Janne Rantala

Järjestelmätestauksen kehittäminen ja koneturvallisuuden huomioiminen testauksessa

Opinnäytetyö
Syksy 2018
SeAMK Tekniikka
Automaatiotekniikan tutkinto-ohjelma

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikan yksikkö

Tutkinto-ohjelma: Automaatiotekniikka

Suuntautumisvaihtoehto: Koneautomaatio

Tekijä: Janne Rantala

Työn nimi: Järjestelmätestauksen kehittäminen ja koneturvallisuuden huomioiminen testauksessa

Ohjaaja: Heikki Rajala

Vuosi: 2018 Sivumäärä: 35 Liitteiden lukumäärä: 2

Opinnäytetyön toimeksiantajana toimi Valmet Automation Oy:n HSEQ-organisaatio Tampereen toimipisteestä. HSEQ-organisaatiosta työssä mukana olivat etenkin laatu ja toiminnallinen turvallisuus. Tavoitteena oli koota Valmet DNA -ohjausjärjestelmän olemassa olevat testausohjeet ja uudistaa ne nykystandardien vaatimuksien mukaisiksi. Testausohjeita tullaan käyttämään Valmet Automationin sisäisiin järjestelmätestauksiin tehdaskoestuksissa ja käyttöönotoissa. Opinnäytetyön teoriaosuudessa on käytetty standardikirjastoja, Valmetin sisäisiä tiedostoja ja opetusmateriaaleja. Työssä on myös haastateltu muutamaa henkilöä tietojen ajantasaisuuden varmistamiseksi.

Aluksi työssä käydään läpi hieman työn taustoja, Valmetin historiaa ja nykytilannetta. Tämän jälkeen tutustutaan Valmet DNA -ohjausjärjestelmään ja sen toimintaan. Kun perusteet on käyty läpi, perehdytään tarkemmin standardien ja FMEA-analyysin asettamiin vaatimuksiin järjestelmän toiminnassa sekä testauksessa. Työn lopussa läpikäydään päivitetyt testit.

Uusia testausohjeita tullaan käyttämään jatkossa jokaisessa Valmet Automationin toimitusprojektissa minimivaatimuksena. Standardisoitu ohje helpottaa järjestelmällistä ja yhdenmukaista testaamista toimitusprojekteilla. Ohjetta tullaan ylläpitämään niin, että se vastaa muuttuvia standardivaatimuksia ja Valmet Automationin prosessinohjausjärjestelmän teknologiamuutoksia.

Avainsanat: Valmet DNA, ohjausjärjestelmät, EU-direktiivit, standardi, testaus, FMEA

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Automation Engineering

Specialisation: Machine Automation

Author: Janne Rantala

Title of thesis: Development of System Testing with a Focus on Machine Safety

Supervisor: Heikki Rajala

Year: 2018 Number of pages: 35 Number of appendices: 2

The thesis was commissioned by the HSEQ organization of Valmet Automation Oy at the Tampere office. From the HSEQ organization, particularly quality and functional safety departments were involved in the project. The aim was to collect the test instructions of the existing Valmet DNA control system and revise them according to the requirements set by the current standards. The test instructions will be used for the Valmet Automation's internal system testing and commissioning. Standard library material, Valmet's internal files and teaching materials were used for the theoretical sections of the thesis. Some people were also interviewed to ensure timely information.

At first the thesis concentrated on the history of Valmet and the current situation of the company. After that the Valmet DNA control system and its operations were introduced. Once the basics had been covered, the requirements set by the standards and the FMEA on system operation and testing were studied in more detail. The updated tests were presented at the end of the thesis.

The new test instructions will be used in the future for each Valmet Automation delivery project as a minimum requirement. Standardized instructions simplify the testing of delivery projects and make it more systematic and consistent. The instructions will be maintained so that they will keep up with the changes in the requirements set by the standards, and also with the changes in the process control system technology of Valmet Automation.

Keywords: Valmet DNA, control systems, EU Directives, standard, testing, FMEA

SISÄLTÖ

KUVALUETTELO

KÄYTETYT LYHENTEET

ACN	Application and Control Node, sovellus- ja ohjauspalvelin
ALS	Alarm Server, hälytyspalvelin
BU	Back Up, varmennuspalvelin
DMZ	Demilitarized Zone, turva-alue (Tietoverkon palomuurein eristetty osa)
DNA	Dynamic Network of Application, automaatiojärjestelmä
EAC	Engineering Activity Client, suunnittelutyöasema
EAS	Engineering Activity Server, suunnittelupalvelin
EMC	Electromagnetic Compatibility, sähkömagneettinen yhteensopivuus
EN	Eurooppalainen standardoimisjärjestö
FAT	Factory Acceptance Test, tehdaskoestus
FMEA	Failure Modes and Effect Analysis, vika- ja vaikutusanalyysi
HAZOP	Hazard and Operability Study, poikkeamatarkastelu
HSEQ	Health, Safety, Environment and Quality, terveys, turvallisuus, ympäristö ja laatu
IEC	International Electronechnical Commission, kansainvälinen sähköalan standardisoimisorganisaatio
I/O	Input/Output, automaatiojärjestelmän sisääntulo-/ulostuloliitäntä
IP	Internet Protocol, verkkoprotokolla

ISO	International Organisation for Standardization, kansainvälinen standardisoimisjärjestö
LVD	Low Voltage Directive, pienjännitedirektiivi
OPS	Operator Server, operointipalvelin
PCS	Process Control Server, prosessinohjauspalvelin
PLC	Programmable Logic Controller, ohjelmoitava logiikka
SFS	Suomen Standardisoimisliitto
SNMP	Simple Network Management Protocol
UPS	Uninterruptible power supply, keskeytymätön virransyöttö
USB	Universal Serial Bus
VA	Valmet Automation

1 JOHDANTO

Tässä luvussa käydään läpi työn taustat, tavoitteet, rakenne, tutkimusmenetelmät sekä kerrotaan perusasioita opinnäytetyön toimeksiantajana toimivasta yrityksestä. Luvussa sivuutetaan myös hieman Valmet DNA -tuoteperhettä.

1.1 Työn tausta

Opinnäytetyön toimeksiantajana toimii Valmet Automation Oy:n HSEQ-organisaatio.

Valmet Automation toimittaa automaatiojärjestelmiä paperi- sekä selluteollisuuteen, energiateollisuuteen ja prosessiteollisuuteen.

Työ käsittelee turvaluokittelemattoman Valmet DNA -prosessinohjausjärjestelmän testausta niin, että testauksessa huomioidaan konedirektiivin ja siihen liittyvien standardien koneturvallisuudelle asettamat vaatimukset.

Valmet DNA -ohjausjärjestelmä ei suoranaisesti kuulu konedirektiivin 2006/42/EY soveltamisalaan, koska ohjausjärjestelmä ei itsessään ole kone. Mutta konedirektiivin vaatimuksia noudatetaan soveltuvin osin, koska Valmet DNA -ohjausjärjestelmän avulla ohjataan koneita.

Konedirektiivin vaatimusten tarkkaa noudattamista vaikeuttaa lisäksi se, että samalla järjestelmällä ohjataan muitakin prosessilaitteita ja -alueita, joita koskevat omat vaatimuksensa on myöskin otettava huomioon.

Konedirektiivi 2006/42/EY koskee Euroopan Unionin sisämarkkinoita, mutta sen mukainen toteutus hyväksytään hyvin yleisesti muissakin maissa muutamia poikkeuksia lukuun ottamatta, esimerkiksi USA ja Kanada.

Tässä työssä ei käsitellä turvaluokiteltuja järjestelmiä, mutta seuraavassa on lueteltu näitä koskevia standardeja, joita on voitu käyttää tässä työssä noudatettujen standardien tukiaineistona:

- SFS-EN 61508 (Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus), koskee laitteiston suunnittelua
- SFS-EN 61511 (Toiminnallinen turvallisuus. Turva-automaatiojärjestelmät prosessiteollisuussektorille), koskee toimitusprojektin toteutusta
- SFS-EN ISO 13849 (Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmän osat)
- SFS-EN 62061 (Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus).

Turvaluokiteltujen järjestelmien tarkkaan määritellystä toteutustavasta poiketen turvaluokittelemattoman ohjausjärjestelmän toteutus on vaihdellut huomattavastikin projektikohtaisesti, eikä testauksille ole ollut tarkkaan määriteltyä ohjeistusta. Nyt testaukset halutaan yhtenäistää ja lisäksi testeistä on puuttunut testit, joilla voidaan osoittaa, että täytetään myöskin turvaluokittelemattomia ohjausjärjestelmiä koskevat kiristyneet koneturvallisuusvaatimukset.

Tässä työssä ei käsitellä myöskään Valmet DNA -järjestelmän prosessikohtaisia sovellusohjelmistoja, koska sovellukset tehdään asiakkaan tekemien toimintakuvausten mukaisesti, ja asiakas vastaa toimintakuvausten vaatimuksenmukaisuudesta.

