitää olla liitettynä domain serveriin. Melkein aina VDI ratkaisun markkinoinnissa korostetaan tehokkuutta, mutta ollaan vaitonaisia kustannuksista ja asetusten haasteista.

Taulukko 2. Vertailu Dell PC- ja Wyse+Horizon –ratkaisujen välillä eurona

	per yksikkö	per 10	per 1 operator	Huomautus
PC (perinteinen):				
Optiplex 3020	525,90	5 259,00	525,90	0% VAT
VDI (virtualized):				
Wyse Z90SW	405,00	4 050,00		0% VAT
Horizon View, 10 lic.		2 455,41	708,91	0% VAT
MS W2k8 R2 Std for Horizon Connection Server		583,84		0% VAT, Active Domain konfigurointi
Ero		**+1 830,05**	**+183,01**	

VDI:n osien lisensointi, ylläpito ja konfigurointi muuttuu haastavaksi ja vaatii automaatioammattilaiselta aiheen syvää tuntemusta. VDI:n toteutus voi olla aika kallis pienissä DCS järjestelmissä.

Thin Client terminaalin verkkoyhteyden kahdennus on vaikea toteuttaa, koska laitetarjonta täyttää vain toimistoverkon vaatimuksia, jolloin yhtä 1 Gbps yhteyttä riittää. WLAN yhteys ei saavuta 1Gbps nopeutta ja testeissä oli hieman takkuinen.

Kun kerran virtualisointialusta on valittu ja otettu käyttöön, vaikea siirtyä toiselle. Esimerkiksi virtuaalikoneiden muunnos VMware:n ja Microsoft:in välillä voi jossakin tapauksissa mahdoton. Automaatiojärjestelmän ohjelmistoriippuvuus yhdestä virtualisointitoimittajasta voi kestää jopa koko elinkaaren ajan.

Harvat DCS:n toimittajat ovat panostaneet virtualisointiin täysmääräisesti. Automaatiotoimittajat voivat hinnoitella oma virtualisointiratkaisuja niin että asiakkaalle toteutus tulee liian kalliiksi. Se voi aiheuttaa toimituksen virtualisoinnin hylkäämistä ja toteutumista perinteisellä tietotekniikalla. Silloin asiakas ei saa monia hyötyjä, jotka virtualisointi tuo.

6.6 Hyödyt

Tuki vanhoille käyttöjärjestelmille antaa lisäaikaa vanhoille DCS:lle ja pienentää päivitystarpeetta ja -tiheyttä. Pitää kuitenkin muistaa että vanhat käyttöjärjestelmät ovat haavoittuvia tietoturva-aukkojen takia.

Skaalattavuus ja joustavuus ovat virtualisoinnin tärkeämpiä ominaisuuksia. Kun virtualisointialusta on muodostettu, on mahdollista olemassa olevan automaatiojärjestelmän joustava migraatio virtuaaliseksi. Sen saa tehdä osittain, jolloin vain DCS:n tarvittavat osat muutetaan virtuaaliseksi, tai vaiheittain, jolloin eri virtuaalikoneiden käyttöönotto saa tehdä automaatiojärjestelmän olleessa toiminnassa ilman alasajoja.

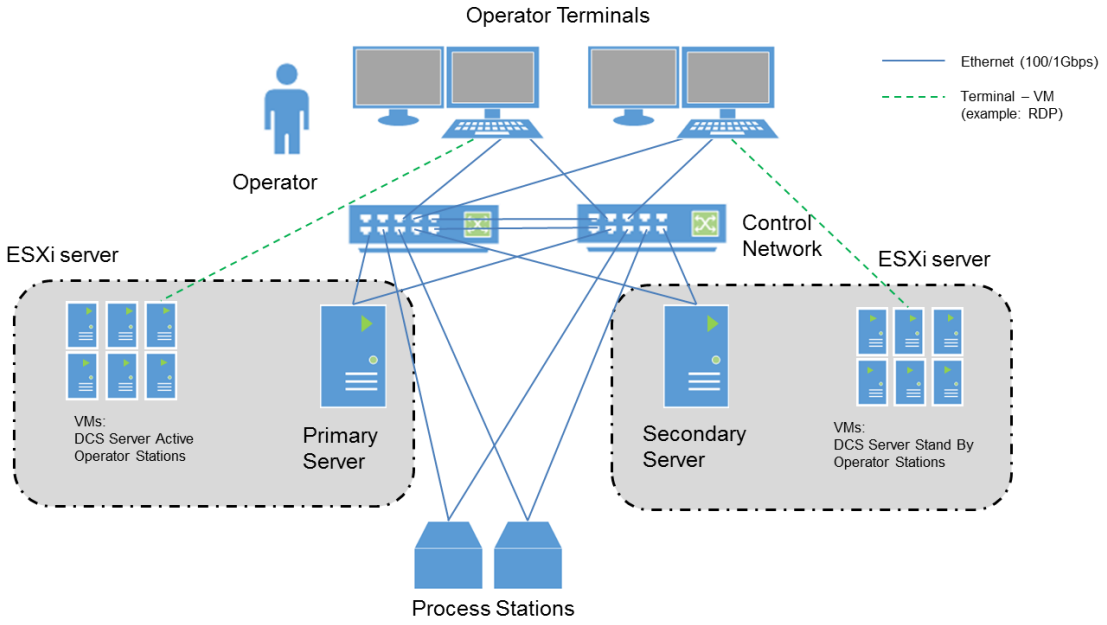
Palvelimien tilan ja -tehon tarpeet ovat pienemmät. Levypalvelimen vaikutus on vielä suurempaa. Nämä pienemmät tarpeet vaikuttavat toimituksen alkuvaiheessa pienemmällä tilainvestoinneilla, ja pitkällä tähtäimellä - alhaisemmalla tehon kulutuksella, joka kuluu prosessointiin ja palvelimien jäähdytyksekseen.

