ESPOO 2004 VTT TIEDOTTEITA 2264

Timo Malm & Maarit Kivipuro

Turvallisuuteen liittyvät ohjausjärjestelmät konesovelluksissa

Esimerkkejä

Työturvallisuus kohti maailman kärkeä
TYÖTAPATURMAOHJELMA 2001–2005

Työsuojelurahasto
Arbetarskyddsfonden
The Finnish Work Environment Fund

VTT

VTT TIEDOTTEITA – RESEARCH NOTES 2264

Turvallisuuteen liittyvät ohjausjärjestelmät konesovelluksissa Esimerkkejä

Timo Malm & Maarit Kivipuro
VTT Tuotteet ja tuotanto

ISBN 951–38–6500–2 (nid.)
ISSN 1235–0605 (nid.)

ISBN 951–38–6501–0 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 5, PL 2000, 02044 VTT
puh. vaihde (09) 4561, faksi (09) 456 4374

VTT, Bergsmansvägen 5, PB 2000, 02044 VTT
tel. växel (09) 4561, fax (09) 456 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 5, P.O.Box 2000, FIN–02044 VTT, Finland
phone internat. + 358 9 4561, fax + 358 9 456 4374

VTT Tuotteet ja tuotanto, Tekniikankatu 1, PL 1307, 33101 TAMPERE
puh. vaihde (03) 316 3111, faksi (03) 316 3495

VTT Industriella System, Tekniikankatu 1, PB 1307, 33101 TAMMERFORS
tel. växel (03) 316 3111, fax (03) 316 3495

VTT Industrial Systems, Tekniikankatu 1, P.O.Box 1307, FIN–33101 TAMPERE, Finland
phone internat. + 358 3 316 3111, fax + 358 3 316 3495

Päällikannen kuvat on kerätty Pilzin, Siemensin ja Himan www-sivuilta [Pilz www-sivut, Hima www-sivut & Siemens image database].

Toimitus Leena Ukskoski

Otamedia Oy, Espoo 2004

Malm, Timo & Kivipuro, Maarit. Turvallisuuteen liittyvät ohjausjärjestelmät konesovelluksissa. Esimerkkejä [Safety-related control systems in machinery. Examples]. Espoo 2004. VTT Tiedotteita – Research Notes 2264. 90 s. + liitt. 4 s.

Avainsanat safety systems, safety principles, safety standards, control system safety

Tiivistelmä

Automaattisten järjestelmien nopeutuessa ja monimutkaistuessa koneiden turvallisuus kohdentuu yhä useammin ohjausjärjestelmään, jonka viat voivat johtaa turvatoimintojen menettämiseen. Tämä tulee esiin tilanteissa, joissa kone suorittaa tehtävää, jonka väärä toiminta voi aiheuttaa vaaratilanteen ihmisen ollessa koneen vaikutuspiirissä. Turvallisuuteen liittyvät standardit antavat hyvän perustan riittävän turvallisuustason saavuttamiseksi. Standardien vaatimusten ja ohjeiden omaksuminen vaikeasta ”lakitekstistä” on suunnittelijoille usein työlästä. Osa turvallisuusperiaatteista voi jäädä huomioimatta tai soveltamatta. Sopivat periaatteelliset esimerkit helpottavat turvallisuusperiaatteiden omaksumista, ja niitä voidaan soveltaa myös omissa suunnitelmissa. Tässä julkaisussa esitetään esimerkkikirjasto turvallisuuteen liittyvistä koneautomaation ohjausjärjestelmistä. Esimerkit ovat periaatteellisia, yleispäteviä ja suunnittelijan sovellettavissa käytetyistä komponenteista riippumatta. Julkaisussa ei esitetä valmiita teknisiä ratkaisuja vaan turvallisuusperiaatteita graafisessa muodossa. Esimerkit on luokiteltu standardin SFS-EN 954-1 (EN ISO 13849-1) mukaan, koska tämän standardin luokittelu perustuu piirirakenteisiin. Siten piirikaaviosta on pääteltävissä esimerkkiratkaisun standardinmukainen luokka. Kolmesta esimerkistä on tehty myös PowerPoint-animaatiot, joissa näkyvät vaiheittain eri toiminnat ja vikatilanteiden kehittymiset. Tämäntyyppinen visualisointi helpottaa ymmärtämistä mutta edellyttää kuitenkin taitoa lukea piirikaavioita.

Malm, Timo & Kivipuro, Maarit. Turvallisuuteen liittyvät ohjausjärjestelmät konesovelluksissa. Esimerkkejä [Safety-related control systems in machinery. Examples]. Espoo 2004. VTT Tiedotteita – Research Notes 2264. 90 p. + app. 4 p.

Keywords safety systems, safety principles, safety standards, control system safety

Abstract

The safety of an automated machine is depending increasingly on the control system, because systems are getting faster and more complex. More and more often the operator or driver is not able to control the system quick or well enough to guarantee alone the safety, but he needs the help of the safety system. However, deficiencies or failures in the control system of a machine may lead to a dangerous loss of safety functions. Safety standards give a good basis to reach adequate safety level. However, it is often hard to adopt safety requirements and guidelines purely from standard text. Suitable, generic examples help to adopt the safety principles and they can be applied to designers own solutions. This report presents an example library concerning safety related machine control systems. The examples are classified according to standard SFS-EN 954-1. The classification of the standard is depending on circuit architecture and therefore the category can be concluded from diagrams. A PowerPoint animation based on three examples was also created. Animation helps in understanding safety principles, but knowledge about circuit diagrams is needed.

Alkusanat

Tähän julkaisuun on kerätty ”Turvallisuuskriittiset ohjausjärjestelmät konesovelluksissa – esimerkkejä” -tutkimuksen tuloksia. Tutkimus on hyväksytty kansalliseen työtapaturmaohjelmaan. Hankkeeseen ovat osallistuneet Timo Malm ja Maarit Kivipuro VTT Tuotteet ja tuotanto -tutkimusyksiköstä, Matti Katajala, Jarmo Niemi, Markku Nurminen ja Suvi Suomalainen Mipro Oy:stä, Markku Laiho, Jalo Vuorinen, Petri Kaivola, Jarmo Taponen ja Jari Hauta-aho Siemensiltä ja Matti Sundquist Uudenmaan työsuojelupiiristä. Lisäksi arvokkaita kommenteja ovat antaneet Jari Karjalainen, Jorma Järvnpää ja Marita Hietikko VTT Tuotteet ja tuotanto -tutkimusyksiköstä. Maarit Kivipuro on kirjoittanut pääosin luvun 2 ja Timo Malm luvut 1, 3, 5 ja 6. Luku 4 on toteutettu yhteistyössä. Kiitämme hankkeeseen osallistuneita yhteistyöstä ja avusta. Hankkeen päärahoittajana on ollut Työsuojelurahasto.

Tämä raportti julkaistaan Työsuojelurahaston avustuksella.

Tampereella 12.8.2004

Tekijät

Sisällysluettelo

1. Johdanto

Tähän julkaisuun on kerätty esimerkkikirjasto turvallisuuteen liittyvistä koneautomaation ohjausjärjestelmistä. Esimerkit on luokiteltu standardin SFS-EN 954-1 mukaan, koska standardin luokittelu liittyy vahvasti järjestelmän arkkitehtuuriin. Esimerkkien keräämisen on tarkoitus jatkua vielä tämän julkaisun julkaisemisen jälkeenkin. Standardin IEC 61508 ja IEC 62061 eheystasoihin otetaan kantaa vain yleisellä tasolla, koska eheystasoihin sisältyy paljon suunnitteluperiaatteisiin ja todennäköisyyksiin liittyviä tekijöitä. Näillä on epäsuora yhteys järjestelmien arkkitehtuuriin ja piirirakenteisiin.

Automaattisen koneen turvallisuus riippuu järjestelmien nopeuden, laajuuden ja monimutkaisuuden lisääntyessä yhä enemmän ohjausjärjestelmästä. Ohjausjärjestelmän viat voivat johtaa turvatoimintojen menettämiseen, odottamattomaan käynnistymiseen tai väärään toimintoon ja sitä kautta tapaturmiin ja muihin vahinkoihin. Ihmiset ovat oppineet luottamaan turvalaitteisiin ja turvallisiin piirirakenteisiin ja siksi niiden viat ovat yllättäviä ja usein myös vaarallisia. Tämän vuoksi on tärkeää varmistaa, että turvapiirit eivät erikoistilanteissakaan – kuten vikatilanteissa – toimi tavalla, joka voisi aiheuttaa vaaratilanteen.

Tässä turvallisuuteen liittyvät ohjausjärjestelmät on jaettu kolmeen ryhmään käyttötarpeen mukaan. Ensimmäiseen ryhmään kuuluvat perinteiset – lähinnä estoihin ja lukituksiin liittyvät – turvatoiminnat, joilla estetään vaaralliset toiminnat lukituksien ollessa voimassa. Esimerkiksi puristimissa ohjausjärjestelmä pysäyttää valoverholta saadun tiedon perusteella vaarallisen liikkeen, ennen kuin ihmisen käsi jää väliin. Myös räjähdysvaarallisissa tiloissa luotetaan turvalliseksi osoitetun ohjausjärjestelmän kykyyn estää lämmityslaitteen ylikuumeneminen. Tähän ryhmään liittyviä esimerkkejä löytyy lähes jokaisesta tuotantojärjestelmästä.

Turvajärjestelmien toisessa ryhmässä ihmisen vastuuta turvallisuudesta on siirretty automaatiojärjestelmälle esim. nopeuden tai monimutkaisten syy- ja seuraussuhteiden vuoksi. Manuaalikoneissa turvallisuus perustuu pitkälti ihmisen toimintaan ja valvontaan. Järjestelmien tullessa yhä monimutkaisemmiksi ja nopeammiksi ei valvontaa enää voida jättää pelkästään ihmisen varaan. Vaaralliset toiminnot pitää voida pysäyttää automaattisesti ja nopeasti. Esim. ”drive-by-wire” tai yleisemmin ”X by wire” -tyyppisiä ohjauksia on käytetty mm. lentokoneiden ja monien työkoneiden ohjauksessa. Näissä mekaaninen yhteys ohjausratista pyöriin tai esim. peräsimeen on korvattu sähköohjauksella. Väärä ohjaus voisi johtaa törmäykseen. Monenlaiset ajoneuvonosturit ja henkilönostimet pysyvät pystyssä ohjausjärjestelmän ja kuormituksen valvontajärjestelmän ansiosta. Ilman valvontajärjestelmää ihminen voisi vahingossa ohjata koneen epästabiiliin tilaan.

Turvajärjestelmien kolmannessa ryhmässä ohjausjärjestelmän vastuuta turvallisuudesta on lisätty vähentämällä kalliita, hitaita ja raskaita rakenteita. ”Järjellä” on siis korvattu ”rautaa”. Esimerkiksi pitkissä paineenalaisissa putkissa seinämän vahvuutta on voitu vähentää toteuttamalla luotettava paineenrajoitusjärjestelmä.

Taulukko 1 kuvaa esimerkkejä turvatoiminnoista ja niiden luokittelusta. Tässä luokittelu on tehty turvatoiminnan monimutkaisuuden mukaan.

Taulukko 1. Tyypillisiä turvatoimintoja.

Päälle/pois-tyyppiset toiminnat	- käynnistäminen, pysäyttäminen, hätäpysäyttäminen, energian katkaisu, jarruttaminen, venttiilin sulku tai avaus, - toimintatavan valinta
Yksinkertaisen suureen valvonta	- lämpötilan, paineen, nopeuden, massan tms. suureen valvonta, - liikealueen rajan tunnistaminen
Laskentaa edellyttävän suureen valvonta	- kuormituksen, vakavuuden, tms. valvonta, - turvallisen toiminnan loogisuuden valvonta, - työkalupisteen nopeus
Turvallisuuteen liittyvät säädöt ja ohjaukset	- nopeuden, kiihtyvyyden säätö, - liikkeen tai liikeradan ohjaus ja valvonta - virtauksen, paineen tms. säätö - työkalun kiinnittäminen ja valvonta

Konepäätöksen mukaan ”Ohjauspiirin logiikkavirhe, häiriö tai vahingoittuminen ei saa johtaa vaaratilanteisiin”. Tämä yleisluonteinen vaatimus on mahdollista tulkita tiukastikin, mutta tarkempia koneiden ohjausjärjestelmiin liittyviä vaatimuksia on esitetty standardeissa. Näistä tärkeimpiä ovat SFS-EN 954-1 ja IEC 61508 sekä siitä johdettu konejärjestelmiin sovellettava standardiluonnos IEC 62061.

1.1 Tekniikan ja vaatimusten kehittyminen

I980-luvun alussa turvallisten piirirakenteiden peruskomponentti oli ns. pakkotoiminen rele. Tämän avulla on mahdollista valvoa apukoskettimilla primäärikoskettimien tilaa luotettavasti. Pakkotoimisilla releillä on mahdollista toteuttaa monenlaisia ”idioottivarmoja” kytkentöjä, joissa yksittäinen vika saadaan paljastettua koskettimien vaihtaessa tilaansa. Pienen epävarmuuden tuo se, että valvonta voi toteutua ainoastaan koskettimien vaihtaessa tilaansa. Valvonta ei siis toimi hyvin kohteissa, joissa koskettimet vaihtavat vain hyvin harvoin (esim. kerran vuodessa) tilaansa. 1980-luvulla elektronisissa piireissä turvallisuus perustui usein pulssitetun tiedon kuljettamiseen ja toisaalta kahden-

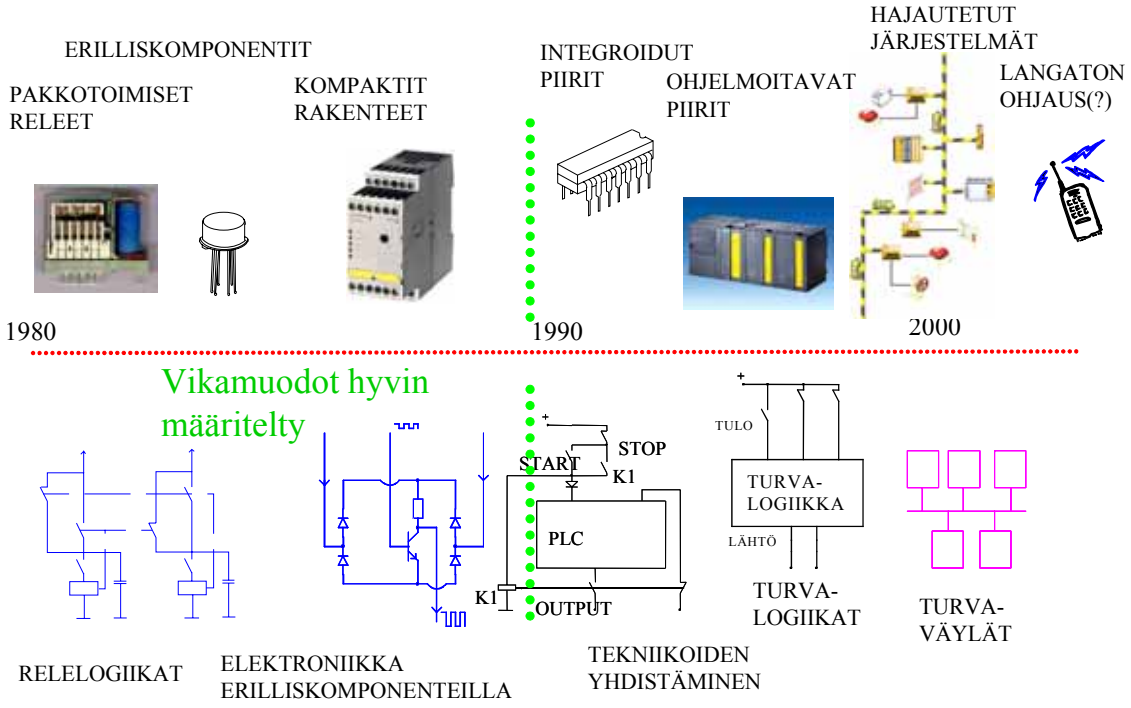
nuksiin ja valvontaan. Edellä mainituissa piirirakenteissa on yhteistä se, että niissä vikamuodot tunnetaan ja että ne ovat kohtuullisesti hallinnassa. Epävarmuutta tuovat yhteisviat, joissa menetetään samanaikaisesti monta varmistavaa tekijää esim. saman ylijännitteen seurauksena.

Ohjelmoitavat laitteet ovat monimutkaisia, ja niiden vikakäyttäytymistä on vaikea hallita. Toiminnan turvallisuutta on jo pitkään parannettu toteuttamalla varmennukset systeemitasolla esim. käyttämällä kahta erilaista logiikkaa. Jos turvallisuus taataan systeemitasolla puuttumatta piirirakenteiden yksityiskohtiin, saattaa järjestelmästä tulla kallis ja silti joidenkin yksityiskohtien varmistukset saattavat jäädä epävarmoiksi. Menetelmässä tavallaan korvataan määrällä tuntemattomaksi jäänyttä laatua (esim. laadukasta ja virheetöntä sovellusohjelmaa). Menetelmällä on omat etunsa, kun käytetään sopivasti erilaisuutta (diversiteettiä) ja riittävää tarkkuutta analyyseissä.

Ensimmäiset turvalogiikat koneautomaation turvapiireihin tulivat markkinoille vasta 1990-luvun puolessa välissä. Turvalogiikoissa toiminta on sisäisesti varmistettu monenlaisella keinoilla. Lisäksi tyypilliset sovellusohjelmat on ”pakotettu” selkeiksi käskykannan monipuolisuutta kaventamalla, mikä tosin saattaa johtaa pidempiin ohjelmiin. Ohjelmoitavien laitteiden validointiin sopivien menetelmien kehitys on osaltaan vaikuttanut turvalogiikkojen hyväksyntään. Ohjelmoitavilla laitteilla on mahdollista toteuttaa huomattavasti monipuolisempaa valvontaa kuin yksinkertaisemmilla tekniikoilla, mutta niissä järjestelmän monimutkaisuus aiheuttaa pientä epävarmuutta. Hajautetuissa järjestelmissä epävarmuutta tuo lisäksi se, että perusratkaisuissa saattaa turvaviestin kuljettamiseen olla käytössä vain yksi signaalitie.

2000-luvulle tultaessa ensimmäiset turvaväylät olivat jo markkinoilla. Hajautetut järjestelmät sisältävät osaltaan ohjelmoitavan järjestelmän siihen liittyvine etuineen ja haittoineen, mutta sarjamuotoinen tiedonsiirto tuo niihin omia piirteitä. Hajautetuissa järjestelmissä yksinkertaiset vikamuodot, kuten tiedonsiirtolinjan menettäminen, ovat tyypillisesti hyvin hallinnassa, koska nämä riskit ovat helposti tunnistettavissa. Toisaalta uudenlaiset vikamuodot, kuten väärät osoitetiedot tai sanomien vääristyminen, voivat saada aikaan yllättäviä seurauksia.

Langatonta ohjausta on käytetty esim. siltanostureiden ohjauksessa jo pitkään. Kuitenkaan kriittisimpiä nostoja tai turvatoimintoja ei ole toteutettu radio-ohjauksella. Uusia haasteita ovat olleet radioyhteyden häiriöllisyys ja mahdollinen ulkopuolisten signaalien pääsy järjestelmään. Turvallisiksi todettuja radiomodeemeja on jo markkinoilla. Kuitenkin laajamittainen langaton ohjaus tai langattomat verkot turvakäytössä ovat vasta tulossa. Kuva 1 esittää turvapiireissä hyväksyttyjen tekniikoiden kehitystä.



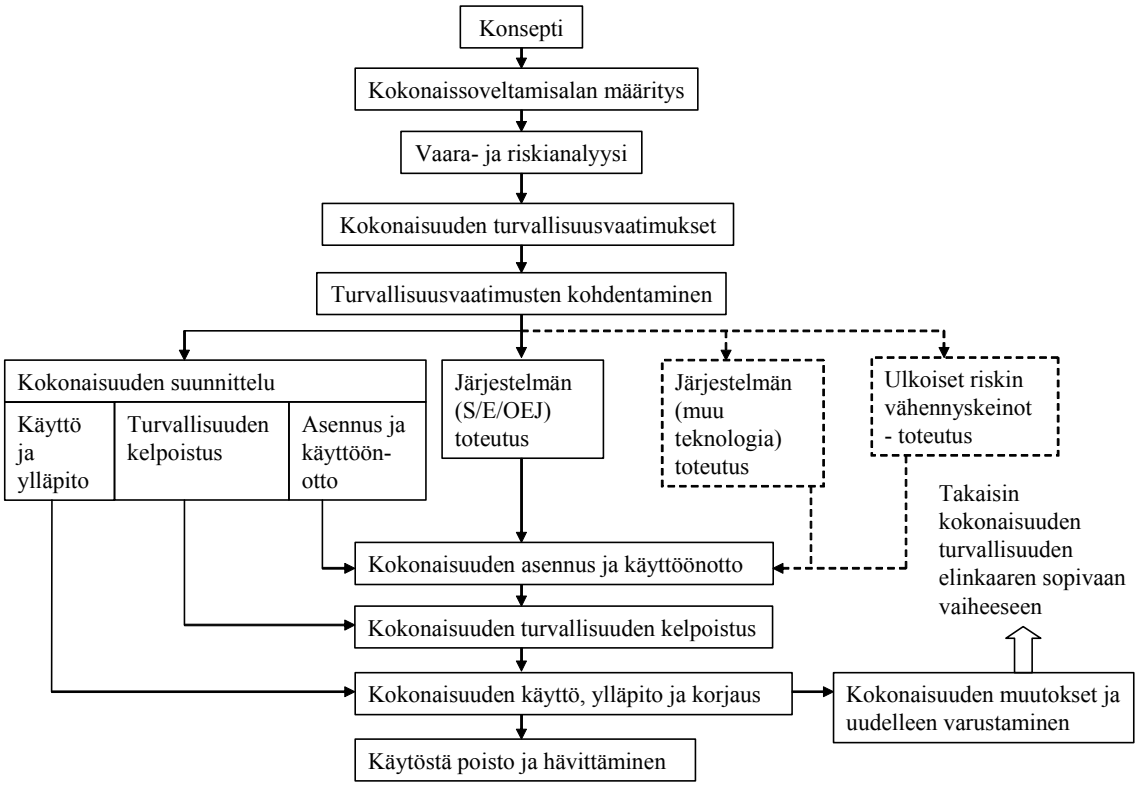
Kuva 1. Turvapiireissä käytetyt tekniikat eri aikoina.

Eräs uudehko kehityssuunta on turvatoimintojen integrointi muuhun järjestelmään. Perinteisesti turvatoiminnot on pyritty erottamaan muista toiminnoista. Toimintojen integrointi yhteen on uutena tekniikkana tuonut uusia teknisiä haasteita. Integroitaessa turvallisuustekijöitä muuhun järjestelmään kasvaa validoinnissa eli kelpuutuksessa tarvittavan työn määrä. Toisaalta komponenttien lukumäärää voidaan hieman vähentää. Tämä sopii usein järjestelmiin ja laitteisiin, joita tuotetaan paljon ja joihin ei tehdä muutoksia. Jos muutoksia on odotettavissa tai järjestelmältä odotetaan erityisen korkeaa turvallisuuden eheyden tasoa, on turvallisuuteen liittyvien osien erottaminen muusta järjestelmästä kannattavaa.

1.2 Ohjausjärjestelmän suunnitteluprosessi

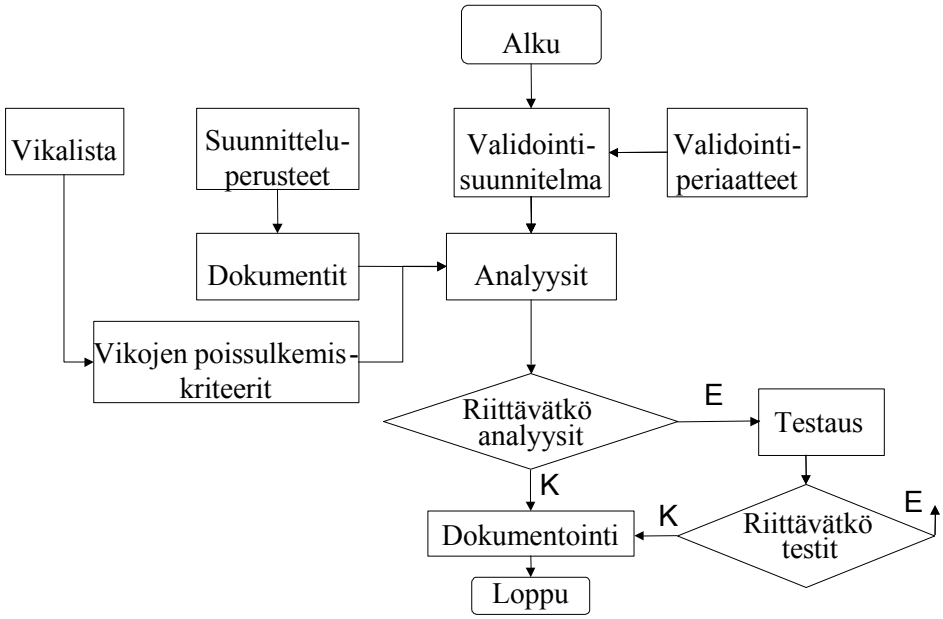
Kuva 2 esittää standardin IEC 61508 mukaista elinkaarimallia. Turvallisuussuunnitteluprosessin pääperiaate on, että aluksi tunnistetaan riskit, kehitetään niitä vastaavat vaatimukset seka kehitetään keinot riskien minimoimiseksi ja lopuksi validoidaan järjestelmä vertaamalla esitettyjä riskienminimoimiskeinoja vaatimuksiin. Validoinnissa käytetään apuna analyysejä ja testaamista. Ohjelmoitavien järjestelmien validoinnissa pitää kiinnittää huomiota koko suunnitteluprosessiin, koska siten pystytään välttämään virheitä paremmin kuin toteuttamalla validointi vain suunnitteluprosessin loppuvaiheessa. Yksi turvallisuuden elinkaarimallin ajatus on, että kun koko suunnitteluprosessi toteutetaan

huolellisesti, virheiden määrä saadaan minimoitua paremmin kuin tarkastettaessa järjestelmä vasta suunnittelun päätteeksi. Standardin mukaan turvallisuus pyritään takaamaan suunnittelemalla järjestelmä toisaalta välttämällä vikoja (luotettavuus) ja toisaalta minimoimalla vikojen seuraukset (varmistukset).



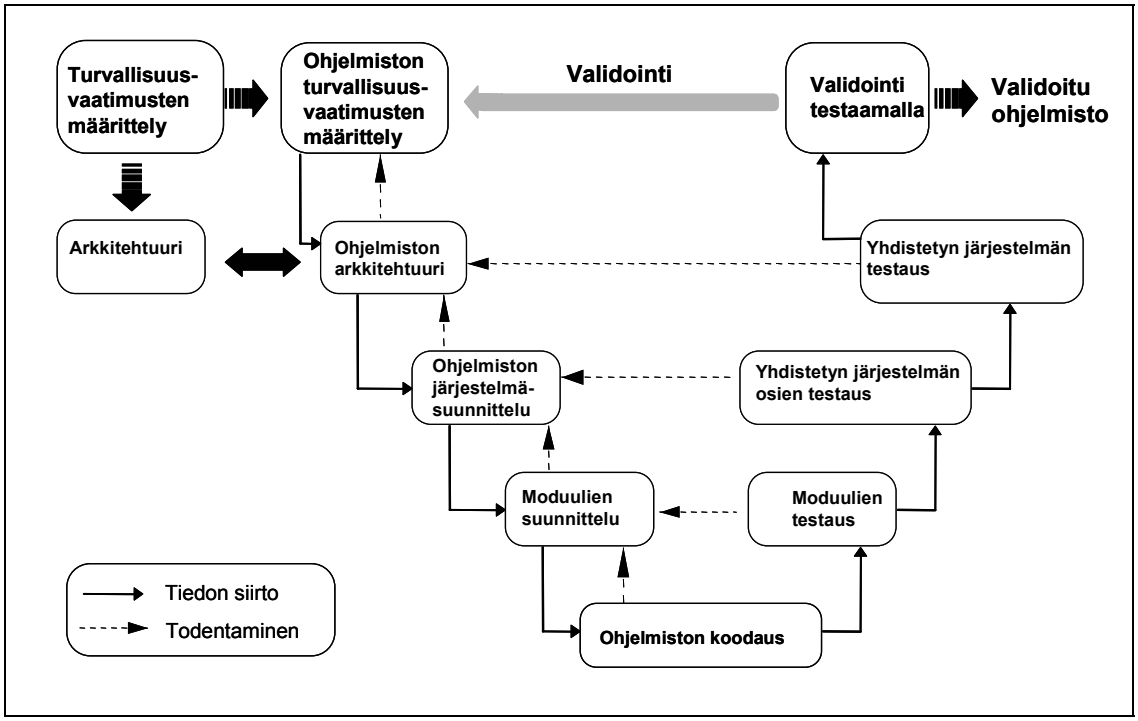
Kuva 2. Standardin IEC 61508 mukainen turvallisuuden elinkaarimalli.

Standardi EN ISO 13849-2 esittää validointiprosessin (vrt. kuva 3), jossa järjestelmän vikoja pyritään tunnistamaan analyyseillä. Validointiprosessissa määritetään aluksi tarkasteltavat vikatyypit, ja sitten tarkastellaan näiden vikatyyppien seurauksia. Validointiprosessi edellyttää huolellista ja tarkkaa piirin analysointia. Käytännössä järjestelmä analysoidaan vika- ja vaikutusanalyysillä. Analyysissä kriittisiksi todettuja kohtia varmistetaan testauksella. Testauksella on mahdollista tarkastaa vain hyvin rajallinen osa monimutkaisesta järjestelmästä.



Kuva 3. Standardin EN ISO 13849-2 mukainen validointiprosessi (kelpuutusprosessi).

Ohjelmoitavien järjestelmien suunnittelu- ja validointiprosessi toteutetaan usein ns. V-mallin mukaan (kuva 4), jossa varsinainen suunnittelu alkaa ylätason määrittelyistä ja päättyy yksityiskohtaiseen koodaukseen. Testausvaihe puolestaan alkaa pienimmistä yksiköistä ja päättyy kokonaisuuden testaukseen. Suunnittelussa ja testauksessa todennetaan aina jokainen vaihe vertaamalla tuloksia kyseisen vaiheen vaatimuksiin. Validointi tehdään testausvaiheessa vertaamalla tuloksia alussa määriteltyihin turvallisuusvaatimuksiin. V-mallia voidaan soveltaen käyttää myös järjestelmien suunnitteluun ja validointiin.



Kuva 4. Ohjelmiston suunnittelun V-malli IEC 61508-3:n mukaan.

2. Tapaturmat

Työsuojeluhallinnon tapaturmaselostusrekisteristä (TAPS) etsittiin ja luokiteltiin koneen ohjausjärjestelmästä aiheutuneita vakavia tapaturmia (51 kpl). Tapaturmat rajattiin sellaisiin, joissa mainittiin sana ”ohjausjärjestelmä”.

Eniten tapaturmia sattui häiriönpoistotilanteissa (43 %), joissa koneen käyttäjä havaitsi virheellisen toiminnan ja meni itse poistamaan häiriötä. Tapaturmista 25 % sattui normaalin tuotannon aikana, 24 % säädön, asetusten muuttamisen, puhdistuksen tai työkalun vaihdon aikana ja 8 % korjauksen ja huollon aikana, jolloin huoltomies oli korjaamassa koneessa ollutta vikaa.

Tapaturmat on tässä luokiteltu tarkastelemalla selostuksia ja poimimalla yleisimmät selostuksissa mainitut syyt. Kaikkiin tapaturmiin on ollut useita syitä. Toimintamuodot, joissa tapaturma on sattunut, on jaettu neljään: tuotantoon, häiriönpoistoon, korjaukseen ja neljäntenä ryhmänä säätöön, asetusten muuttamiseen, puhdistukseen ja työkalun vaihtoon. Kukin tapaus on kuulunut yhteen toimintamuotoon.

Seuraavassa on otteita tapaturmista:

Betonituotetehtaassa valmistettiin betonilaattoja automaattisella konelinjalla. Konelinjan laatankääntö- ja siirtolaitteessa oli ollut toimintahäiriöitä. Uhri oli mennyt tutkimaan häiriön syytä konelinjan ollessa käynnissä ja jäänyt puristuksiin laatan siirtolaitteen väliin. (TAPS sel. nro 11445.)

Tärkeimpiä syitä tapaturmaan olivat
- odottamaton käynnistys
- puutteellinen suojaus
- vaarallinen työmenetelmä.

Lavapakkauslinjalla työskennellyt havaitsi lamellikuljettimen ja nostopöydän välissä tarpeetonta roskaa ja ryhtyi refleksinomaisesti poistamaan sitä. Samanaikaisesti oikaisutela teki paluuliikkeen, jolloin työntekijän käsi jäi telan ja nostopöydän runkorakenteiden väliin. (TAPS sel. nro 21881.)

Tärkeimpiä syitä tapaturmaan olivat
- työntekijän vahinko
- odottamaton käynnistys.

Työntekijä työskenteli maalaamon jatkojalostusosaston automaattisella palasahalla määrämittasahaajana. Syöttötyönnin teki ohjelmaan kuulumattoman virheliikkeen, jolloin

työntekijän käsi jäi puristuksiin syöttötyöntimen ja sivutasaajan väliin. (TAPS sel. nro 05368.)

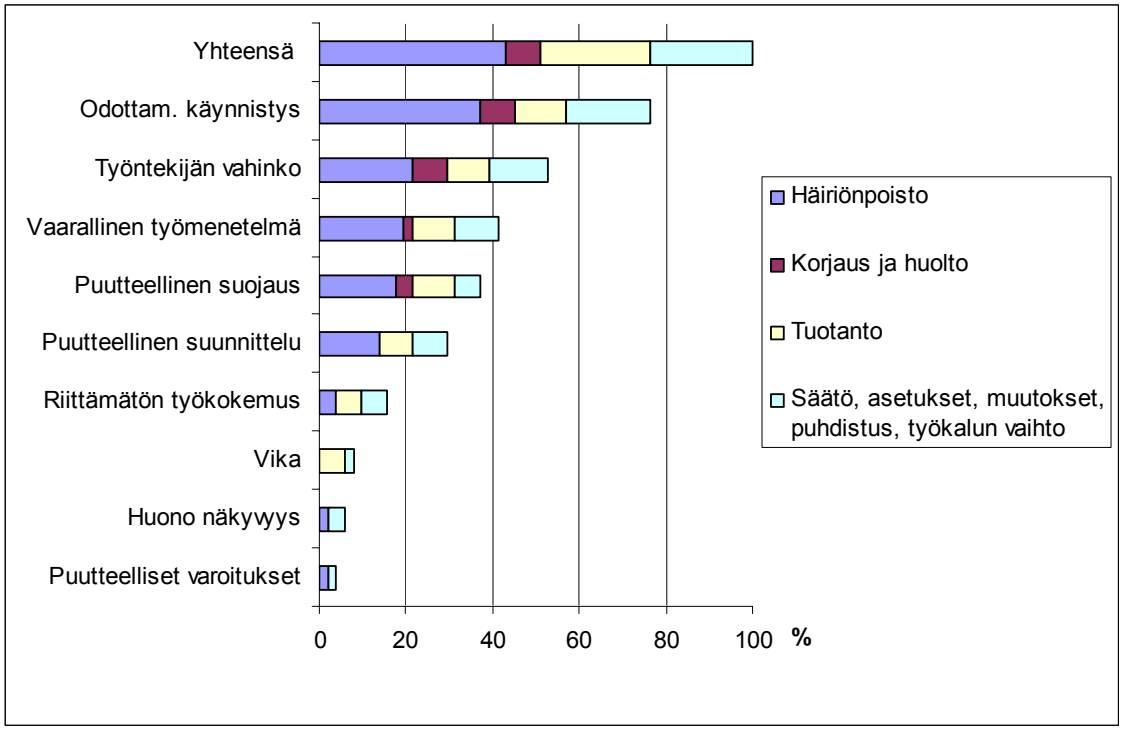
Tärkeimpiä syitä tapaturmaan olivat

- riittämätön työkokemus,
- työntekijän vahinko,
- odottamaton käynnistys.

Puutteellinen suojaus on ollut syynä 37 %:ssa kaikista tapaturmista ja odottamaton käynnistys 76 %:ssa tapaturmista. Näihin kumpaankin tekijään pystytään vaikuttamaan ohjausjärjestelmällä, turvalaitteilla ja suojuksilla. Vaarallinen työmenetelmä (41 %), puutteellinen suunnittelu (esim. paljon häiriöitä) (29 %), huono näkyvyys (6 %) ovat kaikki syitä, joihin voidaan vaikuttaa suunnittelulla ja ohjeilla. Taulukko 2 esittää tapaturmien syitä eri tilanteissa ja kuva 5 tapaturmien syiden suhteellista osuutta eri tilanteissa.

Taulukko 2. Koneen ohjausjärjestelmästä aiheutuneiden TAPSista koottujen tapaturmien syitä ja osuuksia eri toimintamuodoissa.