1.2 Työn tavoite

Opinnäytetyön tavoitteena on tehdä yleismallinen ohje järjestelmätestauksesta ja tutkia konedirektiiviin liittyvien standardien vaatimuksia testauksessa ja suunnitella tarvittavat testit näiden standardien pohjalta.

Valmis työ tulee Valmet Automationille testausohjeeksi toimitusprojekteihin.

1.3 Työn rakenne

Luvussa yksi käydään läpi perusasiat yrityksestä, työn taustasta sekä työn tavoitteista.

Luvussa kaksi kerrotaan Valmet DNA -järjestelmän rakenteesta, vikasietoisuudesta, Valmet DNA -järjestelmän ja koneiden ohjauksen turvallisuudesta sekä toimitusprojektien laadunvarmistuksesta.

Luvussa kolme kerrotaan aluksi koneturvallisuuteen liittyvien standardien vaatimuksista, tehdään vika- ja vaikutusanalyysi (FMEA), sen jälkeen nämä yhdistämällä määritellään tarvittavat testit toimitusprojektin ohjausjärjestelmälle.

Luvussa neljä on yhteenveto työn tuloksista sekä pohdintaa työstä.

1.4 Työn eteneminen

Työ etenee seuraavasti:

- Aluksi työssä tutustutaan Valmet Automationiin yrityksenä ja tämän jälkeen käydään läpi Valmet DNA -järjetelmän perusasiat.
- Seuraavaksi tutkitaan, mitä vaatimuksia konedirektiivi ja standardit asettavat konetta ohjaavalle ohjausjärjestelmälle.
- Ohjausjärjestelmän mahdollisten vikatilanteiden koneohjaukselle aiheuttamat riskit tarkastellaan ja analysoidaan FMEA-vika- ja vaikutusanalyysillä.
- Ohjausjärjestelmälle tarvittavat turvallisuuteen liittyvät testit suunnitellaan FMEA-analyysin tulosten pohjalta. Testejä tullaan käyttämään ja kehittämään edelleen Valmet Automationin toimitusprojekteissa.

1.5 Valmet Oyj

Tässä luvussa käydään läpi koko Valmet Oyj:n toimintaa sekä historiaa. Lisäksi perehdytään Valmet Oyj:n tytäryhtiöön Valmet Automationiin koneautomaatiotoimittajana sekä sen tuoteperheeseen.

1.5.1 Valmetista yleisesti

Valmet Automation Oy on Valmet Oyj:n tytäryhtiö, jonka toiminnan pääpaino on sellu- , paperi- sekä energiateollisuudessa. VA on näiden osalta johtava teknologian, automaation sekä palveluiden toimittaja maailmalla. Valmetilla työskentelee 12 000 ammattilaista ympäri maailman lähellä asiakkaita ja heidän menestystään edistäen. Valmet tarjoaa asiakkailleen automaatioratkaisuja yksittäisistä mittauksista koko tehtaan laajuisiin automaatioprojekteihin. (Valmet [Viitattu 20.6.2018].) Kuvassa 1 on Valmet Oyj:n logo.

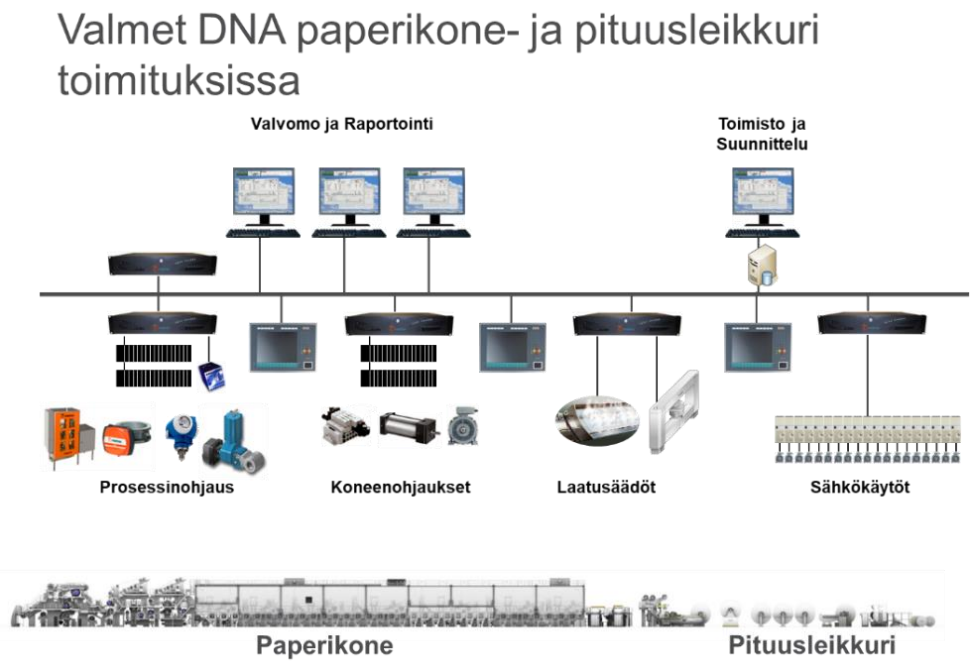
Kuva 1. Valmet Oyj:n logo. (Valmet [Viitattu 20.6.2018].)

Valmetin teollisuushistoria yltää yli 200 vuoden päähän vuoteen 1797, jolloin toimintansa aloitti teknisiä tekstiilejä toimittava Tamfelt. Vuonna 1999 syntyi Metso Oyj Valmetin ja Rauman yhdistyttyä. Ennen yhdistymistä Valmet toimitti paperi- ja kartonkikoneita ja Rauman pääpaino oli kuituteknologiassa, kivenmurskauksessa sekä virtauksensäätöratkaisuissa. Yhdistymisen seurauksena syntyi maailmanlaajuinen prosessiteollisuutta palveleva laitetoimittaja. Vuosien 2000–2009 aikana Metso osti Beloit Corporationin pehmopaperin- ja paperinvalmistusteknologian sekä tämän Ranskan ja Yhdysvaltojen

palvelutoiminnot, Aker Kvaerner ASA:n Pulping- and Power -liiketoiminnot, joihin kuului sellu- ja paperiteollisuus, ja Tamfelt Oyj:n. 2013 Metso jakautui kahdeksi erilliseksi yhtiöksi, Metsoksi ja Valmetiksi. Jakautumisen myötä massa- , paperi- ja voimantuotanto ovat Valmet Oyj:n alaisia liiketoimia ja kaivos- , maanrakennus- sekä automaatiotoiminnat ovat Metso Oyj:n alaisia. Kaksi vuotta myöhemmin Valmet osti prosessiautomaatiojärjestelmät-liiketoiminnan Metsolta. (Valmet [Viitattu 21.6.2018].)

1.5.2 Valmet Automation koneautomaatiotoimittajana

VA toimittaa koneiden ohjausjärjestelmiä osina tehdaslaajuisia automaatiotoimituksia ja yksittäisten koneiden osana sekä Valmetin omissa paperi- , sellu- ja energiaprojekteissa että muiden prosessilaite- ja konetoimittajien toimitusprojekteissa. Seuraavassa esimerkkikuvassa näkyvät VA:n tuotteet paperiteollisuuteen. (Valmet [Viitattu 22.6.2018].) Kuvassa 2 esitellään Valmet DNA -järjestelmän rakenne ja komponenttikokonaisuudet paperikone- ja pituusleikkuritoimituksissa.



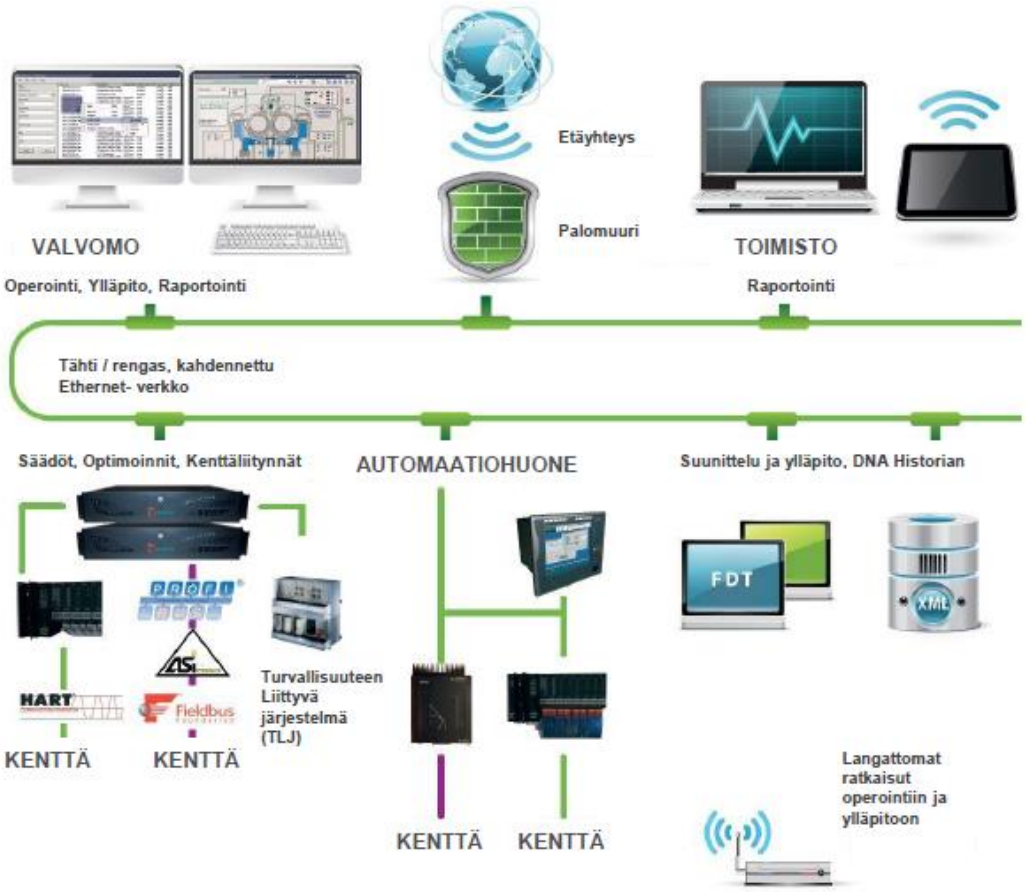
Kuva 2. Valmet DNA paperikone- ja pituusleikkuritoimituksissa. (Valmet [Viitattu 22.6.2018].)

