Tampereen yliopisto

Arto Vihinen

# STEER BY WIRE -OHJAUKSEN VAATIMUKSET TYÖKONEISSA

Tekniikan ja luonnontieteiden tiedekunta
Diplomityö
Toukokuu 2019

# TIIVISTELMÄ

Arto Vihinen: Steer by wire -ohjauksen vaatimukset työkoneissa
Diplomityö
Tampereen yliopisto
Automaatiotekniikan tutkinto-ohjelma
Toukokuu 2019

---

Ajoneuvojen ohjausmenetelmät ovat kehittyneet viime vuosina merkittävästi, ja sähköinen ohjaus on askel kohti etäohjattavia ja itsenäisiä koneita. Sähköisen ohjauksen suurimpia etuja ovat yksinkertainen fyysinen rakenne, ohjauksen tarkkuus sekä ohjelmoitavuus, minkä vuoksi se on jo vakiinnuttanut asemansa lentokoneiden ohjausmenetelmänä. Pyörillä liikkuvien ajoneuvojen ohjauksen sähköistämisen suurimpia haasteita ovat ohjauksen luotettavuus sekä lainsäädännön asettamat vaatimukset.

Tämän diplomityön tavoitteena on selvittää työkoneiden steer by wire -ohjaukselle asetetut vaatimukset. Tutkimuksen oleellinen osa on selvittää työkoneita koskevien lainsäädännön ja kansainvälisten standardien asettamat vaatimukset. Lainsäädännössä ohjaukselle on asetettu yleiset vaatimukset, ja sen tukena käytetään standardeja, joissa paneudutaan teknisiin ominaisuuksiin ja vaatimuksiin. Standardit jakautuvat A-, B ja C-tason standardeihin, ja suunnittelussa käytettävät standardit ovat riippuvaisia koneen tyypistä. Työkoneiden ohjausta koskeva C-tason standardi määrittää ajoneuvolta vaadittavat ominaisuudet, eri nopeusluokkia koskevat vaatimukset sekä ohjauksen toimivuuden todentamiseen käytettävät testiradat. Ohjausjärjestelmä on steer by wire -ohjauksen kriittinen osa, ja siihen kuuluvia vaatimuksia käsitellään B-tason standardeissa. Turvallisuus ja luotettavuus ovat tärkeimpiä ohjaukselta vaadittavia ominaisuuksia, minkä vuoksi A-tason standardissa tarkastellaan riskien arviointia.

Tutkimuksen perusteella voidaan todeta, että steer by wire -ohjauksen soveltaminen työkoneissa on riippuvainen ajonopeudesta sekä toimintaympäristön vaatimuksista. Rinnakkaisten ohjauskanavoiden hyödyntäminen lisää ohjauksen luotettavuutta, ja mahdollistaa ohjauksen säilymisen yksittäisessä vikaantumistilanteessa. Yli 20 km/h ajonopeuden koneilta redundanttiset ohjauskanavat ovat pakollisia. Työkoneilla, joiden korkein ajonopeus alittaa 20 km/h, redundanttisten ohjauskanavien tarve määräytyy työkoneen riskienarvioinnissa saavutetun tason mukaisesti.

Avainsanat: Steer by wire, ohjausmenetelmät, suoritustaso, riskien arviointi, ISO 5010, SFS-EN ISO 13849, SFS-EN ISO 12100

# ABSTRACT

Arto Vihinen: Requirements of Steer by wire in machinery
Diplomityö
Tampere University
Automation Engineering
May 2019

---

The steering methods of vehicles has developed considerably over the last few years, and the steer by wire is step towards remote control and autonomous vehicles. The greatest benefits of steer by wire are simple physical structure, steering accuracy and programmability, which are the main reasons why similar steering method, fly by wire is widely used in aircrafts. The challenges of implementing steer by wire in other machines and vehicles are reliability and the requirements of legislation.

The goal of this thesis is to define the requirements of steer by wire in machines. The pivotal factor of the thesis is to define the current state of legislation and the international standards. The legislation only describes the general steering requirements whereas the standards specifies the technical properties and requirements for steering. Standards are divided into A-, B and C-level standards, and each type of machines uses own set of standards. The C-level standard of the steering of earth-moving machines defines the needed technical requirements, requirements of various operating speeds and the test tracks which are used for verification of the requirements. The control system is a critical part of the steering system and the requirements are defined separately in B-level standards. Safety and reliability are the most important factors of steering which is why risk assessment is covered in A-level standard.

Based on this research, the requirements of steer by wire are dependable of the maximum operating speed of the vehicle and the requirements of the operating environment. The use of redundant control channels increases the reliability of the steering and enables the vehicle to maintain steering in case of a single failure. The redundant control channels are compulsory when the maximum speed of the vehicle exceeds 20 km/h. The demand of redundant control channels with vehicles with maximum speed of under 20 km/h is defined through the risk assessment.

Keywords: Steer by wire, steering methods, performance level, risk assessment, ISO 5010, SFS-EN ISO 13849, SFS-EN ISO 12100

# ALKUSANAT

Diplomityöni on tehty Tampereen teknillisen yliopiston, nykyisen Tampereen yliopiston, automaatiotekniikan tutkinto-ohjelmassa. Työ päättää pitkäksi venyneen 7 vuoden taipaleeni opiskelijana, minkä aikana olen oppinut paljon niin yliopistomaailmassa, Saksan vaihto-opiskeluvuotenani kuin työelämässäkin. Haluankin kiittää kaikkia matkan varrella minua tukeneita henkilöitä. Erityisesti haluan kiittää hydrauliikan laitoksen kärsivällisiä professoreita ja muita opetukseen osallistuneita henkilöitä, jotka ovat mahdollistaneet tutkintoni suorittamisen, sekä kollegoitani Parker Hannifinilla.

Suurimmat kiitokset osoitan perheelleni ja ystävilleni, jotka ovat minua opinnoissani tukeneet ja kannustaneet. Kiitän myös MJTJP:n jäsenistöä mittaamattoman arvokkaasta tuesta opintojen ohessa ja sen ulkopuolella.

Vantaalla, 16.05.2019

Arto Vihinen

# SISÄLLYSLUETTELO

# KUVALUETTELO

# LYHENTEET JA MERKINNÄT

| | |
|---|---|
| $B_{10D}$ | Toiminta-jaksojen lukumäärä ennen kuin 10 % komponenteista vaarallisesti vikaantunut |
| CCF | engl. Common cause failure, yhteisvikaantuminen |
| CEN | ransk. Comité Européen de Normalisation |
| Cenelec | engl. European Committee for Electrotechnical Standardization |
| DC | engl. Diagnostic coverege, Diagnostiikan kattavuus |
| EMC | engl. electromagnetic compatibility, sähkömagneettinen yhteensopivuus |
| FMEA | engl. Failure mode and effects analysis, vika- ja vaikutusanalyysi |
| FTA | engl. Fault tree analysis, vikapuuanalyysi |
| I | Tuloyksikkö |
| $i_m$ | Liitäntävälineet |
| IFA | saks. Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung |
| ISO | engl. International Organization of Standardization |
| L | Logiikka |
| LS | engl. Load sensing, kuorman tunteva |
| m | Valvonta |
| $MTTF_D$ | engl. Mean time to dangerous failure, Keskimääräinen aika vaaralliseen vikaantumiseen |
| O | Lähtöyksikkö |
| OTE | Testauslaitteiston lähdöt |
| $PFH_D$ | engl. Probability of dangerous failure per hour, Vaarallisen vikaantumisen todennäköisyys tuntia kohden |
| PL | engl. Perfomance Level, Suoritustaso |
| SBW | engl. Steer by wire, langallinen ohjausmenetelmä |
| SIL | engl. Safety Integrity Level, turvallisuuden eheyden taso |
| SRP/CS | Safety Related Parts of Control System |
| TFD | engl. Tactile feedback device |
| TE | Testauslaitteisto |

