SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

PAALUTUSKONEEN OHJAUS-JÄRJESTELMÄN TURVAKRIITTISTEN TOIMINTOJEN SUUNNITTELU JA OHJELMOINTI

TEKIJÄ: Jani Järvenpää

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Sähkötekniikan tutkinto-ohjelma	
Työn tekijä(t) Jani Järvenpää	
Työn nimi Paalutuskoneen ohjausjärjestelmän turvakriittisten toimintojen suunnittelu ja ohjelmointi	
Päiväys 7.12.2019	Sivumäärä/Liitteet 30 sivua
Ohjaaja(t) Yliopettaja Arto Toppinen	
Toimeksiantaja/Yhteistyökumppani(t) Junttan Oy, Sami Martikainen	

Tiivistelmä

Tämän opinnäytetyön oli tarkoitus tuottaa ohje paalutuskoneen turvakriittisten toimintojen suunnitteluun.

Työssä tutustutaan paalutuskoneen toimintaan ja käyttöön, käydään läpi EN 16228 standardin vaatimukset, kuinka turvakriittiset toiminnot tunnistetaan, suunnitellaan ja toteutetaan vaatimusten mukaisesti.

Turvatoiminnoille luokitellaan suoritustasot (PL) vikaantumisesta aiheutuvan vaaran perusteella ja standardista saadaan vaarallisen vikaantumisen todennäköisyyden (PFHd) rajat. Turvatoiminto suunnitellaan sähköisesti ja ohjelmallisesti näiden vaatimusten perusteella. Toteutettu turvatoiminto testataan ja kelpuutetaan.

Avainsanat
EN 16228-1, Koneturvallisuus, Paalutuskone

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Electrical Engineering			
Author(s) Jani Järvenpää			
Title of Thesis Designing and programming safety-critical control system functions for piling rigs			
Date	7.12.2019	Pages/Appendices	30 pages
Supervisor(s) Arto Toppinen, Principal Lecturer			
Client Organisation /Partners Junttan Oy, Sami Martikainen			

Abstract

The purpose of the thesis was to produce a desing guideline for safety-critical controlsystem functions of piling rig.

This thesis gives introduction to piling rigs and how they are used. Requirements of standard EN 16228 that are relevant to control system desing were stated. Safety function was identified, designed and implemented to meet the requirements.

Required performance level (PL) of the safety function is selected by concidering the level of danger caused by a fault, and limits for the propability of dangerous failure (PFHd) per hour are set by the standard. Software and the electrical hardware of the safety function was designed, tested and validated.

Keywords
EN 16228, Safety of machinery, Piling rig

SISÄLTÖ

1 JOHDANTO

Opinnäytetyö tehtiin Junttan Oy:lle. Junttan on Kuopiolainen paalutuskoneita suunnitteleva ja valmistava yritys. Junttanilla on yli 40 vuoden kokemus perustusrakentamiseen käytettävien koneiden valmistuksesta ja on alan johtava lyöntipaalutuskoneiden valmistaja. Koneilla tehtävään työhön liittyy vaaroja, kun käsitellään tuhansia kiloja painavia, kymmeniä metrejä pitkiä paaluja.

2 TEORIA

KUVA 1. MPx90 – Multipurpose paalutuskone. (Junttan Oy, 2019)

Paalutuskoneen rakenne voidaan jakaa neljään pääosaan:

- Alavaunu, johon kuuluu telasto ja kääntökehä
- Ylävaunu, johon kuuluu ohjaamo, hydrauliikkatila, vinssit, pystyynnostopukki ja paljon muuta
- Masto eli keili, johon kuuluu johteet, köysipyörät ja yläpäässä oleva kukko (keltainen)
- Työkalu, kuvan tapauksessa vasara eli järkäle, joka kiinnittyy keilin johteisiin ja sitä kannattelee ylävaunulla sijaitseva vinssi.

Koneen voimanlähteenä toimii diesel-moottori, joka tuottaa tehoa hydrauliikkapumpulle. Koneen kaikki liikkeet toimivat hydrauliikalla.

2.1 Koneella tehtävä työ

Paalutuskonetta käytetään rakennusten perustamisen vahvistamiseen. Suomessa yleisin tapa paaluttaa on etukäteen valmistettujen teräsbetonipaalujen asentaminen lyömällä. Paalujen pituudet vaihtelevat yleensä 8-30 metrin välillä, ja yleisimmät mitat ovat 250x250mm ja 300x300mm.
Kone toimitetaan työmaalle lavetilla kuljetuskunnossa.

KUVA 2. MPX90-lavetilla (Junttan Oy, 2019)

Kun kone on otettu alas lavetilta, alkaa koneen pystyynnosto. Keili nostetaan pystyyn ylävaunulla sijaitsevalla pystyynnostopukilla. Keilin ollessa pystyssä siihen kiinnitetään työkalu, ja työ voidaan aloittaa. Lyöntipaalutuksessa apumies kiinnittää paaluvinssin paaluun. Paalu nostetaan pystyyn ja paalun yläpää ohjataan järkäleen alapäässä sijaitsevaan paalupesään. Paalu asemoidaan paalutussuunnitelman mukaiseen paikkaan, ja se lyödään kantavaan maakerrokseen. Lyönti tapahtuu järkäleen sisällä olevalla teräsblokilla,

joka nostetaan ylös ja kiihdytetään alas junttaussylinterillä. Lyöntienergia mitataan blokin loppunopeudesta ja lyöntienergian suuruus riippuu nostokorkeudesta, kiihtyvyydestä ja blokin massasta

2.2 Koneen ohjausjärjestelmä

Nykyaikaiset paalutuskoneet ovat sähköisesti esiohjattuja. Tämä tarkoittaa sitä, että koneen hydraulijärjestelmässä on solenoidiohjatut venttiilit, joita koneen ohjausjärjestelmä ohjaa. Junttanin PMx, PMz ja MPx-sarjan koneiden ohjausjärjestelmät ovat hajautettuja CANopen-protokollaan perustuvia järjestelmiä, joka koostuu noin kymmenestä ohjainlaitteesta ja kolmesta eri CAN-väylästä. Koneen ohjausjärjestelmä on monimutkainen. Ohjelmallisesti ohjattuja venttiilejä koneessa on yli sata, ja ohjausjärjestelmään tulee yli 200 anturi- tai kytkintietoa.

2.3 Koneen turvallisuuteen vaikuttavat ohjausjärjestelmän osat ja turvatoiminnot

Edellä mainitun lisäksi koneessa on yli 20 niin sanotusti kovalla sähköllä (ei ohjelmallisesti) ohjattua venttiiliä. Tätä piiriä käytetään estämään vaaralliset ja konetta vahingoittavat liikkeet, esimerkiksi pystyynnoston aikaiset sylinterien liikkeet. Näistä osa on koneen turvatoimintoja, kuten turvakahvan ohjaamat venttiilit.
Tämä on toteutettu nykyisin releteknikalla. Useat induktiiviset anturit, rajakytkimet, ja kytkimet ohjaavat releitä jotka ohjaavat halutut venttiilit auki tai kiinni. Kone on rakennettu niin että se vikaantuu turvallisesti. Liikkeet ovat estetty venttiilien solenoidien ollessa virrattomina.

2.4 Lyhenteet ja määritelmät

CAN = Controller Area Network, ajoneuvoissa ja liikkuvassa kalustossa käytetty sarjaväylä
MPx = Junttanin X-sarjan multipurpose kone, joka soveltuu kaikkiin työmenetelmiin.
PMx = Junttanin X-sarjan lyöntipaalutuskone
PMz = Junttanin uuden sukupolven lyöntipaalutuskone
SFS = Suomen Standardisoimisliitto
EN = European Norms
ISO = International organization of standardization
PL = Performance level, Suoritustaso
SIL = Safety integrity level, Turvallisuuden eheys taso
EMC = Electromagnetic compliance, sähkömagneettinen yhteensopivuus
DC = Diagnostic coverage, Diagnostiikan kattavuus
MTTFd= Mean time to dangerous failure, Keskimääräinen vaarallisen vikaantumisen aika
PFHd = Propability of dangerous failure per hour, vaarallisen vikaantumisen todennäköisyys tunnissa
CCF = Common cause failure, yhteisvikaantuminen

3 STANDARDIN VAATIMUKSET

Perustus- ja porauskaluston turvallismääräykset tulevat SFS-EN 16228 standardista. Standardin ohjausjärjestelmään ja sähkölaitteistoon liittyvät vaatimukset ovat muun muassa:

- Koneen sähköjärjestelmä on toteutettava EN 60204-1:2006 kohtia 4, 5, 6, 13, 14 ja 15 noudattaen.
    - EN60204-1:2006 (Koneturvallisuus, koneiden sähkölaitteisto) Määrää esimerkiksi: johtimien kuormitettavuudet, lämpötila-alueet, maadoitukset, hätäpysäytykset.