		Kpl tapauksia eri toimintamuodoissa			
	Yht. kpl.	Häiriön-poisto	Korjaus ja huolto	Tuotanto	Säätö, asetusten muuttaminen, puhdistus, työkalun vaihto
Yhteensä kpl	51	22	4	13	12
Yhteensä %	100	43	8	25	24
Odottam. käynnistys	39	19	4	6	10
Työntekijän vahinko	27	11	4	5	7
Vaarallinen työmenetelmä	21	10	1	5	5
Puutteellinen suojaus	19	9	2	5	3
Puutteellinen suunnittelu	15	7		4	4
Riittämätön työkokemus	8	2		3	3
Vika	4			3	1
Huono näkyvyys	3	1			2
Puutteelliset varoitukset	2	1			1



Kuva 5. Tapaturmien syitä ja suhteellisia osuuksia. Jokaiseen tutkittuun tapaturmaan on ollut useita syitä, joten syiden summa on yli 100 %.

Häiriönpoistotilanteissa merkittävämpinä syinä ovat olleet odottamaton käynnistys ja työntekijän vahinko. Vaarallinen työmenetelmä on ollut myös tavallinen tapaturmien syy häiriönpoistossa. Työntekijän vahingon ja vaarallisen työmenetelmän ero on siinä, että ”vaarallinen työmenetelmä” on ollut jatkuva ”normaali” työtapa, kun taas ”työntekijän vahinko” on ollut vahinko tai juuri sillä kerralla käytetty ainutkertainen menetelmä. Näistä erityisesti ”vaaralliseen työmenetelmään” voidaan vaikuttaa koulutuksella ja tiedottamisella. Koska tapaturmia sattuu eniten juuri häiriötilanteissa, olisi häiriöiden vähentämisellä suuri vaikutus myös tapaturmien määrään.

Tuotannonaikaisiin tapaturmiin ovat vaikuttaneet erityisesti odottamaton käynnistys, puutteellinen suojaus, vaarallinen työmenetelmä ja työntekijän vahinko. Näiden osalta ei voida tehdä pitkälle meneviä johtopäätöksiä, koska otos on ollut niin pieni.

Säätö- ja asetustenmuutostilanteissa merkittävimpiä tapaturmien syitä ovat olleet odottamaton käynnistyminen ja työntekijän vahinko.

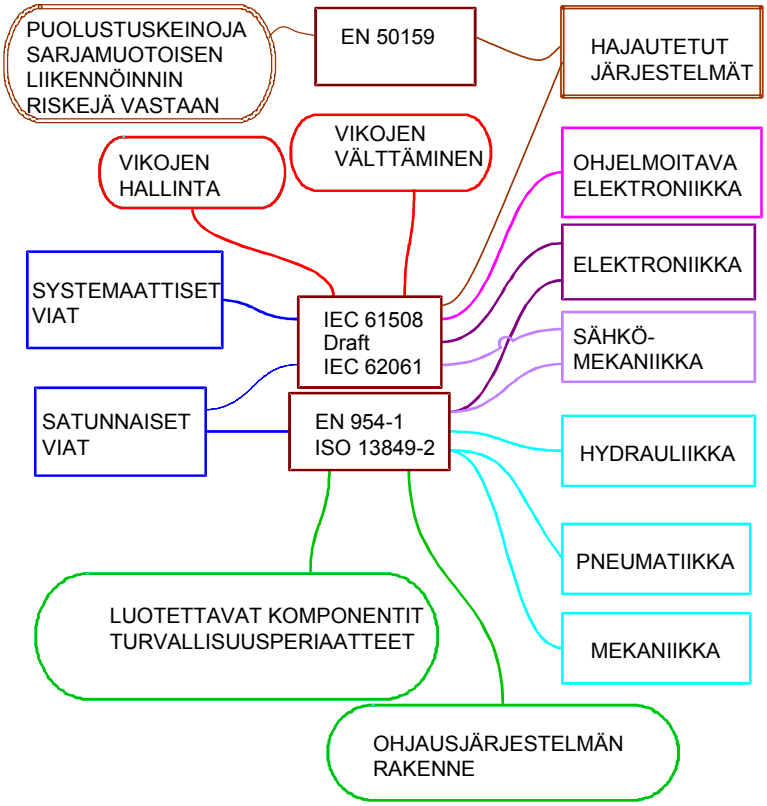
Tapaturmia on korjaustilanteissa sattunut niin vähän, että prosenttiluvut ovat viitteellisiä. Luvuista kuitenkin nähdään, että korjauksen aikaisiin tapaturmiin ovat vaikuttaneet erityisesti odottamaton käynnistys ja työntekijän vahinko.

3. Ohjausjärjestelmiin liittyvät vaatimukset

3.1 Ohjausjärjestelmiin liittyviä standardeja

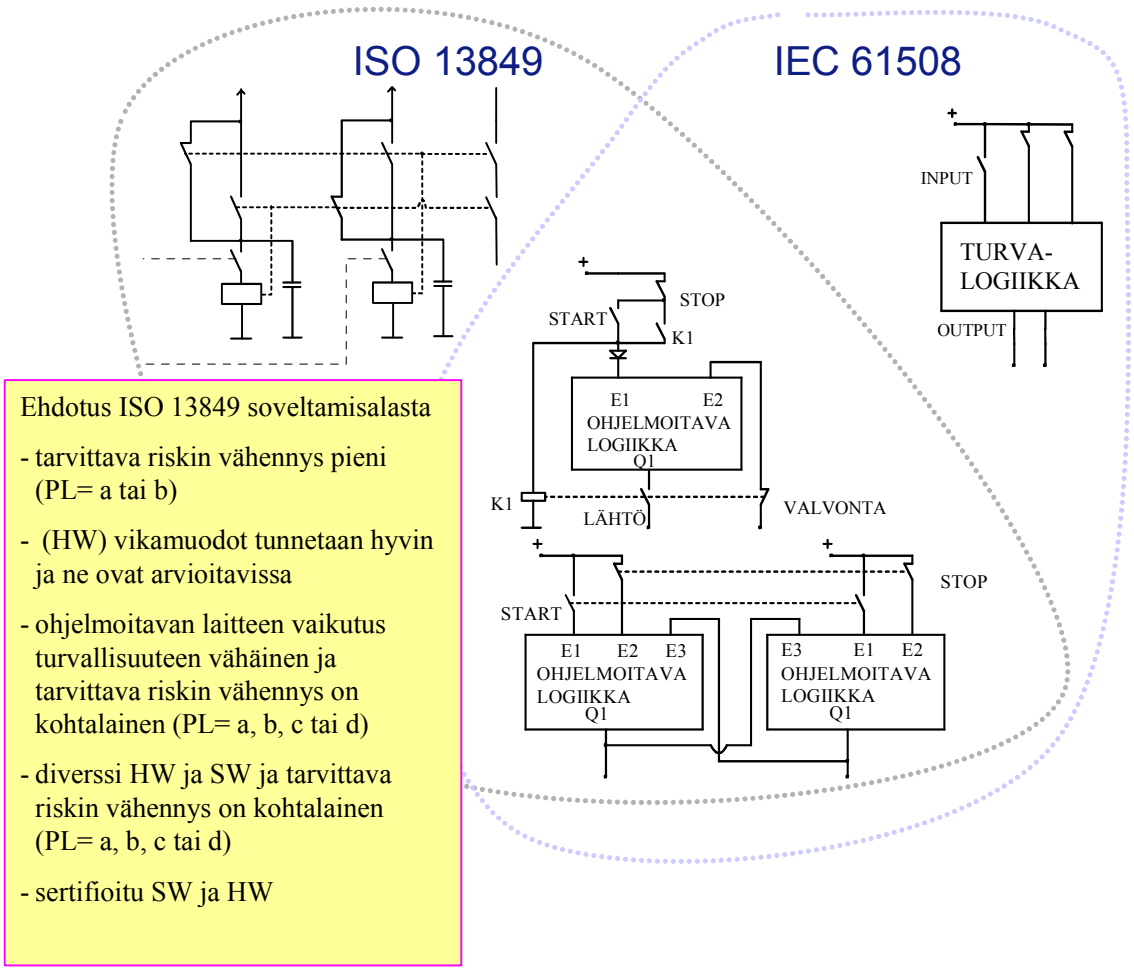
Konejärjestelmien ohjausjärjestelmien toiminnan turvallisuutta käsittelevä perusstandardi on vuonna 1996 ilmestynyt SFS-EN 954-1 ”Turvallisuuteen liittyvät ohjausjärjestelmien osat”. Standardissa luokitellaan turvallisuuteen liittyvät ohjausjärjestelmät vikatilannekäyttäytymisen, sovellettujen turvallisuusperiaatteiden ja luotettavuuden (luokassa 1) mukaan luokkiin B, 1, 2, 3 ja 4. Standardi käsittelee pneumaattisia, hydraulisia, sähköisiä, elektronisia ja jossain määrin ohjelmoitavia (ei kuitenkaan ohjelmistoja) ohjausjärjestelmiä. Standardin 2-osassa EN ISO 13849-2 esitellään vikamuodot, jotka pitää ottaa huomioon ohjausjärjestelmää analysoitaessa.

IEC 61508 (SFS-EN 61508) on IEC:n kattostandardi, joka esittää yleiset periaatteet turvallisuuteen liittyvien järjestelmien tarkasteluun. Standardissa tuodaan esiin järjestelmän elinkaarimalli, jossa kuhunkin vaiheeseen esitetään vaatimuksia, sekä kvantitatiivinen lähestymistapa laitteiston kykyyn toimia turvallisesti. IEC 62061 (EN 62061) on konejärjestelmien ohjausjärjestelmiin suuntautunut IEC 61508:n sovellusstandardi. Järjestelmän IEC 61508 mukainen käsittely edellyttää tarkastavia toimenpiteitä ja dokumentointia suunnittelun kaikissa vaiheissa, eikä ainoastaan lopuksi. Kuva 6 esittää erilaisia turvapiireissä käytettyjä tekniikoita, standardeja sekä niiden esittämiä luokitteluja ja vikoja vastaan esitettyjä puolustuskeinoja. Kuvassa oleva standardi EN 50159 (osat 1 ja 2) liittyy rautateiden viestintään, mutta siinä on esitetty sarjamuotoiseen viestintään liittyviä hyviä ohjeita, jotka soveltuvat myös koneautomaation sovelluksiin.



Kuva 6. Ohjausjärjestelmien toiminnan turvallisuuteen liittyviä standardeja ja niiden käsittelemiä alueita.

Kuva 7 esittää standardiluonnosten EN ISO 13849-1 ja IEC 62061 käsittelemiä sähköisiä ohjausjärjestelmiä. EN ISO 13849-1:n sovellusalue liittyy sähkömekaanisiin, elektronisiin ja vain osittain ohjelmoitaviin järjestelmiin, kun taas IEC 62061:n sovellusalue liittyy erityisesti ohjelmoitaviin ja elektronisiin järjestelmiin. IEC 62061:n käsittelytapa on yleensä monimutkaisempi kuin EN ISO 13849:n, ja siksi valmistajan usein kannattaakin mahdollisuuksien mukaan pitäytyä EN ISO 13849:n (SFS-EN 954-1) käsittelytavassa. Jos järjestelmä sisältää ohjelmoitavia osia, EN ISO 13849:n käsittely ei yksistään riitä, koska ohjelmoitavien osien tarkastelu jää suppeaksi. Tällöin pitää harkita epävarmuuden ratkaisemista ylemmällä tasolla, mikä usein tarkoittaa diversiteettiä ja laitteistokahdennuksia. Toinen vaihtoehto on käsitellä ohjelmoitava järjestelmä yksityiskohtaisesti IEC 62061:n mukaan. Aihetta esittelee tarkemmin kuva 7.



Kuva 7. EN ISO 13849:n ja IEC 62061 soveltamisalat EN ISO 13849-1 standardiluonnoksen mukaan[1] [prEN ISO 13849-1, 2004].

3.2 Pysäytysluokat

Pysäytystoiminnot jaetaan kolmeen luokkaan, jotka ovat seuraavat:

- Luokka 0: pysäyttäminen poistamalla välittömästi teho koneen toimilaitteilta.
- Luokka 1: valvottu pysähtyminen, jossa koneen toimilaitteilla on teho pysähtymisen aikaan saamiseksi. Pysähtymisen jälkeen teho poistetaan toimilaitteilta
- Luokka 2: valvottu pysähtyminen, jossa koneen toimilaitteilla säilytetään teho [SFS- EN 60204-1].

[1] PL=performance level, turvallisuuteen liittyvän osan kyky toteuttaa turvafunktio (ennustettavissa olevissa olosuhteissa), mikä edelleen toteuttaa oletetun riskin vähennyksen.
HW= hardware, laitteisto; SW= software, ohjelmisto

Pysäytyksessä kaikki kolme luokkaa ovat käytettävissä, mutta hätäpysäytyksessä käytetään riskin arvioinnin mukaan joko luokkaa 0 tai 1. Toisin sanoen hätäpysäytyksessä pitää toimilaitteelta purkaa energiat välittömästi tai mahdollisimman nopeasti toimilaitteen pysähdyttyä. Luokan 1 pysäytystä käytetään yleensä silloin, kun järjestelmää ei voida pysäyttää välittömästi vaan se pitää ensin ajaa alas (esim. hidastaa nopeutta). Siis: vaikka hätäpysäytyksen tulee tapahtua mahdollisimman nopeasti, se ei kuitenkaan saa aiheuttaa lisävaaraa.

3.3 Yleisiä turvallisuusperiaatteita

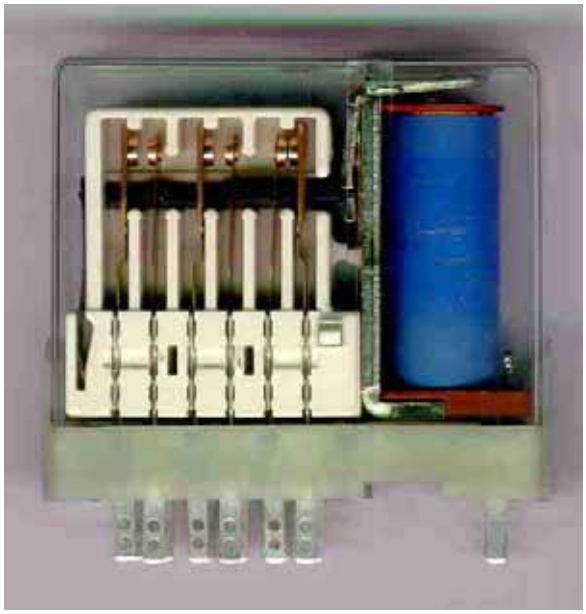
Taulukko 3 esittää standardissa EN ISO 13849-2 luokiteltujahyvin koeteltuja sähköteknisiä turvallisuusperiaatteita. Samassa standardissa on esitetty myös muihin tekniikoihin liittyviä hyvin koeteltuja turvallisuusperiaatteita sekä turvallisuuden perusperiaatteita.

Taulukko 3. Hyvin koeteltuja sähköteknisiin järjestelmiin liittyviä turvallisuusperiaatteita (EN ISO 13849-2).

Toiminta	Huomioita
Pakkotoimiset koskettimet	Käytä valvontatoiminnoissa pakkotoimisia koskettimia (vrt. Kuva). Pakkotoimisissa koskettimissa koskettimet on sidottu jämäkästi toisiinsa siten, että ne pysyvät aina toisiinsa nähden samassa asennossa, vaikka esim. yksi kosketin hitsautuisi kiinni.
Kaapelivikojen välttäminen	Kahden vierekkäisen kaapelin oikosulun välttämiseksi käytä kaapelia, jossa jokainen johdin on suojattu maadoitetulla suojalla, tai lattakaapeleissa käytä signaalijohtimen välissä yhtä maadoitettua johdinta.
Riittävät erotusvälit	Käytä riittäviä etäisyyksiä liittimien, komponenttien ja johdotusten välillä estämään tahattomat kytkennät.
Energian rajoitus	Käytä kondensaattoria syöttämään rajallinen energiamäärä esim. ajastinsovelluksissa.
Sähköisten parametrien rajoitus	Jännitteen, virran, energian tai taajuuden rajoittamisella vaikutetaan esim. momentin rajoittamiseen ja alennettuun nopeuteen sekä vältetään vaaralliseen tilaan joutuminen.
Ei epämääräisiä tiloja	Vältä epämääräisiä tiloja ohjausjärjestelmässä. Suunnittele ja rakenna ohjausjärjestelmä siten, että normaalin toiminnan ja kaikkien odotettavissa olevien toimintojen aikana sen tilat, esim. lähdöt, voidaan ennustaa.
Pakkotoiminen sähkömekaniikka	Liike ohjataan suoraan koskettimiin ilman joustavia osia. Ohjainpäästä (esim. rajakytkimen rullapää) on jäykkä kestävä yhteys koskettimiin. Periaatteessa ohjainpäähän vaikuttamalla saadaan vaikka hitsautuneet koskettimet auki.
Vikamuotojen suuntautuminen	Piirin tulee mikäli mahdollista siirtyä vikaantuessaan turvalliseen tilaan. Vikamuotojen suuntautuminen helpottaa valvontaa huomattavasti, koska voidaan olettaa, että vikatilanteessa piiri käyttäytyy tietyllä tavalla..
Komponenttien vikamuotojen suuntautuminen	Valitaan komponentteja, jotka vikaantuvat tietyllä tavalla. Komponenttien vikamuotojen suuntautumista voidaan hyödyntää valvonnassa.
Ylimitoitus	Virta ja kytkentätaajuus ovat alle 50 % nimellisestä ja oletettavissa oleva kytkentöjen määrä alle kymmenesosan koko eliniästä.
Minimoi vikojen mahdollisuus	Erota turvapiirit muista piireistä. Jos turvapiirit ovat erillään, on tarkasti tarkasteltavien osien määrä pienempi kuin, jos turvapiirit ja muut piirit olisivat integroituina. Tämä periaate pienentää vikojen todennäköisyyttä.
Optimoi monimutkaisuus tai yksinkertaisuus	Monimutkaisuus tuo usein paremman hallittavuuden, kun taas yksinkertaisuus parantaa luotettavuutta.

Pakkotoiminen rele

Kuva 8 esittää pakkotoimista relettä (vrt. EN 50205 ja EN 60947-5-1). Kuvan releessä koskettimet on sidottu toisiinsa muovisillalla, joka pitää ne aina toisiinsa nähden samassa asennossa. Releen valvonta perustuu juuri siihen oletukseen, että releen koskettimet ovat toisiinsa nähden niin luotettavasti suorassa mekaanisessa yhteydessä, että vapaana olevaa kosketinta voidaan käyttää valvontaan (vrt. luvun rele-esimerkit). Lisäksi releen koskettimet on koteloitu siten, että kosketin ei katketessaan pääse aiheuttamaan muualle oikosulkua. Pakkotoiminen rele ei kuitenkaan yksinään paranna turvallisuutta, mutta kun niitä on useita, tietyissä piirirakenteissa niillä pystytään toteuttamaan (vrt. luvun 4 rele-esimerkit) luotettava valvonta.



Kuva 8. Pakkotoiminen rele, joka on tarpeen useimmissa turvallisuuteen liittyvissä relekytkennöissä.

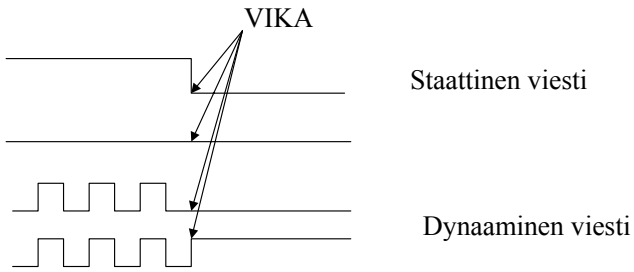
Pakkotoiminen rajakytkin tai painike

Pakkotoimisessa rajakytkimessä tai paikkeessa (vrt. pakkotoiminen sähkömekaniikka) voima välittyy ohjainpäästä luotettavasti suoraan koskettimiin. Jos ohjainpäähän kohdistuva voima on riittävä, niin koskettimet avautuvat, vaikka ne olisivat hitsautuneet kiinni.

Dynaaminen/staattinen viesti

Dynaamisella viestillä tarkoitetaan sitä, että lähetetty viesti muuttaa koko ajan muo-toaan, vaikka looginen tila ei muuttuisikaan. Tämä on tavallista esim. sarjamuotoisessa viestinnässä. Epätavallisempaa jatkuva tilan muuttuminen on sähkömekaniikassa (esim. releet), koska komponenttien jatkuva tilanvaihto kuluttaa niitä. Dynaamisella viestillä saavutetaan

se etu, että sillä voidaan havaita välittömästi yksinkertainen vika, kuten oikosulku tai katkos. Kuva 9 esittää yksinkertaisen dynaamisen viestin ja staattisen viestin vertailua normaali- ja vikatilanteessa. Väyläliikenne on puolestaan huomattavasti monimutkaisempaa kuin tässä esitetty dynaaminen periaate, ja siihen liittyvät vikamuodot ovat myös monimutkaisia (vrt. tämän luvun kohta ”Väyläliikenteen valvontakeinoja”).



Kuva 9. Esimerkki dynaamisen ja staattisen viestin käyttäytymisestä vikatilanteessa. Vikatilanteessa staattisessa tilassa ajaudutaan jompaan kumpaan hyväksyttyyn tilaan, kun taas dynaamisessa viestinnässä havaitaan viestien puuttuminen.

Redundanssi (varmennus)

Tässä on kaksi redundanssin eli varmennuksen määritelmää, joista ensimmäistä on käytetty varsinkin ohjelmoitavissa laitteissa ja jälkimmäistä, suppeampaa, varsinkin sähkötekniikassa.

Redundanssi eli varmennus tarkoittaa menetelmän olemassaoloa sen lisäksi, että on menetelmä, joka olisi riittävä toiminnallisen yksikön suorittaa vaadittava toiminta. Varmennus voi liittyä myös siihen, miten hyvin tieto edustaa informaatiota. Sekä kahdennetut toiminnalliset komponentit että pariteettibittien lisäys ovat molemmat esimerkkejä varmennuksesta. [IEC 61508-4]

Useamman kuin yhden laitteen tai järjestelmän osan käyttäminen varmistamaan toiminta niin, että yhden vikaantuessa toinen on käytettävissä toiminnan suorittamiseen [SFS-EN 60204-1].

Diversiteetti (erilaisuus)

Diversiteetti eli erilaisuus tarkoittaa vaaditun toiminnan toteuttamista erilaisilla tavoilla. Erilaisuus voidaan saavuttaa erilaisilla fysikaalisilla menetelmillä tai erilaisilla suunnittelun lähestymistavoilla.[IEC 61508-4]

Erilaisuudella saavutetaan kahdennetuissa tai äänestävissä järjestelmissä riippumattomuus yhdestä vian syystä. Jos tämä vian syy aiheuttaa yhden kanavan toimimattomuuden, niin muu osa järjestelmästä ei tästä syystä tule toimimattomaksi.

Toiminnallinen valvonta

Toiminnallisessa valvonnassa ohjausjärjestelmän normaalissa toimintarytmissä komponentit vaihtavat tilaansa työkierron aikana ja ohjausjärjestelmä siirtyy toiminnasta toiseen vasta, kun turvalliselle toiminnalle asetetut ehdot täyttyvät.

Ohjelmoitavan elektroniikan valvontakeinot

Ohjelmoitava elektroniikka antaa mahdollisuudet monipuoliseen valvontaan, johon voi liittyä mm. tilavalvontaa, loogisuusvalvontaa, aikavalvontaa, tarkistussummia, toistoa, diversiteettiä, Hamming-koodeja ja luvattoman käytön estoa. Ohjelmoitavilla laitteilla pystytään siis valvomaan asioita, joiden valvonta muulla tekniikalla olisi vaikeaa. Monipuolisuuden ja laajuuden haittapuoli on se, että virheiden mahdollisuus kasvaa.

Väyläliikenteen valvontakeinoja

Sarjamuotoisessa viestinnässä, kuten kenttäväylissä, on tietynlaisia riskejä, joihin on olemassa puolustuskeinoja. Taulukko 4 esittelee sarjamuotoisen viestinnän viesteihin liittyviä uhkia ja puolustuskeinoja. Monenlaiset viat, häiriöt ja ohjelmavirheet johtavat tilanteisiin, joissa juuri viesteille tai viestiliikenteelle tapahtuu muutoksia (vrt. taulukko 4).

Taulukko 4. Sarjamuotoiseen liikennöintiin liittyvät uhat (IEC 61508-2) ja esimerkkejä puolustuskeinoista uhkia vastaan.

Puolustus Viestiin liittyvä uhka	Järjestysnumerot	Aikaleima	Aikaraja	Turvakoodi, esim. CRC	Kuittausviestit	Jäsenmoduulien valvonta	Tunnisteet lähettäjälle ja vastaanottajalle	Toisto	Toimintojen ajoituksiin perustuva arkkitehtuuri	Viestien muuntelu	Merkitsevien viestien välisen eron maksimointi
Toisto	•	•							•	•	
Tuhoutuminen	•	•			•			(•)	•	•	
Lisäys	•				•			•		•	
Väärä järjestys	•	•			(•)			(•)	•	•	
Vääristyminen				•	•			(•)		•	•
Viive		•	•		•				•		
Naamio (esim. väärä osoite)				•	•		•				•

Kommunikointiin ja yleisesti ohjelmistoon liittyviä riskejä voidaan tarkastella myös järjestelmätasolla. Järjestelmätason riskejä ovat: järjestelmän lukkiutuminen (crash), viestien ja toiminnan menettäminen joksikin ajaksi (omission), ajoitusvirheet (timing), data-virhe (data corruption) ja normaalista poikkeava järjestelmän toiminta (byzantine). Näihin ylätason riskien puolustuskeinoihin kuuluvat teknisinä menetelminä arkkitehtuuri, topologia ja redundanssi sekä yleisinä menetelminä yleinen huolellisuus, järjestelmälliset menetelmät, hyvät työkalut, laatu, dokumentointi, validointi yms. Edellä mainituilla viestiliikenteen puolustuskeinoilla on vaikutusta myös järjestelmätason uhkiin. [Hérard et al. 2003.]

Kommunikoinnin alemman tason uhkia ovat erilaiset laiteviat ja häiriöt. Nämä voidaan luokitella esim. seuraavasti: suunnitteluviat (laitteisto ja ohjelmisto), pysyvät viat, palautuvat viat (häiriöt) ja tahalliset viat (esim. virukset ja luvattomat ohjelmistomuutokset).

Kaksoisventtiili

Kaksoisventtiili on lähinnä pneumatiikassa käytetty venttiilirakenne, jossa venttiilissä on kaksi erikseen ohjattavaa karaa. Jos molemmat karat eivät ole liikettä ohjaavassa tilassa, ilma ei pääse venttiilin läpi ja poistuu kohteesta. Venttiili itse siis paljastaa jumiutuneen karan ja toteuttaa turvatoiminnon.

Hydrauliikan turvaventtiilejä

Hydrauliikan erilaisten turvaventtiilien tyypillinen tehtävä on pitää toimilaite hallitusti paikallaan erikoistilanteissakin. Tähän käytetään mm. kuormanlaskuventtiilejä ja letkurikkoventtiilejä. Kuormanlaskuventtiili pitää sisällään vastaventtiilin, toimilaitteen lukinnan ja paineenrajoitustoiminnan. Letkurikkoventtiilillä estetään letkun rikkoutumistilanteesa toimilaitteen hallitsematon liike. Kun venttiilejä käytetään turvallisuuteen liittyvissä toiminnoissa, pitää niissä soveltaa EN ISO 13849-2 (liite C) -standardissa esitettyjä turvallisuusperiaatteita.

4. Standardin SFS-EN 954-1 luokat

Standardin SFS-EN 954-1 mukainen luokka valitaan kohteen riskin tai tarkemmin sanottuna ohjausjärjestelmään kohdistuvan riskin vähennystarpeen mukaan. Mitä suurempi vastuu ohjausjärjestelmällä on turvallisuudesta, ja toisaalta, mitä suuremmat riskit kohteessa on, sitä korkeamman luokan ohjausjärjestelmä on tarpeen. Nykyään on jo monissa standardeissa esitetty tiettyjen toimintojen luokka standardin SFS-EN 954-1 mukaan. Käytännössä tämä tarkoittaa sitä, että standardin tekijä on jo tehnyt kyseisen laitteen funktiolle riskianalyysin ja päätynyt tiettyyn tarvittavaan riskin vähennyksen tasoon. Jos valmista luokkavaatimusta ei ole tiedossa, joudutaan riskin arviointi tekemään itse ja päättelemään tarvittava luokka esim. standardin SFS-EN 954-1 liitteen B mukaan. Ohjausjärjestelmien valintaan liittyvää riskinarviointiprosessia ei tässä julkaisussa käsitellä tarkemmin.

Sitten, kun on valittu luokka (SFS-EN 954-1 mukaan), voidaan ohjausjärjestelmä toteuttaa sen mukaisesti. Taulukko 5 esittää SFS-EN 954-1 -standardin luokkien perusvaatimuksia. Vaatimuksissa esiintyy usein vikatilannekäyttäytymiseen liittyviä vaatimuksia. Tarkempaa tietoa eri komponenteilla huomioonotettavista vikamuodoista on esitetty standardin 2-osassa EN ISO 13849-2. Samoin käsite hyvin koeteltu turvallisuusperiaate on esitetty samassa standardissa eri tekniikoiden osalta.

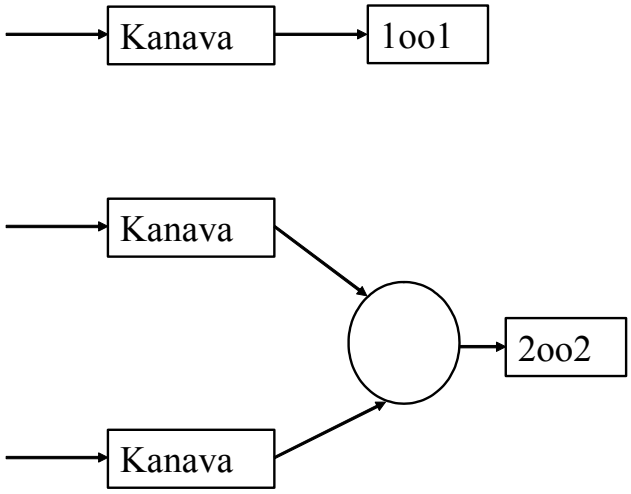
Taulukko 5. SFS-EN 954-1 "Turvallisuuteen liittyvät ohjausjärjestelmien osat" -standardin luokat tiivistetyssä muodossa [SFS-EN 954-1].

	Yhteenveto vaatimuksista	Järjestelmän käyttäytyminen
B	Turvallisuuteen liittyvät ohjausjärjestelmien osat tai niihin liittyvät turvalaitteet sekä myös niiden komponentit on suunniteltava, rakennettava, valittava, kokoonpantava ja yhdistettävä asiaankuuluvien standardien mukaisesti siten, että ne voivat kestää odotettavissa olevat vaikutukset.	Vian esiintyminen voi johtaa turvatoiminnon menettämiseen.
1	On sovellettava luokan B vaatimuksia. On käytettävä hyvin koeteltuja komponentteja ja turvallisuusperiaatteita.	Vian esiintyminen voi johtaa turvatoiminnon menettämiseen, mutta vian esiintymisen todennäköisyys on pienempi kuin luokassa B.
2	On sovellettava luokan B vaatimuksia ja hyvin koeteltuja turvallisuusperiaatteita. Koneen ohjausjärjestelmän on tarkistettava turvatoiminnot sopivin väliajoin.	Vian esiintyminen voi johtaa turvatoiminnon menettämiseen tarkistuksien välillä. Turvatoiminnon menettäminen havaitaan tarkistuksessa.
3	On sovellettava luokan B vaatimuksia ja hyvin koeteltuja turvallisuusperiaatteita. Turvallisuuteen liittyvät osat on suunniteltava siten, että - yksittäinen vika missään osassa ei johda turvatoimintojen menettämiseen, - mahdollisuuksien mukaan yksittäinen vika havaitaan.	Turvatoiminto suoritetaan yksittäisestä viasta huolimatta. Eräät, mutta eivät kaikki viat, havaitaan. Havaitsematta jäävien vikojen kerääntyminen voi johtaa turvatoiminnon menettämiseen.
4	On sovellettava luokan B vaatimuksia ja hyvin koeteltuja turvallisuusperiaatteita. Turvallisuuteen liittyvät osat on suunniteltava siten, että - yksittäinen vika missä osassa tahansa ei johda turvatoiminnon (toimintojen) menettämiseen - yksittäinen vika havaitaan silloin, kun turvatoimintoa tarvitaan seuraavan kerran tai ennen sitä. Jos tämä ei ole mahdollista, vikojen kerääntyminen ei saa johtaa turvatoiminnon menettämiseen.	Turvatoiminto suoritetaan vioista huolimatta. Viat havaitaan ajoissa turvatoiminnon menettämisen estämiseksi.

Luvun 4 kohdasta 4.2 eteenpäin esitetään esimerkkejä, jotka liittyvät eri SFS-EN 954-1 luokissa käytettyihin turvallisuusperiaatteisiin. Tässä ei esitetä valmiita teknisiä ratkaisuja, koska niiden selittäminen veisi paljon aikaa. Lyhyesti esitetyistä periaatteista soveltaja voi nopeasti valita omaan käyttöönsä sopivimmat ja käyttää tässä esitettyjen periaatteiden lisäksi yleistä ”state-of-the-art”-tekniikan tietämystä. Yksikään tässä esitetyistä ratkaisuista ei ole voimassa aina, vaan ratkaisuihin liittyy toteutukseen sisältyviä ehtoja, joista olennaisimpia esim. komponenttivalintoihin liittyviä on esitetty esimerkkien selityksissä, joiden ollessa voimassa esitetty luokka voidaan saavuttaa. Kokonaista järjestelmää suunniteltaessa voidaan vasta kokonaisuutta tarkasteltaessa päätyä tiettyyn luokkaan. Luokat liittyvät toimintoihin, joihin liittyy usein antureita, ohjausjärjestelmä ja toimilaite. Esim. hätäpysäytystä tarkasteltaessa katsotaan painiketta, hätäpysäytyksen toteuttavaa ohjausjärjestelmän osaa sekä jarrun ja moottorin ohjausta.

Esimerkit on pyritty toteuttamaan valmistajista riippumattomilla komponenteilla, mutta joissain tapauksissa valmistajia saattaa olla vain yksi. Turvallisuustekniikkaa myyvät yritykset pyrkivät yhä enemmän kokonaistoimituksiin (valmiita teknisiä ratkaisuja), jolloin kaikki osat voidaan toteuttaa toisiaan vastaavalla luokalla (turvallisuuden tasolla). Tämä epäilemättä vähentää virheiden mahdollisuutta.

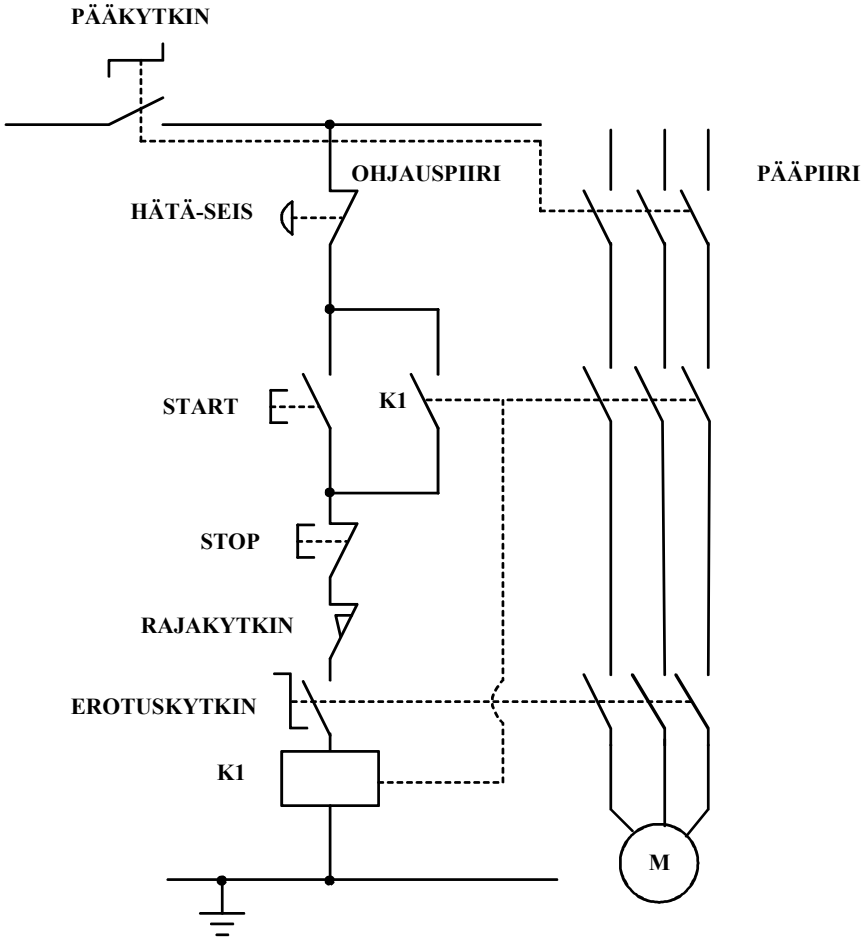
4.1 Esimerkkejä Luokan B ohjausjärjestelmistä



Kuva 10. Luokan B piirit ovat tyypillisesti yksikanavaisia tai joskus kaksikanavaisia (tarvitaan kummankin kanavan toiminta turvafunktion toteuttamiseen), niissä ei ole valvontaa ja niissä yksittäinen vika saattaa aiheuttaa vaaratilanteen.