| | |
|---|---|
| $b_e$ | Ajoneuvon etuakselin pituus |
| $b_t$ | Ajoneuvon takaakselin pituus |
| $d_{op}$ | Keskimääräinen toiminta-aika (päivää vuodessa) |
| $DC_{avg}$ | Keskimääräinen diagnostiikan kattavuus |
| $h_{op}$ | Keskimääräinen toiminta-aika (tuntia päivässä) |
| $k$ | Runko-ohjatun ajoneuvon keskinivelen sijainti (0…1) |
| $L$ | Nivelten välinen pituus |
| $MTTF_{Di}$ | Yksittäisen komponentin vikaantumisaika |
| $n_{op}$ | Keskimääräinen toimintajaksojen lukumäärä vuodessa |
| $R$ | Ajoneuvon pyörän kääntösäde |
| $R_{es}$ | Ajoneuvon sisäetupyörän kääntösäde |
| $R_{eu}$ | Ajoneuvon ulkoetupyörän kääntösäde |
| $R_{max}$ | Ajoneuvon suurin kääntösäde |
| $R_{min}$ | Ajoneuvon pienin kääntösäde |
| $R_{ts}$ | Ajoneuvon sisätakapyörän kääntösäde |
| $R_{tu}$ | Ajoneuvon ulkotakapyörän kääntösäde |
| $T_{10D}$ | Toiminta-aika, mihin mennessä 10 % komponenteista vaarallisesti vikaantunut |
| $t_{toimintajakso}$ | Kahden peräkkäisen toimintajakson alkamisajankohdan välinen keskimääräinen aikaväli (sekuntia) |

| | |
|---|---|
| X | Tuntien lukumäärä vuodessa |
| β | Yhteisvikaantumisalttius |
| $\theta$ | Ajoneuvon kääntökulma |
| $\theta_{es}$ | Ajoneuvon sisäetupyörän kääntökulma |
| $\theta_{eu}$ | Ajoneuvon ulkoetupyörän kääntökulma |
| $\lambda_D$ | Havaitsemattomat vaaralliset vikaantumiset |
| $\lambda_{DD}$ | Havaitut vaaralliset vikaantumiset. |

# 1. JOHDANTO

Ajoneuvojen ohjaus on perinteisesti toteutettu mekaanisella tai hydraulisella yhteydellä ohjauselementin sekä ohjattavien pyörien välillä. Ohjausmenetelmiä on kehitetty ja hiottu viimevuosikymmeninä paljon, mutta vielä nykyäänkin suurimmassa osassa uusissa ajoneuvoissa käytetään mekaanista linkkiä kuljettajan ja pyörien välillä. Viimeistään viimeisten vuosikymmenten aikana tekniikan kehittyminen on mahdollistanut täysin sähköisen ohjauksen.

Steer by wire (SBW)-ohjauksessa renkaiden ja ohjauselementin, kuten ohjauspyörän, välillä ei ole mekaanista kytkentään, vaan ohjaus tapahtuu sähköisesti sensoreiden ja ohjausyksiköiden avulla. Se mahdollistaa ajoneuvon ohjaukselle yksinkertaisemman ja kevyemmän mekaanisen rakenteen sekä korkeamman ohjaustarkkuuden. SBW-ohjaus käyttää energiaa ainoastaan ohjaustyön aikana, minkä ansiosta se on perinteisiä hihnakäyttöisiä hydraulisia ohjausmenetelmiä energiatehokkaampi. [1] SBW-ohjaus ei ole konseptina uusi, vaan lentokoneteollisuudessa vastaavaa Fly by wire – ohjausta on käytetty kaupallisissa lentokoneissa jo 1980-luvulta lähtien [2]. SBW-ohjausta on hyödynnetty myös raskaissa metsäkoneissa. [3] Sähköinen ohjaus on ensimmäinen askel kohti etäohjausta ja itsenäisiä ajoneuvoja.

Tämän diplomityön tarkoituksena on selvittää standardien asettamia vaatimuksia liikkuville työkoneille, sekä tarkastella erilaisia mahdollisuuksia toteuttaa ajoneuvon ohjaus ilman ohjauselementin ja pyörien välistä mekaanista yhteyttä. Pääpainona on selvittää sähköiseen tiedonsiirtoon perustuva ohjausmenetelmän, SBW:n käyttövaatimuksia sekä käyttömahdollisuuksia liikkuvissa työkoneissa. Ohjausta koskevien vaatimusten täyttäminen on mahdollista toteuttaa useilla eri tavoilla, ja vaatimukset ovat riippuvaisia koneen tyypistä sekä maksimi ajonopeudesta. Täysin uuden ohjausjärjestelmän suunnitteluun sekä hyväksymiseen kuluva aikajana on hyvin pitkä, minkä johdosta tässä työssä tarkastellaan ainoastaan standardien asettamia vaatimuksia, eikä täydellistä tyyppihyväksyttyä järjestelmää.

Toisessa kappaleessa käsitellään yleisimpiä pyörillä liikkuvien ajoneuvojen ohjausmenetelmiä ja -mekanismeja. Ajoneuvot voidaan luokitella ohjaustyössä hyödynnettävän teholähteen mukaan käsikäyttöisiin, tehostettuihin ja täysin tehostettuihin ohjauksiin [4]. Kappaleessa käsitellään tyypillisiä liikkuvissa työkoneissa

hyödynnettäviä ohjausmenetelmiä, ja sivutaan kevyemmän liikenteen ajoneuvojen ohjausmenetelmiä. Lisäksi kappaleessa käsitellään yksinkertaistettua SBW-ohjauksen rakennetta, ja ohjauksen tuomia mahdollisuuksia.

Kolmannessa kappaleessa tarkastellaan lainsäädännön asettamia vaatimuksia, sekä standardien merkitystä eurooppalaisen lainsäädännön tukena. Lainsäädännön asettamat vaatimukset kattavat koneelta vaadittavat tekniset vaatimukset erittäin suppeasti, minkä vuoksi konetta koskevien yhdenmukaistettujen standardien vaatimusten mukaisen suunnittelun katsotaan täyttävän lainsäädännön asettamat vaatimukset. Kappaleessa paneudutaan pyörillä liikkuvien työkoneiden C-tyypin standardin ISO 5010 (engl. International Organization of Standardization) asettamiin vaatimuksiin, sekä tarkastellaan maa- ja metsätalous koneiden asetusta 2015/208.

Neljännessä kappaleessa käsitellään koneturvallisuuden riskienhallintaa, joka pohjautuu konedirektiiviin ja standardiin ISO 12100. Suunnittelun ensisijaisena tavoitteena on poistaa kaikki havaitut riskit luontaisilla suunnittelumenetelmillä. Tämän ollessa mahdotonta, voidaan hyödyntää esimerkiksi suojausteknisiä laitteita. [5] Kappaleessa paneudutaan riskin arvioinnin ja pienentämisen prosessiin, sekä tarkastellaan erilaisia riskin pienentämisen keinoja.

Ohjausjärjestelmältä vaadittavia ominaisuuksia käsitellään kappaleessa viisi. Kappaleessa käsitellään standardissa ISO 13849-1 esiteltäviä määrällisiä ja laadullisia vaatimuksia, sekä ohjausjärjestelmien suunnittelun apuna käytettävää SISTEMA-ohjelmistoa. Ohjausjärjestelmän turvallisuutta arvioidaan suoritustasojen (engl. Performance Level, PL) avulla, jotka ovat laskettavissa määrällisten arvojen, kuten vikaantumisaikojen ja diagnostiikan kattavuuksien avulla. Vastaavasti ohjausjärjestelmän laadullisiin arvoihin luetaan muun muassa käytettävissä olevat ohjelmistot ja ympäristöolosuhteet, joiden täyttyminen on dokumentoidusti osoitettava.

