



TAMPEREEN TEKNILLINEN YLIOPISTO

JANI KRISTIAN VÄHÄPESOLA
OHJAUSJÄRJESTELMÄN TURVATOIMINTOJEN TOTEUTUS JA
ANALYSOINTI ERÄÄSSÄ VARASTOJÄRJESTELMÄSSÄ
Diplomityö

Tarkastaja: Karri Palovuori
Tarkastaja ja aihe hyväksytty tieto- ja
sähkötekniikan tiedekuntaneuvoston
kokouksessa 07.03.2012

TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO

Tietotekniikan koulutusohjelma

JANI KRISTIAN VÄHÄPESOLA : OHJAUSJÄRJESTELMÄN TURVATOIMINTOJEN TOTEUTUS JA ANALYSOINTI ERÄÄSSÄ VARASTOJÄRJESTELMÄSSÄ

Diplomityö, 66 sivua, 14 liitesivua

Syyskuu 2012

Pääaine: Sulautetut järjestelmät

Tarkastajat: Karri Palovuori

Avainsanat: Konedirektiivi 2006/42/EY, SFS-EN ISO 13849, turvatoiminto, ylinopeusvahti, varastojärjestelmä, kelpuus

Konevalmistajien on noudatettava Euroopan sisämarkkinoille tuotavien koneiden suunnittelussa ja valmistuksessa konedirektiiviä 2006/42/EY. Tämän diplomityön tarkoituksena oli osaltaan täyttää direktiivin asettamia vaatimuksia eräälle varastojärjestelmälle. Työssä tutkittiin yhtä turvallisuusnäkökohtaa, varaston sisällä liikkuvan sukkulan ylinopeutta. Turvallisuusvaatimusten täytyminen osoitetaan lopulta koneeseen kiinnitettävällä CE-merkinnällä.

Lähtökohtana olivat varastojärjestelmälle tehty riskianalyysi sekä vaatimusmäärittely joiden sisältöä tässä työssä osaltaan tarkennettiin. Varastojärjestelmälle tehdyssä riskianalyysissä todettiin että varaston sisällä liikkuva sukkula voi päätyyn törmätessään aiheuttaa varaston sortumisen joka johtaa mahdollisesti henkilövahinkoihin. Tätä tilannetta varten tarvittiin turvatoiminto joka pysäyttää liikkeen ylinopeuden tapahtuessa. Konedirektiivissä on useita standardeja joita voidaan soveltaa kohteena olevasta järjestelmästä riippuen. Tässä työssä päädyttiin B1-tyyppin standardiin SFS-EN ISO 13849 jossa turvallisuus määritellään suoritustasojen (PL) kautta. Kyseinen standardi valittiin sen yksinkertaisen lähestymistavan vuoksi ja siitä syystä että standardissa on otettu kantaa myös ohjelmoitavan elektroniikan käyttöön jota toteutuksessa oli mukana.

Standardissa esitetyn riskin arvioinnin pohjalta turvatoiminnolle vaadittavaksi suoritustasoksi saatiin c. Turvatoiminnossa käytettävä laitteisto oli jo olemassa joten tässä työssä pyrittiin selvittämään mikä standardin kuvailemista arkkitehtuureista kyseisellä laitteistolla voidaan saavuttaa. Arkkitehtuurin osalta päädyttiin standardissa esitettyyn luokkaan 3 joka koostuu kahdesta itsenäisestä kanavasta. Kanavat suorittavat tulojen ja lähtöjen ohjausta sekä valvontaa ja valvovat toisiaan ristiin.

Turvatoiminnossa käytettävä ohjelmisto suunniteltiin ja toteutettiin toisen kanavan osalta tässä työssä. Lisäksi osoitettiin että turvatoiminnon laitteistolla saavutetaan riittävä riskin vähennys kun ohjelmisto on otettu kokonaisuudessaan huomioon molempien kanavien osalta.

ABSTRACT

TAMPERE UNIVERSITY OF TECHNOLOGY

Master's Degree Programme in Computer Technology

JANI KRISTIAN VÄHÄPESOLA : EVALUATION AND ANALYSIS OF WAREHOUSE CONTROL SYSTEM'S SAFETY FUNCTIONS

Master of Science Thesis, 66 pages, 14 Appendix pages

September 2012

Major: Embedded systems

Examiner: Karri Palovuori

Keywords: Machinery Directive 2006/42/EC, SFS-EN ISO 13849, safety function, speeding guard, warehouse control system, validation

Engine manufacturers must follow Machinery Directive 2006/42/EC with the design and manufacture when machinery is imported in the European internal market. The purpose of this thesis was to make one specific warehouse system meet the requirements of the Directive. We explored one security aspect, speeding of the shuttle inside the warehouse. Compliance with safety regulations is finally addressed by CE marking attached to the machine.

The basis were at risk analysis and requirements specification made for the warehouse system and the content of those documents was specified in this work. In the risk analysis it was found that shuttle moving inside the warehouse can cause its collapse when colliding to the end, which could result in possible personal injury. For this situation a safety function that stops the movement in the event of speeding was required.

Machinery Directive contains a number of standards that can be applied to the system depending of its type. In this work we chose B1-type standard SFS-EN ISO 13849 which defines the security through performance levels (PL). The standard was chosen because of its simple approach, and because it takes account the use of programmable electronics that implementation involved.

The performance level that was required for the safety function was set out as c on the basis of risk assessment defined in the standard. The hardware used in the safety function already existed so in this thesis we tried to identify what architecture described in the standard would fit our design. Architecture of class 3 was chosen from the standard and it contains two independent channels. Channels control the inputs and outputs and also perform monitoring as well as crosswatching of each other.

Software of safety function was designed and implemented for one channel in this work. It was also shown that the equipment used in the safety function achieves adequate risk reduction when the software has been completely taken into account for both channels.

ALKUSANAT

Tämä työ on tehty Suomen Teollisuusosa Oy:lle (STEO) osana varastojärjestelmän turvallisuuteen liittyviä toimintoja. Työstä voin sanoa että se oli alusta asti mielekästä sekä monipuolista, alustavat suunnitelmat toteutukselle tehtiin jo vuoden 2011 lopussa ja työ jatkui käytännössä, muutamia poikkeuksia lukuunottamatta, vuoden 2012 syksyyn asti. Työn edetessä tuli vastaan monia yllättäviä haasteita sekä odottamattomia ongelmatilanteita mutta niistä selvittiin kohtalaisen kunniakkaasti.

Haluan kiittää erityisesti STEO:n työntekijöitä, nimeltä mainitsematta, tukemisessa läpi koko työn sekä siitä miten tekemiseen annettiin riittävästi aikaa. Muuten tähän vaiheeseen pääseminen olisi ollut huomattavasti paljon raskaampaa. Lisäksi kiitokset vanhemmilleni sekä veljelleni Jesselle jotka ovat osaltaan olleet hengessä mukana.

Tampereella 4. Syyskuuta 2012

Jani Vähäpesola

SISÄLLYS

1. Johdanto	1
2. Lähtökohdat ja vaatimukset	3
2.1 Konedirektiivi 2006/42/EY	3
2.1.1 Konedirektiivin soveltaminen järjestelmässä	3
2.1.2 Turvatoiminnossa käytettävä standardi	6
2.2 Standardi SFS-EN ISO 13849	6
2.2.1 Menetelmät suoritustason laskemiseen	8
2.2.2 Suoritustason parametrien kiinnittäminen	11
2.2.3 Dokumentaatio kelpuutusta varten	13
2.3 Laitteiston asettamat rajoitukset	13
2.4 Käytetyt ohjelmistot ja ohjelmointikielet	15
2.5 Turvallisen tilan määrittely	15
3. Ylinopeusvahdin laitteisto	16
3.1 Laitteistoarkkitehtuuri	16
3.1.1 Alijärjestelmät	16
3.2 Laitteiston toteutus	18
3.2.1 Viiva-anturit	18
3.2.2 Ohjauslogiikka	18
3.2.3 Lähdön turvakytkentöjen ohjauksen yleinen periaate	20
3.2.4 Moottoreiden ohjausjännitteen turvakytkentä	21
3.2.5 Jarrujännitteiden turvakytkentä	22
3.2.6 AMR-anturit	23
3.3 Laitteiston suoritustason laskeminen	24
3.3.1 $MTTF_d$	24
3.3.2 DC_{avg}	25
3.3.3 CCF	26
3.3.4 Järjestelmän suoritustaso	28
3.4 Vika -ja vaikutusanalyysi (FMEA)	29
4. Ylinopeusvahdin ohjelmisto	33
4.1 Nopeuden laskenta viiva-antureilla	33
4.2 Virherajat ja rajoitukset	35
4.3 Ohjelmiston laitteistorajapinnat	38
4.4 Yleiskuvaus toiminnasta	38
4.5 Ohjelmiston arkkitehtuuri	39
4.5.1 Nopeuden laskenta	40
4.5.2 Suunnan määrittely	43
4.5.3 Turvakytkentöjen ohjaaminen	43

4.5.4	Ristiinvalvonta	43
4.5.5	Nopeuksien vertailu	45
4.5.6	Kapselin yläaseman määrittely	45
4.5.7	Viiva-anturit	45
4.6	FPGA:n modulkuvaukset ja rajapinnat	45
4.7	Ohjelmistolla toteutettava diagnostiikka (DC_{avg})	49
5.	Turvatoiminnon analyysi ja testaus	50
5.1	Ohjelmiston testaaminen	50
5.2	SIKO:n magneettinen inkrementaalianturi IV58M	51
5.3	Viiva-antureiden testaaminen	52
5.3.1	Häiriötekijöiden vaikutus AD-muunnin-arvoihin	52
5.3.2	Häiriötekijöiden vaikutus laskettuun nopeuteen	55
5.4	FPGA-kanavan testaaminen nostolaitteella	59
5.4.1	Normaaliajo ilman ylinopeutta	60
5.4.2	Ylinopeusvahdin laukeaminen	62
6.	Yhteenveto	66
	Lähteet	67
	A.Liite: Komponenttien MTTF-arvoja	70
	B.Liite: Beta-tekijä	73
	C.Liite: Järjestelmätestauksen testitapaukset	76

TERMIT JA SYMBOLIT

A,B,C,D,E	Standardissa SFS-EN ISO 13849-1 suoritustasoja osoittavat tunnukset
AD	Analog-to-digital, muunnos analogisesta digitaaliseksi
AMR	Anisotropic Magnetoresistance, nostolaitteen antureissa käytetty teknologia
B,1,2,3,4	Standardissa SFS-EN ISO 13849-1 arkkitehtuurin luokkia ja nimettyjä rakenteita osoittavat tunnukset
CCF	Yhteisvikaantuminen, yksittäisen syyn aiheuttama usean komponentin yhtäaikainen vikaantuminen
CRC	Cyclic redundancy check, tarkisteavaimien luontiin tarkoitettu tiivistealgoritmi
DC	Diagnostiikan kattavuus, paljastuneiden vaarallisten vikojen ja vaarallisten vikojen suhde
FMEA	A failure modes and effects analysis, vika -ja vaikutusanalyysi, menetelmä jolla arvioidaan järjestelmän vikaantumista huipputoimintojen menettämisen kautta
FPGA	Field-programmable gate array, ohjelmoitavaa elektroniikkaa
Kapseli	Varastojärjestelmän osa, sukkulaan kuuluva kokonaisuus jonka sisällä paketit siirretään varastojärjestelmässä
LDO	Low-dropout regulator, regulaattori jossa sisääntulon ja ulostulon välinen jännite-ero on hyvin pieni
MTTF _d	Keskimääräinen vaarallinen vikaantumisaika
MTTF	Keskimääräinen vikaantumisaika
Nostolaite	Varastojärjestelmän osa, sukkulan pystysuunnan ja vaakasuunnan liikkeitä ohjaava laite
PFH	Probability of Failure per Hour, vaarallisen keskimääräisen vikaantumisajan todennäköisyys tuntia kohden
PL	Performance level, suoritustaso, erillinen taso jota käytetään määrittelemään turvallisuuteen liittyvien ohjausjärjestelmän osien kyky suorittaa turvatoiminto ennakoitavissa olevissa olosuhteissa standardissa SFS-EN ISO 13849-1
PL _r	Performance level required, vaadittu suoritustaso jolla on tarkoitus saavuttaa vaadittu riskin pienentäminen kullekin turvatoiminnolle standardissa SFS-EN ISO 13849-1
PWM	Pulse-Width Modulation, pulssinleveysmodulaatio on kuormaan menevän jännitteen säätäminen muuttamalla pulssisuhdetta

SIL	Safety integrity level, turvallisuuden luokittelu standardissa SFS-EN 61508
SPI	Serial Peripheral Interface Bus, synkroninen sarjaliikenneväylä
Sukkula	Varastojärjestelmän osa, varaston sisällä liikkuva paketteja siirtävä laite
VCC_MC	Moottorin ohjausjännite, moottoriohjaimen pääteasteiden hilaohjaimen ohjausjännite
VHDL	VHSIC Hardware Description Language, eräs laitteistonkuvauskieli
VHSIC	Very High Speed Integrated Circuit, VHDL:ssä käytetty tekniikkaa
Ylinopeusvahti	Turvatoiminto jolla estetään sukkulan ylinopeus

1. JOHDANTO

Tämän työn kohteena oleva varastojärjestelmä koostuu varastosta sekä siihen kuuluvasta laitteistosta. Varasto on suljettu tila jonka sisäpuolella järjestelmän suoritamat toiminnot tapahtuvat. Se on pystytetty kahdeksi hyllystökseksi ja niiden väliin jää käytävä jossa paketteja siirtävä sukkula pääsee liikkumaan sekä vaakasuunnassa että pystysuunnassa.

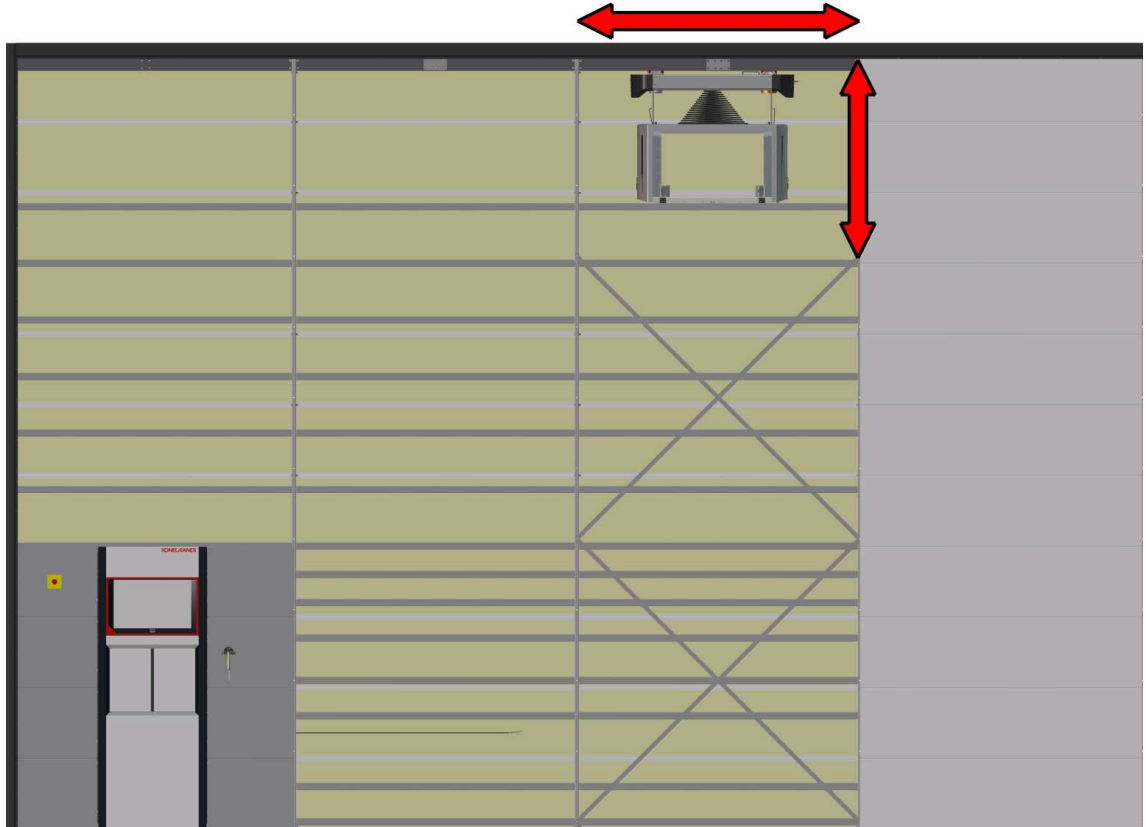
Kuvassa 1.1 on esitetty varasto sekä siihen kuuluvat osat. Sukkula on punaisten nuolien lähellä oleva kappale ja vasemmassa alanurkassa on pakettien jättämiseen tarkoitettu piste. Sukkula koostuu nostolaitteesta ja kapselista. Nostolaite huolehtii sukkulan ajoliikkeestä sekä nostoliikkeestä. Nostolaitteeseen on kiinnitetty hihnoilla kapseli joka lasketaan oikean hyllyn kohdalle pystysuunnassa. Paketit siirretään järjestelmässä kapselin sisällä.

Ulkoapäin varasto on peitetty verhoilulevyillä jotka näkyvät kuvassa oikealla olevana harmaana alueena. Käytävä on lukittu ovella, joten sisäpuolelle varastoon ei pääse ilman tarkoituksellista murtautumista tai avainta. Sukkulan lisäksi järjestelmään kuuluu sitä ohjaava tietokone. Sukkulan ohjaus tapahtuu sähköverkon kautta HomePlug-tekniikalla. Ainoa rajapinta käyttäjälle päin on kosketusnäyttöinen PC jonka käyttöliittymällä varastoon jätetään ja varastosta noudetaan paketteja.

Ajosuunnassa liike tapahtuu varaston katossa olevaa kiskoa pitkin josta sähkö johdetaan sukkulaan hiiliharjojen kautta. Ajoliikkeen tunnistamiseen käytetään viivaantureita jotka mittaavat ajokiskossa olevan nauhan heijastuksia. Järjestelmässä käytetään lisäksi AMR-antureita (Anisotropic magnetoresistance) joilla tutkitaan onko kapseli ylhäällä.

Sähkönsyöttöä varten järjestelmälle on rakennettu oma sähkökaappi jossa on suodatus verkosta tulevia johtuvia häiriöitä vastaan. Suodatus myös estää HomePlugin vuotamisen yleiseen sähköverkkoon päin.

Ajoliikkeen moottoreita ohjataan 12V tasajännitteellä ja niissä on jarrut jotka ovat pakkotoimisesti kiinni. Jarrujen avaaminen tapahtuu 105V tasajännitteen avulla ja jos jännitesyöttö katkeaa jarrut menevät kiinni. Moottoreita pyöritetään takaisinkytketyllä mikroaskelluksella joten mikäli oikeanlainen ohjaus katoaa jäävät moottorit paikalleen. Todennäköisin tilanne jolloin sukkula lähtee ryntäämään toteutuu kun moottoreita ohjaava ohjelma lukittuu pyytämään liian suurta nopeus-



Kuva 1.1: Periaatekuva varastosta

ohjetta moottoreille. Ainoastaan moottorijännitteiden pääteasteita ohjaava FPGA (Field-programmable gate array) kykenee tuottamaan oikeanlaisen virtasekvenssin, joten mikäli se hajoaa jää järjestelmä oletuksena aina turvalliseen tilaan.

Sukkula saa liikkua ajosuunassa sallitulla maksiminopeudella vain silloin kun kapseli on ylhäällä. Muulloin ajoliikkeen nopeusrajan täytyy olla matalampi. Kun kapseli on yläasennossa täytyy tapahtua yläasennon tunnistaminen. Alin mahdollinen paikka määritellään varaston korkeuden mukaan. Ajosuunnassa sukkulan on tunnistettava toinen päädyistä johon sukkula ajetaan sen jälkeen kun järjestelmään on kytketty sähkö. Toinen pääty määritellään varaston pituuden mukaan. Tässä työssä keskityttiin turvatoiminnon toteuttamiseen joka havaitsee kapselin yläaseman ja asettaa sen mukaisesti ajoliikkeen nopeusrajan. Mikäli nopeusraja ylitetään, turvatoiminnon täytyy katkaista jännitteet jarruilta ja ohjausjännitteet ajomoottoreilta. Turvatoiminnon suunnittelussa ja toteuttamisessa seurattiin Konedirektiivin 2006/42/EY standardia SFS-EN ISO 13849-1.

Turvatoimintoa ei vielä tässä työssä kelpuutettu sillä ohjelmistosta jäi puuttamaan toisen kanavan toteutus. Siksi myöskään järjestelmätestejä ei voitu ajaa. Kelpuutuksen osalta standardin SFS-EN ISO 13849-2 dokumentaatiovaatimuksiin on otettu tässä työssä kantaa, laitteiston suoritustaso havaittiin riittäväksi.

2. LÄHTÖKOHDAT JA VAATIMUKSET

2.1 Konedirektiivi 2006/42/EY

Ensisijaiset vaatimukset turvallisuuden kannalta tulevat tälle järjestelmälle konedirektiivin 2006/42/EY kautta. Konedirektiivi koskee säädöksenä kaikkia koneita jotka tuodaan Euroopan sisämarkkinoille. Se määrittää olennaiset terveys -ja turvallisuusvaatimukset yhtenäisen turvatason luomiseksi tapaturmantorjuntaa varten ja sitä on sovellettava sitovasti 29. joulukuuta 2009 alkaen. [1] Koneen valmistajan tulee huolehtia siitä että kone suunnitellaan ja rakennetaan konedirektiivin mukaisesti. Turvallisuusvaatimusten taustalla on aina lähtökohtana ihminen, eli koneen on toimittava siten että se ei aiheuta henkilövahinkoja. Siksi konedirektiivin vaatimukset ja velvollisuudet koneen rakentajalle määräytyvät pääasiallisesti sen mukaan minkälaisen vahingon kone voi toimiessaan aiheuttaa ja mihin luokkaan kone sijoittuu direktiivissä.

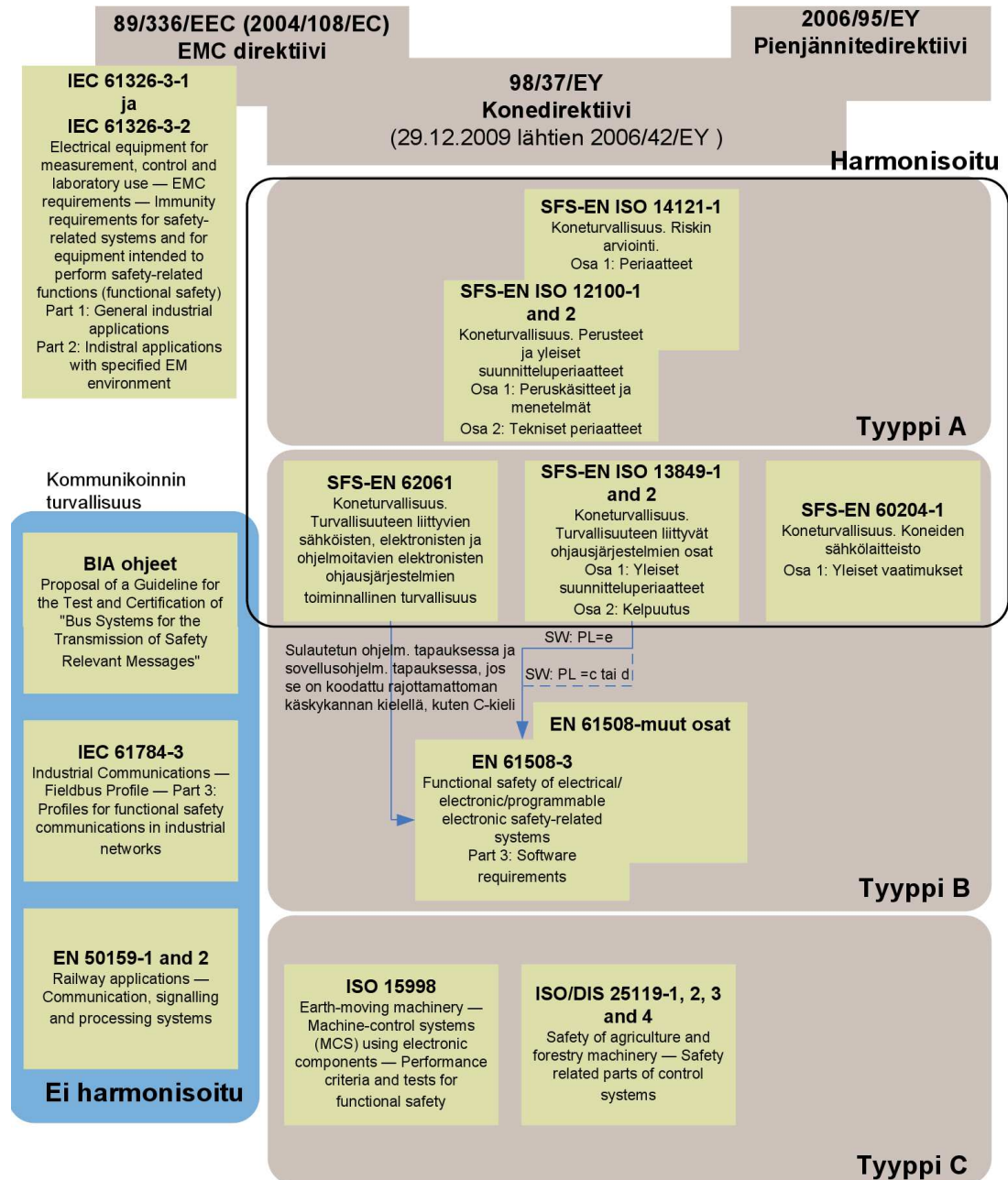
Direktiivin pyrkimyksenä on yhtenäistää käytäntöjä turvallisuusnäkökohtia huomioitaessa ja varmistaa että kaikki Euroopan sisämarkkinoille tuotavat koneet täyttävät samat turvallisuusvaatimukset. [1] Tähän yhtenäistämiseen kuuluu kiinteänä osana myös standardien harmonisointi jossa tavoitteena on että eri valtioiden alueella käytettäisiin samoja standardeja. Toistaiseksi kaikki konedirektiivin standardit eivät ole harmonisoituja mutta yhtenäistäminen on käynnissä. Käytännössä harmonisoitujen standardien käyttö merkitsee valmistajan osalta esimerkiksi sitä että koneen vaatimustenmukaisuutta ei tarvitse tällöin välttämättä arvioida ulkopuolisella taholla vaan siihen riittää sisäinen tarkastus. Lisäksi harmonisoidut standardit helpottavat koneen myyntiä laajemmalla alueella.[1] Kun valmistaja on täyttänyt konedirektiivin vaatimukset, hän osoittaa sen ensisijaisesti koneeseen kiinnittämällä CE-merkinnällä sekä vaatimustenmukaisuusvakuutuksella. [2]

2.1.1 Konedirektiivin soveltaminen järjestelmässä

Konedirektiivin artiklassa 1 on määritelty ne tuotteet joihin direktiiviä voidaan soveltaa ja vastaavasti tuotteet jotka kuuluvat sen soveltamisalan ulkopuolelle. [1] Tämän järjestelmän vaatimusmäärittelyssä on todettu että järjestelmä luokitellaan kokonaisuutena artiklan 1 kohdan a) koneisiin. [3] Koneella tarkoitetaan direktiivissä muun muassa "toisiinsa liitettyjen osien tai komponenttien yhdistelmää, jossa on tai

joka on tarkoitettu varustettavaksi muulla kuin välittömällä ihmis- tai eläinvoimalla toimivalla voimansiirtojärjestelmällä ja jossa ainakin yksi osa tai komponentti on liikkuva ja joka on kokoonpantu erityistä toimintoa varten." [1]

Kuvassa 2.1 on esitetty konedirektiivin alaisuudessa olevia standardeja jotka liittyvät erityisesti tähän järjestelmään. Näistä SFS-EN ISO 12100:ssa on kuvailtu perusteet ja yleiset suunnitteluperiaatteet koneiden turvallisuuteen liittyen. Se toimii perustana kaikille muille konedirektiiviin kuuluville standardeille ja standardiryhmälle joka jakautuu kolmeen osaan taulukon 2.1 mukaisesti.



Kuva 2.1: Konedirektiivin alaiset standardit [4]

Taulukko 2.1: *Standardiryhmä SFS-EN ISO 12100-1 mukaisesti*

Standardin tyyppi	Käyttö
A	perusteet, suunnitteluperiaatteet, yleiset näkökohdat
B	käsittelevät yhtä tai useampaa turvallisuusnäkökohtaa
B1	käsittelevät tiettyä yksittäistä turvallisuusnäkökohtaa
B2	koskevat suojausteknisiä laitteita
C	käsittelevät tietyn koneen tai koneryhmän yksityiskohtaisia turvallisuusvaatimuksia

Tarkempi kohta jota direktiivistä sovelletaan tämän järjestelmän turvatoimintoihin saadaan kun kartoitetaan koneen raja-arvot ja riskitekijät. Kartoitus tehdään riskianalyysin kautta jossa selvitetään mitkä tilanteet voivat aiheuttaa henkilövahinkoja. Riskin arviointi suoritetaan kuvassa 2.1 olevan harmonisoidun standardin SFS-EN ISO 14121-1 pohjalta. Tämä on SFS-EN ISO 12100-1:ssä määritelty A-tyypin mukainen standardi, eli siinä otetaan kantaa yleisiin suunnitteluperiaatteisiin.

Vaatimusmäärittelyssä ja sitä edeltävässä riskianalyysissä löydettiin yksi potentiaalinen riskitekijä jota varten tarvitaan turvatoiminto, eli sukkulan nopeuden kasvaminen rajoittamattomasti ajoliikkeessä. [3] Standardin SFS-EN ISO 14121-1 liitteen A taulukon A.1 kohdassa 1 tämä on esitetty tyypiltään mekaanisena vaarana, alkuperänään kiihtyminen ja hidastuminen (liike-energia). [5] Edelleen kohdassa A.1 on viittaukset standardin SFS-EN ISO 12100-1 kohtiin 4.2.1, 4.2.2 sekä 4.10, eli mekaanisiin vaaroihin jotka on otettava huomioon konetta suunniteltaessa. [6] Tässä tapauksessa kohdat puristuminen, yliajatuksi tuleminen sekä iskut kuvaavat seurauksia joita ihmiselle voi aiheutua mikäli sukkula törmää täydellä vauhdilla varaston päättyyn.

Tarkastelun kohteeksi tulee siis ajoliikettä valvova turvatoiminto joka kuuluu tarkemmin direktiivin liitteen IV kohdan 21 alle, eli logiikkayksiköt turvatoimintoja varten. [2] Tässä direktiivin kohdassa on määritelty että logiikkayksiköt ovat komponentteja ja ohjausjärjestelmän osia, jotka: "vastaavat turvakomponenttien määritelmää (ks. 42 kohta, 2 artiklan toisen kohdan c alakohtaa koskevat huomautukset), analysoivat yhtä tai useaa tulosignaalia ja luovat tietyn algoritmin mukaisesti yhden tai useamman lähtösignaalin sekä on tarkoitettu käytettäväksi koneiden ohjausjärjestelmien yhteydessä tai niiden osana yhden tai useamman turvatoiminnon suorittamista varten." [3] [2] Tällaiset logiikkayksiköt voidaan vaatimusten ja määritelmän osalta rinnastaa konedirektiivissä mainittuihin turvakomponentteihin.

SFS-EN ISO 12100-1:ssä esitetyistä taulukon 2.1 mukaisista standardeista esitetään turvatoiminnon vaatimuksien selvittämiseen tyyppin B1 mukaista standardia joka käsittelee tiettyä yksittäistä turvallisuusnäkökohtaa. Tässä tapauksessa se on ylinopeuden valvonta.