2 VALMET DNA -JÄRJESTELMÄ

Tässä luvussa käydään läpi Valmet DNA -järjestelmän perusrakenne sekä sen vikasietoisuus eri osa-alueiden osalta. Luvussa käsitellään myös ohjausjärjestelmään liittyvää koneiden ohjauksen turvallisuutta sekä toimitusprojektien laadunvarmistusta.

2.1 Valmet DNA -järjestelmän rakenne

Valmet DNA rakentuu eri tehtäviä suorittavista sovelluspalvelimista ja niitä yhdistävästä verkosta (Valmet [Viitattu 20.8.2018]). Kuvassa 3 esitellään Valmet DNA -verkon rakenne järjestelmän eri osien välillä. Kuvasta käy ilmi myös, kuinka verkko on suojattu palomuurilla.



Kuva 3. Valmet DNA -verkon rakenne. (Valmet [Viitattu 20.8.2018].)

Operointipalvelimet lukeutuvat sovelluspalvelimiin ja operointipalvelimiin. Niiden eri toimintoja ovat prosessin operointi, seuranta ja ohjaus käyttöliittymillä, erilaiset raportointityökalut sekä kenttälaitteiden kunnonvalvontatyökalut. Lisäksi sovelluspalvelimiin lukeutuvat prosessinohjauspalvelimet, jotka sisältävät prosessinohjauksen toteuttavat työkalut, kuten optimoinnit, säädöt, turvalukitukset ja liitynnät. Prosessinohjauspalvelimet hoitavat myös liitynnät kenttälaitteisiin kenttäväylien ja I/O-korttien välityksellä. (Valmet [Viitattu 20.8.2018].)

Suunnittelupalvelimella sijaitsevat sovellusohjelmien luontityökalut, lisäksi siellä on suunnittelutietokanta, josta löytyvät prosessinohjauksen sovellukset sekä järjestelmän toiminnan ja rakenteen määrittävät tiedostot. Prosessi- ja hälytystiedot tallennetaan informaatiopalvelimelle, josta ne kerätään trendeihin, raportteihin, valvomon analysointityökaluihin sekä toimistoverkon laitteille. (Valmet [Viitattu 20.8.2018].)

Kenttälaitteiden hallintapalvelin kerää sekä varastoi tietoa, joka liittyy kenttälaitteiden kunnossapitoon ja toimittaa tiedot toimistoverkon sekä valvomon laitteille (Valmet [Viitattu 20.8.2018]).

Verkon turva-alueelle eli DMZ (Demilitarized Zone) -alueelle sijoitetaan palvelimet, joista toimitetaan tietoa Valmet DNA -prosessinohjausjärjestelmän ulkopuolelle (Valmet [Viitattu 20.8.2018]).

Valmet DNA -sovelluspalvelimina esimerkiksi prosessiohjaimina tai operointipalvelimina toimivat ACN (Valmet Application and Control Node) -yksiköt. Operointipalvelimet voivat olla myös langattomia kannettavia laitteita, esimerkiksi älypuhelimia, tabletteja tai kentälle kiinteästi asennettuja paikallisia operointipalvelimia. I/O-yksiköt voivat olla keskitettyjä automaatiotilaan sijoitettavia tai uudenmallisia kentälle hajautettuja yksiköitä, jotka voidaan myös sijoittaa automaatiotilaan keskitetysti. (Valmet [Viitattu 20.8.2018].)

2.2 Valmet DNA -järjestelmän vikasietoisuus

Tässä luvussa käsitellään Valmet DNA -järjestelmän vikasietoisuutta aluksi rakenteen osalta. Seuraavaksi syvennytään diagnostiikkaan, jonka avulla voidaan havaita nopeammin järjestelmän sisäisiä ongelmia. Luvussa käydään läpi Valmet DNA -verkon rakennetta ja laitteiden oikeaoppista kytkemistä verkkoon. Luvussa käsitellään myös toimitusprojektien laadunvarmistusta.

2.2.1 Valmet DNA -rakenne

Järjestelmän palvelimet ja verkkorakenteet sekä valvomo- ja prosessiväylät voidaan kahdentaa niin että yksittäinen laite- taikka kaapelivika taikka irtoaminen eivät aiheuta häiriötä prosessissa (Valmet [Viitattu 21.8.2018]).

Valmet DNA -järjestelmässä on erillinen varmennusasema, jolta järjestelmän palvelimet lataavat tarvitsemansa ohjelmistot mahdollisten vikatilanteiden, esimerkiksi laiterikkojen jälkeen (Valmet [Viitattu 21.8.2018]).

DNA-kaapeissa on akut, jotka toimivat 30 minuuttia ulkoisen jännitteen katkettua tai tehonsyöttö on varmennettu erillisellä UPS (Uninterruptible Power Supply) -laitteistolla (Valmet [Viitattu 21.8.2018]).

Valmet DNA -prosessinohjausverkon ulkopuolelle siirrettäessä tietoa, käytetään verkon turva-aluetta (DMZ alue (demilitarized zone)), koska tämä on tietoturvan kannalta turvallisin tapa. Näin estetään viruksien tulo järjestelmään. (Valmet [Viitattu 21.8.2018].)

Hima-laitteilla tehdään turvaluokitellut suojaukset sekä ohjaukset (Valmet [Viitattu 21.8.2018]). Hima on HIMA Paul Hildebrandt Gmbh -yrityksen valmistama turva-automaatiojärjestelmä.

Kaikille eri sovelluksille on yksi ja sama järjestelmä, joka vähentää järjestelmien välisiä rajapintoja, ja vähentää yhteensopivuusongelmia (koneohjaukset on liitetty muuhun prosessinohjaukseen) (Valmet [Viitattu 21.8.2018]).

2.2.2 Diagnostiikka

Diagnostiikka on sisäänrakennettuna Valmet DNA -järjestelmässä, jotta järjestelmän sisäiset ongelmat huomataan helpommin sekä nopeammin ja diagnostiikan avulla on helpompi selvittää vikoja (Valmet [Viitattu 22.8.2018]).

I/O- ja kenttäväylät sisältävät itsediagnostiikan ja hälyttävät vioista, jotta viat huomattaisiin mahdollisimman nopeasti, ja ne päästäisiin korjaamaan mahdollisimman nopeasti. On myös tärkeää tietää, millaisesta viasta on kyse, ja korjaustoimenpiteet voidaan suunnata oikealle alueelle järjestelmässä. (Valmet [Viitattu 22.8.2018].)

PLC-, sarja- ja Ethernet-liitännöille voidaan tehdä diagnostiikkaa, jotta voidaan tunnistaa liitettyjen laitteiden vikatilanteita. Nämä diagnostiikat tehdään tapauskohtaisesti kussakin toimitusprojektissa liitettävistä laitteista riippuen. (Valmet [Viitattu 22.8.2018].)

DNA-hälytysnäytöllä näkyvät Ethernet-laitteiden viat, tämä nopeuttaa toimenpiteisiin ryhtymistä, koska viat havaitaan ajoissa (Valmet [Viitattu 22.8.2018]).

Verkkokytkimissä on SNMP-protokollat (Simple Network Management Protocol), jolla valvotaan kytkimien toimintaa. Web Diagnostic -ohjelmalla pystytään tutkimaan yksityiskohtaisemmin näitä vikoja. (Valmet [Viitattu 22.8.2018].)

Diagnostiikka on sisäänrakennettuna järjestelmässä, jotta järjestelmän sisäiset ongelmat huomataan helpommin sekä nopeammin, diagnostiikan avulla on helpompi selvittää vikoja (Valmet [Viitattu 22.8.2018]).

Diagnostiikka-anturit valvovat järjestelmän tilaa sekä aiheuttavat hälytyksen, jos siihen on tarve (Valmet [Viitattu 22.8.2018]).