Viimeisessä, eli kuudennessa kappaleessa tarkastellaan kahta erilaista SBW-ohjausjärjestelmän rakennetta. Ensimmäinen järjestelmä on yksinkertainen yksikanavainen ohjausjärjestelmä, jonka olematon vikasietoisuustaso rajoittaa käytettävyyttä. Toinen on redundanttinen järjestelmä, jollaisella on mahdollista saavuttaa vaadittava vikasietoisuustaso. Molemmissa järjestelmissä tarkastellaan venttiiliohjattua järjestelmään, jotka ohjaavat vaadittavan tilavuusvirran sylintereille. Järjestelmät kuvaavat ylätason suunnittelua, eivätkä käsittele määrällisten tai laadullisten vaatimusten täyttymistä.

# 2. OHJAUSMENETELMÄT

Ajoneuvon ohjaustyypit voidaan jakaa ohjaukseen käytettävän teholähteen mukaan käsikäyttöisiin, tehostettuihin - ja täysin tehostettuihin ohjauksiin. Perinteisessä käsikäyttöisessä ohjauksessa hyödynnetään ainoastaan ajoneuvon ohjaajan lihasvoimaa. Vastaavasti tehostetussa ohjauksessa hyödynnetään yhtä tai useampaa teholähdettä, kuten hydraulipumppua tai akkua. Tehostetuissa ohjauksissa on ohjattavien pyörien sekä ohjauselementin välillä aina mekaaninen tai hydraulinen yhteys, minkä ansiosta ajoneuvoa on mahdollista ohjata myös teholähteen vikaantuessa. Vikaantumistilanteessa kuljettajalta vaadittava ohjaustyö on tosin merkittävästi normaalia suurempi. Täysin tehostetussa ohjauksessa ohjaustyöhön käytettävä voima saadaan yhdestä tai useammasta teholähteestä. Ohjaus voi sisältää tehostetun ohjauksen tavoin mekaanisen tai hydraulisen linkin ohjauselementin ja ohjattavien pyörien välillä, mutta kuljettajan ei ole mahdollista ohjata ajoneuvoa puhtaasti lihasvoimalla ohjausliikkeen raskaudesta tai mekaanisen yhteyden puuttumisesta johtuen. [4, 6]

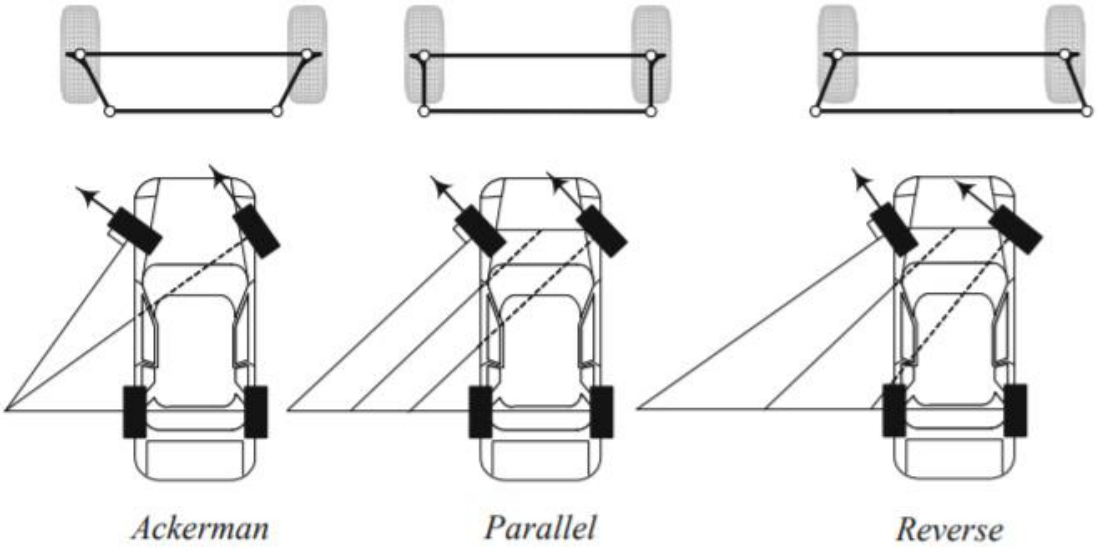
Täysin käsikäyttöisiä ohjauslaitteita käytetään nykypäivänä ainoastaan kevyissä sovelluksissa, ja tieliikenteen ajoneuvoissa käytetään lähes ainoastaan tehostettuja ohjausjärjestelmiä. Tehostetut ohjauslaitteet käyttävät edelleen samoja mekanismeja liikkeen välittämiseen pyörille kuin käsikäyttöiset, mutta ne tyypillisesti sisältävät hydrauli- ja/tai sähköpiirin, jotka alentavat kuljettajalta vaadittavaa voimaa sekä lyhentävät ohjausliikkeen laajuutta. Täysin tehostettuja ohjauksia on perinteisesti käytetty lähinnä raskaissa työkoneissa, joiden kääntämiseen vaadittava ohjaustyö on merkittävästi henkilöautoja suurempi. Steer by wire -ohjauksessa ei ole mekaanista yhteyttä pyörien ja ohjauselementin välissä, jolloin se luokitellaan täysin tehostetuksi ohjaukseksi.

Tyypillisiä ajoneuvojen ohjaustapoja ovat Ackermann-ohjaus, runko-ohjaus sekä liukuohjaus. Ackermann-ohjaus on yleisin käytössä oleva ohjaustapa, ja muistuttaa vahvasti tasaohjausta, jossa ohjattavien pyörien kääntökulmat ovat keskenään identtiset. Ackermann-ohjauksessa kuljettajan ohjausliike kääntää ohjattavien pyörien kulmaa siten, että sisäpuolen pyörä saavuttaa ulkopuolen pyörää suuremman ohjauskulman. Runko-ohjauksessa samalla akselilla olevien pyörien kulma säilyy vakiona, ja ohjaus tapahtuu muuttamalla ajoneuvon etu- ja takaosan välistä kulmaa. Runko-ohjauksella saavutetaan erinomainen ohjattavuus, ja se on käytössä lähinnä raskaissa työkoneissa. Differentiaaliohjausta, eli liukuohjausta, käytetään sekä teloilla

että pyörillä liikkuvissa ajoneuvoissa. Ajoneuvon kääntyminen saavutetaan liikuttamalla toisen puolen telaa tai pyöriä toista puolta nopeammin. Tässä diplomityössä ei käsitellä differentiaaliohjausta tarkemmin, ja seuraavissa alakappaleissa käsitellään Ackermann- ja runko-ohjausta, tyypillisimpiä ohjausmekanismeja sekä Steer by wire-ohjausta.

## 2.1 Ackermann-ohjaus

Yksinkertaisessa ajoneuvon tasaohjauksessa käännettävät pyörät ovat samassa kulmassa, jolloin ne kääntyvät eri keskipisteen mukaisesti, mikä aiheuttaa vähintään toisen etupyörän sivuliukua. Ratkaisu ongelmaan kehitti saksalainen Georg Lankensperger 1800-luvulla. Hänen kehittämässä ohjausmenetelmässä ohjattavien pyörien kääntökulmat ovat toisiinsa nähden erisuuruiset. Kaarteessa sisemmän pyörän kääntökulma on suurempi kuin ulkoradan pyörällä, minkä ansiosta pyörät kääntyvät saman keskipisteen mukaisesti. Ohjausmenetelmä tunnetaan nykyään Ackermann-ohjauksena patentoijansa Rudolf Ackermannin mukaan. [7] Kuvassa 1 esitellään tasaohjauksen, Ackermann ja anti-Ackermann ohjauksen geometriaa.