- Ohjausjärjestelmä on totetettava EN 60204-1:2006 kohtia 9, 10 ja 11 noudattaen.

- Koneessa pitää olla hätäseis-kytkin.
    - Toiminnot eivät saa käynnistyä uudelleen hätäseis-kytkimen palautuessa.

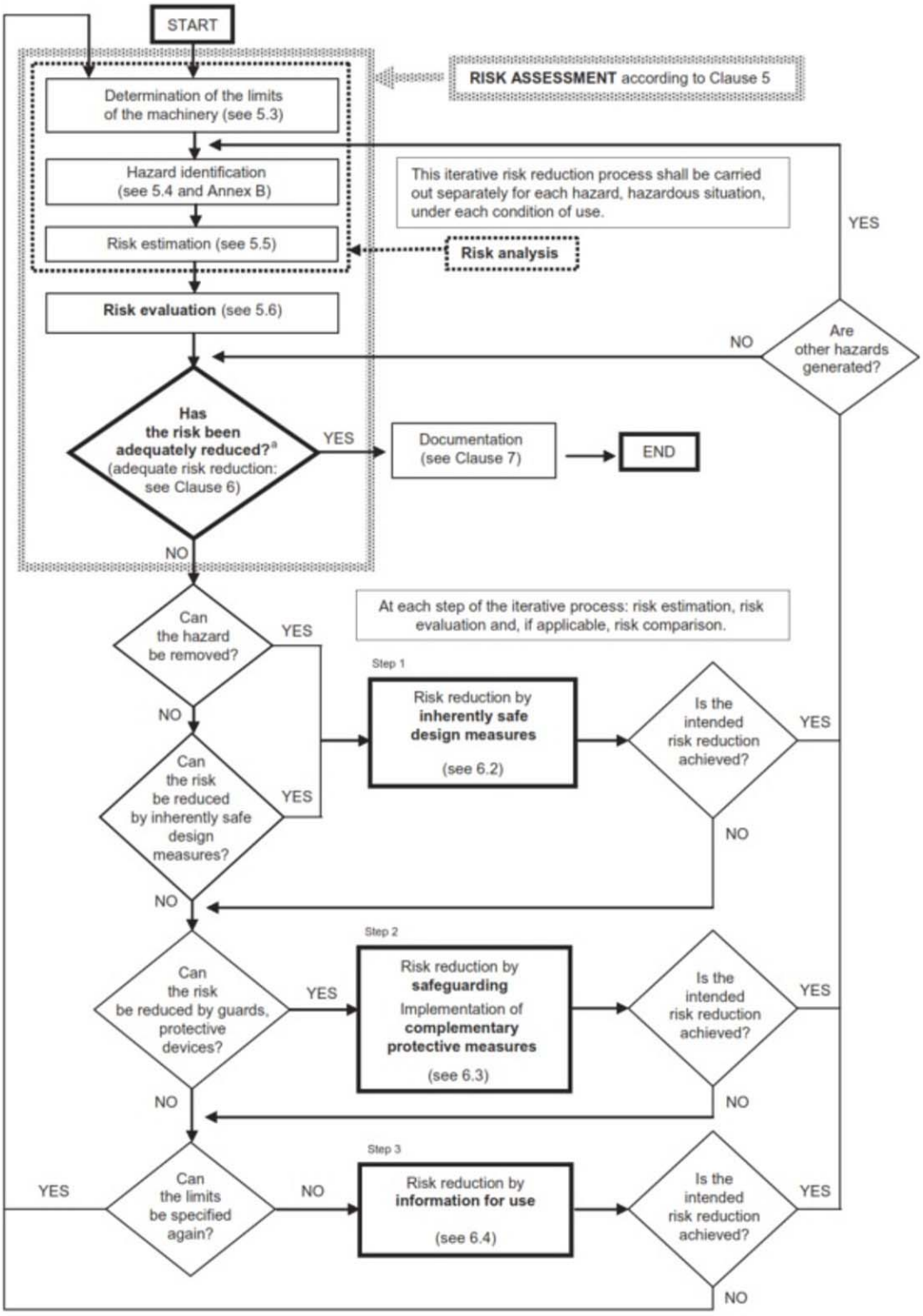
- Koneen toiminnasta on tehtävä riskinarviointi ja riskien vähentäminen ISO 12100:2010 mukaan.
    - Riskinarvioinnin ja riskien vähentämisen kautta saadaan turvatoiminnot.

- Turvatoimintojen on täytettävä EN ISO 13849-1:2008 mukaiset vaatimukset.
    - Turvatoiminnot on oltava dokumentoituja, suoritustasojen ja vaatimusten mukaisia.

- Ohjausjärjestelmän on täytettävä EN 16228-1 taulukon 3 mukaiset vaatimukset.

- Koneen sähköjärjestelmä on EMC testattava hyväksytysti EN 13309:2010 mukaan.
    - EN60204-1:2006 kohdassa 4.4.2 myös EMC vaatimuksia.

3.1 Riskinarviointi



KUVA 3. Kaaviollinen esitys riskin pienentämisprosessin iteratiivisesta kolmen askeleen menetelmästä
(International Organization for Standardization, 2010)

Koneen riskinarviointi ja riskin vähentäminen tulee tehdä standardin ISO 12100:2010 mukaisesti. Kun riskinarviointi tehdään standardin mukaisesti, saadaan tarvittavat asiakirjat joiden mukaan turvatoiminnot suunnitellaan. Turvatoiminnot ja suojaukset saadaan riskien vähentämisen seurauksena, mikäli turvallisilla suunnittelukäytännöillä saavutetun riskin vähentämisen jälkeen jäännösriski on yhä merkittävä.

3.2 Suoritustasot

Table 3 — Required performance level

No. of safety function	Safety function requirements	Required Performance Level PL_r
	Travelling	
1	Ability to stop	**c**
	Tramming	
2	Ability to stop	**c**
	Slewing	
3	Ability to stop	**c**
	Lifting in the process	
4	Ability to stop	**c**
5	Keeping the load stationary	**c**
6	Limiters/over-hoist	**b**
	Winching (Pulling/anchoring)	
7	Ability to stop	**c**
8	Limiters/over-hoist	**b**
	Working platforms for lifting personnel	
9	Ability to stop	**c**
10	Limiters/over-hoist	**c**
	Machine stability jacks and ground anchor systems	
11	Ability to stop	**c**
12	Ability to hold	**c**
	Activation of Safeguards	
13	Stopping rotation/feed on activation of interlocked guards or protective devices	**c**
	Restricted Operating Mode	
14	Engagement and maintenance of slow rotation and feed speed	**c**
	Drill rotation/feed during special protective mode for specific circumstances	
15	Stopping rotation/feed on activation of pressure sensitive devices	**c**
	Clamping and breaking of tools	
16	Ability to hold	**b**
	Rod handling devices	
17	Ability to stop the device	**c**
	Mast/boom/leader positioning system	
18	Ability to stop the mast/boom/leader	**c**
19	Ability to hold the mast/boom/leader in position	**c**

KUVA 4. Vaaditut suoritustasot (European Commitee for Standardization, 2014)

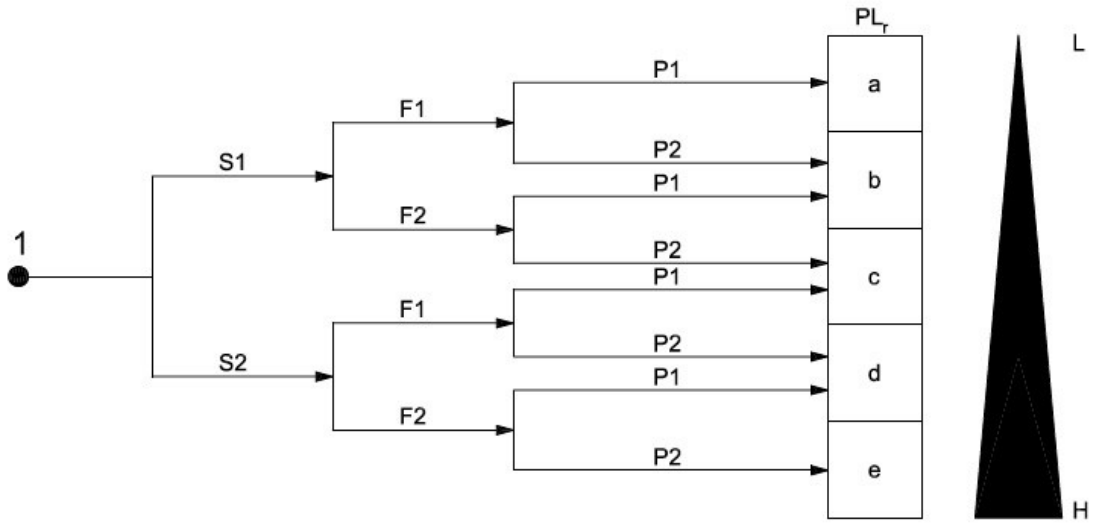
EN 13849-1 Standardista tulee suoritustasot, josta määräytyy laitteiston vaarallisen vikaantumisen todennäköisyys rajat. Standardissa otetaan huomioon myös hydrauliset ja pneumaattiset ohjausjärjestelmän osat.