7 Käytön esimerkkejä

7.1 Erillinen Hypervisor-palvelin

Toteutus on esitetty kuviossa 17. Tällä hetkellä se on vallitseva ratkaisu automaatiotoimittajien keskuudessa. Yhden tai useamman Hypervisor-palvelimien ratkaisu tuo laitteisto-, tila- ja virtakulutussäästöjä. DCS:n verkon topologian muutokset on pieniä.

Tälle ratkaisulle on ominaista se että automaatiotoimittajat voivat varmistaa omien DCS lisenssien myyntiä entisellä tavalla. Pelkkä hypervisorin (ESXi server tai Hyper-V) lisensointi on edullista tai jopa ilmaista, koska edistyneiden ominaisuuksia ei käytetä ja perustoiminnot, kuten varmuuskopiointi, on käytössä. Tämän ratkaisun yleistymiselle lienee olla toinen selitys: automaatiotoimittajat myyvät vai testatut ja varmat ratkaisut, ja korkean käytettävyyden ratkaisut ei ole vielä testattu kunnolla ja tuotteistettu monilla automaatiovalmistajilla. Esimerkiksi ESXi server ohjelmisto on ollut vuosia markkinoilla ja kerännyt paljon kokemusta ja sen lisäksi osoittautunut varmaksi ja helppokäyttöiseksi alustaksi.

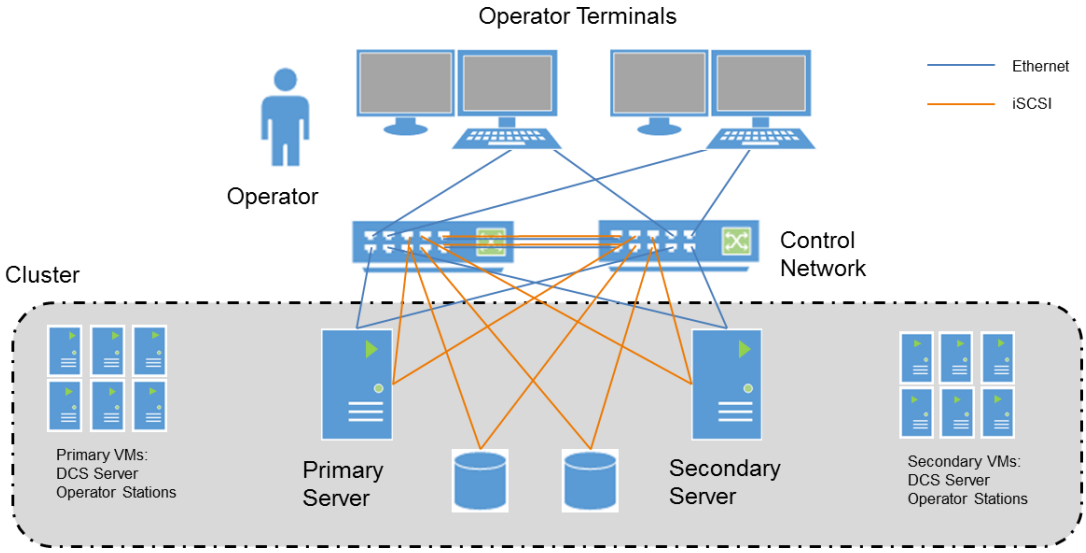


Kuvio 17. ESXi erillispalvelimien toteutus.

Tämän ratkaisun heikkona puolena voi pitää se että virtuaaliset koneet ovat sijoitettu yhteen palvelimeen. Yksittäisen ESXi-palvelimen pettäessä prosessiohjauksen aikana tapahtuu kaikkien sen palvelimen VM:den menetys ja ohjaus voi halvaantua.