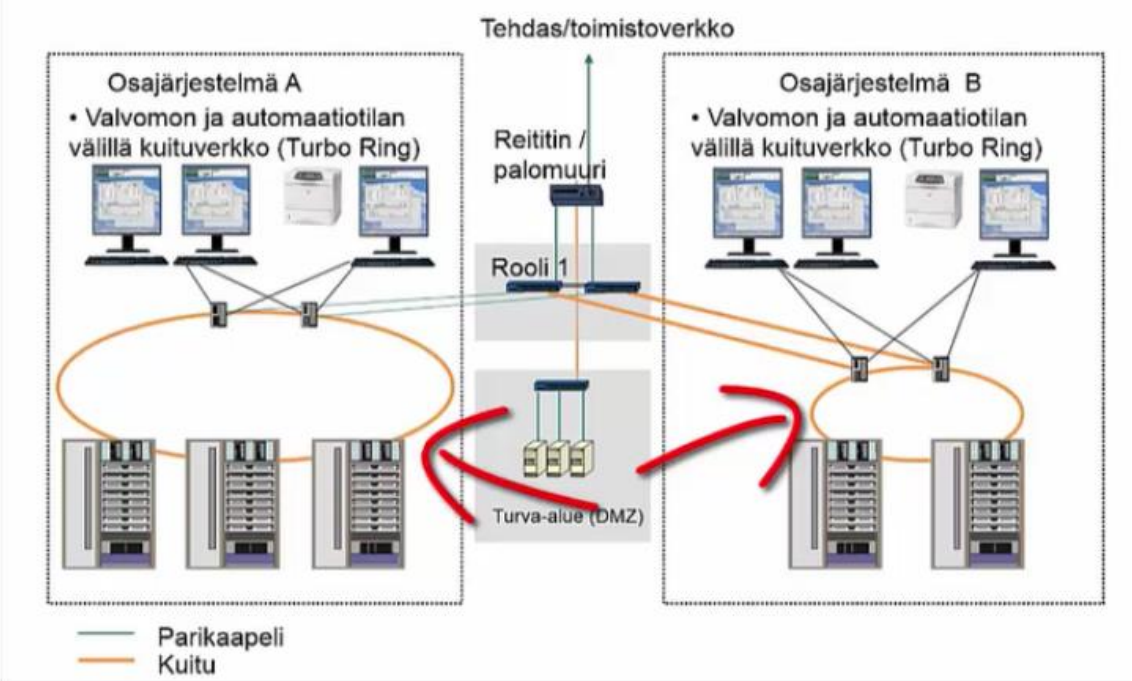
2.2.3 Valmet DNA -I/O-korttien turvatoiminnot

I/O-korteissa on turvatila-toiminto, jossa niille voidaan määritellä, mihin tilaan kortti asettuu häiriötilanteessa. Tällainen häiriötila voi olla esimerkiksi kaapeli- tai

laitevika, joka katkaisee kortin yhteyden prosessinohjaimeen. Binääri- ja analogialähtökorttien lähdöt voidaan jäädyttää ennen häiriötä olleeseen tilaan tai määritellä ohjautumaan ohjattavan laitteen turvallisen tilan mukaiseen uuteen ohjausarvoon. (Valmet [Viitattu 23.8.2018].)

2.2.4 Valmet DNA -verkko

Valmet DNA -verkko on kahdennettu ja hyvin vikasietoinen, mutta kytkimen tai reitittimen vikaantuessa ja laitetta vaihtaessa varaosaan tulee varakytkimelle siirtää ensin oikea konfiguraatio ja vasta tämän jälkeen laite kytketään verkkoon. Konfiguroimatonta laitetta ei saa koskaan kytkeä Valmet DNA -verkkoon, koska siellä ovat kahdennusasetukset ja verkkoon voi tulla silmukka ilman niitä ja se lakkaa toimimasta ylikuormituksen vuoksi. Poikkeuksena edellä mainittuun ovat vanhanmalliset Valmet ACN -kaappikytkimet, jotka eivät tarvitse konfigurointia. (Valmet [Viitattu 24.8.2018].) Kuvassa 4 esitetään Valmet DNA -verkon kahdennusperiaate.



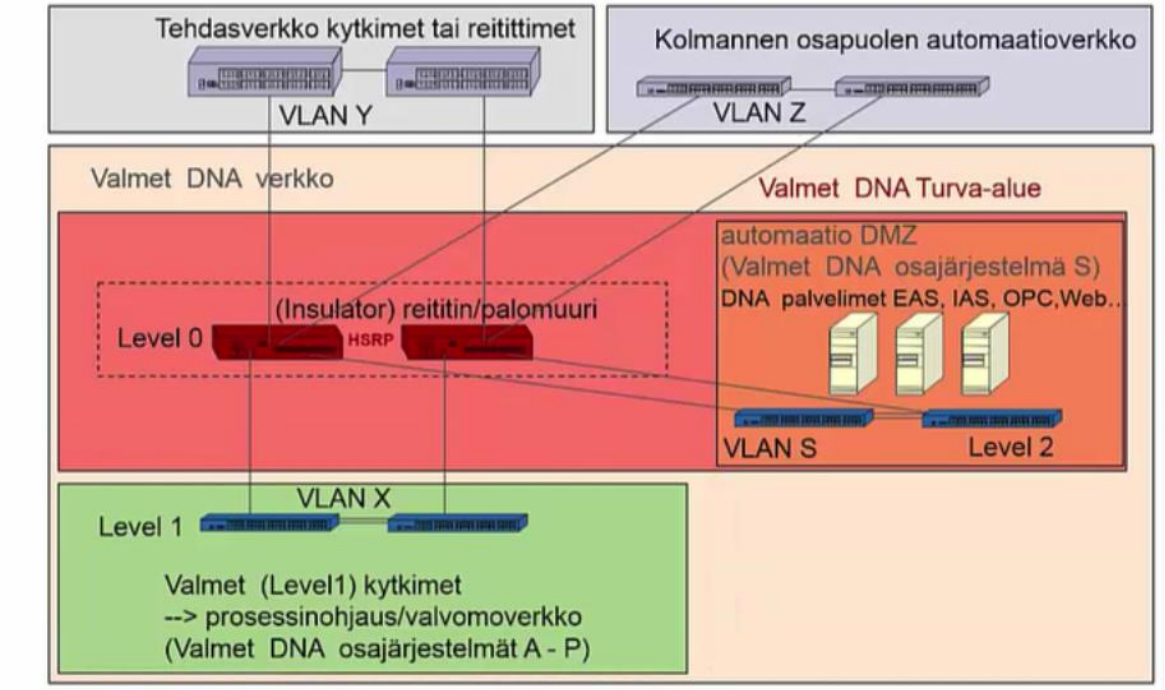
Kuva 4. Valmet DNA -verkon kahdennus. (Valmet [Viitattu 24.8.2018].)

2.2.5 DMZ

DMZ-alueella eli turva-alueella on käytössä Valmet DNA -liikennöintiprotokolla, joka ei ole yleisesti tunnettu ja tämän ansiosta ei luo tietoturvariskiä. Virukset ja hakkerit eivät osaa käyttää sitä hyväkseen yhtä helposti kuin muita yleisemmin tunnettuja protokollia. (Valmet [Viitattu 25.8.2018].)

Reitittimellä hallitaan kaikkea Valmet DNA -järjestelmään liittyvää verkkoliikennettä eri verkkojen välillä. Konfiguroitaessa reititinpalomuuria määritellään yksityiskohtaisesti, mitkä eri työasemat, palvelimet, portit sekä protokollat voivat liikennöidä mihinkin suuntaan. Mikäli prosessidataa, esimerkiksi tehtaan käynnin osalta kriittisiin ohjausjärjestelmiin, kulkee reititinpalomuurin läpi, tulee reititin/palomuuri kahdentaa. (Valmet [Viitattu 25.8.2018].)

Suorat yhteydet ulkomaailmasta prosessinohjausverkkoon pystytään estämään DMZ-aluetta käyttämällä ja tällä tavalla saadaan nostettua tietoturvatasoa (Valmet [Viitattu 25.8.2018]). Kuvassa 5 esitetään Valmet DNA -verkon DMZ-periaate.



Kuva 5. DMZ-alue verkon rakenteessa. (Valmet [Viitattu 25.8.2018].)

2.2.6 Tietoturva Valmet DNA -järjestelmässä

Tietoturvan kannalta automaatioverkon suojaus on erittäin tärkeää, koska aktivistit, rikolliset ja muut yritysten tietoja tahtovat yrittävät tunkeutua ympäri maailman suurenevissa määrin teollisuusyritysten verkkoihin.