2.1.2 Turvatoiminnossa käytettävä standardi

Kun mahdolliset riskit on kartoitettu, selvitetään turvatoiminnon ja koneen tyyppin perusteella mitä standardia turvatoiminnon vaatimuksiin sovelletaan. Sen lisäksi että etsitään tyyppin B1 mukaista standardia tiedetään turvatoiminnon laitteiston sisältävän mekaniikkaa, elektroniikkaa ja ohjelmoitavaa elektroniikkaa. Tämä asettaa tiukemmat vaatimukset suunnittelulle. Kuvassa 2.1 olevista B ja C-tyypin standardeista SFS-EN 62061, SFS-EN ISO 13849 sekä EN 61508 soveltuvat käytettäväksi myös monimutkaisempien järjestelmien ollessa kyseessä. [3]

SFS-EN 61508 on kehitetty ohjelmoitavaa elektroniikkaa sisältäviä laitteita varten. Siinä annetaan ohjeita ja vaatimuksia myös ohjelmiston suunnitteluun ja huomiota on kiinnitetty funktionaaliseen turvallisuuteen pelkän arkkitehtuurin sijasta. Turvallisuus määritellään suoritustasojen SIL (Safety integrity level) kautta. [7] Suoritustason laskennassa otetaan huomioon sekä rakenne että vikaantumisaika ja dokumentointi kuuluu osana suunnitteluun. Vikaantumisten havaitsemisessa ja torjunnassa käytettyjä menetelmiä ovat esimerkiksi Markovin prosessit sekä vikapuuanalyysi. [7] SFS-EN 61508:sta johdettu standardi SFS-EN 62061 käsittelee vielä tarkemmin ohjelmoitavia elektronisia laitteita. [8]

SFS-EN ISO 13849 on osin johdettu käytöstä poistetusta standardista SFS-EN 954-1 jossa lähestymistapa oli hyvin mekaaninen ja arkkitehtuureittain määritelty. Aikana jolloin se julkaistiin (1997) koneet ja niiden turvatoiminnot sisälsivät enemmän puhtaasti mekaniikkaa sekä yksinkertaista elektroniikkaa jolloin turvallisuus voidaan määritellä helpommin rakenteiden kautta. SFS-EN 954-1:ssä ohjelmistoa ja dokumentointia ei juuri oteta huomioon ja turvatoiminnolla saavutettavaan suoritustasoon (PL, Performance level) vaikuttaa ennenkaikkea turvatoiminnon toteuttavan ohjausjärjestelmän arkkitehtuuri.

SFS-EN ISO 13849 on luotu ensisijaisesti sitä varten että saataisiin yhteys vanhan standardin SFS-EN 945-1 arkkitehtuurien ja uudemman SFS-EN 62061:n suoritustasojen välille. Standardia voidaan soveltaa myös monimutkaisempiin järjestelmiin ja siinä on esitetty yksinkertaistettu menetelmä suoritustason määrittämiseksi. Etuna SFS-EN 62061:een verrattuna on yleisesti helpompi lähestymistapa. [9] Tämän järjestelmän turvatoimintojen vaatimusten määrittelyssä käytettäväksi standardiksi valittiin SFS-EN ISO 13849-1 joka on B1-tyypin standardi.

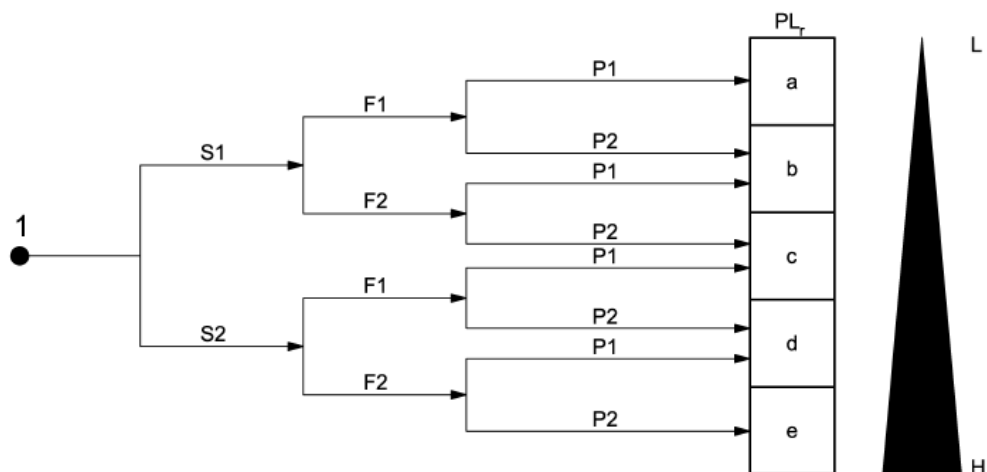
2.2 Standardi SFS-EN ISO 13849

Riskianalyysissä kartoitetaan järjestelmän rajoituksia, mahdollisia riskejä, niiden esiintymistodennäköisyyttä sekä vakavuutta käyttäjälle toteutuessaan. Riskien arvioinnin perustana käytetään konedirektiivissä standardia SFS-EN ISO 14121-1. Siinä on esitetty yleisesti asioita jotka täytyy ottaa huomioon riskitekijöitä

määriteltäessä. Tällaisia ovat esimerkiksi koneen raja-arvojen määrittäminen joihin kuuluvat käyttörajat, tilarajat sekä aikarajat. [5] Tässä järjestelmässä aikarajoista täytyy ottaa huomioon ennenkaikkea viiva-antureiden IR-ledien käyttöikä. IR-ledit ovat turvatoiminnon komponenteista nopeimmin vikaantuvia ja koska viiva-anturit muodostavat ainoan lähteen nopeuden laskennalle, ovat ne kriittisessä asemassa raja-arvojen osalta.

Raja-arvojen määrittelemistä seuraa vaaran tunnistaminen jossa etsitään mahdollisia vaaratilanteita joita koneen käyttöön sekä käyttöönottoon saattaa liittyä. Jokaiselle vaaratilanteelle suoritetaan tämän jälkeen riskin suuruuden arviointi jossa selvitetään vahingon vakavuus sekä vahingon esiintymistodennäköisyys. Riskianalyysistä johdettiin yksi ihmiselle vakava riski johon on puututtava. Mikäli sukkula törmää liian suurella nopeudella varaston pätyyn, voi tästä seurata koko varaston sortuminen mikä puolestaan voi johtaa vakaviin henkilövahinkoihin tai kappaleiden sinkoutumiseen. [3]

Turvatoiminnolta vaadittava suoritustaso määritellään riskin arvioinnin perusteella. Kuvassa 2.2 on esitetty standardin SFS-EN ISO 13849-1 mukainen menetelmä riskien arvioinnille ja vaadittavan suoritustason määrittelemiselle riskigraafin avulla. Se pohjautuu standardeihin SFS-EN ISO 12100-1 ja SFS-EN ISO 14121-1.



Kuva 2.2: Standardin SFS-EN ISO 13849-1 mukainen riskigraafi [10]

Asteikko on viisitasonen A..E missä E edustaa korkeinta vaadittavaa suoritustasoa ja A matalinta. S tarkoittaa riskin vakavuutta missä S1 on lievä ja S2 vakava. F puolestaan tarkoittaa riskin esiintymisen todennäköisyyttä missä F1 tapahtuu harvoin ja F2 usein. P tarkoittaa sitä voidaanko riski estää, P1 mahdollisesti ja P2 tuskin milloinkaan.

Riskianalyysissä vakavuudeksi arvioitiin 3 joka graafista määritetään S2:ksi eli vakavaksi. Todennäköisyydeksi arvioitiin 2 ja sille valitaan graafista F1 eli harvoin.

Hallitsematon ylinopeus on tilanteena harvinainen. Vaaran välttämistä ei suoraan arvioitu riskianalyyseissä, mutta asetamme sille arvoksi P1 eli mahdollista tietäisissä olosuhteissa. Näin siksi että käyttäjä kuulee suurella todennäköisyydellä törmäämisen päätyyn eikä varasto sorru niin nopeasti etteikö käyttäjä ehtisi alta pois. Näillä arviointiperusteilla saatiin vaadittavaksi suoritustasoksi $PL_r = C$ johon turvatoiminnon on vähintään kyettävä.

2.2.1 Menetelmät suoritustason laskemiseen

Kun riskin aiheuttaman vahingon suuruus ja vakavuus on arvioitu, eli ollaan määritellyt turvatoiminnolta vaadittava suoritustaso PL_r , suunnitellaan tämän jälkeen itse turvatoiminto ja katsotaan minkälaiseen suoritustasoon (PL) toteutus ylittää. Mikäli saavutettu suoritustaso jää pienemmäksi kuin turvatoiminnolta vaaditaan, joudutaan toteutusta muuttamaan. Standardi SFS-EN ISO 13849-1 antaa kaksi erilaista menetelmää suoritustason laskentaan. Toisessa huomioidaan laajamittaisemmin kaikki standardissa esitetyt asiaan kuuluvat muuttujat ja laskentaan soveltuvat menetelmät. Toinen on nimettyihin rakenteisiin ja lohkomenetelmään perustuva yksinkertaistettu lähestymistapa, jota tässä järjestelmässä käytettiin. [3] [10]

Yksinkertaistetussa menetelmässä jonka standardi määrittelee otetaan suoritustasoa laskettaessa huomioon lähinnä neljä parametria: $MTTF_d$ (Mean time to dangerous failure), DC_{avg} (Average diagnostic coverage), CCF (Common case failure) ja Arkkitehtuuri (Architecture).

Standardin mukaan turvatoiminnon arkkitehtuurin on oltava vähintään 1 jos sillä halutaan saavuttaa turvataso C. Rajoituksena on myös että luokkien 2, 3 ja 4 järjestelmien täytyy saada CCF:stä vähintään 65-pistettä. [10] Taulukossa 2.2 on esitetty erilaisia yhdistelmiä $MTTF_d$:lle, DC_{avg} :lle ja arkkitehtuurille jotta saavutettaisiin turvataso C joka turvatoiminnolta vaaditaan.

Taulukko 2.2: Yhdistelmiä turvatason C saavuttamiseksi

Turvataso (PL)	Arkkitehtuuri	$MTTF_d$	DC
C	1	korkea	nolla
C	2	korkea	matala
C	2	keskimääräinen	keskimääräinen
C	3	keskimääräinen	matala
C	3	matala	keskimääräinen

$MTTF_d$

Standardin mukaan kanava määritellään poluksi jonka vikaantuminen voi johtaa turvatoiminnon menettämiseen. Se voi tarkoittaa esimerkiksi vain sisääntuloa, ohjauslogiikkaa tai ulostuloa. Standardi määrittelee että yksittäisen kanavan $MTTF_d$ voi olla maksimissaan 100 vuotta riippumatta kanavan sisältämien komponenttien

vikaantumisajoista. Lisäksi standardi kertoo että koko järjestelmän turvatasoa lasettaessa täytyy ottaa huomioon sarjaan kytkettyjen alijärjestelmien turvatasojen vaikutus. Esimerkiksi mikäli järjestelmä pitää sisällään useamman kuin kaksi kappaletta tason C alijärjestelmiä, tippuu koko järjestelmän turvataso yhdellä B:hen.

Standardin mukaan $MTTF_d$:n täytyy olla koko järjestelmällä yli kymmenen vuotta, jotta saavutetaan turvataso C luokan 3 arkkitehtuurilla. Komponentin $MTTF_d$:ksi voidaan antaa standardin mukaan oletusarvona 10-vuotta mikäli sitä ei ole ilmoitettu. Jos komponentteja on turvatoimintoa toteuttamassa suuri määrä, tarkoittaa tämä sitä että standardin määrittelemä oletusarvo ei riitä. Yleensä valmistajat ilmoittavat esimerkiksi B_{10} , $MTTF$, $MTTF_d$ tai $MTBF$ -arvot vikaantumiselle.

Kun jokaisen yksittäisen turvatoimintoon kuuluvan komponentin $MTTF_d$ -arvo on saatu selvitettyä, voidaan koko kanavan vikaantumisaika laskea standardin mukaisella kaavalla (2.1).

$$\frac{1}{MTTF_d} = \sum_{i=1}^N \frac{1}{MTTF_{di}} = \sum_{j=1}^N \frac{n_j}{MTTF_{dj}} \quad (2.1)$$

Mikäli redundanttiset kanavat on toteutettu samalla tavalla, niiden yhdistetty $MTTF_d$ on sama, eli ne eivät laske toistensa vikaantumisaikoja. Jos taas molemmilla kanavilla ei ole samaa $MTTF_d$:tä, voidaan arviointiin käyttää standardin liitteen D mukaista kaavaa D.2. [10] Redundanttisten kanavien tapauksessa standardi käsittää maksimissaan kaksi kanavaa, tätä useamman kanavan mahdolliseen hyötyyn ei oteta laskennallista kantaa.

DC_{avg}

Diagnostiikan kattavuuden (DC) laskentaan annetaan standardissa yleisiä ohjeita. Laskennassa määritetään paljastuneiden vaarallisten vikaantumisten ja kaikkien vaarallisten vikaantumisten välinen suhde. Jokainen turvatoimintoon vaikuttava komponentti on otettava huomioon ja mikäli jonkin komponentin vaarallista vikaantumista ei testata mitenkään sen $DC = 0$. Järjestelmässä olevia komponentteja voidaan mallintaa alijärjestelmien kautta siten että ne voivat koostua useista fyysisistä komponenteista. Näin kaikkia komponentteja ei huomioida yksittäin samalla tavalla kuin $MTTF_d$:tä lasettaessa sillä diagnostiikkaa lasettaessa meitä kiinnostaa vain koko alijärjestelmän lähdön tila ja sen havaitseminen.

Jos järjestelmä koostuu useista alijärjestelmistä joille on jokaiselle laskettu oma DC-arvonsa, saadaan koko järjestelmän DC_{avg} laskettua standardin mukaisesti kaavalla (2.2).

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d1}} + \dots + \frac{DC_n}{MTTF_{dn}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d1}} + \dots + \frac{1}{MTTF_{dn}}} \quad (2.2)$$

Standardissa EN-61508 on esitetty kattavampi tapa laskea diagnostiikkaa ottamalla huomioon paljastuneiden vaarallisten vikaantumisten ja kaikkien vaarallisten vikaantumisten suhteet jokaiselle yksittäiselle komponentille erikseen. [7] Käytämme kuitenkin EN ISO-13849-1:n arviointitaulukoita, joissa kattavuus komponentille lasketaan pikemmin tietyn arviointitavan perusteella.

Laskennassa käytetään erilaisia menetelmiä riippuen siitä onko kyseessä tulo, logiikka vai lähtöyksikkö. Liitteen A taulukoissa on esitetty ehtoja diagnostiikan kattavuuden arviointiin. DC johon jokaisella kanavalla täytyy minimissään päästä pyrittäessä turvatasolle C on matala eli 60%. Seuraavaksi tarkastelemme kohtia joita voidaan soveltaa turvatoimintoja toteutettaessa.

CCF

CCF eli yhteisvikaantuminen tarkoittaa tilannetta jossa yksittäinen syy aiheuttaa useiden komponenttien yhtäaikaisen vikaantumisen. CCF:n laskennassa käytetään standardin mukaista taulukkoa liitteessä B jossa annetaan pisteitä järjestelmän täyt- täessä määrättyjä ehtoja. Arkkitehtuurien 2, 3 tai 4 mukaan tehdyn turvatoiminnon on saatava vähintään 65 pistettä jotta se voidaan hyväksyä. Jokainen taulukon kohta on sellainen että siitä saa joko 0 pistettä tai täydet pisteet. [10] CCF on huomioitava jokaiselle alijärjestelmälle erikseen, matalimmat pisteet määräävät koko järjestelmän pisteytyksen.

On huomattava että elektronisia komponentteja ei standardin mukaan yleisesti pidetä hyvin koeteltuina, joten tätä kohtaa ei voida soveltaa pisteytyksessä [10].

Arkkitehtuuri

Ohjelmoitava elektroniikka asettaa itsessään ehdoksi ja toisaalta myös toteuttaa vähintään luokan 2 järjestelmän arkkitehtuurin. Sillä saavutetaan turvataso C kun $MTTF_d$ on korkea ja DC_{avg} matala tai kun $MTTF_d$ on keskimääräinen ja DC_{avg} keskimääräinen. [3] Arkkitehtuurin 1 valinta on käytännössä mahdoton sillä siinä vaaditaan hyvin koeteltuja komponentteja eikä tämä ehto toteudu ohjelmoitavien elektronisten laitteiden ollessa kyseessä. Arkkitehtuuri 4 asettaa liian tiukat vaatimukset valvonnalle, joista ei tässä tapauksessa ole lisähyötyä. Yleisesti standardi suosittelee käyttämään vaadittavaan riskin vähennykseen kykenevää eikä sitä ylittävää ratkaisua. Alijärjestelmiä ei voida toteuttaa luokkien B tai 1 arkkitehtuureilla. Tämä johtuu siitä että luokassa B ei päästä turvatasolle C ja luokassa 1 taas komponenttien on oltava hyvin koeteltuja. [10]

Ohjelmistovaatimukset

Standardi esittää vaatimuksia ja rajoituksia jotka turvatoiminnon suorittavan

ohjelmiston on täytettävä vaadittavasta suoritustasosta riippuen. Nämä ehdot perustuvat pitkälti standardiin EN ISO 61508-3, SFS-EN ISO 13849:n ollessa vain käytännönläheisempi. Turvatoiminnon toteuttavan ohjelmiston osalta on huomattava että toisen kanavan ohjelmisto tehdään rajoittamattoman käskykannan ohjelmointikielellä, eli MSP-mikrokontrollerille C-kielellä. Tällöin täytyy ottaa tarkemmin huomioon kaikki vaatimusmäärittelyssä ja standardissa esitetyt vaatimukset sekä noudattaa hyväksi todettuja ohjelmoinnin käytäntöjä. Kuitenkin myös rajoittamattoman käskykannan ohjelmointikielillä on mahdollista saavuttaa standardin SFS-EN ISO 13849-1 esittämät suoritustasot a..e.

Ohjelmiston kehitysprosessi pitää sisällään määrittelyn ja suunnittelun ennen toteutusta. Jokaisessa kehitysvaiheessa tehdään riittävä määrä katselmointeja jotta yksilöistä johtuvat virheet saataisiin mahdollisimman aikaisessa vaiheessa kiinni. Kehitysvaiheisiin kuuluu verifiointi jolla varmennetaan että suunnittelu seuraa määrittelyä. Validoinnissa todetaan että määrittely itsessään on ollut järkevä ja toteutettu ohjelmisto määrittelyssä haluttujen vaatimusten mukainen.

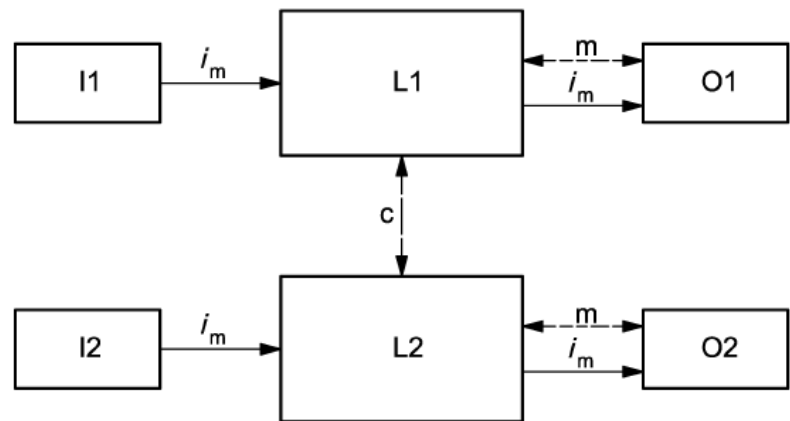
Jotta ohjelmasta saataisiin vaatimusten mukainen, seurataan suunnittelussa ja toteutuksessa standardin SFS-EN ISO 13849-1 liitteen J vaatimuksia. [10] Tässä työssä sekä VHDL:ää (VHSIC Hardware Description Language) että C:tä varten on käytössä ohjelmointistandardit.

2.2.2 Suoritustason parametrien kiinnittäminen

Turvatoiminnon arkkitehtuuri toteutetaan luokan 3 mukaisesti siksi että tällöin $MTTF_d$:n ei tarvitse olla niin korkea eikä valvonnan tasolta vaadita liikaa. Kuvassa 2.2.2 on esitetty standardin luokkaa 3 vastaava arkkitehtuuri. Tässä arkkitehtuurissa vaaditaan redundanssia siten että järjestelmässä on vähintään kaksi itsenäistä kanavaa. Lisäksi arkkitehtuuri edellyttää ristiinvalvontaa kanavien ohjauslogiikoiden välillä sekä jonkinlaista takaisinkytkentää lähtöyksiköltä.

Muiden parametrien osalta luokassa 3 vaaditaan CCF:ltä vähintään 65-pistettä, $MTTF_d$:stä arvoa matala sekä DC_{avg} arvoa matala. Kuitenkin joko $MTTF_d$:n tai DC_{avg} :n on oltava tasolla keskimääräinen mikäli toinen parametreista saa arvon matala. CCF:lle laskettavat pisteet esitetään kappaleessa 3.3.3. Tässä järjestelmässä pyritään $MTTF_d$:n osalta tasoon keskimääräinen jolloin liikutaan välillä 10 vuotta $\leq MTTF_d \leq 30$ vuotta. Vastaavasti DC_{avg} :n osalta pyritään tasoon matala eli $60\% \leq DC \leq 90\%$.

Standardissa olevaa systemaattista vikaantumista ei huomioida kohta kohdalta sillä yksinkertaistettu menetelmä ei tätä vaadi. Tärkeintä on että turvatoiminto perustuu nimettyihin rakenteisiin ja selvitykseen niiden käytöstä. Nimetyt rakenteet on esitetty standardin kappaleessa 6.2 jokaisen luokan yhteydessä. Tässä dokumentissa on kuvattu lohkokaavioiden avulla turvatoiminnon rakenne ja turvatoiminnon osat



Katkoviivat esittävät kohtuudella mahdollista vikojen paljastamista.

Merkintöjen selitys:

i_m	kytkentävälineet
c	ristiinvalvonta
I1, I2	tuloyksikkö (esim. anturi)
L1, L2	logiikat
m	valvonta
O1, O2	lähtöyksikkö (esim. pääkontaktori)

Kuva 2.3: Luokan 3 mukainen nimetty rakenne standardissa SFS-EN ISO 13849-1 [10]

on jaettu selkeästi lohkoihin kanavien mukaisesti. Lohkomenetelmän kuvaus löytyy standardin liitteestä B.

Osittain CCF:ää laskettaessa otetaan kantaa samoihin asioihin kuin systemaattisen vikaantumisen välttämiseksi. Siksi CCF:ää laskettaessa pisteitä ei ole otettu kohdan "Suunnittelu, soveltaminen ja kokemukset" alakohtasta "Suojaustoimenpiteet". Systemaattinen vikaantuminen on soveltuvilta osin huomioitu suunnittelussa ja esimerkiksi tärkeimmät asiat siihen liittyen eli turvallisuuden peruseriaatteet ja hyvin koetellut turvallisuusperiaatteet on otettu huomioon.

2.2.3 Dokumentaatio kelpuutusta varten

Standardissa SFS-EN ISO 13849-2 on määritelty dokumentaatiovaatimus sen perusteella minkä luokan arkkitehtuurin mukaan turvatoiminto on toteutettu. Järjestelmässä käytetään luokan 3 arkkitehtuuria ja vaadittavat dokumentit löytyvät standardin taulukosta 2.[11] Tässä dokumentissa on pyritty soveltuvilta osin ottamaan kantaa välttämättömiin kohtiin jotka taulukossa on mainittu. Järjestelmän suunnittelussa on otettu huomioon turvallisuuden peruseriaatteet jotka löytyvät standardin taulukosta D.1 sekä hyvin koetellut turvallisuusperiaatteet jotka löytyvät standardin taulukosta D.2. [11] Odotettavissa olevista toimintarasituksista voidaan mainita viiva-anturin ja ajokiskon nauhan likaantuminen sekä kuluminen. Käsiteltävien materiaalien vaikutuksia ei oteta tässä dokumentissa huomioon.

Suorituskyky muiden asiaan kuuluvien ulkoisten vaikutusten aikana huomioidaan EMC-testeissä ja järjestelmätestauksessa. Ennakoitavissa olevat yksittäiset viat, jotka on otettu huomioon suunnittelussa, sekä käytetyt havaitsemismenetelmät huomioidaan vika -ja vaikutusanalyysissä 3.4, DC-tasoissa 3.3.2 sekä ohjelmistossa 4.7. Tunnistetut yhteismuotovikaantumiset ja niiden estämistavat löytyvät kappaleesta 3.3.3. Ennakoitavissa olevat poissuljetut yksittäiset viat-taulukosta ei ole tässä järjestelmässä sovellettu yhtään kohtaa. Viat jotka on havaittava esitetään ohjelmistossa 4.7 sekä kappaleessa 3.3.2. Miten turvatoiminto ylläpidetään kunkin vian (vikojen) sattuessa löytyy vika -ja vaikutusanalyysistä 3.4.

2.3 Laitteiston asettamat rajoitukset

Nopeuden laskentaan käytetään viiva-antureita jotka mittaavat erivärisiin osiin jaetun nauhan heijastamaa valoa. Nopeus määritellään eriväristen osien muutoskohdissa mitatuista ajoista. Nauhan eriväristen osien pituudet voivat vaihdella. Maksiminopeus johon turvatoiminto reagoi asetetaan varastokohtaisesti ja se on esitetty vaatimusmäärittelyssä. [3]

Ideaalinen maksimikiiltyvyys sukkulalle voidaan laskea kun tiedetään että ajomoottoreita on 4kpl ja niistä jokaisella on maksimissaan 4Nm vääntömomentti. Ajo-

moottoreiden pyörän akselin säde on 5cm. Sukkulan paino tyhjänä on 100kg. Näistä tiedoista saadaan sukkulalle teoreettinen maksimikiikhtyvyys:

$$\tau = Fr \Leftrightarrow a = \frac{2\tau}{rm} = \frac{4 \times 4Nm}{0.05m * 100kg} = 3.2 \frac{m}{s^2} \quad (2.3)$$

Käytännössä esimerkiksi kitkat rajoittavat tätä maksimiarvoa. Turvatoiminnossa kahdella viiva-anturilla mitattujen nopeuksien erotus saa olla maksimissaan $0.25 \frac{m}{s}$ kapselin ollessa alhaalla. Kapselin ollessa ylhäällä saa nopeuksien erotus olla maksimissaan $0.5 \frac{m}{s}$. Kun kapseli on alhaalla saa maksiminopeus olla $0.25 \frac{m}{s}$. Kapselin ollessa ylhäällä maksiminopeus täytyy olla asetettavissa välille $1.0 - 3.0 \frac{m}{s}$ järjestelmäkohtaisesti. Valittu maksiminopeus asetetaan kiinteästi siten että se voidaan muuttaa vain ohjauslogiikan uudelleenohjelmoinnilla. Valittuja nopeuksia on perusteltu kappaleessa 4.2. Tässä järjestelmässä päädyttiin lujuuslaskelmien pohjalta maksiminopeuteen $1.25 \frac{m}{s}$. [3]

Näytteistystaajuus viiva-anturin dataa luettaessa on 4.545kHz. Tätä nopeammin anturin MSP ei ehdi toimia asetetulla pakettikoolla. Viiva-anturin SPI:n (Serial Peripheral Interface Bus) kellotaajuus on 250kHz ja yksi datapaketti pitää sisälleen kolmen ledin 12-bittiset AD-muunninarvot sekä 8-bittisen CRC:n (Cyclic redundancy check). Pakettikokoa ja protokollaa ei lähdetty muuttamaan koska sille ei ole kriittistä vaatimusta ja tällä hetkellä käytössä oleva toteutus on testattu ja hyväksihavaittu. Tässä on huomattava että tuotantotestauksessa on jotenkin testattava viiva-anturin absoluuttisen nopeuden näyttämä jotta voidaan todeta nopeuden pysyvän kappaleessa 4.2 laskettujen virherajojen sisällä.

Maksimissaan sukkulan nopeus on $3 \frac{m}{s}$. Kun kahden ledin välinen etäisyys on 1.2cm ja viiva-antureiden näytteistystaajuus 4.545kHz saadaan maksiminopeudella nopeuden laskentaa varten 18 näytettä yhtä 1.2cm:n matkaa kohden. Edelleen tällä nopeudella saadaan 54 näytettä ennenkuin ollaan ehditty kulkea yhden nauhanosan verran joka on 3.6cm. Nämä rajoitukset täytyy ottaa huomioon kun päätetään kuinka monen peräkkäisen näytteen perusteella tehdään tulkinta nauhan muutoskohdasta.

FPGA:lla käytetään pelkästään VHDL:ää turvatoiminnon logiikassa. Nios-prosessoria jolle voidaan kääntää C-kielisiä ohjelmia ei ohjauksessa käytetä. FPGA:n kellotaajuus on 50MHz ja koska operaatioita voidaan tehdä rinnakkain ei FPGA aseta kriittisiä rajoja suorituskyvyille. Esimerkiksi jakolasku 16-bittisille luvuille jota tarvitaan nopeuden laskennassa voidaan suorittaa muutaman kellojakson aikana. Ohjauslogiikoista MSP asettaa rajat suorituskyvyn osalta.

MSP:llä käytetään sisäistä 16Mhz:n oskillaattoria. Valmistajan mukaan tässä järjestelmässä olevalla MSP:llä päästään suorituskyvyn osalta 16 MIPS:iin. [12] Datalehdestä huomataan tutkimalla kaikkien käskyjen osalta sitä kuinka monta kel-

lojaksoa niiden suoritus vie keskimäärin että suorituksessa päästään vähintään 5 MIPS:iin. [13] Jos käytetään tätä arvoa pahimpana mahdollisena alarajana voidaan arvioida kuinka monta käskyä keskimäärin kyetään suorittamaan kun sukkula kulkee yhden nauhanosan verran ajokiskolla. Tässä oletetaan että nauhanosan pituus on 3.6cm.

Suurimmalla mahdollisella nopeudella $3\frac{m}{s}$ saadaan 54 näytettä yhdelle nauhanosalle ja se vie aikaa 12ms. Tässä ajassa saadaan 5 MIPS-mikrokontrollerilla suoritettua $5 \times 10^6 \times 0.012 = 60000$ käskyä. 4.545kHz:n näytteistyksellä saadaan suoritettua $5 \times 10^6 \times 0.0002 = 1100$ käskyä yhden näytteen aikana. Yksittäisen näytteen hylkääminen ei siis vaikuta merkittävästi nopeuden laskennan tuloksiin.

2.4 Käytetyt ohjelmistot ja ohjelmointikielet

Kehitystyö toteutettiin Linux-käyttöjärjestelmällä ja siihen kuuluvilla ohjelmistoilla. Ohjelmointikieleksi Texasin MSP430-mikrokontrollerille valittiin rajoittamattoman käskykannan kieli C. Ohjelmien kääntäminen tälle alustalle tehdään kehitystyökalulla IAR embedded Workbench for MCS-51 7.51A Kickstart. Laitteistonkuvauskieleksi valittiin VHDL jolla tehdään Alteran FPGA:n ohjauslogiikan kuvaus. VHDL:n kääntämiseen ja syntetisointiin käytettiin Alteran Quartus-kehitysympäristöstä versiota 10.0.

VHDL:lle tehtyjen modulien testauksessa ja simuloinnissa käytettiin apuna ilmaista vhdsim-ohjelmaa joka käyttää GHDL:ää python-rajapinnan kautta. Matemaattisissa yhtälöissä ja kaavojen laskennassa hyödynnettiin linux:lle tehtyä mathematic-ohjelmaa. Standardin mukaisen suoritustason laskentaan käytettiin SISTEMA-nimistä työkalua.