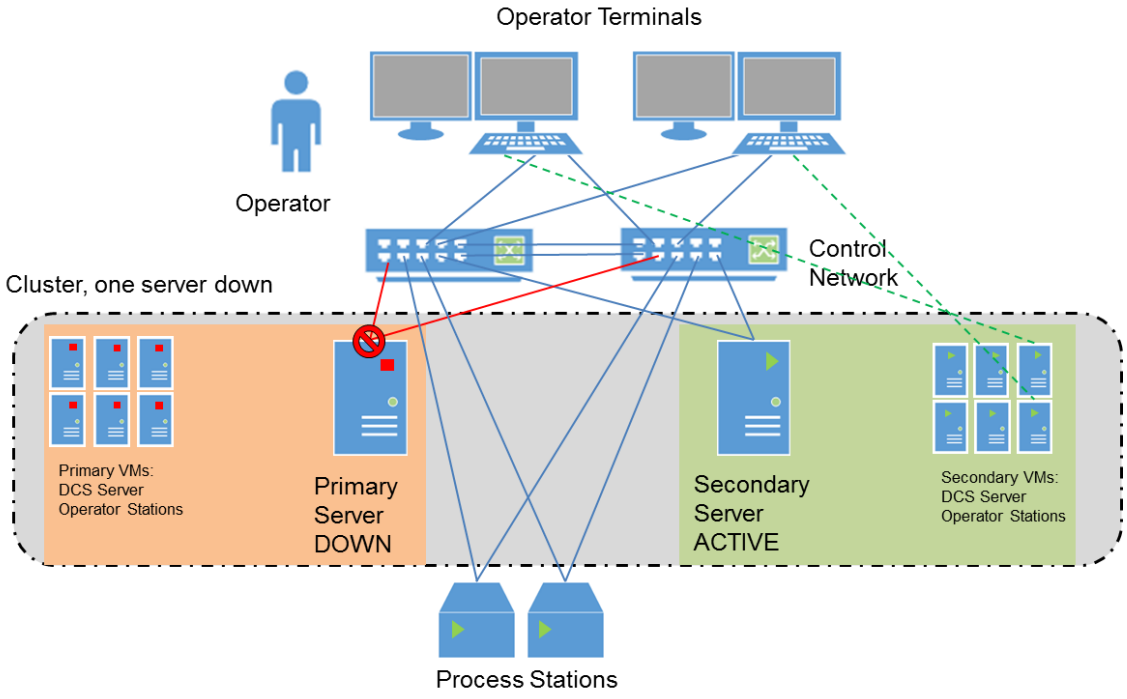
7.2 Korkean käytettävyyden klusteri, iSCSI

Tällainen ratkaisu (kuvio 18) tuo enemmän joustavuutta ja vikasietokykyä verrattuna edelliseen. Ratkaisu vaatii SAN tai NAS komponenttia ja tuo kompleksisuutta. iSCSI-komponenttien suunnittelu ja toteutus vaatii myös Ethernet-verkon asiantuntemusta. VMWare:n HA-klusterin lisenssit ovat hintavia, ja sen takia taloudellinen hyötyy olisi vain suurissa DCS toimituksissa.



Kuvio 18. HA klusteri, iSCSI, prosessiohjaimet ja kenttälaitteet eivät ole kuviossa.

Yksittäisen ESXi palvelimen pettäessä järjestelmä palvelee tauottomasti koska ajo siirtyy varalla oleville VM:ille toisella ESXi palvelimella (kuvio 19).



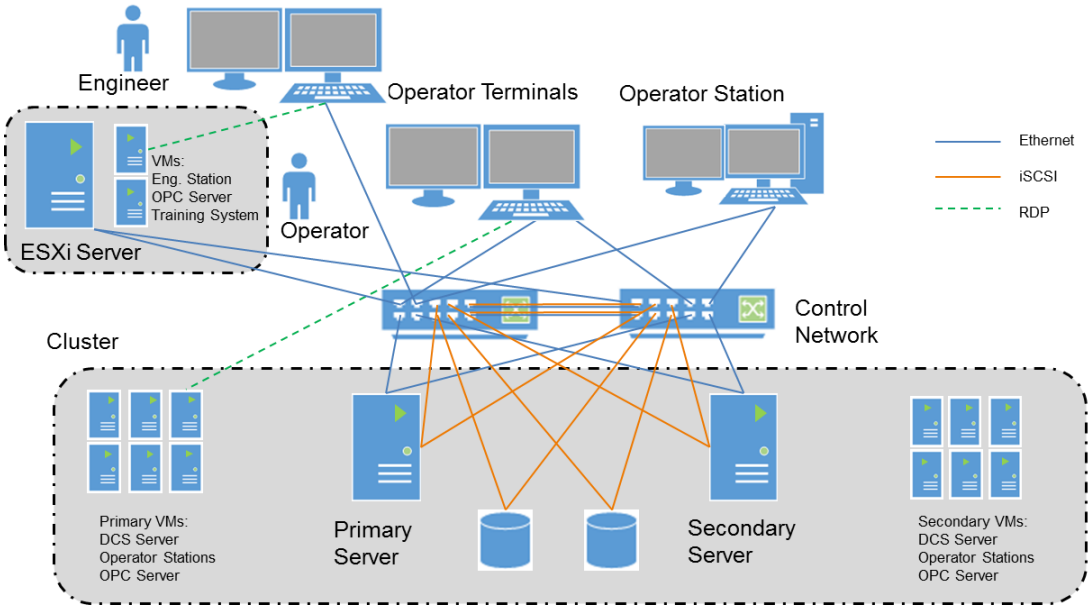
Kuvio 19. Vikatilanne ESXi palvelimella, ohjaus siirtyy varalla olevalle palvelimelle