Luokan B (kuva 10) järjestelmissä ei ole valvontaa, ja vika voi aiheuttaa vaaratilanteen. Tosin niiden käyttökohteet eivät liity turvallisuuteen. Niissä käytetään perustekniikkaa (”state-of-the-art”). Luokan B kaksikanavaisissa järjestelmissä toinen kanava on järjestelmän luotettavuuden parantamista varten. Kaksi kahdesta -järjestelmissä (2 out of 2) yksi pysäytyskäsky ei vielä aiheuta pysäytystä. Luokan B järjestelmät eivät riitä IEC 61508:n mukaisiin turvallisuuden eheystasoihin (SIL).

4.1.1 Esimerkki kytkentäelimien sijainnista (luokka B)



Kuva 11. Esimerkki turvalaitteina käytettävien kytkentäelimien kytkennästä (luokka B).

Toiminnan kuvaus (kuva 11)

- Kytkentä esittää, mitkä käynnistykseen ja pysäytykseen liittyvät komponentit kytketään pääpiiriin ja mitkä ohjauspiiriin.
- Turvatoiminto voidaan menettää vikatilanteessa. Kytkennän komponentteja ei valvota, ja siksi viat eivät paljastu.
- Vaarallinen vika syntyy, jos rele K1 jää vetäneeseen tilaan tai pysäytykseen liittyvän hallintalaitteen koskettimet hitsautuvat kiinni.

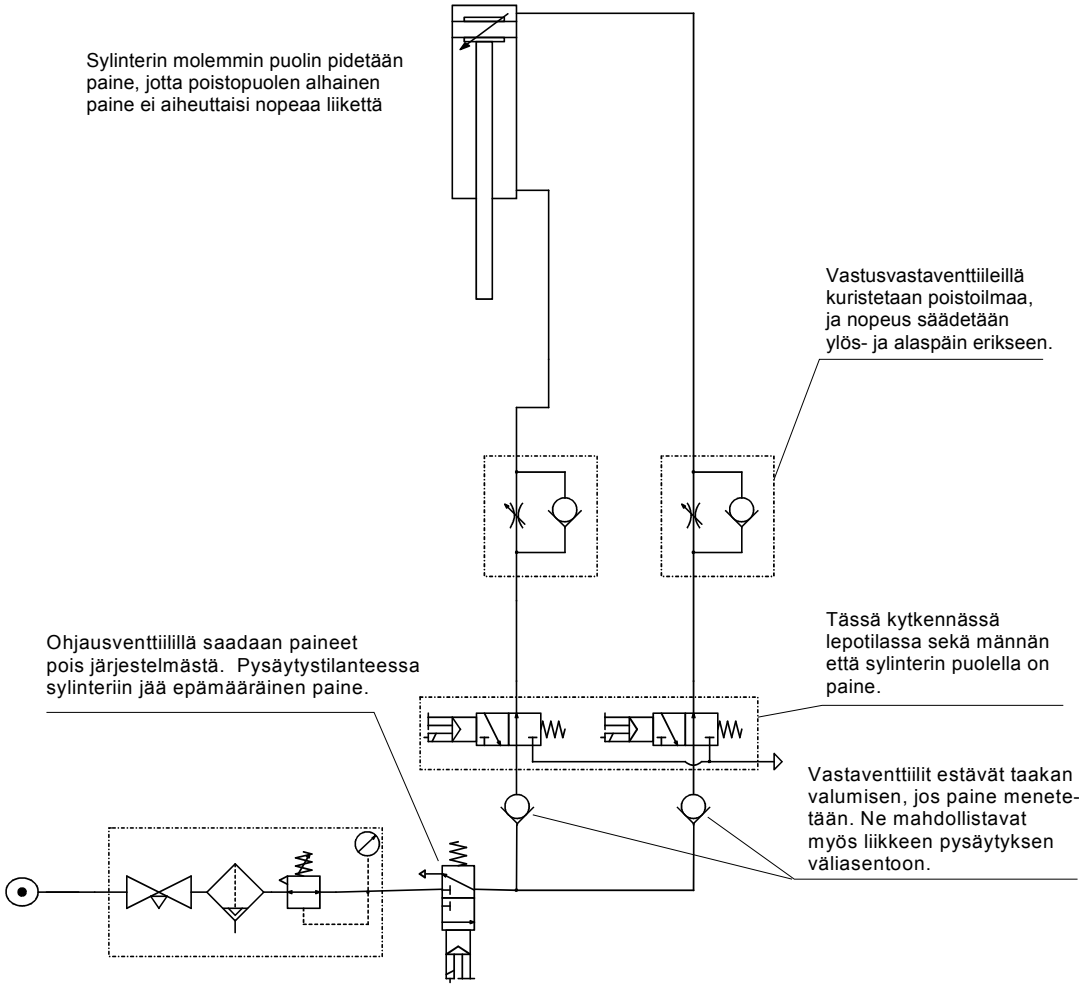
Turvallisen toiminnan edellytykset

- START-painikkeen valvonta on tarpeen monissa sovelluksissa.

Käyttö

- Käyttökohteena ohjaus- ja hätäpysäytyspiirit (pysäytysluokka 0 SFS-EN 60204-1 mukaan).

4.1.2 Ohjaus- ja vastaventtiilin toimintaan perustuva sylinterinohjaus (luokka B)

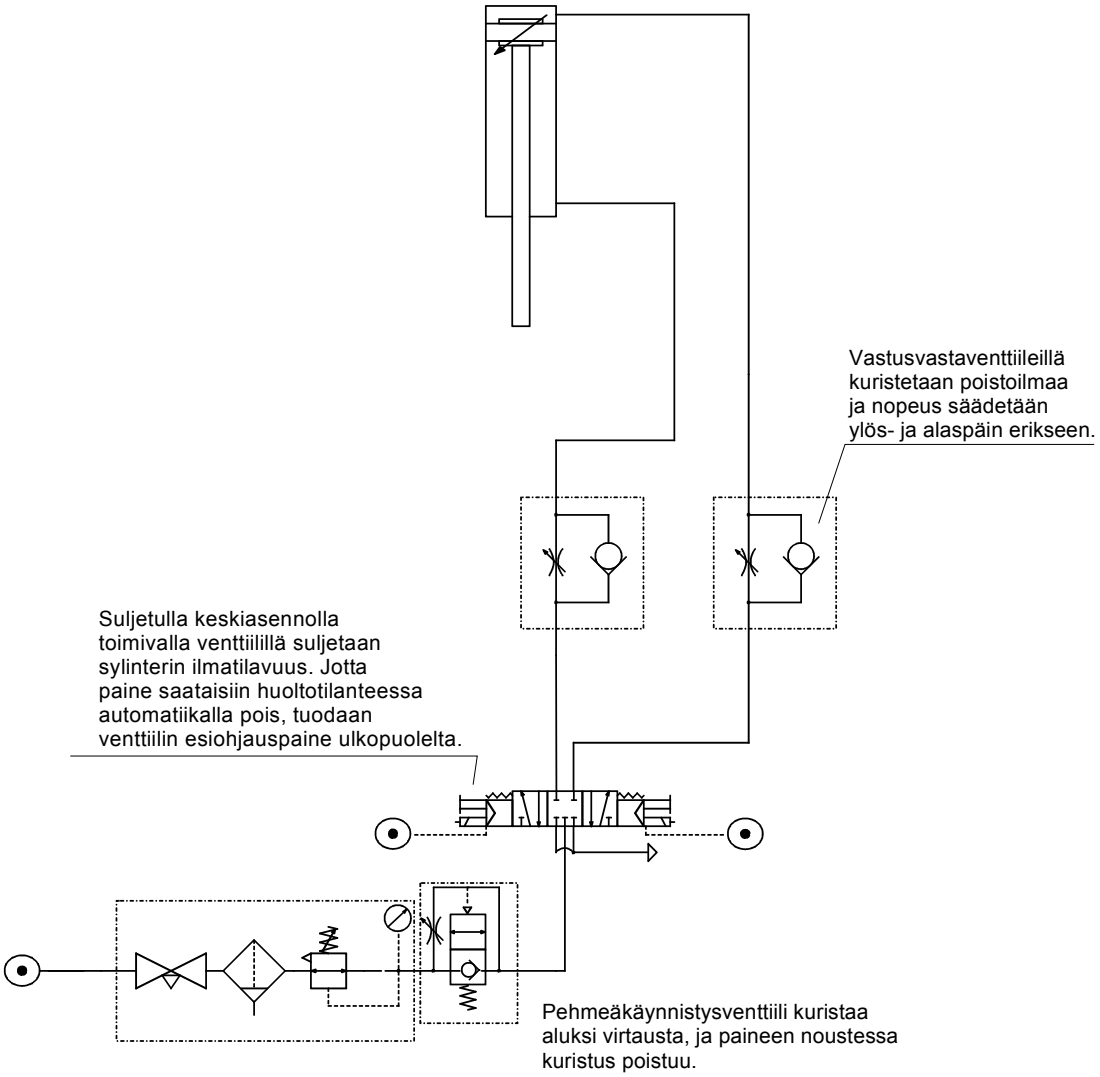


Kuva 12. Paineilmakaavioesimerkki ohjaus- ja vastaventtiilin toimintaan perustuvassa sylinterinohjauksesta (luokka B).

Toiminnan kuvaus (kuva 12)

- Piirissä ilma poistetaan toisella ohjausventtiilillä ja liike saadaan pysäytettyä estämällä ilman poistuminen tai estetään kuvassa alhaalla olevalla ohjausventtiilillä paineen tulo järjestelmään. Jälkimmäisessä tapauksessa pysähtyminen jää hieman epämääräiseksi ja liike voi jatkua päätyyn asti, vaikka siinä ei olekaan normaalia tehoa.
- Piirissä ei ole valvontaa. Vaikka kuvassa alhaalla olevalla ohjausventtiilillä voidaan estää uudet liikkeet, venttiili ei välttämättä pysäytä jo alkanutta liikettä.
- Kuvassa vasemmanpuoleisen vastaventtiilin vika aiheuttaa sylinterin männän varren ajautumisen alas. Jos ohjausventtiili päästää ilmat pois, niin sylinterin kara liikkuu toiseen päätyyn. Letkurikko voi aiheuttaa vaarallisen liikkeen. [Malm & Järvenpää 1998]

4.1.3 Yhdellä ohjausventtiilillä toteutettu sylinterinohjaus (luokka B)



Kuva 13. Paineilmakaavioesimerkki yhdellä ohjausventtiilillä toteutetusta sylinterinohjauksesta (luokka B).

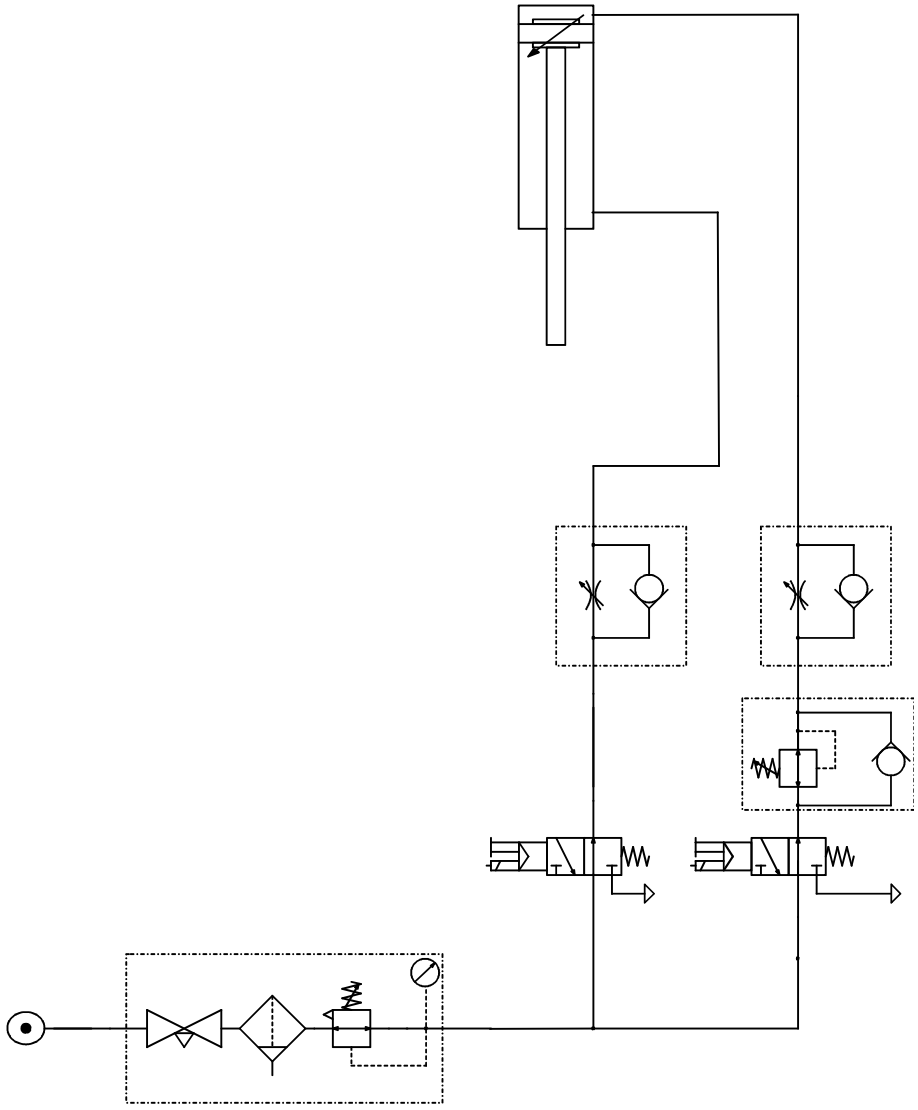
Toiminnan kuvaus (kuva 13)

- Ohjausventtiili pysäyttää liikkeen sulkemalla kummankin puolen ilmatilavuuden. Liike pysähtyy sylinterin puoliskojen saavuttaessa tasapainotilan.
- Piirissä ei ole valvontaa. Letkurikko aiheuttaa vain pienen liikkeen, jos sylinterin toinen puoli jää paineiseksi.
- Ohjausventtiilin vika tai häiriö voi aiheuttaa vaarallisen liikkeen tai estää pysäytyksen.

Turvallisen toiminnan edellytykset

- Pysäytyksen jälkeisessä käynnistyksessä pitää käyttäjän olla varovainen, koska sylinteriin on voinut jäädä alhainen paine, jonka seurauksena liikenopeus voi olla suuri [Malm & Järvenpää 1998].

4.1.4 Painetasapainoon perustuva sylinterinohjaus (luokka B)

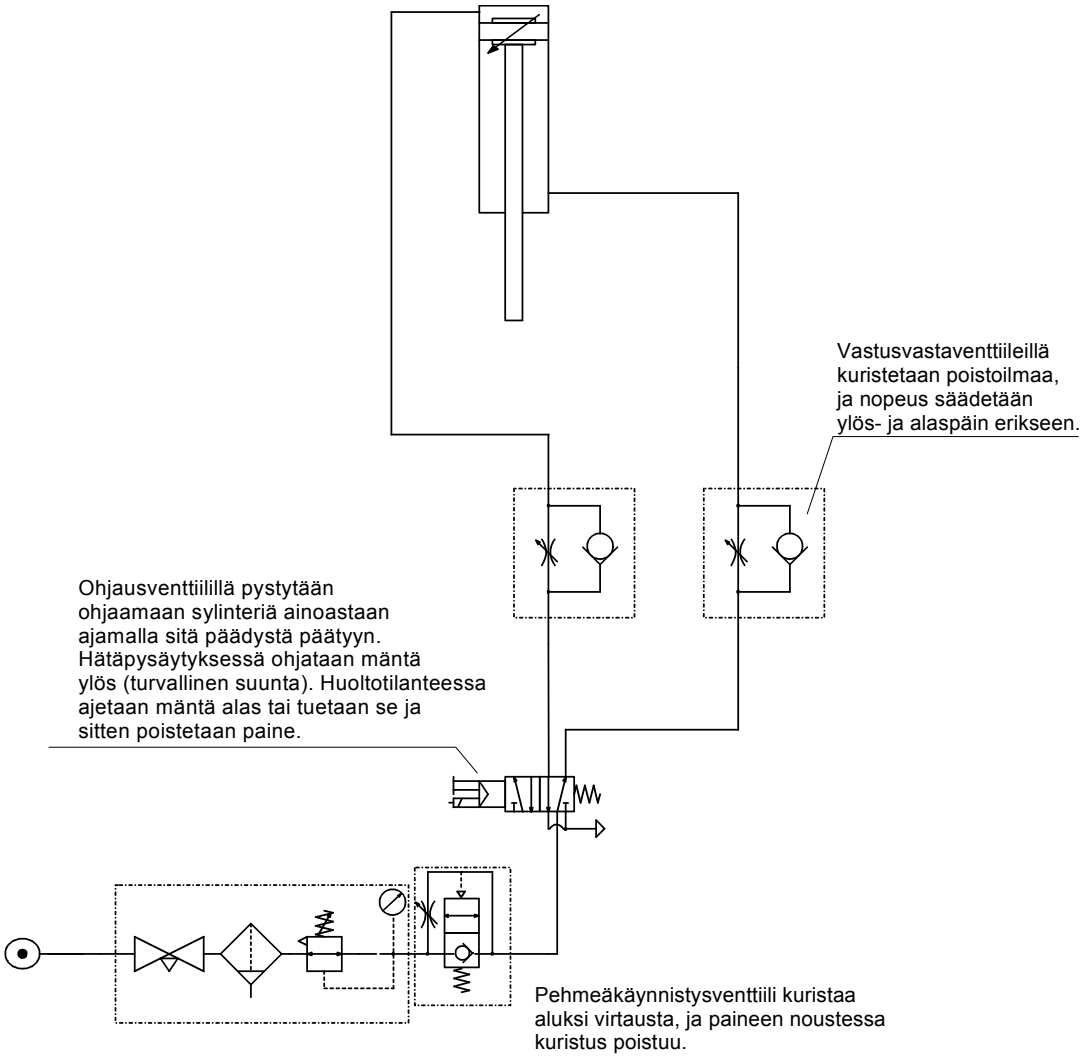


Kuva 14. Paineilmakaavioesimerkki sylinterinohjauksesta, jossa pysäytys perustuu painetasapainoon (luokka B).

Toiminnan kuvaus (kuva 14)

- Sylinterin liike pysäytetään ohjaamalla sylinterin molemmille puolille paine. Pysäytyksen jälkeen sylinteri lähtee liikkeelle hallitusti, koska sylinterin molemmilla puolilla on täysi paine. Pysäytystilanteen jälkeen liike tapahtuu hallitusti, koska sylinterin molemmilla puolilla on käynnistettäessä paine.
- Piirissä ei ole valvontaa.
- Ohjausventtiilin vika voi estää pysäytyksen. Letkurikko aiheuttaa hallitsemattoman liikkeen [Malm & Järvenpää 1998].

4.1.5 Päädystä päätyyn ajo paineilmajärjestelmässä (luokka B)



Kuva 15. Paineilmakaavioesimerkki, jossa sylinteriä voidaan ajaa vain päädystä päätyyn (luokka B).

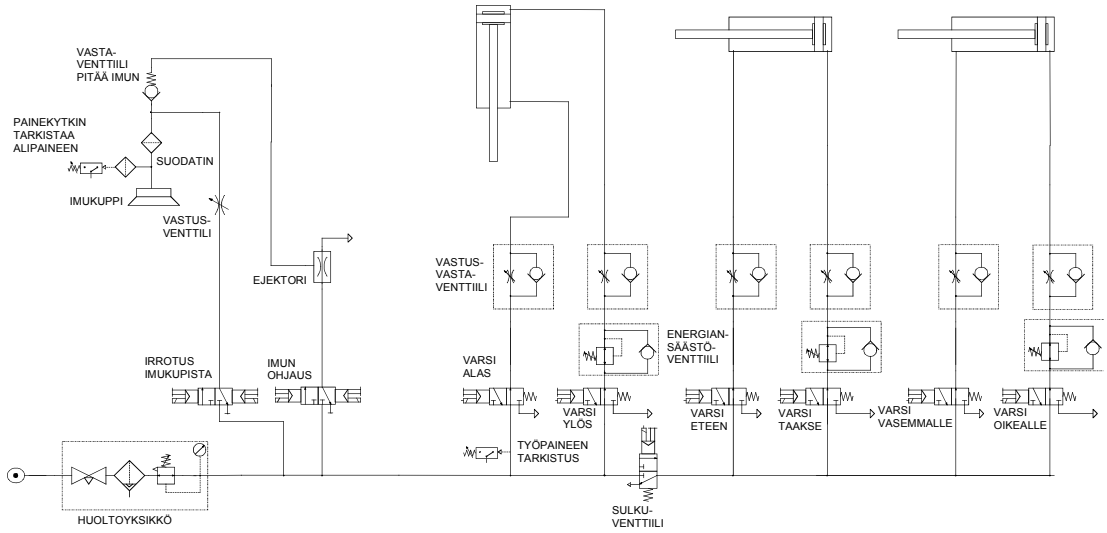
Toiminnan kuvaus (kuva 15)

- Ohjausventtiilillä ei voida pysäyttää liikettä sylinterin päätyasentojen välille, vaan tarvittaessa vaihdetaan liikkeen suuntaa.
- Piirissä ei ole valvontaa.
- Ohjausventtiilin vika tai letkurikko voi aiheuttaa hallitsemattoman liikkeen.

Turvallisen toiminnan edellytykset

- Paluuliikkeen pitää olla vaaraton, koska laitteen pitää olla pysäytettävissä tai liike pitää voida ohjata vaarattomaan suuntaan [Malm & Järvenpää 1998].

4.1.6 Kolmiakselinen tarttujalla varustetuttu pneumaattinen manipulaattori (luokka B)



Kuva 16. Paineilmakaavioesimerkki kolmiakselisesta tarttujalla varustetusta manipulaattorista (luokka B).

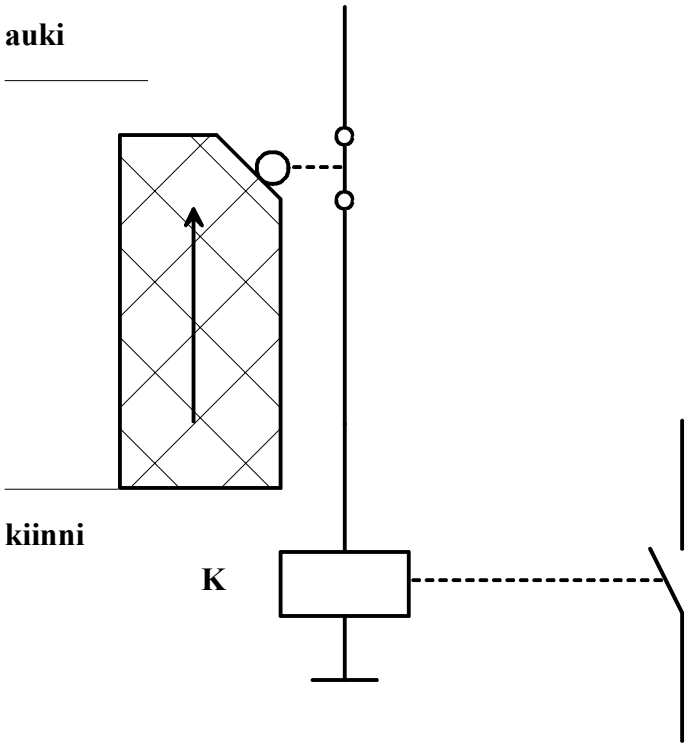
Toiminnan kuvaus (kuva 16)

- Kuvassa esimerkki kolmeakselisesta manipulaattorista, jossa on imukuppitarttuja. Pysäytystilanteessa pysäytetään liikkeet ja tarvittaessa voidaan vaakaliikkeistä poistaa paineet.
- Alhaisesta paineesta saadaan hälytys. Liikkeet estetään, jos paine on liian pieni liikkeiden toteuttamiseen. Huonosta imukupin tartunnasta saadaan hälytys.
- Ohjausventtiilin vika voi aiheuttaa vaaratilanteen [Malm & Järvenpää 1998].

4.2 Esimerkkejä Luokan 1 ohjausjärjestelmistä

Luokan 1 ohjausjärjestelmissä voi yksittäinen vika aiheuttaa vaarallisen vian, mutta vaarallisten vikamuotojen oletetaan olevan hyvin harvinaisia. Vikojen harvinaisuus on saatu aikaan käyttämällä standardissa EN ISO 13849-2 hyvin koeteltuja turvallisuusperiaatteita ja hyvin koeteltuja komponentteja. Taulukko esittää lyhyesti hyvin koeteltuja periaatteita standardin EN ISO 13849-2 sähkökomponenteille. Käytännössä luokan 1 järjestelmissä komponentit on mitoitettava sietämään mm. ylikuormitusta. Luokan 1 järjestelmissä komponentit ovat yleensä mekaanisesti tukevia. Tavallisimpia tämän luokan komponentteja ovat rajakytkimet, releet ja kytkimet. Elektronisia komponentteja ei luokkaan 1 juurikaan hyväksytä. Luokan 1 järjestelmät eivät yleensä liity eheystasoihin, koska luokan 1 tekniikka liittyy tyypillisesti mekaanisiin järjestelmiin, kun taas eheystasojen lähtökohtana ovat yleensä elektroniset järjestelmät.

4.2.1 Rajakytkimellä valvottu portti (luokka 1)



Kuva 17. Esimerkki portista, jonka aukioloa valvotaan rajakytkimellä (luokka 1).

Toiminnan kuvaus (kuva 17)

- Esimerkissä on portti, jonka aukioloa valvotaan rajakytkimellä. Vaaralliset liikkeet tai tilat estetään tai keskeytetään releen K koskettimen kautta, kun portti avataan
- Turvatoiminto voidaan menettää vikatilanteessa. Kytkennän komponentteja ei valvota.
- Viat eivät paljastu ja rajakytkimen mahdollista irtoamista ei havaita
- Vaarallinen vika syntyy, jos rele K jää vetäneeseen tilaan tai sen koskettimet hitsautuvat kiinni.

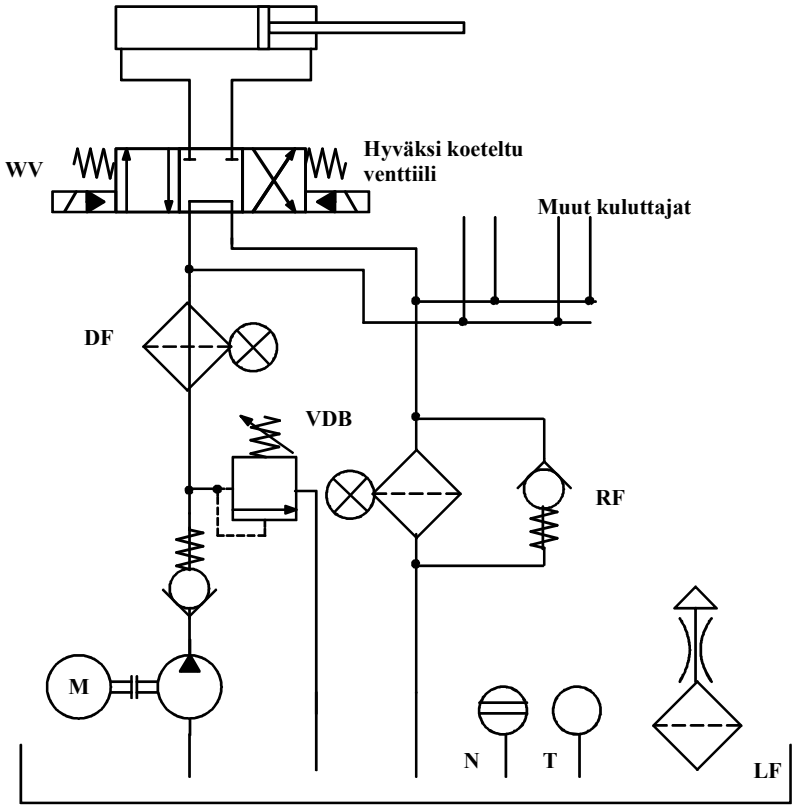
Turvallisen toiminnan edellytykset

- Valitaan hyvin koeteltu pakkotoiminen rajakytkin ja luotettava rele (EN 50205, EN 60947-5-1). Jos käytetyt komponentit ovat tavallisia, niin kytkennällä saavutetaan luokka B.

Käyttö

- Voidaan käyttää kohteissa, joissa vaara-alueelle on tarvetta mennä harvoin ja todennäköisesti vaara voidaan ehkäistä vielä muilla toimenpiteillä. Sovelluskohteina esim. pysäytys- ja ohjauspiirit. [BIA-Report 6/97e, 1997] [Malm et al. 1998]

4.2.2 Hydraulinen sylinterin ohjaus (luokka 1)



Kuva 18.Esimerkki hydraulisesta ohjausjärjestelmästä (luokka 1).

Toiminnan kuvaus (kuva 18)

- Vaarallisia liikkeitä tai tiloja valvotaan yhdellä suuntaventtiilillä WV, joka on hyvin koeteltu (vrt. EN ISO 13849-2 liite C, taulukot C1 ja C2 esittävät turvallisuusperiaatteita).
- Suuntaventtiilin vikaantuminen voi johtaa turvatoiminnon menettämiseen. Vika on riippuvainen suuntaventtiilin luotettavuudesta.
- Hydrauliikkapiirissä ei ole vian tunnistusta.

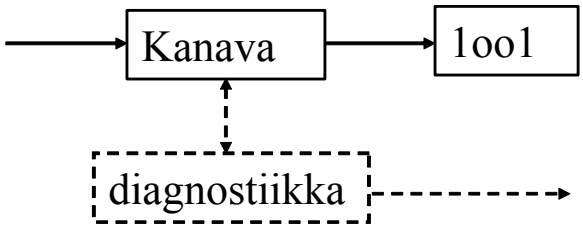
Turvallisen toiminnan edellytykset

- Komponenttien on oltava hyvin koeteltuja standardin EN ISO 13849-2 liitteen C mukaan.

Käyttö

- Piirin käyttökohteita ovat sylinterin ohjauspiirit [BIA-Report 6/97e, 1997].

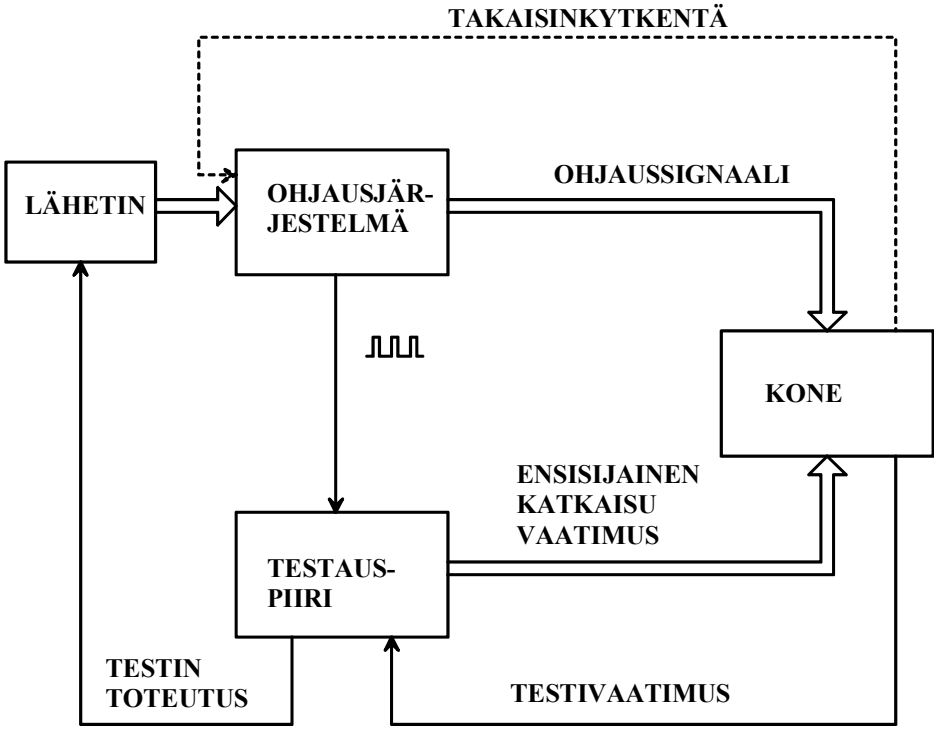
4.3 Esimerkkejä Luokan 2 ohjausjärjestelmistä



Kuva 19. Luokan 2 piirit ovat tyypillisesti yksikanavaisia, mutta niissä on valvontaa.

Luokan 2 (kuva 19) ohjausjärjestelmissä toimintaa valvotaan ainakin jossakin toimintakierron vaiheessa. Piiri ei kuitenkaan ole välttämättä kahdennettu, joten tietynlainen vika esim. lähdössä voi johtaa vaaratilanteeseen. Luokan 2 järjestelmä on helppo toteuttaa elektroniikalla, mutta sähkömekaniikalla, hydrauliikalla ja pneumatiikalla toteutus saattaa olla hankalaa; joskus jopa hankalampaa kuin luokan 3 järjestelmän toteuttaminen. Usein näihin tekniikoihin liittyvä valvonta on järkevää toteuttaa elektroniikalla. Hydrauliikassa ja pneumatiikassa valvontatieto saadaan yleensä karan asennosta, sylinterin asematiedosta tai paineesta. Luokan 2 järjestelmät vastaavat usein turvallisuuden eheystasoa 1 (IEC 61508 mukaan). Tähän voidaan päätyä siitä, että niitä käytetään kohteissa, joissa riskit tai ohjausjärjestelmän riskin vähennys vastaavat toisiaan. Luokan 2 ja eheystason 1 suunnittelu- ja validointiprosessi poikkeavat toisistaan selvästi.

4.3.1 Periaatekuva ohjausjärjestelmästä (luokka 2)



Kuva 20. Esimerkki ohjausjärjestelmästä (luokka 2).

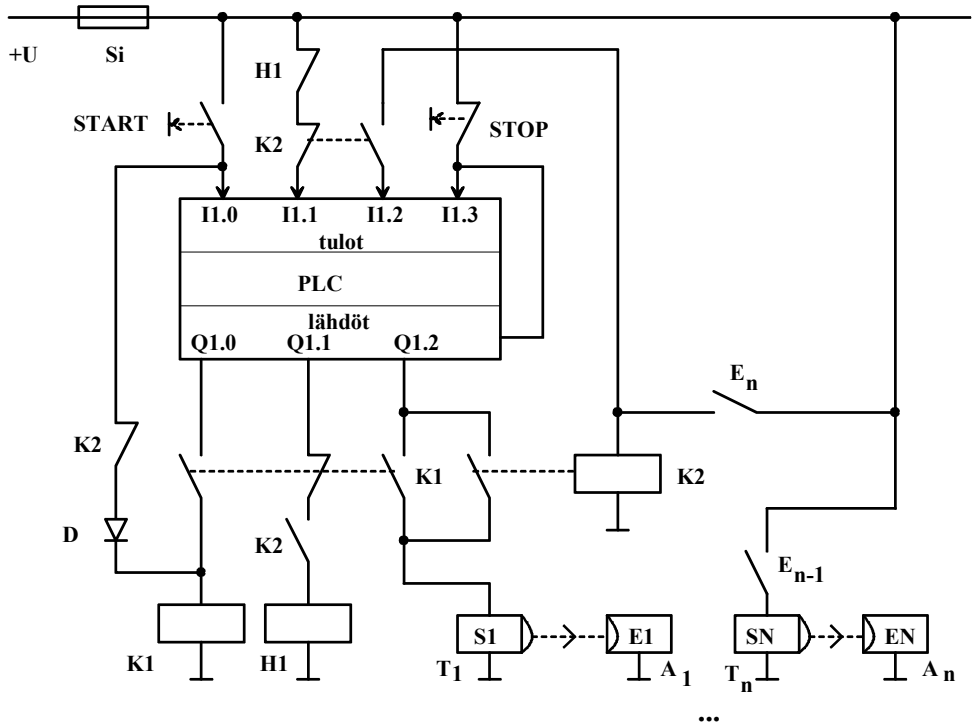
Toiminnan kuvaus (kuva 20)

- Vaarallisia liikkeitä tai tiloja kontrolloidaan lähettimen funktiona.
- Turvatoiminnon testaus tapahtuu joko konetta käynnistettäessä tai tietyin väliajoin. Testin aikana turvatoiminto testataan täydellisesti; vaarallisten liikkeiden pysäytys on estetty testauksen aikana. Testin tai turvatoiminnon tulee säilyä yksittäisen vian tapahtuessa. Turvatoiminnon vikaantuminen havaitaan seuraavan testin yhteydessä.
- Toinen itsenäinen pysäytystie mahdollistaa järjestelmän pysäyttämisen siinäkin tapauksessa, että normaali pysäytystie vikaantuu.
- Testi kattaa lähettimen ja pysäytyspiirin testauksen.

Käyttö

- Käyttökohteena ovat ohjauspiirit [BIA-Report 6/97e, 1997].