Turvaluokitelluissa sähkökomponenteissa käytetään usein EN 61508 mukaisia turvallisuuden eheystasoja (SIL, Safety Integrity Level). PL ja SIL eivät ole suoraan yhteneviä, mutta niillä on vastaavat vaarallisen vikaantumisen todennäköisyysrajat. EN 61508 standardi huomioi vain ohjelmalliset ja sähköiset turvallisuuteen liittyvät järjestelmän osat.

Taulukko 1. SIL ja PL luokitusten yhteneväisyydet

Performance level (PL)	Safety integrity level (SIL)	Average probability of a dangerous failure on demand per hour (1/h)
a	Ei vastinetta	$>10^{-5}$ to 10^{-4}
b	1	$>3x10^{-6}$ to 10^{-5}
c	1	$>10^{-6}$ to $3x10^{-6}$
d	2	$>10^{-7}$ to 10^{-6}
e	3	$>10^{-8}$ to 10^{-7}

3.2.1 Suoritustason määrittäminen



Key

1	starting point for evaluation of safety function's contribution to risk reduction
L	low contribution to risk reduction
H	high contribution to risk reduction
PL_r	required performance level

Risk parameters:

S	severity of injury
S1	slight (normally reversible injury)
S2	serious (normally irreversible injury or death)
F	frequency and/or exposure to hazard
F1	seldom-to-less-often and/or exposure time is short
F2	frequent-to-continuous and/or exposure time is long
P	possibility of avoiding hazard or limiting harm
P1	possible under specific conditions
P2	scarcely possible

Figure A.1 — Graph for determining required PL_r for safety function

KUVA 5. Vaadittavan suoritustason valinta graafi

(International Organization for Standardization, 2006)

Vaadittava suoritustaso saadaan käyttämällä kuvan 5 graafia riskinarvioinnin pohjalta saatavilla tiedoilla.

Suoritustasoon vaikuttaa seuraavat tekijät:

- Arkkitehtuuri luokka (Architecture Category)
- Yhteisvikaantuminen (CCF = Common Cause Failure)
- Diagnostiikan kattavuus (DC = Diagnostic Coverage)
- Keskimääräinen vaarallinen vikaantumisaika (MTTFd= Mean time to dangerous failure)

3.2.1.1 Arkkitehtuuri

Turvatoimintojen arkkitehtuurit voidaan jakaa viiteen luokkaan: B, 1, 2, 3 ja 4.

Luokka B

Key

i_m interconnecting means
I input device, e.g. sensor
L logic
O output device, e.g. main contactor

Figure 8 — Designated architecture for category B

KUVA 6. Luokan B lohkokuvaus (International Organization for Standardization, 2006)

Luokan B arkkitehtuurilla on mahdollista toteuttaa korkeintaan PL b-suoritustason järjestelmä. Tässä luokassa:

- Diagnostiikan kattavuus on nolla
- Keskimääräinen vaarallinen vikaantumisaika on pienempi kuin 30 vuotta
- Yhteisvikaantumisella ei ole merkitystä

Luokka 1

Key

i_m interconnecting means
I input device, e.g. sensor
L logic
O output device, e.g. main contactor

Figure 9 — Designated architecture for category 1

KUVA 7. Luokan 1 lohkokuvaus (International Organization for Standardization, 2006)

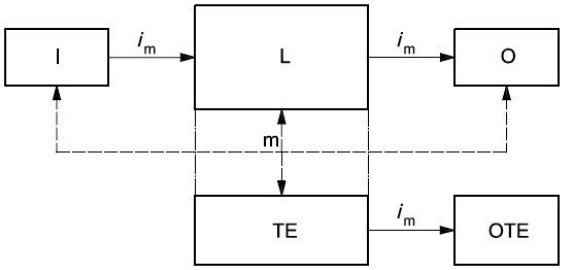
Luokan yksi arkkitehtuurilla suurin saavutettava suoritustaso on PL c. Tässä luokassa:

-Diagnostiikan kattavuus on nolla

-Keskimääräinen vaarallinen vikaantumisaika on yhtä kuin tai suurempi kuin 30 vuotta

-Yhteisvikaantumisella ei ole merkitystä

Luokka 2



Dashed lines represent reasonably practicable fault detection.

Key

i_m interconnecting means
I input device, e.g. sensor
L logic
m monitoring
O output device, e.g. main contactor
TE test equipment
OTE output of TE

Figure 10 — Designated architecture for category 2

KUVA 8. Luokan 2 lohkokuvaus (International Organization for Standardization, 2006)

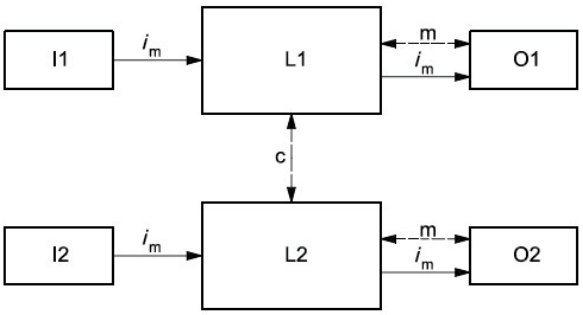
Luokan kaksi järjestelmällä suurin saavutettavissa oleva suoritustaso on PL d. Tässä luokassa:

- Keskimääräinen diagnostiikan kattavuus (DCavg) on vähintään matala
- Keskimääräinen vaarallinen vikaantumisaika on 3-100 vuotta
- Yhteisvikaantumisen välttämiseksi tehtävien toimenpiteiden pisteiden oltava 65 tai suurempi

Diagnostiikan kattavuutta ja vikaantumisaikoja laskiessa huomioidaan vain I, L, ja O lohkot, mutta ei tarkistuskanavan lohkoja.

Tämä arkkitehtuuri voidaan toteuttaa esimerkiksi Lockstep-järjestelmällä, joka vikatilanteessa ohjaa lähtöjen syöttöjännitteen pois päältä.

Luokka 3



Dashed lines represent reasonably practicable fault detection.

Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O2	output device, e.g. main contactor

Figure 11 — Designated architecture for category 3

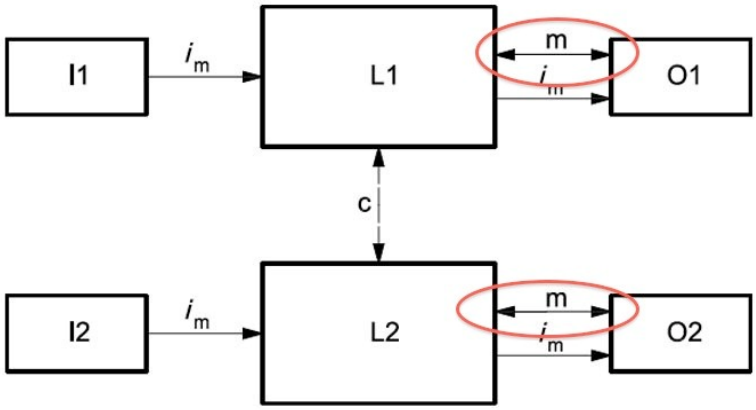
KUVA 9. Luokan 3 lohkokuvaus (International Organization for Standardization, 2006)

Luokan kolme järjestelmällä suurin saavutettavissa oleva suoritustaso on PL e. Tässä järjestelmässä:

- Keskimääräinen diagnostiikan kattavuus (DCavg) on matala tai keskisuuri
- Keskimääräinen vaarallinen vikaantumisaika on 3-100 vuotta
- Yhteisvikaantumisen välttämiseksi tehtävien toimenpiteiden pisteiden oltava 65 tai suurempi

Luokan kolme järjestelmässä yksittäinen vika ei koskaan johda turvatoiminnon menettämiseen, mutta koska diagnostiikan kattavuus ei ole korkea, kaikki viat eivät paljastu. Kertyneet viat voivat johtaa turvatoiminnon menettämiseen.