***Kuva 1.*** *Tasaohjauksen ja Ackermann-ohjauksen geometria [8]*

Täydellisessä Ackermann-ohjauksessa pyörien kääntökulmat ovat riippuvaisia ajoneuvon akselien pituudesta sekä akselivälistä. Olettamalla ajoneuvon kääntyvän hitaasti, ja etteivät keskipakoisvoimat vaikuta ajoneuvoon, Ackermann-ohjausta hyödyntävien ajoneuvojen kääntökulmat sekä kääntöympyröiden säteet voidaan laskea seuraavasti:

$$R_{es} = \frac{L}{\sin \theta_{es}}, \quad (1)$$

jossa $\theta_{es}$ ja $R_{es}$ ovat sisäetupyörän ohjauskulma ja kääntöympyrän säde, ja L on ajoneuvon akseliväli. Samalla kaavalla voidaan laskea ohjattavan ulkopyörän kääntöympyrän säde vaihtamalla ohjauskulmaksi $\theta_{eu}$. Vastaavasti takapyörien kääntöympyröiden säteet voidaan laskea kaavalla

$$R_{ts} = R_{es} \cdot \cos \theta_{es} - (b_t - b_e)/2, \quad (2)$$

jossa $R_{ts}$ on sisäpuolen takapyörän kääntösäde, $b_t$ taka-akselin pituus ja $b_e$ etuakselin pituus. Taaemman ulkopyörän kääntösäde saadaan laskettua sijoittamalla kaavaan 2 muuttujat $R_{eu}$ ja $\theta_{eu}$, sekä vähentämisen sijaan lisäämällä akseleidenpituusero tulokseen. [9]

Ulomman etupyörän ohjauskulma voidaan selvittää hyödyntämällä etuakselin pituustietoa laskemalla

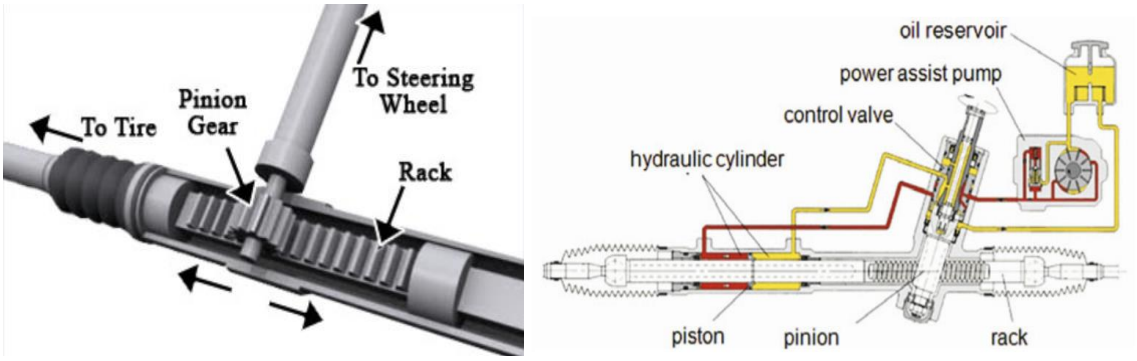
$$\theta_{eu} = \operatorname{arccot}\left(\frac{b_e}{L} + cot\theta_{es}\right), \quad (3)$$

josta nähdään ulomman pyörän ohjauskulman riippuvuus ajoneuvon mitoista sekä sisäpyörän ohjauskulmasta. [9] Ohjauskulman erot pyörien välillä suurenevat etuakselin pituuden ja akselivälin suhteen kasvaessa. Esimerkiksi ajoneuvolla, jonka suurin kääntökulma on 40 astetta, akseliväli 4 m ja akselin pituus 2 m, ulomman etupyörän ohjauskulma on jyrkimmillään noin 30 astetta.

Ajoneuvoissa Ackermann ohjaus tyypillisesti toteutetaan neli- tai kuusinivelsysteemillä, jolloin raidetangon pituus on akselia lyhyempi, kuten kuvasta 1 nähdään. Ajoneuvoissa ei tyypillisesti käytetä täydellistä Ackermann-ehtoa täyttävää ohjausta, vaan ehdon täyttämistä voidaan merkitä 0-100 %, jossa 0 % tarkoittaa tasaohjausta ja 100 % täydellistä Ackermann-ohjausta. Ackermann-ohjausta voidaan tietyissä sovelluksissa, kuten kilpa-autoissa, käyttää käänteisenä niin kutsuttuna Anti-Ackermann-ohjauksena, jolloin ulomman pyörän kääntökulma on sisäpuolen pyörää suurempi. Radalla ajettavien kilpa-autojen pyörien kulku- ja ohjaussuunnan välisen kulmat, eli sortokulmat, sekä ulkopyörille jakautuvat kuormitukset ovat huomattavasti suurempia kuin henkilöautoissa. Kääntämällä ulkopyörää sisäpyörää suuremmalla ohjauskulmalla, saavutetaan korkeampi kääntymiseen tarvittava sivuttaisvoima. [8, 10, 11]

Ackermann-ohjaus voidaan toteuttaa usealla eri ohjausmekanismilla, joista yleisimmät ovat kuvissa 2 ja 3 esiteltävät hammastanko- ja kiertokuulaohjaus. Molempia mekanismeja voidaan käyttää käsikäyttöisissä sekä tehostetuissa ohjauksissa, jolloin

lisäteholähteenä voidaan käyttää esimerkiksi hydraulipiiriä tai sähkömoottoria. Hammastanko-ohjauksessa kuljettajan tekemä ohjauspyörän kääntöliike pyörittää hammasratasta, jolloin hammastangon lineaarinen liike aiheuttaa renkaiden kääntymisen. Ohjauksen välityssuhteen määrittää hammaspyörän koko hammasjaon pysyessä vakiona, esimerkiksi 16:1 välityssuhde tarkoittaa ohjauspyörän yhden kokonaisen käännöksen vastaavan 1/16 käännöstä renkailla, eli noin 23 asteen kääntökulmaa. Nykyisin mekanismi on laajasti käytössä yhdistettynä hydrauliseen tai sähköiseen järjestelmään. [12, 13]

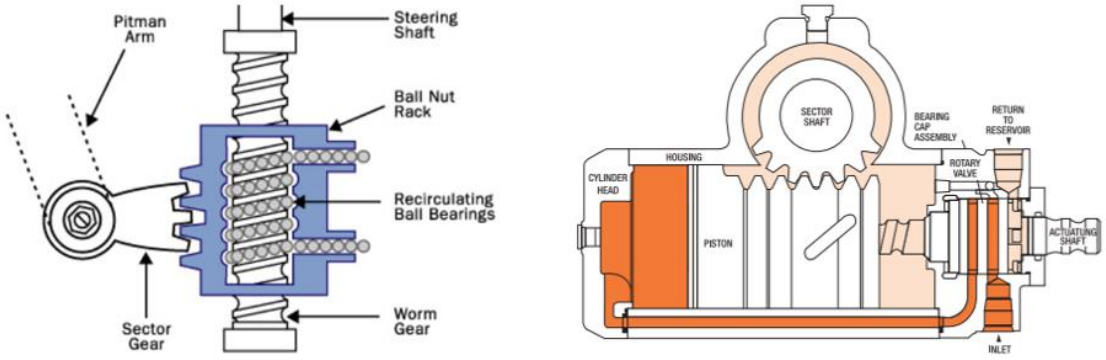



***Kuva 2.*** *Hammastanko-ohjaus [13, 14]*

Hammastanko-ohjausta voidaan tehostaa hydraulisesti, sähköisesti tai näiden kahden hybridinä. Hydraulisesti tehostetussa ohjauksessa hyödynnetään kaksitoimista sylinteriä, joka keventää kuljettajalta vaadittavaa ohjausvoimaa. Hydraulipumppua voidaan pyörittää ajoneuvon moottoriin kytketyn hihnan avulla, jolloin ohjaustehostus on toiminnassa ainoastaan ajoneuvon moottorin ollessa käynnissä. Pumpun pyörittämisessä voidaan hyödyntää myös sähköjärjestelmää, jota käytetään ainoastaan kääntymisen aikana, milloin saavutetaan alhaisempi energian kulutus. Ohjauksen tehostus voidaan toteuttaa myös täysin sähköisesti sähkömoottorin avulla. [12, 13]