4.3.2 Turvavaloverhon ja logiikan kytkentä (luokka 2)



Kuva 21. Esimerkki turvavaloverhokytkennästä, jossa on käytetty ohjelmoitavaa logiikkaa (luokka 2).

Toiminnan kuvaus (kuva 21)

- Vaaralliset liikkeet tai tilat ajetaan alas redundanttisesti PLC:n lähdön Q1.1 ja releen K2 kautta, kun säde katkaistaan valoverhossa S1/E1.
- PLC testaa lähdön Q1.2 kautta valoverhon turvatoiminnon START-komennon antamisen jälkeen ohjelmallisesti sammuttamalla lähettimen ja valvomalla vastaanottimen reaktiota tulojen I1.1 ja I1.2 kautta. Valoverhon vikaantuminen ja virheellinen viiveen paljastuminen on ohjelmiston takana. Testin aikana turvatoiminto on keskeytyksissä.

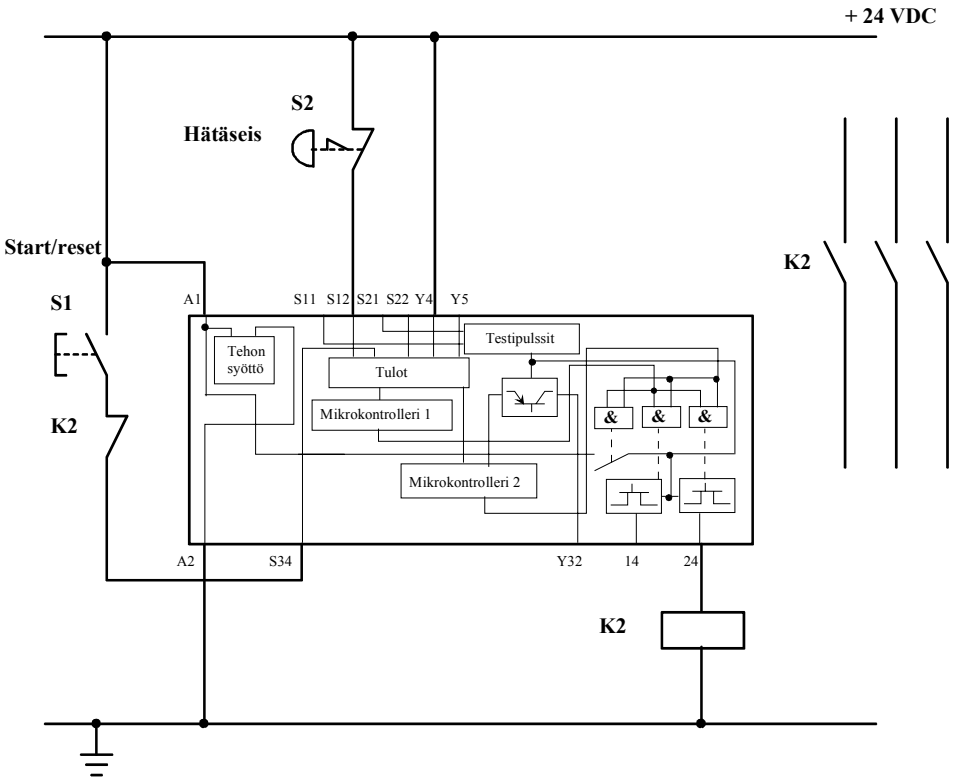
Turvallisen toiminnan edellytykset

- Valoverhojen tulee vastata tavoiteltua luokkaa (EN 61496).
- Releiden K1 ja K2 tulee olla pakkotoimisia.
- Useita lähetin-vastaanotinjärjestelmiä voidaan kytkeä yhteen ja valvoa lisäämällä PLC:n tuloja.

Käyttö

- Käyttökohteena ovat koneen toimintaan kytketyt valoverhopiirit [BIA-Report 6/97e, 1997].

4.3.3 Hätäpysäytyspiiri (luokka 2)



Kuva 22. Esimerkki hätäpysäytyspiiristä, jossa on käytetty hätäpysäytysrelettä (luokka 2).

Toiminnan kuvaus (kuva 22)

- Vaaralliset liikkeet tai tilat pysäytetään hätäpysäytysreleen avulla releen K2 kautta, kun hätäpysätyspiiriin vaikutetaan.
- Releen K2 vikaantumista valvotaan käynnistyksen yhteydessä.
- Hätäpysäytysreleen toimintakuntoa valvotaan sisäisesti.

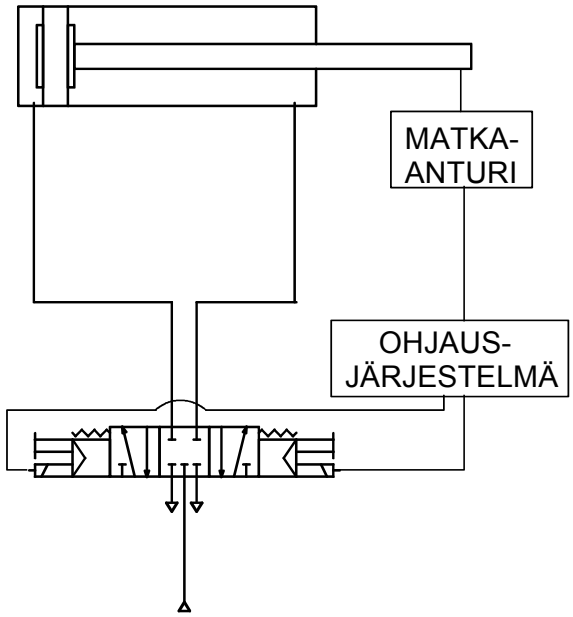
Turvallisen toiminnan edellytykset

- Jos K2 on pakkotoiminen, valvonta on luotettavampi.

Käyttö

- Käyttökohteena ovat hätäpysäytyspiirit [Pilz CD].

4.3.4 Matka-anturilla valvottu paineilmasylinteri (luokka 2)



Kuva 23. Paineilmakaavioesimerkki yhdellä ohjausventtiilillä toteutetusta sylinterin-ohjauksesta, jossa anturi valvoo liikettä (luokka 2).

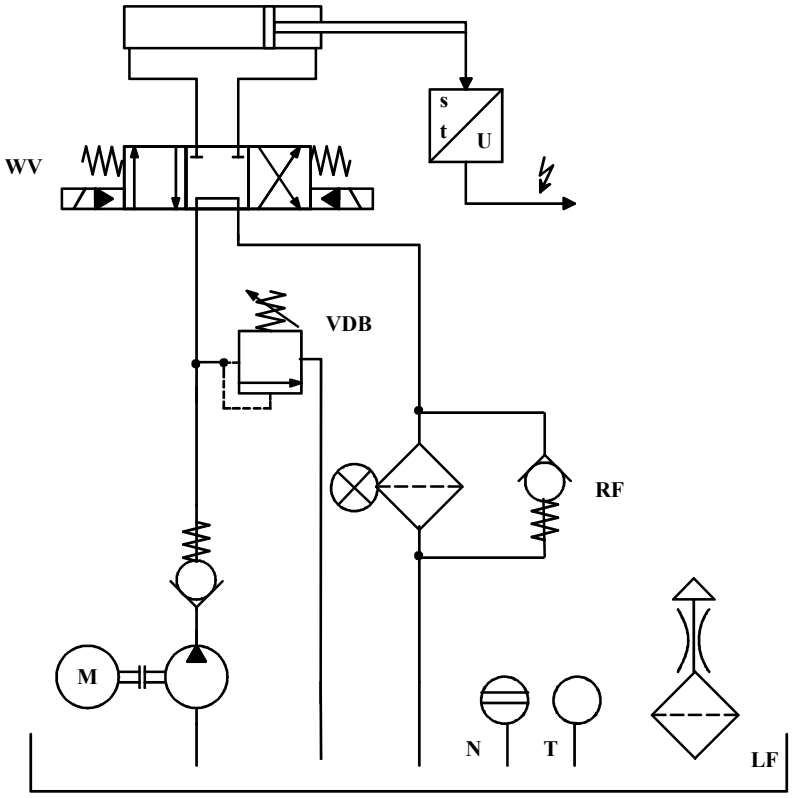
Toiminnan kuvaus (kuva 23)

- Ohjausventtiilillä pysäytetään liike sulkemalla sylinterin ilmatila.
- Toimintaa valvotaan matka-anturilla. Valvonnalla saadaan selville myös sähköohjauksen viat. Jos vika havaitaan, niin liikettä ei voida välttämättä pysäyttää mutta uusi liike voidaan estää.
- Venttiilin vika voi estää pysäytyksen.

Turvallisen toiminnan edellytykset

- Piirin pysäytyksen on oltava mahdollista järjestelmän yhteisellä venttiilillä (ei kuvassa), jolloin havaitun vian seurauksena järjestelmä voidaan pysäyttää.
- Piiriin ei ole piirretty nopeuden säätöä. Myös paineen valvonta voi olla tarpeen. [BIA-Report 6/97e, 1997] [Malm & Järvenpää 1998]

4.3.5 Hydrauliikkasylinterin ohjaus (luokka 2)



Kuva 24. Esimerkki hydraulisesta ohjausjärjestelmästä (luokka 2).

Toiminnan kuvaus (kuva 24)

- Sylinterin liikkeitä ohjataan suuntaventtiilillä WV.
- Suuntaventtiilin toimintaa valvotaan seuraamalla sylinterin liikkeitä. Jos ohjattu liike ei toteudu, saadaan vikailmoitus.

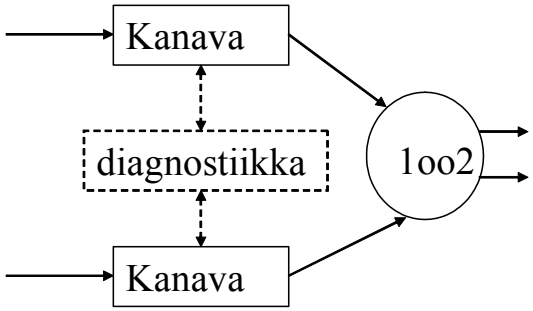
Turvallisen toiminnan edellytykset

- Sähköisen valvonnan tulee ohjata sylinteri pysäytystilaan, jos liike ei toteudu.

Käyttö

- Käyttökohteena ovat hydrauliset ohjauspiirit [BIA-Report 6/97e, 1997].

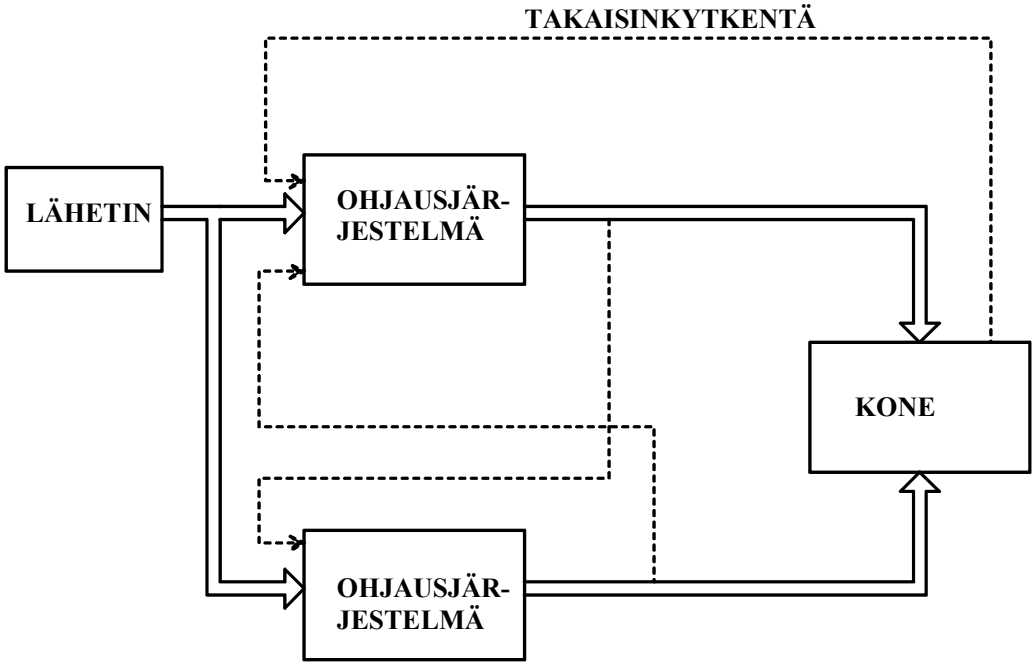
4.4 Esimerkkejä Luokan 3 ohjausjärjestelmistä



Kuva 25. Luokan 3 järjestelmät ovat tyypillisesti kaksikanavaisia ja niissä on jonkun verran vikadiagnostiikkaa.

Luokan 3 (kuva 25) järjestelmissä on lähes aina kaksi kanavaa, koska määritelmän mukaan yksittäinen vika ei saa aiheuttaa vaaraa ja tämän vuoksi ainakin osa järjestelmästä on kahdennettu. Järjestelmissä on tyypillisesti myös jonkun verran valvontaa, mutta aivan kaikki viat eivät välttämättä paljastu. Luokan 3 järjestelmä on selkeä toteuttaa kaikilla tekniikoilla kahdentamalla komponentteja. Luokan 3 järjestelmän suunnittelu ei ole niin vaativaa kuin luokan 4, koska siinä sallitaan piilovikoja, joiden kasautuminen voi johtaa vaaratilanteeseen. Luokan 3 järjestelmän toteuttaminen voi olla selvästi kalliimpaa kuin alempien luokkien toteuttaminen, koska siinä usein kahdennetaan komponentit. Luokan 3 järjestelmiä on kuitenkin mahdollista toteuttaa siten, että kahdennus koskee vain esim. lähtöä. Tällöin pitää varmistaa, että järjestelmän kaikki yksittäiset viat johtavat turvalliseen tilaan tai eivät vaikuta turvallisuuteen. Tämä edellyttää puolestaan suurempaa panostusta suunnitteluun ja validointiin. Luokan 3 järjestelmä vastaa usein turvallisuuden eheystasoa 2 (IEC 61508 mukaan).

4.4.1 Periaatekuva, esimerkki ohjausjärjestelmästä (luokka 3)



Kuva 26. Esimerkki ohjausjärjestelmästä (luokka 3).

Toiminnan kuvaus (kuva 26)

- Vaarallisia liikkeitä tai tiloja ohjataan kahden itsenäisen kanavan (ohjausjärjestelmän) kautta. Kanavat valvovat toisiaan ristiin. Takaisinkytkentä koneelta tulee toiseen kanavaan.
- Ristikkäisvalvonta paljastaa ohjausjärjestelmän lähtöjen viat. Takaisinkytkentä koneelta paljastaa koneen toiminnan vikoja.

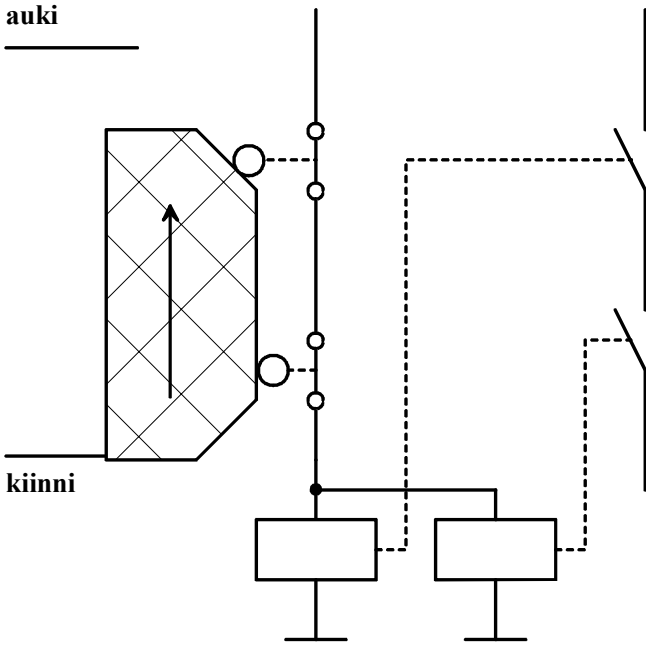
Turvallisen toiminnan edellytykset

- Myös lähettimen ja koneen ohjauspiireissä tarvitaan redundanssia. Kanavien toiminnan erillisyys osaltaan vaikuttaa siihen, että yhden kanavan vika ei vaikuta toiseen. Kun lähetin kytketään molempiin kanaviin, täytyy pitää huolta, että tulot erotetaan (erotusdiodit), jottei yhden kanavan vikaantuminen aiheuttaisi myös toisen vikaantumista. [BIA-Report 6/97e, 1997]

Käyttö

- Käyttökohteena ovat ohjauspiirit.

4.4.2 Rajakytkimillä valvottu portti (luokka 3)



Kuva 27. Esimerkki portista, jonka aukioloa valvotaan rajakytkimillä (luokka 3).

Toiminnan kuvaus (kuva 27)

- Esimerkissä on portti, jonka aukioloa valvotaan rajakytkimillä. Vaaralliset liikkeet tai tilat estetään tai keskeytetään releiden koskettimien kautta, kun portti avataan
- Kytkennässä ei ole valvontaa. Rajakytkimet on asennettu siten, että samanlainen vika (irtoaminen tai ohjainpään rikkoutuminen) molemmissa rajakytkimissä ei aiheuta vaaraa.
- Yksittäisen komponentin vikaantuminen ei aiheuta vaaraa, mutta viat eivät paljastu.
- Vaarallinen vika syntyy, kun molemmat releet jäävät vetäneeseen tilaan tai koskettimet hitsautuvat kiinni.

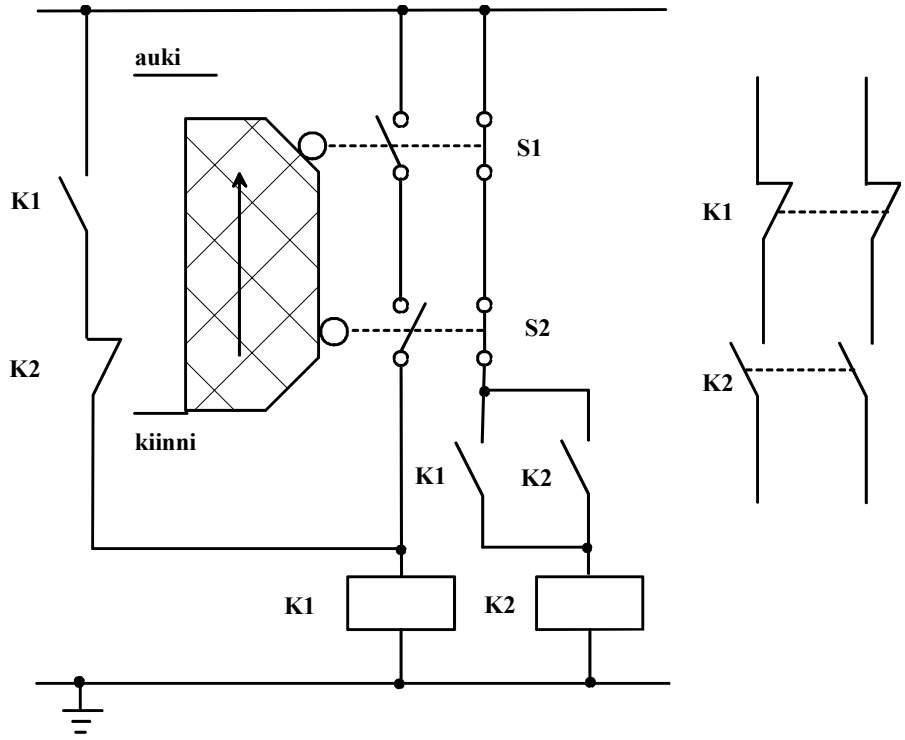
Turvallisen toiminnan edellytykset

- Sovelletaan hyvin koeteltuja turvallisuusperiaatteita. Kuvassa ylempi rajakytkin on pakkotoiminen.

Käyttö

- Sovelluskohteena ovat koneen toimintaan kytketyt suojukset [Malm et al. 1998].

4.4.3 Toinen rajakytkimillä valvottu portti (luokka 3)



Kuva 28. Esimerkki portista, jonka aukioloa valvotaan rajakytkimillä (luokka 3).

Toiminnan kuvaus (kuva 28)

- Esimerkissä on portti, jonka aukioloa valvotaan rajakytkimillä. Vaaralliset liikkeet tai tilat estetään tai keskeytetään avautuvien ja sulkeutuvien koskettimien avulla, kun portti avataan. Piirin toiminta edellyttää alkutestausta, joka tehdään avaamalla ja sitten sulkemalla portti.
- Rajakytkimen siirtyminen paikaltaan havaitaan. Alkutestauksella todetaan, että piiri toimii turvallisesti. Releen K2 vikoja ei piiri havaitse.
- Turvatoiminto säilyy yhden komponentin vikaantuessa.
- Useimmat komponenttiviat havaitaan.

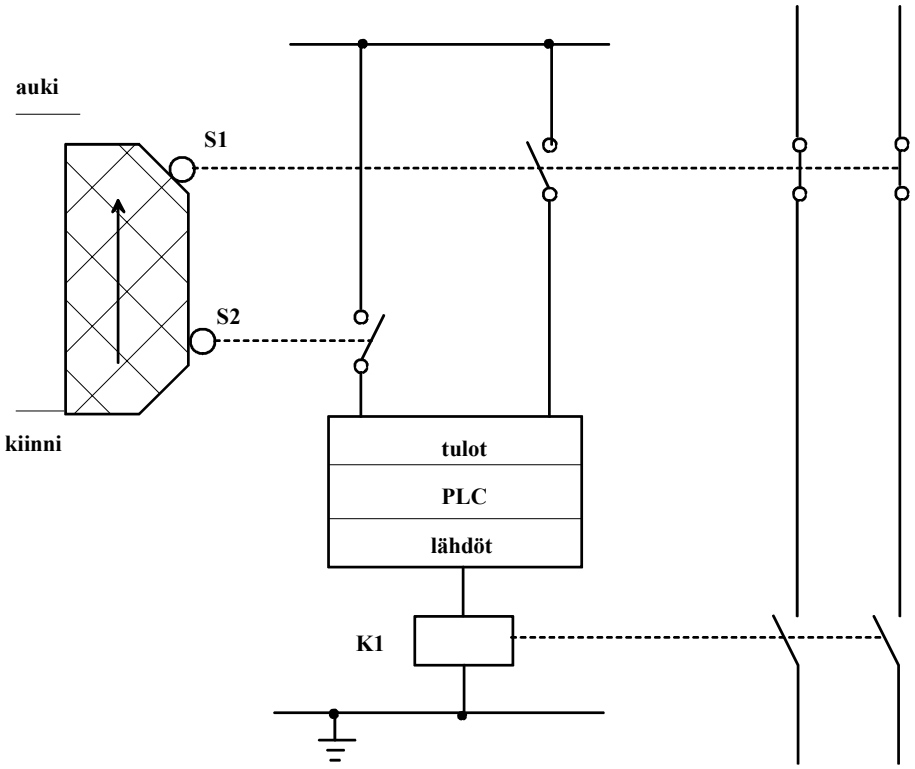
Turvallisen toiminnan edellytykset

- Sovelletaan hyvin koeteltuja turvallisuusperiaatteita. Releiden ja rajakytkimien pakkotoimisuus parantaa turvallisuutta samoin kuin rajakytkimien avautuvien ja sulkeutuvien koskettimien erillisjohdotus. [BIA-Report 6/97e, 1997]

Käyttö

- Sovelluskohteena ovat koneen toimintaan kytketyt suojukset.

4.4.4 Rajakytkimillä ja logiikalla valvottu portti (luokka 3)



Kuva 29. Esimerkki portista, jonka aukioloa valvotaan rajakytkimillä (luokka 3).

Toiminnan kuvaus (kuva 29)

- Esimerkissä on portti, jonka aukioloa valvotaan rajakytkimillä. Vaaralliset liikkeet tai tilat estetään tai keskeytetään avautuvien ja sulkeutuvien koskettimien kautta, kun portti avataan.
- Ohjelmoitava logiikka valvoo rajakytkimien S1 ja S2 vikaantumista ja pysäyttää toiminnot K1:n kautta.
- Turvatoiminto säilyy yhden komponentin vikaantuessa.
- Ohjelmoitavan logiikan ja releen K1 vikoja ei havaita. Vaarallinen vikaantuminen syntyy lisävian, esim. S1:n, vikaantumisen seurauksena.

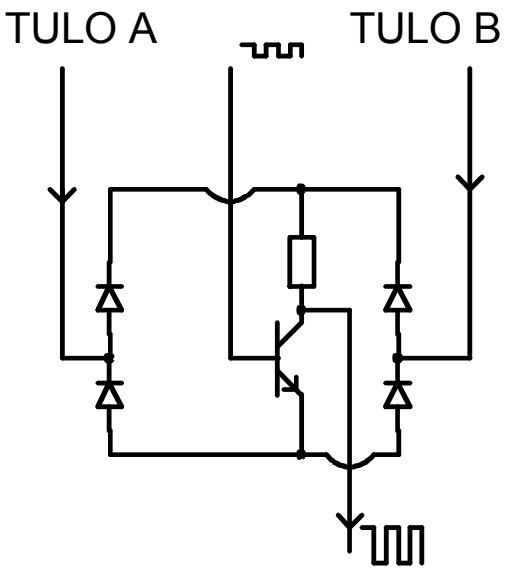
Turvallisen toiminnan edellytykset

- Sovelletaan hyvin koeteltuja turvallisuusperiaatteita. Rajakytkimien pakkotoimisuus parantaa turvallisuutta samoin kuin rajakytkimien avautuvien ja sulkeutuvien koskettimien erillisjohdotus.

Käyttö

- Sovelluskohteena ovat koneen toimintaan kytketyt suojukset [BIA-Report 6/97e, 1997].

4.4.5 Elektroninen erivaiheisuuden valvonta (luokka 3)



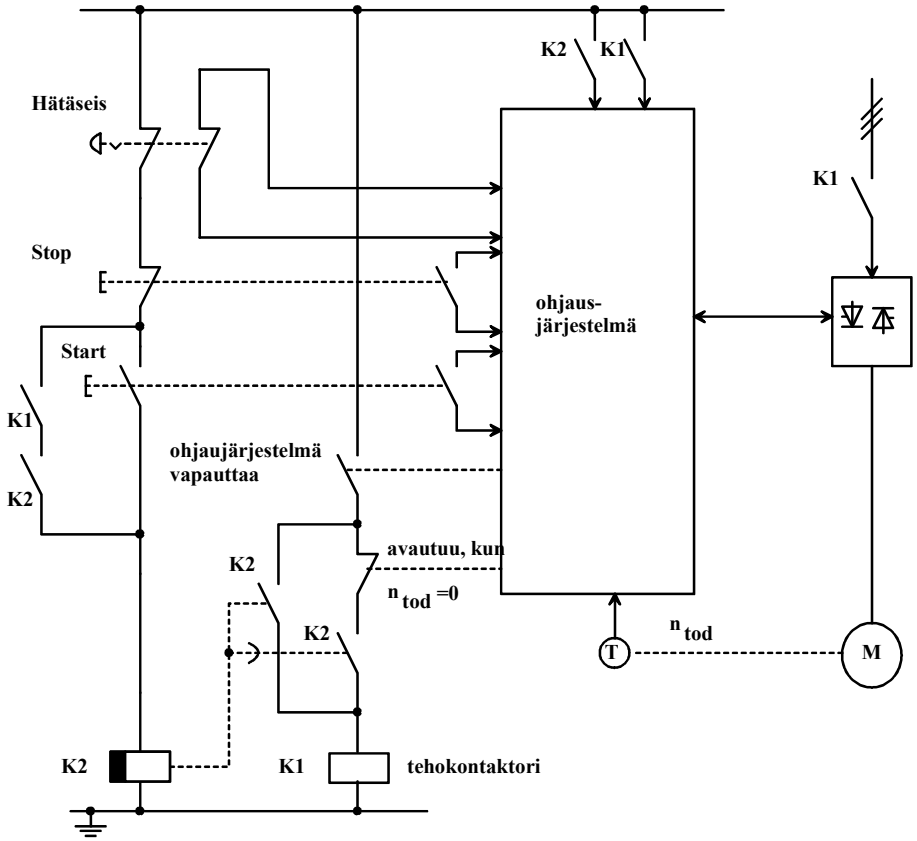
TULO A	TULO B	LÄHTÖ
1	1	⎯⎯
0	1	⎍⎍
1	0	⎍⎍
0	0	⎯⎯

Kuva 30. Esimerkki kahden tulon erivaiheisuuden valvonnasta. Oikealla on kuva siitä, miten lähtö muuttuu tulojen tilan vaihtuessa. (Luokka 3).

Toiminnan kuvaus (kuva 30)

- Esimerkissä valvotaan sitä, että kaksi tuloa ovat aina eri tilassa. Jos tulot ovat samassa tilassa tai komponentti vikaantuu, pulssitus vaimenee. Tällä periaatteella on transistori saatu melko korkeaan luokkaan ilman varsinaista kahdennusta.
- Piiri valvoo omaa toimintaansa ja paljastaa useimmat yksittäiset viat. Diodien oikosulut aiheuttavat tulopiirien oikosulun, joka voi paljastua tulojen ollessa eri vaiheissa (esim. sulake palaa) tai vialla ei ole välitöntä vaikutusta turvallisuuteen. Useimmat transistorin viat johtavat pulssituksen vaimenemiseen. Transistorin kanta-kollektorioikosulussa pulssitus voi päästä piirin läpi vaimentuneena.

4.4.6 Moottorin nopeuden hallintapiirin käyttö hätäpysäytyksessä



Kuva 31. Esimerkki hätäpysäytyspiiristä, jossa käyttökoneistoa jarrutetaan energian takaisinkytkennällä (luokka 3).

Toiminnan kuvaus (kuva 31)

- Käyttökoneistoa jarrutetaan energian takaisinkytkennällä, kun hätäpysäytyspiiriin vaikutetaan. Tehokontaktorin K1 täytyy jäädä vetäneeseen tilaan, kunnes käyttökoneisto on pysähtynyt. Kun n_{tod} on nolla, muunnin antaa tehokontaktorille käskyn päästää. Jos katkaisua ei tapahdu edellä kuvatun mukaan, katkaisu tapahtuu normaalin jarrutusajan jälkeen viivästetysti K2:n kautta.
- Riippuen viasta käyttökoneistoa ei jarruteta mutta tehot katkaistaan viiveen kuluttua K2:n ja K1:n kautta tai vaihtoehtoisesti tehoja ei katkaista jarrutuksen jälkeen. Tehonsyötön katkaisee siis viasta riippuen joko kontaktori K1 tai ohjausjärjestelmä.

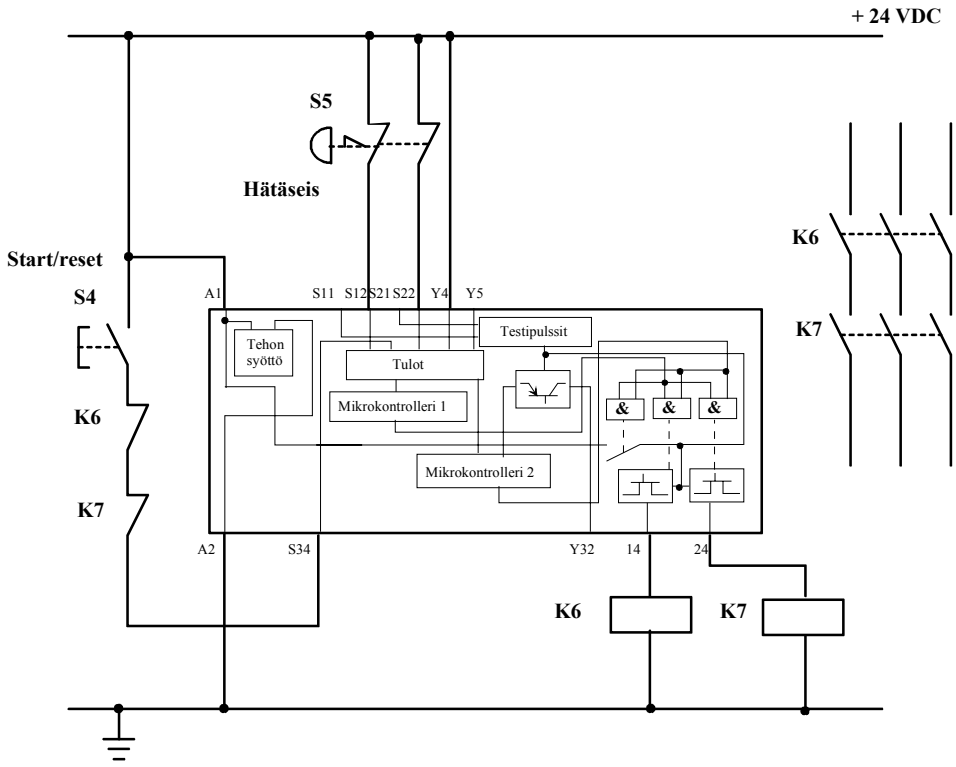
Turvallisen toiminnan edellytykset

- Kontaktoreiden tulee olla pakkotoimisia, jotta niiden valvonta toteutuisi.

Käyttö

- Käyttökohteena ovat moottorin ohjauspiirit [BIA-Report 6/97e, 1997].

4.4.7 Hätäpysäytyspiiri (luokka 3)



Kuva 32. Esimerkki hätäpysäytyspiiristä, jossa käytetään kuvassa keskellä olevaa hätäpysäytysrelettä (luokka 3).

Toiminnan kuvaus (kuva 32)

- Vaaralliset liikkeet tai tilat pysäytetään hätäpysäytysreleen avulla releiden K6 ja K7 kautta, kun hätäpysätyspiiriin vaikutetaan. Käynnistyksen yhteydessä valvotaan releitä K6 ja K7.
- Yhden komponentin vikaantuminen ei aiheuta turvatoiminnon menetystä.
- Hätäpysäytyksen tulopiirejä ei valvota. Hätäseispainikkeen jännitteen ja tulojen välinen oikosulku aiheuttaa turvatoiminnon menetyksen.
- Hätäpysäytysreleellä on oma sisäinen valvonta (luokka 4).

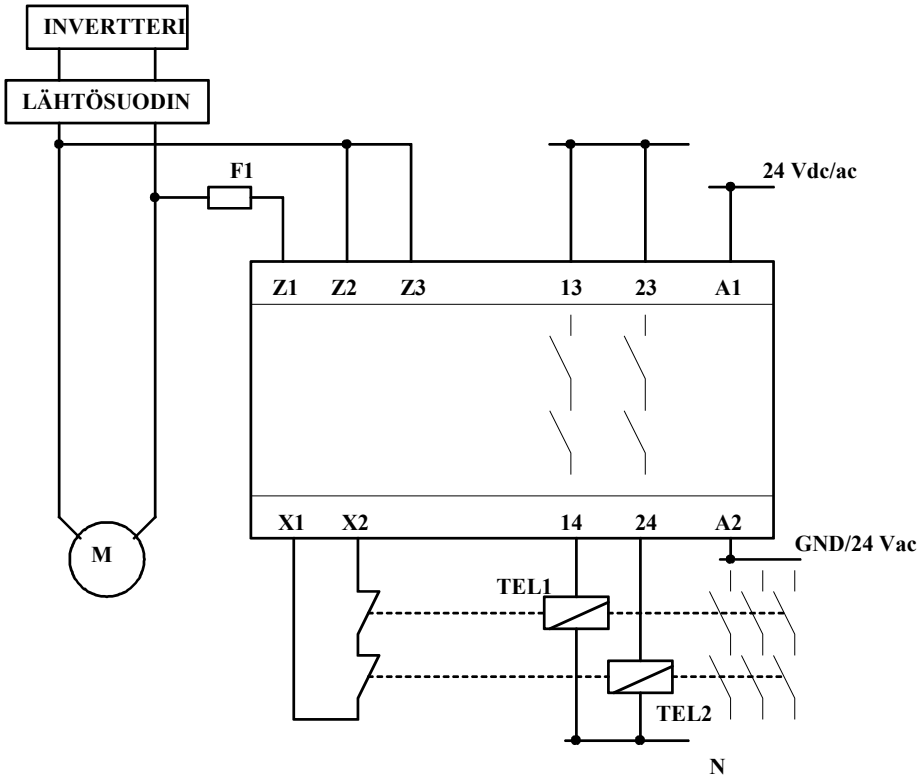
Turvallisen toiminnan edellytykset

- Valvonnan luotettavuus paranee, jos releet K6 ja K7 ovat pakkotoimisia. Jos lisäksi tulopiirien oikosulun mahdollisuus voidaan eliminoida (riittävät etäisyydet ja erilliset kaapelit), voi piirikokonaisuuden luokka kasvaa.

Käyttö

- Käyttökohteena ovat hätäpysäytyspiirit [Pilz CD].

4.4.8 Pysäytyksen valvontapiiri (luokka 3)



Kuva 33. Esimerkki pysähdyksen valvonnasta (luokka 3).

Toiminnan kuvaus (kuva 33)

- Piiri valvoo sitä, että moottorilla ei ole jännitettä. Piirin lähdöillä ohjataan relettä, jolla voidaan esim. katkaista jännite.
- Piirin sisäinen valvonta valvoo itseään ja ohjaavia releitä.