2.5 Turvallisen tilan määrittely

Turvallisessa tilassa järjestelmän ajomoottorit asetetaan energiattomaan tilaan jolloin niiden ohjausjännitteet ja jarrujännitteet on katkaistu. Tämä toteutuu käytännössä siten että turvakytkentöjä ohjaavat sisääntulot vedetään alas jolloin myös lähtöjen jännitteet menevät alas. Kun järjestelmä on kerran ohjattu turvalliseen tilaan se myös pysyy siinä siihen asti kunnes koko järjestelmästä on katkaistu jännitteet. Kun järjestelmä ohjataan turvalliseen tilaan, nostolaitteen ledit VMC sekä VBRK menevät pois päältä. Ledit on kytketty turvakytkentöjen ulostuloihin, joten ne osoittavat suoraan raudalla että moottorin ohjausjännitteet ja jarrujännitteet ovat pudonneet riittävän matalalle tasolle.

3. YLINOPEUSVAHDIN LAITTEISTO

3.1 Laitteistoarkkitehtuuri

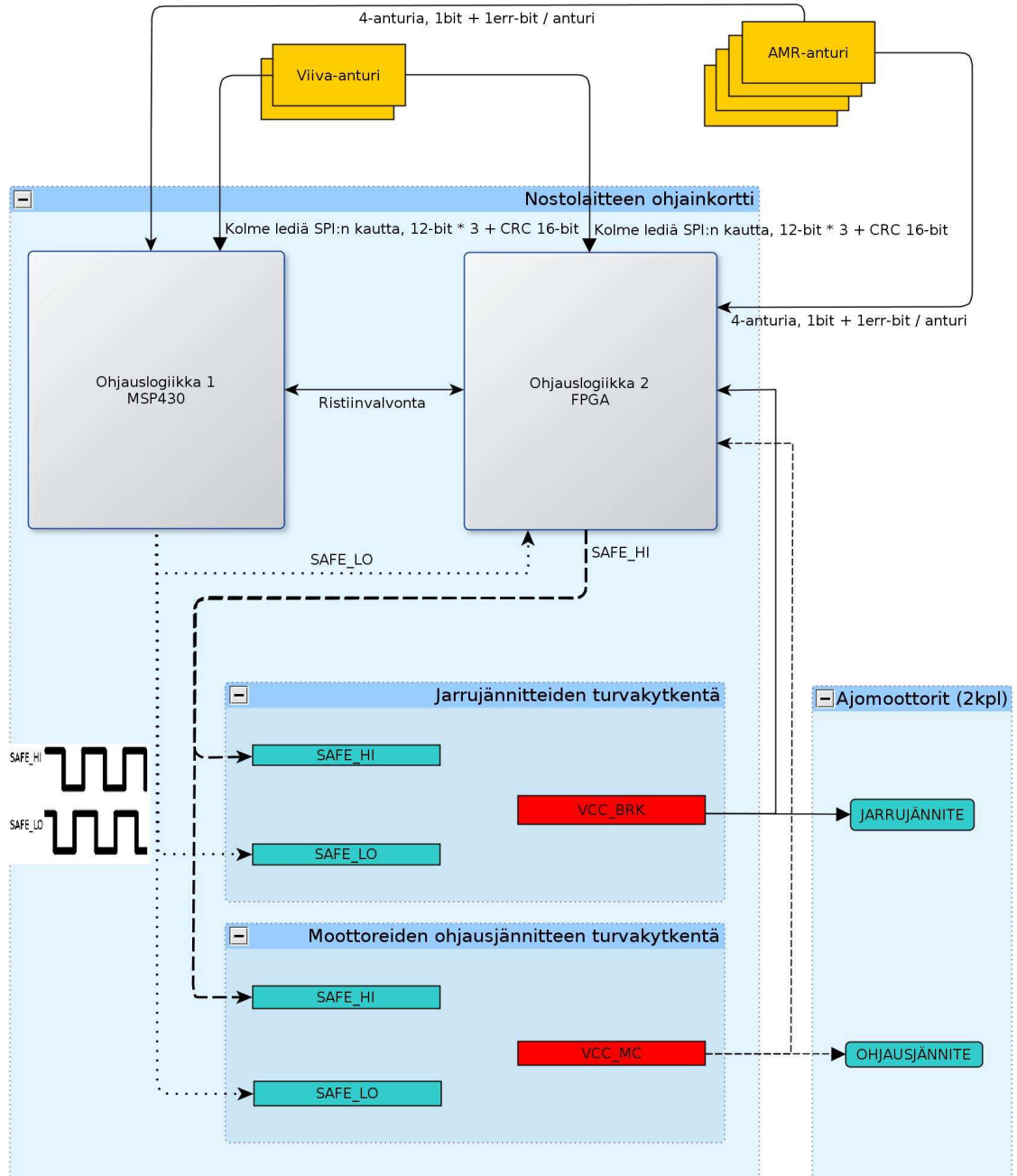
Järjestelmässä ylinopeusvahdin toteuttava elektroniikka sisältyy osaksi nosto -ja ajoliikkeen ohjausjärjestelmän elektroniikkaa (nostolaite). Tuotannollisista syistä ja siksi että kaikki turvatoiminnon tarvitsemat anturit, logiikkayksiköt sekä muut komponentit löytyvät tästä ohjausjärjestelmän osasta, ei ole haluttu lähteä toteuttamaan turvatoimintoa erillisellä ulkoisella laitteistolla. Suurimmaksi osaksi eriyttäminen muusta järjestelmästä, missä sitä on käytetty, tapahtuu ohjelmoitavan elektroniikan avulla siten että turvatoiminnon ohjelmistot on erotettu muista ohjausjärjestelmän ohjelmistoista. Kuvassa 3.1 on esitetty laitetason arkkitehtuuri turvatoiminnolle.

Kuvassa näkyvät viiva-anturit sijaitsevat fyysisesti omilla piirilevyillään ja ne on kytketty nostolaitteeseen kaapeleilla. Kaikki muu turvatoiminnon tarvitsema elektroniikka sijaitsee nostolaitteen kortilla. Myös lähdössä näkyvät moottorit on kytketty nostolaitteen ulkopuolelle ja ne on yhdistetty nostolaitteeseen kaapeleilla. Kuvan turvakytkennöissä ovat SAFE_LO, SAFE_HI sekä VCC_MC ja VCC_BRK tarkoittavat kytkentöjen sisääntuloja sekä lähtöjä. Vastaavasti ajomootoreissa ovat jarrujännite sekä ohjausjännite tarkoittavat sisääntuloja.

Turvatoiminto toteuttaa laitteiston osalta standardin SFS-EN ISO 13849-1 luokkaa 3 vastaavan arkkitehtuurin vaatimukset. Se sisältää kaksi kanavaa joista toisen logiikkaa ohjaa MSP ja toisen FPGA. Tuloissa on nopeuden valvonta kahdennettu viiva-antureilla. Samoin yläaseman valvonta on kahdennettu AMR-anturien osalta. Rinnakkaisuuden vuoksi yksittäiset virheet eivät johda turvatoiminnon menettämiseen mutta virheen sattuessa turvatoiminto aina suoritetaan.

3.1.1 Alijärjestelmät

Kuvan 3.1 arkkitehtuurista voidaan erottaa kaksi kanavaa sekä kolme alijärjestelmää molemmille kanaville: tulot, ohjauslogiikka ja lähdöt. Turvatoiminnon tulosignaalit koostuvat viiva-antureiden sekä AMR-antureiden datasta. Nopeuden muutoksista saadaan tietoa viiva-antureilla. Niiden toiminta perustuu IR-ledien käyttöön ja ne mittaavat valon heijastuksen muutoksia ajokiskossa olevasta nauhasta. Antureita on kaksi kappaletta, yksi sukkulan edessä ja yksi takana. Nostolaitteessa on lisäksi neljä AMR-anturia jotka ilmoittavat kun kapseli on yläasennossa. Anturit on sijoitettu



Kuva 3.1: Turvatoiminnon laitteistoarkkitehtuuri

fyysisesti nostolaitteen neljään eri kulmaan eli jos sukkula on vinossa eivät kaikki antureista näytä samaa tilaa.

Turvatoiminnon ohjauslogiikka on sijoitettu kahteen eri paikkaan: MSP-mikrokontrollerille sekä FPGA:lle. Viiva-antureiden ja AMR-antureiden kaikki signaalit on kytketty molempiin ohjauslogiikoista. Lähdöt koostuvat turvakytkennoistä joilla ohjataan moottoreiden ohjausjännitettä ja jarrujännitettä. Sekä MSP:llä että FPGA:lla on yksi signaali jolla ne voivat ohjata näitä turvakytkentöjä. Moottorin ohjausjännitettä ohjataan omalla kytkennällään ja jarrujännitettä omallaan, MSP ja FPGA on kytketty näistä molempiin kuten kuvasta 3.1 nähdään. Jos jompikumpi ohjauslogiikoista havaitsee ylinopeustilanteen, se pystyy katkaisemaan jarruilta ja moottoreilta jännitteet.

3.2 Laitteiston toteutus

Tässä kappaleessa on esitetty tarkemmin ylinopeusvahdin laitteiston alijärjestelmät sekä niiden toteutus.

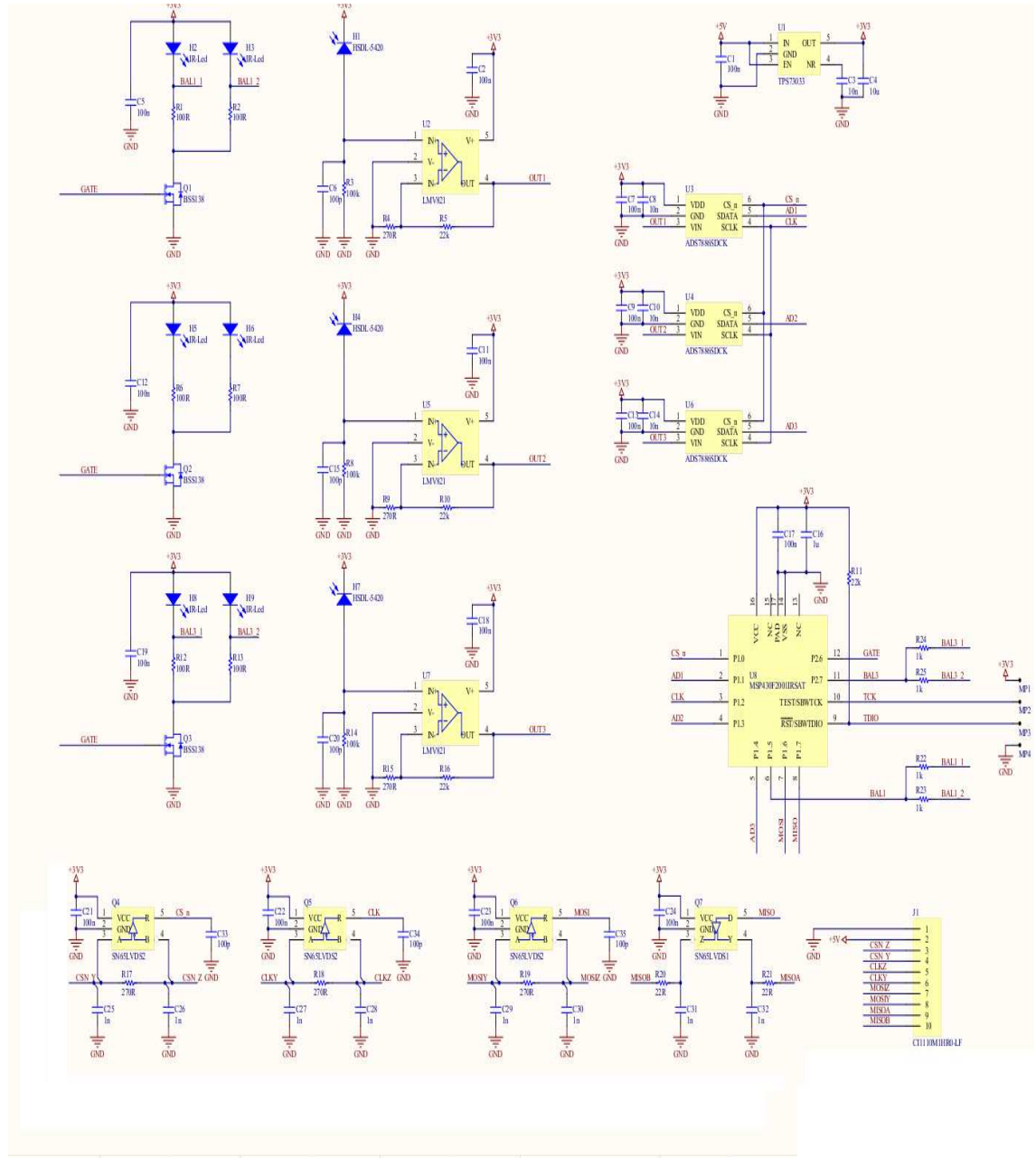
3.2.1 Viiva-anturit

Kuvassa 3.2 on esitetty viiva-anturin piirikaavio. Kuten kuvasta nähdään on anturissa kolme IR-lediä lähetykseen (HSDL-4420, jokainen näistä kahdennettu) sekä kolme IR-lediä vastaanottoon (fotodiodeja HSDL-5420). Lähettävien IR-ledien läpi kulkevaa virtaa ohjataan MOSFET:ien hilalle tuotavalla jännitteellä. Virta halutaan mahdollisimman pieneksi sillä sen suuruus vaikuttaa ratkaisevasti ledien elinikään. Vastaanotossa on fotodiodeja sekä tämän muodostaman virran vahvistukseen operaatiovahvistinkytkentä.

Viiva-anturit toimivat siten että ledit muodostavat lähetin-vastaanotinparin jossa jokaista lähettävää lediä varten on yksi vastaanottava ledi. Vastaanotossa tutkitaan viivanauhasta heijastunutta valoa siten että operaatiovahvistimen ulostuloon muodostuu fotodiodilla havaitun valon intensiteettiä vastaava jännite. Tämä jännite ohjataan edelleen AD-muuntimelle (ADS7886) ja siitä mikrokontrollerin sisääntuloon. Viiva-anturin älyn muodostaa MSP430 mikrokontrolleri jonka kanssa kommunikoidaan SPI-väylän yli turvatoiminnon ohjauslogiikoilla. Kahden viiva-anturin signaalipolut on eriytetty toisistaan eli molemmille on omat kaapelinsa.

3.2.2 Ohjauslogiikka

Ohjauslogiikat toimivat toisistaan erillään ja valvovat toisiaan ristiin siten että toisen vikaantuessa turvatoimintoa ei menetetä. Sekä viiva-anturit että AMR-anturit on kytketty näistä molempiin. Mikäli jompikumpi ohjauslogiikoista havaitsee tilanteen missä sukkula liikkuu ylinopeutta ne kytkvät ajomoottoreiden

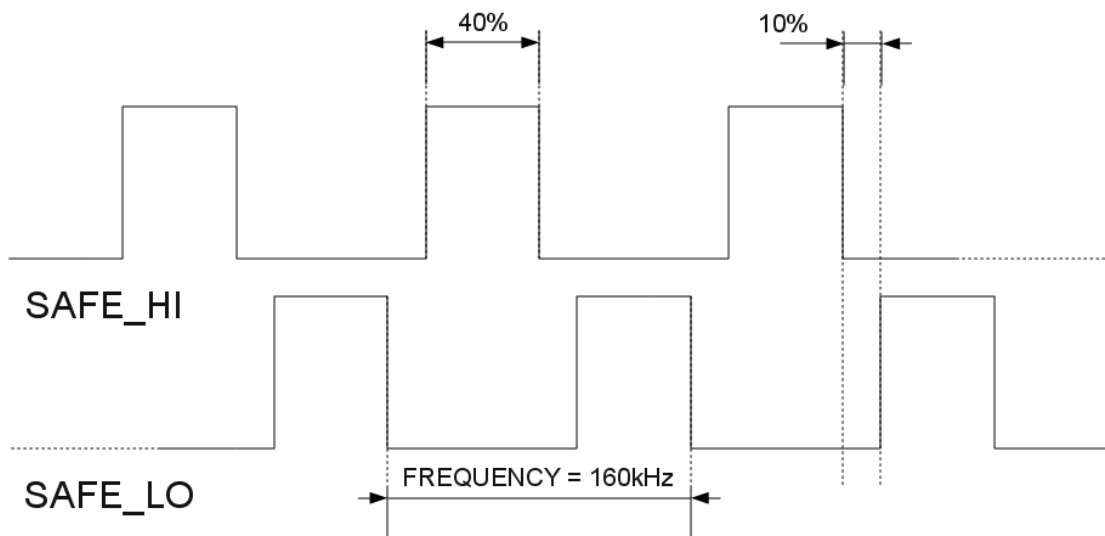


Kuva 3.2: Viiva-anturin piirikaavio

jarruilta jännitteet pois päältä ja katkaisevat moottoreilta tehot. Ylinopeusraja asetetaan kapselin yläaseaman perusteella. Kuvassa 3.1 olevat signaalit SAFE_HI ja SAFE_LO edustavat näitä ohjaussignaaleja.

3.2.3 Lähdön turvakytkentöjen ohjauksen yleinen periaate

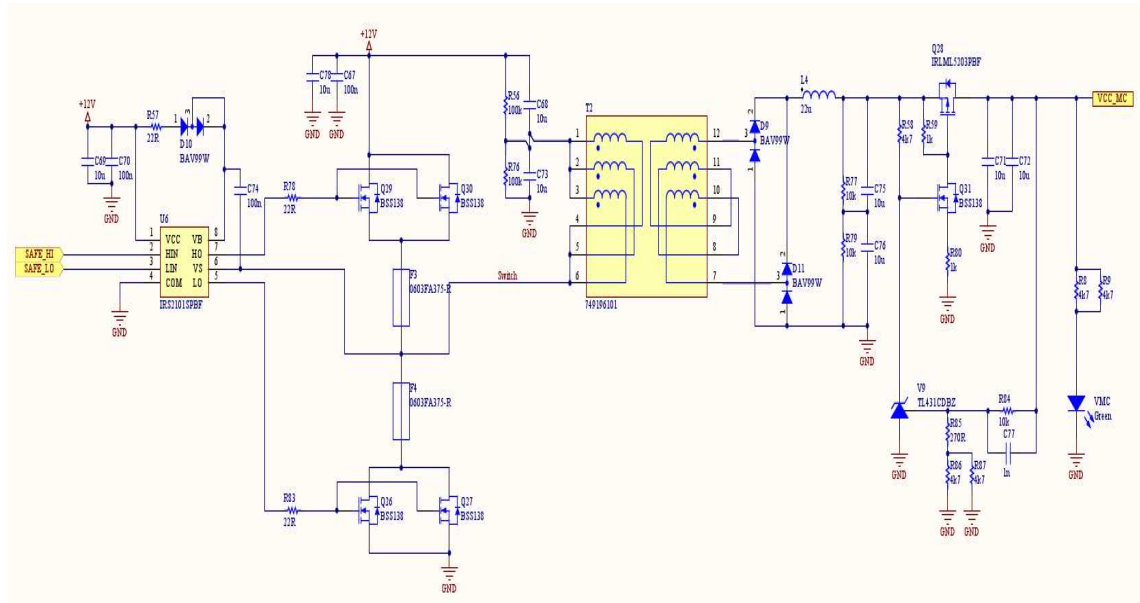
Moottorin ohjausjännitteelle ja jarrujännitteelle on omat turvakytkentänsä. Tämä johtuu siitä että tarvittavat ulostulon jännitetasot ovat erilaiset. Moottorille vaadittava ohjausjännite on 12V kun taas jarrujännite on 105V. Kuvassa 3.3 on esitetty turvakytkentöjen ohjaussignaalien muoto.



Kuva 3.3: Safe-signaalit

Turvakytkentöjen ohjaussignaalit ovat SAFE_HI ja SAFE_LO joista SAFE_LO saadaan MSP:ltä ja SAFE_HI FPGA:lta. Nämä signaalit muodostetaan PWM:llä (Pulse-Width Modulation) siten että molemmat niistä ovat taajuudeltaan ja pulssinleveydeltään samanlaisia, toinen signaaleista on vain viivästetty versio toisesta ja se generoidaan eri ohjauslogiikalla. MSP:llä generoitava SAFE_LO on primaarinen ja se ohjataan turvakytkentöjen lisäksi FPGA:n sisääntuloon jossa siitä luodaan viivästetty versio. Ohjaussignaalit ovat pulssisuhteeltaan 40%, joten aika jolloin molemmat signaaleista ovat alasvedettyinä on 20%. Signaaleissa käytettävän PWM:n taajuus on 160kHz.

Signaalit eivät ole milloinkaan ylhäällä yhtä aikaa, vaan ne ovat vuorotellen ylhäällä ja alhaalla. Mikäli jompikumpi signaaleista ei ole muodoltaan oikeanlaista kanttiaaltoa tai se jää esimerkiksi ylös tai maahan vedetyksi, ei turvakytkentöjen ulostuloon synny oikeanlaista jännitettä. Tästä taas seuraa että jarrut menevät



Kuva 3.4: Turvakytkentä moottorin ohjausjännitteelle

päälle eikä moottoreille siirry tehoa. Ehto sille että turvakytkennän ulostulo on oikeassa tilassa ja jännitteessä on siis että molemmat PWM-signaaleista ovat muodoltaan ja ajoitukseltaan oikeanlaisia. Tämä taas vaatii molempien ohjausloogiikoiden oikeaa toimintaa.

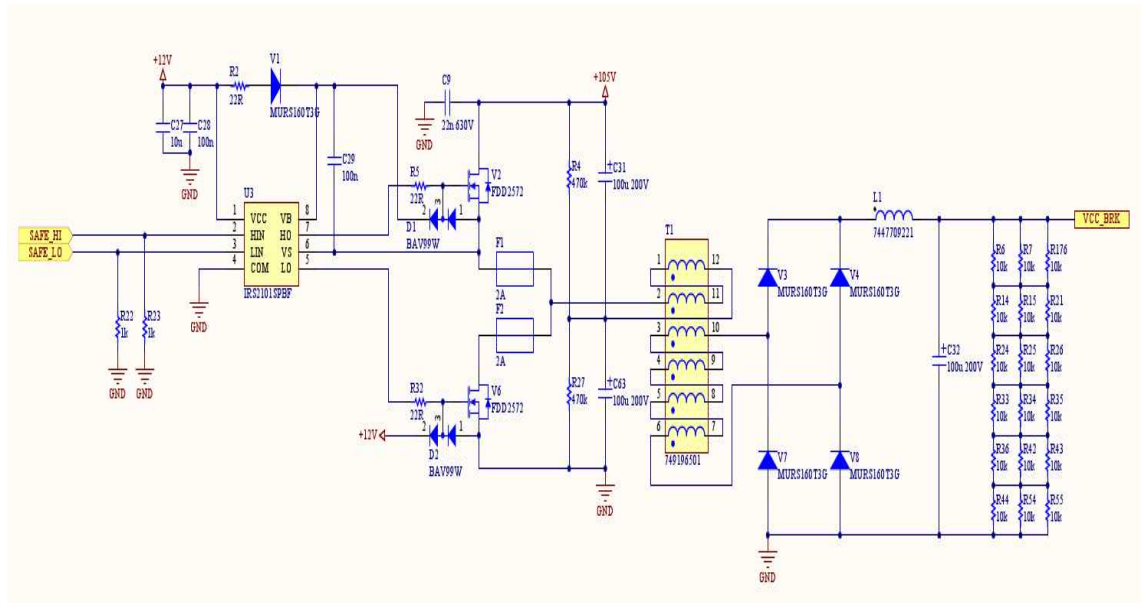
Turvakytkentöjen sisääntulojen SAFE-ohjaussignaalit täytyy asettaa päälle rampilla siten että pulssinleveys kasvatetaan vähän kerrallaan normaaliksi. Mikäli pulssinleveys asetetaan suoraan normaalitilaan, virrat nousevat liian nopeasti ja syöksyvirta hajottaa jarrujen turvakytkennässä olevat kondensaattorit.

3.2.4 Moottoreiden ohjausjännitteen turvakytkentä

Kuvassa 3.4 on esitetty piirikaavio moottoreiden ohjausjännitteen turvakytkennästä. Sisääntulot turvakytkennälle ovat signaalit SAFE_HI ja SAFE_LO. Ulostulo on signaali VCC_MC. Yleisesti turvakytkennän topologiasta voidaan sanoa että se on Buck-tyyppinen step-down hakkuri, jonka sisääntuloina ovat kaksi PWM-kanttialtoa. Vielä tarkemmin hakkuri on push-pull johtuen siitä että jännite hakkurille generoidaan muuntajakytkennällä.

Lähdössä on hakkurin jälkeen LDO (Low-dropout regulator) ja transistorit sen vuoksi etteivät kytkennän jännitehäviöt tiputtaisi ulostulojännitettä alle 12V:n ja toisaalta siksi että ulostulojännite pysyisi vakaasti 12V:ssa. Koska takaisinkytkentää sisääntuloon ei ole, tarvitaan lähdössä regulointi 12V:iin. Muuntajan toisiopuolella oleva jännite voi kuitenkin vaihdella huomattavasti.

Muuntajan ensiöpuolella jännitettä ohjataan kahdella MOSFET-kytkennällä, FET:it on kahdennettu siksi ettei yksittäisen komponentin läpi kulkeva virta olisi lii-



Kuva 3.5: Turvakytkentä moottorin jarrujännitelle

an suuri. Vuorotellen luodaan positiivinen ja negatiivinen huippujännite sisääntulon PWM-signaaleilla jotka sitten tasasuunnataan muuntajan toisiopuolella ja saadaan näin kanttiaalto hakkurille.

Safe-kytkennän sisääntulot on erotettu lähdöistä muuntajalla. Mikäli molemmat sisääntuloista ovat nollassa, ei ulostulossa näy jännitettä. Tällöin ohjaavat FET:it eivät johda ja muuntajan ensiöpuoli kelluu. Jos molemmat sisääntuloista on vedetty ylös, molemmat FET:it johtavat jolloin ylivirta hajottaa sulakkeet eikä ulostulossa näy jännitettä. Sulakkeet suojaavat myös molempia vaiheita erikseen siinä tapauksessa että jommankumman FET:in kautta kulkee ylivirta. DC-jännitteet eivät pääse muuntajakytkennän läpi.

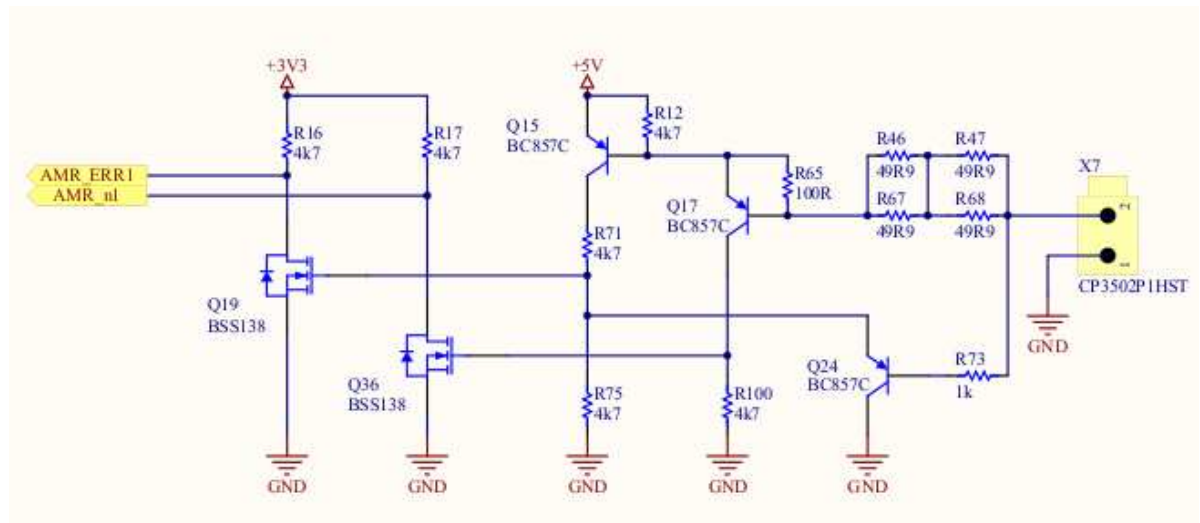
Mikäli vain toinen sisääntuloista on kanttiaaltoa ja toinen vedetty ylös tai mahaan, ei lähtöön muodostu riittävän suurta jännitettä vaan se jää tasasillan ja muuntajan vuoksi liian pieneksi. Jos jompikumpi FET:eistä hajoaa, lähtöön ei muodostu joko ollenkaan jännitettä tai sulake katkaisee piirin ylivirralla.

3.2.5 Jarrujännitteiden turvakytkentä

Kuvassa 3.5 on esitetty piirikaavio jarrujännitteen turvakytkennästä. Sisääntulot turvakytkennälle ovat signaalit SAFE_HI ja SAFE_LO. Ulostulo on signaali VCC_BRK. Kytkentä on hyvin samantapainen kuin moottoreiden ohjausjännitteen tapauksessa. Lähdössä ei ole regulointia siksi että jarrujännitettä ohjataan FPGA:lla sen mukaan miten jännite vaihtelee, joten tässä tapauksessa takaisinkytkentä on olemassa. Sisääntulossa jännitettä ohjaavia FET:tejä on yksi kumpaakin signaalin vaihetta kohti.

3.2.6 AMR-anturit

Kuvassa 3.6 on esitetty piirikaavio yhdelle AMR-anturille. AMR-antureita on neljä kappaletta eli yksi jokaista sukkulan kulmaa varten. Näin voidaan varmistaa että kapseli on suorassa ja ylhäällä kaikkien kulmien suhteen. Anturit on yhdistetty nostolaitteeseen ja ne vaihtavat tilaansa kun kapselin katossa olevat magneetit ovat tarpeeksi lähellä antureita eli kapseli on riittävän ylhäällä. Tällöin signaali AMR_n vaihtaa tilansa alas. Jokaisessa anturissa on myös virhesignaali AMR_ERR joka on ylhäällä mikäli piirin sisääntulo on avoin (anturia ei ole kytketty) tai piirin sisääntulo on oikosulussa.



Kuva 3.6: AMR-anturin piirikaavio

3.3 Laitteiston suoritusasteen laskeminen

Kappaleessa 2.3 on esitetty ne standardin SFS-EN ISO 13849-1 mukaiset parametrit jotka täytyy ottaa huomioon laskettaessa suoritusastea johon järjestelmä kykenee. Tässä kappaleessa on kuvattu tarkemmin parametreja sekä perusteltu arvoja jotka järjestelmälle on laskettu.

3.3.1 MTTF_d

Komponenttien vaarallisten vikaantumisten aikojen (MTTF_d) selvittämiseen käytettiin kahta lähdettä. Kaikissa peruspassiivikomponenteissa kuten FET:issä, vastuksissa, diodeissa, kondensaattoreissa ja kuristimissa käytettiin lähteenä suoraan standardin SFS-EN ISO 13849-1 liitteen C MTTF_d-arvoja sähköisille komponenteille.[10] Niissä IC-piireissä ja komponenteissa joita ei löytynyt standardista on käytetty valmistajien ilmoittamia tai valmistajan antaman kaavan mukaan laskettuja arvoja. Esimerkiksi Texasilla on omille komponenteilleen kattavat luotettavuustiedot, samoin Alteralla. Viiva-antureiden kytkennässä oleville IR-ledeille ei valmistaja ole ilmoittanut suoraan vikaantumisaikojia mutta antaa kuitenkin kaavan jonka avulla voidaan laskea erilaisissa olosuhteissa MTTF_d:t. On huomattavaa että kaikilla komponenteilla käytettiin pahimman mahdollisen tapauksen mukaista vikaantumisaikaa, eli esimerkiksi standardissa ilmoitetuista ajoista on käytetty kymmenen kertaa pienempiä arvoja kuin normaalitapauksessa. Samoin muilla komponenteilla vikaantumisaajat on jaettu kymmenellä, lukuunottamatta IR-LED:ejä, jolloin saadaan entistä tiukemmat rajat ja tätä kautta suurempi varmuus luotettavuudelle.

Yleensä valmistajat ilmoittavat vikaantumisaajat esimerkiksi termeillä B₁₀, FIT, MTTF, MTTF_d tai MTBF. Tässä järjestelmässä kaikkien komponenttien vikaantumisaajat on ilmoitettu MTTF_d-arvoina ja ne on esitetty liitteen A taulukossa A.1.