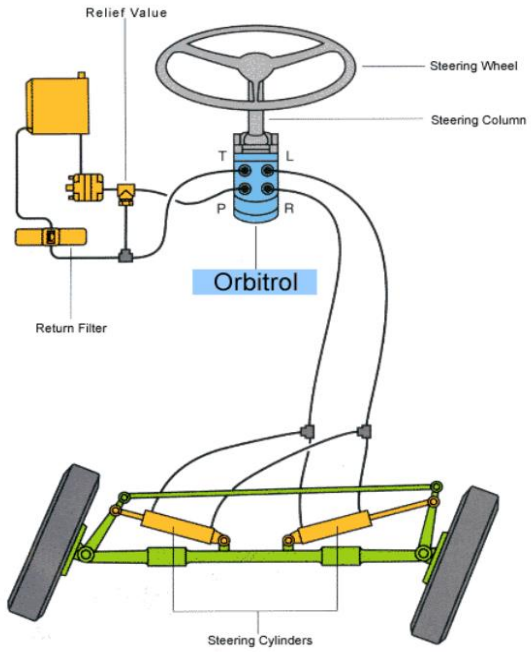
Kiertokuulaohjaus on yleinen ohjausmekanismi raskoissa ajoneuvoissa, kuten rekoissa, sen tarjoaman korkean välityssuhteen ja pienen tilantarpeen ansiosta. Kuvassa 3 näkyvän kiertokuulaohjauksen pääosat ovat kierukkavaihde, kuulamutteri, hammassegmentti sekä ohjausnivel. Kiertokuulaohjauksessa kuljettajan ohjausliike pyörittää kierukkavaihdetta, joka aiheuttaa kuulamutterin lineaarisen liikkeen. Hammassegmentti pyörii kuulamutterin suunnan mukaisesti, ja kääntää ohjausliikkeen pyörille välittävää ohjausniveltä. Ohjauksen välityssuhteen määrittää kierukkavaihteessa olevien kierteiden lukumäärä suhteessa pituuteensa. Korkea määrä kierteitä mahdollistaa tarkan ja kevyen ohjauksen, jolloin kääntymisen suorittamiseen vaaditaan suurempia ohjausliikkeitä ohjauksen hidastuessa. [12, 13, 15] Kiertokuulaohjausta

voidaan myös tehostaa hydraulisesti. Kuvan oikealla puolella oleva hydraulisesti tehostetussa ohjauksessa hyödynnetään kuulamutterin tilalla mäntää, jonka liikuttamiseen vaadittava tilavuusvirta saadaan hydraulipumpulta.




***Kuva 3.*** *Manuaalinen ja hydraulisesti tehostettu kiertokuulaohjaus [16, 17]*

Maastossa liikkuvissa työkoneissa voidaan hyödyntää hydrostaattista orbitroli-ohjausta, joka tarjoaa perinteisiä mekanismeja joustavamman ohjausmenetelmän. Orbitroli-ohjauksessa kuljettajan ja pyörien välillä ei ole edellä esiteltyjen kaltaista mekaanista yhteyttä, minkä ansiosta hydrostaattinen ohjaus on laajasti käytössä traktoreissa ja muissa työkoneissa. Mekaanisen liitännän sijaan, hydrostaattisessa ohjauksessa kuljettajan ohjausliike välitetään ohjausyksikön kautta hydraulisylintereille, jotka valitun ohjaustavan mukaan ohjaavat joko koneen pyörien tai rungon kulmaa. Sylintereinä voidaan käyttää yhtä differentiaalisylinteriä, yhtä symmetristä sylinteriä tai kahta ristiinkytkettyä differentiaali sylinteriä. Käytettäessä ainoastaan yhtä differentiaalisylinteriä on huomioitava, että ohjaustyö ja liikenopeus ovat erisuuruisia eri liikesuunnissa. Kuvassa 4 esitellään hydrostaattinen Ackermann-ohjaus, jossa käytetään kahta ristiin kytkettyä differentiaali sylinteriä.[18, 19]



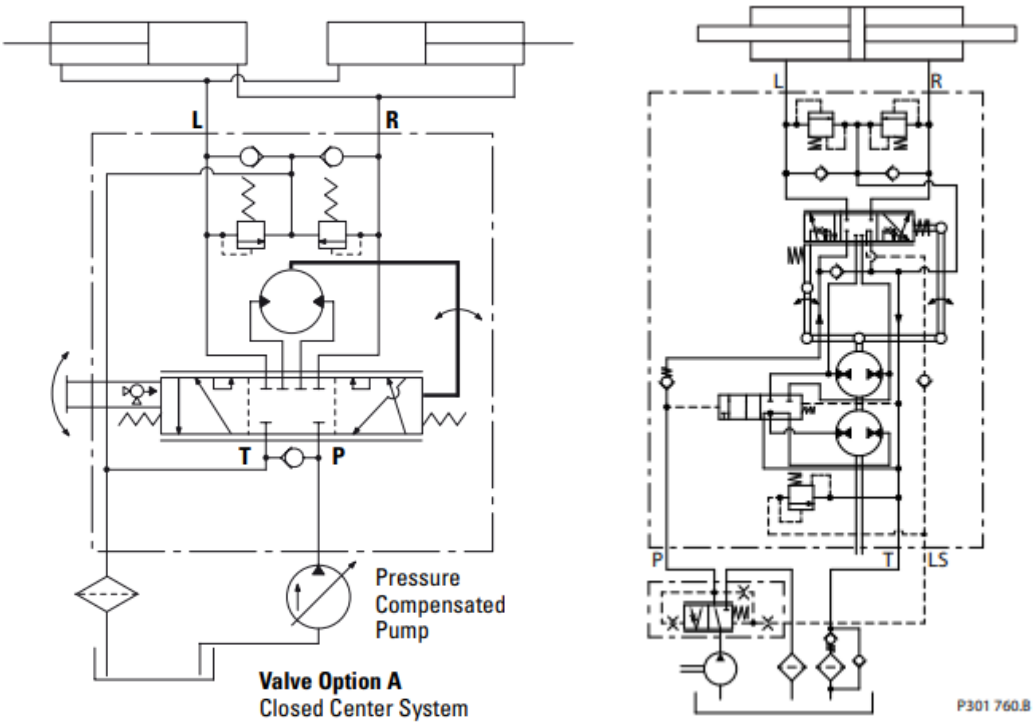

***Kuva 4.*** *Hydrostaattinen Ackermann-ohjaus [20]*

Tyypillinen hydrostaattinen ohjausjärjestelmä koostuu hydrostaattisesta ohjausyksiköstä, eli niin sanotusta orbitrolista, pumpusta, säiliöstä, suodattimesta, paineenalennusventtiilistä sekä sylintereistä. Järjestelmän monimutkaisin komponentti on ohjauspyörään kytketty orbitroli, jonka pääkomponentit ovat venttiili ja hydraulipumppu. Kuljettajan kääntäessä ohjauspyörää, venttiili ohjaa tilavuusvirran orbitrolin pumpun kautta sylintereille. Orbitrolin pumpun tehtävänä on annostella ohjausliikkeen mukainen määrä väliainetta sylintereille. Venttiili seuraa sekä pumpun liikettä, ja sulkeutuu ohjausarvon ja sylintereille syötetyn tilavuusvirran vastatessa toisiaan. [18, 19, 21]