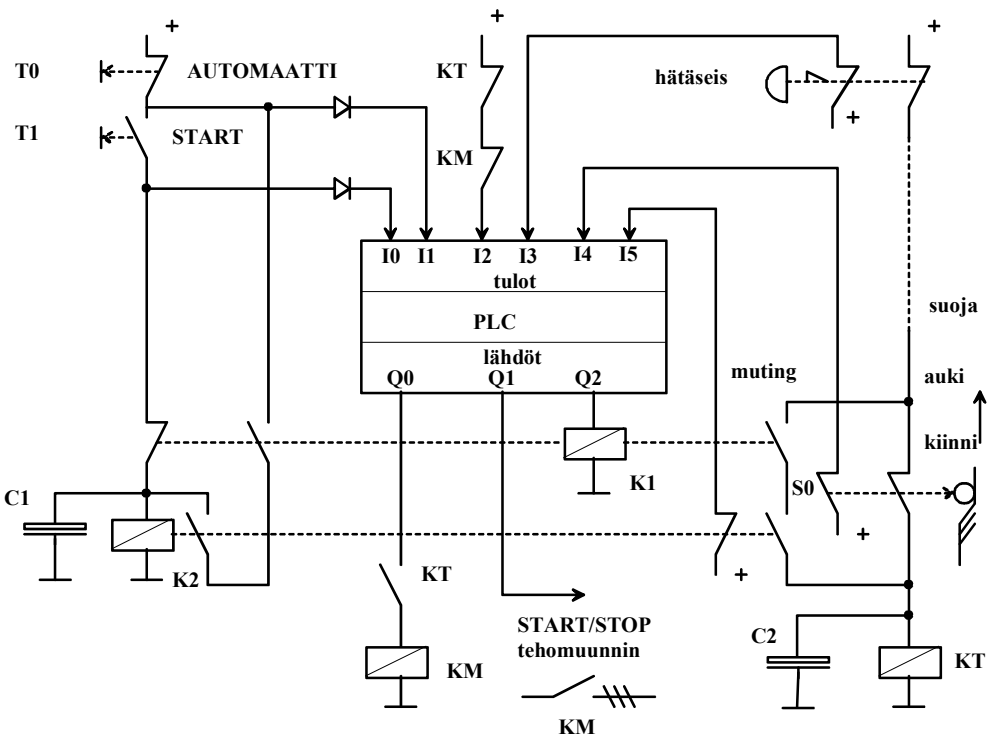
Turvallisen toiminnan edellytykset

- Releiden valvontaa parantaa se, että ne ovat pakkotoimisia.

Käyttö

- Piirin käyttökohteena ovat mm. moottorin ohjauksen valvontapiirit [Carlo Gavazzi -esite].

4.4.9 Logiikalla toteutettu turvalaitteen passivointi (luokka 3)



Kuva 34. Esimerkkipiirissä suojuksen avauksen aiheuttama komento passivoidaan ohjelmoitavalla logiikalla (luokka 3).

Toiminnan kuvaus (kuva 34)

- Vaaralliset liikkeet tai tilat estetään tai keskeytetään ohjelmoitavan logiikan ja erillisen elektroniikan avulla, kun suoja avataan tai painetaan hätäpysäytyspainiketta. Pakkotoimisen rajakytkimen S0 koskettimet avautuvat ja rele KT päästää viiveen kuluttua. Kun KT päästää, myös päärele KM päästää ja tehonsyöttö käyttökoneistolle keskeytyy. Rajakytkimen S0 mykistäminen aiheuttaa releen K2 päästämisen. Tämä on toteutettu redundanttisesti PLC:n avulla releen K1 kautta ja toisaalta PLC:stä riippumatta K2:n kautta.
- Ohjelmoitavan logiikan ohjelmisto valvoo releiden K1, K2, KT ja KM vikaantumista.

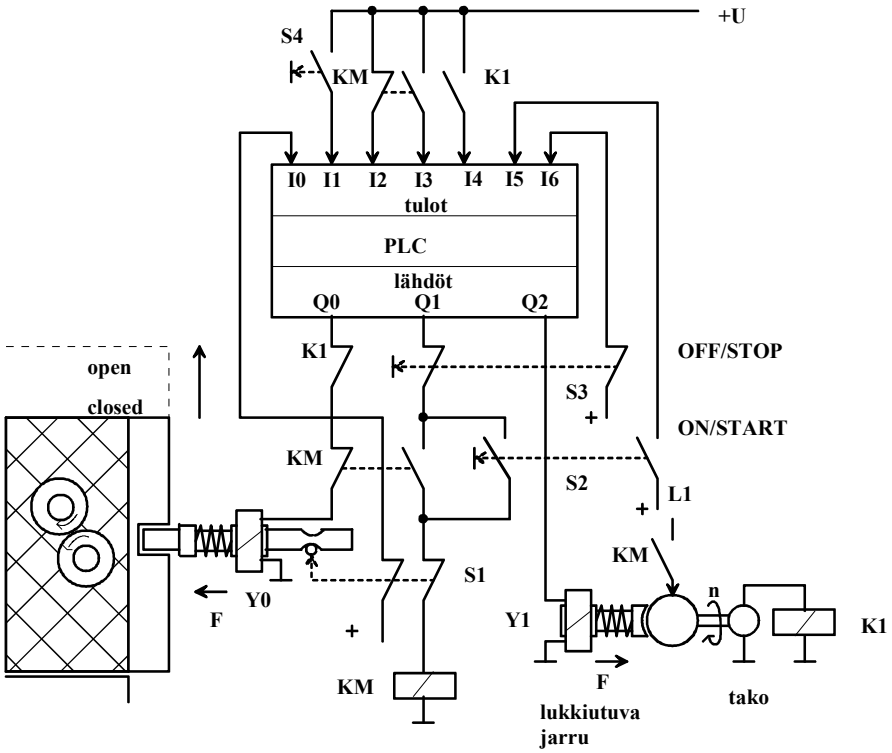
Turvallisen toiminnan edellytykset

- Rajakytkimen S0 tulee olla pakkotoiminen.
- Releiden K1, K2, KT ja KM tulee olla pakkotoimisia.

Käyttö

- Käyttökohteena ovat koneen toimintatilan ohjaus- ja passivointipiirit [BIA-Report 6/97e, 1997].

4.4.10 Logiikalla toteutettu suojan lukituksen valvonta (luokka 3)



Kuva 35. Suojan lukituksen valvonta käyttäen ohjelmoitavaa logiikkaa (luokka 3).

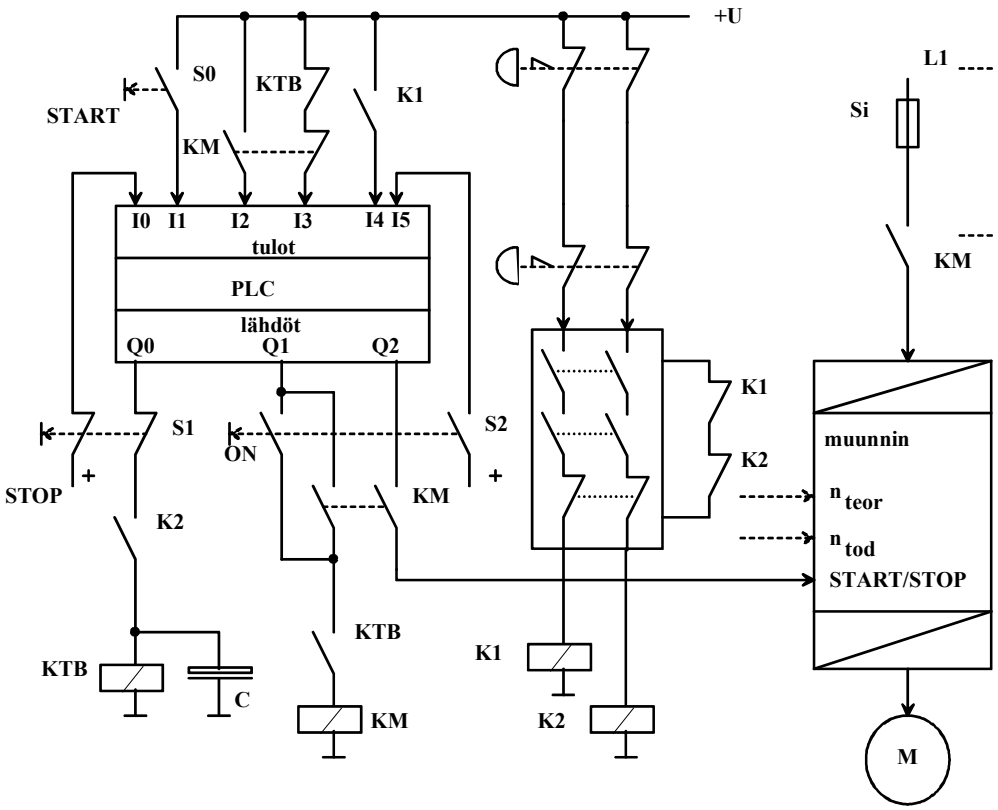
Toiminnan kuvaus (kuva 35)

- Suojan tulee olla kiinni, jotta vaarallinen kone voidaan käynnistää. Suoja avataan vetämällä salpa taakse, kun avausmagneetti on jännitteellinen. Kun START-kytkimeen vaikutetaan, PLC aktivoi ensin lähdön Q2, joka vapauttaa jarrun, sitten moottorikontaktori KM liipaistaan asettamalla lähtö Q1. Kun KM vetää, S2 voidaan vapauttaa. Kun STOP-käsky annetaan aktivoimalla kytkin S3, moottorikontaktori päästää. Tulon 12 kautta alkaa ennalta asetettu jarrutusperiodi PLC:n käyttäjäohjelmistossa, jonka jälkeen kela Y1 kytketään pois lähdön Q2 kautta.
- Lukituspultin asentoa valvoo pakkotoiminen rajakytkin S1, josta tieto välittyy edelleen PLC:lle. Toinen avautuva kosketin vaikuttaa moottorin kontaktoriin KM, jonka sekä avautuva että sulkeutuva kosketin on kytketty PLC:lle.
- PLC:n vikaantuessa suojaa ei voi avata, koska lukitusmekanismin avaamiseksi tarvittavaa virtaa ei ole K1:n ollessa jännitteellinen. Yksittäinen vika lukitusmekanismissa havaitaan – kuten takogeneraattorin ja K1:n tai moottorikontaktorin vika – testeillä ja aika-asetuksilla PLC:n käyttäjäohjelmistossa, ja seurauksena suoja lukitaan tai vaaralliset liikkeet lopetetaan.

Turvallisen toiminnan edellytykset ja käyttö

- Rajakytkimen S1 samoin kuin releiden K1 ja KM tulee olla pakkotoimisia [BIA-Report 6/97e, 1997].

4.4.11 Logiikalla toteutettu koneiston ohjaus (luokka 3)



Kuva 36. Esimerkki ohjelmoitavalla logiikalla toteutetusta käyttökoneiston ohjauksesta pysäytysluokan 1 mukaisesti (luokka 3).

Toiminnan kuvaus (kuva 36)

- Hätäpysäytyksessä K1 ja K2 päästävät välittömästi, logiikka saa tiedon K1-koskettimelta ja antaa edelleen pysäytys- tai jarrutuskäskyn muuntimelle. Rele KTB päästää viiveellä, minkä jälkeen rele KM katkaisee moottorilta virran.
- Releen KM vika johtaa siihen, että moottorilta ei katkaista jännitettä, vaikka pysäytys toimiikin. Logiikka havaitsee vian ja antaa hälytyksen. Muiden releiden viat havaitaan ennen vikojen vaikutusta. Logiikan lähdön Q2 vika johtaa siihen, että jarrutus ei toimi, vaikka jännite katkeaa oikein.

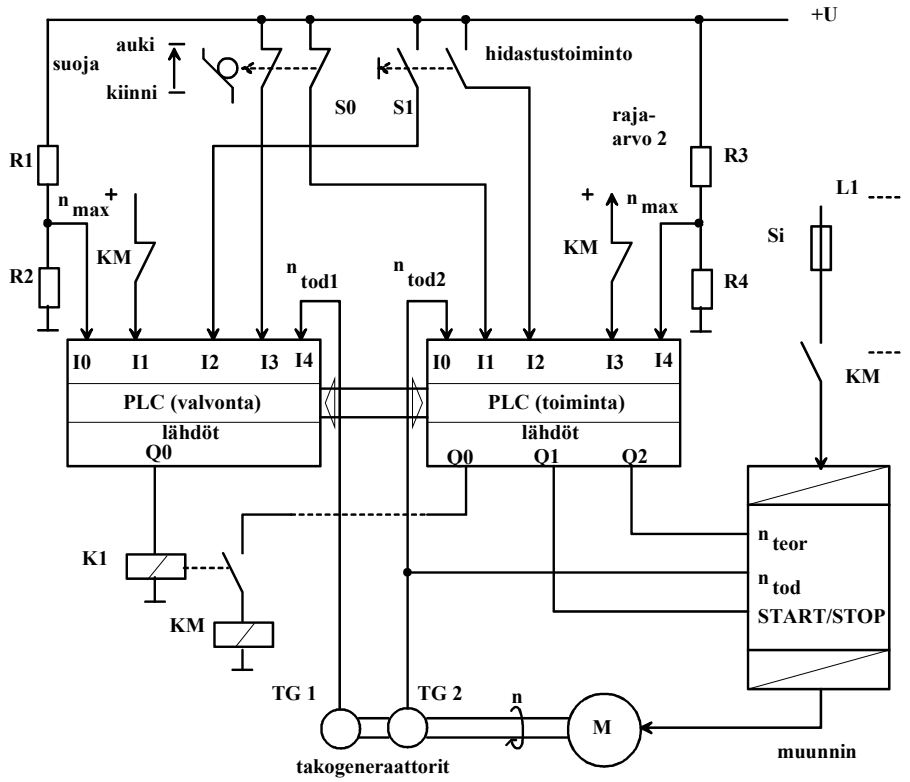
Turvallisen toiminnan edellytykset

- Releiden KTB ja KM tulee olla pakkotoimisia.

Käyttö

- Käyttökohteena ovat moottorin ohjauspiirit [BIA-Report 6/97e, 1997].

4.4.12 Kahdennettu logiikka ohjaamassa ja valvomassa koneistoa (luokka 3)



Kuva 37. Esimerkki ei-toiminnallisesta ohjelmoitavan logiikan redundanssista (luokka 3).

Toiminnan kuvaus (kuva 37)

- Toiminnasta vastaava logiikka antaa jarrutuskomennon ja katkaisee jännitteet viiveellä releen KM kautta. Logiikka valvoo nopeuden toteutumista takogeneraattorilla TG2.
- Valvontalogiikka toteaa nopeuden sekä oikeat komennot ja vikatilanteessa katkaisee jännitteen releiden K1 ja KM avulla. Molemmilla logiikoilla on oma maksiminopeuden asetusarvo.
- Valvontalogiikkaa valvotaan vain suppeasti. Jos valvontalogiikka vikaantuu ensin, vaarallinen vika voi syntyä toimintalogiikan vikaantuessa. Valvontalogiikan turvatoiminto täytyy tarkistaa tietyin testi- ja kunnossapitovälein, kun järjestelmä on pysähdyksissä.

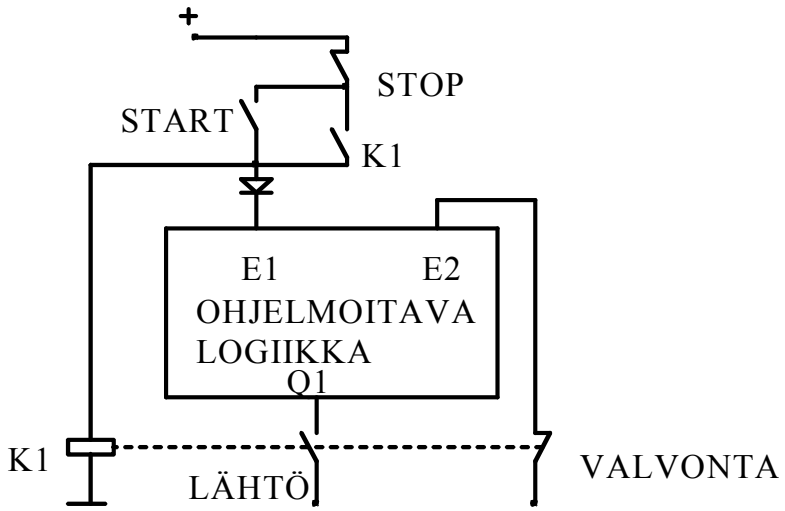
Turvallisen toiminnan edellytykset

- Releen KM tulee olla pakkotoiminen.

Käyttö

- Käyttökohteena ovat moottorin ohjauspiirit [BIA-Report 6/97e, 1997].

4.4.13 Redundanssi käyttäen logiikkaa ja relettä (luokka 3)



Kuva 38. Esimerkki logiikan ja releen käytöstä varmistamassa toistensa toimintakuntoa (luokka 3).

Toiminnan kuvaus (kuva 38)

- Esimerkissä on lähtöä ohjaamassa logiikka ja rele. Logiikka valvoo releen toimintakuntoa.
- Logiikka valvoo releen kosketinta. Rele K1 antaa tulolle itsepidon. Logiikan vikoja ei valvota.

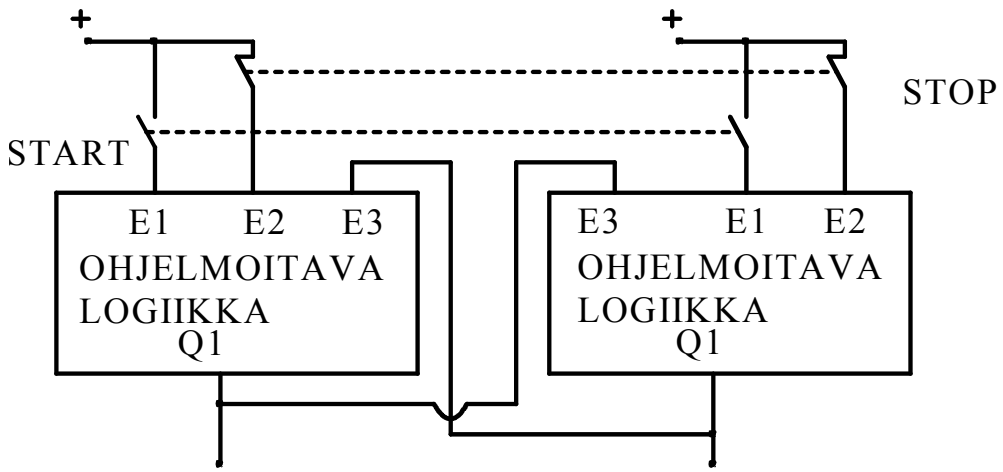
Turvallisen toiminnan edellytykset

- Releen valvonta edellyttää pakkotoimista relettä. Releen valvonta ei toimi, jos ohjausta käytetään erittäin harvoin.

Käyttö

- Käyttökohteena ovat ohjauspiirit [Kleinbreuer 1997].

4.4.14 Redundanssi käyttäen kahta logiikkaa (luokka 3)



Kuva 39. Esimerkissä logiikat valvovat toinen toisiaan (luokka 3).

Toiminnan kuvaus (kuva 39)

- Esimerkissä kaksi logiikkaa ovat varmistamassa toistensa toimintakuntoa. Logiikoissa on sama sovellusohjelma. Yhden logiikan lähdön vikaantuminen havaitaan toisella logiikalla.
- Kummankin logiikan tulot ja lähdöt sekä käynnistys ja pysäytyskoskettimet tulevat valvotuiksi käytön aikana. Logiikkojen sisäisiä vikoja ei valvota.

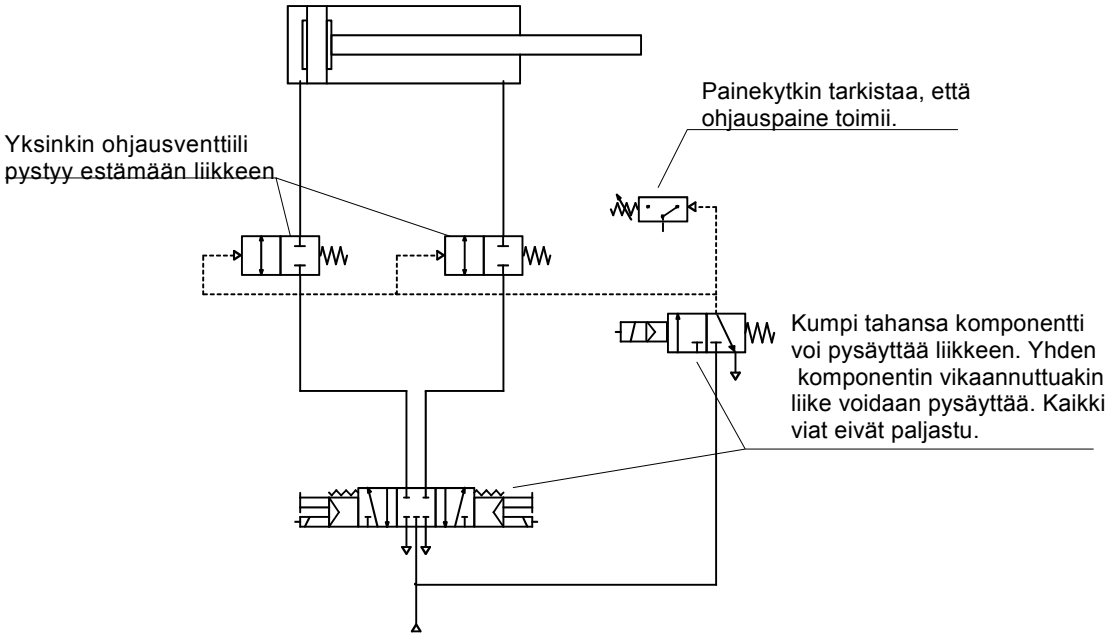
Turvallisen toiminnan edellytykset

- Turvallisuutta on mahdollista parantaa käyttämällä eri logiikkamalleja ja ohjelmia (diversiteetti). Diversiteetti pienentäisi logiikkoihin tulevien samanlaisten vikojen mahdollisuutta.

Käyttö

- Käyttökohteena ovat ohjauspiirit.
- Valvonta edellyttää lähtöjen ja tulojen jatkuvaa käyttöä [Kleinbreuer 1997].

4.4.15 Paineilmasylinterin pysäytys sulkemalla ilmatila (luokka 3)



Kuva 40. Paineilmakaavioesimerkki ilmatilavuuden sulkemiseen perustuvalla pysäytyksellä toteutetusta sylinterinohjauksesta (luokka 3).

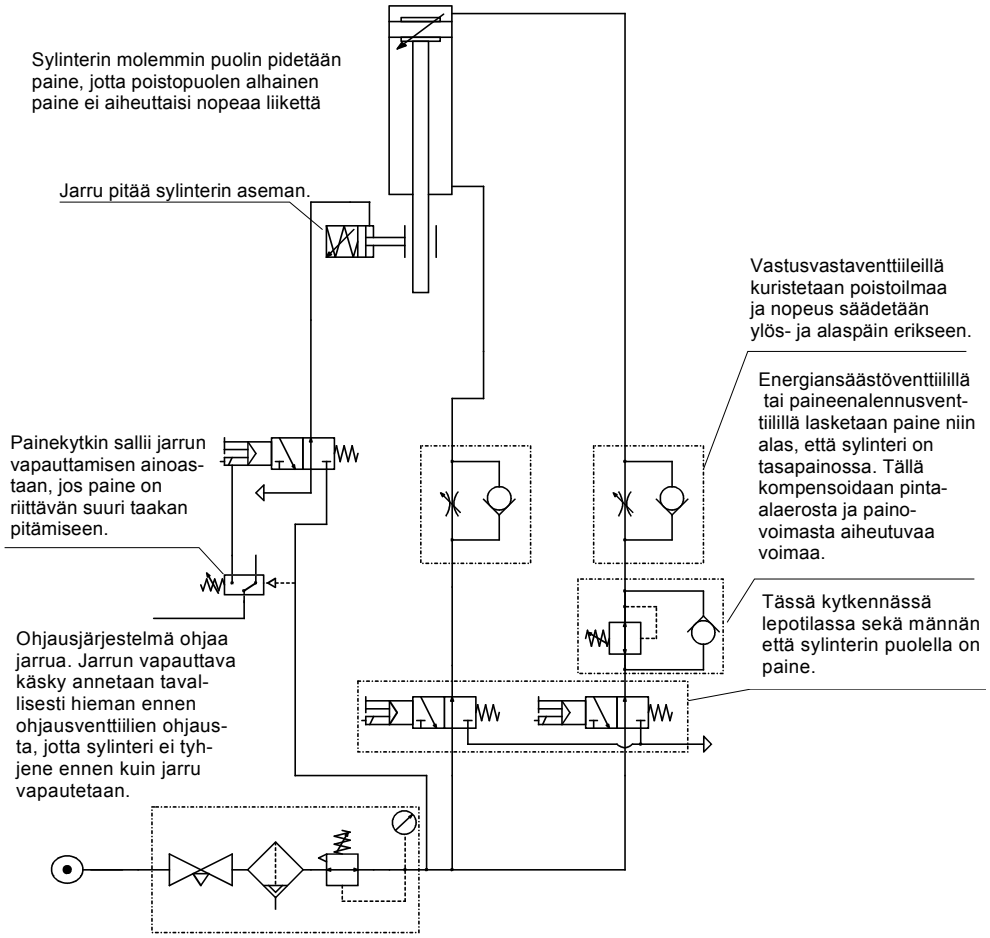
Toiminnan kuvaus (kuva 40)

- Kytkennällä suljetaan sylinterin ilmatilavuus. Liike pysähtyy, kun sylinterin toinen tai molemmat puolet sulkeutuvat.
- Painekytkin valvoo ohjauspainetta. Ohjauspaineen vioista voi sähköinen ohjausjärjestelmä saada tiedon ja antaa varoituksen tarpeen mukaan.
- Vaarallinen vika syntyy, jos sekä paineohjatut venttiilit että alhaalla oleva 5/3-venttiili jumiutuvat auki. Jos 5/3-venttiili jumiutuu, niin sylinteri tekee ainoastaan yhden liikkeen, ja jos paineohjatut venttiilit jumiutuvat, niin painekytkin paljastaa vian.

Turvallisen toiminnan edellytykset

- Paineohjatut ohjausventtiilit tulee kytkeä suoraan sylinteriin, jotta letkun irtoaminen ei aiheuta sylinterin liikettä ja toisaalta ohjattava ilmamäärä olisi mahdollisimman pieni.
- Paineilman syöttö on normaaliolosuhteisiin sopiva. Piiriin ei ole piirretty vastusventtiiliä, joka voi olla tarpeen nopeuden säädössä. Pysäytyksen jälkeen sylinterissä voi olla normaalia alhaisempi paine, joka voi uudelleenkäynnistyksessä johtaa yllättävään liikkeeseen.
- Esimerkissä ei ole ulkopuolista valvontaa. Pysäytystilanteessa sylinteriin jää suljettu painetila, joka pitää tyhjentää ennen huoltotoimenpiteitä esim. käyttämällä sylinteriä ilman syöttöpainetta. [Malm & Järvenpää 1998]

4.4.16 Paineilmasylinterin pysäytys täyttämällä ilmatila (luokka 3)



Kuva 41. Paineilmakaavioesimerkki ilmatilavuuden täyttämiseen perustuvalla pysäytyksellä toteutetusta sylinterinohjauksesta Jarru varmistaa toimintaa (luokka 3).

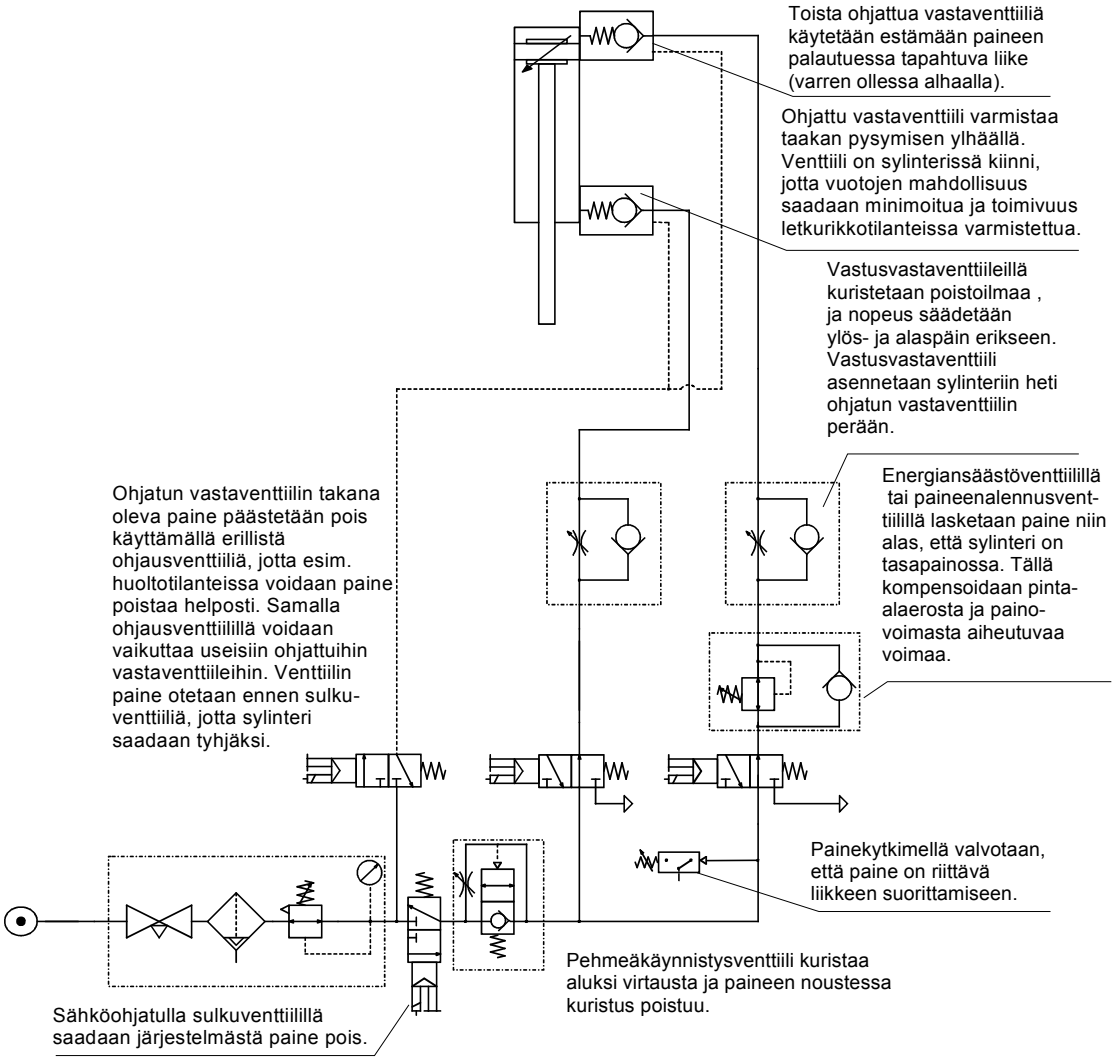
Toiminnan kuvaus (kuva 41)

- Ohjausventtiilit toteuttavat varsinaisen pysäytyksen ja sylinterin kummallekin puolelle jää täysi tasapainotilan paine. Jarru varmistaa pysäytyksen lopuksi.
- Turvallisuus perustuu ohjausventtiilien toimintaan ja jarrun varmistavaan toimintaan. Varsinaista valvontaa ei ole.
- Vaarallinen vika syntyy, jos ohjausventtiili ei toimi ja jarru ei pidä. Vaarallinen tilanne voi syntyä myös, jos toinen venttiili päästää ilman pois ja jarru pitää aluksi ja sitten jarru vapautuu. Tämän seurauksena syntyy yllättävä liike siihen suuntaan, missä ei ole painetta.

Turvallisen toiminnan edellytykset

- Jos jarrua käytetään kahdennukseen, sen rakenteen pitää kestää myös jarrutus [Malm & Järvenpää 1998].

4.4.17 Paineilmasylinterin pysäytys vastaventtiileillä (luokka 3)

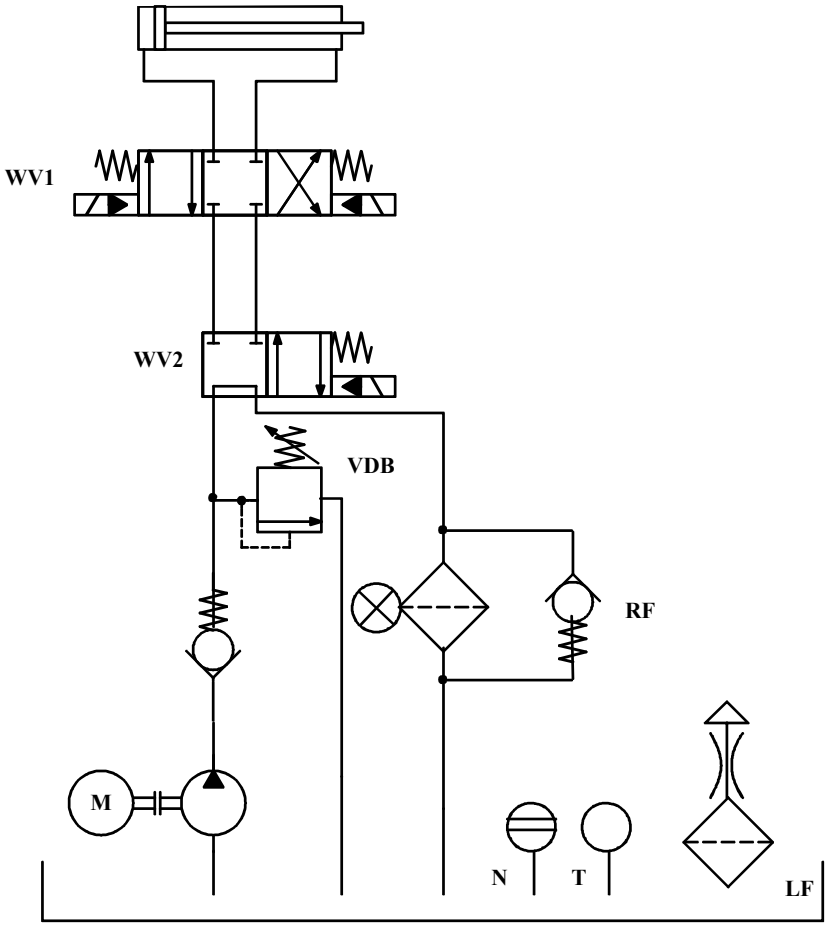


Kuva 42. Paineilmakaavioesimerkki ohjattujen vastaventtiilien toimintaan perustuvasta sylinterinohjauksesta. Pysäytyksessä täytetään ilmatila (luokka 3).

Toiminnan kuvaus (kuva 42)

- Piirissä liikettä ohjataan sekä sallimalla ilman kulku ohjatuilla vastaventtiileillä että ohjaamalla tasapainopaine sylinteriin. Kummat komponentit tahansa voivat toteuttaa pysäytyksen.
- Painekytkimellä valvotaan, että paine riittää liikkeen suorittamiseen. Jos paine on alhainen, käynnistystä ei sallita.
- Vaarallinen vika (hallitsematon liike) syntyy, jos sekä ohjattu vastaventtiili (tai sen ohjaus) että samassa linjassa oleva ohjausventtiili pettää. Jos toinen ohjausventtiili vikaantuu ja päästää ilmat pois, niin sylinterin toiselle puolelle jää alhainen paine ja seuraava liike tapahtuu normaalia nopeammin. Jos painekytkin vikaantuu, voi muun vian seurauksena syntynyt alhainen paine jäädä havaitsematta ja käynnistys voi johtaa väärään suuntaan tapahtuvaan liikkeeseen. [Malm & Järvenpää 1998]

4.4.18 Hydraulinen sylinterin ohjaus (luokka 3)



Kuva 43. Esimerkki hydraulisesta ohjausjärjestelmästä (luokka 3).

Toiminnan kuvaus (kuva 43)

- Vaarallisia liikkeitä tai tiloja valvotaan kahdella suuntaventtiilillä WV1 ja WV2.
- Jomman kumman suuntaventtiilin yksittäinen vikaantuminen ei johda turvatoiminnan menettämiseen.
- Vikoja ei havaita. Jotkut viat paljastuvat toiminnassa. Suuntaventtiilien peräkkäinen vikaantuminen voi johtaa vaaralliseen vikaan.

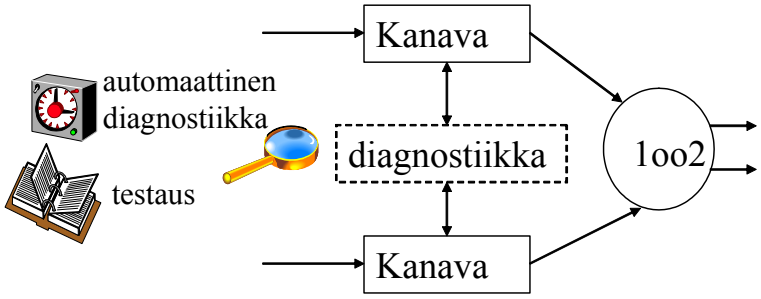
Turvallisen toiminnan edellytykset

- Komponenttitoimittajien esittämät ympäristövaatimukset tulee täyttää.
- Letkurikko sylinterin tuloissa voi aiheuttaa pienen liikkeen. Tarvittaessa tämä voidaan välttää vaihtamalla sylinterille menevät letkut putkiin.