7.3 Sekaratkaisu

Kahden edellisen ratkaisun sekatoteutus on hyvä ratkaisu, kun halutaan lisätä vikasietokykyä kriittiselle prosessiohjaukselle ja käyttää vähemmän ATK-laitteistoa ei-kriittisillä ohjausalueilla (kuvio 20). Ei-kriittiset alueet tai komponentit, esimerkiksi yksittäiset OPC-palvelimet, sovellusasemat ja opetuskokonaisuudet ovat alun perin yksittäisiä koneita tai ryhmä koneita, jotka ei ole kahdennettu, ja kaatumistilanteessa eivät haitallisesti vaikuta DCS:n toimintaan.

Kriittiset osat toteutetaan korkean käytettävyyden klusterissa ja se takaa prosessiohjauksen toimintaa tietoteknisten osien häiriö- ja vikaantumistilanteissa.

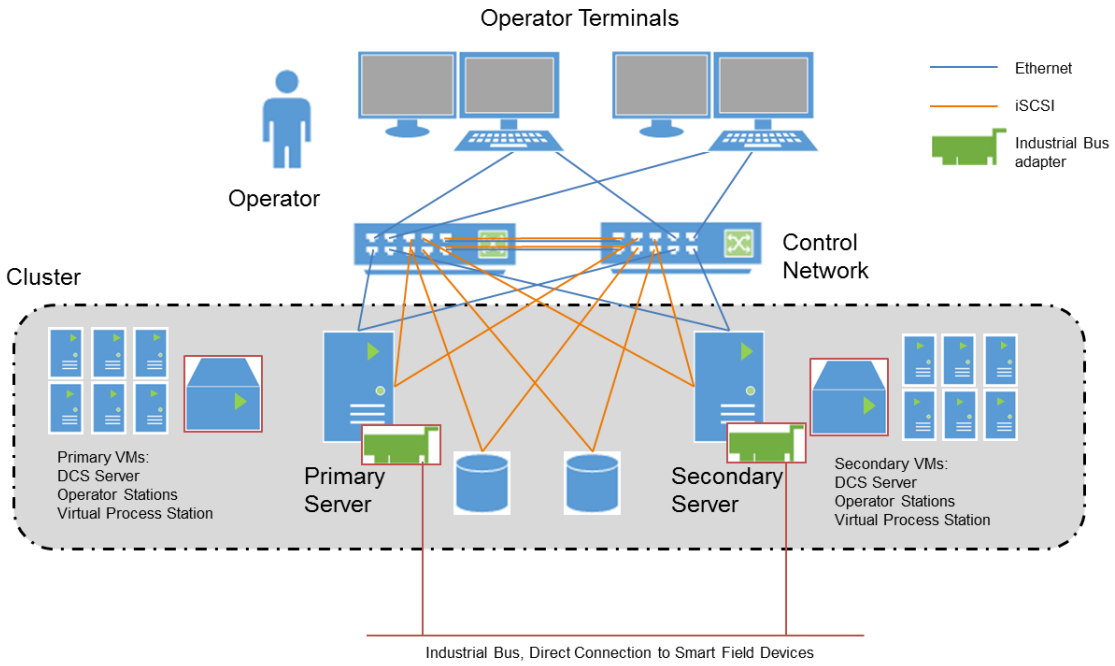
Sekalainen toteutus sopii myös silloin, kun halutaan laajentaa olemassa oleva DCS käyttäen nykyaikaista tietotekniikkaa.



Kuvio 20. Sekaratkaisu. HA-kluster ja erillinen ESXi server.