Hydrostaattisia ohjausyksiköitä on useita erilaisia, ja ne voidaan jakaa avoimen ja suljetun keskiasennon -, Power Beyond – sekä kuormantunteviin (engl. Load Sensing, LS) yksiköihin. Yksinkertaisin ja hankintakustannuksiltaan edullisin järjestelmä on avoimen keskiasennon ohjausyksikkö, jolle kiinteätilavuuspumppu tuottaa tilavuusvirran. Järjestelmä soveltuu erityisesti pienen kokoluokan koneisiin. Ohjausyksikkö voi olla toiminnaltaan reaktiivinen, jolloin esimerkiksi tien epätasaisuudesta johtuvat ulkoiset voimat välittyvät ohjauspyörään. Ei-reaktiivinen yksikkö ei välitä ulkoisia voimia ohjauspyörälle, ja näin ollen soveltuu paremmin epätasaisessa maastossa liikkuville koneille. Power Beyond -yksiköissä järjestelmän pääpumpun tuotto voidaan ohjata myös muihin koneen toimintoihin. Ohjaustoiminnot ovat aina ensisijaisia, ja pumpun tuotto ohjataan prioriteettiventtiilin kautta joko ohjaukselle tai muihin toimintoihin. Suljetun keskiasennon yksiköissä käytetään säätötilavuuspumppuja, jolloin säästytään turhalta

öljyn kierrättämiseltä venttiilin kautta. Järjestelmä soveltuu erityisesti suuriin työkoneisiin. Kuorman tuntevissa yksiköissä voidaan käyttää sekä avointa keskiasentoa, jolloin hyödynnetään prioriteettiventtiiliä, että suljettua keskiasentoa, jolloin käytössä on säätötilavuuspumppu. LS-yksiköt voidaan jakaa staattisiin ja dynaamisiin malleihin. Staattisissa yksiköissä pumpun tuotto ohjautuu ohjausyksille ainoastaan ohjattaessa, jolloin järjestelmän häviöt ovat minimoitu. Menetelmän haittapuolena ovat mahdolliset lämpöiskut, jotka voivat vahingoittaa ohjausyksikköä, sekä mahdolliset karan jumiutumiset. Dynaamisissa malleissa ohjausyksikön lävitse kulkee jatkuvasti pieni tilavuusvirta, joka pitää ohjausyksikön ja järjestelmän öljyn lämpötilan vakiona. [18, 19]

Kuvan 5 vasemmalla puolella esitellään suljetun keskiasennon ohjausyksikkö, joka ohjaa säätötilavuuspumpun tuoton kahdella differentiaalisylinterille. Pumpun tai sen teholähteen vikaantuessa tai sammuessa, konetta voidaan ohjata manuaalisesti orbitrolin avulla. Vikaantumistilanteessa kuljettajan ohjausliike pyörittää orbitrolin pumppumoottoria, joka pumppaa tarvittavan tilavuusvirran tankista sylintereille. Manuaalista ohjausta varten tankki- ja painelinjat ovat yhdistetty vastaventtiilillä, jotta manuaalinen ohjaus molempiin suuntiin olisi mahdollista. Ohjaus muuttuu tehostuksen katoamisen myötä luonnollisesti huomattavasti raskaammaksi ja hitaammaksi. Raskaissa ajoneuvoissa manuaalinen ohjaus voi olla liian raskasta tai jopa mahdotonta käytettäväksi. Tällöin voidaan hyödyntää järjestelmiä, joissa on erillinen paineenvahvistin tai kaksi erikokoista orbitrol-pumppumoottoria, kuten kuvan 5 oikealla puolella olevassa järjestelmässä. Kahden pumppumoottorin järjestelmässä molemmat ovat käytössä normaalin ajon tilanteessa, ja vikaantumistilanteissa käytetään vain toista orbitrol-pumppumoottoria. Pumpun tuotto on suoraan verrannollinen kääntömomenttiin, minkä vuoksi manuaalisessa ohjauksessa käytetään kahdesta orbitrol-pumppumoottorista pienempää. [20-23]

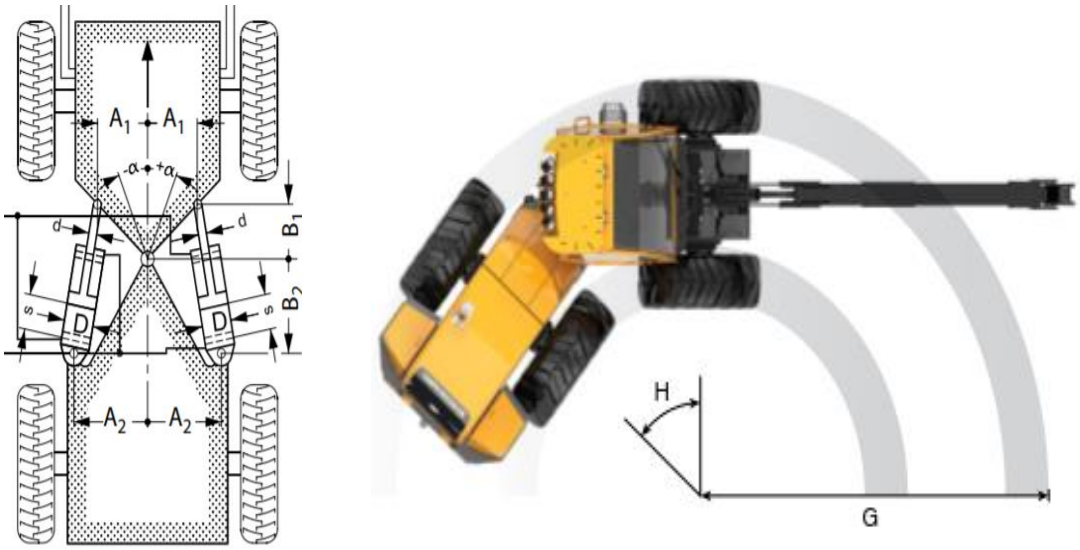



***Kuva 5.*** *Hydrostaattisen ohjauksen hydraulikaavioita [18, 19]*

## 2.2 Runko-ohjaus

Useissa työkoneissa, kuten pyöräkuormaajissa ja metsäkoneissa, hyödynnetään runko-ohjausta. Toisin kuin Ackermann-ohjauksessa, runko-ohjauksessa samalla akselilla olevat renkaat ovat yhdensuuntaisia, ja koneen kääntyminen tapahtuu runkojen välisen kulman muutoksella. Runko-ohjatut koneet koostuvat etu- ja takaosasta, jotka ovat kiinnitetty toisiinsa nivelellä. Tyypillisesti koneen runkoihin on kiinnitetty kaksi ristiin kytkettyä hydraulisylinteriä, yksi molemmilla puolilla niveltä. Koneen kääntyminen saadaan aikaan ajamalla runkoihin kiinnitettyjä hydraulisylintereitä sisään ja ulospäin. Runko-ohjauksen suurin etu on erinomainen ohjattavuus, joka mahdollistaa etu ja takapyörien liikkumisen samoja jälkiä pitkin, sekä pienemmän kääntösäteen Ackermann-ohjaukseen verrattuna [9]. Etujensa ansiosta runko-ohjaus soveltuu erityisen hyvin muun muassa kaivos-, maatalous- sekä metsäkoneisiin.

Runko-ohjaus voidaan toteuttaa hydraulisesti edellä esitellyn orbitrolin tai SBW-ohjauksen avulla. Myös energiatehokkaamman sähkömekaanisen runko-ohjauksen toteuttamista on tutkittu, mutta ratkaisun kaupallistamisen haasteina ovat kuitenkin korkeammat kustannukset, komponenttien saatavuus sekä huonompi tehontiheys verrattuna hydrauliseen järjestelmään. Kuvassa 6 esitellään eräs kaksisylinterinen runko-ohjaus sekä Sampo Rosenlewin runko-ohjatun HR46x metsäharvesterin liikerata.