Käyttö

- Käyttökohteena ovat hydrauliset ohjauspiirit [BIA-Report 6/97e, 1997].

4.5 Esimerkkejä Luokan 4 ohjausjärjestelmistä

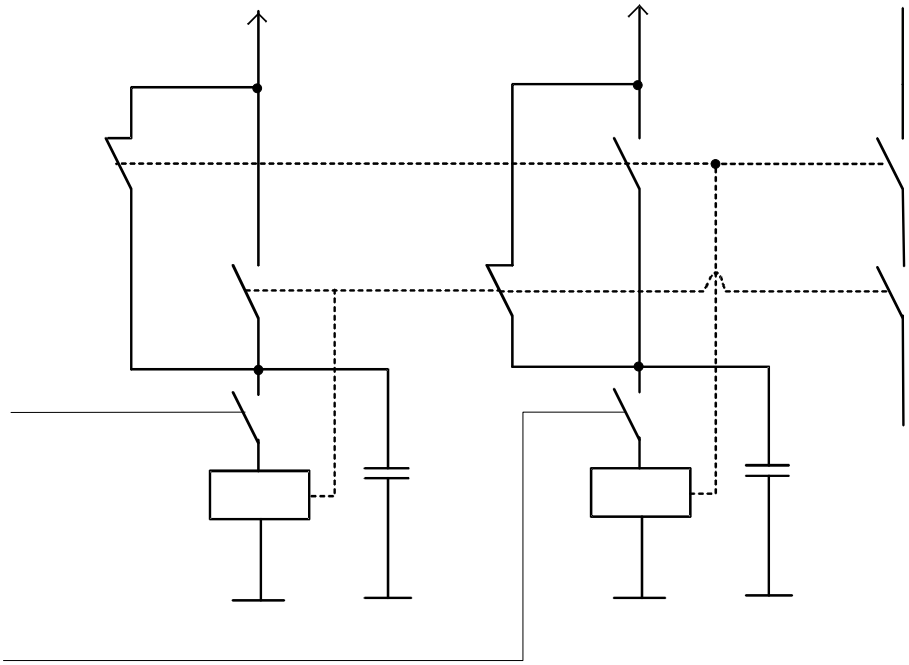


Kuva 44. Luokan 4 järjestelmät ovat tyypillisesti kaksikanavaisia, niissä on kattava automaattinen diagnostiikka ja lisäksi niiden toimintakuntoa testataan usein.

Luokan 4 (kuva 44) järjestelmissä valvotaan vikaantumista tarkkaan, ja periaatteessa kaikki yksittäiset viat paljastuvat tai johtavat turvalliseen tilaan. Tämä edellyttää suunnittelulta huolellisuutta ja lopuksi tarkkaa validointia. Luokan 4 järjestelmä onkin selvästi kalliimpi toteuttaa kuin luokan 3 järjestelmä. Sähkömekaanisilla komponenteilla on mahdollista toteuttaa ”idioottivarmoja” kytkentöjä, joissa yksittäiset viat paljastuvat. Niiden heikkoutena ovat mahdolliset samanaikaiset vikaantumiset tai käyttämättömyydestä johtuvat pitkän ajan kuluessa syntyneet monien toimintojen ”jumiutumiset”. Elektroniikalla ja ohjelmoitavalla elektroniikalla voidaan luokan 4 järjestelmissä valvoa toimintoja jatkuvasti. Tämäntyyppisissä järjestelmissä ongelmana on puolestaan monimutkaisuus, jonka vuoksi on vaikea osoittaa, ettei järjestelmään voi tulla vaarallisia vikoja. Pneumatiikassa luokan 4 järjestelmissä (esim. puristimissa) käytetään yleensä kaksoisventtiiliä, joka valvoo itse omaa toimintakuntoaan. Hydrauliikassa luokan 4 järjestelmissä käytetään sähköisesti valvottuja komponentteja, jolloin myös osa valvonnasta on toteutettu sähkötekniikalla.

Joissain tapauksissa luokkien 3 ja 4 raja voi riippua tilanteesta. Esim. joidenkin hätäseis-releiden luokka voi riippua siitä, onko niissä tulojen oikosulun valvontaa (vrt. kuva 51). Jos tulot on mahdollista toteuttaa siten, että ne ovat kaukana toisistaan (erilliset kaapelit eikä vierekkäisiä liittimiä), voidaan oikosulun mahdollisuus sulkea pois, ja kyseisessä tilanteessa päästä järjestelmässä luokkaan 4 (vrt. kuvat 32 ja 48). Luokan 4 järjestelmät vastaavat usein eheystasoa 3 (IEC 61508 mukaan). Nämä ovat korkeimpia konejärjestelmissä käytettyjä luokkia tai eheystasoja. Korkeammat tasot eivät ole tarpeen, koska konejärjestelmät eivät väärin toimiessaan aiheuta katastrofia, vaan vaara kohdistuu korkeintaan muutamaan henkilöön.

4.5.1 Kahden tulosignaalin samanaikaisuuden valvonta (luokka 4)



Kuva 45. Kahden tulosignaalin samanaikaisen toiminnan valvonta (luokka 4).

Toiminnan kuvaus (kuva 45)

- Piirin kytkennässä releitä ohjataan samanaikaisesti tulevilla signaaleilla. Jos tulot saavat jännitteen eriaikaisesti, se tulkitaan viaksi eikä toinen rele vedä.
- Releet valvovat toinen toisiaan käynnistystilanteessa. Kondensaattorit antavat jännitteen pieneksi ajaksi koskettimien vaihtaessa asentoa.
- Releiden yhtäaikainen jääminen vetäneeseen tilaan (esim. koskettimien hitsautuminen johtuen samasta ylijännitteestä) voi aiheuttaa vaaratilanteen.

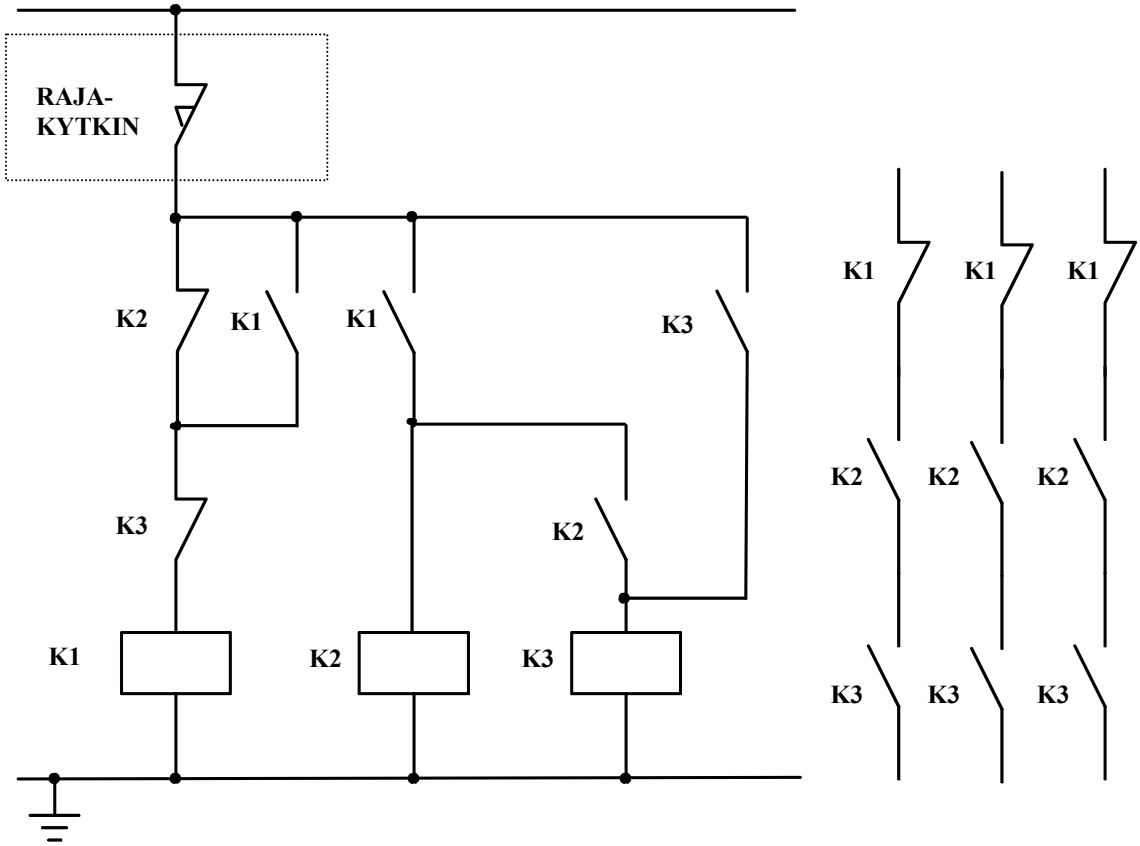
Turvallisen toiminnan edellytykset

- Releiden tulee olla pakkotoimisia, jotta valvonta toimii ja esitetty luokka saavutetaan.

Käyttö

- Käyttökohteena ovat ohjauspiirit, joissa valvotaan kahden tulon samanlaista toimintaa.

4.5.2 Esimerkki valvotusta ohjauksesta (luokka 4)



Kuva 46. Esimerkki rajakytkimeen liitetystä valvotusta ohjauksesta. Rajakytkintä ei piirissä valvota, ja esitetty luokka koskee vain piiriä ilman rajakytkintä (luokka 4).

Toiminnan kuvaus (kuva 46)

- Vaaralliset liikkeet tai tilat pysäytetään itseään valvovan kosketinkombinaation kautta, kun rajakytkimeen vaikutetaan. Käynnistyksessä aluksi K1 vetää, tämän jälkeen K2, jonka jälkeen K3 ja tämän jälkeen edelleen K1 päästää ja käynnistys on sallittu. Kaikki releet vaihtavat asentoa käynnistyksessä ja, jos jokin kosketin ei toimi, niin käynnistystä ei sallita.
- Rajakytkintä ei piirissä valvota. Rajakytkimen oikosulku tai ohjainpään rikkoutuminen johtaa vaaralliseen vikaan. Rajakytkimen sijaan piirissä voi olla esim. turvalaitteen lähtö.

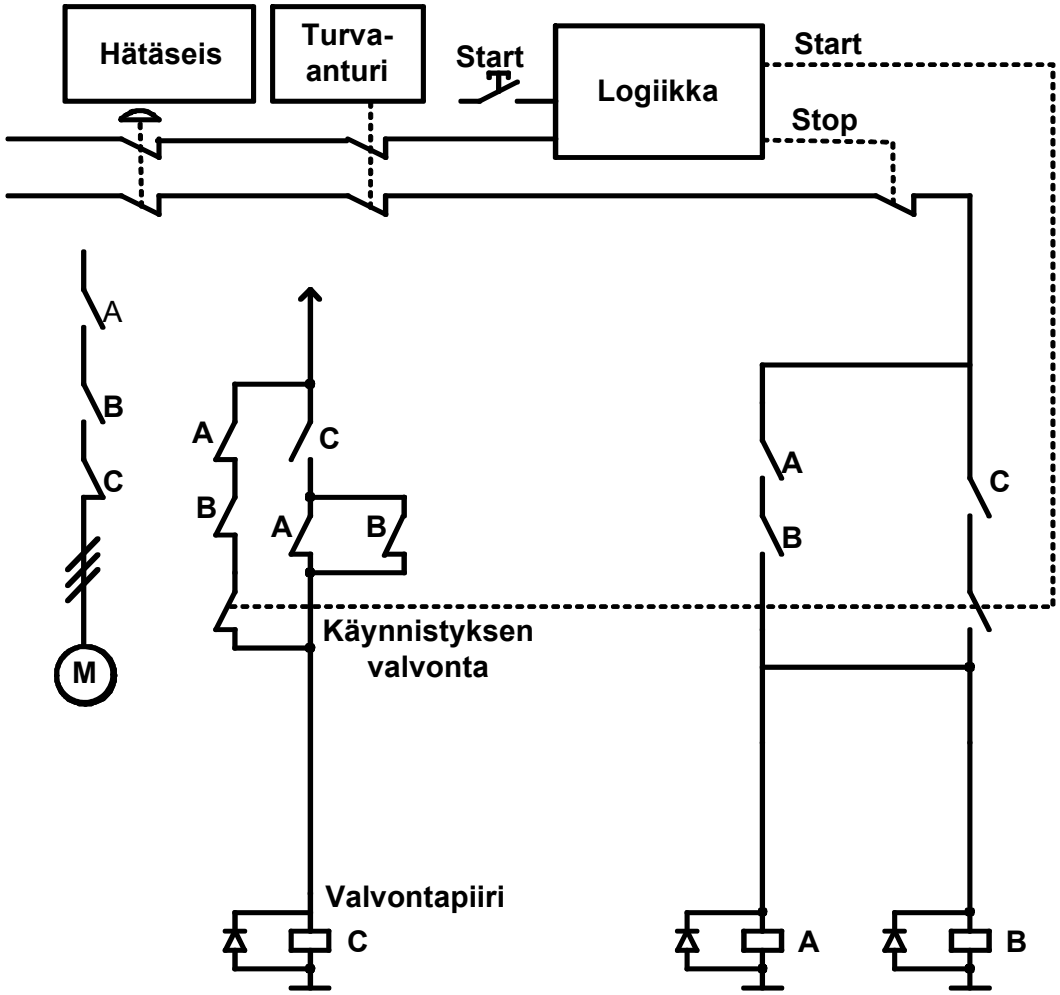
Turvallisen toiminnan edellytykset

- Releiden tulee olla pakkotoimisia

Käyttö

- Käyttökohteena ovat ohjauspiirit [BIA-Report 6/97e, 1997].

4.5.3 Käynnistyksen ohjauksen valvonta (luokka 4)



Kuva 47. Esimerkki käynnistyksen ohjauksen valvonnasta (luokka 4).

Toiminnan kuvaus (kuva 47)

- Käynnistyskomento menee suoraan logiikkaan, josta se edelleen välittyy releille. Pysäytystiedot välittyvät sekä releille että logiikkaan. Sekä logiikka että releet voivat toteuttaa pysäytyksen. Käynnistyspainiketta painettaessa releet A ja B vetävät ja tämän jälkeen rele C päästää.
- Piirissä releet valvovat toinen toisiaan ja lisäksi valvotaan käynnistystä. Moottorin uudelleenkäynnistys on mahdollista vain, jos käynnistyksen ohjaus palaa alkutilaansa. Käynnistyksen valvonta voidaan toteuttaa myös logiikassa.

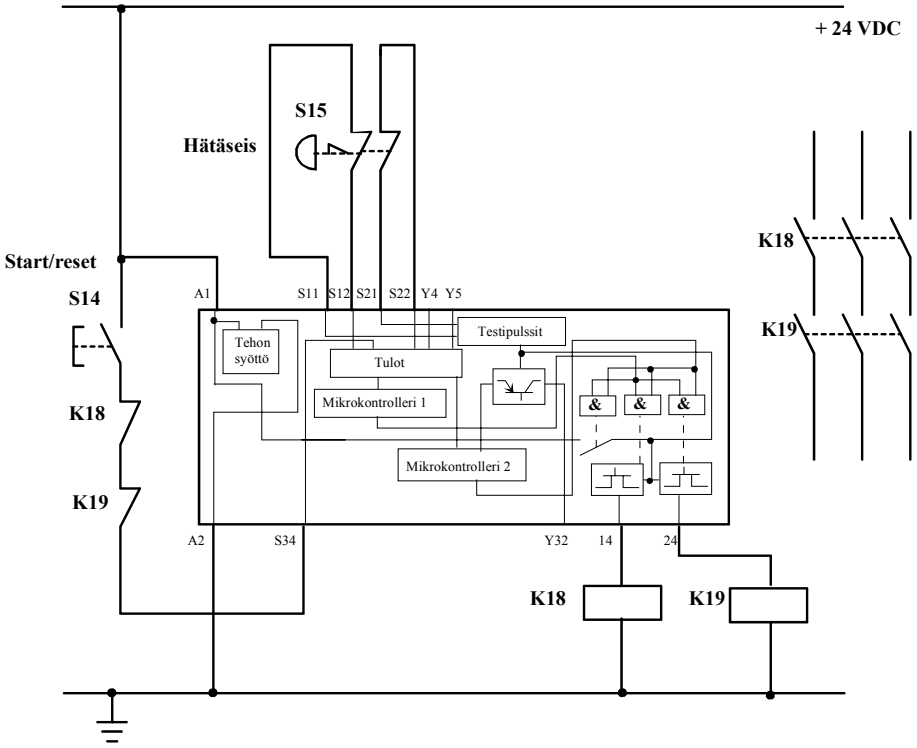
Turvallisen toiminnan edellytykset

- Piirin releiden ja käynnistyksen ohjauksen tulee olla pakkotoimisia.

Käyttö

- Käyttökohteena ovat valvotut moottorinohjauspiirit.

4.5.4 Hätäpysäytysrele esimerkki (luokka 4)



Kuva 48. Esimerkki hätäpysäytyspiiristä, jossa on käytetty hätäpysäytysrelettä (luokka 4).

Toiminnan kuvaus (kuva 48)

- Vaaralliset liikkeet tai tilat pysäytetään hätäpysäytysreleen avulla releiden K18 ja K19 kautta, kun hätäpysätyspiiriin vaikutetaan.
- Käynnistyksen yhteydessä valvotaan releitä K18 ja K19. Hätäpysäytyspiiri valvoo itse omaa toimintakuntoaan. Tulopiirien oikosulkua valvotaan testipulsseilla.

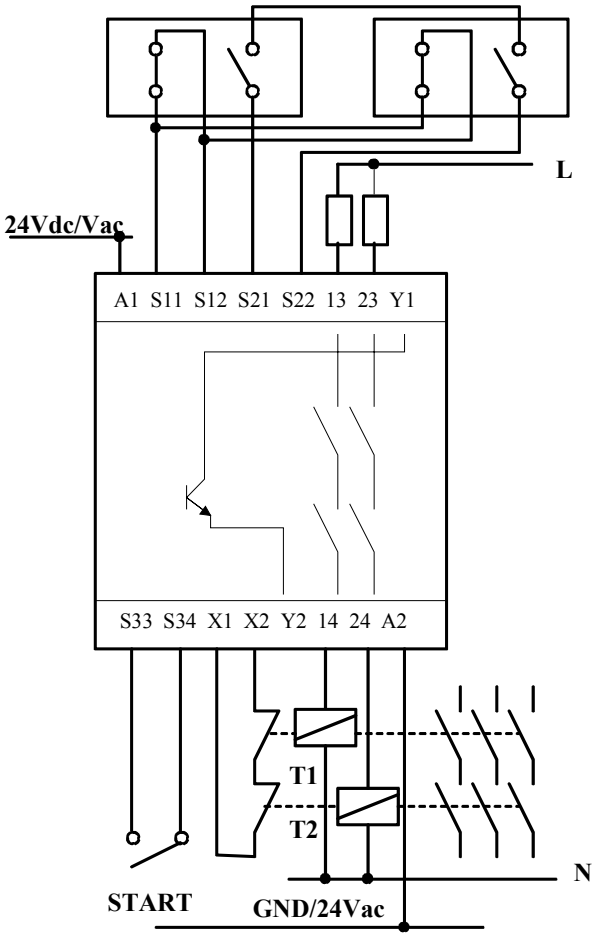
Turvallisen toiminnan edellytykset

- Releiden tulee olla pakkotoimisia.

Käyttö

- Käyttökohteena ovat hätäpysäytyspiirit [Pilz CD].

4.5.5 Esimerkki magneettikytkimen valvonnasta (luokka 4)



Kuva 49. Esimerkki magneettikytkimestä (luokka 4).

Toiminnan kuvaus (kuva 49)

- Kahdennetun magneettikytkimen avautuvat koskettimet on kytketty valvontayksikköön rinnan ja sulkeutuvat koskettimet sarjassa. Jos jompi kumpi magneettikytkimistä vaikuttuu, niin releet T1 ja T2 päästävät.
- Releiden T1 ja T2 toimintaa valvotaan käynnistystilanteessa.

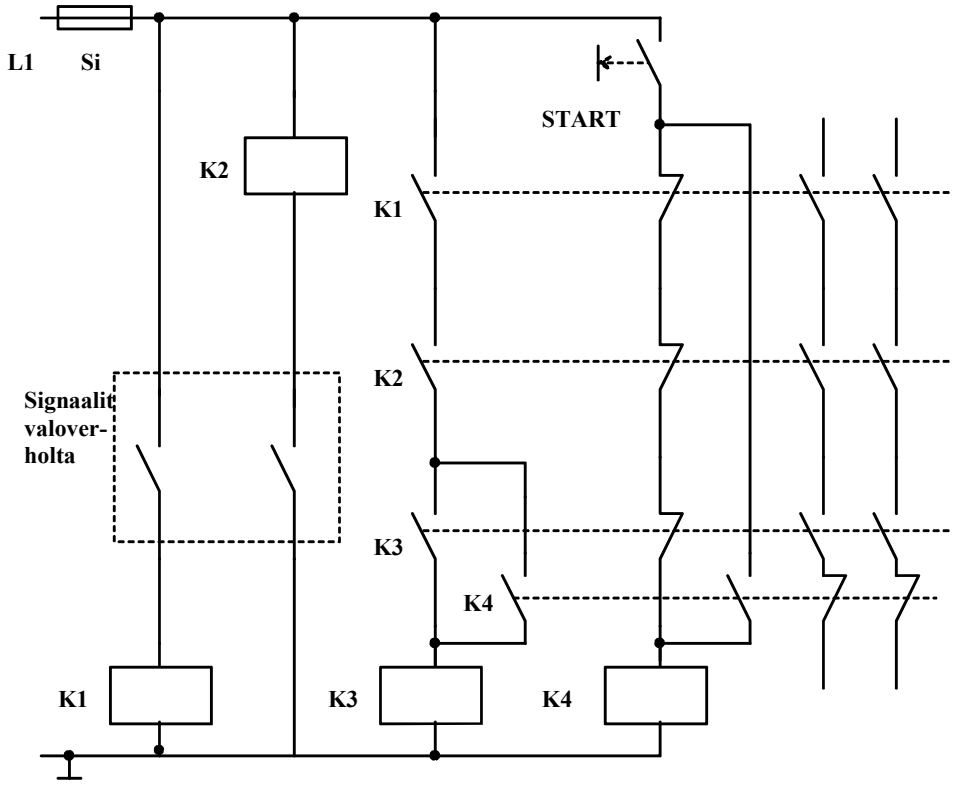
Turvallisen toiminnan edellytykset

- Releiden T1 ja T2 tulee olla pakkotoimisia, jotta esitetty luokka saavutettaisiin.

Käyttö

- Käyttökohteena ovat magneettikytkimen ohjaus- ja valvontapiirit [Carlo Gavazzi -esite].

4.5.6 Esimerkki turvalaitteen kytkennästä ohjaukseen (luokka 4)



Kuva 50. Turvallisuuteen liittyvien signaalien kytkentä koneen ohjaukseen; esimerkkinä valoverho (luokka 4).

Toiminnan kuvaus (kuva 50)

- Valoverhon turvallisuuteen liittyvät signaalit (2 sulkeutuvaa kosketinta) kytkevät releet K1 ja K2. Käynnistyspainikkeen painamisen jälkeen rele K4 vetää hetkeksi ja K3 vetää. K4 päästää vasta, kun käynnistyspainike vapautetaan.
- Releet valvovat toistensa toimintakuntoa käynnistyksen yhteydessä. Käynnistys-painikkeen jumiutumista valvotaan. Käynnistyspainikkeen jumiutuminen estää käynnistyksen.

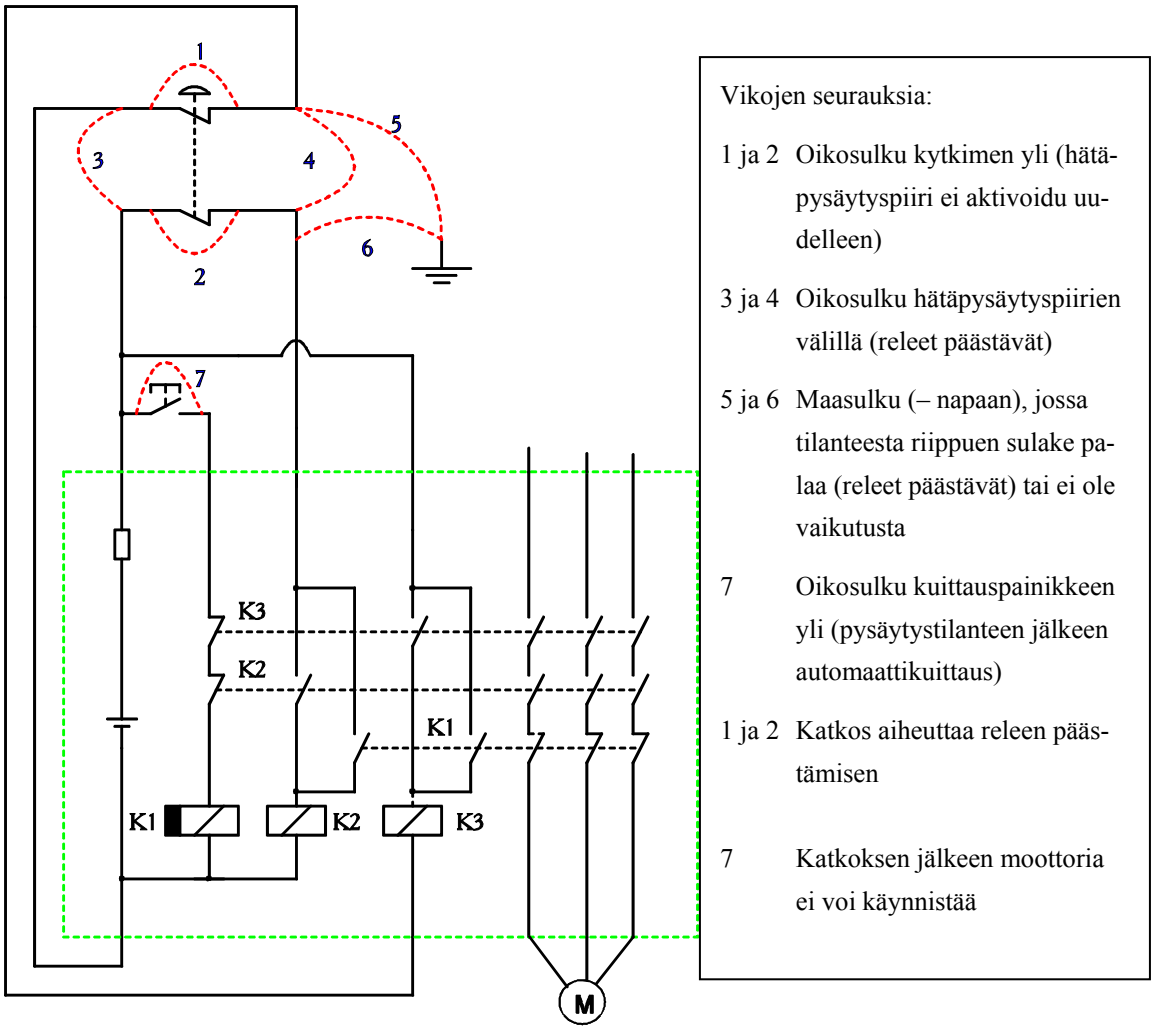
Turvallisen toiminnan edellytykset

- Releiden K1, K2, K3 ja K4 tulee olla pakkotoimisia. Valoverhon pitää vastata muun järjestelmän luokkaa (tyypin 4 valoverho).

Käyttö

- Käyttökohteena ovat valoverhojen ja -kennojen suojauspiirit [BIA-Report 6/97e, 1997].

4.5.7 Esimerkki turvareleestä ja sen vikamuodoista (luokka 4)

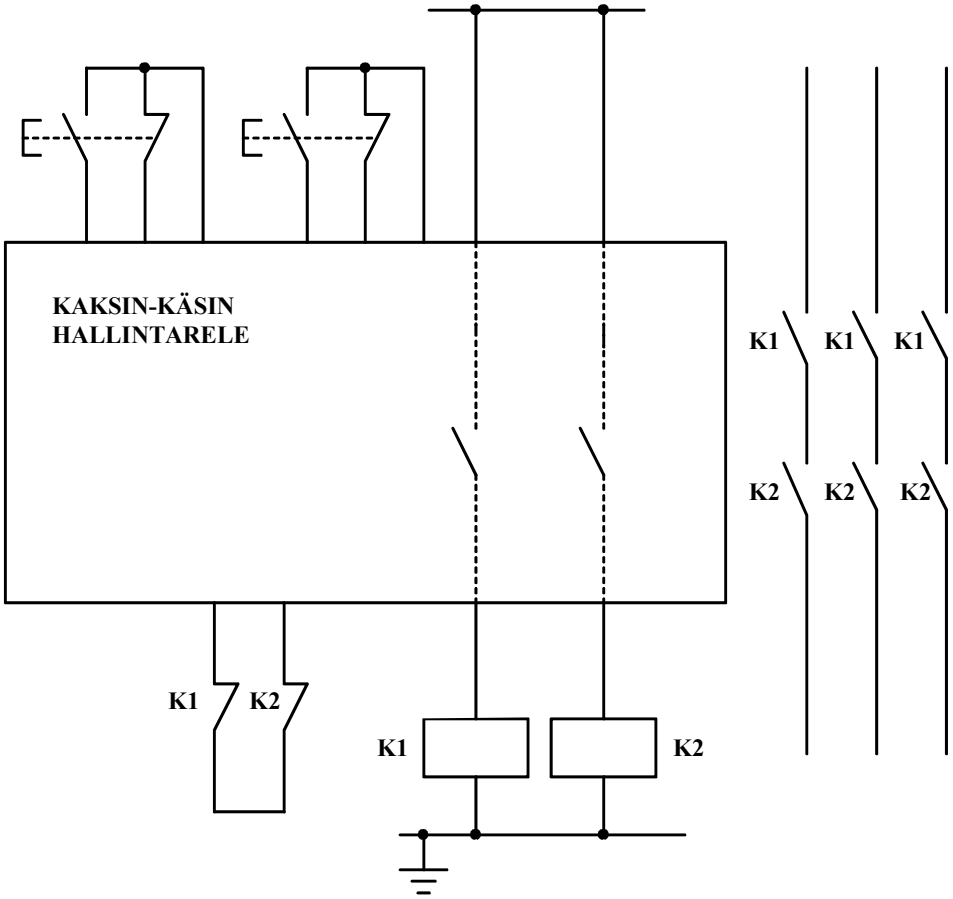


Kuva 51. Esimerkki erään turvareleen kytkennästä (luokka 4).

Toiminnan kuvaus (kuva 51)

- Piiri käynnistetään painikkeella kohdassa 7. Tällöin K1 vetää, ja heti tämän jälkeen K2 ja K3 vetävät. Viiveen jälkeen K1 päästää ja moottori voi käynnistyä. Hätäpysäyttimen painaminen avaa ohjattavan piirin.
- Releet valvovat toisiaan käynnistyksen yhteydessä ja, jos hätäpysäytyspiirit koskettavat toisiinsa, sulake palaa. Kuvassa on numeroitu eri kohteita, joiden oikosulkua valvotaan. Käynnistyspainiketta ei valvota, ja sen oikosulku aiheuttaa hätäpysäyttimen vapauttamisen jälkeisen automaattikäynnistyksen. Jos manuaalikäynnistystä ei tarvita, niin käynnistyspainike voidaan myös oikosulkea.
- Releiden tulee olla pakkotoimisia. Hätäpysäytysrele kytketään kahteen pysäyttävään elimeen, joiden tulee toimia samanaikaisesti. [Malm et al. 1998]

4.5.8 Kaksinkäsinhallintareleen käyttö (luokka 4)



Kuva 52. Esimerkki kaksinkäsinohjauksesta releyksikön avulla toteutettuna (luokka 4).

Toiminnan kuvaus (kuva 52)

- Kun kaksinkäsinhallintalaitteen painikkeisiin vaikutetaan samanaikaisesti, niin piiri ohjaa releet K1 ja K2 vetäneeseen tilaan.
- Piiri valvoo sisäisesti omaa toimintakuntoaan ja releiden K1 ja K2 toimintakuntoa käynnistyksen yhteydessä.

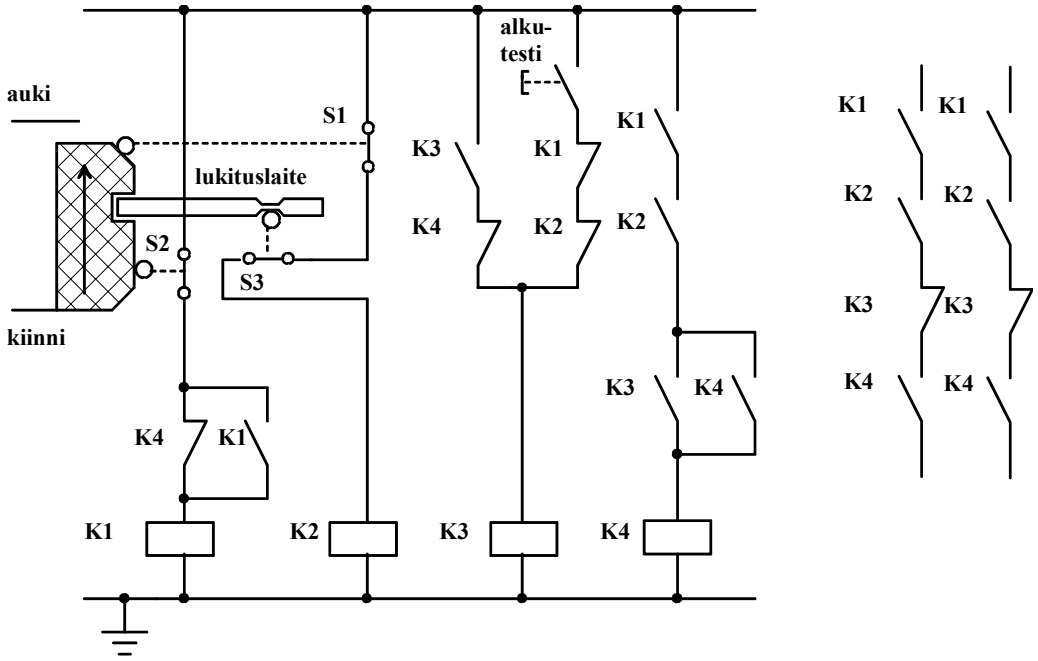
Turvallisen toiminnan edellytykset

- Kuvassa releyksikkö on tyyppiä III C EN 574 mukaan. Jos keskusyksikkö vaihdetaan, voidaan saavuttaa toinen EN 574 -tyyppi.

Käyttö

- Käyttökohteena ovat kaksinkäsinhallintalaitteet [BIA-Report 6/97e, 1997].

4.5.9 Portin lukituksen valvontapiiri (luokka 4)



Kuva 53. Esimerkki portista, jonka aukioloa valvotaan rajakytkimillä. Portilla lukitus- ja aloitustesti (luokka 4).

Toiminnan kuvaus (kuva 53)

- Piirillä valvotaan sekä portin kiinnioloa että lukittumista. Jos lukko ja portti avataan, valvottu kone pysähtyy. Uudelleenkäynnistys tehdään alkutestipainiketta painamalla portin ollessa auki. Alkutesti ei toimi, jos portti on kiinni.
- Lukitusmekanismia ja porttia valvotaan pakkotoimisilla rajakytkimillä. Releet valvovat toisiaan alkutarkastuksen yhteydessä. Turvatoiminto säilyy vikaantuneena. Kaikki viat havaitaan toiminnan aikana tai, kun porttiin vaikutetaan.
- Vikojen kasaantuminen perättäisten käyttökertojen välillä voi johtaa turvatoiminnon menettämiseen. Alkutestipainiketta ei valvota, mutta toisaalta sen vaikutus turvallisuuteen on vähäinen tai riippuu kohteesta.

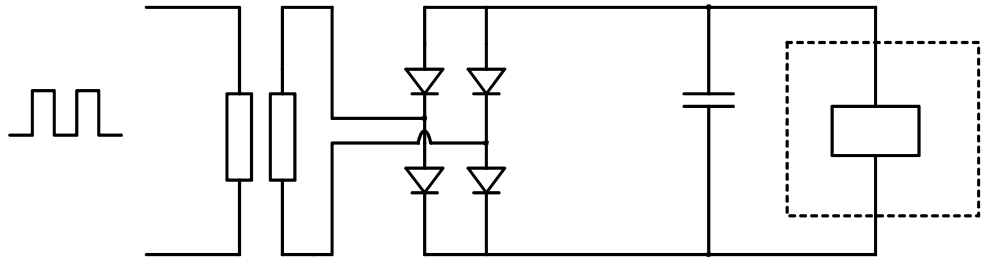
Turvallisen toiminnan edellytykset

- Rajakytkimien S1 ja S3 tulee olla pakkotoimisia. Releiden K1, K2, K3 ja K4 tulee olla pakkotoimisia. Rajakytkimien S1, S2 ja S3 tulee olla erillisjohdotettuja.
- Eri turvapiirien rajakytkimiä ei tule kytkeä sarjaan, koska vikojen valvonta ei silloin toimi.