Luokka 4



Solid lines for monitoring represent diagnostic coverage that is higher than in the designated architecture for category 3.

Key

i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. sensor
L1, L2	logic
m	monitoring
O1, O2	output device, e.g. main contactor

Figure 12 — Designated architecture for category 4

KUVA 10. Luokan 4 lohkokuvaus (International Organization for Standardization, 2006)

Luokan neljä järjestelmällä suurin saavutettavissa oleva suoritustaso on PL e. Tässä järjestelmässä:

- Keskimääräinen diagnostiikan kattavuus (DCavg) on korkea
- Keskimääräinen vaarallinen vikaantumisaika on 30-100 vuotta
- Yhteisvikaantumisen välttämiseksi tehtävien toimenpiteiden pisteiden oltava 65 tai suurempi

Luokan neljä järjestelmässä yksittäinen vika ei koskaan johda turvatoiminnon menettämiseen ja vika paljastuu. Mikäli tämä ei ole mahdollista, paljastumattomien vikojen kertyminen ei saa johtaa turvatoiminnon menettämiseen. Kunkin kanavan keskimääräisen kanavan vikaantumisajan on oltava korkea.

3.2.1.2 Keskimääräinen vaarallinen vikaantumisaika

$MTTF_d$

Standardin kohdassa C.5.1 mainitaan että komponentin MTTFd on kaksi kertaa MTTF.

$$MTTF_d = MTTF * 2$$

Komponenttivalmistajat antavat yleensä komponenttien vikaantumisajat suoraan datalehdissään. Sähkömekaanisten komponenttien kuten rajakytkinten tai releiden kesto ilmoitetaan kuitenkin kytkentäkertoina. Standardin liitteenä olevista taulukoista löytyy tyypilliset vikaantumisajat elektroniikalle ja sähkömekaanisille komponenteille.

$MTTF_d$ voidaan laskea komponentin B_{10d}-arvosta seuraavalla kaavalla:

$$MTTF_d = \frac{B_{10d}}{0{,}1 * n_{op}}, jossa\ n_{op} = \frac{d_{op} * h_{op} * 3600s/h}{t_{cycle}}$$

$MTTF_d$ = Keskimääräinen vaarallinen vikaantumisaika

B_{10d} = Keskimääräinen kytkentämäärä jossa 10% komponenteista vikaantuu vaarallisesti

n_{OP} = Keskimääräinen vuosittainen toimintojaksojen lukumäärä

h_{OP} = Keskimääräinen toiminta-aika, tuntia päivässä

d_{OP} = Keskimääräinen toiminta-aika, päivää vuodessa

t_{cycle} =kahden peräkkäisen toimintajakson alkamiskohdan aikaväli, sekuntia per toimintajakso

jos B_{10d}-arvoa ei ole saatavilla, 50% B10:stä voidaan käyttää.

B_{10} = Keskimääräinen kytkentämäärä kun 10% komponenteista vikaantuu

Kanavan $MTTF_d$

Kanavan $MTTF_d$ lasketaan seuraavalla yhtälöllä:

$$MTTF_d = 1/\sum(n_j/MTTF_{dj})$$

Jossa

$MTTF_d$= Koko kanavan keskimääräinen vaarallinen vikaantumisaika

n_j= Lukumäärä

$MTTF_{dj}$=Yksittäisen komponentin vikaantumisaika

Esimerkki: Koneen hätäseispiiri

- Koneessa on neljä hätäseis nappia, jossa BACO 33S01 2xNC kontaktit joiden B_{10}= $1*10^6$
- Turvarele Duelco NST-3 $MTTF_d$ = 125,8 vuotta kun d_{op}= 365 d, h_{op}= 24 h ja n_{op}= 12, Cat 3
- On/Off venttiili Bosch rexroth, $MTTF_d$ = 150 vuotta, mainittu standardin kohdassa C.3

Hätäseis nappi:

B_{10d}-arvoa ei löytynyt datalehdestä, joten käytetään arvoa 0,5* B_{10}

Käytetään samaa vuosittaista toimintojaksojen lukumäärää kun turvareleessä, n_{op}= 12.

Huom! Jos tiedetään että hätäseisnappia käytetään useammin, valitaan korkeampi arvo.

$MTTF_d = \frac{0{,}5*10^6}{0{,}1*12}$ = 416 666,67 vuotta

Kanavan $MTTF_d$:

j	komponentti	lukumäärä	MTTFdj	1/MTTFdj	nj/MTTFdj	
1	Hätäseis nappi	4	416666,67	2,4E-06	9,6E-06	
2	Turvarele	1	125,8	7,95E-03	7,95E-03	+
3	venttiili	1	150	6,67E-03	6,67E-03	+
				SUM=	1,46E-02	
				MTTFd=1/SUM=	68,37	vuotta

Toiminta-aika

Komponenttien toiminta-aika rajoittuu T10d arvoon. Ennen tätä komponentit on uusittava.

$$T_{10d} = \frac{B_{10d}}{n_{op}}$$

T_{10d}= Keskimääräinen toiminta-aika kun 10% komponenteista vikaantuu vaarallisesti

Tämä on tasan 10% $MTTF_d$-arvosta, ja siten 20% MTTF-arvosta, mutta korkeintaan 20 vuotta.

3.2.1.3 Diagnostiikan kattavuus

DC

Diagnostiikan kattavuuden karkean arvion saa standardin ISO 13849-1 liitteen E taulukoista. Kyseisissä taulukoissa on konkreettisia esimerkkejä, kuten:

Toimenpide	**Diagnostiikan kattavuus (DC)**
Tuloyksikkö	
Suora valvonta (esim. ohjausventtiilin asennon sähköinen valvonta, sähkömekaanisen laitteen valvonta mekaanisesti yhdistetyillä kosketinelementeillä)	99%
Anturien ominaisuuksien valvonta (vasteaika, analogisten signaalien vaihteualue)	60%

Useimmissa tapauksissa diagnostiikan kattavuus täytyy kuitenkin laskea yhtälöllä:

$$DC\% = \frac{\lambda \mathrm{dd}}{\lambda \mathrm{d}} * 100 \text{ , jossa } \lambda \mathrm{d} = \lambda \mathrm{dd} + \lambda \mathrm{ud}$$

jossa,

DC%= Diagnostic coverage, diagnostiikan kattavuus

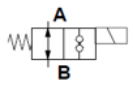
λd= vaarallinen vikaantuminen

λdd= tunnistettava vaarallinen vikaantuminen

λud= ei tunnistettavissa oleva vaarallinen vikaantuminen

Vikaantumistilanteet saadaan vika- ja vaikutusanalyysillä (FMEA= Failure mode and effects analysis). Kuvassa 11 on esitetty esimerkki on/off solenoidiventtilin vika- ja vaikutusanalyysistä.

	A	B	C	D	E
1	Estoventtiili				
2	**Vika**	**Vaikutus**	**Vaarallisuusaste**	**Tunnistettavuus**	**Todennäköisyys**
3	Venttiili jumittuu kiinni	Venttiili ei avaudu ja liikkeitä ei saada estettyä	IV	6	A
4	Venttiili jumittuu auki	Venttiili ei sulkeudu ja liikkeet ovat estetty	I	1	A
5	Solenoidi palaa	Venttiili ei sulkeudu ja liikkeet ovat estetty	I	1	E
6	Venttiili menee tukkoon	Esiohjauspaineet eivät pääse tankkiin, liikkeitä ei saada estettyä	IV	5	B
7	Tankkiletku vahingoittuu	öljyt vuotavat maahan liikkeen ollessa estetty	III	2	C
8	Esiohjauspaineletku vahingoittuu	Liikkeet estyvät	III	1	C
9					
10		**Vaarallisia tunnistettavia vikaantumisia**	0		
11		**Vaarallisia vikaantumisia**	2		
12					
13		**DC**	0 %		
14					
15					
16	**Severity (S)**				
17	**Rating**	**Meaning**			
18	I	No relevant effect on reliability or safety			
19	II	Very minor, no damage, no injuries, only results in a maintenance action (only noticed by discriminating customers)			
20	III	Minor, low damage, light injuries (affects very little of the system, noticed by average customer)			
21	IV	Critical (causes a loss of primary function; Loss of all safety margins, 1 failure away from a catastrophe, severe damage, severe injuries, max 1 possible death)			
22	V	Catastrophic (product becomes inoperative; the failure may result in complete unsafe operation and possible multiple deaths)			
23	**Detection (D)**				
24	**Rating**	**Meaning**			
25	1	Certain - fault will be caught on test			
26	2	Almost certain			
27	3	High			
28	4	Moderate			
29	5	Low			
30	6	Fault is undetected by Operators or Maintainers			
31	**Probability (P)**				
32	**Rating**	**Meaning**			
33	A	Extremely Unlikely (Virtually impossible or No known occurrences on similar products or processes, with many running hours)			
34	B	Remote (relatively few failures)			
35	C	Occasional (occasional failures)			
36	D	Reasonably Possible (repeated failures)			
37	E	Frequent (failure is almost inevitable)			



KUVA.11 Estoventtiilin FMEA

Diagnostiikan kattavuus tulee laskea kaikille turvatoimintoon liittyville komponenteille.