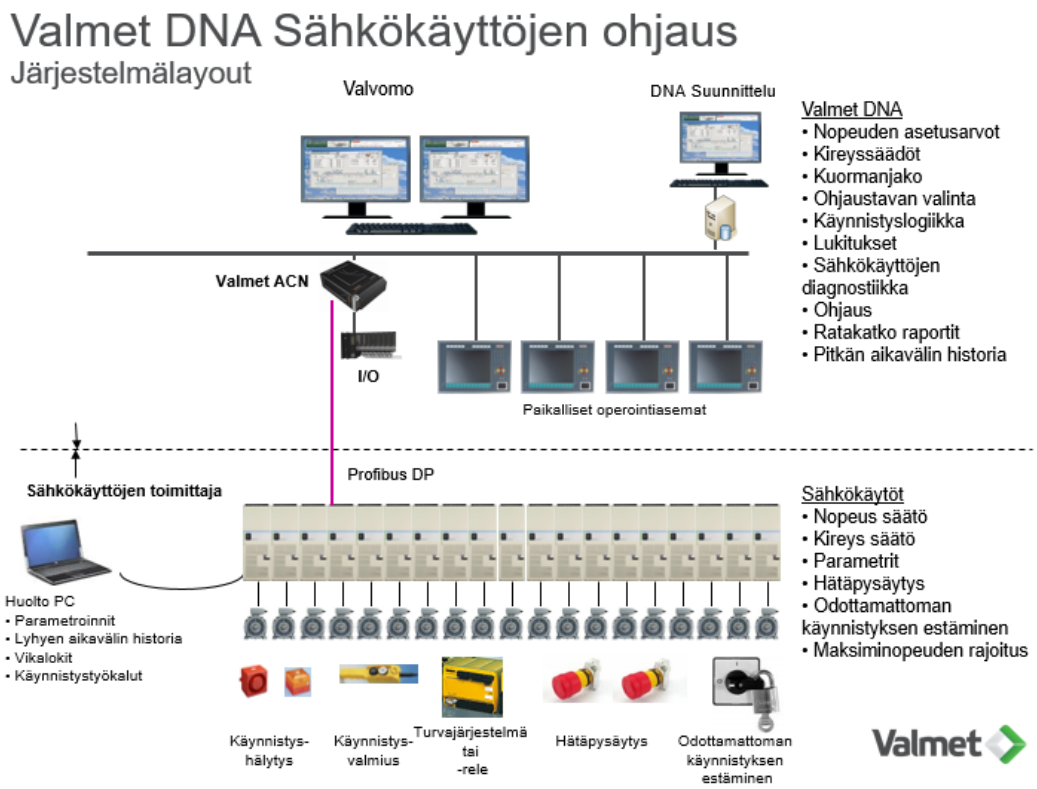
DNA-järjestelmä on suojattu kerroksittaisella suojauksella, jossa ensimmäinen suojaustapa on reitittimessä oleva palomuuri, jonka pääsylistoille on määritelty yksityiskohtaisesti kaikki IP-osoitteet, portit sekä protokollat, jotka saavat liikennöidä minkäkin verkon osan kanssa. Kaikki muu verkkoliikenne on estetty. Tämän vuoksi kaikki automaatioverkon ulkopuoliset verkot tulee kytkeä reititin/palomuurin kautta järjestelmään. Etäyhteyksien kanssa käytetään raskasta tunnistautumista, jotta kukaan ulkopuolinen ei pääse verkkoon käsiksi. Isommat DNA-verkot voidaan jakaa osa-alueisiin vianhaun, käytettävyyden sekä tietoturvan parantamiseksi. Tunkeutumisenestolaitteita ja -ohjelmistoja voidaan käyttää suojaamaan verkkoa. Järjestelmän kaikista Windows-koneista on poistettu DNA-käytössä turhat ohjelmat, prosessit sekä toiminnot eli koneet ovat hardenoitu. Kaikilla verkkolaitteilla ja tietokoneilla vaaditaan salasana, jotta ulkopuoliset henkilöt eivät pääse niihin käsiksi. Windows-koneiden tietoturvapäivitykset täytyy pitää ajan tasalla. DNA-järjestelmän kanssa työskenteleville on tärkeä tiedottaa tietoturvaan liittyvät menettelyt, esimerkiksi samoja kannettavia laitteita, esimerkiksi USB-tallennusvälineitä, ei käytetä muissa verkoissa automaatioverkon lisäksi. (Valmet [Viitattu 26.8.2018].)

2.3 Valmet DNA ja koneiden ohjauksen turvallisuus

Koneilla työskenneltäessä täytyy turvallisuus varmistaa tekemällä koneet virrattomiksi, estämällä käynnistys hätäseiskytkimillä valvomossa ja kentällä, lukituslaitteilla ohjauskytkimissä ja moottorikeskuksissa sekä turvalogiikoilla (Valmet [Viitattu 27.8.2018]).

Käytönaikaiset turvallisuusriskit kartoitetaan HAZOP-riskiarvioissa, ja riskien poislukitsemiseksi tehdään tarvittavat suojaukset turvalogiikoilla. Vastaavat lukituslogiikat toteutetaan yleensä myöskin Valmet DNA -sovellusohjelmilla, vaikka ne eivät olekaan varsinaisia turvaluokiteltuja toimintoja. (Valmet [Viitattu 27.8.2018].)

FMEA-analyysissä määritellään turvaluokittelemattoman ohjausjärjestelmän, esimerkiksi Valmet DNA -järjestelmän, vika-analyysi ja toimenpiteet mahdollisten väärien ohjausjärjestelmien aiheuttamien ohjausten estämiseksi. Järjestelmätesteillä todennetaan näiden toimenpiteiden oikea toiminta. Mikäli FMEA-analyysissä ilmenee riskejä, joita ei voida estää itse ohjausjärjestelmässä, täytyy ne huomioida turvalogiikan toteutuksessa tai koneen mekaanisessa suojauksessa. (Valmet [Viitattu 27.8.2018].) Kuvassa 6 näkyy, mitä eri turvalaitteita sähkökäyttöihin sisältyy.



Kuva 6. Valmet DNA -sähkökäyttöjen ohjaus ja turvalaitteet. (Valmet [Viitattu 27.8.2018].)

2.4 Valmet Automation -toimitusprojektin laadunvarmistus

VA-tuotekehitys testaa tuotekehitysvaiheessa järjestelmään suunnitellut omien laitteiden sekä järjestelmässä käytettävien muiden toimittajien laitteiden toiminnan sekä erilaisia järjestelmän peruskokoonpanoja. Näissä testeissä varmistetaan, että kehitetyt/valitut laitteet täyttävät niitä koskevan Pienjännitedirektiivin (LVD) 2014/35/EU ja Sähkömagneettista yhteensopivuutta (EMC) koskevan 2014/30/EU-direktiivin tuoteturvallisuusvaatimukset.

Toimitusprojekteihin tulevat laitteet testataan valmistusvaiheessa valmistajan toimesta ennen toimitusta projektille.

Toimitusprojekteissa testataan, että järjestelmäkokonaisuudet toimivat häiriöttömästi ja asetettujen vaatimusten mukaisesti. Tässä työssä perehdytään juuri toimitusprojektien järjestelmäkokonaisuuksien vaatimuksien, kuten toiminnallisen turvallisuuden vaatimuksien mukaisen toiminnan varmistamiseen riittävillä testeillä.

3 KONETURVALLISUUDEN VAATIMIEN TESTIEN KEHITTÄMINEN

Tässä luvussa käydään läpi standardien vaatimukset Valmet DNA -ohjausjärjestelmälle ja suunnitellaan uusia testejä vaatimuksien ja FMEA-analyysin pohjalta. Luvun lopusta löytyy yksi esimerkki, jossa käydään läpi vanha testaustyyli sekä vaatimuksien mukaiset uudet testit kyseiseen asiaan liittyen.

3.1 Standardien vaatimukset

Tässä luvussa käydään läpi Konedirektiivin ja siihen liittyvien standardien vaatimuksia, jotka koskevat Valmet DNA -ohjausjärjestelmää ja joiden mukaan suunnitellaan uusia testejä luvussa 3.3.

3.1.1 ´´Konedirektiivi´´ Euroopan parlamentin ja neuvoston direktiivi 2006/42/EY

Ohjausjärjestelmä ei saa aiheuttaa vaaratilanteita ja sen on pyrittävä estämään niiden syntyminen. Vaaratilanteita ovat esimerkiksi koneen ennalta arvaamaton käynnistyminen tai, että käyvää konetta ei saada pysäytettyä. (EY 2006/42, 37.)

Vaaratilanteen aiheuttava järjestelmävika voi olla joko järjestelmälaitteistossa taikka ohjelmistossa (EY 2006/42, 37).

Mahdollisen laitteistovian poissulkemiseksi järjestelmän komponentit valitaan huolellisesti ja järjestelmätestataan erilaisissa häiriötilanteissa ja ympäristöolosuhteissa ennen niiden hyväksymistä järjestelmän osaksi ja toimitettavaksi projekteissa. Tyypillisiä häiriötilanteita ovat jännitteen päälle- ja poiskytkemiset, sähkömagneettiset häiriöt (EMC), laiteviat ja syövyttävistä aineista aiheutuvat komponenttien vaurioitumiset ja virhetoiminnot. (EY 2006/42, 37.)