Käyttö

- Käyttökohteena ovat koneen toimintaan kytketyt suojukset [BIA-Report 6/97e, 1997].

4.5.10 Pulssituksen muunto kytkentätiedoksi muuntajalla (luokka 4)

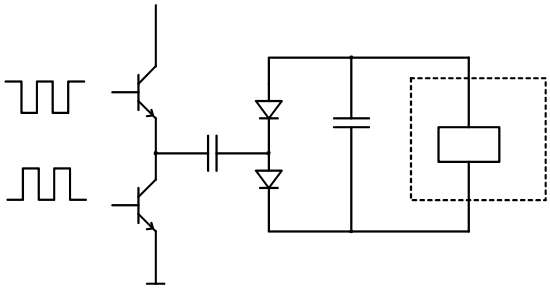


Kuva 54. Esimerkki piiristä, jolla elektroniikan pulssitus muutetaan releiden kosketintiedoksi. Katkoviivalla merkitty laatikko esittää turvareleyksikköä (luokka 4).

Toiminnan kuvaus (kuva 54)

- Esimerkkipiirissä pulssitus ohjataan muuntajalle, jonka läpi pääsee siis ainoastaan vaihtovirta. Virta tasasuunnataan ja ohjataan turvareleyksikölle. Ideana on, että muuntajan oikea puoli saa energiaa ainoastaan muuntajan välityksellä ja pulssituksen vaimeneminen johtaa releen saaman jännitetason laskuun, jolloin rele päästää. Piirin viat johtavat pulssituksen vaimenemiseen, jolloin rele päästää.
- Esitetyn luokan vaatimuksena on, että muuntajan käämit on riittävän tehokkaasti erotettu toisistaan (ei ensiö- ja toisiopiirin välistä oikosulkuvaaraa) ja releyksikkö on valittu esitetyn luokan mukaisesti.

4.5.11 Pulssituksen muunto kytkentätiedoksi varauspumpulla (luokka 4)

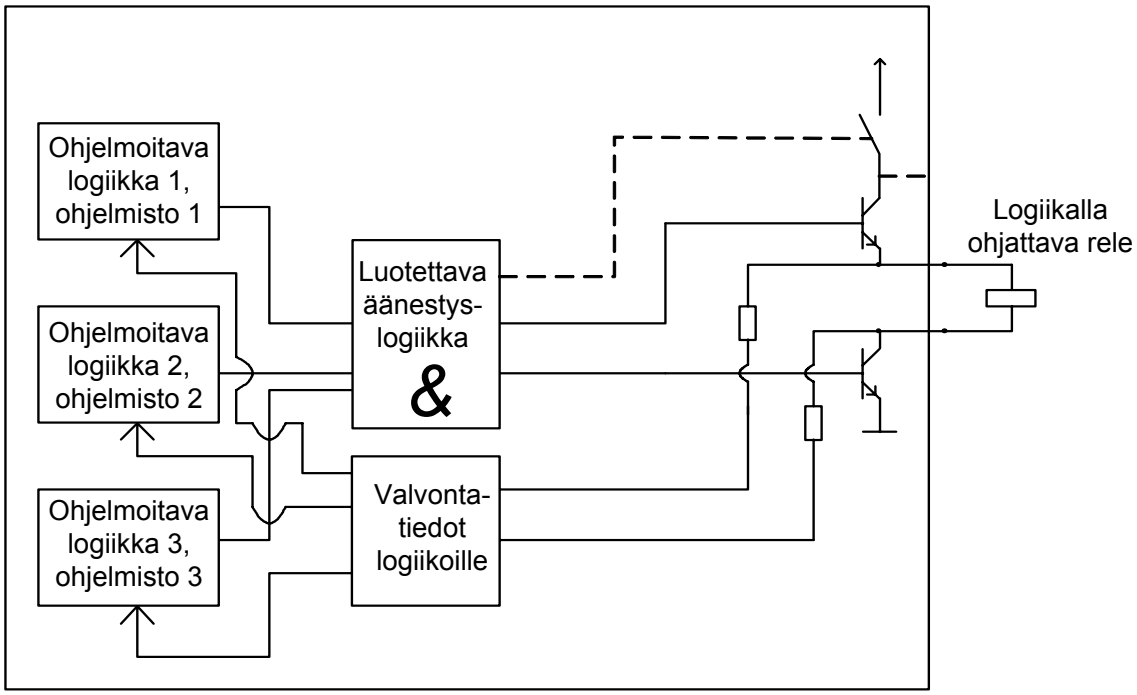


Kuva 55. Esimerkki piiristä, jolla elektroniikan pulssitus muutetaan releiden kosketintiedoksi. Katkoviivalla merkitty laatikko esittää turvareleyksikköä (luokka 4).

Toiminnan kuvaus (kuva 55)

- Esimerkkipiirissä kahdella vastakkaisvaiheisella pulssituksella ohjataan transistoreita, joilla edelleen ”pumpataan” kondensaattoria (”varauspumppu”). Virta tasasuunnataan ja ohjataan edelleen turvareleyksikölle. Piirien läpi pääsee ainoastaan vaihtovirta. Pulssituksen vaimeneminen johtaa releen saaman jännitetason laskuun, jolloin rele päästää.
- Piirin viat johtavat pulssituksen vaimenemiseen, jolloin rele päästää.
- Esitetyn luokan vaatimuksena on, että releyksikkö on valittu esitetyn luokan mukaisesti.

4.5.12 Esimerkki turvalogiikan yhden lähdön ohjauksesta (luokka 4)



Kuva 56. Esimerkki erään turvalogiikan (Pilz) yhden lähdön toteutuksesta (luokka 4).

Toiminnan kuvaus (kuva 56)

- Erään turvalogiikan yhden lähdön toteutus. Turvalogiikalla ohjataan oikealla olevaa relettä transistoreilla ja optoerottimilla. Kaikkien logiikkojen pitää ohjata rele vetämään, jotta rele vetäisi. Jos yksikin logiikka on eri mieltä, niin rele päästää.
- Transistorien toimivuutta testataan jatkuvasti nopeilla pulsseilla, joiden aikana rele ei ehdi päästää. Jos diagnostiikka havaitsee vian, niin transistorit jäävät estotilaan ja rele katkaisee jännitteen kaikilta lähdöiltä.

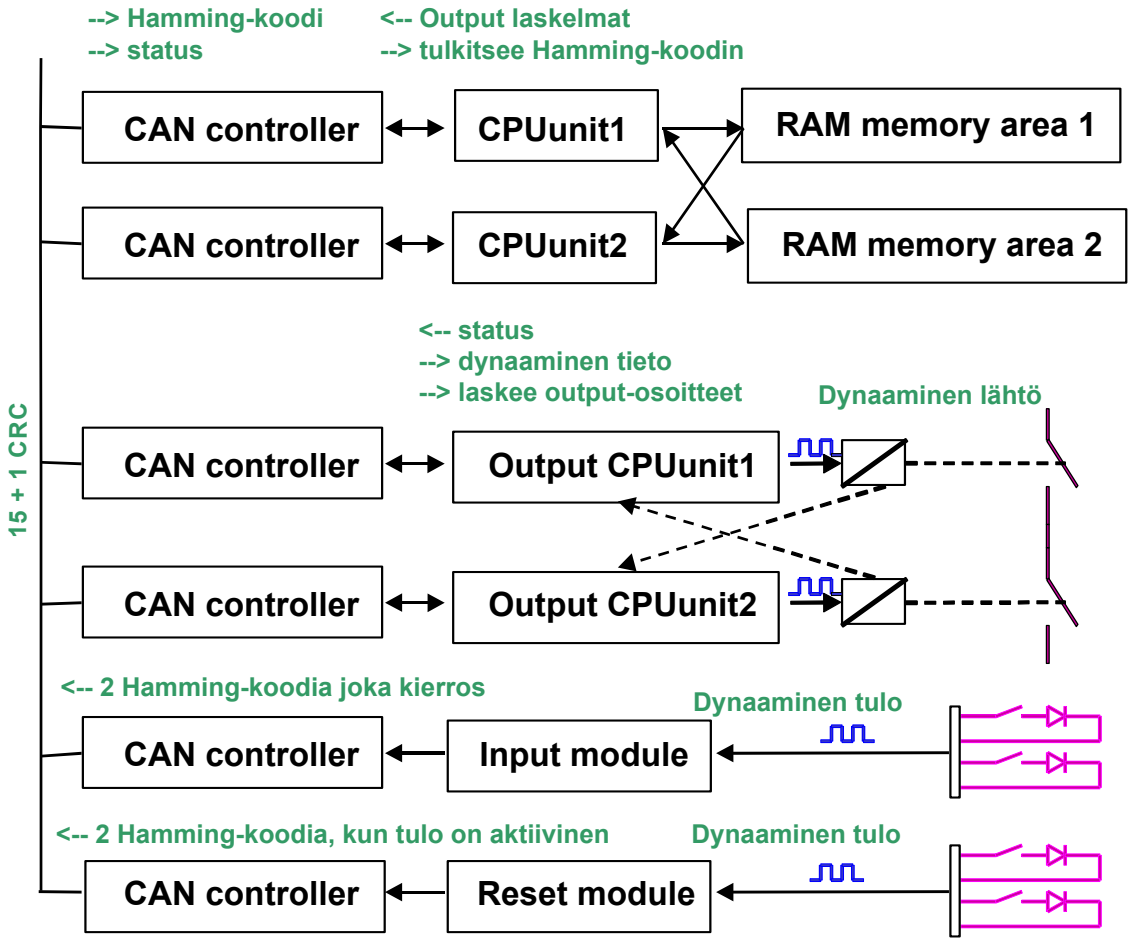
Turvallisen toiminnan edellytykset

- Käytetään eri logiikkoja ja ohjelmistoja. Käytetään jatkuvaa sopivasti ajoitettua testausta transistorien toimintakunnon varmistamiseen.
- Logiikkapiiri testaa myös ohjattavan releen vastusarvon pysymisen samana, joten relettä ei voi kytkeä helposti pois käytöstä. Oikosulut ja katkokset paljastuvat testeissä.

Käyttö

- Piiri soveltuu jatkuvaan käyttöön ja kohteisiin, joissa lähtö vaihtaa tilaansa jatkuvasti tai erittäin harvoin [Pilz-esite].

4.5.13 SAFELOC-turvaväyläjärjestelmä (luokka 4)

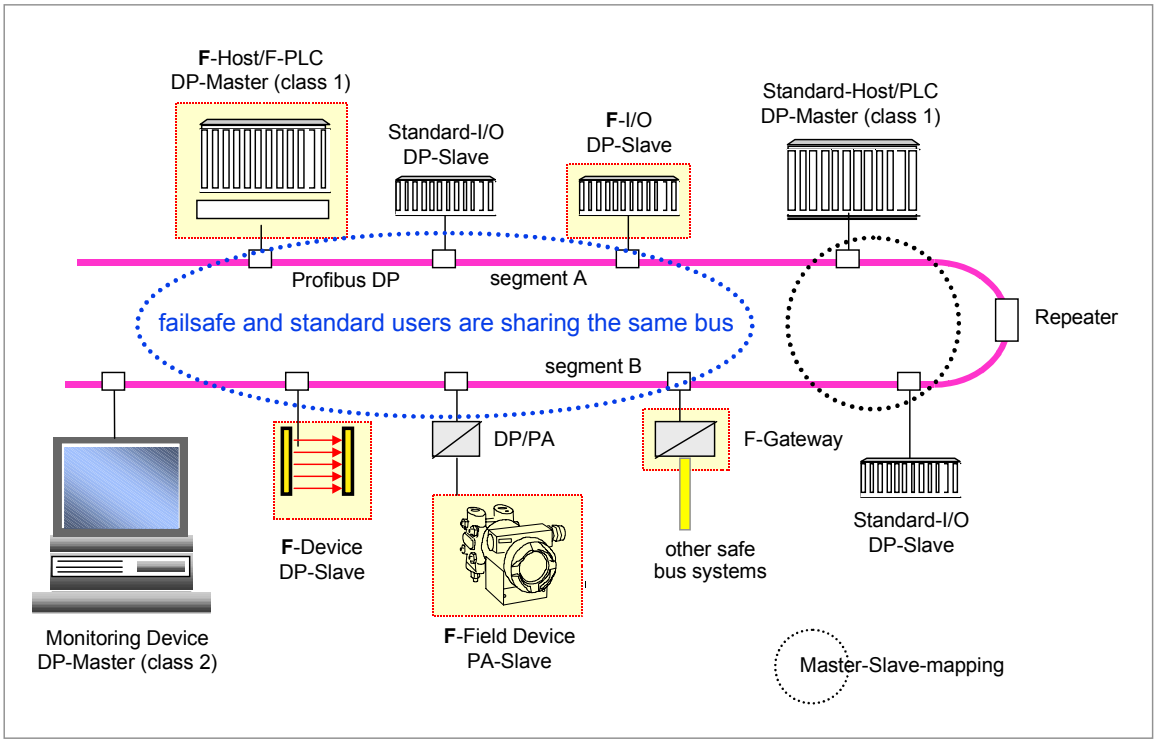


Kuva 57. Safeloc-turvaväyläesimerkki on kehitetty tutkimustarkoituksiin [Hérard et al. 2000].

Toiminnan kuvaus (kuva 57)

- Safeloc on toteutettu Ruotsissa lähinnä tutkimuskäyttöön eikä sitä ole kaupallisesti saatavissa. Safeloc valvoo robottijärjestelmän turvallisuutta. Järjestelmään kytketään turvalaitteet, painikkeet ja kytkimet CAN-väylän avulla. Käytössä on standardiväylä siihen liittyvine valvontoineen, mutta sanomiin ja laitteistoon on lisätty erilaisia turvatoimintoja.
- Viestit ovat dynaamisia (vaihdellaan kahta viestiä), ja ainoastaan tietty viesti estää turvatoiminnon. CPU:n valvonnassa käytetään mm. kahdennettua keskusyksikköä, kaksoismuistia (ristiinkirjoitus ja luku) sekä osoitteiden laskentaa joka lähetyskertaan. Lähtömoduulit on kahdennettu ja valvottu. Tulojen valvonta perustuu vaihtelevaan viestiin, joka saadaan aikaan diodin ja signaalin vaihtelun avulla. [Hérard et al. 2000]

4.5.14 ProfiSafe-turvaväyläjärjestelmä (luokka 4)



Kuva 58. Esimerkki turvaväylän (Profisafe) ja standardiväylän (Profibus DP) yhdistämisestä [Barthel et al. 1999] (luokka 4).

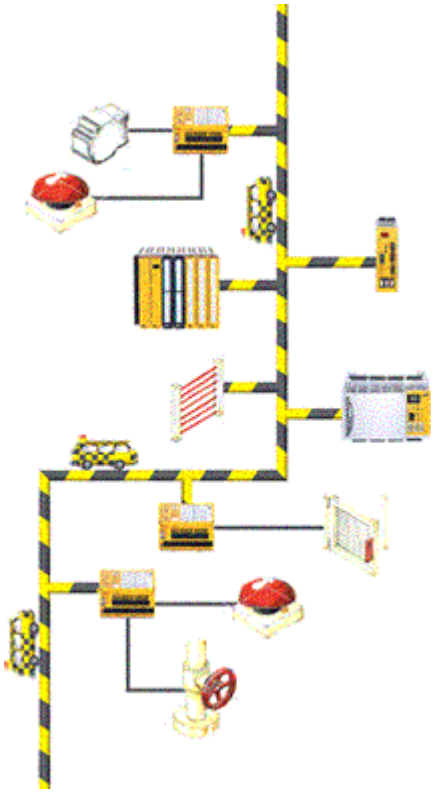
Toiminnan kuvaus (kuva 58)

- Esimerkissä on sekä turvallisuustietoa välittäviä moduuleja (F-kirjaimella alkavat moduulit) että tavallisia moduuleja. Kaikki moduulit viestivät samannäköisiä standardisanomia, mutta turvasanomiin on lisätty erityisiä turvakoodeja (tarkastussumma) sekä osoitteen ja funktion varmistustietoa. Tämän lisäsi käynnistyksen yhteydessä lasketaan tarkistussumma toimilaitteista, joita hyödynnetään myöhemmin tarkistuksissa.
- Yhden väylän järjestelmä sopii kohteisiin, joissa on yksi pysyvä turvallinen tila (pysäytys, sähköt poissa). Jos esim. kaapeli menee poikki, niin moduulien pitää osata itsenäisesti siirtyä turvalliseen tilaan. Turvamoduulit ovat esimerkissä luokkaa 4 ja standardimoduulit luokkaa B.

Käyttö

- Käyttökohteena ovat ohjauspiirit.

4.5.15 SafetyBus p -turvaväyläjärjestelmä (luokka 4)



Kuva 59. Periaatekuva turvaväylästä (SafetyBus p), jossa kaikki moduulit ovat turvallisuuteen liittyviä [Pilz www-sivut] (luokka 4).

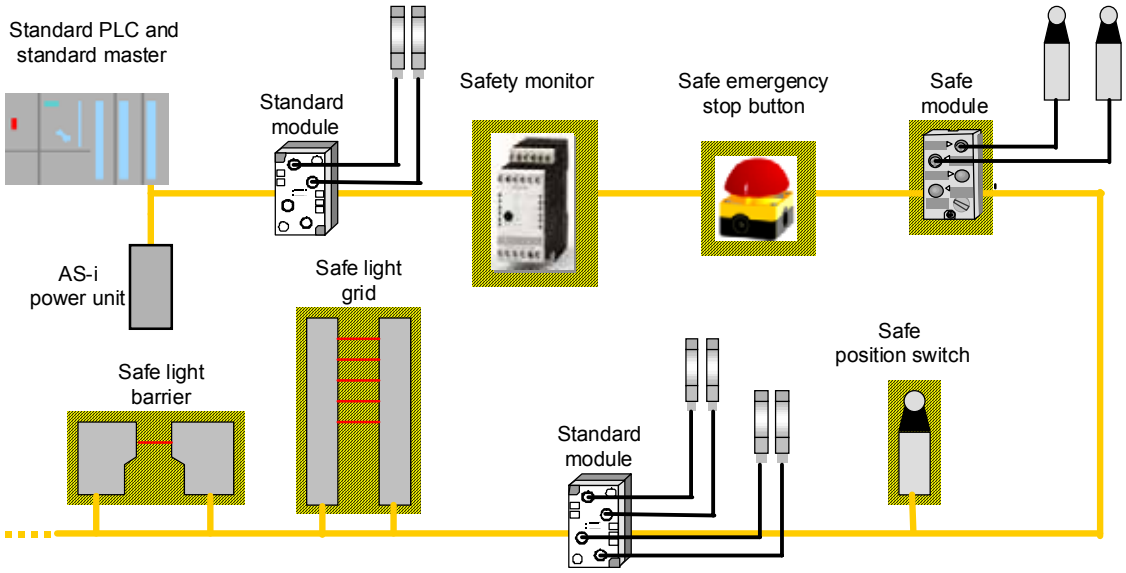
Toiminnan kuvaus (kuva 59)

- Esimerkissä kaikki väylään liitetyt moduulit ovat turvamoduuleja eikä väylään voi liittää tavallisia moduuleja. Väylän perustana on standardi CAN-väylä, johon on lisätty ominaisuuksia, jotta toteutus sopii luokkaan 4.
- Yhden väylän järjestelmä sopii kohteisiin, joissa on yksi pysyvä turvallinen tila (pysäytys, sähköt poissa). Jos esim. kaapeli menee poikki, niin moduulien pitää osata itsenäisesti siirtyä turvalliseen tilaan.

Käyttö

- Käyttökohteena ovat ohjauspiirit.

4.5.16 AS-i Safety at work -turvaväyläjärjestelmä (luokka 4)



Kuva 60. Esimerkki turvaväylän (AS-i Safety at work) ja standardiväylän (AS-i) yhdistämisestä [ASI] (luokka 4).

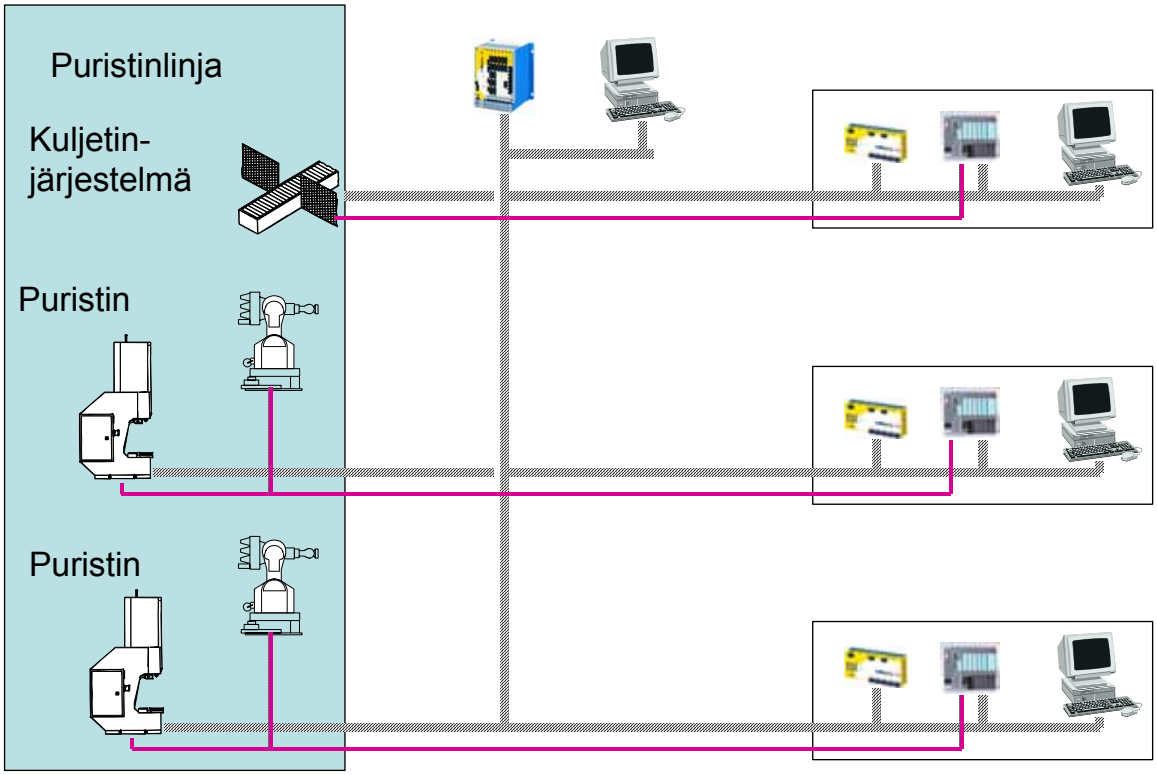
Toiminnan kuvaus (kuva 60)

- Esimerkissä on sekä turvallisuustietoa välittäviä moduuleja (raidoitetut moduulit) että tavallisia moduuleja. Kaikki moduulit viestivät samannäköisiä standardisanomia, jotka ovat lyhyitä (viesti on vain 4 bittiä pitkä). Jos turvamoduulit pystyvät toimittamaan omasta kooditaulukostaan poimittuja sanomia oikeassa järjestyksessä turvamoduulille (safety monitor), tämän lähdöt pysyvät ylhäällä. Lähtö putoaa alas, jos sanoma on muotoa ”0000” tai se poikkeaa odotetusta sanomamuodosta.
- Esimerkissä on vain yksi turvallinen lähtö. Esimerkin järjestelmä sopii kohteisiin, joissa on yksi pysyvä turvallinen tila (pysäytys, sähköt poissa). Jos esim. kaapeli menee poikki, niin moduulien pitää osata itsenäisesti siirtyä turvalliseen tilaan. Turvamoduulit ovat esimerkissä luokkaa 4 ja standardimoduulit luokkaa B.

Käyttö

- Käyttökohteena ovat ohjauspiirit [ASI].

4.5.17 SafeEthernet-turvaväyläjärjestelmä (luokka 4)

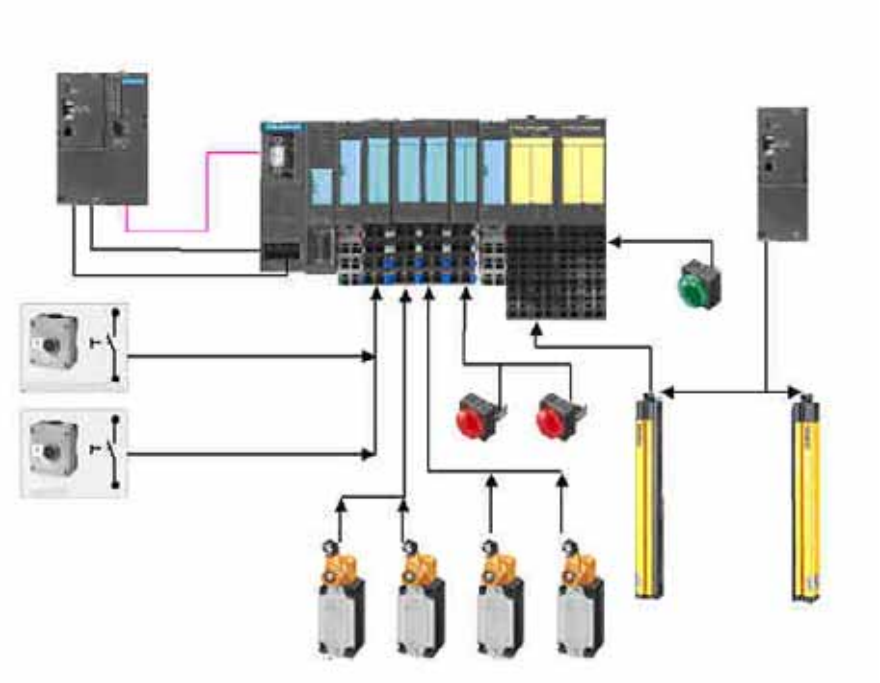


Kuva 61. Esimerkki turvaväylän (SafeEthernet), tavallisen väylän ja PC:n yhdistämisestä (turvaväyläluokka 4).

Toiminnan kuvaus (kuva 61)

- Esimerkissä puristimien turvatoimintoja ohjataan SafeEthernetillä (raidalliset viivat) ja muut ohjaukset on toteutettu tavallisella logiikalla. PC toimii lähinnä tiedonkeruutehtävissä, vaikka se onkin yhteydessä SafeEthernetiin. Samassa järjestelmässä voi olla erilaisia väyliä, ja tässä SafeEthernetissä voi olla sekä turvamoduuleja että tavallisia moduuleja. [HIMA]
- Yhden (turva)väylän järjestelmä sopii kohteisiin, joissa on yksi pysyvä turvallinen tila (pysäytys, sähköt poissa). Jos esim. kaapeli menee poikki, niin moduulien pitää osata itsenäisesti siirtyä turvalliseen tilaan.

4.5.18 ProfiSafe-turvaväylä ja turvalaitteen passivointi (luokka 4)

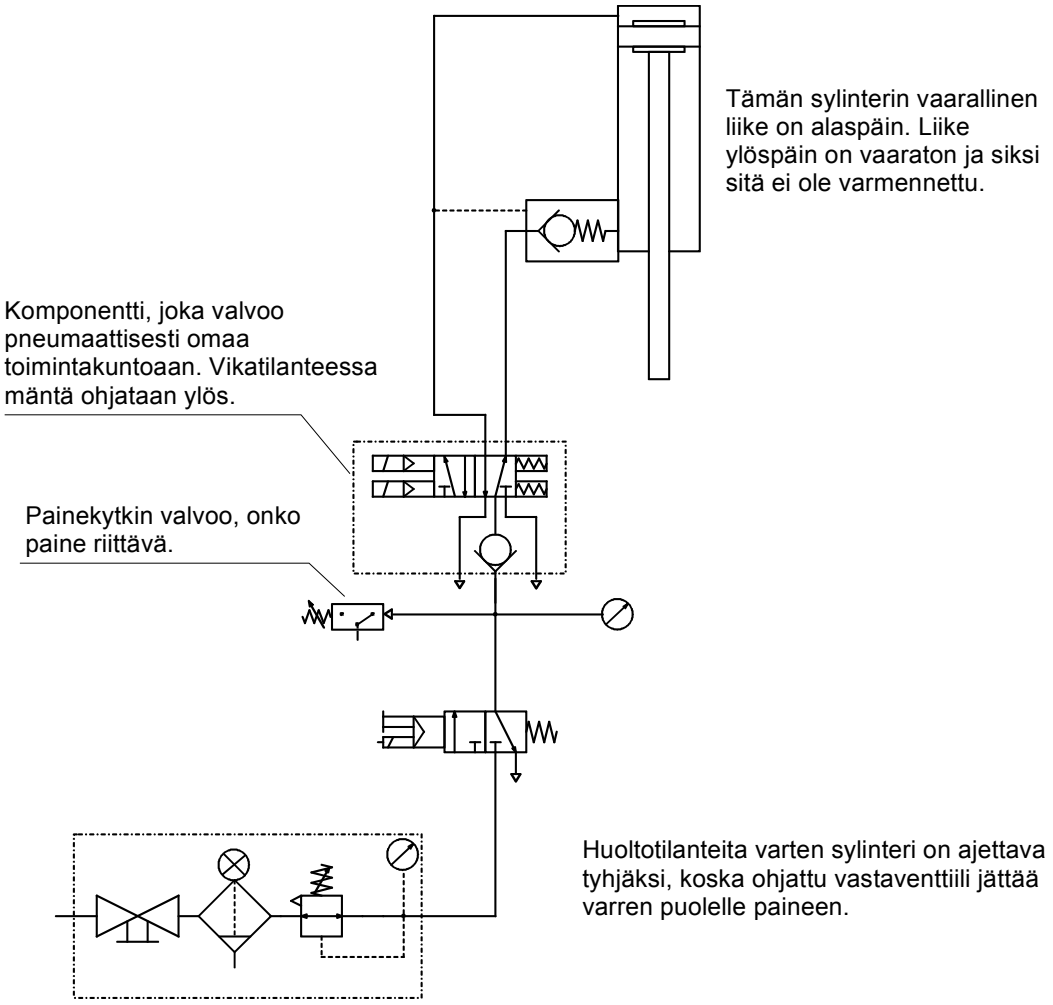


Kuva 62. Esimerkki turvaväylän (Profisafe) käytöstä valoverhon passivointi ja kuittauskytkennässä [Siemens].

Toiminnan kuvaus (kuva 62)

- Esimerkissä valoverho aiheuttaa normaalisti koneen pysäytyksen, mutta se voidaan passivoida rajakytkimillä. Kuittaus ja käynnistys tehdään erillisillä kytkimillä. Punaiset merkkilamput (kuvassa logiikan alapuolella) ilmaisevat passivoinnin olevan toiminnassa, ja oikealla oleva merkkilamppu ilmaisee koneen olevan toiminnassa. Esimerkin komponentit on kytketty Profisafe-väylään, joka sopii luokan 4 järjestelmiin.

4.5.19 Paineilmasylinterin ohjaus valvotulla kaksoisventtiilillä (luokka 4)



Kuva 63. Kaksoisventtiilin toimintaan perustuva sylinterinohjaus (luokka 4).

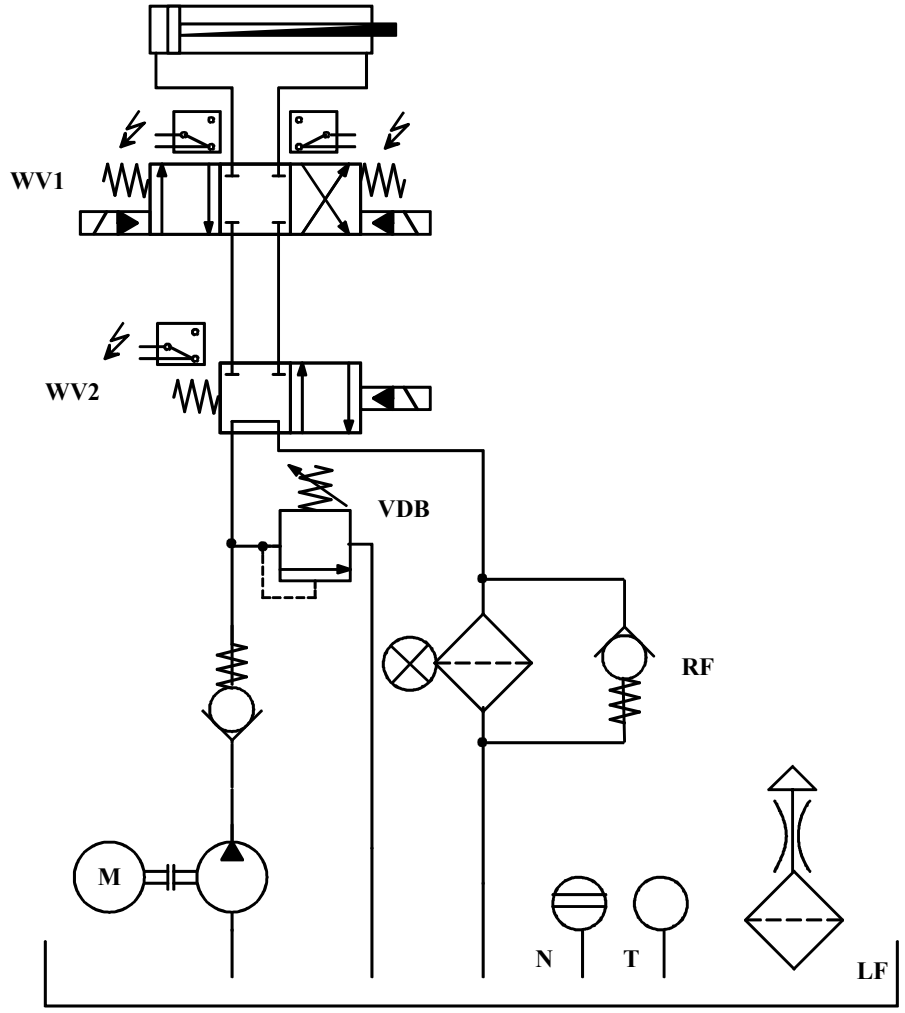
Toiminnan kuvaus (kuva 63)

- Kaksikarainen venttiili ohjaa pysäytystilanteessa paineen sylinterin kummallekin puolelle. Ohjattu vastaventtiili estää liikkeen alaspäin esim. letkurikkotilanteessa. Liike toteutuu vain, jos kaksoisventtiilin molemmat karat ovat samassa sallivassa asennossa. Muutoin ilma ohjataan ulos. Kaksoisventtiili valvoo omaa toimintaansa ja sitä ohjaavien sähköpiirien toimintaa. Paineilmaventtiili on kuitenkin huomattavasti hitaampi kuin sähköpiirit. Letkurikko voi aiheuttaa tarkoituksettoman liikkeen ylöspäin, mutta tämä oletetaan vaarattomaksi liikkeeksi.

Turvallisen toiminnan edellytykset

- Kaksoisventtiilin pitää olla riittävän suuri, jotta ilma poistuu vikatilanteissakin riittävän nopeasti. Varmistettu liike on kuvassa alaspäin, joten tässä esimerkissä oletetaan, että liike ylöspäin on vaaraton. Kuvaan ei ole piirretty nopeuden säätöä. [Malm & Järvenpää 1998] [BIA-Report 6/97e, 1997].

4.5.20 Hydraulisylinterin ohjaus valvotuilla venttiileillä (luokka 4)



Kuva 64. Esimerkki hydraulisesta ohjausjärjestelmästä (luokka 4).

Toiminnan kuvaus (kuva 64)

- Vaarallisia liikkeitä tai tiloja valvotaan kahdella suuntaventtiilillä, WV1 ja WV2. Jomman kumman suuntaventtiilin vikaantuminen ei johda turvatoiminnan menettämiseen. Viat kummassakin suuntaventtiilissä tunnistetaan.

Turvallisen toiminnan edellytykset

- Kummassakin suuntaventtiilissä on sähköinen karan aseman valvonta, jousikeskitys ja karan positiivinen peitto. Venttiilin sähköinen valvonta tulee toteuttaa esitetyn luokan mukaisesti.

Käyttö

- Käyttökohteena ovat hydraulisylinterin ohjauspiirit [BIA-Report 6/97e, 1997].

5. Ohjausjärjestelmän toiminnan havainnollistaminen

Laajat ohjausjärjestelmät ovat monimutkaisia, ja niiden toiminnan ymmärtäminen pelkkien piirikaavioiden perusteella on hidasta. Tämä pätee erityisesti turvatoimintojen varmistuksiin. Varmistukset eivät vaikuta ohjausjärjestelmän normaaliin toimintaan, vaan ne tulevat esille vasta vika- ja erikoistilanteissa. Tämän vuoksi niiden havaitseminen ilman selityksiä on usein vaikeaa. Varsinkin muutostilanteissa on tärkeää tietää vanhan järjestelmän turvatoimintojen varmistuksista, jotta uuteenkin järjestelmään pystytään järjestämään vastaavat varmistukset.