DC_{avg}

Koko toiminnon Keskimääräinen diagnostiikan kattavuus (DC_{avg}) lasketaan käyttäen yksittäisten komponenttien diagnostiikan kattavuutta. Diagnostiikan kattavuus luokitellaan neljään tasoon:

Table 5 — Diagnostic coverage (DC)

DC	
Denotation	**Range**
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC

NOTE 1 For SRP/CS consisting of several parts an average value DC_{avg} for DC is used in Figure 5, Clause 6 and E.2.

NOTE 2 The choice of the DC ranges is based on the key values 60 %, 90 % and 99 % also established in other standards (e.g. IEC 61508) dealing with diagnostic coverage of tests. Investigations show that (1 - DC) rather than DC itself is a characteristic measure for the effectiveness of the test. (1 - DC) for the key values 60 %, 90 % and 99 % forms a kind of logarithmic scale fitting to the logarithmic PL-scale. A DC-value less than 60 % has only slight effect on the reliability of the tested system and is therefore called "none". A DC-value greater than 99 % for complex systems is very hard to achieve. To be practicable, the number of ranges was restricted to four. The indicated borders of this table are assumed within an accuracy of 5 %.

KUVA 12. DC-tasot (International Organization for Standardization, 2006)

Keskimääräinen diagnostiikan kattavuus saadaan laskettua seuraavalla kaavalla:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}}$$

KUVA 13. DC_{avg}-arvon arvioinnin yhtälö (International Organization for Standardization, 2006)

Esimerkki: Koneen hätäseispiiri

-Venttiilin vika- ja vaikutusanalyysistä saatiin venttilille DC-arvo 0%

-Releen DC-arvoksi ilmoitetaan datalehdessä 66,98%

-Hätäseis napin DC arvo on 0%, sillä mitään vikoja ei tunnisteta

Komponentti	DC%	MTTFd (vuotta)
Hätäseis nappi	0	416666,7
Rele	66,98	125,8
Venttiili	0	150

Näiden arvojen perusteella laskettu diagnostiikan kattavuus:

$$DC_{avg} = \frac{\frac{0}{416666,7} + \frac{0}{416666,7} + \frac{0}{416666,7} + \frac{0}{416666,7} + \frac{0,6698}{125,8} + \frac{0}{150}}{\frac{1}{416666,7} + \frac{1}{416666,7} + \frac{1}{416666,7} + \frac{1}{416666,7} + \frac{1}{125,8} + \frac{1}{150}} = 36\%$$

3.2.1.4 Yhteisvikaantuminen

Jos yhden vian seurauksena muitakin komponentteja vikaantuu, tätä ensin mainittua vikaa yhdessä kaikkien siitä seuraavien vikojen kanssa on pidettävä yksittäisenä vikana. Kahta tai useampaa erillistä vikaa, jolla on yhteinen syy, on pidettävä yksittäisenä vikana. Kahden tai useamman eri syistä johtuvan vian esiintymistä pidetään erittäin epätodennäköisenä eikä sitä tarvitse ottaa huomioon. (International Organization for Standardization, 2006)

Arkkitehtuuriltaan luokkien 2, 3 ja 4 järjestelmien suunnittelussa on otettava huomioon yhteisvikaantuminen. Yhteisvikaantumisen estämiseksi on tehtävä erilaisia toimenpiteitä joista saadaan pisteytys. Saatujen pisteiden yhteenlaskettu määrä on oltava 65 tai suurempi.

No.	Measure against CCF	Score
1	**Separation/ Segregation**	
	Physical separation between signal paths, for example: — separation in wiring/piping; — detection of short circuits and open circuits in cables by dynamic test; — separate shielding for the signal path of each channel; — sufficient clearances and creepage distances on printed-circuit boards.	15
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: — first channel electronic or programmable electronic and second channel electromechanical hardwired, — different initiation of safety function for each channel (e.g. position, pressure, temperature), and/or digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or Components of different manufactures.	20
3	**Design/application/experience**	
3.1	Protection against over-voltage, over-pressure, over-current, over-temperature, etc.	15
3.2	Components used are well-tried.	5
4	**Assessment/analysis**	
	For each part of safety related parts of control system a failure mode and effect analysis has been carried out and its results taken into account to avoid common-cause-failures in the design.	5
5	**Competence/training**	
	Training of designers to understand the causes and consequences of common cause failures.	5
6	**Environmental**	
6.1	For electrical/electronic systems, prevention of contamination and electromagnetic disturbances (EMC) to protect against common cause failures in accordance with appropriate standards (e.g. IEC 61326–3-1). Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. NOTE For combined fluidic and electric systems, both aspects should be considered.	25
6.2	Other influences Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).	10
	Total	**[max. achievable 100]**

Total score	Measures for avoiding CCF[a]
65 or better	Meets the requirements
Less than 65	Process failed ⇒ choose additional measures

Kuva 14. Yhteisvikaantuminen (International Organization for Standardization, 2006)

3.2.1.5 Vaarallisen vikaantumisen todennäköisyys sekä suoritustaso

MTTFd	Cat B(MTTFd below 30 years)	PL	Cat 1 (MTTFd over 30 years)	PL	Cat 2 Dcawg= low	PL	Cat2 Dcavg= med		Cat 3 DCawg= low	PL	CAT 3 DCawg= med	PL	Cat 4 high DCawg (99%) and MTTFd over 30 years for all channels	PL
3	3,80E-05	a			2,58E-05	a	1,99E-05	a	1,26E-05	a	6,09E-06	b		
3,3	3,46E-05	a			2,33E-05	a	1,79E-05	a	1,13E-05	a	5,41E-06	b		
3,6	3,17E-05	a			2,13E-05	a	1,62E-05	a	9,37E-06	a	4,86E-06	b		
3,9	2,93E-05	a			1,95E-05	a	1,48E-05	a	9,37E-06	b	4,40E-06	b		
4,3	2,65E-05	a			1,76E-05	a	1,33E-05	a	8,39E-06	b	3,89E-06	b		
4,7	2,43E-05	a			1,60E-05	a	1,20E-05	a	7,58E-06	b	3,48E-06	b		
5,1	2,24E-05	a			1,47E-05	a	1,10E-05	a	6,91E-06	b	3,15E-06	b		
5,6	2,04E-05	a			1,33E-05	a	9,87E-06	b	6,21E-06	b	2,80E-06	c		
6,2	1,84E-05	a			1,19E-05	a	8,80E-06	b	5,53E-06	b	2,47E-06	c		
6,8	1,68E-05	a			1,08E-05	a	7,93E-06	b	4,98E-06	b	2,20E-06	c		
7,5	1,52E-05	a			9,75E-06	b	7,10E-06	b	4,45E-06	b	1,95E-06	c		
8,2	1,39E-05	a			8,87E-07	b	6,43E-06	b	4,02E-06	b	1,74E-06	c		
9,1	1,25E-05	a			7,94E-06	b	5,71E-06	b	3,57E-06	b	1,53E-06	c		
10	1,14E-05	a			7,18E-06	b	5,14E-06	b	3,21E-06	b	1,36E-06	c		
11	1,04E-05	a			6,44E-06	b	4,53E-06	b	2,81E-06	c	1,18E-06	c		
12	9,51E-06	b			5,84E-06	b	4,04E-06	b	2,49E-06	c	1,04E-06	c		
13	8,78E-06	b			5,33E-06	b	3,64E-06	b	2,23E-06	c	9,21E-07	d		
15	7,61E-06	b			4,53E-06	b	3,01E+06	b	1,82E-06	c	7,44E-07	d		
16	7,13E-06	b			4,21E-06	b	2,77E-06	c	1,67E-06	c	6,76E-07	d		
18	6,34E-06	b			3,68E-06	b	2,37E-06	c	1,41E-06	c	5,67E-07	d		
20	5,71E-06	b			3,26E-06	b	2,06E-06	c	1,22E-06	c	4,85E-07	d		
22	5,19E-06	b			2,93E-06	c	1,82E-06	c	1,07E-06	c	4,21E-07	d		
24	4,76E-06	b			2,65E-06	c	1,62E-06	c	9,47E-07	d	3,70E-07	d		
27	4,23E-06	b			2,32E-06	c	1,39E-06	c	8,04E-07	d	3,10E-07	d		
30			3,80E-06	b	2,06E-06	c	1,21E-06	c	6,94E-07	d	2,65E-07	d	9,54E-08	e
33			3,46E-06	b	1,85E-06	c	1,06E-06	c	5,94E-07	d	2,30E-07	d	8,57E-08	e
36			3,17E-06	b	1,67E-06	c	9,39E-07	c	5,16E-07	d	2,01E-07	d	7,77E-08	e
39			2,93E-06	c	1,53E-06	c	8,40E-07	d	4,53E-07	d	1,78E-07	d	7,11E-08	e
43			2,65E-06	c	1,37E-06	c	7,34E-07	d	3,87E-07	d	1,54E-07	d	6,37E-08	e
47			2,43E-06	c	1,24E-06	c	6,49E-07	d	3,35E-07	d	1,34E-07	d	5,76E-08	e
51			2,24E-06	c	1,13E-06	c	5,80E-07	d	2,93E-07	d	1,19E-07	d	5,26E-08	e
56			2,04E-06	c	1,02E-06	c	5,10E-07	d	2,52E-07	d	1,03E-07	d	4,73E-08	e
62			1,84E-06	c	9,06E-07	d	4,43E-07	d	2,13E-07	d	8,84E-08	e	4,22E-08	e
68			1,68E-06	c	8,17E-07	d	3,90E-07	d	1,84E-07	d	7,68E-08	e	3,80E-08	e
75			1,52E-06	c	7,31E-07	d	3,40E-07	d	1,57E-07	d	6,62E-08	e	3,41E-08	e
82			1,39E-06	c	6,61E-07	d	3,01E-07	d	1,35E-07	d	5,79E-08	e	3,08E-08	e
91			1,25E-06	c	5,88E-07	d	2,61E-07	d	1,14E-07	d	4,94E-08	e	2,74E-08	e
100			1,14E-06	c	5,28E-07	d	2,29E-07	d	1,01E-07	d	4,29E-08	e	2,47E-08	e