Ohjelmistovirheet voivat aiheutua virheestä järjestelmän perusohjelmistossa tai projektikohtaisessa sovellusohjelmistossa (EY 2006/42, 37). Perusohjelmiston mahdolliset viat pyritään löytämään ja poistamaan tuotekehitysvaiheessa ennen

ohjelmistoversion toimittamista projekteille. Projektikohtaisen sovelluksen virheet pyritään löytämään ja poistamaan VA:n omassa FAT-testauksessa ja tämän jälkeen asiakkaan kanssa tehtävässä FAT testauksessa.

Turvalaitteiden tulee pysyä toimintakykyisinä tai niiden tulee antaa pysäytyskäsky, mikäli ohjausjärjestelmä lakkaa toimimasta. Tästä johtuen koneen ohjauspiirit tulee toteuttaa niin, että turvalaitteiden ohjaus toimii ohjausjärjestelmän toimimattomuudesta riippumatta ja estää ohjausjärjestelmästä tulevat ristiriitaiset ohjaukset koneelle. Pysäytyskäskyn täytyy kuitenkin mennä aina perille riippumatta siitä, mistä järjestelmästä se on annettu. Mikäli pysäytyskäsky on jo annettu, ei pysähtymistä saa estää. Mikäli ei saada oikeita ohjaussignaaleja taikka yhteys menetetään langattomassa ohjauksessa, tulee tällöin aikaansaada automaattinen pysäytys. (EY 2006/42, 38.)

Mikäli koneessa on useampia käynnistysohjaimia ja käyttäjät voivat aiheuttaa toisilleen vaaratilanteen, tulee tällaisissa tilanteissa asentaa lisälaitteita ja toteuttaa järjestelmä niin, että koko järjestelmää tai sen osaa ei pysty ohjaamaan kuin yksi käyttäjä kerrallaan (EY 2006/42, 39).

Koneessa tulee olla ohjauslaite, jolla koko kone pystytään pysäyttämään (EY 2006/42, 39).

Jokaisella työasemalla tulee myös olla ohjauslaitteet, joilla pystytään pysäyttämään vain osa koneen toiminnoista tai kaikki toiminnot niin, että kone saadaan turvalliseen tilaan (EY 2006/42, 39).

Pysäytyslaitteiden tulee toimia ensisijaisesti käynnistyslaitteisiin nähden, jotta vältytään vaarantamasta koneen luona työskenteleviä (EY 2006/42, 39).

Koneen tai sen vaarallisten toimintojen pysähdyttyä, tulee energiansyöttö katketa asianomaisiin toimilaitteisiin (EY 2006/42, 39).

3.1.2 SFS-EN ISO 12100:2010 (Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen)

Vaaratilanne voi syntyä, mikäli ohjausjärjestelmän logiikan rakenne on huonosti suunniteltu tai siihen on tehty harkitsematon muutos. Ohjelmistovirheen lisäksi vaaratilanteen voi aiheuttaa ohjausjärjestelmän laitevika, ongelmat tehonsyötössä tai tahallinen turvalaitteiden toiminnan estäminen. (SFS-EN ISO 12100 2010, 38.)

3.1.3 SFS-IEC 62443 (Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus.)

Oleellinen asia turvallisen ohjauksen varmistamisessa on huolehtia, että toteutuksen yksityiskohtaiset tiedot eivät joudu ulkopuolisten haltuun, ja että toteutettuun järjestelmään ei ole ulkopuolisilta pääsyä. Tietoturva varmistetaan salasanakäytännöillä, tietoverkkojen palomuureilla, työasemien ja palvelimien hardenoinneilla (tarpeettomat ohjelmat poistetaan ja käyttöoikeuksia rajoitetaan vain tarpeellisiin ohjelmiin), virustorjunnalla ja käyttöjärjestelmäohjelmistojen päivityksillä. Lisäksi laitteet tulee sijoittaa niin, että niiden luokse pääsevät vain asianomaiset henkilöt. Edellä mainittujen asioiden vaatimuksia ja käytännön toteutusta on ohjeistettu standardissa IEC 62443 (Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus). (SFS-IEC 62443 2013.)

3.1.4 SFS-EN ISO 14118:2018 (Koneturvallisuus. Odottamattoman käynnistymisen estäminen)

Valvontajärjestelmän häiriö ei saa aiheuttaa koneen käynnistyskomentoa (SFS-EN ISO 14118 2018, 7). Standardi ei määritä valvontajärjestelmän suorituskyvyn tasoja tai turvallisuuden eheystasoja järjestelmien turvallisuuteen liittyvissä osissa. Standardi ei myöskään määrittele käytettäviä keinoja odottamattoman käynnistyksen estämiseksi. Jos näiden määrittelyä ei voida tehdä muiden liittyvien standardien avulla niin määrittely tehdään vika- ja vaikutusanlyysin (FMEA) avulla.

3.1.5 SFS-EN 60204-1 (Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset)

SFS-EN 60204-1 -standardi asettaa lähinnä sähkömekaanisia rakennevaatimuksia sille Valmet DNA -järjestelmän osalle, joka on kytketty suoraan ohjattavaan koneeseen. Näiden vaatimusten mukaiset ratkaisut on määritelty Valmetin erillisessä suunnitteluohjeessa.

3.2 FMEA (Vika- ja vaikutusanalyysi)

Vika- ja vaikutusanalyysi on systemaattinen järjestely, jossa tunnistetaan mahdollisia vikoja, niiden syitä ja seurauksia järjestelmän toiminnassa (SFS-EN 60812 2006, 15). Valmet DNA -järjestelmässä tämä tarkoittaa laitteistoa ja ohjelmistoa. Tässä työssä Örsted-biokattilatoimitukseen kehitetty Valmet DNA -järjestelmän FMEA on liitteessä 1 FMEA-analyysin Test-sarakkeessa on määritelty, millä järjestelmätestausohjeen (liite 2) testillä voidaan varmistaa, että kyseinen vika ei aiheuta turvallisuusriskiä. Tätä FMEA-analyysiä voidaan käyttää mallina muissa Valmet DNA -toimitusprojekteissa. Kunkin projektin sisällönmukainen tarkka analyysi tehdään projektin alussa määrittelyvaiheessa, jotta viat voitaisiin ottaa huomioon järjestelmän suunnittelussa ja valmistuksessa, eikä tarvittaisi kalliita muutoksia jo valmistettuun järjestelmään.

Vika- ja vaikutusanalyysiä täytyy kuitenkin tarkastella myöskin järjestelmän toteutusvaiheessa, jotta pystytään huomioimaan mahdollisesti vasta silloin esille tulleet vikamahdollisuudet (SFS-EN 60812 2006, 15).

Valmet DNA -järjestelmän FMEA-analyysillä halutaan löytää mahdollisia järjestelmän toimintaa haittaavia vikoja etenkin, jos viat saattavat aiheuttaa vaaratilanteita koneiden käyttäjien turvallisuudelle. Usein asiakkaat vaativat FMEA-tarkastelun jo toimitussopimuksessakin, jotta pystyvät huolehtimaan työntekijöidensä turvallisuudesta.

Usein FMEA-analyysin toteuttamisessa ja esittämisessä on ollut vaihtelua tekijöistä riippuen. Suositeltava tapa on esittää mahdolliset vikatilat, niiden syyt ja vaikutukset

sekä keinot niiden ehkäisemiseen taulukossa, joka sisältää tuvallisuuteen vaikuttavat järjestelmän toiminnot ja laitteet. (SFS-EN 60812 2006, 19.)

Valmet DNA -järjestelmän FMEA-taulukko sisältää järjestelmän eri osat ja niiden toiminnot, järjestelmäväylät, järjestelmän kahdennukset sekä tulot ja lähdöt. Taulukossa kuvataan näiden todennäköisimmät vikatilanteet ja niiden yksityiskohtaiset syyt.

Eri vikatiloille määritellään tapa, kuinka vika havaitaan järjestelmän diagnostiikalla ja kuinka vika esitetään järjestelmän hälytysnäytössä, tai mahdollisesti tarvittavat testausmenettelyt vian havaitsemiseksi esimerkiksi järjestelmän toimitus- tai käyttöönottovaiheessa.

Erillisten järjestelmäkomponenttien lisäksi tulee tarkastella myös mahdollinen yhteismuotoinen vikatila, joka voi aiheuttaa useamman järjestelmäkomponentin samanaikaisen vikatilanteen (SFS-EN 60812 2006, 33).

Tässä työssä keskitytään itse järjestelmän vikatilanteisiin, koska käyttäjien inhimillisiltä virheiltä suojaavat lukitukset ja ohjaukset toteutetaan sovellusohjelmissa asiakkaalta saatujen lähtötietojen mukaisesti.

Vikatilanteet, joita ei voida poistaa itse ohjausjärjestelmässä (jäännösriski), tulee huomioida turvajärjestelmän ja turvalaitteiden suunnittelussa (SFS-EN 60812 2006, 61).