7.4 Visio – vPLC, Virtual Process Station

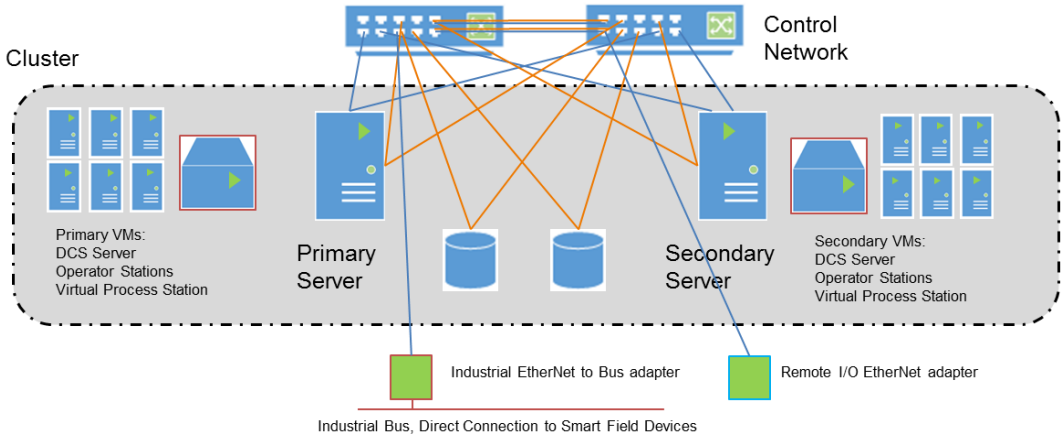
Hyvin mahdollista ja toivottavaa on, että virtualisointialustojen toimittajat tekevät automaatiotoimittajien kanssa yhteistyötä ja kehittävät tietokoneiden laajennuskorttien yhteensopivuutta virtualisointialustojen kanssa. Tämä mahdollistaisi teollisuusväyläkorttien käyttöä virtualisoidussa ympäristöissä (kuvio 21).



Kuvio 21. Visio virtuaalisien prosessiohjaimien käytöstä ja teollisuusväylän soveltamisesta virtualisoidun ympäristöön.

Tänä päivänä uteliaat kokeilijat yrittävät käyttää olemassa olevia teollisuussovittimia virtualisoidussa ympäristössä mutta ongelmia ilmenee [8]. Vaikka olisi tuki Windowsille, PCI-kortti tai muu tietokoneeseen liitetty adapteri ei välttämättä toimi virtualisoidussa ympäristössä.

Toinen vaihtoehto olisi Ethernet-teollisuusväylien tai Remote I/O -sovittimien käyttö [12], (kuvio 22). Tällöin fyysinen prosessiohjain korvataan virtuaalisella koneella (Virtual Process Station), joka kommunikoi kenttälaitteiden kanssa I/O-sovittimien avulla.



Kuvio 22. Esimerkki Ethernet sovittimien soveltamisesta.

Molemmissa tapauksissa on ratkaisevaa, lähteekö automaatiotoimittajat ja teollisuuskomponenttien valmistajat kehittämään laitteita, sovellusohjelmistojaan ja ajureita. Tähän kehityksen polulle pienet laitevalmistajat olisivat ehkä enemmän halukkaita lähtemään koska se voi olla kasvun mahdollisuus ja heillä ei olisi oman ison DCS ekosysteemin kahleita.

Nykyinen Metso DNA prosessiautomaation rakenne on mielenkiintoinen, koska I/O -väylänä on käytetty Ethernet [sivu 9, 17]. Periaatteessa se on Industrial Ethernet –väylällä toteutettu RTU-ratkaisu [18]. Metson esitteessä on kerrottu [sivu 5, 17], että prosessiohjain voi toteuttaa myös tavallisella PC:llä. Jos ACN-ohjain ei vaadi erikoisia laajennuslisäkortteja tai muita kopiointi- ja suojausmenetelmiä, niin teoriassa ACN-prosessiasema ohjauspalvelimen lisäksi voisi toteuttaa virtuaalisena.

8 Yhteenveto

ICT:n käyttö DCS-toteutuksessa on lisääntynyt merkittävästi viime vuosikymmenillä, ja nyt on mahdollista soveltaa myös virtualisoinnin tekniikkaa, joka on kehitetty alun perin ICT:tä varten. Käyttämällä ICT:n virtualisointia automaatiossa syntyy merkittäviä laitteisto-, energia- ja tilasäästöjä. Kokonaisjärjestelmän konfigurointi ja ylläpito monipuolistuu ja osittain vaikeutuu riippuen henkilökunnan osaamistasosta ja osastojen välisestä yhteistyöstä.

Virtualisoidun DCS:n merkittävä etu on järjestelmän elinkaaren pidentäminen, joka johtuu siitä, että virtuaaliympäristössä saa ajaa DCS:n keskeisiä osia (muun muassa

prosessiohjauspalvelimia, operointiasemat) riippumatta siitä, mikä on datakeskuksen eli suurtehoisen palvelimen laitteisto tai ohjelmisto. Tuki vanhemmille OS:ille antaa arvokasta lisäaikaa DCS:n vanhoille tietokoneille, mutta pitää muistaa, että turvallisuusriski on iso vanhojen käyttöjärjestelmien haavoittuvuuden takia.