Kuva 15. ISO 13849-1 taulukon K.1 pohjalta tehty laskentataulukko
(International Organization for Standardization, 2006)

Vaarallisen vikaantumisen todennäköisyyttä (PFD_h) ei lasketa.
Se valitaan aiemmin laskettujen arvojen perusteella kuvan 15 taulukosta.

Esimerkki: Aiemmin laskettu hätäseis-toiminto

Toiminnolle saatiin $MTTF_d$-arvoksi 68,37 vuotta ja DC-arvoksi 36 %.

Kyseessä on Tulo-Logiikka-Lähtö tyyppinen arkkitehtuuri, jossa on ainoastaan yksi lähtö eikä tarkistuskanavaa. Minkä tahansa komponentin vikaantuminen aiheuttaa turvatoiminnon menettämisen. Kyseessä on siis luokan yksi arkkitehtuuri. Taulukosta saadaan vaarallisen vikaantumisen todennäköisyys $1{,}68*10^{-6}$ (1/h) ja saavutettu suoritustaso PL c.

4 TOTEUTUS

4.1 Riskinarviointi

Koneen vaaroista on tehty riskinarviointi EN ISO 12100:2010 periaatteita noudattaen. Riskinarviointi on yrityksen sisäiseen käyttöön eikä sitä julkaista. Riskinarvioinissa määritettiin koneen raja-arvot, tunnistetiin vaarat, arvioitiin riskin suuruus ja merkitys, sekä suunniteltiin toimenpiteet riskin pienentämiseksi.

4.2 Turvatoiminnot

Riskinarvioinnin perusteella ei vaadita uusia turvatoimintoja. Toteutettavaksi jää EN 16228-1 standardin vaatimat turvatoiminnot. Suoritustasot lasketaan sähköisille ja hydraulisille järjestelmille mutta ei mekaanisille.

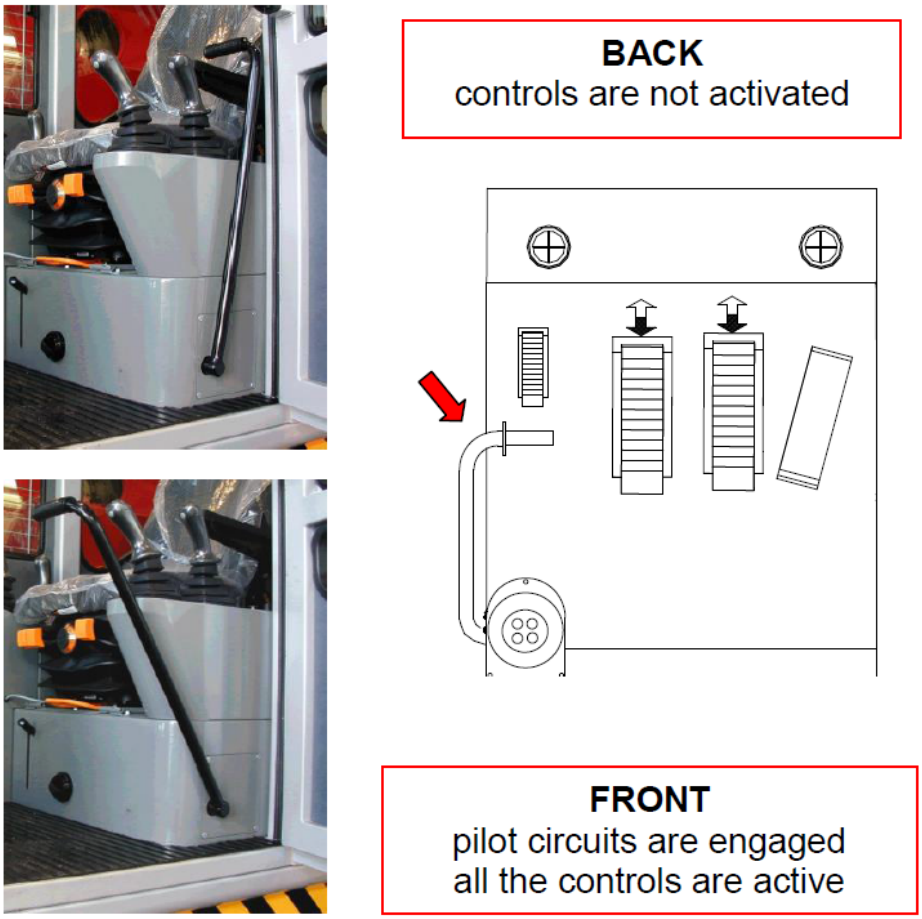
Taulukko 2. Vaatimukset ja vastaavuudet.

Turvatoiminto	Vaadittava suoritus-taso	Toteuttava toiminto	kommentti
Siirtyminen			
Pysähtyminen	PL c	Turvakahva	ajovoimansiirrossa jarru joka aukeaa kun moottoreille tulee paine.
Siirtyminen työkun-nossa			
Pysähtyminen	PL c	Turvakahva	Turvakahva, ajovoimansiirrossa jarru joka aukeaa kun moottoreille tulee paine.
Ylävaunun kääntö			
Pysähtyminen	PL c	Turvakahva	Turvakahva, käännöllä sähköisesti avattava jarru
Työskentelyyn liittyvä nostaminen			
Pysähtyminen	PL c	Turvakahva	Turvakahva, vinsseissä jarru joka aukeaa työpaineesta. Jarrun avaus estettävissä sähköisellä ON-OFF venttiilillä.
Kuorman paikallaan pitäminen	PL c	Turvakahva	Turvakahva, vinsseissä jarru joka aukeaa työpaineesta.
Nostorajat	PL b	sähköiset rajat ja mekaaniset ylärajat	Jarrun avaus estettävissä sähköisellä ON-OFF venttiilillä.
Vinssaus (vetäminen/ankkurointi)			
Pysähtyminen	PL c	Turvakahva	Turvakahva, vinsseissä jarru joka aukeaa työpaineesta. Jarrun avaus estettävissä sähköisellä ON-OFF venttiilillä.
Nostorajat	PL b	sähköiset rajat ja mekaaniset ylärajat	Jarrun avaus estettävissä sähköisellä ON-OFF venttiilillä.
Henkilöitä nostavat työtasot			
Pysähtyminen	PL c	Turvakahva	Vinsseissä jarru joka aukeaa työpaineesta. Jarrun avaus estettävissä sähköisellä ON-OFF venttiilillä. Nostokorissa hätäseis
Nostorajat	PL c	sähköiset rajat ja mekaaniset ylärajat. Mekaaninen putoamisen esto jarru	Jarrun avaus estettävissä sähköisellä ON-OFF venttiilillä.
Koneen tukijalat ja maahan ankkurointi			