Viiva-anturin IR-LEDit (HSDL-x42x)

Komponentille ei löytynyt valmistajan ilmoittamaa arvoa. Osramin tekemässä tutkimuksessa on käsitelty LED:ejä yleisesti ja siinä on otettu huomioon muun muassa ympäristöolosuhteet sekä mahdolliset vikaantumiset asennuksessa ja ennen käyttöönottoa. [14] Tutkimuksesta voidaan havaita esimerkiksi että LED:ien elinikä noudattelee niin kutsuttua bathtub-käyrää jossa suurin osa LED:istä vikaantuu eliniän alussa ja lopussa. Huonoimmat MTTF_d-arvot ovat tyypillisesti kymmenien vuosien luokkaa normaaliolosuhteissa (lämpötila, virta).

IR-LED:ien valmistaja Avago antaa menetelmän vikaantumisen ennustamiseksi Arrheniuksen kaavalla ja Weibullin tilastollisella analyysillä. Kaavalla (3.1) saatava TTF ilmoittaa vikaantumisen kilotunteina HSDL-4420 tyyppin lähettävälle IR-LED:ille. [15]

$$MTTF = \frac{A}{I} \exp\left(\frac{E_a}{k} \left(\frac{1}{278 + 125^\circ} - \frac{1}{T}\right)\right) \quad (3.1)$$

A on vakio jolle valmistaja on ilmoittanut arvon 200 kilotuntia johon mennessä 1% komponenteista on vikaantunut. Ledi katsotaan vikaantuneeksi kun sen lähettämän valon määrä on pudonnut puoleen alkuperäisestä. I kertoo ledin läpi kulkevan virran joka turvakytkenässä on 9mA, Boltzmannin vakio $k = 8.62E-5eV$, aktivaatioenergia $E_a = 0.43eV$ ja ympäristön maksimilämpötila $T = 50^\circ C$. Näillä arvoilla saamme $MTTF_d$:ksi 46-vuotta. Lämpötila jolla verrokkidata on valmistajan testissä laskettu on $125^\circ C$. Tässä järjestelmässä ympäristön maksimilämpötilaksi on kiinnitetty $50^\circ C$.

Samoja elinikäitietoja saadaan myös Avagon designer's guidesta. [16] Vastaavasti HSDL-5420 tyyppin vastaanottavia IR-ledejä voidaan verrata esimerkiksi Avagon fototransistoreihin joiden luotettavuusdatalehddestä saadaan ledeille tätä järjestelmää vastaavissa olosuhteissa $MTTF_d$:ksi 66-vuotta. [17] Yleisesti erilaisille optisille komponenteille on arvioitu vikaantumisaikoja esimerkiksi Rome air development centerin raportissa. [18] Fototransistoreille saatiin näissä testeissä yli 100 vuoden elinikä, joten 66 vuotta on hyvin tämän rajan alapuolella.

3.3.2 DC_{avg}

Turvatoimintojen valvonta suoritetaan MSP ja FPGA ohjauslogiikoidan sisään-tulojen perusteella. Tässä järjestelmässä yksittäisiä komponentteja mallinnetaan myös alijärjestelmien kautta siten että ne voivat koostua useista fyysisistä komponenteista. Esimerkiksi viiva-anturi käsitetään yksittäisenä komponenttina, samoin lähtöjen turvakytkenät. Tällä tavalla valvonnan tasoa ei tarvitse määrittellä jokaiselle fyysiselle komponentille erikseen vaan se voidaan huomioida alijärjestelmän tulojen ja lähtöjen perusteella. Laskennassa käytetään erilaisia menetelmiä riippuen siitä onko kyseessä tulo, logiikka vai lähtöyksikkö. Seuraavaksi otamme tarkasteluun turvatoiminnon alijärjestelmät ja määrittelimme niille DC_{avg} :n. Kohdat joita voidaan soveltaa DC_{avg} :n laskentaan löytyvät standardin SFS-EN ISO 13849-1 liitteestä E.

Tulot (tuloyksikkö)

Viiva-antureiden signaalipolut on eriytetty toisistaan, joten vika yhdessä anturissa ei normaalisti vaikuta toisen anturin tuottamaan dataan. Myös AMR-antureiden signaalipolut on eriytetty toisistaan. Viiva-anturit sisältävät mikrokontrollerin jolla jokaiseen siirrettävään datapakettiin saadaan lisättyä CRC-tarkistus. Sekä viiva-anturit että AMR-anturit on reititetty ohjauslogiikoista molempiin ja näillä logiikoilla verrataan ristiin antureiden tuottamaa dataa.

Viiva-antureiden $MTTF_d$ on IR-ledeistä johtuen matala, joten DC_{avg} :sta täytyy saada vähintään 90% viiva-antureiden alijärjestelmälle. Antureihin voidaan soveltaa standardista diagnostiikan kattavuudelle kohtaa : - "Jos oikosulkuja ei voida paljastaa, tulosiinaalien ristiinvalvonta yhdessä dynaamisen testauksen kanssa (useille I/O-yksiköille) 90%"[10]

Ohjauslogiikka (logiikka)

MSP-mikrokontrolleri ja FPGA valvovat toisiaan ristiin. Lisäksi ne tarkastavat sekä sisääntulosignaalien että ulostulosignaalien tilojen mielekkyyttä. $MTTF_d$ on tällä alijärjestelmällä keskimääräinen joten DC_{avg} :sta täytyy saada vähintään 60%. Ristiinvalvonnasta johtuen voidaan soveltaa standardin kohtaa: - "Logiikan toiminnan tilapäinen yksinkertainen valvonta (esim. ajastinvahti jolloin liipaisukohdat ovat logiikan ohjelmassa) 60%"[10]

Lähdöt (lähtöyksikkö)

Turvatoimintojen lähdöt pitävät sisällään jarrujännitteen ja moottorin ohjausjännitteen turvakytkenät. Koska näistä molemmilla saadaan yksittäin turvatoiminnot suoritettua, voidaan ajatella signaalin sulkupolun olevan redundantti. Lisäksi molempien turvakytkenöiden ulostuloja valvotaan FPGA-ohjauslogiikalla. $MTTF_d$ on tällä alijärjestelmällä keskimääräinen joten DC_{avg} :sta täytyy saada vähintään 60%. Standardista sovelletaan kohtaa: - "Redundanttinen signaalin sulkupolku yhden toimilaitteen valvonnalla joko logiikan tai testauslaitteen avulla 90%"[10]

3.3.3 CCF

Standardissa SFS-EN ISO 13849-1 oletetaan CCF:ää laskettaessa redundanttisten järjestelmien osalta että standardin IEC 61508-6:2000 liitteessä D esitetty β -tekijä on enintään 2%. Liitteen B taulukoissa B.1, B.2 ja B.3 on esitetty ne standardin IEC 61508-6:2000 taulukon D.1 kohdat joita on käytetty β -tekijän laskennassa. Yhteispisteet saadaan summaamalla taulukoiden X -ja Y-termit. X-termiin vaikuttaa lisäksi termi Z, jonka suuruuden määrää diagnostiikan taso ja vaste. Yhden rivin pisteet voidaan laskea standardin IEC 61508-6:2000 kaavalla $S = X(Z + 1) + Y$. Tässä käytetään Z:lle kerrointa 1 joka perustuu standardin taulukoihin D.2 ja D.3. Diagnostiikka toteutuu ristiinvalvonnan kautta jonka vaste on alle minuutin. Standardin IEC 61508-6:2000 taulukoissa E.1 ja E.2 on esitetty lisää tekijöitä joilla voidaan vaikuttaa β :n suuruuteen.

Taulukossa 3.1 on vastaavasti esitetty ne arviointiperusteet joita standardista SFS-EN ISO 13849-1 on sovellettu laskettaessa pisteitä CCF:lle. Seuraavaksi arvioimme järjestelmää yhteisvikaantumisen kannalta ja tutkimme kohtia joista pisteitä on annettu sekä perusteluita pisteiden antamiselle.

Taulukko 3.1: Pisteet CCF:lle

Arviointiperuste	Alakohta	Pisteet
Erottelu/erottaminen	-	15
Erilaisuus (diversiteetti)	-	20
Ympäristöolosuhteisiin liittyvät toimenpiteet	Häiriönsieto	25
	Muut vaikutukset	10
Yhteensä		70

Erottelu / erottaminen

Ehtona on signaalireittien fyysinen erottaminen:

- johdotuksen/putkituksen erilleen sijoittaminen
- riittävät ilma -ja pintavälit piirilevyissä [10].

Jokaisen viiva-anturin signaalit nostolaitteelle on sijoitettu omaan kaapeliinsa. Piirilevyillä pintavälit on toteutettu standardien IEC 60664-3:2003/A1:2010 ja EN 50178 mukaisesti. [19] [20]

Erilaisuus (diversiteetti)

Ehtona pisteiden antamiselle on "erilaisten teknologioiden, toteutustapojen tai fyysisten periaatteiden käyttö"[10]. Järjestelmässä on käytetty erilaisuutta ohjauslogiikassa ja lähdöissä seuraavasti: Ohjauslogiikka sisältää kaksi teknologiaaltaan erilaista yksikköä; MSP-mikrokontrollerin ja FPGA:n. Lähtöjen turvakytkenät on eriytetty toisistaan.

Suunnittelu, soveltaminen ja kokemukset

Kohdasta ei ole otettu pisteitä mukaan laskentaan ylijännitteiden vaikutusten vuoksi. Tässä on kuitenkin esitetty asioita jotka on huomioitu turvatoiminnossa kohtaan liittyen. Osio on jaettu standardissa kahteen eri kohtaan, joista ensimmäinen käsittää suojaustoimenpiteet esimerkiksi ylijännitteelle, paineelle ja niin edelleen. Toinen kohta pitää sisällään hyvin koetellut komponentit jota ei voida ottaa huomioon. Suojaustoimenpiteistä joita turvatoiminnossa on käytetty voidaan mainita seuraavaa:

- Erotusmuuntaja isoloi turvatoiminnon kaikki osat verkkosähköstä hakkuria lukuunottamatta
- Verkkosyötössä on sulakkeet jotka estävät ylivirran
- Poikkeavat käyttöjännitteet eivät aiheuta molempien logiikoiden yhtäaikaista vaarallista vikaantumista. MSP:n datalehden mukaan sen maksimijännite on 3.6V, FPGA:n datalehden mukaan vastaavasti 3.9V. [21] [22]
- Moottoreiden vaihevirran ylivirtasuojia, joka on toteutettu raudalla

- Välipiirin yli -ja alijännitteiden valvonta, joka on toteutettu VHDL:llä
- Nostoliikkeen laskuvaiheessa suojautuminen generoituvilta tehoilta piirilevyllä päin kun syöttöjännitteet katoavat
- Nostoliikkeen nostovaiheessa jännitteen laskeminen havaitaan kun syöttöjännitteet katoavat

Ympäristöolosuhteisiin liittyvät toimenpiteet

Tämä on jaettu kahteen eri kohtaan joista ensimmäinen sisältää likaantumisen estämisen sekä sähkömagneettisen yhteensopivuuden soveltuviin standardien mukaisesti. Toinen kohta sisältää kaikkien muiden ympäristövaikutusten huomioonottamisen joita ovat esimerkiksi lämpötila, iskut, värinä ja kosteus. Ensimmäistä kohtaa sovellettaessa järjestelmässä toteutuu:

- Nostolaite on suojattu liialta ja pölyltä koteloinnilla sekä lakkauksella jolla saavutetaan likaisuusluokka 1. [19]

Häiriönsieto on huomioitu koko järjestelmän osalta soveltuviin EMC-standardien mukaisesti. Seuraavassa on lueteltu häiriönsiedon eri muodot sekä luokitukset jotka järjestelmälle pyritään saavuttamaan EMC-testeissä.

Häiriötyyppi	Saavutettava taso	Standardi
Säteilevien häiriöiden emissio	luokka A	[23]
Säteilevien häiriöiden immunitetti	3V/m 80% AM, modulation on, 1kHz	[24]
Johtuvien häiriöiden emissio	luokka B	[23]
Johtuvien häiriöiden immunitetti	10V 80% AM, modulation on, 1kHz	[25]
Nopeiden transienttien sieto	$\pm 1\text{kV}$	[26]
Suurten jännitteiden sieto	$\pm 1\text{kV}$ line to earth, $\pm 0,5\text{kV}$ line to line	[27]

Toista kohtaa sovellettaessa toteutuu:

- Kotelo suojaa värinältä, iskuilta ja lämmöltä [19]

3.3.4 Järjestelmän suoritustaso

Ylinopeusvahdille laskettiin SISTEMA:lla PFH:ksi (Probability of Failure per Hour) $2.66\text{E}-6$ joka vastaa suoritustasoa C. Ylinopeusvahdin vikaantumisaikat on esitetty taulukossa 3.2. Taulukoissa on esitetty myös alijärjestelmien PFH-arvot joissa on otettu huomioon kaikki vikaantumisiin vaikuttavat tekijät kuten MTTF_d , DC_{avg} ja CCF. DC_{avg} :lle käytettyjä kohtia on perusteltu kappaleissa 3.3.2 sekä 4.7. CCF:lle

saatiin 70 pistettä, arviointiperusteet selviävät taulukosta 3.1.

Taulukko 3.2: Ylinopeusvahdin alijärjestelmien $MTTF_d$ -arvot

Alijärjestelmä	$MTTF_d$ [a]	PFH [1/h]	DC_{avg}
Viiva-anturit	8.24	1.73E-6	90%
Ohjauslogiikka	100	1.01E-7	60%
Safety-lähdöt	29.04	7.26E-7	60%
AMR-anturit	100	1.01E-7	90%
Yhteensä		2.66E-6	81%

3.4 Vika -ja vaikutusanalyysi (FMEA)

Vika -ja vaikutusanalyysin, FMEA (A failure modes and effects analysis), tarkoituksena on selvittää minkälaiset viat voivat johtaa jonkin huipputoiminnon menettämiseen ja mitä siitä seuraa järjestelmän toiminnan kannalta. Tässä tapauksessa ylinopeusvahti on huipputoiminto ja taulukoissa 3.3, 3.4 ja 3.5 on määritelty vikoja jotka voivat johtaa sen menettämiseen.

Analyysissä on otettu huomioon komponentti, toiminto josta/joista se huolehtii, vikamuoto, vaikutus joka toiminnon menettämisestä seuraa sekä menetelmä jonka kautta vika havaitaan. Havaitsemismenetelmät viittaavat kappaleisiin ohjelmiston määrittelyssä ja diagnostiikkaan. Lähdön SAFE-turvakytkennöissä havaitsemismenetelmiä ei ole huomioitu sillä komponenttien vikaantumiset näissä kytkennöissä johtavat turvalliseen tilaan. Vika -ja vaikutusanalyysi on tehty standardin IEC 60812:2006 pohjalta. [28]

Taulukko 3.3: Vika -ja vaikutusanalyysi

Komponentti	Toiminto	Vikamuoto	Vaikutus	Paljastuu
Viiva-anturi	Datan lukeminen ajokiskon nauhasta	Mikrokontrolleri hajooa Kaapeli hajooa AD-muunnin ADS7886SDCK hajooa Operaatiovahvistin LMV821 hajooa Fotodiiodi HSDL-5420 hajooa IR-lähetin HSDL-4420 hajooa Passiivikomponentti hajooa	Ei saada dataa anturilta Ei saada dataa anturilta Data vääristynyt Data vääristynyt Data vääristynyt Data vääristynyt Data vääristynyt Data vääristynyt	CRC-tarkastus, 4.5.7 CRC-tarkastus, 4.5.7 Nopeuksien vertailu, 4.5.5 Nopeuksien vertailu, 4.5.5 Nopeuksien vertailu, 4.5.5 Nopeuksien vertailu, 4.5.5 Nopeuksien vertailu, 4.5.5
		Ajokiskon teipin vikaantuminen	Data vääristynyt	Nopeuksien vertailu, 4.5.5

Taulukko 3.4: Vika -ja vaikutusanalyysi

Komponentti	Toiminto	Vikamuoto	Vaikutus	Paljastuu
AMR-anturi	Kapselin yhden kulman yläasema	Kaapeli irtoaa	Ei saada anturilta dataa	ERR-signaali, 4.5.6
		Oikosulku kaapelissa	Ei saada anturilta dataa	ERR-signaali, 4.5.6
		Passiivikomponentit hajoavat	Anturin tuottama data virheellistä	ERR-signaali + muut AMR:it, 4.5.6
FPGA	Nopeuden laskenta Yläaseman päättely Safe-signaalin ohjaaminen	Looginen vika ohjelmassa	Lasketaan virheelliset nopeudet	Nopeuksien vertailu, 4.5.5
		Looginen vika ohjelmassa	Lasketaan virheellinen yläasema	Maksiminopeuden valinta, 4.5.6
		Looginen vika ohjelmassa	Virheellinen ohjaus	Lähtöjen tarkkailu toisella ohjauslogiikalla, 4.7
MSP	Nopeuden laskenta Yläaseman päättely Safe-signaalin ohjaaminen	FPGA hajooa	Toinen kanava poistuu käytöstä	Ristiinvalvonta toisen ohjauslogiikan kanssa, 4.7
		Looginen vika ohjelmassa	Lasketaan virheelliset nopeudet	Nopeuksien vertailu, 4.5.5
		Looginen vika ohjelmassa	Lasketaan virheellinen yläasema	Maksiminopeuden valinta, 4.5.6
MSP	Nopeuden laskenta Yläaseman päättely Safe-signaalin ohjaaminen	Looginen vika ohjelmassa	Virheellinen ohjaus	Lähtöjen tarkkailu toisella ohjauslogiikalla, 4.7
		Looginen vika ohjelmassa	Toinen kanava poistuu käytöstä	Ristiinvalvonta, 4.7
		MSP hajooa	Toinen kanava poistuu käytöstä	Ristiinvalvonta, 4.7

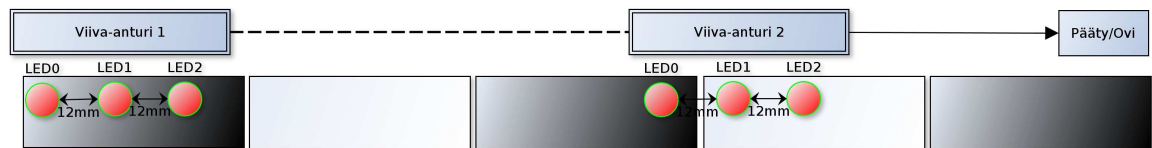
Taulukko 3.5: Vika- ja vaikutusanalyysi

Komponentti	Toiminto	Vikamuoto	Vaikutus	Paljastuu
SAFE-moottorijännite	Moottorin ohjauksen ohjaaminen	Sisääntulon FET:eistä Q29, Q30, Q26, Q27 menee oikosulkuun Sisääntulon FET:eistä Q29, Q30, Q26, Q27 jää pysyvästi johtamattomaan tilaan Sisääntulon MOSFET U3 hajooa Lähdön tasasuuntaussillan diodi(t) D9, D11 menee oikosulkuun Lähdön tasasuuntaussillan diodi(t) D9, D11 muodostaa avoimen piirin Lähdön LDO Q28 hajooa	Sulake F1/F2 hajooa Ulostuloon ei muodostu riittävän suurta jännitettä Sulakkeet F1/F2 hajoaavat tai ulostuloon ei siirry tehoa Sisääntulossa sulake F1/F2 hajooa Tehoa ei siirry Tehoa ei siirry, turvallinen vikaantumien	
SAFE-jarrujännite	Moottorin jarruohjauksen ohjaaminen	Sisääntulon FET:eistä V2 ja/tai V6 menee oikosulkuun Sisääntulon FET:eistä V2 ja/tai V6 jää pysyvästi johtamattomaan tilaan Sisääntulon puolisuuntaussillan diodi(t) IRS2101SPBF U3 hajooa Lähdön tasasuuntaussillan diodi(t) V3, V4, V7, V8 menee oikosulkuun Lähdön tasasuuntaussillan diodi(t) V3, V4, V7, V8 muodostaa avoimen piirin	Sulake F3/F4 hajooa Ulostuloon ei muodostu riittävän suurta jännitettä Sulakkeet F3/F4 hajoaavat tai ulostuloon ei siirry tehoa Sisääntulossa sulake F3/F4 hajooa Tehoa ei siirry, jarrut menevät kiinni	

4. YLINOPEUSVAHDIN OHJELMISTO

4.1 Nopeuden laskenta viiva-antureilla

Kuvassa 4.1 on periaatekuva viiva-antureiden ledeistä sekä nauhasta jota niillä tutkitaan.



Kuva 4.1: Nostolaitteen viiva-anturit ja ajokiskon nauha

Käytössä on kaksi viiva-anturia ja nopeutta lasketaan näillä molemmilla itsenäisesti. Laskenta suoritetaan niiden aikojen perusteella jolloin kaksi peräkkäistä lediä ovat ylittäneet jonkin nauhan muutoskohdan. Kahden peräkkäisen ledin välimatka on 12mm. Nauhan yhden osan pituus on normaalisti 36mm. Kun aika jolloin ensimmäinen ledi havaitsee muutoskohdan on t_1 ja seuraavan ledin muutosajankohta on t_2 , sekä tunnetaan ledien välinen etäisyys s , saadaan nopeus laskettua kaavalla:

$$v = \frac{s}{t_2 - t_1} \quad (4.1)$$

Mittauksessa syntyviä epätarkkuuksia voidaan arvioida matemaattisesti esimerkiksi osittaisdifferentiaalilin avulla kaavan (4.2) mukaisesti jolla saadaan laskettua nopeus virherajoineen.

$$\begin{aligned} v &= \frac{s}{t_2 - t_1} \pm \Delta v \\ \Leftrightarrow \Delta v &= \sum_{i=0}^N \left(\frac{\partial v}{\partial x_i} \Delta x_i \right) \\ &= \frac{\partial v}{\partial t} \frac{s}{t_2 - t_1} \Delta t + \frac{\partial v}{\partial s} \frac{s}{t_2 - t_1} \Delta s \\ &= \frac{-s}{(t_2 - t_1)^2} \Delta t + \frac{1}{(t_2 - t_1)} \Delta s \end{aligned} \quad (4.2)$$

Käytettäessä kaavaa 4.1 on kahdesta ajasta laskettu nopeus virheellinen mikäli

kappale on kiihtyvässä liikkeessä. Viiva-antureilla lasketun ja todellisen nopeuden välistä virhettä voidaan arvioida kaavalla (4.3).

$$\Delta v_{kiihtyvyyys} = at_2 - \left(\frac{s}{t_2 - t_1} \pm \Delta v \right) \quad (4.3)$$

Kiihtyvyyden aiheuttama suhteellinen virhe nopeuteen voidaan laskea kaavaa (4.3) soveltaen kaavalla (4.4)

$$\begin{aligned} v &= 1 - \frac{s_{ledit}}{(t_2 - t_1) at_2} \frac{1}{at_2} \\ &\Leftrightarrow 1 - \frac{s/3}{\left(\sqrt{\frac{2(sn+1)}{a}} - \sqrt{\frac{2s}{a}} \right) a \sqrt{\frac{2(sn+1)}{a}}} \frac{1}{a \sqrt{\frac{2(sn+1)}{a}}} \\ &\Leftrightarrow 1 - \frac{1 + \sqrt{\frac{3n}{3n+1}}}{2} \end{aligned} \quad (4.4)$$

Kaavassa (4.4) n on nauhojen pituuksien n :nnes monikerta, s nauhan pituus ja $s/3$ on kahden ledin etäisyys toisistaan. Supistetusta kaavasta nähdään että vakiomatkan pituus s ja kiihtyvyyys eivät vaikuta nopeuden suhteelliseen virheeseen. Virheen suuruus määräytyy kuljetun matkan monikertojen mukaisesti ja pienenee mitä kauemmas ollaan kuljettu. Alhaisilla nopeuksilla virheellä ei ole merkitystä ja vastaavasti suurilla nopeuksilla, jossa ylinopeus on havaittava tarkasti, virheen suuruus suhteessa todelliseen nopeuteen muuttuu marginaaliseksi peräkkäisten mittausten välillä.

Epäideaalisuudet kuten poikkeama ledien välisessä etäisyydessä sekä väärin mitatut ajat aiheuttavat lisää virhettä suhteessa todelliseen nopeuteen. Kun otetaan kaavaan (4.4) mukaan epäideaalisuudet voidaan suhteellinen virhe laskea kaavalla (4.5).

$$v = 1 - \left(\frac{s_{ledit}}{(t_2 - t_1)} \pm \Delta v \right) \frac{1}{at_2} \quad (4.5)$$

Sen lisäksi että kiihtyvyyys aiheuttaa virhettä yhdellä viiva-anturilla laskettuun nopeuteen, se aiheuttaa myös poikkeamaa kahdella viiva-anturilla laskettuihin nopeuksiin siten että ne eivät ole koskaan samat. Poikkeama johtuu siitä että kahden viiva-anturin ledien etäisyydet seuraavaan mittaushetkeen ovat erisuuruiset. Nopeuksien poikkeama voidaan laskea kaavalla (4.6)

$$\Delta v_{viiva-anturit} = \left[\left(\frac{s_2}{t_4 - t_3} \pm \Delta v_2 \right) - \left(\frac{s_1}{t_2 - t_1} \pm \Delta v_1 \right) \right] \quad (4.6)$$

Δv lasketaan kaavalla (4.2), s_2 ja s_1 ovat ledien etäisyydet jotka kiinnitetään samaan vakioarvoon $s=12\text{mm}$ ja ajat t_4, t_3, t_2, t_1 mitataan niistä kohdista kun kahden viiva-anturin peräkkäiset ledit ylittävät reunan.

4.2 Virherajat ja rajoitukset

Vaatusmäärittelyssä on asetettu toleranssiksi mitattavalle ylinopeudelle $v_{max} \pm 10\%$. [3] Tämä tarkoittaa käytännössä sitä että ylinopeus tunnustetaan tilanteessa jossa mitattava nopeus on maksimissaan joko 10% pienempi tai 10% suurempi kuin todellinen nopeus. Turvatoiminnon kannalta kuitenkin vain tilanne jossa todellinen nopeus on suurempi kuin laskettu nopeus on vaarallinen. Yhdellä viiva-anturilla mitatun nopeuden virherajojen lisäksi etsitään virherajat kahdella viiva-anturilla mitattujen nopeuksien poikkeamalle toisistaan. Tutkittavat nopeudet ovat $1.0\frac{m}{s}$ joka on matalin asetettava maksiminopeus, $3.0\frac{m}{s}$ joka on suurin asetettava maksiminopeus sekä $1.25\frac{m}{s}$ jota käytetään nykyisessä varastojärjestelmässä maksiminopeutena. Sekä maksiminopeuden että nopeuksien poikkeaman suhteen käytetään turvatoiminnossa absoluuttiarvoja joihin viiva-antureilla mitattuja nopeuksia verrataan. Mikäli arvot ylittyvät suoritetaan turvatoiminto.

Mittausepäätarkkuuksista johtuvat virheet

Kaavalla (4.2) voidaan laskea mittausepäätarkkuuksista johtuvan virheen suuruus vakionopeudella. Kun poikkeama ledien etäisyydessä on 1mm ideaalisesta ja poikkeama ajassa $1\mu s$ saadaan eri nopeuksille taulukon 4.1 mukaiset virherajat.

Taulukko 4.1: Virherajat

Nopeus (m/s)	Virhe \pm	Virhe %
1.0	0.083	8.33
1.25	0.104	8.32
3.0	0.25	8.31

Näissä virheen suuruus on noin 8% nopeudesta. Vastaavasti poikkeaman ollessa 2mm virheen suuruus kasvaa 16%:iin. Tällä perusteella ledien välillä ei hyväksytä yli 1mm:n poikkeamaa sillä toleranssit ovat $\pm 10\%$. Kiihtyvyyden aiheuttama lisäys virheeseen korostuu pienillä nopeuksilla, nopeuden kasvaessa virhe pienenee ja suurilla nopeuksilla pysytään 10%:n sisällä.

IR-ledien ladonnasta vastaava yritys on ilmoittanut että ledien paikka piirilevyllä voi vaihdella maksimissaan ledille tarkoitettujen padien leveyden verran. Koska kaksi lediä voivat poiketa pahimmassa tapauksessa eri suuntiin tämän leveyden verran on poikkeama ledien etäisyydelle ideaalisesta arvosta maksimissaan $2pad$ joka ei

saa ylittää 1mm:ä.

Kiihtyvyyden aiheuttama virhe

Kiihtyvyyden aiheuttama virhe suhteessa todelliseen nopeuteen saadaan kaavalla (4.4). Virheen suuruus ensimmäisessä mittauskohdassa voi olla maksimissaan 50%, eli silloin kun $n=0$. Näin suuri virhe saadaan kuitenkin vain liikkeellelähdetessä eikä virheen suuruudella ole tällöin merkitystä sillä nopeus on alussa hyvin pieni. Kymmenennessä mittauspisteessä, kun $n=10$, virheen suuruus on enää 1%:n luokkaa.

Virhe voidaan laskea edellä mainitulla tavalla silloin kun mittausepä tarkkuuksia ei ole eli mitatut ajat ovat tarkkoja ja ledien väliset etäisyydet ovat todellisuudessa täsmälleen samat kuin laskennassa käytettävät arvot. Mikäli poikkeamaa ledien etäisyydessä on 1mm ja poikkeamaa ajassa 1μ , on virhe kaavan 4.5 mukaisesti 10% nopeudella 1m/s. Nopeuden kasvaessa virhe pienenee. Edellä on määritelty että poikkeama ei saa olla yli 1mm, joten virhe säilyy vaatimusmäärittelyssä esitetyn 10%:n virherajoissa kun maksiminopeus on pienimmillään 1.0m/s. Nämä virherajat on laskettu pahimmassa mahdollisessa tapauksessa teoreettisella kiihtyvyyden huippuarvolla $3.2\frac{m}{s^2}$.

Nopeuksien poikkeama kahdella viiva-anturilla

Kahdella viiva-anturilla mitattujen nopeuksien poikkeama voidaan laskea kaavalla (4.6). Pahin mahdollinen tapaus saadaan silloin kun lähdetään levosta liikkeelle jolloin kiihtyvyyden aiheuttama virhe on suurimmillaan ja kun samalla viiva-antureiden etummaisten aikaa mittaavien ledien poikkeama toisistaan suhteessa seuraavaan reunaan on suurin mahdollinen. Oletetaan että kiihtyvyys on $3.2\frac{m}{s^2}$ ja etummaisten ledien poikkeama toisistaan on 3.4cm siten että toisen viiva-anturin lähin reuna on 3.5cm:n päässä ja toisen viiva-anturin 0.1cm:n päässä. Luku on valittu siten että molemmilla viiva-antureilla jää vähintään 1mm:n etäisyys reunaan 3.6cm:n nauhanosalla jotta bitti tulkitaan yksiselitteisesti AD-muunninarvon mukaan joko 1:ksi tai 0:ksi.

Jos edelleen ledien välinen etäisyys poikkeaa ideaalisesta arvosta molemmilla viiva-antureilla 1mm siten että toisen $s_{ledit} = 13mm$ ja toisen $s_{ledit} = 11mm$ saadaan kaavasta (4.6) nopeuksien erotukseksi ensimmäisessä nopeuden mittauskohdassa 0.28m/s. Absoluuttinen virhe kasvaa sitä mukaa kuin nopeuskin ja esimerkiksi nopeudella 1.25m/s on nopeuksien erotuksen suuruus 0.30m/s. Vastaavasti nopeudella 3m/s on nopeuksien erotuksen suuruus 0.49m/s. Absoluuttiarvoksi johon nopeuksien erotusta verrataan kapselin ollessa ylhäällä kaikilla maksiminopeuksilla valitaan 0.5m/s suurimman asetettavan maksiminopeuden 3m/s mukaisesti.

Turvatoiminnon reagointiaika

Se, millä vasteella turvatoiminto reagoi, riippuu sukkulan nopeudesta. Uusi päätös siitä suoritetaanko turvatoiminto vai ei voidaan tehdä kun viiva-anturin peräkkäisillä ledeillä on laskettu uusi nopeus nauhanosan reunasta. Reunojen välimatka on normaalisti 3.6cm joten uusi arvo nopeudelle saadaan tällä resoluutiolla.