Ohjauspiirien visualisointi on yksi tapa parantaa piirikaavion lukijan mahdollisuuksia ymmärtää ohjausjärjestelmän toimintaa. Visualisointi voi olla toteutettu esim. videopätkänä, ”slide-show:na” tai erillisinä toimintaa esittävinä kuvina. Visualisoinnissa voidaan korostaa piirin toimintoja väreillä, liikkeellä tai paksumpana viivana. Vaikka visualisointi parantaakin piirien ymmärtämistä, se on kuitenkin tarkoitettu alan osaajille. Jos henkilö ei ole tottunut lukemaan piirikaavioita, on niitä vaikea ymmärtää, vaikka piirikaavioita visualisoitaisiinkin.

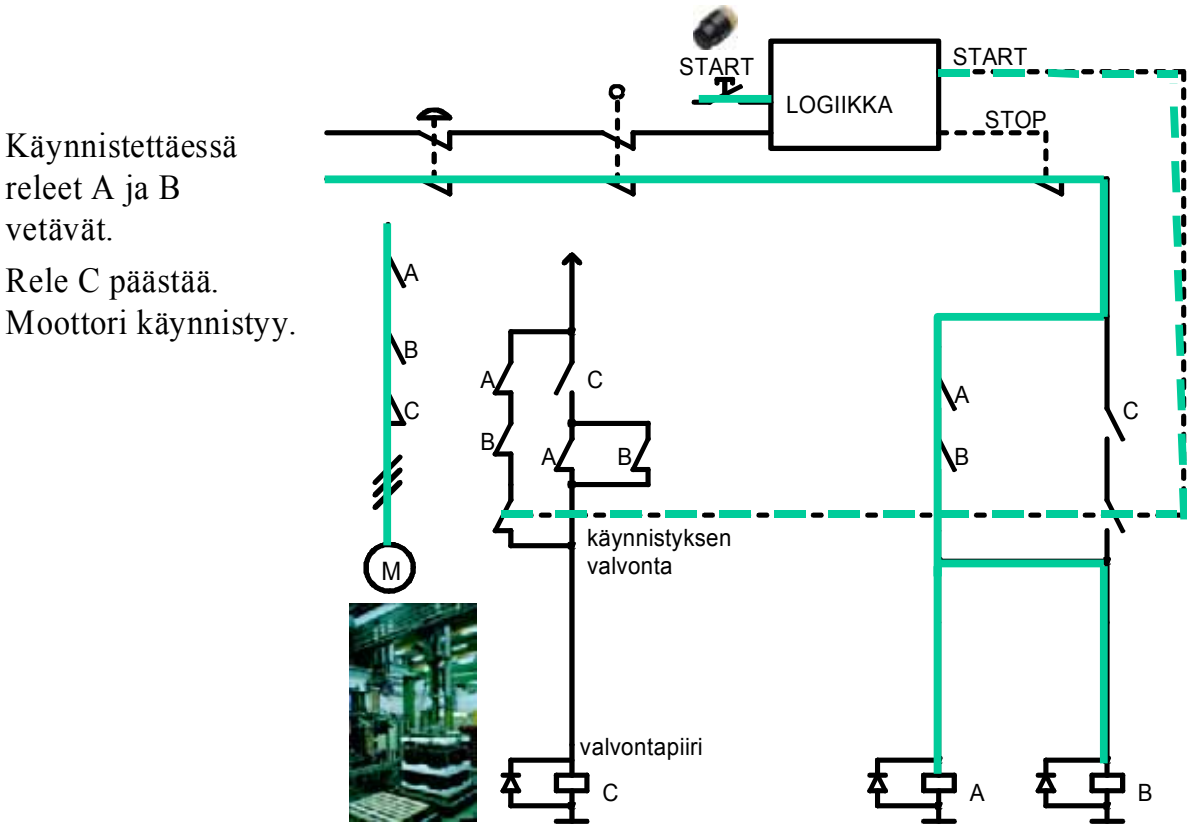
Esimerkki PowerPointilla toteutetusta visualisoinnista

Esimerkissä ovat perusideoina olleet kohtalaisen helppo soveltaminen eri piiriesimerkkeihin, värien käyttö, paksujen viivojen käyttö ja toimintojen vaiheittain tapahtuva eteneminen. PowerPoint-esityksessä kuvataan piirin käynnistystä, pysäytystä ja eri komponenttien vikaantumisesta seuraavia tilanteita. Esimerkkinä on pieni piirikaavio (vrt. kuvat 47 ja 65), jossa on toteutettu useita eri varmistuksia. Pysäyttävät releet on varmennettu, ja niiden vika paljastuu ennen seuraavaa käynnistystä. Käynnistys on varmistettu siten, että uudelleenkäynnistys ei voi toteutua, elleivät käynnistyksen toteuttavat kytkimet ole palautuneet alkuasentoon. Piirikaaviossa on myös logiikka, joka osaltaan varmistaa toimintaa, mutta varsinaiset turvatoiminnot on kuitenkin toteutettu sen ulkopuolella.

Esityksessä taustakuvana on koko ajan käsiteltävä piirikaavio. Piirikaaviosta voi koko ajan nähdä komponentit, ja kuvaa ei muuteta tai animoida. Animaatio, värilliset toimintaa kuvaavat viivat ja selventävät tekstit näkyvät piirikaavion päällä tai sivulla vain halutuissa näkymissä. Animaatiota on käytetty kuvaamaan eri toimintojen järjestystä. Tässä on käytetty paljon erillisiä kuvia, jotka esittävät toiminnan muutoksen eri vaiheita. Kuvien katsoja voi siten pysähtyä kuvaan haluamakseen ajaksi.

Vikatilanteita on PowerPoint-esityksessä tarkasteltu kuvavalikon kautta. Piirikaavion päälle kriittisten komponenttien kohdalle on piirretty salaman kuvia, joita klikkaamalla

saa esille kyseisen komponentin vikamuodot. Kuvissa on myös lyhyitä selostuksia eri varmistusten merkityksestä.



Kuva 65. Esimerkkikuva yhdestä piirin toiminnan vaiheesta.

Kokemuksia visualisoinnista

Tässä joitain kuvista tehtyjä huomioita:

- Animaatio etenee kohtalaisen nopeasti, ja piirikaaviota ensimmäistä kertaa katsova ei ehdi seurata sitä. Animaation hidastaminen toisaalta tekee piiriä tuntevalle käsittelyn hitaaksi. Animaatio ei siis ole piirien ymmärtämisen kannalta välttämätöntä, jos peräkkäiset kuvat on toteutettu hyvin.
- Kun tarkasteltava piirikaavio on jätetty pohjakuvaksi, voidaan kuvan päälle piirtää eri värillä esilletuotavia asioita nopeasti. Pohjakuvaan ei tehdä vahingossa muutoksia.
- Yhteen kuvaan ei kannata laittaa liian monia peräkkäisiä tapahtumia, vaan kannattaa käyttää useampia kuvia toimintojen kuvaamiseen.

6. Päätelmiä

Tässä julkaisussa esitetään turvallisuusteknisiä piiriratkaisuperiaatteita. Esimerkeissä keskitytään piirirakenteisiin, eikä niinkään esim. luotettavuuteen, komponenttivalintoihin tai lay-out-suunnitteluun, joilla myös on vaikutusta turvallisuuteen. Tämä valinta on tehty siksi, että luotettavuuteen liittyviä tekijöitä ei yleensä voida päätellä piirikaavioista. Samasta piirikaaviosta voidaan siis toteuttaa joko luotettava tai epäluotettava ratkaisu. Tosin monet piirikaavioistakin nähtävät suojaavat komponentit (esim. suodattimet, ylijännitepiikkien poistajat ja paineenrajoittimet) parantavat luotettavuutta. Yleisiä turvallisuusperiaatteita esitetään mm. lukuisissa standardeissa (mm. SFS-EN 954-1), mutta periaatteiden ymmärtäminen pelkästään periaatteita lukemalla on työlästä. Esimerkit helpottavat turvallisuusperiaatteiden ymmärtämistä. Ne auttavat näkemään, miten valvonta kattaa eri piirien osat ja toisaalta miten valvonta perustuu usein tiettyihin toimintasarjoihin. Esimerkkien ymmärtäminen edellyttää kuitenkin teknistä ymmärrystä, vaikka piirikaavioiden toimintaa visualisoitaisiinkin esim. luvussa 5 esitetyllä tavalla.

Esimerkit eivät kuitenkaan anna valmiita ratkaisuja sovelluksiin, vaan esitettyjä periaatteita pitää muokata omaan sovellukseen sopivaksi. Tässä julkaisuissa esitetään vain joitain periaateratkaisuja turvallisuusteknisten haasteiden toteuttamiseksi. Muitakin toteutustapoja on siis olemassa. Esimerkkien esittämisen riski joissain tapauksissa (esim. standardeissa) voi olla se, että lukijat käyttävät ainoastaan valmiita ratkaisuja eivätkä suunnittele uusia piiriratkaisuja.

Tässä julkaisussa esitetyt ratkaisut pitävät paikkansa ainoastaan tiettyjen ehtojen ollessa voimassa. Usein tiettyjen vikamuotojen todennäköisyys saadaan sopivilla toimenpiteillä niin pieneksi, että vikamuoto voidaan jättää huomioimatta.

Tietyn periaatteen turvatoiminta on mahdollista vesittää liittämällä kytkentään huonosti suunniteltuja piirirakenteita. Näin käy esim. kytkettäessä turvapiiri ohjaamaan yksittäistä ilman valvontaa olevaa relettä, joka edelleen ohjaa turvatoimintoa. Tällöin siis valvomattoman releen vika voi aiheuttaa vaaratilanteen, vaikka kytkennässä onkin käytössä turvapiiri.

Turvalogiikat ovat yleistymässä, ja niitä käytetään yhä useammin varsinkin turvarelekytkentöjen sijaan. Logiikat valvovat itseään monipuolisesti, ja niillä on mahdollista toteuttaa monipuolisia laitteisto valvontoja (HW). Ne tuovat kuitenkin mukanaan uuden riskitekijän: ohjelmistot. Pitkien ohjelmien oikeellisuutta on vaikea osoittaa. Turvalogiikoissa käytetään tyypillisesti suppeaa käskykantaa luotettavuuden lisäämiseksi. Tällä on toisaalta myös kääntöpuolensa. Jos turvalogiikalla haluaa toteuttaa monimutkaisen funktion, voi joutua tekemään tavalliseen logiikkakieleen nähden selvästi pidemmän ohjelman. Ohjelmistojen tarkastusmenetelmät ovat vuosien varrella kehittyneet, mutta silti pitkän ja monimutkaisen ohjelman tarkastaminen on haasteellista. Ohjelmistojen

validointi ei ole saavuttanut samaa uskottavaa tasoa kuin laitteiston validointi. Validoinnissa käytetään mm.

- testausta; Ohjelmistopolkujen laajojen kombinaatioiden vuoksi testaus jää suppeaksi.
- analyysejä; Analyyseillä tunnistetaan ohjelmistojen kriittisiä kohtia ja voidaan edellyttää näiltä sopivaa redundanssia ja diversiteettiä, mutta varsinaisten virheiden löytäminen on vaikeaa.
- auditoinnit ja läpikäynnit; Menetelmissä seurataan tyypillisesti ohjelmoijan ajattelua, ja siten uusien virheiden löytäminen voi olla vaikeaa.
- laadun varmistaminen; Menetelmillä varmistetaan ohjelmistojen tekemisen taustat, mutta varsinaisia virheitä ei löydetä.

Ohjelmistoista voidaan tuskin koskaan saada ”idioottivarmoja”. Testauksella ja tarkastuksella voidaan osoittaa ohjelmistovirheiden olemassaolo, mutta niillä ei voida osoittaa ohjelman virheettömyyttä. Ainakaan toistaiseksi ohjelmistovirheiden määrä lähdekielistä riviä kohden ei ole olennaisesti parantunut kolmenkymmenen viime vuoden kuluessa. Tosin virheiden syyt ovat monelta osin nykyään erilaisia. Ohjelmistovirheiden olemassaolo jouduttaneen siis hyväksymään, ja turvallisuuteen liittyvissä järjestelmissä pitää entistä enemmän kiinnittää huomiota vikasietoisuuteen ja kykyyn toipua virheistä. Turvallisesti käyttäytyvien ohjelmistojen kehittämisessä ja validoinnissa on kuitenkin vielä tutkimista.

Turvalogiikoista on edelleen kehitetty turvaväyliin perustuvia hajautettuja järjestelmiä. Niissä on keskusyksikkönä turvalogiikka, ja liikennöinti eri moduulien välillä on toteutettu parikaapelilla sarjamuotoisesti. Turvaväylän etuja turvalogiikkaan nähden ovat tyypillisesti kaapeleissa saavutettavat säästöt, laajan järjestelmän helpompi ymmärtäminen, kaapelointivirheiden väheneminen ja laajat diagnostiikkatiedon saantimahdollisuudet järjestelmän eri osista. Vastaavasti haittapuolena voi olla se, että liikennöintinopeus ei välttämättä riitä vielä nopeimpiin sovelluksiin, tai se, että johdon katkeamisen seurauksena voidaan menettää koko liikennöinti, tai että kaikki eivät ymmärrä hajautettujen järjestelmien periaatteita.

Perinteistä väyläliikennettä enemmän mahdollisuuksia antavia sovelluksia ovat verkot, kuten Internet ja langattomat verkot. Näiden käyttö lisää kuitenkin järjestelmään tunkeutumisen mahdollisuutta, ja tätä riskiä ei kaikissa kohteissa kannata ottaa. Verkkoliikenteestä saavutettavat hyödyt turvasovelluksissa eivät yleensä vielä ole riittäviä kustannuksiin ja riskeihin nähden. Erityisen pitkillä yhteyksillä, esim. rautatieliikenteen sovelluksissa, suljetuilla verkko- tai väyläratkaisuilla on etunsa.

Tulevaisuudessa ohjausjärjestelmien vastuulle tulee monia uusia kohteita, kun ”rautaa” korvataan ”järjellä” (vrt. luku 1). Tämän vuoksi turvallisuuteen liittyvät ohjausjärjestelmät yleistyvät. Eräs suuntaus on se, että laitevalmistajat tarjoavat valmiita turvallisia ohjausjärjestelmäpaketteja, joita koneensuunnittelijat soveltavat erilaisissa kohteissa.

Lähdeluettelo

ASI. AS-Interface Safety at Work – Safety now included. AS-International Association. 2000. 19 s. http://www.as-interface.com/asi/safetyenglish.ppt

Barthel H., Dönges E., Gräff U., Hannen H.-T., Kühn T., Lausberg G., Laux T. & Stripf W. Profibus-DP/PA. Profisafe, Profile for Failsafe Technology, V1.0. 1999. 56 s. http://www.itk.ntnu.no/fag/fordypning/SIE3092/SIE30AB/PDF/ProfiSafe-Profil-100e.pdf

Carlo Gavazzi -esite.

Categories for Safety-related Control Systems in Accordance with EN 954-1. 1997. BIA-Report 6/97e.

EN ISO 13849-2. 2003. Safety of machinery – Safety-related parts of control systems – Part 2: Validation. CEN. 55 s.

Hérard J., Sjöström H., Olsen O., Stålhane T., Juul Wedde. K., Løken T., Söderberg A., Malm T. & Hietikko M. 2000. "Round Robin Tests" of Safety-related Control System for Machinery – comparison of validation results. Nordtest Project 1504-00. 31 s.

Hérard J., Hedberg J., Kivipuro M., Malm T., Edler H., Sjöström H. & Strawinski T. 2003. Validation of communication in safety-critical control systems. Nordtest report. 104 s.

HIMA www-sivut. 14.7.2004. http://www.hima.com/default.asp

IEC 61508–1. 1998. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1: General requirements.

IEC 61508-2. 2000. Functional safety of electrical/electronic/programmable electronic safety-related system Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems.

IEC 61508–3. 1998. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 3: Software requirements.

IEC 61508–4. 1998. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 4: Definitions and abbreviations.

IEC 61508–5. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 5 Guideline on the application of Part 1.

IEC 61508-6. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6: Guidelines on the application of parts 2 and 3.

IEC 61508-7. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 7: Overview of techniques and measures.

IEC 62061 (draft). 2002. Safety of Machinery – Functional safety of electrical, electronic and programmable control systems for machinery. 44/380/CD. 90 s.

Kleinbreuer, W. 1997. Machinen und Gerätesicherheit. HVBG, BIA-Report 4/97. 241 s. + liitt. 49 s. ISBN 3-88383-449-1.

Malm, T., Kivipuro, M. & Tiusanen, R. 1998. Laajojen koneautomaatiojärjestelmien turvallisuus. Espoo: VTT Tiedotteita – Research Notes 1938. 72 s. ISBN 951-38-5410-8; 951-38-5411-6

Malm, T. & Järvenpää, J. 1998. Pneumatiikalla toteutetun kappaletavara-automaation turvallisuus. Espoo: VTT Tiedotteita – Research Notes 1886. 49 s. + liitt. 23 s. ISBN 951-38-5187-7; 951-38-5188-5

Pilz, Company and Product Information CD.

Pilz-esite.

Pilz-www-sivut. 14.7.2004.
http://www.pilz.com/english/products/safety/bus/concept.htm

prEN ISO 13849-1. 2004 (draft). Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design (ISO/DIS 13849-1:2004). CEN. 64 s.

SFS-EN 954-1. 1996. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Helsinki: Suomen Standardisoimisliitto. 64 s. Yhdenmukaistettu OJ No C 141, 97.05.08

SFS-EN 60204-1. 1997. Koneturvallisuus. Koneiden sähkölaitteisto. Osa 1: Yleiset vaatimukset. Helsinki: Suomen Standardisoimisliitto. 180 s. Yhdenmukaistettu 20.5.2000.

Siemens. 2002. Simatic Expert Communication. Safety Integrated Function Example 5. V 1.0. 15 s.

Siemens image database. 14.7.2004. Siemensin www-sivut. http://www3.ad.siemens.de/bilddb//index.asp?lang=en&nodeID=1000002&foldersopen

Liite A: Turvajärjestelmäesimerkki

Esimerkin taustaa

Tässä esimerkissä esitetään turvajärjestelmän suunnittelun eri vaiheita. Lopuksi päädytään turvatoimintoihin, jotka toteutetaan tässä turvalogiikalla.

Katkaisulinja 2 on AvestaPolarit Oy:n Tornion tehtaalla toimiva automaattilinja. Linja uusittiin 2002–2003, ja samalla linjan automaatiotasoa ja nopeutta nostettiin. Linjalla peltiä katkaistaan maksimissaan 40 m/min pellin liikkuessa. Turvajärjestelmä toteutettiin linjalle, koska automaatiotason nousu toi uusia riskejä, jotka haluttiin saada modernilla tavalla hallintaan. Turvajärjestelmän toimitti Mipro Oy.

Turvajärjestelmän suunnittelu aloitettiin automaatiojärjestelmän suunnittelun jälkeen. Tarjouskyselyn yhteydessä asiakas toimitti alustavan turvajärjestelmän määrittelyn, jota Mipro Oy:n projektipäällikkö tarkensi. Asiakas teki mekaniikan valmistajan toimittaman vaaratekijäluettelon pohjalta linjan riskianalyysin. Riskianalyysin perusteella havaittiin uusia vaaratekijöitä, joita perussuunnittelussa ei ollut huomioitu, joten turvajärjestelmän määrittelyä parannettiin jälleen.

Käyttöönoton yhteydessä havaittiin vielä joitakin puutteita. Esimerkiksi eräiden koneiden pysähtymisaika ei ollut riittävän lyhyt, jotta pääsy koneen luokse olisi voitu suojata valoverhoilla. Turvajärjestelmään tehtiin siten muutoksia mm. vaihtamalla valoverhot turvaportteihin.

Turva-alue 3 turvajärjestelmän suunnittelu

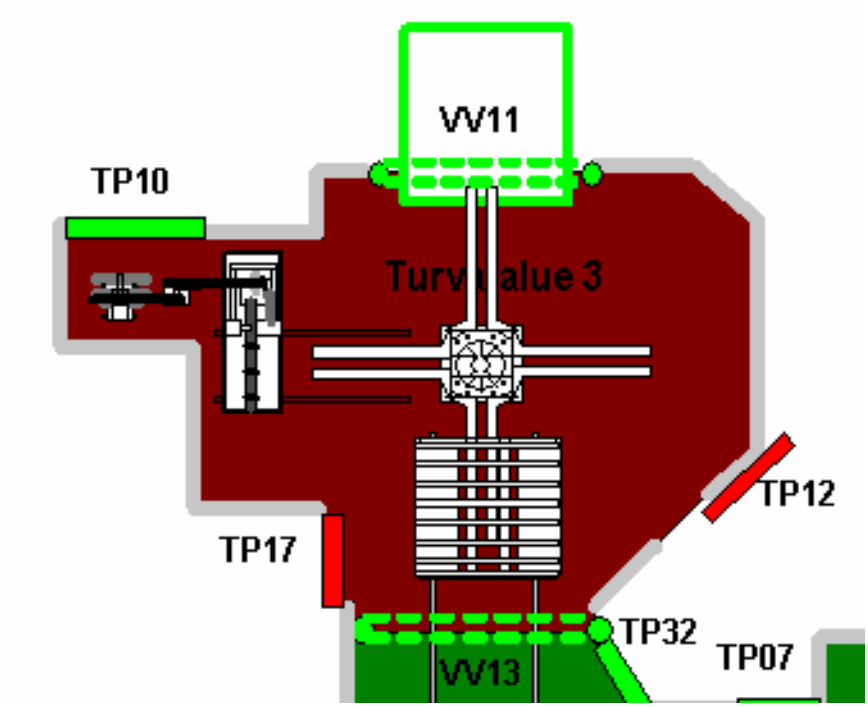
Turva-alueella 3 (turvajärjestelmän valvoma alue) on seuraavia laitteita: kääntöristi, rullansiirtovaunu (liikkuu kahdella alueella TA3 ja TA4), vihivaunu (liikkuu alueella TA3 ja linjan ulkopuolella), sitomakone. Kuva A1 esittää turva-aluetta 3 ja taulukko A1 lyhyesti eri koneisiin liittyvät tärkeimmät vaaratekijät.

Suunnittelussa piti ottaa huomioon se, että rullansiirtovaunun ja vihivaunun itsenäisen liikkumisen takia ei voitu käyttää turvaportteja.

Taulukko A1. Turva-alueella 3 olevat koneet ja niihin liittyvät tärkeimmät vaaratekijät.

Kone	Vaaratekijä
Kääntöristi	Kääntymisnopeus on melko hidas, mutta rullansiirtovaunun ja/ tai vihivaunun ollessa alueella litistymisvaara ilmeinen.
Rullansiirtovaunu	Liike on vaarallinen.
Vihivaunu	Tömäys ja litistymisvaara
Sitomakone	Liike asemapaikan ja kääntöristin välillä on vaarallinen. Sitominen on vaarallinen työvaihe.

Turva-alueelle pääsee kahdesta valoverhosta ja kolmesta turvaportista. Turva-alueella turvajärjestelmä keskustelee kahden ohjausjärjestelmän kanssa. Rullansiirtovaunu, kääntöristi ja vihivaunu ovat linjan ohjausjärjestelmässä. Sitomakoneella on oma erillinen ohjausjärjestelmänsä.



Kuva A1. Turva-alue 3 (turvajärjestelmän valvoma alue). TP = turvaportti, VV = valoverho.

Turvaportin ohjauskotelosta käyttäjä voi painaa ”sisään”-painiketta, jolloin turvajärjestelmä lähettää pysäytyspyynnön laitteiden ohjausjärjestelmille. Laitteet suorittavat mahdollisen sekvenssin loppuun, jonka jälkeen turvajärjestelmä havaitsee laitteiden tilatiedosta, että laitteet ovat pysähtyneet. Tämän jälkeen turvaportti aukeaa.

Alueen laitteiden käsiajot tehdään turva-alueen ulkopuolella olevasta ohjauskotelosta. Käsiajolla laitteiden liikkeet ovat hitaita, ja laitteet ovat käyttäjälle suorassa näköyhteydessä, joten liikkeet sallitaan alueen ollessa ns. vaaratilassa.

Vihivaunun ja rullansiirtovaunun tuleminen alueelle estetään, jos alue on vaaratilassa. Valoverhon passivointi on toteutettu saamalla tieto siirtovaunun asemasta sekä induktiosilmukasta ja vihivaunun paikkatiedosta. Siten passivoinnissa käytetty tieto on kahdennettu ja redundanttiset osat ovat toisistaan riippumattomia.

Alueella käytettäviä turvalaitteita ovat kuittaus- ja sisäänpyyntöpainikkeet, turvaportit, valoverhot ja valoverhojen passivointijärjestelmä.

Turva-alueen 3 toteutus

Turva-alueen ollessa vaaratilassa pysäytetään alueen laitteet ja kielletään rullansiirtovaunun ja vihivaunun tulo alueelle. Alueella oleva sitomakone on itsenäinen laite, jonka kanssa turvalogiikka kättelee suoraan.

TP10-portista kuljetaan sitomakoneelle. Pyydettäessä porttia auki avaus odottaa rullansiirtovaunua, jos rullantuonti ristille on kesken. Rullansiirtovaunun annetaan tuoda rulla ristille ja poistua turva-alueelle 4, ennen kuin porttien sallitaan avautua. Samoin, jos ristin pyöritys on menossa, annetaan sen pyöriä pääteasemaansa ennen porttien avauslupaa.

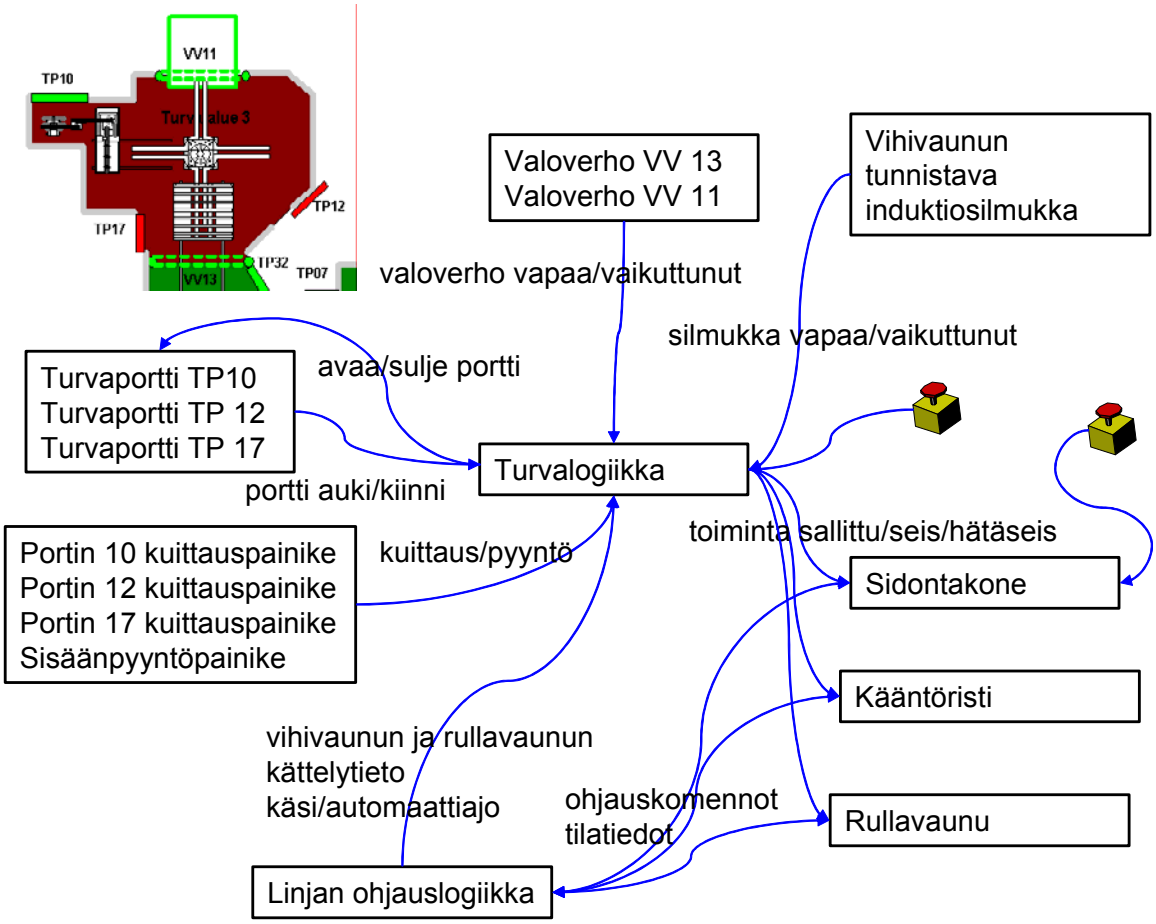
Vihivaunu käy hakemassa rullan vihiristiltä valoverhon VV11 läpi. Valokenno passivoidaan vihikättelyn ja induktiosilmukan avulla. Vihivaunun induktiosilmukalta ilmoitetaan tieto linjalogiikalle, joka estää ristin pyörityksen.

Jos valoverho 11 tai 13 laukeaa, turvajärjestelmä antaa seis-käskyn sekä sidontakoneelle että kääntöristille. Tämä pysäytys tapahtuu välittömästi. Pysäytyskäsky saattaa aiheuttaa sekvenssin keskeytymisen, joten alueelle mentäessä kannattaa käyttää turvaportteja, jos tilanne ei välttämättä vaadi välitöntä menoa alueelle.

TP12 sijaitsee päällekelaimen työskentelytasolta laskevien portaiden alapäässä. Portin toiminta on vastaava kuin TP10:llä. Pyydettäessä auki turvaporttia TP12 avautuu myös TP17. Porttiin asennetaan sisäpuolelle lukituskahva, jolla portti voidaan lukita mekaanisesti sisäpuolelta. Porttien kuittaus sallitaan ainoastaan kyseisten porttien kuittauspainikkeista. Näin mahdollistetaan läpikulku linjan taakse ja sitomakoneelle.

VV13 sijaitsee turva-alueiden 3 ja 4 välissä. Valoverho passivoidaan rullansiirtovaunun liikkeiden mukaan. Passivoinnissa käytetään turvalogiikan ja linjanlogiikan kättelyä. Valoverhon ollessa lauennut tai passivoitu leviää vaaratila molemmille alueille. Sidontakoneella on oma hätäpysytys, joka vaikuttaa vain sidontakoneeseen.

Kuva A2 esittää eri koneiden ja turva- sekä ohjauslaitteiden välistä kommunikointia. Turvalogiikan ohjelma on toteutettu varsin pitkälle tilakoneena, joka vaihtaa tilaansa sallitusta toiseen. Jos tila ei vastaa anturitietoja, annetaan hätäpysäytys.



Kuva A2. Turva-alueen 3 turvalaitteiden ja koneiden väliset yhteydet.

Julkaisija

Julkaisun sarja, numero ja raporttikoodi

VTT Tiedotteita 2264
VTT–TIED–2264

Tekijä(t)
Malm, Timo & Kivipuro, Maarit

Nimeke

Turvallisuuteen liittyvät ohjausjärjestelmät konesovelluksissa Esimerkkejä

Tiivistelmä

Automaattisten järjestelmien nopeutuessa ja monimutkaistuessa koneiden turvallisuus kohdentuu yhä useammin ohjausjärjestelmään, jonka viat voivat johtaa turvatoimintojen menettämiseen. Tämä tulee esiin tilanteissa, joissa kone suorittaa tehtävää, jonka väärä toiminta voi aiheuttaa vaaratilanteen ihmisen ollessa koneen vaikutuspiirissä. Turvallisuuteen liittyvät standardit antavat hyvän perustan riittävän turvallisuustason saavuttamiseksi. Standardien vaatimusten ja ohjeiden omaksuminen vaikeasta ”lakitekstistä” on suunnittelijoille usein työlästä. Osa turvallisuusperiaatteista voi jäädä huomioimatta tai soveltamatta. Sopivat periaatteelliset esimerkit helpottavat turvallisuusperiaatteiden omaksumista, ja niitä voidaan soveltaa myös omissa suunnitelmissa. Tässä julkaisussa esitetään esimerkkikirjasto turvallisuuteen liittyvistä koneautomaation ohjausjärjestelmistä. Esimerkit ovat periaatteellisia, yleispäteviä ja suunnittelijan sovellettavissa käytetyistä komponenteista riippumatta. Julkaisussa ei esitetä valmiita teknisiä ratkaisuja vaan turvallisuusperiaatteita graafisessa muodossa. Esimerkit on luokiteltu standardin SFS-EN 954-1 (EN ISO 13849-1) mukaan, koska tämän standardin luokittelu perustuu piirirakenteisiin. Siten piirikaaviosta on pääteltävissä esimerkkiratkaisun standardinmukainen luokka. Kolmesta esimerkistä on tehty myös PowerPoint-animaatiot, joissa näkyvät vaiheittain eri toiminnat ja vikatilanteiden kehittymiset. Tämäntyyppinen visualisointi helpottaa ymmärtämistä mutta edellyttää kuitenkin taitoa lukea piirikaavioita.

Avainsanat
safety systems, safety principles, safety standards, control system safety

Toimintayksikkö
VTT Tuotteet ja tuotanto, Tekniikankatu 1, PL 1307, 33101 TAMPERE

ISBN			Projektinumero
951–38–6500–2 (nid.) 951–38–6501–0 (URL: http://www.vtt.fi/inf/pdf/)			G2SU00322
Julkaisuaika Lokakuu 2004	Kieli Suomi, engl. tiiv.	Sivuja 90 s. + liitt. 4 s.	Hinta B
Projektin nimi Turvallisuuskriittiset ohjausjärjestelmät konesovelluksissa Esimerkkejä		Toimeksiantaja(t) Työsuojelurahasto	
Avainnimeke ja ISSN VTT Tiedotteita – Research Notes 1235–0605 (nid.) 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)		Myynti: VTT Tietopalvelu PL 2000, 02044 VTT Puh. (09) 456 4404 Faksi (09) 456 4374	

Published by

Series title, number and
report code of publication

VTT Research Notes 2264
VTT–TIED–2264

Author(s)
Malm, Timo & Kivipuro, Maarit

Title

Safety-related control systems in machinery
Examples

Abstract
The safety of an automated machine is depending increasingly on the control system, because systems are getting faster and more complex. More and more often the operator or driver is not able to control the system quick or well enough to guarantee alone the safety, but he needs the help of the safety system. However, deficiencies or failures in the control system of a machine may lead to a dangerous loss of safety functions. Safety standards give a good basis to reach adequate safety level. However, it is often hard to adopt safety requirements and guidelines purely from standard text. Suitable, generic examples help to adopt the safety principles and they can be applied to designers own solutions. This report presents an example library concerning safety related machine control systems. The examples are classified according to standard SFS-EN 954-1. The classification of the standard is depending on circuit architecture and therefore the category can be concluded from diagrams. A PowerPoint animation based on three examples was also created. Animation helps in understanding safety principles, but knowledge about circuit diagrams is needed.

Keywords
safety systems, safety principles, safety standards, control system safety

Activity unit
VTT Industrial Systems, Tekniikankatu 1, P.O.Box 1307, FIN–33101 TAMPERE, Finland

ISBN	Project number
951–38–6500–2 (soft back ed.) 951–38–6501–0 (URL: http://www.vtt.fi/inf/pdf/)	G2SU00322

Date	Language	Pages	Price
October 2004	Finnish, Engl. abstr.	90 p. + app. 4 p.	B

Name of project	Commissioned by
Safety-related control systems in machinery Examples	The Finnish Work Environment Fund

Series title and ISSN	Sold by
VTT Tiedotteita – Research Notes 1235–0605 (soft back edition) 1455–0865 (URL: http://www.inf.vtt.fi/pdf/)	VTT Information Service P.O.Box 2000, FIN–02044 VTT, Finland Phone internat. +358 9 456 4404 Fax +358 9 456 4374

Ohjausjärjestelmien turvallisen toiminnan merkitys kasvaa järjestelmien nopeutuessa, monimutkaistuessa ja korvattaessa ”rautaa järjellä”. Ohjausjärjestelmällä on merkittävä vastuu turvallisuudesta silloin, kun sen väärä toiminta voi johtaa vahinkoon. Monet standardit antavat hyviä ohjeita turvallisen ohjausjärjestelmän toteuttamiseksi, mutta suunnittelijoiden on usein vaikea omaksua kaikkia ohjeita ja vaatimuksia pitkistä teksteistä. Julkaisuun on kerätty esimerkkikirjasto, joka helpottaa turvallisuusperiaatteiden omaksumista. Esimerkit ovat periaatteellisia, yleispäteviä ja suunnittelijan sovellettavissa käytetyistä komponenteista riippumatta. Esimerkit on luokiteltu standardin SFS-EN 954-1 (EN ISO 13849-1) mukaan.

Tätä julkaisua myy
VTT TIETOPALVELU
PL 2000
02044 VTT
Puh. (09) 456 4404
Faksi (09) 456 4374

Denna publikation säljs av
VTT INFORMATIONSTJÄNST
PB 2000
02044 VTT
Tel. (09) 456 4404
Fax (09) 456 4374

This publication is available from
VTT INFORMATION SERVICE
P.O.Box 2000
FIN–02044 VTT, Finland
Phone internat. + 358 9 456 4404
Fax + 358 9 456 4374

ISBN 951–38–6500–2 (nid.)
ISSN 1235–0605 (nid.)
ISBN 951–38–6501–0 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455–0865 (URL: http://www.vtt.fi/inf/pdf/)