pysähtyminen	PL c	Turvakahva	Takajaloissa työpaineella aukeavat lukkoventtiilit
Paikallaan pitäminen	PL c	Turvakahva, hätäseis	Takajaloissa lukkoventtiilit
Turvasuojien aktivointi			
Pyörityksen ja syötön pysähtyminen toimintaan kytkentyn suojuksen tai muun turvalaitteen toimiessa	PL c	-	Ei sovellettavissa Junttan koneisiin. Käyttäjä ei pääse työn aikana käsiksi liikkuviin osiin.
Rajoitettu käyttötapa			
Hitaan pyörityksen ja alennetun syöttönopeuden aloittaminen ja ylläpitäminen	PL c	-	Ei sovellettavissa Junttan koneisiin. Työskentely vaara-alueella kairan pyöriessä kielletty.
Poran pyöritys ja syöttö erityisissä olosuhteissa käytettävän erityisen suojauskäyttötavan aikana			
Pyörityksen ja syötön pysäyttäminen kosketuksen tunnistavan turvalaitteen toimiessa	PL c	-	Ei sovellettavissa Junttan koneisiin. Ei erityistä suojauskäyttötapaa.
Työkalun kiinnitys ja irroitus			
Paikallaan pysyminen	PL b	Turvakahva	Työkalut mekaanisesti kiinnitetty
Poratankojen/-kankien käsittelylaiteet			
Laitteen pysähtyminen	PL c	Turvakahva	Käsitellään pitelijöillä. Sylintereissä lukkoventtiilit.
Maston, puomin tai ohjausmaston siirtämisjärjestelmä			
Maston, puomin tai ohjausmaston pysähtyminen	PL c	Turvakahva	Sylintereissä työpaineella aukeavat lukkoventtilit
Maston, puomin tai ohjausmaston pysyminen paikoillaan	PL c	Turvakahva	Sylintereissä työpaineella aukeavat lukkoventtilit

4.2.1 Turvakahva

Junttan paalutuskoneissa koneen liikkeet on estettävissä turvakahvalla. Kaikki liikkeet ovat hydraulisia, ja saavat käyttövoimansa hydrauliikkapumpuilta. Turvakahva aktivoituna toimilaitteet eivät saa painetta sillä esiohjauspaineet on ohjattu paineetomaan tankkiin.



Kuva 16. Turvakahvan toiminta PMx24-koneen käyttöohjeesta. (Junttan Oy, 2019)

4.2.2 Vinssien sähköiset rajat

Vinssien sähköiset rajat ohjaavat turvatoimintoja jotka estävät köysiä kiristävät liikkeet. Kun mikä tahansa vinssi ajetaan ylärajaan, on kaikkien vinssien vetäminen sekä köysiä kiristävät sylinterien liikkeet estetty ohjaamalla toimilaitteiden esiohjauspaineet tankkiin.

4.3 Vaadittavat suoritustasot

Turvatoiminnoille on laskettiin seuraavat vikaantumistodennäköisyydet:

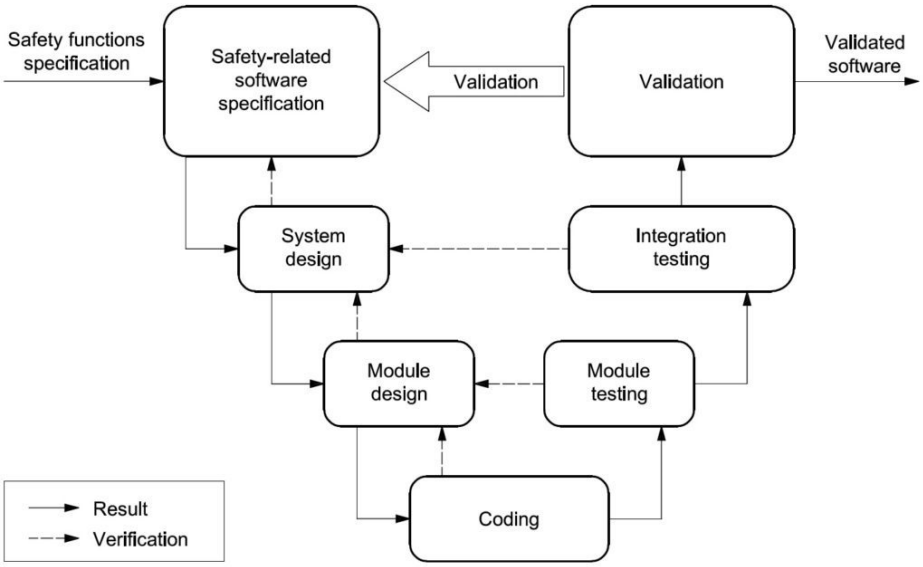
Turvatoiminto	**Vaadittava PL**	**Saavutettu PFHd**	**Saavutettu PL**
Turvakahva	PL c	$1{,}39*10^{-6}$	PL c
Riippurajat	PL b	$1{,}14*10^{-6}$	PL c

Koneen turvatoiminnot täyttävät standardin vaatimukset. Käytetyt laskentataulukot ovat yrityksen sisäiseen käyttöön eikä niitä julkaista.

5 OHJELMALLINEN TOTEUTUS JA TESTAUS

Turvatoiminnot ovat toteutettu nykyisin releillä, mutta tilalla voidaan käyttää tarvittaessa ohjelmoitavaa ohjainlaitetta. Turvatoimintojen totetutusta varten teollisuus- ja koneen ohjaussovelluksissa turvatoimintoihin liittyvät tulot ja lähdöt sekä ohjelmisto on eriytetty muusta ohjausjärjestelmästä. Tällä varmistetaan että turvatoiminnon toimintaa ei voida vahingossa muuttaa esim. ohjaussovellusta päivittäessä. Turvasovellus on usein salasanalla suojattu, joten turvatoiminnon päivittäminen ilman hyväksyntää ja kelpuutusta on estetty.

Turvatoiminnot toteuttava ohjelmisto on suunniteltava täyttämään ohjelmiston turvallisuusvaatimukset, EN ISO 13849-1 kohta 4.6. Vaatimusten päätavoitteena on saada aikaan luettavaa, ymmärrettävää testattavaa ja ylläpidettävää ohjelmistoa. (International Organization for Standardization, 2006)



KUVA 17. V-malli (International Organization for Standardization, 2006)

Ohjelmiston tekeminen alkaa määrittelemällä (puhekielessä speksaamalla). Ohjelmistomäärittelyssä kuvataan mitä ominaisuuksia ohjelmassa on ja kuinka ohjelmiston tulee toimia. Määrittely tulee hyväksyä ennen toteutusta. Testattavuuden kannalta toteutettu ohjelmisto tulee purkaa testattaviin aliohjelmiin ja funktioihin. Ohjelmistomoduulit sekä koko ohjelmisto tulee testata, raportoida, katselmoida ja kelpuuttaa. Tämän jälkeen testattu ja validoitu ohjelmisto voidaan julkaista ja asentaa.
Testaus tulee suunnitella ja suorittaa vaikka turvatoimintoa ei olisikaan toteutettu ohjelmallisesti. Testaus on helppoa, mikäli piiri toteuttaa ainoastaan kombinaatiologiikkaa. Kombinaatiologiikan toiminta voidaan määritellä täysin totuustauluilla.

PL c tai PL d vaatimustason turvatoiminnon toteuttavalle sulautetulle ohjelmistolle on listattu lisävaatimuksia standardin EN ISO 13849-1 kohdassa 4.6.2, kuten projektin hallintajärjestelmä ja laadunhallintajärjestelmä esim. standardeja IEC 61508 ja ISO 9001 vastaavasti.

5.1 Automaattinen ohjelmistotestaus

Monimutkaisia ja laajoja ohjelmistoja toteuttaessa manuaalinen ohjelmistotestaus ei ole enää järkevää. Ohjelman testiajo manuaalisesti kestää helposti useita työpäivä ja ammattitaitoinenkin testaaja väsyy ja tekee virheitä. Sulautettujen järjestelmien testaamiseen käytetään usein Hardware-In-Loop simulaatiota, jossa simulaatiolaitteisto ja ohjausjärjestelmä on kytketty toisiinsa. Testiohjelmalla simuloidaan konetta tai laitetta, jota ohjausjärjestelmä ohjaa. Simulaattorilaitteistolla lähetetään ohjaussignaaleja ohjausjärjestelmän tuloihin ja seurataan miten ohjausjärjestelmän lähdöt reagoivat. Simulaatiosta generoituu testiraportti joka paljastaa onko testit suoritettu hyväksytysti.
Usein turvatoiminnot ovat kuitenkin yksinkertaisia ja niiden toiminnan testaus manuaalisesti on mahdollinen vaihtoehto.