Viiveet sisääntuloista ohjauslogiikkaan ja edelleen lähtöihin ovat niin pieniä että ne eivät virheen suuruuteen juuri vaikuta. Virherajojen laskennassa käytetään tässä arvoa $1\mu s$ signaaliviiveille, joka on riittävän suuri, sillä FPGA:n kellotaajuus on 50Mhz ja MSP:n vastaavasti 16Mhz. Uusi muutos voidaan rekisteröidä 4.545kHz:n taajuudella viiva-anturin nopeudesta johtuen. Koska reunan tunnistukseen käytetään kolmea peräkkäistä arvoa, on ajan poikkeama 0.7ms suhteessa siihen reunaan joka ylitettäessä voidaan laskea uusi nopeus. Vakionopeudella tämä näytteistys aiheuttaa offset-virheen ajassa, mutta koska nopeus mitataan kahdella ledillä, virhe kompensoituu. Kiihtyvässä liikkeessä näytteistystaajuus aiheuttaa kuitenkin virhettä mitatussa nopeudessa.

Taulukossa 4.2 on esitetty reagointiajat eri nopeuksille yhden nauhanosan matkalla kun nauhanosan pituus on 3.6cm ja kiihtyvyys $3.2\frac{m}{s^2}$. Lisäksi taulukossa on kerrottu kuinka paljon nopeus ehtii muuttua kahden peräkkäisen nauhanosan välillä kyseisen nopeuden lähistössä.

Taulukko 4.2: Virherajat

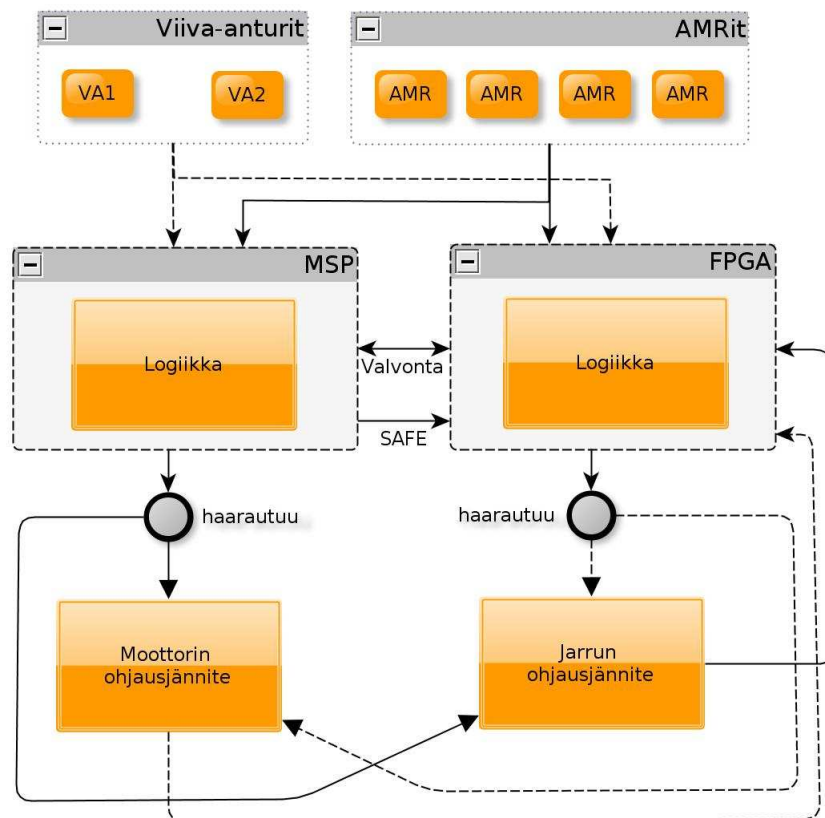
Nopeus (m/s)	Reagointiaika (ms)	Muutosnopeus (m/s)
1.0	34	0.11
1.25	28	0.09
3.0	12	0.04

Kuten taulukosta havaitaan, reagointiaika on pahimmillaan alhaisimmalla maksiminopeudella, jolloin uusi arvo saadaan 34ms sisällä. Vastaavasti suurimmalla asetettavalla maksiminopeudella 3m/s saadaan reagointiajaksi 12ms. Myös muutosnopeus on suurin alhaisimmalla nopeudella jolloin perättäisten nauhanosien välillä nopeus kasvaa 0.11m/s.

Edellä esitetyn perusteella ei haittaa vaikka nopeuksia mitattaessa menetettäisiin yksittäinen reuna, virheraja $\pm 10\%$ maksiminopeudessa ei silti ylity. Suurempia nopeuksia ei tämän osalta tarvitse huomioida sillä nopeuden kasvaessa vakio-kiihtyvyydellä muutosnopeus kahden reunan välillä pienenee. Vastaavasti myös reagointiaika pienenee.

4.3 Ohjelmiston laitteistorajapinnat

Kuvassa 4.2 on esitetty laitteistoarkkitehtuurin pohjalta ne sisääntulot ja lähdöt jotka turvatoiminnon ohjelmistolla on käytettävissä. Kuvasta nähdään että molemmat ohjauslogiikat saavat sisääntulonaan kaikkien AMR-antureiden datan sekä viiva-antureiden datan. FPGA saa tiedon myös turvakytkeiden lähtöjen tilasta. Lisäksi MSP:llä generoitu SAFE_LO-signaali ohjataan FPGA:lle. Ohjauslogiikat kommunikoi keskenään ja suorittavat näin ristiinvalvontaa. Molemmilla logiikoista ohjataan nostolaitteessa olevia ajomoottoreiden ohjausjännitteen sekä jarrujännitteen turvakytkeitä.



Kuva 4.2: Laitteistorajapinnat

4.4 Yleiskuvaus toiminnasta

Kun laitteeseen on kytketty virrat päälle ylinopeusvahti tarkkailee sen jälkeen jatkuvasti nopeuden muutoksia kahdella viiva-anturilla. Lisäksi ylinopeusvahti tarkkailee AMR-antureiden datan perusteella kapselin yläasemaa. Maksimiarvo johon nopeuksia verrataan asetetaan sen perusteella onko kapseli ylhäällä vai alhaalla.

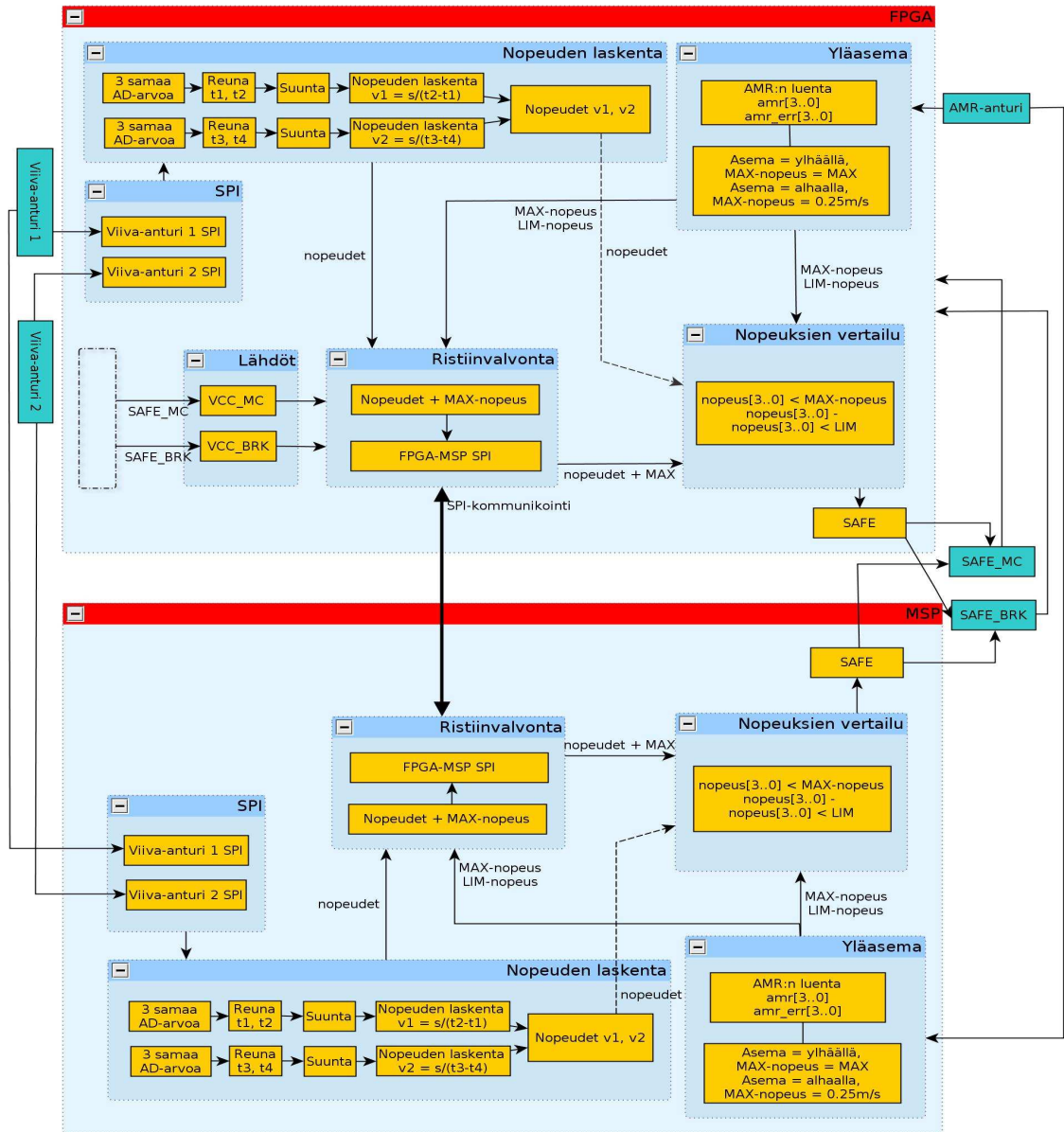
Nopeutta lasketaan molemmilla ohjauslogiikoilla ja kun ollaan saatu lasketua uusi nopeus molemmilla viiva-antureilla ohjauslogiikat lähettävät nopeudet

toisilleen. Mikäli lähetys epäonnistuu suoritetaan turvatoiminto. Molemmat ohjauslogiikat vertaavat sekä itse laskemiaan että toisen ohjauslogiikan laskemia nopeuksia asetettuun kiinteään maksiminopeuteen. Lisäksi kaikkia nopeuksia verrataan keskenään asetettuun nopeuksien poikkeaman maksimiarvoon. Mikäli jokin näistä ylittyy suoritetaan turvatoiminto. Arvot joihin nopeuksia verrataan on määritelty luvussa 4.2. Kuvassa 4.3 on esitetty vuokaavio siitä miten ohjelman toiminta etenee erilaisissa tilanteissa. Koska MSP:n suorituskyky ei riitä siihen että luettaisiin jatkuvasti viiva-antureiden dataa ja samanaikaisesti suoritettaisiin ristiinvalvontaa FPGA:n kanssa, täytyy ohjelman eri vaiheiden suoritusjärjestys olla määritelty. Kahden ohjauslogiikan pitää toimia synkronissa ristiinvalvonnan ja nopeuden laskennan vuorotellessa. Lyhyesti toiminta voidaan kuvata seuraavasti molemmille ohjauslogiikoille:

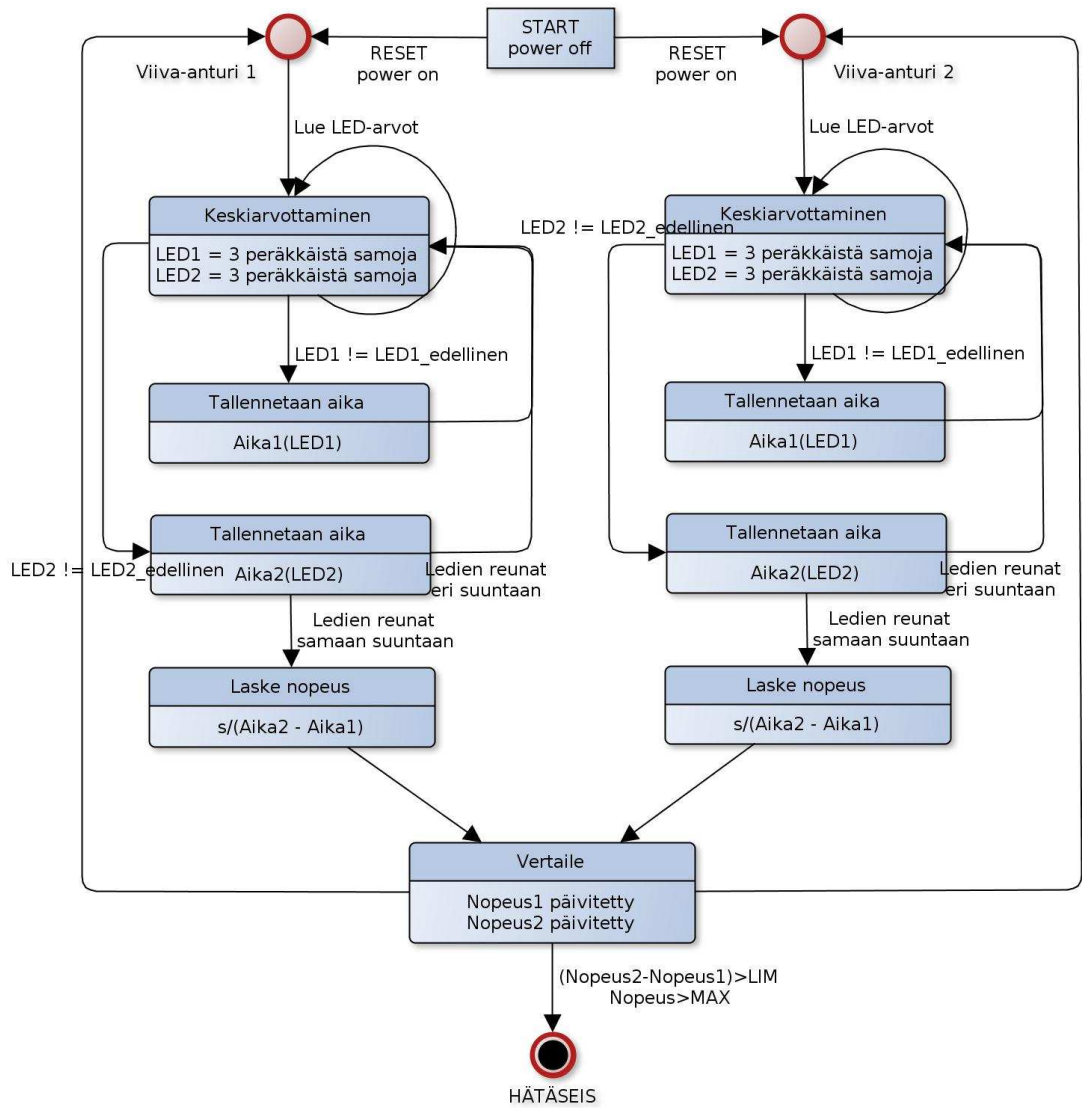
1. Luetaan molempien viiva-antureiden kaikkien ledien dataa ja muutetaan ledien AD-luvut biteiksi.
 - Jos saadaan viiva-anturilta liian monta CRC-virhettä suoritetaan turvatoiminto.
 - Jos ei olla tietyn ajan sisällä rekisteröity yhtään reunaa suoritetaan ristiinvalvonta, siirrytään kohtaan 5.
 - Jos ei olla tietyn ajan sisällä rekisteröity reunaa viiva-anturilta, nollataan sen nopeus.
2. Rekisteröidään reuna jos jommallakummalla aikaa mittaavista ledeistä 3-peräkkäistä bittiä ovat samoja ja bitit ovat erisuuria kuin viimeksi.
3. Jos saatiin toisella viiva-anturilla nopeus, verrataan maksiminopeuteen.
4. Jos saatiin molemmilla viiva-antureilla nopeudet siirrytään ristiinvalvontaan.
5. Suoritetaan ristiinvalvonta, lähetetään uusimmat nopeudet toiselle ohjauslogiikalle.
 - Jos ei saada yhteyttä toiseen ohjauslogiikkaan suoritetaan turvatoiminto.
6. Vertaillaan nopeuksia ja jos maksimiarvot ylittyvät suoritetaan turvatoiminto.
7. Palataan takaisin kohtaan 1. lukemaan viiva-antureiden dataa.

4.5 Ohjelmiston arkkitehtuuri

Tässä luvussa on esitelty turvatoiminnon arkkitehtuuri ja sen lohkot yleisellä tasolla. Arkkitehtuuri nähdään kuvasta 4.4. Toiminnalliset osat ja ohjelman suoritus ovat samanlaiset molemmilla ohjauslogiikoilla. Koska toinen logiikoista on kuitenkin perinteinen mikrokontrolleri (MSP) ja toinen vastaavasti FPGA on ohjelmien toiminnan kuvaus erilaista. MSP:lle ohjelma tehdään käännettävällä ohjelmointikielellä ja FPGA:lle puolestaan laitteistonkuvauskielellä. Ohjauslogiikoista FPGA toimii masterina SPI-kommunikoinnissa.



Kuva 4.4: Ylinopeusvahdin ohjelmistoarkkitehtuuri



Kuva 4.5: Nopeuden laskennan tilakaavio

4.5.2 Suunnan määrittely

Kuvassa 4.6 on esitetty tilanteet miten kaksi reunaa tutkivaa lediä voivat olla sijoituneet eriväristen nauhanosien päälle riippuen kulkusuunnasta. Siitä myös selviää miten ledit ovat nauhanosien päällä ennen ja jälkeen reunan ylityksen. Turvatoiminnon täytyy tietää että peräkkäiset reunanmuutokset ovat tapahtuneet samalla reunalla. Ei riitä että rekisteröidään peräkkäiset muutokset kun kaksi lediä ovat ylittäneet jonkin reunan sillä on mahdollista että ensimmäinen muutos rekisteröidään kulkusuuntaan nähden taaemmalta lediltä ja seuraava muutos kulkusuuntaan nähden etummaiselta lediltä.

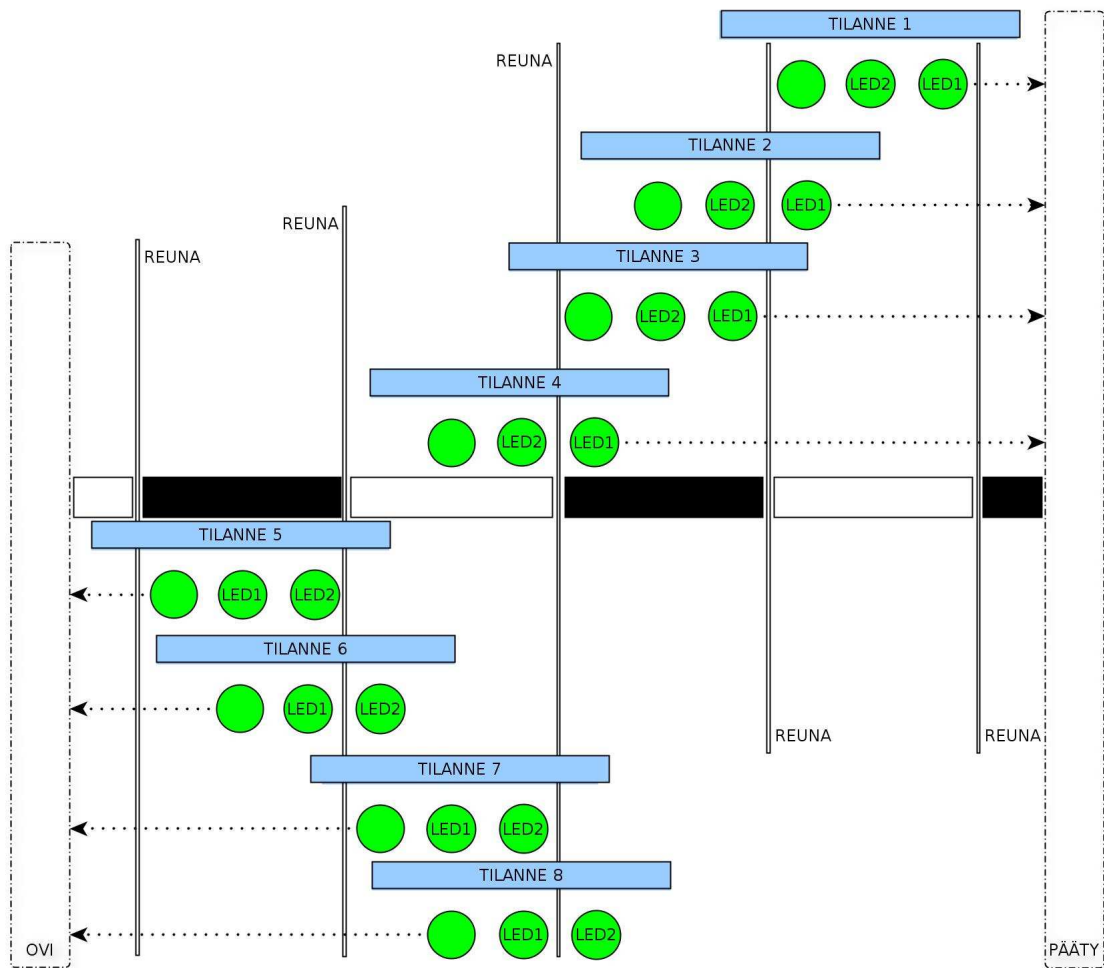
Näin käy mikäli ledit eivät ole molemmat samanvärisen nauhanosan kohdalla lähtötilanteessa tai ollaan muutettu suuntaa, esimerkkinä kuvan 4.6 tilanne 2. Jos lähdetään tästä tilanteesta liikkeelle ja lasketaan aikaa vain kahden peräkkäisen ledin ylittäessä jonkin reunan saadaan väärä aika. Siksi peräkkäisten reunanylitysten ajasta laskettu nopeus hyväksytään vain jos peräkkäiset muutokset ovat olleet samaan suuntaan, eli mustasta valkoiseen tai valkoisesta mustaan. Muussa tapauksessa odotetaan seuraavaa reunaa ja aloitetaan laskenta alusta.

4.5.3 Turvakytkentöjen ohjaaminen

Molemmilla ohjauslogiikoilla on yksi ulostulo jolla ne pystyvät ohjaamaan sekä moottorin ohjausjännitteen että moottorin jarrujännitteen turvakytkentöjä. Sama ulostulo ohjataan molemmille turvakytkennöistä. Signaalit ovat muodoltaan kanttiaaltoja ja niiden käyttö on tarkemmin kuvattu kappaleessa 3.2.3. Oletuksena signaalit ovat päällä oikeassa vaiheessa siten että turvakytkennät sallivat moottoreiden ja jarrujen käytön. Mikäli ylinopeusvahdin ohjauslogiikoista jompikumpi havaitsee tilanteen jossa sen tulee suorittaa turvatoiminto, kyseinen ohjauslogiikka ohjaa oman SAFE-signaalinsa nollajännitteeseen.

4.5.4 Ristiinvalvonta

Ristiinvalvonnassa toinen ohjauslogiikoista (FPGA) lähettää ensin pyynnön johon toinen ohjauslogiikka vastaa (MSP) eli suoritetaan kättely. Tämän jälkeen molemmat logiikoista lähettävät uusimmat lasketut nopeutensa sekä senhetkisen maksiminopeuden toisilleen. Lisäksi datapaketin mukana lähetetään CRC-tunniste jolla varmistetaan että molemmat logiikat ovat saaneet lähetettyä ja vastaanotettua paketin oikein. Ristiinvalvonta suoritetaan 1 sekunnin sisällä mikäli ei olla rekisteröity yhtään reunaa. Kun yhden nauhanosan pituus on 3.6cm tarkoittaa tämä sitä että nopeuden ollessa alle 3.6cm/s ei välttämättä verrata uusimpia nopeuksia toisiinsa. Tällä ei kuitenkaan ole merkitystä sillä nopeuksien erotus aiheuttaa turvatoiminnon laukeamisen vasta kun erotus on pienimmillään 0.25m/s.



Kuva 4.6: Suunnan määrittely

4.5.5 Nopeuksien vertailu

Aina kun jommalla kummalla viiva-antureista on laskettu uusi nopeus, verrataan sitä maksiminopeuteen. Kun molemmilta viiva-antureilta on laskettu uudet nopeudet, nopeuksia verrataan keskenään ja myös toisella ohjauslogiikalla laskettuihin. Mikäli nopeudet poikkeavat liikaa toisistaan tai jokin niistä ylittää asetetun nopeuden maksimiarvon suoritetaan turvatoiminto.

Vertailussa käytetään maksiminopeutena aina sitä nopeutta joka on kahden ohjauslogiikan ilmoittamista maksiminopeuksista pienempi. Mikäli toinen ohjauslogiikka havaitsee yläaseman muutoksen ennen toista tai yläaseman tarkastelun logiikka vikaantuu, asetetaan maksiminopeus aina ohjauslogiikoista pienimmän maksiminopeuden mukaan.

4.5.6 Kapselin yläaseman määrittäminen

Kapselin yläasema määritellään AMR-antureiden datan perusteella. Kun kaikki anturit näyttävät nolaa tulkitaan asema siten että ollaan ylhäällä. Jos kaikki anturit eivät näytä samaa arvoa tai jonkin anturin virhesignaali menee päälle tulkitaan se niin että ollaan alhaalla. Maksiminopeus johon nopeuksia vertaillaan määritellään yläaseman mukaan siten että kapselin ollessa ylhäällä käytetään varastokohtaista maksiminopeutta ja kapselin ollessa alhaalla arvoa $0.25 \frac{m}{s}$. Nopeuksien erotusten vertailussa maksimiarvo johon erotusta verrataan on kapselin ollessa alhaalla $0.25 \frac{m}{s}$ ja vastaavasti kapselin ollessa ylhäällä $0.5 \frac{m}{s}$.

4.5.7 Viiva-anturit

IR-ledejä ohjataan viiva-anturin MSP:llä asettamalla 30%:n pulssisuhteella oleva PWM-signaali MOSFET:n hilalle. Ledien yli on noin 0.8V:n häviö jolloin MOSFET:n lähteessä on vastaavasti 2.5V maksimissaan. Näin ledien läpi kulkeva virta on noin 9mA 100 ohmin vastuksella. Edelleen fotodiodien rekisteröimät arvot luetaan AD-muunninten kautta. Kommunikointi ohjauslogiikoiden kanssa tapahtuu SPI:llä ja yksi datapaketti sisältää aina kolmen ledin 12-bittiset arvot sekä 8-bittisen CRC:n.

4.6 FPGA:n modulkuvaukset ja rajapinnat

Tässä kappaleessa on esitetty yksityiskohtaisemmin ylinopeusvahdin moduliin rajapinnat FPGA:lla. Taulukossa 4.3 on esitetty kaikki modulit ja niiden sisään- ja ulostulot. Jos parametrin nimen perään ei ole määritelty kokoa on se yksibittinen signaali. Muussa tapauksessa parametrin koko bitteinä on esitetty hakasuluissa.

Taulukko 4.3: Modulien rajapinnat

Moduli / Funktio	Sisääntulot	Ulostulot
spi	miso	mosi spi_clk spi_csn tape_sensor[35..0] crcerror_tape_sensor updatednow_tape_sensor
bit_from_ad	tape_sensor[35..0] updatednow_tape_sensor crcerror_tape_sensor	data_valid bit[5..0]
calc_time	data_valid bit[5..0]	updated time[15..0]
max_velocity	amr[3..0] amr_err[3..0]	max_velocity[15..0] diff_velocity[15..0]
mcp	mcu_miso crc_init spi_lock_in spi_write_data[7..0] spi_req_in	mcu_csn mcu_clk mcu_mosi crc_data_out[7..0] crc_data_in[7..0] spi_read_data[7..0] spi_ack_out spi_locked
crosswatch	velocity ₁ [15..0] velocity ₂ [15..0] max_velocity[15..0] crosswatch_req crc_data_out[7..0] crc_data_in[7..0] spi_read_data[7..0] spi_ack_out spi_locked	crosswatch_velocity ₁ [15..0] crosswatch_velocity ₂ [15..0] crosswatch_max_velocity[15..0] crosswatch_ack crc_error_out crc_init spi_write_data[7..0] spi_req_in spi_lock_in
compare	velocity ₁ [15..0] velocity ₂ [15..0] max_velocity[15..0] crosswatch_velocity ₁ [15..0] crosswatch_velocity ₂ [15..0] crosswatch_max_velocity[15..0] diff_velocity_in compare_req compare_max	speeding_diff speeding_max speeding
safe	speeding safe_synch	safe_signal

SPI (spi) ottaa sisääntulonaan viiva-anturin SPI:n kautta tulevan datan (miso) ja antaa ulostuloon ledien arvot (tape_sensor) sekä tiedon siitä oliko paketin CRC oikein (crcerror_tape_sensor). Ledit 2, 1 ja 0 ovat tape_sensor-vektorissa indekseissä 35..24, 23..12 ja 11..0. Kun ollaan vastaanotettu uusi paketti kokonaisuudessaan, ilmoitetaan siitä signaalilla updatednow_tape_sensor (1=uusi arvo). Lisäksi SPI-moduli ohjaa SPI:n kelloa (spi_clk) 250kHz taajuudella, SPI:n ulostuloa (mosi) käytetään vain resetin yhteydessä jolloin asetetaan valoteho viiva-antureille. Molemmille viiva-antureille on oma SPI-modulinsa. CRC:n pituus on 8-bittiä.

Bittimuunnos (bit_from_ad) ottaa sisääntulonaan viiva-anturin ledien AD-muunninarvot (tape_sensor) ja antaa ulostuloon jokaisen ledin edellisen sekä tämänhetkisen bitin (bit[5..0]) joista voidaan päätellä nauhanosan reunat. Ledien 2, 1 ja 0 edellinen ja tämänhetkinen bitti ovat bit-vektorissa indekseissä 5..4, 3..2 sekä 1..0. Modulissa ledin AD-arvo muunnetaan kiinteään raja-arvon mukaisesti bitiksi siten että 12-bittinen luku (0-4095) on nolla (musta nauhanosa) mikäli arvo on alle raja-arvon ja 1 (valkoinen nauhanosa) mikäli se on yli raja-arvon. Raja-arvo on oletuksena 2000. Bitti lukitaan vasta kun sama bitti ollaan saatu luettua kolme kertaa peräkkäin. Näin estetään yksittäiset häiriösignaalit. Kun virrat asetetaan päälle, hylätään alustuksen yhteydessä ensimmäiset paketit viiva-anturilta ja vasta sen jälkeen kun data on oikean muotoista asetetaan data_valid-signaali päälle (1=valid).

Ajanlaskenta (calc_time) ottaa sisääntulonaan ledien 2, 1 ja 0 reunat (bit[5..]) sekä tiedon siitä onko data oikean muotoista (data_valid). Modulissa lasketaan aikaa jonka sisällä kaksi peräkkäistä aikaa mittaavaa lediä ovat ylittäneet saman reunan. Kun uusi aika on saatu ilmoitetaan siitä signaalilla updated (1=uusi arvo). Bittivektorissa time[15..0] on uusi aika. Molemmille viiva-antureille on oma ajanlaskentamodulinsa.

Maksiminopeus (max_velocity) ottaa sisääntuloinaan neljän AMR-anturin päälläolosignaalit (amr[3..0], 0=ylhäällä, 1=alhaalla) sekä virhesignaalit (amr_err[3..0], 1=virhe, 0=ei virhettä). Se antaa ulostulonaan maksiminopeuden yläaseman perusteella (max_velocity[15..0]). Modulista saadaan myös absoluuttiarvo johon nopeuksien erotusta verrataan (diff_velocity[15..0]). Nopeuksien erotuksen vertailuarvo riippuu siitä onko kapseli ylhäällä vai alhaalla. Logiikka yläaseman määrittelyyn on kuvattu edellä kappaleessa 4.5.6.