3.3 Opinnäytetyössä tunnistetut ja suunnitellut koneturvallisuuteen liittyvät Valmet DNA -järjestelmätestit

Tässä työssä kehitetty Valmet DNA -järjestelmän systemaattinen perustestaus auttaa pääosin jo varmistamaan, että järjestelmä toimii luotettavasti eikä aiheuta ohjattavan koneen vaaratilanteita.

Seuraavissa luvuissa on kuvattu konedirektiivin ja siihen liittyvien standardien vaatimuksenmukaisuuden todentamiseksi tarvittavia lisätestejä.

3.3.1 ´´Konedirektiivi´´ Euroopan parlamentin ja neuvoston direktiivi 2006/42/EY

Tässä luvussa käydään läpi Euroopan parlamentin ja neuvoston direktiivin 2006/42/EY vaatimusten pohjalta suunnitellut uudet Valmet DNA -ohjausjärjestelmätestit. Luetelmassa on kuvattu uudet Valmet DNA -järjestelmätestit ja ne on sisällytetty päivitettyyn Valmet Automationin sisäiseen järjestelmätestausohjeeseen.

- Testauksen aikana tulee seurata, että kone ei käynnisty ilman käynnistyskäskyä.
- Koneen pysäytyksien toimivuus tulee testata.
- Jännitteen päälle- ja poiskytkemisen toimivuuden testaus.
- Ohjausjärjestelmän lakatessa toimimasta tulee turvalaitteiden pysyä toimintakykyisinä tai niiden tulee antaa pysäytyskäsky.
- Käynnistyskäskyt tulee testata niin, että niitä ei voi antaa kuin yksi henkilö kerrallaan. Tämä tulee huomioida, mikäli ohjaus on mahdollinen suorittaa useammasta valvomosta.
- Koko koneen pysäyttävä laite ja työasemakohtaiset pysäytyslaitteet, joilla pysäytetään vain osa toiminnoista, tulee testata.
- Mikäli järjestelmä sisältää useamman kuin yhden valvomon, josta konetta voidaan ohjata, tulee testata, että operointioikeus on vain sen valvomon operointipäätteeltä, joka kussakin tilanteessa on oikeutettu operoimaan.

3.3.2 SFS-EN ISO 12100:2010 (Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen)

Tässä luvussa käydään läpi SFS-EN ISO 12100:2010 -standardin vaatimusten pohjalta suunniteltu uusi Valmet DNA -ohjausjärjestelmätesti. Luetelmassa on

kuvattu uusi Valmet DNA -järjestelmätesti ja se on sisällytetty päivitettyyn Valmet Automationin sisäiseen järjestelmätestausohjeeseen.

- Ohjausjärjestelmän logiikan rakenteen oikeanlainen suunnittelu ja harkitsemattomien muutosten testaus toteutetaan laittamalla esimerkiksi moottorilähtö päälle ohjelmasta ja seuraamalla, että testeissä ei käynnisty muita moottoreita. Testausta tulee jatkaa niin, että käynnissä oleva moottori pystytään pysäyttämään eri vikatilanteissa Valmet DNA -järjestelmän ohjauspäätteeltä.

3.3.3 SFS-IEC 62443 (Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus)

Tässä luvussa käydään läpi SFS-IEC 62443 -standardin vaatimusten pohjalta suunnitellut uudet Valmet DNA -ohjausjärjestelmätestit. Luetelmassa on kuvattu uudet Valmet DNA -järjestelmätestit ja ne on sisällytetty päivitettyyn Valmet Automationin sisäiseen järjestelmätestausohjeeseen.

- Tietoturva-asiat tulee varmistaa testaamalla salasanakäytännöt ja katsomalla, että vain asianomaiset tahot pääsevät käsiksi heille tarkoitettuihin tietoihin ja toimintoihin järjestelmässä.

- Tietoverkkojen palomuurit ja virustorjunta tulee tarkistaa sekä testata niiden toimivuus.

- Järjestelmästä tulee tarkistaa, että siellä on vain tarpeelliset ohjelmat ja tarpeettomat ohjelmat poistetaan tarvittaessa.

- Käyttöjärjestelmäohjelmistojen ajantasaisuus päivityksien osalta tulee tarkistaa ja päivittää ne tarvittaessa uudempiin.

3.3.4 SFS-EN 60204-1 (Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset)

Tässä luvussa käydään läpi SFS-EN 60204-1 -standardin vaatimusten pohjalta suunniteltu uusi Valmet DNA -ohjausjärjestelmätesti. Luetelmassa on kuvattu uusi Valmet DNA -järjestelmätesti ja se on sisällytetty päivitettyyn Valmet Automationin sisäiseen järjestelmätestausohjeeseen.

- Testauksen ajan tulee tarkastella, että ohjausjärjestelmän häiriöt eivät aiheuta koneelle käynnistyskomentoja. Aiheeton käynnistyskomento voi olla seurausta virheestä ohjausjärjestelmässä.

3.4 Esimerkki opinnäytetyössä kehitellystä Konedirektiivin/standardien vaatimasta lisätestistä Valmet DNA -ohjausjärjestelmälle

Seuraavaksi käydään läpi yksi esimerkki opinnäytetyön tuloksesta ohjausjärjestelmätestaukseen.

Liitteen 2 kohdassa 5.1.24 (I/O-cabinet Power Supply Redundancy Testing) on aikaisemmin järjestelmätestissä testattu tilannetta, jossa vuoron perään käännetään toinen päävirtakatkaisijoista off-tilaan, niin mikään muu komponentti tehonsyöttöyksikön lisäksi järjestelmässä ei saa sammua. Opinnäytetyössä tarkasteltiin Konedirektiiviä 2006/42/EY ja tämä direktiivi määrittelee, että kone ei saa käynnistyä ilman käynnistyskäskyä. Vaikka Valmet DNA -ohjausjärjestelmä ei ole kone, mutta se ohjaa konetta ja tästä syystä kone voi käynnistyä virheestä ohjausjärjestelmässä. Tämän vaatimuksen pohjalta työssä määriteltiin uusi testi, jossa tarkastetaan katkaisemalla vuoron perään kumpikin jännitesyötöistä, ettei toisen jännitesyötön katkeaminen aiheuta tahattomia käynnistyksiä ohjausjärjestelmässä. Tämä edellä mainittu testi on sisällytetty Valmetin sisäisen testausohjeen kohtaan 5.1.24, jonka sisällysluettelo on liitteenä 2.

4 YHTEENVETO JA POHDINTA

Lait, asetukset ja etenkin teknologia muuttuvat, minkä vuoksi teknologiayritysten tulee jatkuvasti seurata uusia vaatimuksia ja kehittää niiden pohjalta toimintaansa sekä tuotteitansa. Valmet Automationilla oli tarve ajantasaiselle vaatimusten mukaiselle testausohjeelle toimitusprojekteihin.

4.1 Työn tavoitteet sekä ongelmat

Työn tavoitteena oli kehittää ja päivittää Valmet Automationin prosessinohjausjärjestelmä testausohjetta vastaamaan uudistuneita standardeja. Tämä yhtenäistetty ja päivitetty ohje helpottaa eri toimitusprojektien järjestelmällistä testausta.

Työn ongelmana oli löytää laajasta standardikirjastosta työtä koskevat vaatimukset etenkin, koska turvaluokittelemattoman ohjausjärjestelmän vaatimukset ovat osittain tulkinnanvaraisia. Koska Valmet DNA -ohjausjärjestelmän rakenne voi vaihdella huomattavasti käyttökohteesta riippuen, niin FMEA-analyysissä huomioitavat vikatilanteetkin vaihtelevat toimitusprojektikohtaisesti.

4.2 Työn tulokset

Tässä työssä on kehitetty Valmet DNA -ohjausjärjestelmän testausohje. Testausohjeen sisällysluettelo löytyy liitteestä 2. Tarkka testausohje on rajattu vain Valmet Automationin sisäiseen käyttöön. Näiden uusien testien myötä ohjausjärjestelmän toiminnan luotettavuus saadaan paremmin standardisoitua. Testausohjetta tullaan käyttämään Valmet Automationin tulevissa toimitusprojekteissa.

Vanhoista testausohjeista koottu ensimmäinen yhtenäinen testausohjeen versio tehtiin Inovynin kemiantehtaan sekä Rauma 2 sellutehtaan automaatiojärjestelmien uudistamisprojekteihin. Näistä kehitetty uusi versio lisättynä koneturvallisuuden vaatimilla testeillä otettiin käyttöön Örstedin Biovoimalaitos-projektissa.

4.3 Pohdinta

Työ oli vaikea saada alkuun sekä koota teksti luontevaksi kokonaisuudeksi, mutta hiljalleen asiat alkoivat selkeytymään ja niitä oli helpompi käsitellä. Työn loppua kohden oli huomattavasti helpompi käsittää asioita kokonaisuutena ja niiden vaikutuksia toisiinsa. Opin työn aikana paljon Valmet DNA -ohjausjärjestelmän rakenteesta sekä toiminnasta. Lisäksi työn aikana opin lukemaan sekä tulkitsemaan standardeja paremmin.