***Kuva 6.*** *Runko-ohjaus [19, 22]*

Ackermann-ohjauksen tavoin, myös runko-ohjatulle ajoneuvolle voidaan määrittää jokaisen pyörän kääntöympyrän säde. Aiemmin määriteltyjen mittojen lisäksi, suuri merkitys on etu- ja takaosan erottavan nivelen sijainnilla, joka ilmoitetaan suhdelukuna k. Keskinivelen ollessa lähempänä taka-akselia tai etäisyys molempiin akseliin on yhtä suuri, eli k ≥ 0.5, kääntöympyrän suurin säde on ulommaisella takapyörällä ja pienin sisemmällä etupyörällä. Kääntöympyrän säteet laskea seuraavasti

$$R_{tu} = R_{max} = \frac{L}{\sin\theta} * (k + (1-k)cos\theta) + \frac{b_t}{2}, \tag{4}$$

ja

$$R_{es} = R_{min} = \frac{L}{\sin\theta} * (kcos\theta + 1 - k) - \frac{b_e}{2}, \tag{5}$$

joissa $\theta$ on ohjauskulma. Samalla akselilla olevien pyörien ohjauskulma on sama, jolloin kääntöympyrän säde saadaan selville lisäämällä tai vähentämällä akselinpituus laskettuun sisä- tai ulkopyörän säteeseen. Nivelen ollessa lähempänä etuakselia, voidaan kääntöympyrän säteet laskea kaavoilla

$$R_{eu} = R_{max} = \frac{L}{\sin\theta} * (kcos\theta + 1 - k) + \frac{b_e}{2} \tag{6}$$

ja

$$R_{ts} = R_{min} = \frac{L}{\sin\theta} * (k + (1-k)cos\theta) - \frac{b_t}{2}, \tag{7}$$

jolloin suurin kääntösäde on ulommalla etupyörällä ja pienin sisemmällä takapyörällä. [9]

Runko-ohjauksen suurin etu on sen erinomainen ohjattavuus, mikä mahdollistaa huomattavasti pienemmän kääntösäteen Ackermann-ohjaukseen verrattuna. Esimerkiksi kuvassa 6 esitellyn runko-ohjatun Sampo Rosenlewin harvesterin HR46x maksimikääntökulma on 50°, ja kääntöympyrän ulkosäde on 4020 mm. Mikäli HR46x hyödyntäisi runko-ohjauksen sijaan Ackermann-ohjausta, voidaan kääntöympyrän sädettä arvioida hyödyntämällä kaavoja 1 ja 3, sekä huomioimalla renkaiden leveys, jolloin säteeksi saadaan,

$$R_{es} = \frac{2735\ mm}{\sin\ \{\operatorname{arccot}\left(\frac{1600\ m}{2735\ mm} + \cot 50°\right)\}} + \frac{500\ mm}{2} \approx 5009\ mm, \tag{8}$$

jossa 500 mm on renkaan leveys. Näin ollen, runko-ohjauksella saavutetaan noin 20 % pienenempi kääntöympyrän säde, kun oletetaan muiden arvojen pysyvän vakiona ja vertailukohteena on täydellinen Ackermann-ohjaus. Todellisuudessa Ackermann-ohjauksen kääntökulma on lähempänä 40 astetta, jolloin kääntöympyröiden säteiden ero kasvaisi yli 30 %: in.

Toinen runko-ohjauksella saavutettu etu on etu- ja takapyörien liikkuminen samoja jälkiä pitkin, mikä helpottaa ohjaamista erityisesti ahtaissa väleissä. Se ei kuitenkaan koske kaikkia runko-ohjattuja koneita, sillä renkaiden liikkuminen samoja jälkiä pitkin on seurausta ajoneuvon keskinivelen sijainnista suhteessa etu ja taka-akseliin. Keskinivelen sijaitessa yhtä kaukana etu ja taka-akselista, saavutetaan pyörien liikkuminen samoja jälkiä pitkin.

## 2.3 Sähköinen ohjaus

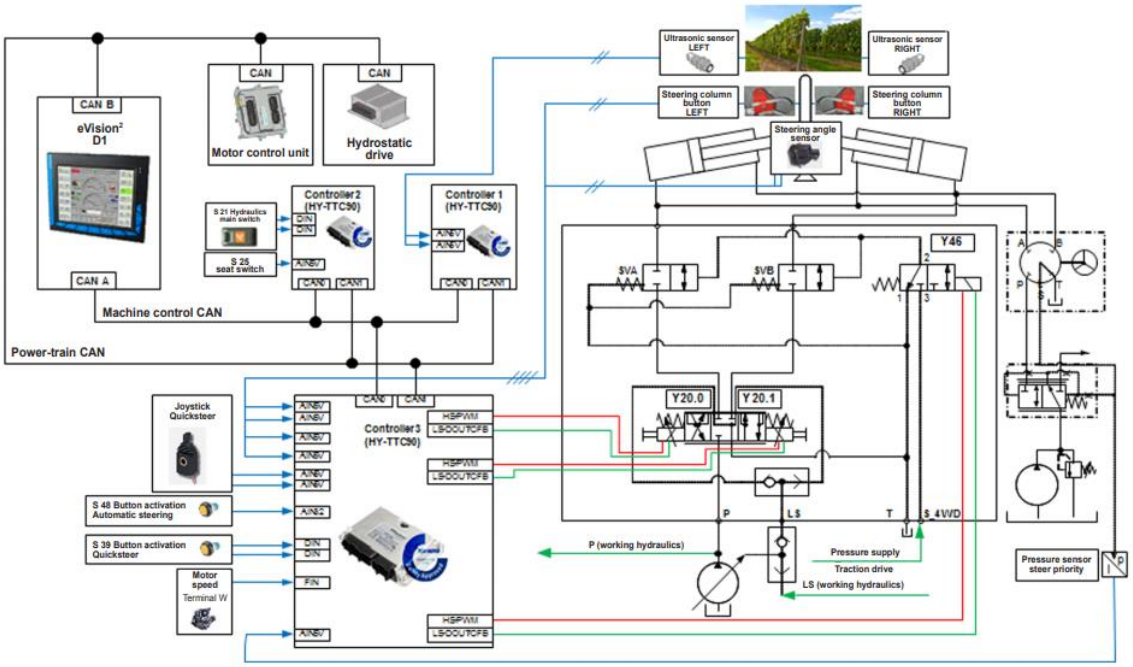
Steer by wire -ohjauksessa pyörien ja ohjauselementin, välillä ei ole mekaanista kytkentään, vaan ohjaus tapahtuu sähköisesti sensoreiden ja ohjausyksiköiden avulla. Se mahdollistaa ohjaukselle yksinkertaisemman ja kevyemmän fyysisen rakenteen sekä korkeamman energiatehokkuuden ja ohjaustarkkuuden [23, 24]. SBW-ohjaus ei ole uutta teknologiaa, sillä lentokoneteollisuudessa vastaavaa Fly by wire – ohjausta on käytetty kaupallisissa lentokoneissa jo 1980-luvulta lähtien [2]. Myös raskaissa metsäkoneissa SBW-ohjausta on hyödynnetty jo usean vuosikymmenen ajan. [3] Tulevaisuudessa SBW-ohjauksen avulla voidaan nostaa ajoneuvon automaation tasoa etä- ja automaattiohjauksen muodossa.