Ristiinvalvonta (crosswatch) ottaa sisääntuloinaan kyseisellä ohjauslogiikalla lasketut nopeudet (velocity1[15..0], velocity2[15..0]) sekä maksiminopeu-

den (`max_velocity[15..0]`). Se antaa ulostulonaan toisen ohjauslogiikan laskemat nopeudet (`cw_velocity1[15..0]`, `cw_velocity2[15..0]`) sekä maksiminopeuden (`cw_max_velocity[15..0]`). Ristiinvalvontamoduli ohjaa myös FPGA:n ja MSP:n välistä SPI-liikennöintiä jossa se toimii masterina. MSP:ltä tuleva data luetaan `spi_read_data`:sta ja dataa kirjoitetaan `spi_write_data`an. Uusi tavu voidaan kirjoittaa kun `spi_ack_out`:lla ja `spi_ack_req`:llä on sama arvo. Kun halutaan kirjoittaa uusi tavu, invertoidaan `spi_req_in`:n arvo. Tämän jälkeen jäädytään odottamaan että signaalit ovat taas samat jolloin voidaan kirjoittaa uusi tavu.

Signaalilla `spi_lock_in` (1=lukittu) kerrotaan SPI-modulille että halutaan lukea tämä prosessi SPI:n käyttöön. Vastaavasti `spi_locked` (1=lukittu) kertoo jos toinen prosessi on lukinnut SPI:n omaan käyttöönsä jolloin jäädytään odottamaan lukon vapautumista. Signaaleissa `crc_data_out` ja `crc_data_in` on ulosmenevän ja sisääntulevan datan CRC:t. Signaalia `crc_init` kutsutaan aina kun aloitetaan uuden paketin lähetyksen joka pitää sisällään kättelyn, nopeudet ja maksiminopeuden. Paketin koko on 64-bittiä. Paketin siirto tapahtuu siten että ristiinvalvontamoduli aloittaa kättelykomennolla johon MSP vastaa. Kun ollaan saatu oikea vastaus siirretään loput paketista.

Vertailu (compare) ottaa sisääntuloinaan molempien ohjauslogiikoiden laskemat nopeudet (`velocity1[15..0]`, `velocity2[15..0]`, `cw_velocity1[15..0]`, `cw_velocity2[15..0]`), maksiminopeudet (`max_velocity[15..0]`, `cw_max_velocity[15..0]`) sekä erotusnopeuden (`diff_velocity_in`). Ulostulonaan se tuottaa tiedon nopeuksien erotuksen ylittymisestä (`speeding_diff`, 1=ylinopeus) ja ylinopeudesta (`speeding_max`, 1=ylinopeus). Lisäksi ulostuloon ohjataan signaali `speeding` joka on looginen OR `speeding_diff` ja `speeding_max`-signaaleista. `Compare_max` on yhden kellojakson mittainen signaali ja sillä pyydetään vertailemaan ohjauslogiikalla laskettuja nopeuksia maksiminopeuteen. `Compare_req` on yhden kellojakson mittainen signaali ja sillä pyydetään vertailemaan molempien ohjauslogiikoiden laskemia nopeuksia maksiminopeuteen sekä nopeuksien erotuksia erotusnopeuteen.

Turvakytkentä (safe) ottaa sisääntulonaan ylinopeustiedon (speeding), MSP:n generoiman SAFE-signaalin (safe_synch) ja tuottaa ulostuloon turvakytkentöjä ohjaavaa kanttiaaltoa (safe_hi). Mikäli ylinopeus on havaittu ohjataan ulostulo nolnaan. Signaali speeding asetetaan päälle mikäli viiva-antureilta tai ristiinvalvonnalta on saatu liian monta CRC-virhettä tai jos havaitaan joko ylinopeus (speeding_max) tai nopeuksien erotuksen (speeding_diff) ylittyminen. CRC-virheiden maksimimäärä on 10 perättäistä virhettä. 4.545kHz näytteistyksellä tämä tarkoittaa 2ms:a.

4.7 Ohjelmistolla toteutettava diagnostiikka (DC_{avg})

Tulot

Kappaleen 3.3.2 kohdassa tulot on esitetty standardin SFS-EN ISO 13849-1 taulukon E.1 kohta jota sovelletaan tuloyksikköön diagnostiikan tason osalta: "Jos oikosulkuja ei voida paljastaa, tulosignaalien ristiinvalvonta yhdessä dynaamisen testauksen kanssa (useille I/O-yksiköille) 90%". Viiva-antureiden tuottamaa dataa valvotaan ristiin nopeuksien vertailun kautta kappaleiden 4.5.5 ja 4.5.4 mukaisesti. Lisäksi viiva-antureilta vastaanotetusta datasta saadaan CRC-tieto jota tutkitaan molemmilla ohjauslogiikoilla. AMR-antureiden dataa valvotaan maksiminopeuden kautta molemmissa ohjauslogiikoissa kappaleiden 4.5.6 ja 4.5.4 mukaisesti.

Ohjauslogiikka

Kappaleen 3.3.2 kohdassa ohjauslogiikka on esitetty standardin SFS-EN ISO 13849-1 taulukon E.1 kohta jota sovelletaan logiikkaan diagnostiikan tason osalta: "Logiikan toiminnan tilapäinen yksinkertainen valvonta (esim. ajastinvahti jolloin liipaisukohdat ovat logiikan ohjelmassa) 60%". Ohjauslogiikoissa on määritelty aika jonka sisällä ristiinvalvonta suoritetaan mikäli uusia reunoja ei olla havaittu kappaleen mukaisesti. Ristiinvalvonnassa käytetään CRC:tä jolla havaitaan mikäli toinen ohjauslogiikka ei enää vastaa tai sen lähettämä data on virheellistä.

Lähdöt

Kappaleen 3.3.2 kohdassa lähdöt on esitetty standardin SFS-EN ISO 13849-1 taulukon E.1 kohta jota sovelletaan lähtöyksikköön diagnostiikan tason osalta: "Redundanttinen signaalin sulkupolku yhden toimilaitteen valvonnalla joko logiikan tai testauslaitteen avulla 90%". FPGA vastaa tässä yhtä toimilaitetta sillä safe-kytkentöjen lähdöt on ohjattu FPGA:lle joka välittää ne edelleen ristiinvalvonnan kautta MSP:lle. Sulkupolku on redundanttinen sillä molemmilla safe-kytkennöistä saavutetaan turvatoiminto. Mikäli ohjauslogiikoilla havaitaan tilanne jossa jompikumpi safe-kytkentöjen lähdöistä ei vastaa oletettua tilannetta, ohjataan safe-kytkentöjen sisääntulot alas kappaleen 4.5.3 mukaisesti.

5. TURVATOIMINNON ANALYYSI JA TESTAUS

5.1 Ohjelmiston testaaminen

Ohjelmistojen testaus voidaan jakaa esimerkiksi kolmelle tasolle seuraavasti: moduulitestausta, integrointitestausta sekä järjestelmätestausta. Tässä järjestelmässä testaus toteutetaan käyttäen moduulitestausta yksittäisille komponenteille sekä lopuksi järjestelmätestausta valmiille järjestelmällä joka pitää sisällään integrointitestausta. Lisäksi turvatoiminnossa käytettävälle laitteistolle suoritetaan erikseen laitteistotestaus jossa todetaan esimerkiksi ulostulon turvakytkeiden oikeanlainen vikaantuminen.

Moduulitestausta

Testitapaukset luodaan glass-box menetelmän mukaisesti. VHDL-komponenttien moduulitestausta varten luodaan testitapaukset vhdlsim-ohjelmalla. Jokainen komponentti testataan syöttämällä sisääntuloihin arvoja sekä vertaamalla lähtöjen arvoja oletettuihin. Tapauksissa joissa sisääntulo tai lähtö on yksibittinen signaali tutkitaan kaikki mahdolliset kombinaatiot. Tapauksissa joissa sisääntulo tai lähtö on bittivektori ja mahdollisten syötekombinaatioiden määrä on liian suuri, testataan signaali ääriarvoilla sekä riittävällä määrällä satunnaisia arvoja. Testitapausten syötteet ja oletetut ulostulot on kuvattu testipenkien koodissa.

C-kielisten komponenttien moduulitestausta varten luodaan testitapaukset C-kielisillä testiajureilla, mitään valmista testausympäristöä kuten CUnit:tä ei käytetä. Jokainen funktio testataan riittävällä määrällä syötteiden kombinaatioita ja vertaamalla lähtöjen arvoja oletettuihin.

FPGA:lle tehdyssä moduulitestauksessa testattiin taulukon 4.3 moduleista: bit_from_ad, calc_time, max_velocity, crosswatch, compare, safe, msp.

Järjestelmätestausta

Järjestelmätestauksessa tutkitaan koko järjestelmän toimintaa eli korkeimman tason toimintoja siten että kaikki tarvittavat moduulit ovat mukana ja testattu. Laitteiston osalta tutkitaan miten turvatoiminto havaitsee erilaiset laitteiston vikaantumiset ja sitä vikaantuuko järjestelmä aina niin että se jää turvalliseen tilaan. Jokais-

sa testitapauksessa turvallinen tila todetaan ensisijaisesti siitä että nostolaitteen VMC sekä VBRK-ledit sammuvat. Näistä ledeistä tiedetään että safe-signaaleissa ei ole ohjausta. Nopeuksien todentamisessa käytetään SIKO:n magneettista inkrementaalianturia. Järjestelmätestit on esitetty liitteessä C.

5.2 SIKO:n magneettinen inkrementaalianturi IV58M

Jotta voitaisiin vertailla kuinka lähellä todellista nopeutta viiva-antureiden datasta lasketut nopeudet ovat, käytettiin referenssinä SIKO:n valmistamaa magneettista inkrementaalianturia. [29] Anturi ilmoittaa paikan muutoksen kahdella kanavalla, A ja B, siten että yhden kierroksen aikana anturista saadaan molemmista kanavista 1000 pulssia. Pulssit ovat muodoltaan kanttiaaltoa. Anturiin on kiinnitetty kaapeli ja valmistajan datalehden mukaan kaapeli kulkee yhden kierroksen aikana noin 0.2m. Valmistaja ei anna kuitenkaan täysin tarkkaa arvoa. Mittauksissa anturista käytettiin pelkästään A-kanavaa ja se kytkettiin digitaali-oskilloskooppiin jolla dataa näytteistettiin 100kHz:n taajuudella näytteistysajan ollessa 1s.

Nopeus saadaan laskettua inkrementaalianturista pulssien sisältämien näytteiden määrän perusteella. Kun tunnetaan pulssien määrä ja kaapelin kulkema matka yhden kierroksen aikana sekä oskilloskoopin näytteistystaajuus ja näytteiden määrä yhden pulssin aikana, voidaan nopeus laskea kaavalla (5.1)

$$v = \frac{\frac{1}{n} \times f \times s}{p} = \frac{\frac{1}{n} \times 100kHz \times 0.2m}{1000} \quad (5.1)$$

Kaavassa n = näytteiden määrä yhden jakson aikana, f = näytteistystaajuus, s = kaapelin kulkema matka yhden kierroksen aikana ja p = pulssien määrä yhden kierroksen aikana. Kaava ilmaisee hetkellisen nopeuden yhden pulssin ajalta pulssin sisältämien näytteiden perusteella. Tällä tavalla tarkkuudeksi saadaan 1000 nopeusnäytettä 0.2m:n matkalle. Näytteistystaajuudeksi oskilloskoopissa valittiin 100kHz sillä suurilla nopeuksilla ja pienellä näytteistystaajuudella näytteiden määrä yhtä inkrementaalianturin pulssia kohden on liian pieni. Tällöin pulssi voi sisältää ylhäällä ja alhaalla ollessaan vain yhden näytteen ja resoluutio on huono. Toisaalta liian suurella näytteistyksellä ei päästä kovin paljoa tarkempiin tuloksiin mutta datan käsittelystä ja siirrosta oskilloskoopilla tulee hidasta.

Kun anturilla mitatuista tuloksista piirrettiin nopeuskuvaaja kaavan (5.1) mukaisesti, havaittiin että nopeudessa oli huomattavasti häiriötä. Tämä voidaan nähdä esimerkiksi kuvasta 5.14. Häiriön poistamiseksi lopullisista tuloksista käytettiin painotetun keskiarvon alipäästösuodatusta. Kun uusi arvo huomioitiin 1%-osuudella, saatiin kuvan 5.13 mukainen tulos jossa häiriö on saatu poistettua miltei kokonaan ja josta nähdään paremmin nopeus.

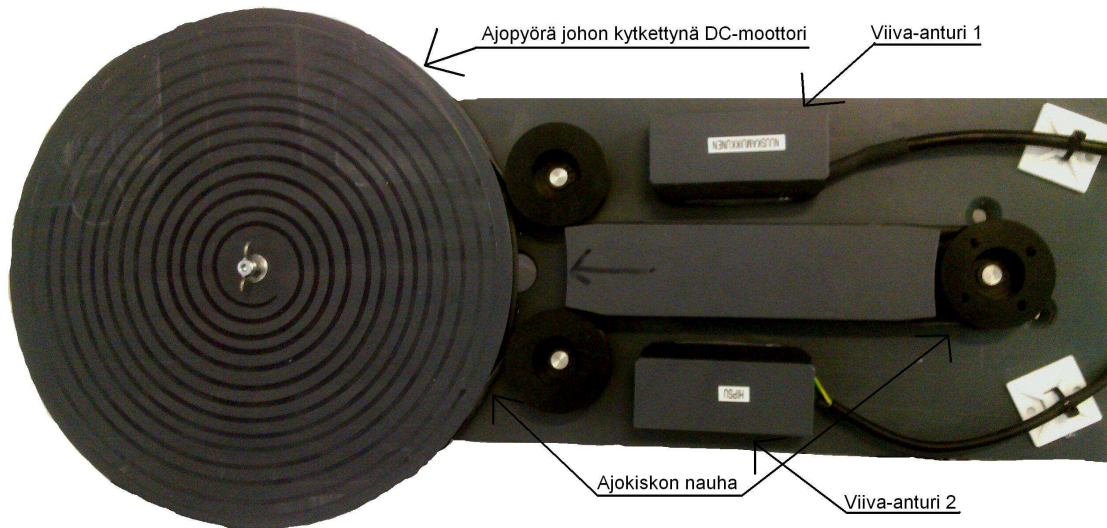
5.3 Viiva-antureiden testaaminen

Oikeassa järjestelmässä nopeutta mitataan itsenäisesti kahdella viiva-anturilla. Viiva-antureiden testaamiseksi yhdessä rakennettiin testilaite jolla voidaan tutkia miten erilaiset tekijät vaikuttavat antureiden tuottamaan dataan ja sen perusteella laskettuun nopeuteen. Pöytätestissä voidaan generoida huomattavasti helpommin ja monipuolisemmin häiriöitä kuin oikeassa järjestelmässä joka on lopulta suljetussa tilassa. Pöytätestissä saadaan myös aikaiseksi todellista järjestelmää suurempia kiihtyvyyksiä joilla voidaan tutkia miten paljon kahdella eri viiva-anturilla lasketut nopeudet todellisuudessa poikkeavat toisistaan pahimmassa tapauksessa.

Kuvassa 5.1 on esitetty testilaite jolla antureita tutkittiin. Siinä sukkulan liikettä simuloimaan on rakennettu teline johon on kiinnitetty pyörästö. Pyörästön kautta kulkee uralle sijoitettu, päistään yhteen sidottu nauha, jota voidaan liikuttaa yhdellä ajopyörällä. Nauha koostuu 3.6cm:n mittaisista mustista ja valkoisista osista aivan kuten todellisessa järjestelmässä oleva ajokiskon nauha. Testilaitteessa 24V:n DC-moottori on kytketty ajopyörään joka saa jännitteensä 0-30V:n tasajännitelähteestä. Viiva-anturit on kytketty FPGA-korttiin jossa on kaksi SPI-väylää antureiden ohjaamiseen. FPGA-kortilla käytettiin samoja ohjelmamoduleita kuin oikean järjestelmän piirilevylläkin. Eri lähteistä näytteistettävää dataa varten testilaitteen FPGA:lle on kuvattu myös Nios-prosessori sekä siihen ohjelmisto jota ohjataan ethernetin yli PC:llä. Ohjelmassa voidaan määritellä taajuus näytteistykselle sekä tässä tapauksessa seurantaan esimerkiksi viiva-anturin AD-muunninarvot, viiva-antureilla lasketut nopeudet sekä hätäseissignaalien tila. Näytteistyksen aikana data kerätään testilaitteen DDR-muistiin ja kun näytteistys lopetetaan data siirretään yhtenäisenä pakettina PC:lle tulkittavaksi. Viiva-antureilta saadaan uusi näyte 4.545kHz taaajuudella myös testilaitteessa. Näin nopeasti dataa ei tarvitse kuitenkaan näytteistää sillä reunat tulkitaan kolmen samanlaisen peräkkäisen näytteen perusteella.

5.3.1 Häiriötekijöiden vaikutus AD-muunninarvoihin

Häiriötekijöitä jotka vaikuttavat nopeuden tulkintaan ovat esimerkiksi ajokiskon nauhan kuluminen ja likaantuminen, vakiopituudesta poikkeavat nauhanosat, ympäristön taustavalo sekä muut säteilevät ja johtuvat häiriöt. Myös IR-ledien etäisyyden poikkeamat piirilevyllä ja muutokset viiva-anturin kotelossa aiheuttavat sekä optisia virheitä että eroja oletetussa vakiomatassa. Viiva-anturin IR-ledeissä käytettävän virran määrä vaikuttaa siihen miten hyvin AD-muuntimen arvot saturoituvat alueen ylärajalle valkoisen nauhanosan kohdalla sekä toisaalta siihen miten korkealle AD-muuntimen arvot nousevat mustan nauhanosan kohdalla.

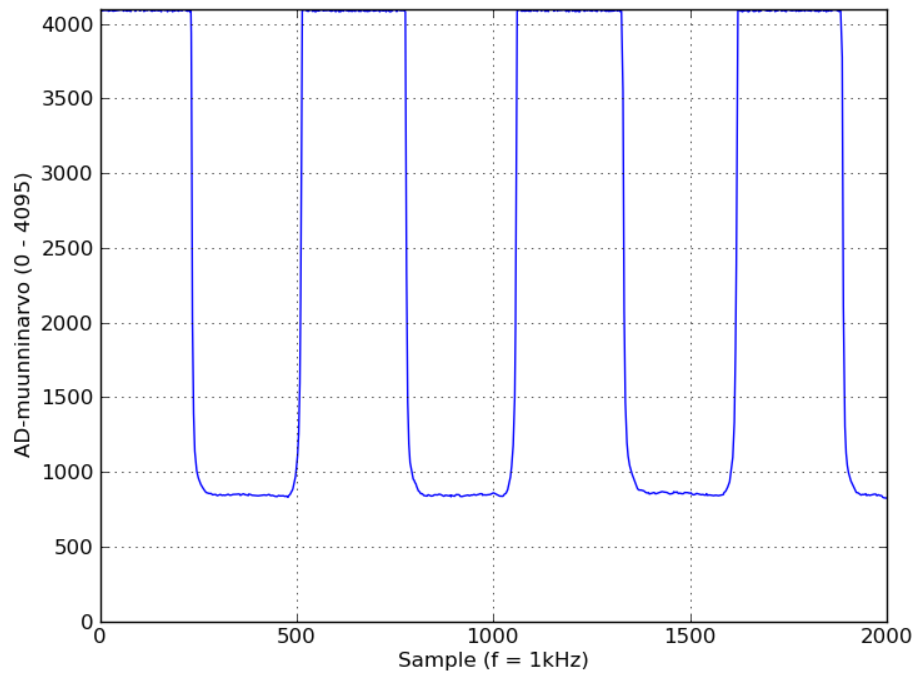


Kuva 5.1: Viiva-antureiden testauslaite

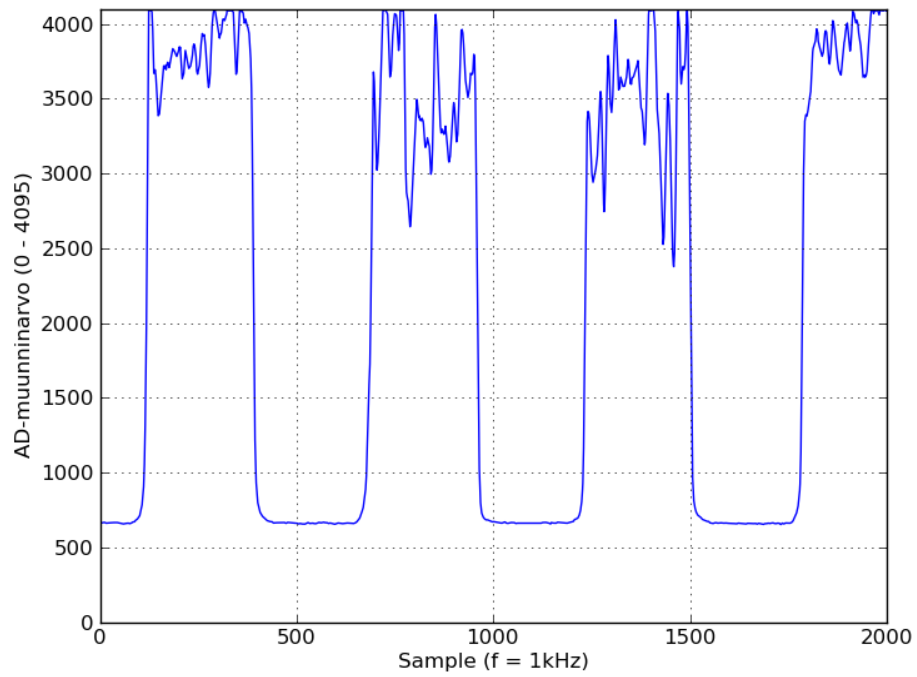
Lähtävien IR-ledien virta halutaan mahdollisimman pieneksi siksi että suurilla virroilla ledit vikaantuvat nopeammin ja tällöin ei päästä haluttuun arvoon $MTTF_d$:n osalta. Tässä järjestelmässä maksimiarvoksi virralle on määritelty 9mA, jolla saadaan muut valitut ympäristöolosuhteet huomioonottaen riittävän suuri $MTTF_d$. Tutkittaessa valotehon vaikutusta testilaitteella käytettiin mittauksissa 1kHz:n näytteistystaajuutta, 2s näytteistysaikaa ja DC-moottorin jännitteenä 5V. Kuvassa 5.2 on esitetty viiva-anturin yhden AD-muuntimen arvoja kun IR-ledien läpi kulkeva virta on noin 4.5mA. Kuvasta nähdään että musta ja valkoinen nauhanosa erotetaan riittävän selvästi toisistaan, valkoisen nauhanosan kohdalla arvot satureituvat 4095:een, eikä signaalissa ole soimista tai muita häiriötekijöitä.

Kuvassa 5.3 on vastaavasti ohjattu IR-ledejä noin 1.5mA:n virralla. Kuvasta havaitaan että musta nauhanosa luetaan edelleen oikein ja AD-muunninarvot ovat hieman matalampia kuin suuremmalla valoteholla. Valkoisen nauhanosan kohdalla arvot vaihtelevat kuitenkin yli tuhannella. Tilannetta voidaan parantaa lisäämällä hystereesiä, mutta näin huonoja arvoja ei voida kuitenkaan hyväksyä. Mittausten perusteella 4.5mA oli suurimmassa osassa riittävä virta jolla AD-muunninarvojen vaihtelu pysyy tarpeeksi pienenä myös valkoisen nauhanosan kohdalla. Mikäli valoteho on liian pieni, vastaanottavat IR-ledit "näkevät" nauhassa olevat epäideaalisuudet, liian, ilmakuplat ja niin edelleen. Vastaavasti valotehon ollessa liian suuri IR-ledit kuluvat nopeammin ja mustalla nauhanosalla luettu AD-muunninarvo kasvaa suuremmaksi. Koska mustan ja valkoisen nauhanosan erottelussa halutaan käyttää yhtä raja-arvoa, eikä hystereesiä, on mustan nauhanosan AD-muunninarvojen pysyttävä riittävän matalina ja valkoisen nauhanosan vastaavasti riittävän korkeina.

Ajokiskolle sijoitettu sukkula voi kallistua etenemissuuntaansa nähden sivut-

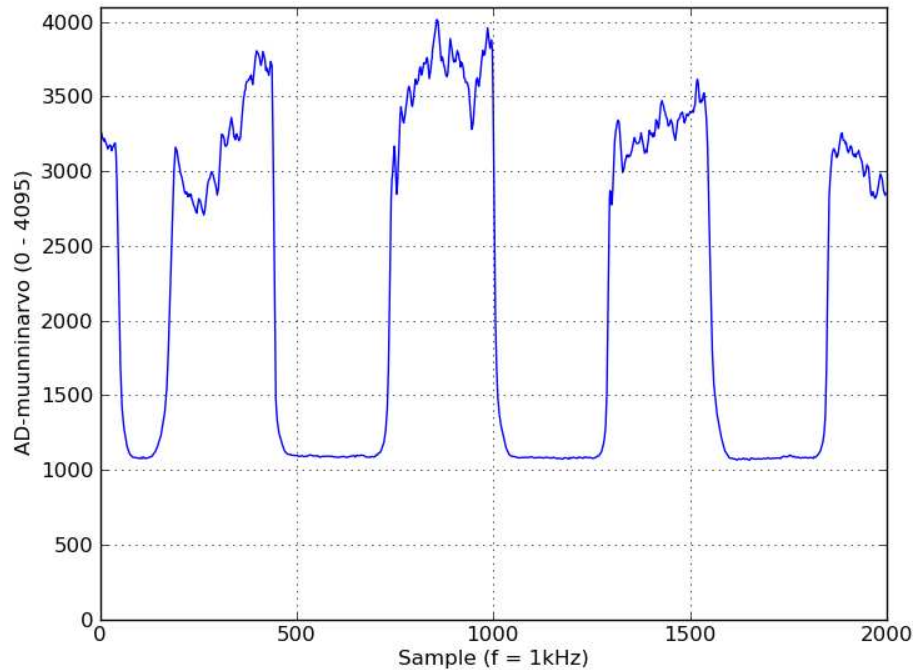


Kuva 5.2: AD-muunninarvo riittäväällä valoteholla



Kuva 5.3: AD-muunninarvo liian vähäisellä valoteholla

taisessa suunnassa esimerkiksi silloin kun sukkulassa olevan paketin painopiste ei ole sukkulan keskellä. Mikäli kallistus on liian suurta, tapahtuu samanlainen ilmiö kuin liian vähäisellä valoteholla. Kuvassa 5.4 on esitetty AD-muunninarvoja yhdellä muuntimella kun viiva-anturia on kallistettu sivuttaissuunnassa noin 20° (Näin suurta kallistus ei normaalisti voi olla).

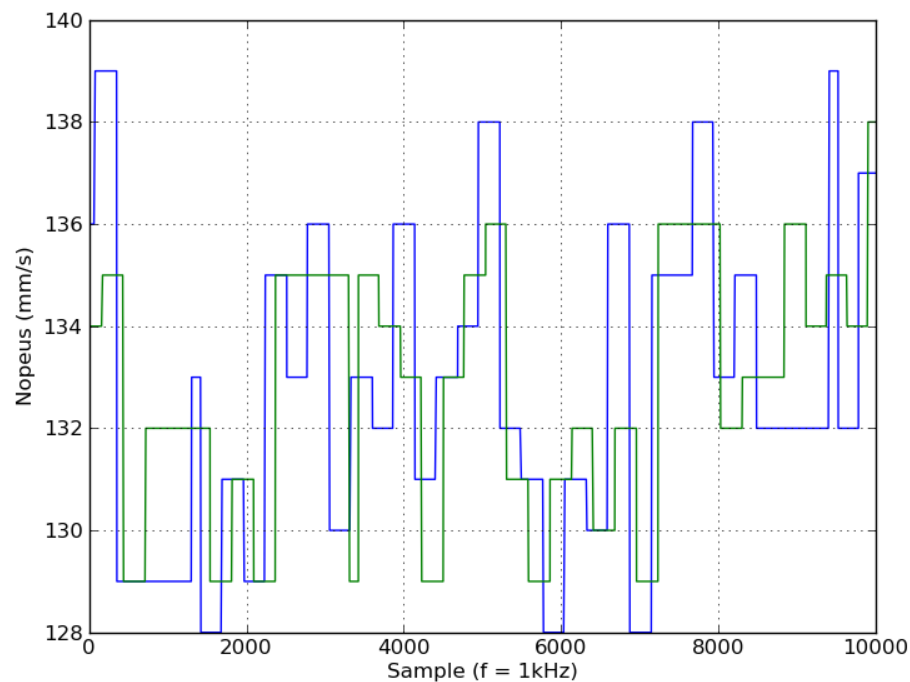


Kuva 5.4: AD-muunninarvo riittävällä valoteholla kun anturia kallistetaan

5.3.2 Häiriötekijöiden vaikutus laskettuun nopeuteen

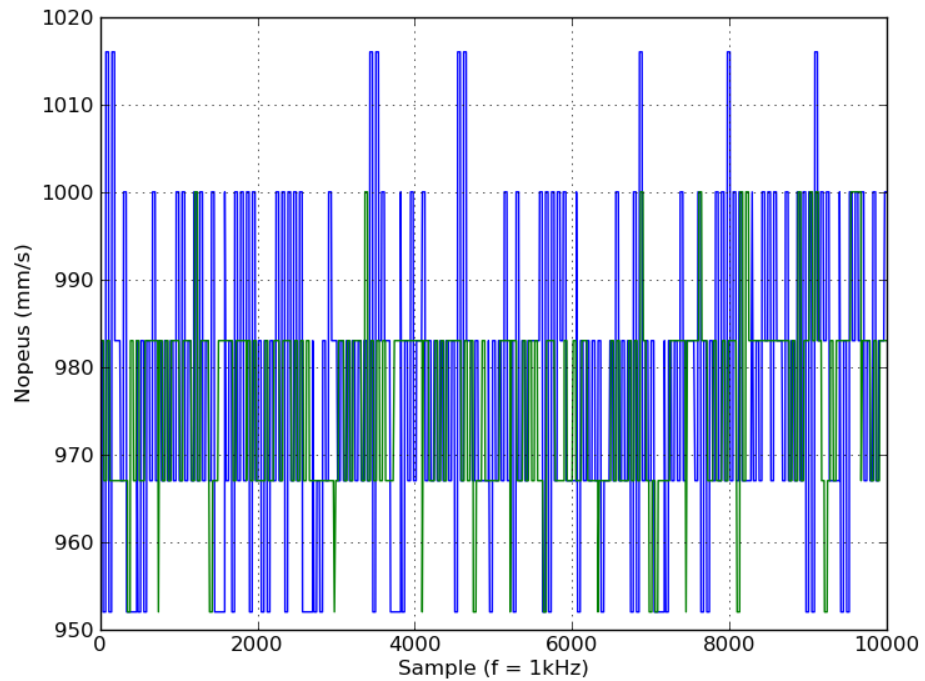
Tutkittaessa viiva-antureilla laskettuja nopeuksia käytettiin mittauksissa 1kHz:n näytteistystaajuutta ja 10s näytteistysaikaa. Kuvassa 5.5 on kahdella viiva-anturilla laskettuja nopeuksia kun IR-ledien läpi kulkeva virta on noin 4.5mA ja DC-moottoria pyöritetään 5V:n jännitteellä. Koska nopeus lasketaan aina kahden saman peräkkäisen IR-ledin ylittäessä saman reunan, pitäisi lasketun nopeuden olla vakio ideaalisessa tapauksessa vakionopeudella. Osittain vaihtelua aiheuttavat viiveet signaalipoluissa, DC-moottorin ohjaus, ajopyörän epätasaiset kitkat, valon heijastukset ja nauhojen reunakohdissa olevat epäideaalisuudet. Yhden suurimmista poikkeamista vakionopeudella aiheuttaa kuitenkin kahden perättäisen IR-ledin tason muutosnopeus ja muutoskohta kun siirrytään mustasta valkoiseen tai valkoisesta mustaan nauhanosaan. Siirryttäessä toiseen suuntaan muutosnopeus on e-

risuuruinen eri ledeillä kuin siirryttäessä toiseen suuntaan. Tämän vuoksi laskettu nopeus muodostaa kanttikuvion jossa lähes joka toinen arvo nousee ylemmäs (valkoisesta mustaan) ja joka toinen laskee alemmas (mustasta valkoiseen). Tämä ei kuitenkaan haittaa niin kauan kuin pysytään 10%-toleranssin sisällä. Kuvasta 5.5 nähdään että poikkeama suurimman ja pienimmän arvon välillä on 11mm/s kun nopeus on keskimäärin 134mm/s. Kuvasta 5.6 nähdään viiva-antureilla laskettuja nopeuksia kun tasajännitelähteestä ohjataan DC-moottoriin 30V, jolloin todellinen nopeus on hieman alle 1m/s. Tässäkin tapauksessa pysytään 10%-toleranssin sisällä ja havaitaan että virhe kasvaa melko lineaarisesti nopeuden kasvaessa.