Honeywellin esimerkki todistaa sen, että automaatiojärjestelmien ICT puolella on tapahtumassa iso muutos: suuren määrän ATK-koneiden ja palvelimien tilalle on tulossa keskitettyjä ratkaisuja, kuten datakeskuksia, ethernet-verkon suorituskyky ja monimutkaisuus kasvavat, automaation asiantuntijoiden ICT- ja virtualisointiosaaminen korostuu. Prosessiohjauksen toiminnan kahdennus on siirtymässä laitteistosta infrastruktuurin tasolle.

Kun Ethernet yleistyy I/O-väylänä, se avaa mahdollisuuksia korvata prosessiohjaimia virtuaalikoneilla. Tämä voi muuttaa automaatiojärjestelmän rakennetta merkittävästi ja mullistaa automaatiotoimittajien markkinat samalla tavalla kuin mobiilipuhelimien alaa. Automaatio-osista, kuten I/O-kortit ja prosessiohjaimet (myös VM:nä), tulisi avoimia, ja kuka tahansa voisi tarjota omia ratkaisuja. Silloin vain systeemisuunnittelu, kyberturvallisuus ja toteutus olisivat tärkeässä roolissa. Automaatiotoimittajalla olisi vahva asema integraattorina, joka on kokonaisvastuussa järjestelmän toiminnasta.

Automaatiotoimittajat joutuvat kireämpään kilpailutilanteeseen suunnittelu- ja konsultointiyrityksien kanssa. Virtualisointiin erikoistunut automaatiosuunnitteluyritys pystyisi suunnittelemaan ja toimittamaan virtualisoitu DCS:n ICT infrastruktuuria, koska käytettävissä olevat laitteisto- ja infrastruktuuriohjelmistot ovat myös automaatiotoimittajien laajassa käytössä. ICT-laitteistoriippuvuus automaatiotoimittajilta vähenee.

Lähteet

1 Virtualisointi http://www.vmware.com/virtualization/, luettu 27.01.2014

2 Manufacturing Operations Management, Dennis Brandl http://www.futuristix.co.za/content/S95_Tutorial.pdf, luettu 17.4.2014

3 Virtualisointi http://software.intel.com/en-us/articles/the-advantages-of-using-virtualization-technology-in-the-enterprise, luettu 27.01.2014

4 Teollisuusautomaation tietoturva, https://www.cert.fi/attachments/cip/5na1SblCp/SAS29_TeollisuusautomaationTietoturva.pdf, luettu 19.2.2014

5 VMware ja Microsoft Hyper-V lissensoinnin vertailu, http://www.techrepublic.com/blog/the-enterprise-cloud/microsofts-hyper-v-r2-vs-vmwares-vsphere-a-cost-comparison/1851/, luettu 20.2.2014

6 Guide to Industrial Control Systems (ICS) Security http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, luettu 3.3.2014

7 Korkean käytettävyyden klusteri http://www.vladan.fr/how-to-configure-vmware-high-availability-ha-cluster/, luettu 17.4.2014

8 Siemens CP5512 access on Virtual PC http://www.plctalk.net/qanda/showthread.php?t=34491, luettu 17.4.2014

9 Honeywell Brings Virtualization to Blade Servers for Process Industries http://www.automationworld.com/control/honeywell-brings-virtualization-blade-servers-process-industries?utm_source=News_Insights&utm_medium=newsletter&spMailingID=6378318&spUserID=NDA3MDU0NjIyNzUS1&spJobID=76159888&spReportId=NzYxNTk4ODgS1, luettu 17.4.2014

10 vStart 50 tietokeskus http://www.dell.com/us/business/p/dell-vstart-50/pd, luettu 26.2.2014

11 Yokagwa DCS käytettävyys http://www.yokogawa.com/sbs/Yokogawa-plus/S-Essay/vol1/sbs-S-essay-e01.htm, luettu 26.2.2014

12 Remote module for Profibus http://www.bradharrisonsales.com/pdfs/112016.pdf, luettu 17.4.2014

13 Siemens forum http://www.automation.siemens.com/WW/forum/guests/PostShow.aspx?PageIndex=1&PostID=246257&Language=en, luettu 17.4.2014

14 Blog, DMZ http://blog.industrialdefender.com/?p=385, luettu 17.4.2014

15 Blog, Network Segmentation http://blog.industrialdefender.com/?p=271, luettu 17.4.2014

16 Free Technical PDFs http://www.vladan.fr/free-resources/, luettu 17.4.2014

17 Metso DNA, Technical overview http://www.metso.com/Automation/ip_prod.nsf/WebWID/WTB-110922-2256F-BB6C0/$File/E8724_EN_05-Metso%20DNA%20Overview.pdf, luettu 17.4.2014