Työssä käsiteltiin lähes kaikki alussa määritellyt asiat, mutta muutama aiheeseen liittyvä standardi jätettiin käsittelemättä. Osa standardeista jätettiin käsittelemättä, koska ne eivät liittyneet suoraan turvaluokittelemattomaan ohjausjärjestelmään.

Suuri kiitos Valmet Automationin HSEQ-tiimin jäsenille avusta opinnäytetyön asioiden läpikäynnin tiimoilta. Sain tiimiltä paljon apua ja neuvoja siitä, miten kannattaa tutkimuksessa edetä ja mistä kertoa.

LÄHTEET

EY 2006/42. Euroopan parlamentin ja neuvoston direktiivi koneita koskevasta lainsäädännöstä.

SFS-EN 60204-1. 2006. Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset. Helsinki: Suomen Standardisoimisliitto.

SFS-EN 60812. 2006. Analysis techniques for system reliability. Procedure for failure mode and effects analysis (FMEA). Helsinki: Suomen Standardisoimisliitto.

SFS-EN ISO 12100. 2010. Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen. Helsinki: Suomen Standardisoimisliitto.

SFS-EN ISO 14118. 2018. Koneturvallisuus. Odottamattoman käynnistymisen estäminen. Helsinki: Suomen Standardisoimisliitto.

SFS-IEC 62443. 2013. Teollisuuden tietoliikenneverkot. Verkkojen ja järjestelmien tietoturvallisuus. Helsinki: Suomen Standardisoimisliitto.

Valmet. Ei päiväystä. DNA ja koneiden ohjauksen turvallisuus. [Verkkosivu]. Valmet Automation Oy. [Viitattu 27.8.2018]. Saatavissa: Vain yrityksen sisäisessä käytössä.

Valmet. Ei päiväystä. DNA-järjestelmän rakenne. [Verkkosivu]. Valmet Automation Oy. [Viitattu 20.8.2018]. Saatavissa: Vain yrityksen sisäisessä käytössä.

Valmet. Ei päiväystä. DNA-järjestelmän vikasietoisuus diagnostiikka. [Verkkosivu]. Valmet Automation Oy. [Viitattu 22.8.2018]. Saatavissa: Vain yrityksen sisäisessä käytössä.

Valmet. Ei päiväystä. DNA-järjestelmän vikasietoisuus DMZ. [Verkkosivu]. Valmet Automation Oy. [Viitattu 25.8.2018]. Saatavissa: Vain yrityksen sisäisessä käytössä.

Valmet. Ei päiväystä. DNA-järjestelmän vikasietoisuus I/O-korttien turvatoiminnot. [Verkkosivu]. Valmet Automation Oy. [Viitattu 23.8.2018]. Saatavissa: Vain yrityksen sisäisessä käytössä.

Valmet. Ei päiväystä. DNA-järjestelmän vikasietoisuus rakenteen osalta. [Verkkosivu]. Valmet Automation Oy. [Viitattu 21.8.2018]. Saatavissa: Vain yrityksen sisäisessä käytössä.

Valmet. Ei päiväystä. DNA-järjestelmän vikasietoisuus tietoturvan osalta. [Verkkosivu]. Valmet Automation Oy. [Viitattu 26.8.2018]. Saatavissa: Vain yrityksen sisäisessä käytössä.

Valmet. Ei päiväystä. DNA-järjestelmän vikasietoisuus verkon osalta. [Verkkosivu]. Valmet Automation Oy. [Viitattu 24.8.2018]. Saatavissa: Vain yrityksen sisäisessä käytössä.

Valmet. Ei päiväystä. Historia. [Verkkosivu]. Valmet Oyj. [Viitattu 21.6.2018]. Saatavissa: https://www.valmet.com/fi/valmet-yrityksena/valmet-lyhyesti/historia/

Valmet. Ei päiväystä. Valmet Automation. [Verkkosivu]. Valmet Automation Oy. [Viitattu 22.6.2018]. Saatavissa: Vain yrityksen sisäisessä käytössä.

Valmet. Ei päiväystä. Valmet lyhyesti. [Verkkosivu]. Valmet Oyj. [Viitattu 20.6.2018]. Saatavissa: https://www.valmet.com/fi/valmet-yrityksena/valmet-lyhyesti/

LIITTEET

Liite 1. Ote Örsted biokattilalaitoksen Valmet DNA FMEA-analyysistä

Liite 2. Valmet DNA-järjestelmätestausohjeen sisällysluettelo

Liite 1. Ote Örsted biokattilalaitoksen Valmet DNA FMEA-analyysistä

Feature or Function	Failure Mode	Effect or Hazard	How is the operator made aware	Diagnostic or corrective measures	Action Required	Test	Action No.
Hardware							
Operator Workstation – DNA Operate	Processor fails	Stops the update of process information onto screens. Stops operator interaction with the plant.	Screen goes blank or possibly a blue screen appears. Alarm generated.	Call maintenance to repair. Continue to operate plant with another operator workstation.		5.1.4 Valmet DNA Node Tests 5.1.7 Ethernet Network Testing	
	Internal power supply fails. (supply is derived from a UPS)	Stops the update of process information onto screens. Stops operator interaction with the plant.	Blank screens. Alarm generated.	Call maintenance to repair. Continue to operate plant with another operator workstation.		5.1.4 Valmet DNA Node Tests 5.1.7 Ethernet Network Testing	
	Loss of power (UPS) in control room and recovery from Power Failure	Stops the update of process information onto screens. Stops operator interaction with the plant.	Blank screens.	Call maintenance to repair. Operation possible after few seconds when power comes back.	Operator workstations should have a separate power supply.	5.1.4 Valmet DNA Node Tests 5.1.7 Ethernet Network Testing	
	One network connection lost (Failed network component or connection cable)	No effect. Redundant system network.	An alarm is generated.	Call maintenance to repair.		5.1.4 Valmet DNA Node Tests 5.1.7 Ethernet Network Testing	
	Network connection lost (Failed network component(s) or connection cables)	Stops the update of process information onto screens. Stops operator interaction with the plant.	An alarm is generated. All dynamic data in open displays to fault color (purple).	Call maintenance to repair. Continue to operate plant with another operator workstation.		5.1.4 Valmet DNA Node Tests 5.1.7 Ethernet Network Testing	
	Keyboard failure	No commands from keyboard. (Keyboard is used only infrequently)	No commands from keyboard.	Call maintenance to repair / replace. Use another workstation if keyboard is needed.		5.1.4 Valmet DNA Node Tests	
	Mouse failure	Unable to operate plant from workstation with failed mouse.	Mouse not working.	Call maintenance to repair / replace. Continue to operate plant with another operator workstation.		5.1.4 Valmet DNA Node Tests	

Osa FMEA analyysistä Örsted biokattilalaitoksen Valmet DNA-järjestelmälle sivu 1. (Valmetin sisäiset tiedostot)

Feature or Function	Failure Mode	Effect or Hazard	How is the operator made aware	Diagnostic or corrective measures	Action Required	Test	Action No.
	LCD screen failure	Faulty screen blank. The second screen still in use.	Blank screen	Call maintenance to repair / replace. Continue to operate with the 2nd screen.		5.1.4 Valmet DNA Node Tests	
	Failure of graphics card	Blank screens.	Blank screens.	Call maintenance to repair. Continue to operate plant with another operator workstation.		5.1.4 Valmet DNA Node Tests	
Alarm station (included in Operator Workstations)	Processor fails	No effect. Alarm station is redundant.	Alarm generated.	Call maintenance to repair.		5.1.8 Valmet DNA Redundancy Check	
	Internal power supply fails. (supply is derived from a UPS)	No effect. Alarm station is redundant.	Alarm generated.	Call maintenance to repair.		5.1.8 Valmet DNA Redundancy Check	
	Failure of speaker or its associated sound card	No effect. Redundant set of speakers.	No sound from one set of speakers.	Call maintenance to repair / replace.		5.1.8 Valmet DNA Redundancy Check	
	Alarms from different speakers could be slightly out of sync. and not be accepted at the same time	Irritation to the operators				5.1.16 Master Clock Definition Check 5.1.13 Alarm Horns and Alarm History Test	
Control room extender	Extender failure, power loss or cable connection broken / disconnected	Possible effects: Blank screens, mouse not working, keyboard not working.	Blank screens.	Call maintenance to repair. Continue to operate plant with another operator workstation.	Extenders should have separate power supply like operator workstations.	5.1.27 System, Network and Media Converter Cabinet Power Supply Checking	

Osa FMEA analyysistä Örsted biokattilalaitoksen Valmet DNA-järjestelmälle sivu 2. (Valmetin sisäiset tiedostot)

Liite 2. Valmet DNA-järjestelmätestausohjeen sisällysluettelo

Table of Contents

DNA-järjestelmätestaus Valmet DNA-ohjausjärjestelmälle sivu 1. (Valmetin sisäiset tiedostot)

DNA-järjestelmätestaus Valmet DNA-ohjausjärjestelmälle sivu 2. (Valmetin sisäiset tiedostot)

DNA-järjestelmätestaus Valmet DNA-ohjausjärjestelmälle sivu 3. (Valmetin sisäiset tiedostot)