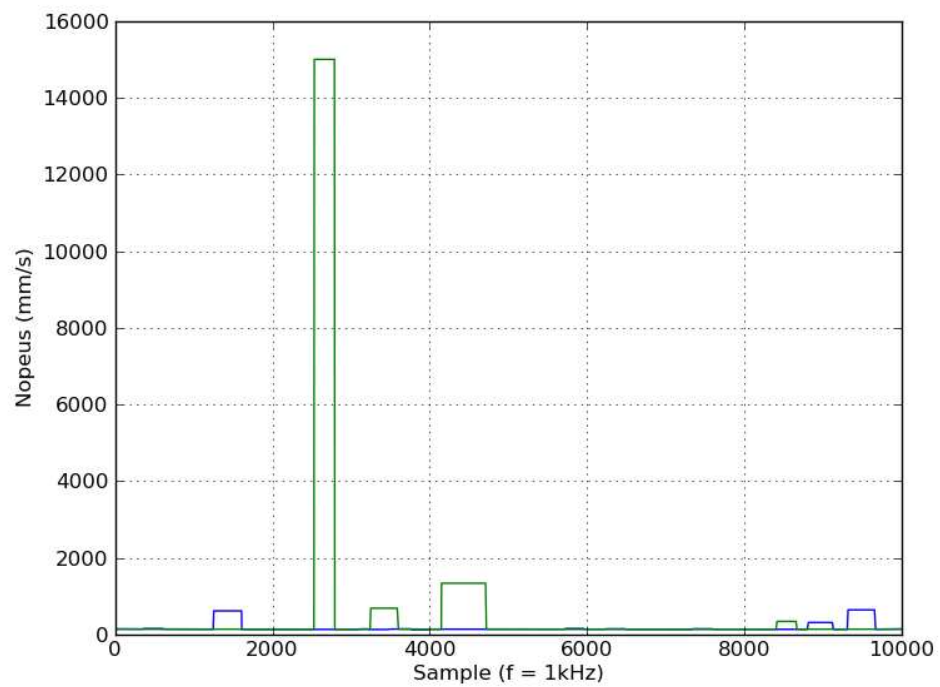


Kuva 5.5: Nopeus kahdella viiva-anturilla riittävällä valoteholla

Kun lähettävissä IR-ledeissä oleva valoteho on liian pieni, eli AD-muunninarvot ovat kuvan 5.3 mukaisia, tapahtuu nopeuden laskennassa virhetulkintoja. Tämä johtaa herkästi ylinopeustilanteeseen sillä peräkkäiset reunat havaitaan liian nopeasti AD-muunninarvojen värähdellessä ääriarvojen välissä. Kuvassa 5.7 on esitetty tulokset kun mittauksessa käytetty valoteho on ollut liian pieni. Kuvassa jokainen korkeampi pylväs edustaa ylinopeustilannetta. Pienelläkin valoteholla virheelliset tulkinnat johtavat värähtelyn takia kuitenkin yleensä turvalliseen vikaantumiseen eli ylinopeustilanteeseen joka laukaisee turvatoiminnon. Vain tapauksessa jossa IR-ledeihin ei johdeta virtaa ollenkaan, ei saada rekisteröityä reunoja ja tällöin nopeus tulkitaan jatkuvasti 0mm/s:ksi.



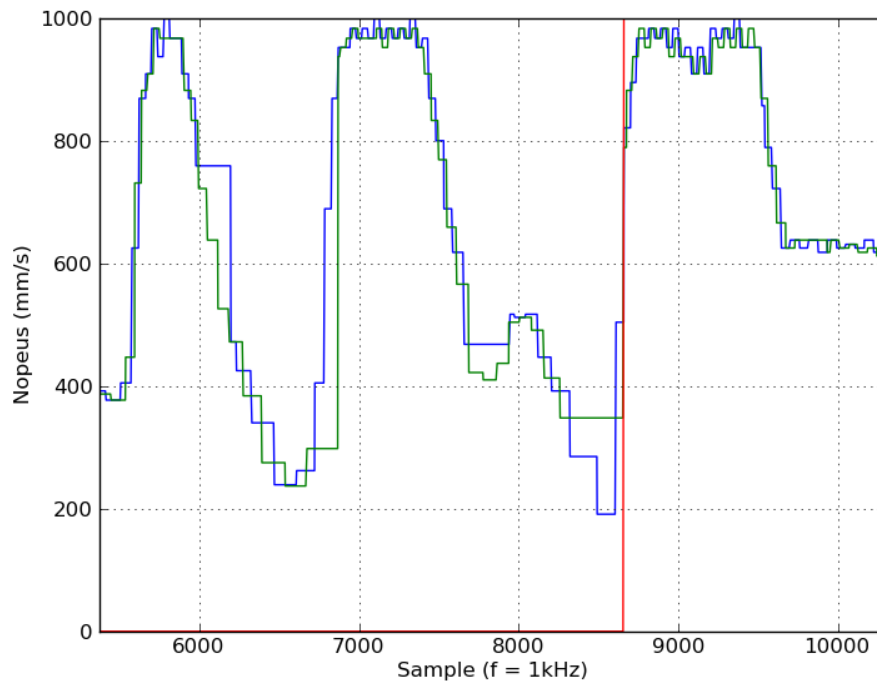
Kuva 5.6: Nopeus kahdella viiva-anturilla riittävällä valoteholla 1



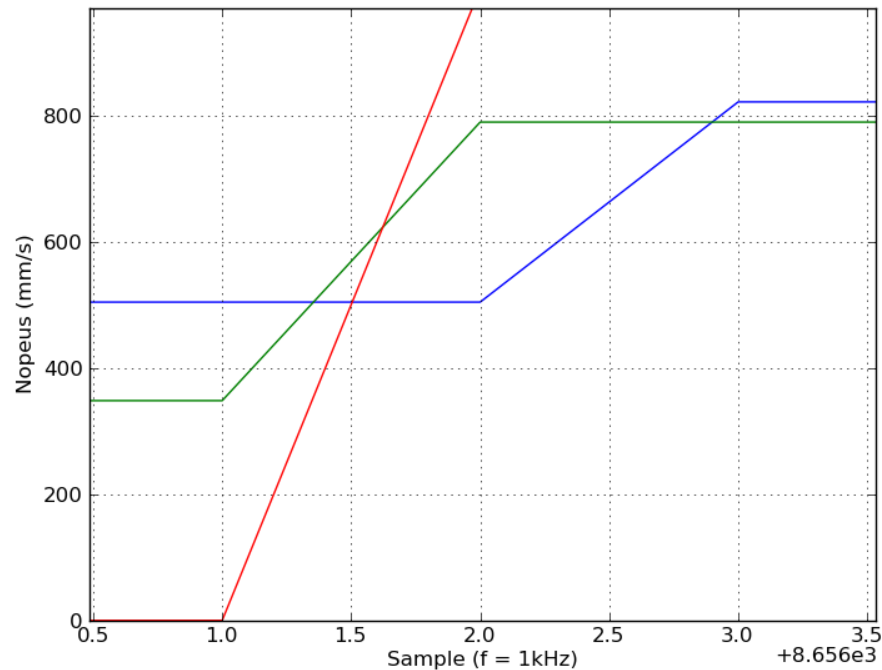
Kuva 5.7: Nopeus kahdella viiva-anturilla liian vähäisellä valoteholla

Kuvassa 5.8 DC-moottoria on kiihdytetty ja hidastettu 30V:n tasajännitelähteellä. Jännitettä on käytetty 0V:n ja 30V:n välillä siten että ollaan lopulta saatu ylitettyä nopeuksien erotuksen maksimi-arvo joka on 0.25m/s. Testilaitteessa olevaan nauhaan oli yhteen kohtaan teipattu mustia ja valkoisia osia joiden pituus oli lyhyempi kuin kahden perättäisen ledin etäisyys viiva-anturissa. Tällaiset nauhanosat aiheuttavat käytännössä sen että nopeutta ei voida rekisteröidä sillä peräkkäiset ledit eivät voi ylittää samaa reunaa kun toinen ledestä on jo rekisteröinyt uuden reunan eri suuntaan.

Kuvasta 5.8 nämä kohdat nähdään varsinkin kiihdytystilanteissa siten että toisella viiva-anturilla laskettu nopeus on muuttunut kolme kertaa samalla kun toisen nopeus ei ole muuttunut kertaakaan. Kohta jossa viiva-antureilla laskettujen nopeuksien erotus on ylittänyt maksimi-arvon, eli ollaan generoitu hätäsignaali, näkyy kuvassa 5.8 pystyviivana nollasta tuhanteen. Kuvassa 5.9 on sama tilanne tarkemmin rajattuna. Kuten siitä nähdään, toisella viiva-anturilla laskettu nopeus on pysynyt noin 0.5m/s:ssa samalla kun toisen nopeus on muuttunut arvoon 0.8m/s.



Kuva 5.8: Ylinopeus kun kahden viiva-anturin nopeuksien erotus on liian suuri



Kuva 5.9: Ylinopeus kun kahden viiva-anturin nopeuksien erotus on liian suuri, tarkennettu

5.4 FPGA-kanavan testaaminen nostolaitteella

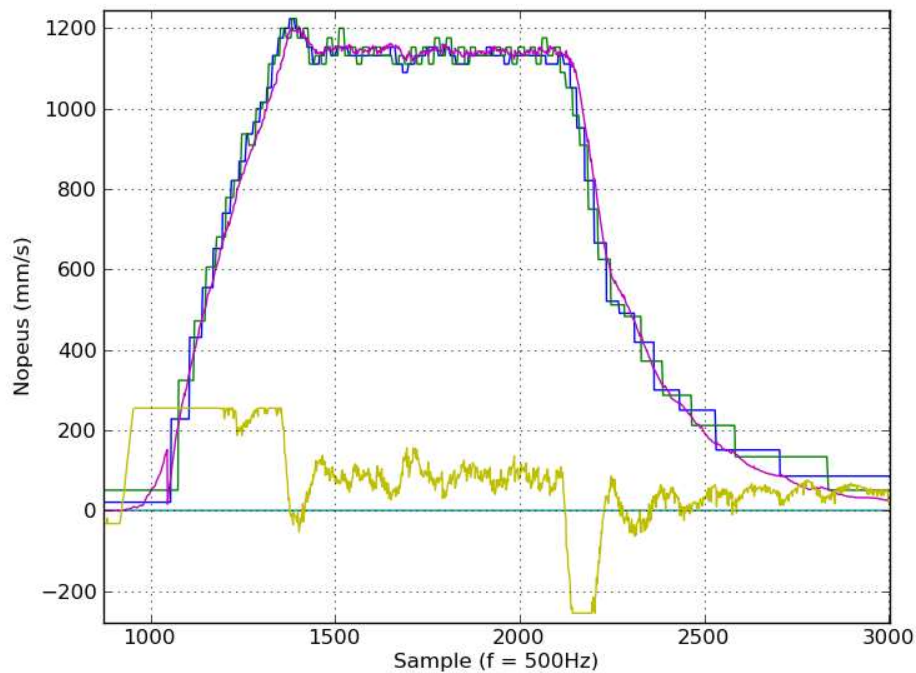
Koko järjestelmää testattiin ajokiskolle asetetulla nostolaitteella jossa ei ollut kapselia kiinni. Nostolaitteen painoksi ilman kapselia on arvioitu 65kg joten kiihtyvyydet saadaan tällä tavalla nostettua korkeammiksi. Turvatoiminnosta oli tässä vaiheessa vasta toisen kanavan toteutus valmiina, siksi MSP:tä ei huomioitu testauksessa. Datan näytteistykseen käytettiin samanlaista menetelmää kuin viiva-antureiden testilaitteen tapauksessakin, eli FPGA:lle kuvattua Nios-prosessoria. Näytteistyksessä käytettiin 500Hz:n taajuutta. Koska nostolaitteen testissä oli koko ketju alusta loppuun asti toteutettuna yhden kanavan osalta, kiinnosti tässä tutkia erityisesti turvatoiminnon vastetta eli sitä kuinka nopeasti turvatoiminto havaitsee ylinopeustilanteen. Lisäksi pyrittiin selvittämään kuinka nopeasti nostolaite pysähtyy ja kuinka pitkä jarrutusmatka nostolaitteella on.

Kiihdytysvaiheessa ajomoottoreita ajetaan ensin maksivääntömomentilla, kunnes ollaan saavutettu haluttu vakionopeus. Edelleen jarrutusvaiheessa jarrutetaan maksimivääntömomentilla. Moottoreita ohjataan PID-säätimellä joka on tässä järjestelmässä käytännössä PI-säädin. Testissä käytettiin kahta ajomoottoria joista molempien teoreettinen vääntömomentti on maksimissaan 4.0Nm. Kuitenkin ohjattaessa ajomoottoreita vääntömomentti jää käytännössä 3.0Nm:n tasolle. Ajomoot-

toreiden kulma-antureilta saatava nopeus on skaalattu vastaamaan viiva-antureiden nopeutta mutta se ei ole kuitenkaan tarkka arvo. Nopeus on lisätty sen vuoksi että nähtäisiin kahdella eri tekniikalla toteutetun nopeudenlaskennan vastaavuus toisiinsa.

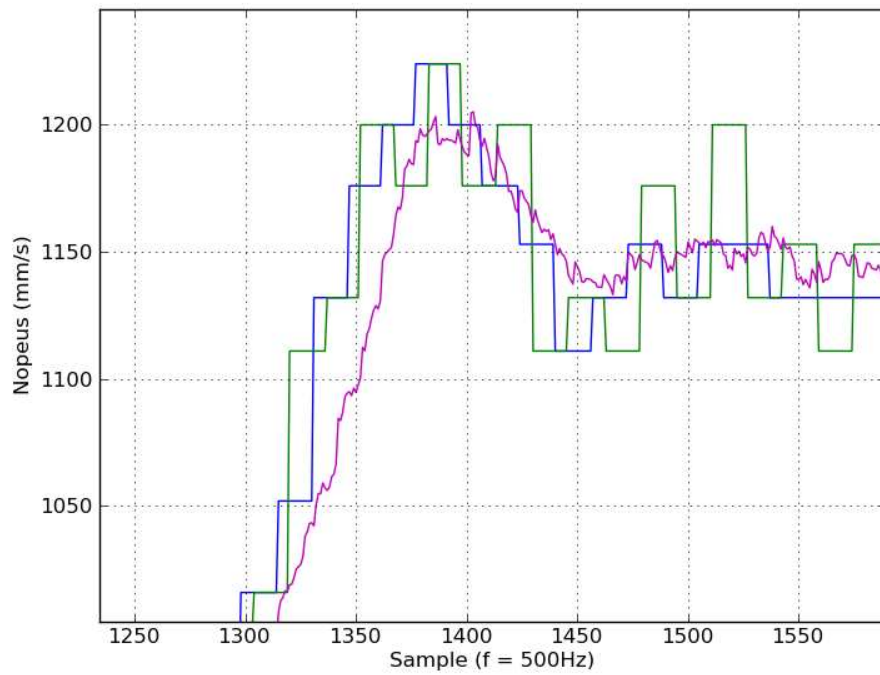
5.4.1 Normaaliajo ilman ylinopeutta

Kuva 5.10 esittää tilannetta jossa nostolaitetta on ajettu normaalisti ylinopeusvahdin nopeusrajan ollessa 1.25m/s. Kuvassa epätarkalla resoluutiolla olevat sininen ja vihreä kuvaaja edustavat viiva-antureiden datasta laskettuja nopeuksia, violetti kuvaaja edustaa skaalattua ajomoottoreiden kulma-antureiden datasta laskettua nopeutta ja keltainen vääntömomenttia jolla moottoria ajetaan. Kuvissa 5.11 ja 5.12 on rajatutimmat kuvat kiihdytyksen loppuvaiheesta sekä jarrutuksen alkuvaiheesta joista nähdään paremmin viiva-antureiden datasta laskettujen nopeuksien vaihtelut sekä kulma-antureiden datasta laskettu nopeus.

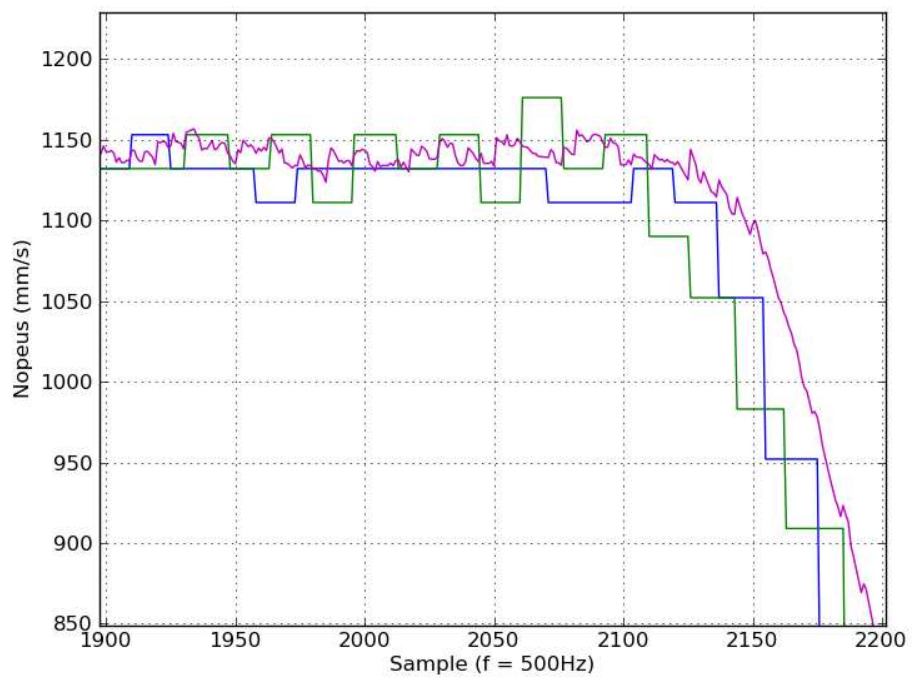


Kuva 5.10: Normaaliajo 2.5m:n matkalla kun nopeusraja asetettu arvoon 1.25m/s

Kiihdytyksessä ja jarrutuksessa ajomoottoreiden vääntömomentti on hetkellisesti maksimissaan jolloin arvot ovat kuvassa joko -255 tai 255 suunnasta riippuen. Newtonmetreinä mitattuna vääntömomentit ovat hieman yli 3Nm molempiin suuntiin. Moottorin säätimelle on asetettu maksiminopeudeksi noin 1.25m/s ja huippuarvo



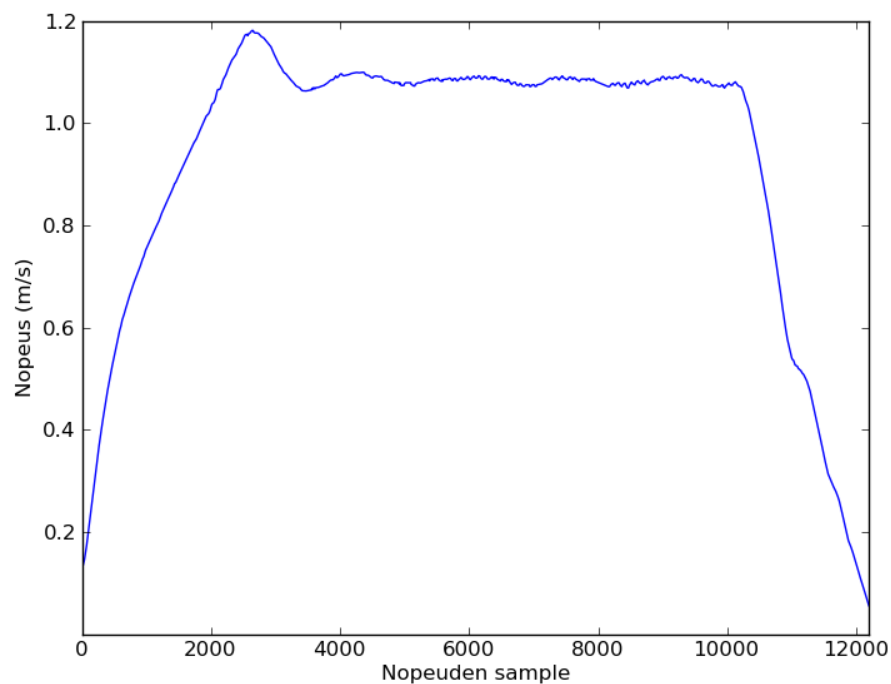
Kuva 5.11: Normaaliajo, tarkennus kiihdytyksestä



Kuva 5.12: Normaaliajo, tarkennus jarrutuksesta

joka tässä saavutetaan kiihdytyksen aikana on 1.23m/s , joten nopeusrajaksi asetettu 1.25m/s on kireä. Kun nostolaitetta ajettiin 48-tunnin ajolla edestakaisin lähellä tätä asetettua maksiminopeutta, ei ylinopeusvahti lauennut kertaakaan. Maksiminopeus joka saavutettiin yhteen suuntaan liikuttaessa oli tällöin aina 5%:n sisällä ylinopeusvahdille asetetusta nopeusrajasta joten ylinopeusvahti on riittävän robusti.

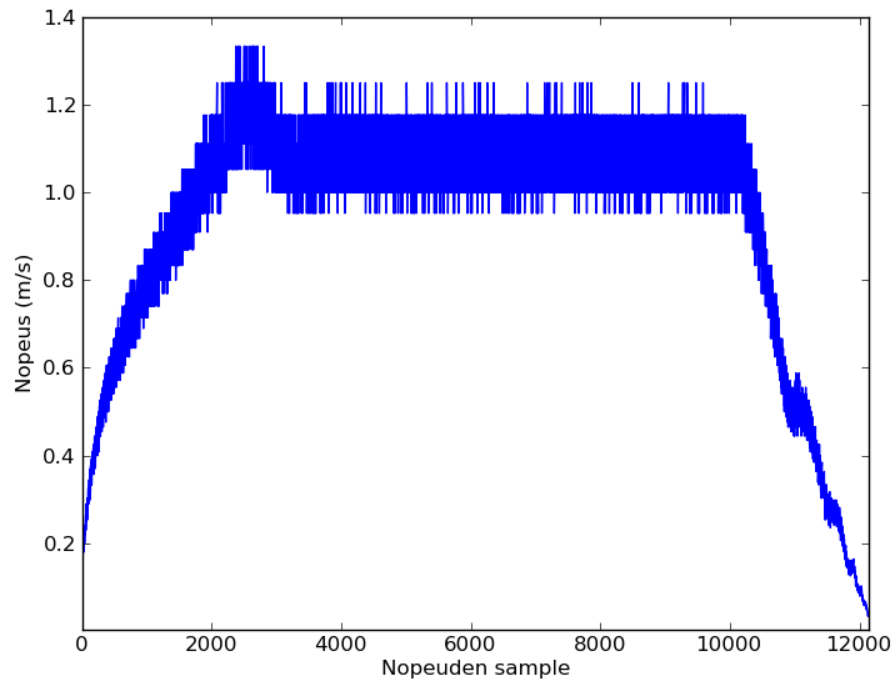
Kuvassa 5.13 on esitetty inkrementaalianturista IV58M mitatun datan perusteella laskettu nopeus suodatettuna. Kuvassa 5.14 on sama tulos suodattamattomana. Kun tuloksia verrataan viiva-antureilla laskettuun nopeuteen, huomataan että nopeudet poikkeavat maksiminopeudella noin 0.04m/s toisistaan, eli noin 3%. Kaikki epävarmuustekijät huomioonottaen tätä voidaan pitää riittävänä tarkkuutena.



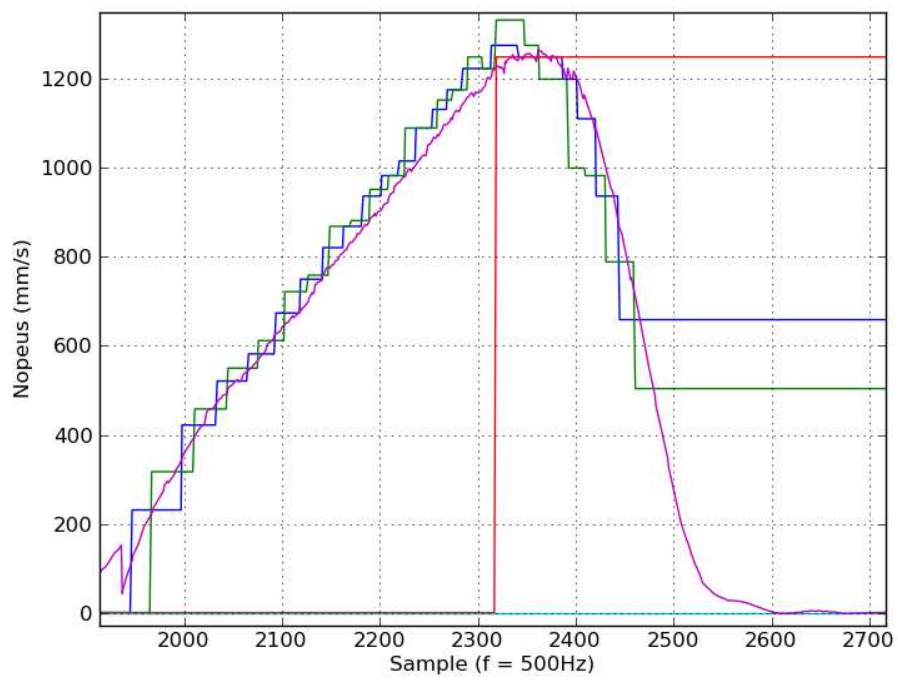
Kuva 5.13: Magneettisen inkrementaalianturin tulos suodatettuna

5.4.2 Ylinopeusvahdin laukeaminen

Kuva 5.15 esittää tilannetta missä ylinopeusvahdin nopeusraja on asetettu arvoon 1.25m/s ja nostolaitetta on kiihdytetty siten että turvatoiminto on lauennut. Kuvassa sininen ja vihreä kuvaaja edustavat viiva-antureiden datasta laskettua nopeutta ja violetti kuvaaja skaalattua ajomoottoreiden kulma-antureiden datasta laskettua nopeutta. Punainen kuvaaja osoittaa hetkeä jolloin ylinopeus on havaittu nousemalla asetettuun nopeusrajaan.



Kuva 5.14: Magneettisen inkrementaalianturin tulos suodattamattomana



Kuva 5.15: Ylinopeus kun nopeusraja asetettu arvoon 1.25m/s

Ylinopeus havaitaan FPGA:n ohjauslogiikassa välittömästi kun toisen viiva-anturin nopeus on kasvanut yli asetetun nopeusrajan. Käytännössä viiva-anturilta saadaan näyttöä 4.545kHz:n taajuudella ja reunan muutoksia lasketaan aina kolmen peräkkäisen arvon ollessa samoja. Näin muutos rekisteröidään nopeimmillaan 1.5kHz:n taajuudella. Kuvan ja näytteistetyn datan perusteella koko jarrutusmatkaan käytetty aika on noin 0.57s ylinopeuden havaitsemisesta siihen että nostolaite on kokonaan pysähtynyt. Aika joka kuluu ylinopeuden havaitsemisesta jarrutuksen aloittamiseen on noin 0.16s. Tänä aikana nopeus on laskenut 50mm/s siitä kun ylinopeus havaittiin. Kun jarrut ovat menneet kiinni ja moottoreilta on katkaistu jännitteet, tapahtuu jarrutus noin hidastuvuudella $4.4\frac{m}{s^2}$. Hidastuvuuden ollessa tasaista aikaa kuluu 0.26s ja tällöin nostolaitteen nopeus on laskenut arvosta 1.2m/s arvoon 0.06m/s eli nostolaite on käytännössä pysähtynyt. Koko jarrutusmatkan keskihidastuvuus voidaan laskea kun tiedetään että jarrutuksessa aikaa kuluu noin 0.4s ja tällöin nopeus laskee arvosta 1.25m/s nolnaan. Tällöin hidastuvuus on $a = \frac{1.25m/s}{0.4s} = 3.1\frac{m}{s^2}$.

Ajomootoreiden jarrut kykenevät jarruttamaan valmistajan mukaan noin 8Nm:n vääntömomentilla. Kun ajomootoreita on kaksi ja nostolaitteen paino on 65kg, saadaan hidastuvuudeksi

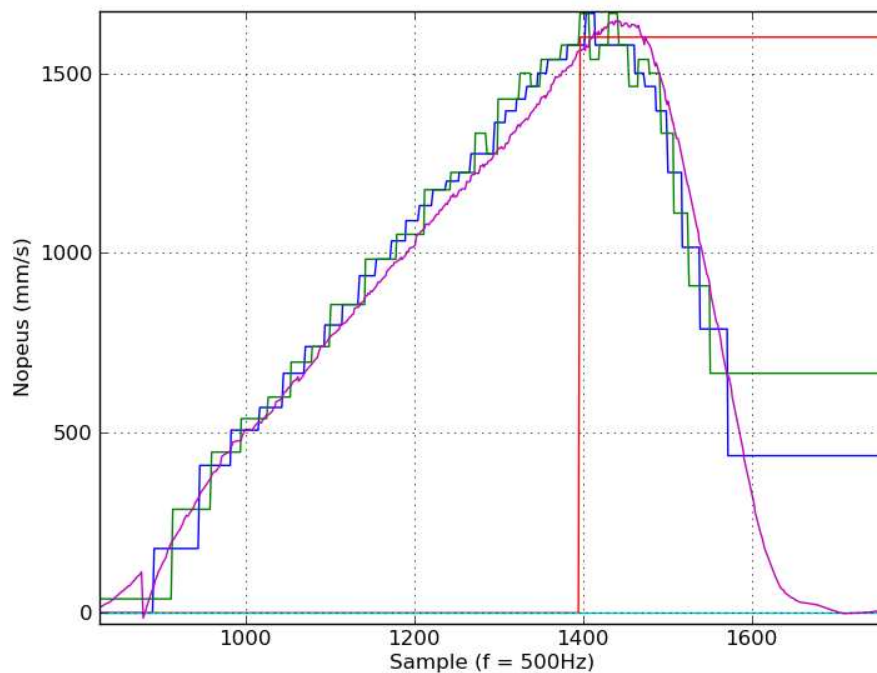
$$a = \frac{2\tau}{rm} = \frac{2 \times 8Nm}{0.05m \times 65kg} = 4.9\frac{m}{s^2} \quad (5.2)$$

Teoreettisesti laskettu arvo $4.9\frac{m}{s^2}$ on riittävän lähellä nostolaitteen jarrutuksessa saatujen tietojen pohjalta laskettua maksimiarvoa $4.4\frac{m}{s^2}$. Molemmissa tavoissa laskea on epävarmuustekijöitä. Tarkkaa arvoa jarrujen vääntömomentille ei ole tiedossa ja jarrutuksen aloitusajankohta on mittauksissa tulkinnanvarainen. Jarrutusmatkan ja hidastuvuuden laskeminen on kuitenkin lähinnä suuntaa antavaa, tarkkoja arvoja ei tässä työssä tarvita. Täytyy myös huomata että vääntömomentin pohjalta lasketussa arvossa ei ole huomioitu esimerkiksi kitkoja jotka kasvattavat hidastuvuutta. Kuvasta 5.15 nähdään että nostolaitteen liike hidastuu noin kaksi kertaa nopeammin kuin mitä nostolaite kiihtyy ohjattaessa ajomootoreita maksimimomentilla. Koska teoreettinen maksimikiihtyvyys nostolaitteelle kahdella ajomootorilla on $2.4\frac{m}{s^2}$, voidaan olettaa kuvan 5.15 ja saatujen tulosten perusteella että hidastuvuus on luokkaa $4.8\frac{m}{s^2}$.