18 Remote Terminal Unit, http://en.wikipedia.org/wiki/Remote_Terminal_Unit, luettu 17.4.2014

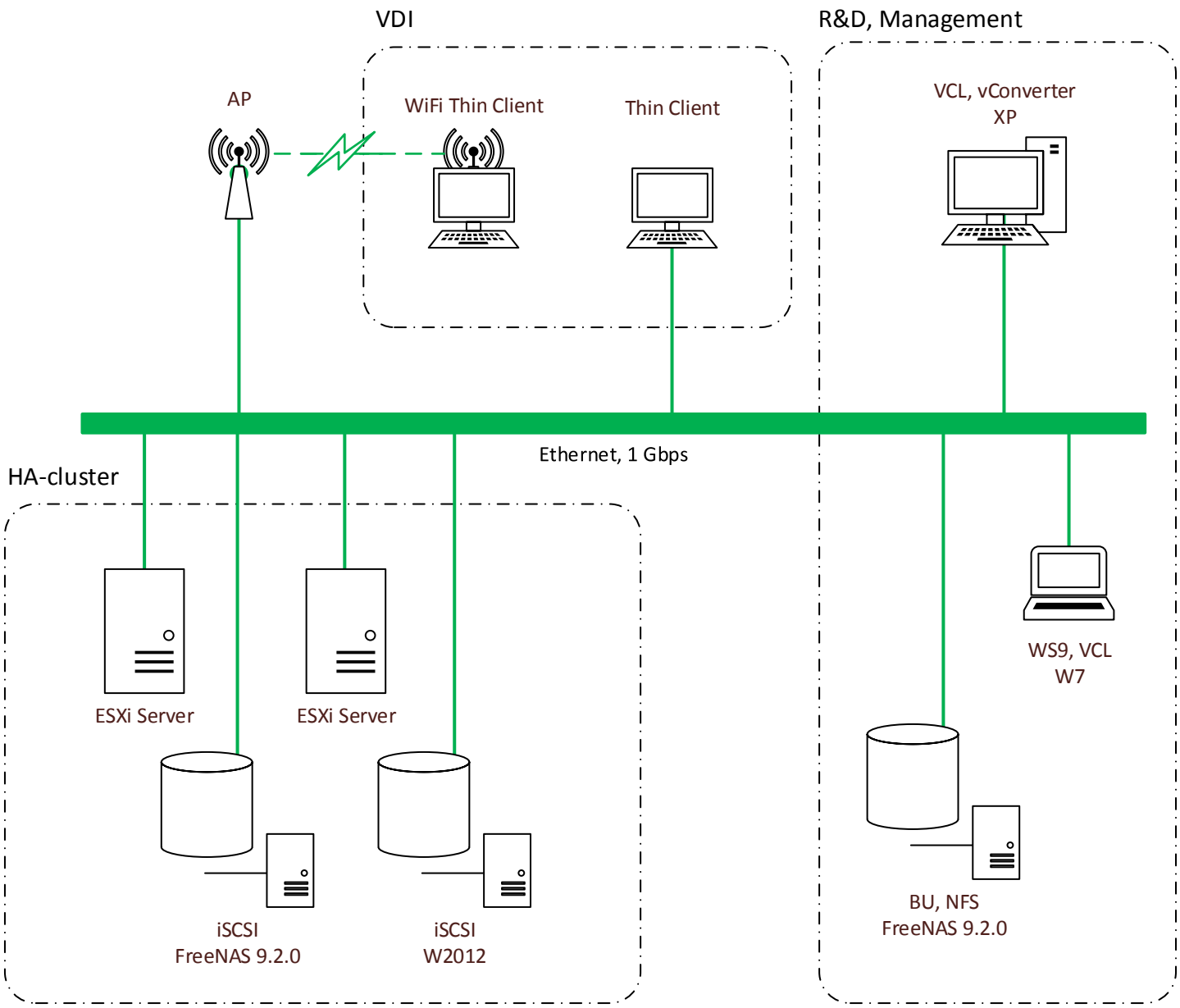
19 Artikkeli teollisuusvakoilusta http://ru.reuters.com/article/topNews/idRUMSEA0L02N20140122?pageNumber=2&virtualBrandChannel=0, luettu 17.4.2014

20 Paul Hodge, Advanced Virtualization Benefits with the New PremiumPlatform https://www.honeywellprocess.com/library/news-and-events/presentations/Hon-EMEA13-Hodge-Experion-Virtualization-Premium.pdf, luettu 17.4.2014, vaatii rekisteröintiä

21 DELL 3-2-1 REFERENCE CONFIGURATIONS: HIGH-AVAILABILITY VIRTUALIZATION WITH DELL POWEREDGE R720 SERVERS http://www.principledtechnologies.com/Dell/R720_321_configuration.pdf, luettu 7.3.2014