5.2 Ohjelmointisäännöt

Ohjelmointia varten on standardin EN ISO 13849-1 mukaan laadittava säännöt ja käytännöt. Yhteisvikaantumisen varalta on tärkeää että voidaan selvittää ohjelmiston tekijä, ohjelman lataamisen päivämäärä ja versio. Ohjelmointisäännöissä voidaan esimerkiksi sopia muuttujien ja funktioiden nimeämistavat sekä tulojen ja lähtöjen käsittelytavat.

5.3 Sähköjärjestelmän testaus

Turvatoiminnot on testattava ennen koneen käyttöönottoa. EN 60204-1 kohdan 18 mukaan on tehtävä toiminnalliset testit, sekä todennettava, että sähkölaitteisto on dokumentaation mukainen.

5.4 EMC testaus

Paalutuskoneen ohjausjärjestelmä on oltava yhteensopiva EN 13309:2010 (Construction machinery, Electromagnetic compatibility of machines with internal electrical power supply) standardin kanssa. (European Commitee for Standardization, 2014) Standardissa on määritelty konkreettiset rajat testattavan laitteiston lähettämälle häiriölle sekä kuinka paljon laitteiston on siedettävä ulkopuolta tulevaa häiriötä. Sähköiset alikokoonpanot joihin kuljettaja pystyy koskemaan, on testattava staattisia purkauksia varten. Alikokoonpanojen virransyöttö on myös testattava johdettujen transienttien varalta.
Sähkölaitteisto on toteutettava EN 60204-1 kohdan 4 mukaan, jossa on listattuna EMC yhteensopivuuden kannalta olennaisia säteilyä rajoittavia toimenpiteitä.

6 KELPUUTUS

Kelpuutuksella osoitetaan että kaikki turvatoiminnot toteuttava ohjausjärjestelmä täyttää kaikki asiaan kuuluvat EN ISO 13849-1 vaatimukset. Kelpuutuksessa tulee näyttää että jokainen turvatoiminto ja niiden yhdistelmä/kokonaisuus täyttää vaatimukset. Kelpuutusraportissa tulee olla listattuna turvatoimintokohtaisesti kaikki vaatimukset, kuinka toteutus vastaa vaatimusta ja viittaukset toteutuksen dokumentteihin.

7 KUNNOSSAPITO

Ohjausjärjestelmän kunnossapitoon liittyvät asiat sekä määräaikaiset tarkastukset ja niiden ohjeet tulee liittää koneen käyttöohjeeseen. Turvatoimintoon liittyvien osien vanheneminen voi johtaa turvatoiminnon menetykseen ja jopa vaaratilanteeseen ja niille on tarvittaessa suunniteltava ennaltaehkäisevää huoltoa tai komponenttien vaihtoa.

8 TEKNISET ASIAKIRJAT

Suunnitellessa turvallisuuteen liittyvää ohjausjärjestelmän osaa on dokumentoitava asiaankuuluvat tiedot, joita käytetään yrityksen sisäisesti eikä ole tarkoitettu toimitettavaksi koneen hyödyntäjille. Tarvittavat asiakirjat on listattu EN ISO 13849-1 kohdassa 10, ja niihin kuuluu muun muassa:

- Luotettavuuden kannalta merkitykselliset muuttujat ($MTTF_d$, DC, CCF, Toiminta-aika…)
- Arkkitehtuuriluokat
- Suoritustasot
- Toimenpiteet systemaattisen vikaantumisen estämiseksi
- Vika ja vaikutus-analyysit
- Käytetyt teknologiat
- Ohjelmistoa koskeva dokumentaatio
- Toimenpiteet kohtuudella ennakoitavissa olevan väärinkäytön estämiseksi

9 KÄYTTÖÄ KOSKEVAT TIEDOT

Käyttöä koskevat tiedot toimitetaan asiakkaalle. Listattuna on osa vaadituista tiedoista.

ISO 13849-1 kohdan 11 mukaan on noudatettava ISO 12100 periaatteita sekä muita asiaankuuluvien standardien sovellettavissa olevia kohtia kuten EN 60204-1 kohta 17.

EN 60204-1 kohdan 17 mukaan sähkölaitteiston mukana on toimitettava muun muassa:

- Osa- tai dokumenttiluettelo
- Lisädokumentteja joissa:
  - Selvä kattava kuvaus laitteistosta, asennuksesta ja varustelusta
- Tiedot fyysisestä ympäristöstä (Tärinä, epäpuhtaudet)
- Kuvaukset turvalaitteista, sisältäen ulkoisen johdotuskaavion
- Yleiskaavio milloin tarkoituksen mukaista
- Piirikaavio (-kaaviot)

ISO 12100 kohta 6.4 mukaan mukana toimitettavaan kirjalliseen ohjeeseen on sisällytettävä muun muassa:

- Koneen, sen varusteiden, suojusten ja/tai turvalaitteiden yksityiskohtainen kuvaus
- Mahdolliset kielletyt käyttötavat
- Sähkölaitteita koskevat asiakirjat

ISO 13849-1 kohdassa 1 on lisäksi eriteltynä tietoja joita laitteen hyödyntäjälle toimitetaan mm.

- Turvallisuuteen liittyvien osien rajat ja kaikki vikojen poissulkemiset
- Selkeät turvallisuuteen liittyvien ohjausjärjestelmän osien ja turvalaitteiden rajapintojen kuvaukset
- Kunnossapidon tarkastuslistat
- Turvatoimintojen passivointi ja poistaminen
- Suoritustaso: a, b, c, d tai e
- Viittaus EN ISO 13849-1 standardiin
- Luokka B, 1, 2, 3 tai 4

10 YHTEENVETO

Paalutuskoneen ohjausjärjestelmän toteutuksella on tarkat vaatimukset sillä koneella tehtävässä työssä on paljon riskejä ja vaaroja. Koneen käyttö on kuitenkin turvallista kun koneen hyödyntäjät tottelevat konevalmistajan suosituksia sekä ohjeita ja koneenvalmistaja suunnittelee laitteet standardien mukaisesti. Standardien läpikäyminen ja niiden mukaan toimiminen on jokapäiväistä arkea koneenrakennusalalla ja CE-merkinnän kannalta välttämätöntä.

11 POHDINTA

Sulautettujen ohjausjärjestelmien kehitys on huimaa. Monet konevalmistajat, mukaan lukien Junttan, ovat yhdistäneet koneiden ohjausjärjestelmiä Internetiin ja pilvipalvelimiin. Moniin ohjausmoduuleihin ohjelmat ladataan jo IP-verkon yli. Tämä luo mahdollisuuksia mm. etänä tehtäviin ohjelmapäivityksiin, kaluston seurantaan ja diagnostiikkaan. Tätä standardeissa ei kuitenkaan huomioida, vaikka tämä aiheuttaa ihan suoranaisia riskejä. Uusimmissakin ohjausmoduuleissa ethernet-rajapinta on täysin suojaamaton ja ohjaimen liittäminen suojaamattomaan verkkoon mahdollistaa, että kuka vain voi luoda yhteyden ohjausjärjestelmään.

Työ oli haastava ja työläs. Asioita tehtiin useampaan kertaan, sillä standardit eivät ole kovinkaan konkreettisia, mikä johtaa helposti väärinymmärryksiin. Tästä syystä aiheesta löytyy paljon kirjoja ja työkaluja, jotka helpottavat standardien soveltamista. Onneksi apuna oli ammattilaisia, jotka ovat tehneet töitä vuosia näiden standardien parissa. Työ sai hyvän vastaanoton toimeksiantajalta ilman moitteita. Julkaistavasta materiaalista sovittiin, että riskiarviointia ja laskentataulukoita ei julkaista. Työstä oli selvä hyöty toimeksiantajalle, sillä tämä helpottaa tulevia suunnitteluprojekteja. Tämä tieto tulee kuitenkin osittain vanhenemaan lähivuosina, sillä EN16228-standardista on tulossa uusi versio lähivuosina. Uudesta standardista on esitetty ensimmäinen vedos, jossa on muutoksia vaatimustasojen ja ohjelmistosuunnitteluprosessin osalta.

12 LÄHDELUETTELO

International Organization for Standardization. (2006). *EN ISO 13849-1 Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet.*

International Organization for Standardization. (2010). *EN ISO 12100 Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen.*

European Commitee for Standardization. (2006). *EN 60204-1 Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset.*

European Commitee for Standardization. (2014). *EN 16228-1, Drilling and foundation equipment-Safety.*

Junttan Oy. (2019).