Kulma-antureiden datasta saadun nostolaitteen aseman perusteella havaitaan että nostolaite liikkuu noin 4000 yksikköä jarrutuksen aikana. Kun yksi kierros on jaettu 4095:een osaan ja ajopyörän halkaisija on 10cm, saadaan jarrutusmatkaksi $(4000/4095) \times \Pi \times 10cm = 30cm$. Lähes samaan arvoon päästään kun havaitaan että viiva-anturit päivittävät jarrutuksen aikana uuden nopeuden 8 kertaa ja yhden viivanosan pituus on 3.6cm. Tästä saadaan jarrutusmatkaksi $8 \times 3.6cm = 29cm$.

Jarrutuksen aloitusajankohdaksi on valittu hetki jolloin ylinopeusvahti havaitsee ylinopeuden. Jarrut eivät kuitenkaan mekaanisesti sulkeudu vielä tällöin. Viivettä aiheuttaa ohjaussignaalien kulkeutuminen turvakytkentöihin, tehon poistuminen asteittain turvakytkennöistä sekä jarrujen mekaniikka. Tehot moottoreilta poistuvat nopeammin kuin jarrut sulkeutuvat, joten nostolaite liikkuu hetken aikaa vapaalla turvatoiminnon laukeamisen jälkeen. Tämä voidaan nähdä myös kuvasta 5.15 jossa hidastuvuus ei välittömästi nouse maksimiarvoonsa.

Kuva 5.16 esittää tilannetta missä ylinopeusvahdin nopeusraja on asetettu arvoon 1.60m/s ja nostolaitetta on kiihdytetty siten että turvatoiminto on lauennut. Tässä koko jarrutukseen käytetty aika on noin 0.61s ylinopeuden havaitsemisesta siihen että nostolaite on pysähtynyt. Jarrutusmatkaksi saadaan 43cm kulma-anturin datasta ajomoottorin aseman perusteella laskemalla ja sama arvo viiva-antureiden päivitysten määrästä. Viiva-anturin arvo päivittyy 12 kertaa jolloin matka on $12 \times 3.6\text{cm} = 43\text{cm}$. Edelleen kulman perusteella nostolaite liikkuu 5654 yksikköä jolloin kuljettu matka on $(5654/4095) \times \Pi \times 10\text{cm} = 43\text{cm}$. Hidastuvuus on maksimissaan noin $4.8 \frac{\text{m}}{\text{s}^2}$ ja keskihidastuvuudeksi koko matkalle saadaan $3.2 \frac{\text{m}}{\text{s}^2}$ mikä on samaa luokkaa kuin ylinopeusvahdin nopeusrajan ollessa $1.25 \frac{\text{m}}{\text{s}}$.



Kuva 5.16: Ylinopeus kun nopeusraja asetettu arvoon 1.60m/s

6. YHTEENVETO

Tässä työssä oli tavoitteena suunnitella ja toteuttaa varastojärjestelmään ylinopeusvahti jolla estetään varaston sisällä olevan sukkulan ylinopeus. Vaatimukset suunnittelulle ja toteutukselle tulivat konedirektiivin 2006/42/EY kautta. Konedirektiiviin kuuluvassa standardissa SFS-EN ISO 13849-1, jota tähän järjestelmään sovellettiin, turvallisuuden taso määritellään suoritustasojen (PL) kautta. Riskianalyysin perusteella ylinopeusvahdilta vaadittavaksi suoritustasoksi (PL_r) saatiin c.

Turvatoiminnossa käytettävä laitteisto oli jo olemassa ennen suunnittelun aloittamista. Tästä syystä jouduttiin vaatimusten kartoittaminen tekemään siten että standardista valittiin nimetty rakenne johon olemassaoleva toteutus sopii ja laskettiin sitten tälle toteutukselle laitteiston osalta suoritustaso johon se kykenee. Olemassaoleva laitteisto asetti $MTTF_d$:n osalta rajoitukset joihin voitiin vaikuttaa ainoastaan viiva-antureissa olevien IR-ledien virtaa säätämällä. Ledien virraksi valittiin 9mA jolloin ledeillä saadaan $MTTF_d$:ksi 46-vuotta. Alijärjestelmissä tavoiteltiin $MTTF_d$:lle tasoa keskimääräinen ja DC_{avg} :lle tasoa matala. Ohjauslogiikoiden ja lähtöjen osalta tämä onnistui mutta tulojen viiva-antureiden $MTTF_d$ sai arvon matala jonka vuoksi alijärjestelmän suoritustasoa kasvatettiin nostamalla sen DC_{avg} 90%:iin.

Suoritustaso (PL) johon ylinopeusvahti kykenee laskettiin ottamalla huomioon standardissa SFS-EN ISO 13849-1 määritetyt parametrit. Lähestymistavoista käytettiin standardissa esitettyä yksinkertaistettua menetelmää. Laitteiston komponenttien vikaantumisaajat ($MTTF_d$) laskettiin SISTEMA:lla. Valvonnan taso (DC_{avg}) sensijaan arvioitiin ohjelmiston suunnittelun kautta ja alijärjestelmien yhdistetyksi DC_{avg} :ksi saatiin 81%. Kun kaikki parametrit otettiin huomioon, saatiin koko järjestelmän vikaantumisajaksi $2.66E-6$ (PFH) joka vastaa suoritustasoa c. Turvatoiminto on siis suunnittelun osalta riittävä sille asetettuihin vaatimuksiin nähden.

Toteutuksen osalta työssä saatiin valmiiksi kokonaisuudessaan toinen kanava. Kanavan toiminta testattiin ja toteutus todettiin riittävän robustiksi, tarkaksi sekä vasteeltaan tarpeeksi nopeaksi. Koska kanavien toimintaperiaate on samanlainen, voidaan todeta että turvatoiminnossa käytetyllä suunnittelulla täytetään sille asetetut vaatimukset. Turvatoiminnolle tehtiin myös vika -ja vaikutusanalyysi vaarallisten vikojen löytämiseksi sekä suunniteltiin järjestelmätestit analyysin pohjalta.

LÄHTEET

- [1] 2006/42/EY. 2006, 1. painos. Konedirektiivi. Euroopan parlamentti ja Euroopan unionin neuvosto.
- [2] 2006/42/EY Soveltamisopas. 2010, 2. painos. Konedirektiivin soveltamisopas. Euroopan komissio, yritys -ja teollisuustoiminta.
- [3] Ylinopeusvahdin vaatimusmäärittely. 2012. Konecranes Oyj (STEO).
- [4] Hietikko, M., Malm, T., & Alanen, J. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus. Espoo 2009, Valtion teknillinen tutkimuskeskus (VTT) Tiedotteita 2485. 75 s. + liit. 14 s.
- [5] SFS-EN ISO 14121-1. 2007. KONETURVALLISUUS. Riskin arviointi. Osa 1: Periaatteet. Suomen standardisoimisliitto SFS.
- [6] SFS-EN ISO 12100-1. 2003. KONETURVALLISUUS. Perusteet ja yleiset suunnitteluperiaatteet. Osa 1: Peruskäsitteet ja menetelmät. Suomen standardisoimisliitto SFS.
- [7] SFS-EN 61058-1. 2011, 2. painos. Sähköisten/elektronisten/ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallinen turvallisuus. Osa 1: yleiset vaatimukset. Suomen standardisoimisliitto SFS.
- [8] SFS-EN 62061. 2005. KONETURVALLISUUS. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus. Suomen standardisoimisliitto SFS.
- [9] Lereverend, P. Inside the standardization jungle: IEC 62061 and ISO 13849-1, complementary or competing?. 2008. IEEE. 5 s.
- [10] SFS-EN ISO 13849-1. 2007. KONETURVALLISUUS. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. Suomen standardisoimisliitto SFS.
- [11] SFS-EN ISO 13849-2. 2008, 2. painos. KONETURVALLISUUS. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 2: Kelpuutus. Suomen standardisoimisliitto SFS.
- [12] MSP430x2xx MIPS [WWW]. [viitattu 27.01.2012]. Saatavissa: <http://focus.ti.com/paramsearch/docs/parametricsearch.tsp?familyId=912§ionId=95&tabId=1528&family=mcu>

- [13] MSP430x2xx Family User's Guide [WWW]. [viitattu 27.01.2012]. Saatavissa: www.ti.com/lit/ug/slau144i/slau144i.pdf
- [14] Osram reliability and lifetime of LEDs [WWW]. [viitattu 23.01.2012]. Saatavissa: http://catalog.osram-os.com/jsp/download.jsp?rootPath=/media/&name=Reliability_and_Lifetime_of_LEDs.pdf&docPath=Graphics/00046672_0.pdf&url=/media//_en/Graphics/00046672_0.pdf
- [15] Avago HSDL-x42x reliability [WWW]. [viitattu 23.01.2012]. Saatavissa: <http://forums.avagotech.com/showthread.php?740-How-can-the-lifetime-or-MTTF-of-optocouplers-be-estimated-with-LEDs-operated-at-various-stress-conditions-%28different-drive-currents-and-different-operating-temperatures%29&p=741%www.avagotech.com/docs/5988-3940EN>
- [16] Avago Designers guide to isolation circuits [WWW]. [viitattu 23.01.2012]. Saatavissa: www.avagotech.com/docs/5989-0802EN
- [17] Avago phototransistor reliability [WWW]. [viitattu 23.01.2012]. Saatavissa: www.avagotech.com/docs/5988-8640EN
- [18] Fail rates for fiber optic [WWW]. [viitattu 23.01.2012]. Saatavissa: <http://www.theriac.org/informationresources/demosanddownloads/Unlimited%20Distribution/Fail%20Rates%20for%20Fiber%20Optic%20Assys%20ADA092315.pdf>
- [19] IEC 60664-3:2003/A1:2010. Insulation coordination for equipment within low-voltage systems. Part 3: Use of coating, potting or moulding for protection against pollution. Cenelec.
- [20] EN 50178:1997. Electronic equipment for use in power installations. Cenelec.
- [21] MSP430x2xx Datasheet [WWW]. [viitattu 09.02.2012]. Saatavissa: <http://www.ti.com/lit/gpn/msp430f123>
- [22] Cyclone III Device Data Sheet [WWW]. [viitattu 09.02.2012]. Saatavissa: http://www.altera.com/literature/hb/cyc3/cyc3_ciii52001.pdf
- [23] SFS-EN 55022. 2008, 1. painos. Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement. Suomen standardoimisliitto SFS.
- [24] SFS-EN 61000-4-3. 2006, 1. painos. Electromagnetic compatibility (EMC). Part 4-3: Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test. Suomen standardoimisliitto SFS.

- [25] SFS-EN 61000-4-6. 2008, 1. painos. Electromagnetic compatibility (EMC). Part 4-6: Testing and measurement techniques - Immunity to conducted disturbances, induced by radio-frequency fields. Suomen standardoimisliitto SFS.
- [26] SFS-EN 61000-4-4. 2008, 1. painos. Electromagnetic compatibility (EMC). Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test. Suomen standardoimisliitto SFS.
- [27] SFS-EN 61000-4-5. 2008, 1. painos. Electromagnetic compatibility (EMC). Part 4-5: Testing and measurement techniques - Surge immunity test. Suomen standardoimisliitto SFS.
- [28] IEC 60812:2006. Analysis techniques for system reliability - Procedure for failure mode and effect analysis (FMEA). Cenelec.
- [29] IV58M Magneettinen inkrementaalianturi [WWW]. [viitattu 20.07.2012]. Saatavissa: http://www.sikoproducts.com/pdf/KDB_IV58M_Magnetic-incremental-encoder_2-1_08-2011_E.pdf

A. LIITE: KOMPONENTTIEN MTTF-ARVOJA

Taulukossa A.1 on ilmoitettu vaarallisten vikaantumisten aikoja turvatoiminnon suorittaville komponenteille. Komponentit on jaoteltu alijärjestelmien ja kanavien mukaisesti.

Niille komponenteille joiden vikaantumisaajat on otettu standardista on kerrottu $MTTF_d$:n lisäksi standardin liitteessä C oleva taulukko josta arvot löytyvät.

Taulukko A.1: Komponenttien MTTF-arvoja

Alijärjestelmä	Komponentti	$MTTF_d$ (a)	Standardista
Sisääntulo Viiva-anturi	LMV821	93952	-
Sisääntulo Viiva-anturi	TPS73033	285388	-
Sisääntulo Viiva-anturi	ADS7886	126839	-
Sisääntulo Viiva-anturi	SN65LVDS2	39363	-
Sisääntulo Viiva-anturi	MSP430F2001	18721	-
Sisääntulo Viiva-anturi	IR-ledi HSDL-5420	100	-
Sisääntulo Viiva-anturi	IR-ledi HSDL-4420-011	46	-
FPGA-ohjainkortti	EP3C55F484C8N	8583	-
FPGA-ohjainkortti	MSP430F235	18721	-
SAFETY-jarru	IRS2101SPBF	601	-
SAFETY-moottori	IRS2101SPBF	601	-
SAFETY-moottori	TL431CDBZ	95129	-
Passiivikomponentit	Vastus (Metallikalvo)	114155	C.5
Passiivikomponentit	Kondensaattori (Keraaminen)	4566	C.4
Passiivikomponentit	Kondensaattori (Elektrolyytti)	4566	C.4
Passiivikomponentit	Kuristin	4566	C.6
Passiivikomponentit	Diodi (Tasasuuntaussilta)	2283	C.3
Passiivikomponentit	Diodi (Yleiskäyttöinen)	22831	C.3
Passiivikomponentit	FET	4566	C.2
Passiivikomponentit	Tehotransistori	228	C.2

Kaikilla komponenteilla pahin mahdollinen tapaus $MTTF_d$:lle on määritelty SISTEMAAN siten että otetaan kymmenen prosenttia lasketusta arvosta. Jos esim. $MTTF_d = 10000$ vuotta, käytetään arvoa 1000 vuotta. Vain IR-ledien tapauksessa on käytetty suoraan annettua $MTTF_d$:tä.

LMV821

Valmistaja ilmoittaa MTTF:ksi 823024794 tuntia eli 93952 vuotta.

<http://www.national.com/pf/LM/LMV821.html#Reliability>

TPS73033

Valmistaja ilmoittaa FIT = 0.4 josta MTTF = 285388 vuotta.

<http://focus.ti.com/quality/docs/singlesearchresults.tsp?&templateId=5909&navigationId=11213&appType=folders&searchType=orderableOption&partialSearch=false&mtbfType=true&orderablePartNumber=TPS73033DBVR>

ADS7886

Valmistaja ilmoittaa FIT = 0.9 josta MTTF = 126839 vuotta

<http://focus.ti.com/quality/docs/singlesearchresults.tsp?&templateId=5909&navigationId=11213&appType=folders&searchType=orderableOption&partialSearch=false&mtbfType=true&orderablePartNumber=ADS7886SBDBVR>

SN65LVDS2

Valmistaja ilmoittaa FIT 2.9 josta MTTF = 39363 vuotta.

<http://focus.ti.com/quality/docs/singlesearchresults.tsp?&templateId=5909&navigationId=11213&appType=folders&searchType=orderableOption&partialSearch=false&mtbfType=true&orderablePartNumber=SN65LVDS2D>

MSP430F2001

Valmistaja ilmoittaa MTTF:ksi 164000000 tuntia eli 18721 vuotta.

<http://mtbf.polimore.com/index.php?P=20044110108&F=create.microcircuits.html&SHAREDMTBF=0K&ID=270>

HSDL-5420 + HSDL-4420-011

Valmistajan ilmoittamaa kaavaa soveltavalla laskentamenetelmällä saamme lasketua MTTF:ksi 46 vuotta kun virta on 9mA ja ympäristön maksimilämpötila 50C.

<http://www.avagotech.com/docs/5988-3940EN> (Arrheniuksen kaava yleisesti)

<http://forums.avagotech.com/showthread.php?740-How-can-the-lifetime-or-MTTF-of-optocouplers-be-estimated-with-LED-s-operated-at-various-stress-conditions-%28different-drive-currents-and-different-operating-temperatures%29&highlight=DESIGNER%27s+GUIDE+ISOLATION+CIRCUITS>

EP3C55F484C8N

Valmistajan luotettavuusraportista saadaan 8583 vuotta
www.altera.com/literature/rr/rr.pdf

MSP430F235

Valmistaja ilmoittaa MTTF:ksi 164000000 tuntia eli 18721 vuotta
<http://mtbf.polimore.com/index.php?P=20044110108&F=create.microcircuits.html&SHAREDMTBF=OK&ID=270>

IRS2101SPBF

Valmistaja ilmoittaa 5214439 tuntia eli 595 vuotta.
<http://www.irf.com/technical-info/appnotes.htm>

TL431CDBZ

Valmistaja ilmoittaa FIT = 1.2 josta MTTF = 95129 vuotta.
<http://focus.ti.com/quality/docs/singlesearchresults.tsp?&templateId=5909&navigationId=11213&appType=folders&searchType=orderableOption&partialSearch=false&mtbfType=true&orderablePartNumber=TL431CD>

B. LIITE: BETA-TEKIJÄ

Taulukko B.1: Beta-tekijä lähdöt

Item	X	Y	S
Separation/segregation			
Are all signal cables for the channels routed separately at all positions?	1.0	2.0	4.0
If the sensor/final elements have dedicated control electronics, is the electronics for each indoors and in separate cabinets?	2.5	1.5	6.5
Diversity/redundancy			
Do the devices employ different electrical principles/designs, for example, digital and analogue, different manufacturer (not re-badged) or different technology?	6.5		13.0
Complexity/design/application/maturity/experience			
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	1.0	1.0	3.0
Assessment/analysis and feedback of data			
Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)	0.5	3.5	4.5
Procedures/human interface			
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.) intended to be independent of each other, are not to be relocated?	0.5	0.5	1.5
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0.5	1.5	2.5
Environmental control			
Is personnel access limited (for example locked cabinets, inaccessible position)?	0.5	2.5	3.5
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3.0	1.0	7.0
Environmental testing			
Has the system been tested for immunity to all relevant environmental influences.. ?	10.0	10.0	30.0
Yhteensä			75.5

Taulukko B.2: Beta-tekijä logiikka

Item	X	Y	S
Separation/segregation			
Are all signal cables for the channels routed separately at all positions?	1.5	1.5	4.5
Are the logic subsystems physically separated in an effective manner? For example, in separate cabinets.	2.5	0.5	5.5
Diversity/redundancy			
Do the channels employ different electronic technologies for example, one electronic, the other programmable electronic?	6.0	0.0	12.0
Complexity/design/application/maturity/experience			
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	0.5	1.0	2.0
Assessment/analysis and feedback of data			
Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)	0.5	3.5	4.5
Procedures/human interface			
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0.5	1.0	2.0
Competence/training/safety culture			
Have designers been trained (with training documentation) to understand the causes and consequences of common cause failures?	2.0	3.0	7.0
Environmental control			
Is personnel access limited (for example locked cabinets, inaccessible position)?	0.5	2.5	3.5
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3.0	1.0	7.0
Environmental testing			
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10.0	10.0	30.0
Yhteensä			78.0

Taulukko B.3: Beta-tekijä sensorit

Item	X	Y	S
Separation/segregation			
Are all signal cables for the channels routed separately at all positions?	1.0	2.0	4.0
If the sensor/final elements have dedicated control electronics, is the electronics for each channel on separate printed-circuit boards?	2.5	1.5	6.5
If the sensor/final elements have dedicated control electronics, is the electronics for each indoors and in separate cabinets?	2.5	1.5	6.5
Complexity/design/application/maturity/experience			
Does cross-connection between channels preclude the exchange of any information other than that used for diagnostic testing or voting purposes	0.5	0.5	1.5
Is the design based on techniques used in equipment that has been used successfully in the field for > 5 years?	1.0	1.0	3.0
Assessment/analysis and feedback of data			
Are all field failures fully analyzed with feedback into the design? (Documentary evidence of the procedure is required.)	0.5	3.5	4.5
Procedures/human interface			
Do the documented maintenance procedures specify that all parts of redundant systems (for example, cables, etc.) intended to be independent of each other, are not to be relocated?	0.5	0.5	1.5
Is all maintenance of printed-circuit boards, etc. carried out off-site at a qualified repair centre and have all the repaired items gone through a full pre-installation testing?	0.5	1.5	2.5
Environmental control			
Is personnel access limited (for example locked cabinets, inaccessible position)?	0.5	2.5	3.5
Is the system likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc., over which it has been tested, without the use of external environmental control?	3.0	1.0	7.0
Environmental testing			
Has the system been tested for immunity to all relevant environmental influences (for example EMC, temperature, vibration, shock, humidity) to an appropriate level as specified in recognized standards?	10.0	10.0	30.0
Yhteensä			70.5

C. LIITE: JÄRJESTELMÄTESTAUKSEN TESTITAPAUKSET

Testitapaus 1	
Kuvaus Testataan ajaa nostolaitetta yli maksiminopeuden kun AMR-anturit ilmoittavat kapselin olevan alhaalla ja todetaan molempien kanavien reagoiminen ylinopeuteen erikseen.	
Valmistelevat toimenpiteet Nostolaite ajokiskolla ja PC jolla voidaan ohjata nostolaitetta HomePlugin kautta. Ympäristön lämpötila välillä 20C - 30C. Magneetit irrotetaan ensin vuorotellen yksi kerrallaan jokaisesta AMR-anturista ja lopuksi kaikista AMR-antureista. Jokainen kohta testataan MSP:lle ja FPGA:lle erikseen: MSP:n testauksessa FPGA:n maksiminopeus asetetaan kapselin ollessa alhaalla arvoon 5m/s. Vastaavasti FPGA:n testauksessa asetetaan MSP:n maksiminopeus kapselin ollessa alhaalla arvoon 5m/s.	
Testausprosessi Nostolaitetta ajetaan kiihdyttäen jokaisessa kohdassa kunnes turvatoiminto ohjaa järjestelmän turvalliseen tilaan. Testausjärjestys(AMR-anturi jossa ei ole magneettia): AMR 1, 2, 3, 4. Lopuksi kaikista AMR-antureista irrotetaan magneetti.	
Hyväksymiskriteerit Turvatoiminto suoritetaan jokaisessa kohdassa kun nopeus on saavuttanut arvon $0.25m/s \pm 10\%$.	
Tulokset	Pass
Kommentit	
Testaajan nimi	

Testitapaus 2	
Kuvaus Testataan ajaa nostolaitetta yli maksiminopeuden kun AMR-anturit ilmoittavat kapselin olevan ylhäällä ja todetaan molempien kanavien reagoiminen ylinopeuteen erikseen.	
Valmistelevat toimenpiteet Nostolaite ajokiskolla ja PC jolla voidaan ohjata nostolaitetta HomePlugin kautta. Ympäristön lämpötila välillä 20C - 30C. Magneetit on kytketty kaikkiin AMR-antureihin. Testit suoritetaan MSP:lle ja FPGA:lle erikseen. MSP:n reagoiminen ylinopeuteen todetaan asettamalla FPGA:n maksiminopeus jokaisessa testitapauksessa kiinteästi arvoon 5m/s ja vaihtelemalla MSP:n maksiminopeutta. Vastaavasti FPGA:n reagoiminen ylinopeuteen todetaan asettamalla MSP:n maksiminopeus jokaisessa testitapauksessa kiinteästi arvoon 5m/s ja vaihtelemalla FPGA:n maksiminopeutta.	
Testausprosessi Nostolaitetta ajetaan kiihdyttäen kunnes nopeus on yli asetetun maksiminopeuden jolloin järjestelmä ohjataan turvalliseen tilaan. Testaus suoritetaan kolmella eri maksiminopeuden arvolla: alueen minimiraja 1.0m/s, alueen maksimiraja 3.0m/s sekä arvolla 1.25m/s.	
Hyväksymiskriteerit Turvatoiminto suoritetaan jokaisessa kohdassa valitulla kanavalla kun nopeus on ylittänyt arvon maksiminopeus $\pm 10\%$	
Tulokset	Pass
Kommentit	
Testaajan nimi	

Testitapaus 3	
Kuvaus Testataan viiva-antureiden nopeutta mittaavien ledien hajoaminen.	
Valmistelevat toimenpiteet Nostolaite ajokiskolla ja PC jolla voidaan ohjata nostolaitetta HomePlugin kautta. Ympäristön lämpötila välillä 20C - 30C. Magneetit on kytketty kaikkiin AMR-antureihin. Asetetaan valoa vastaanottavat ledit näyttämään jatkuvasti samaa arvoa peittämällä ne yksi kerrallaan sekä lopuksi peittämällä kaikki ledit.	
Testausprosessi Nostolaitetta ajetaan kiihdyttäen kunnes turvatoiminto havaitsee nopeuksien poikkeaman viiva-antureiden ilmoittamissa arvoissa ja ohjaa järjestelmän turvalliseen tilaan. Testausjärjestys(nopeutta mittaavat ledit jotka peitettynä): viiva-anturin 1 ledi 1, viiva-anturin 1 ledi 2, viiva-anturin 2 ledi 1, viiva-anturin 2 ledi 2. Viiva-anturin 1 kaikki ledit, viiva-anturin 2 kaikki ledit.	
Hyväksymiskriteerit Turvatoiminto suoritetaan kun nopeus on saavuttanut arvon $0.5m/s \pm 10\%$.	
Tulokset	Pass
Kommentit	
Testaajan nimi	

Testitapaus 4	
Kuvaus Testataan yhteyden katkeaminen viiva-antureihin.	
Valmistelevat toimenpiteet Nostolaite ajokiskolla ja PC jolla voidaan ohjata nostolaitetta HomePlugin kautta. Ympäristön lämpötila välillä 20C - 30C. Magneetit on kytketty kaikkiin AMR-antureihin. Kytetään vuoronperään toinen viiva-antureista irti sekä lopuksi molemmat viiva-anturit.	
Testausprosessi Nostolaitetta ajetaan alle sallitun maksiminopeuden. Testausjärjestys: Irrotetaan viiva-anturin 1 johto, irrotetaan viiva-anturin 2 johto, lopuksi molempien viiva-antureiden johdot. Kaikissa testitapauksissa irrottaminen tapahtuu nostolaitteen ollessa liikkeessä.	
Hyväksymiskriteerit Turvatoiminto ohjaa nostolaitteen turvalliseen tilaan CRC-virhetarkastuksessa kun johto on irrotettu, turvatoiminnon vasteen on oltava alle 0.1s.	
Tulokset	Pass
Kommentit	
Testaajan nimi	

Testitapaus 5	
Kuvaus Testataan yksittäisen häiriön vaikutus ajokiskon teipissä molemmilla viiva-antureilla erikseen	
Valmistelevat toimenpiteet Nostolaite ajokiskolla ja PC jolla voidaan ohjata nostolaitetta HomePlugin kautta. Ympäristön lämpötila välillä 20C - 30C. Magneetit on kytketty kaikkiin AMR-antureihin. Ajokiskon teipissä on yksittäinen kohta jossa mustan alueen leveys on 5mm, eli lyhyempi kuin kahden ledin välinen etäisyys.	
Testausprosessi Testissä nostolaite asetetaan ajokiskolle siten että ajosuuntaan nähden molemmat viiva-anturit ovat kapean teipinosan takana ja tämän jälkeen nostolaitetta ajetaan kiihdyttäen alle sallitun maksiminopeuden siten että lopussa molemmat viiva-anturit ovat ylittäneet kapean teipinosan.	
Hyväksymiskriteerit Turvatoimintoa ei suoriteta sillä virhe viiva-antureiden mittaamissa nopeuksissa ei ole tarpeeksi suuri.	
Tulokset	Pass
Kommentit	
Testaajan nimi	

Testitapaus 6	
Kuvaus Testataan kaikkien AMR-antureiden johdon irtoaminen yksi kerrallaan sekä tilanne jossa kaikkien AMR-antureiden johdot on irrotettu. Todetaan molempien kanavien reagoiminen ylinopeuteen erikseen.	
Valmistelevat toimenpiteet Nostolaite ajokiskolla ja PC jolla voidaan ohjata nostolaitetta HomePlug-in kautta. Ympäristön lämpötila välillä 20C - 30C. Magneetit on kytketty kaikkiin AMR-antureihin. Testit suoritetaan MSP:lle ja FPGA:lle erikseen. MSP:n reagoiminen ylinopeuteen todetaan asettamalla FPGA:n maksiminopeus jokaisessa testitapauksessa kiinteästi arvoon 5m/s ja vaihtelemalla MSP:n maksiminopeutta. Vastaavasti FPGA:n reagoiminen ylinopeuteen todetaan asettamalla MSP:n maksiminopeus jokaisessa testitapauksessa kiinteästi arvoon 5m/s ja vaihtelemalla FPGA:n maksiminopeutta.	
Testausprosessi Nostolaitetta ajetaan kiihdyttäen jokaisessa kohdassa. Testausjärjestys: irrotetaan AMR-anturi 1, AMR-anturi 2, AMR-anturi 3, AMR-anturi 4 siten että vain yksi anturi kerrallaan on irrotettuna. Lopuksi irrotetaan kaikkien AMR-antureiden johdot.	
Hyväksymiskriteerit Turvatoiminto suoritetaan jokaisessa kohdassa kun nopeus on saavuttanut arvon $0.25m/s \pm 10\%$.	
Tulokset	Pass
Kommentit	
Testaajan nimi	

Testitapaus 7	
Kuvaus Testataan tilanne jossa yhteys ohjauslogiikoiden välillä katoaa	
Valmistelevat toimenpiteet Nostolaite ajokiskolla ja PC jolla voidaan ohjata nostolaitetta HomePlugin kautta. Ympäristön lämpötila välillä 20C - 30C. Tehdään MSP:n ja FPGA:n välisen SPI:n MOSI-signaalin välille jumpperi joka voidaan irrottaa lennosta.	
Testausprosessi Ajetaan nostolaitetta kiihdyttäen alle sallitun maksiminopeuden ja irrotetaan jumpperi kun nostolaite on ajoliikkeessä.	
Hyväksymiskriteerit CRC-tarkastukset aiheuttavat turvatoiminnon suorituksen, turvalliseen tilaan siirtymisen vasteen on oltava alle 1s.	
Tulokset	Pass
Kommentit	
Testaajan nimi	
Testitapaus 8	
Kuvaus Testataan safe-kytkennän MSP-sisääntulon (signaali SAFE_LO) jääminen ylösvedetyksi.	
Valmistelevat toimenpiteet Nostolaite pöydällä. Ympäristön lämpötila välillä 20C - 30C. Kytetään safe:n MSP-sisääntulo +3.3V:iin.	
Testausprosessi Kytetään jännitteet nostolaitteeseen.	
Hyväksymiskriteerit Turvatoiminto suoritetaan ja ohjataan järjestelmä turvalliseen tilaan. Todetaan mittamalla että sulakkeet safe-kytkennöissä hajoavat.	
Tulokset	Pass
Kommentit	
Testaajan nimi	

Testitapaus 9	
Kuvaus Testataan safe-kytkennän FPGA-sisääntulon (signaali SAFE_HI) jääminen ylösvedetyksi.	
Valmistelevat toimenpiteet Nostolaite pöydällä. Ympäristön lämpötila välillä 20C - 30C. Kytetään safe:n FPGA-sisääntulo +3.3V:iin.	
Testausprosessi Kytetään jännitteet nostolaitteeseen.	
Hyväksymiskriteerit Turvatoiminto suoritetaan ja ohjataan järjestelmä turvalliseen tilaan. Tode- taan mittaamalla että sulakkeet safe-kytkennöissä hajoavat.	
Tulokset	Pass
Kommentit	
Testaajan nimi	