22 Configuring a PowerConnect 5424 or 5448 Switch for use with an iSCSI storage system, http://en.community.dell.com/techcenter/storage/w/wiki/2721.configuring-a-powerconnect-5424-or-5448-switch-for-use-with-an-iscsi-storage-system.aspx, luettu 7.3.2014

Koelaitteiston yleiskaavio:



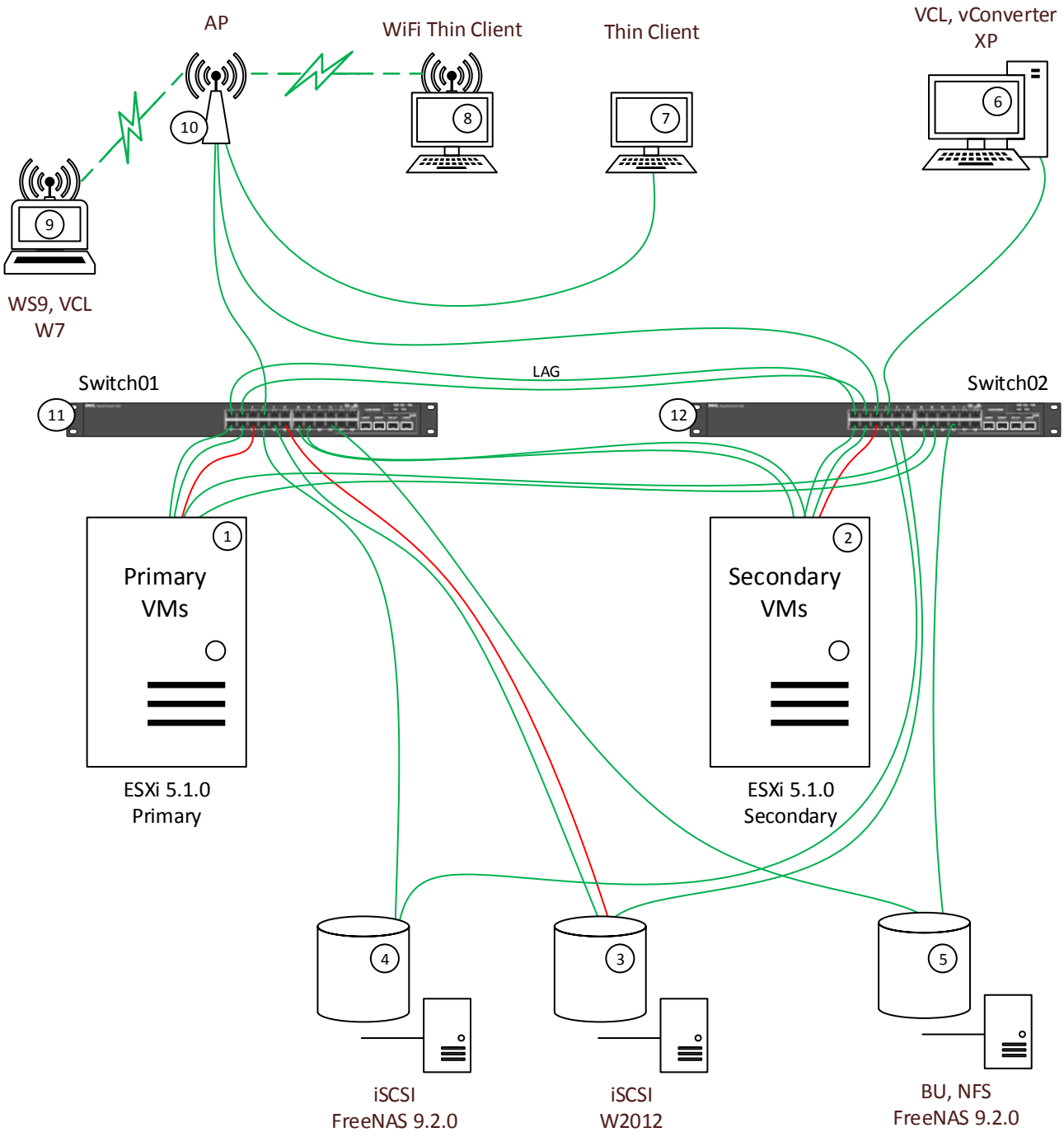
VMware:
VCL -vSphere Client
WS9 -Workstation 9
ESXi -hypervisor

AP -Access Station
BU -Back-Up

Microsoft:
W7-Windows 7
W2012-Windows 2012
XP-Windows XP

Kuvio 23 Virtualisoitu hajautettu prosessiohjausjärjestelmä

Koelaitteiston topologia:



IP address	Description
10.1.0.x	DCS, iSCSI: 1-12 Management: 3-5, 10-12 BU: 5, 6
10.1.2.x	Reserved for iSCSI
10.1.3.x	Management: 1-3

Kuvio 24 Ethernet-verkon topologia