Mekaanisen/hydraulisen yhteyden puuttuminen ohjaamon ja pyörien välillä mahdollistaa suunnittelussa ohjauselementin vapaamman sijoittamisen ajoneuvoon, mitä voidaan hyödyntää esimerkiksi yhdenmukaistamalla vasemman ja oikean puolen ohjausta käyttäviä ajoneuvoja. Lentokoneteollisuudessa FBW-ohjaus on yksinkertaisuutensa,

edullisuutensa ja erityisesti turvallisuutensa takia laajasti käytössä. Pyörillä liikkuvilla ajoneuvoilla toimintaympäristö on ohjauksen kannalta täysin erilainen, mikä on osaltaan hidastanut SBW-ohjauksen leviämistä autoihin ja muihin pyörillä liikkuviin ajoneuvoihin. SBW-ohjaus on kuitenkin laajasti käytössä raskaissa off-road metsätyökoneissa erityisesti mekaanisen rakenteensa ja ergonomisuutensa ansiosta. [3] Sähköistä ohjausta ei pidetä yhtä turvallisena kuin mekaanista tai hydraulista yhteyttä kuljettajan ja pyörien välillä hyödyntäviä ohjausjärjestelmiä, minkä vuoksi SBW-ohjaukselle on asetettu tiukat turvallisuusvaatimukset. Käytännössä ajoneuvolta vaaditaan redundanttisia, eli rinnakkaisia ohjausjärjestelmiä, joka vaikuttaa merkittävästi SBW-ohjausjärjestelmän hintatasoon. Perinteinen ohjaustapa on edelleen käytössä osassa kevyissä ja pienissä lentokoneissa, mikä kuvastaa hyvin järjestelmän kustannusten sekä etujen välistä suhdetta. [3, 25, 26]

Sähköhydraulinen SBW-ohjausjärjestelmä koostuu ohjauselementistä, ohjausyksiköstä, sensoreista sekä ohjattavasta toimilaitteesta, kuten sähkömoottorista tai venttiilistä, kuten kuvassa 7 esitellään. Ohjauselementin liike välitetään ohjausyksikölle, joka ohjaa toimilaitteen, tässä tapauksessa venttiilin asemaa. Pumpun tuotto ohjataan venttiilin kautta sylintereille, joiden asematieto välitetään sensoreiden kautta takaisin ohjausyksikölle. Sähköisen ohjauskäskyn ansiosta ohjauselementtinä voidaan ohjauspyörän sijaan käyttää myös vähemmän tilaa vieviä ohjausvipuja, joita käytetään esimerkiksi raskaissa metsäkoneissa. Toisin kuin mekaanisessa ohjauksen välityksessä, SBW-ohjauksessa välityssuhde voidaan ohjelmoida halutun kaltaiseksi. Ohjelmoitava ohjausyksikkö mahdollistaa eri nopeusalueille erisuuruiset välityssuhteet, jolloin alhaisella nopeudella voidaan hyödyntää herkempää ohjausta, ja suurilla nopeuksilla vastaavasti stabiilimpaa ohjausta. [3, 26, 27]

Kuvan 7 koneen ohjaus koostuu kahdesta erillisestä järjestelmästä. Vasemmalla puolella esitetään ohjausvivullinen sähköinen ohjaus, ja kuvan oikeassa laidassa on nähtävissä ohjauspyörällä ohjattava orbitrol, sen prioriteettiventtiili sekä pumppu. Syyt rinnakkaisiin ohjausjärjestelmiin ovat SBW-ohjauksen tuomat edut, kuten ”Quicksteer” ja automaattinen ohjaus, sekä koneelta vaadittava turvallisuus. Lainsäädännön ja standardien asettamia turvallisuusvaatimuksia tarkastellaan kappaleissa 3, 4 ja 5.




***Kuva 7.*** *Steer by wire ja Orbitrol-ohjaus rinnakkain [28]*

Perinteisissä mekaanisissa ja hydraulisissa ohjausjärjestelmissä ohjauselementille välittyvät pyöriin vaikuttavat ulkoiset voimat, eli kyseessä on Human-In-The-Loop -ohjaus. Vastaavan ohjaustuntuman puuttumisen SBW-ohjauksesta on havaittu heikentävän ohjausta, johtaen ali- tai yliohjaamiseen [3]. SBW-ohjauksessa ohjaustuntuma voidaan keinotekoisesti luoda esimerkiksi sähkömoottorin tai TFD:n (engl. Tactile feedback device) avulla, joka luo mekaanisen kytkennän kaltaisen vääntömomentin ohjauspyörään. [3, 13]

SBW-ohjauksella on merkittäviä etuja verrattuna perinteisiin ohjausmenetelmiin, kuten yksinkertaisempi fyysinen rakenne, ohjauksen ohjelmoitavuus sekä ohjauksen tarkkuus. SBW-ohjaus voidaan toteuttaa sähkömekaanisena tai sähköhydraulisena hybridinä. Sähköisen ohjauksen suurimpia haasteita ovat ohjauksen luotettavuus sekä vaativa ja muuttuva lainsäädäntö, jonka eri osa-alueita käsitellään kappaleissa 3-5.

# 3. LAINSÄÄDÄNTÖ

Eurooppaan myytävät koneet ovat EY-tyyppihyväksyttyjä, eli niiden on täytettävä konetta koskevien direktiivien ja asetusten vaatimukset. Lainsäädännön asettamat vaatimukset ovat laajoja kokonaisuuksia, eivätkä tyypillisesti käsittele tarkasti teknisiä vaatimuksia. Tekniikan kehittyessä, yksityiskohtainen lainsäädännön ylläpitäminen on hyvin vaativaa, minkä vuoksi lainsäädännön tukena käytetään eri organisaatioiden laatimia standardeja. [29, 30]

Tunnettuja kansainvälisiä standardoimisjärjestöjä ovat ISO sekä IEC (engl. International Electrotechnical Commission), joka on erikoistunut sähkötekniikan standardeihin. Suurimmat Euroopassa toimivat standardoimisjärjestöt ovat CEN (ransk. Comité Européen de Normalisation) ja Cenelec (engl. European Committee for Electrotechnical Standardization), joiden laatimia standardeja merkitään lyhenteellä EN. Eurooppalaiset standardointijärjestöt voivat hyväksyä kansainvälisen standardointijärjestön laatiman standardin, jolloin sitä kutsutaan harmonisoiduksi standardiksi, ja standardin nimessä ilmoitetaan molempien järjestöjen lyhenteet. Suomessa standardoimisjärjestöjä edustaa Suomen standardoimisliitto SFS, jonka laatimia standardeja merkitään etuliitteellä SFS.

Yhdenmukaistettujen, eli harmonisoitujen, standardien tarkoitus on selkeyttää vaatimuksia, joita koneelta vaaditaan. Toisin kuin direktiivien, standardien vaatimusten täyttäminen on yleisesti ottaen vapaaehtoista, mutta viranomaiset voivat toimivaltojensa rajoissa vaatia standardien noudattamista. Harmonisoitujen standardien mukaisesti suunniteltujen koneiden katsotaan täyttävän lainsäädännön asettamat vaatimukset, minkä ansiosta koneenrakentajan on helpompaa osoittaa koneen täyttävän eurooppalaisen lainsäädännön vaatimukset. [31-33]

Standardit jakautuvat kolmeen eri tasoon: A-, B- ja C-tyyppiin. Koneturvallisuuden A-tyypin standardi SFS-EN ISO 12100, on turvallisuuden perusstandardi, joka esittelee yleisellä tasolla koneisiin sovellettavia perusteita, suunnitteluperiaatteita, yleisiä näkökohtia sekä riskienhallintaa. B-tyypin standardit käsittelevät pienenpää osa-aluetta, kuten yksittäisiä turvallisuusnäkökohtia tai suojausteknisiä laitteita. Yleisiä ohjausjärjestelmistä käytettyjä B-tyypin standardeja ovat SFS-EN ISO 13849 ja SFS-EN 62061, joita käsitellään myös tässä diplomityössä. C-tyypin standardit käsittelevät tietyn koneen tai koneryhmän yksityiskohtaisia turvallisuusvaatimuksia. [5, 29, 34]

Suunnittelun alkuvaiheessa tulisi selvittää C-luokan standardin olemassaolo. Yksityiskohtaisuutensa vuoksi, sen asettamat vaatimukset ovat ensisijaisia verrattuna A

ja B-tyypin standardeihin, jolloin ristiriitatilanteessa noudatetaan C-tyypin standardin vaatimuksia. C-tyypin standardit usein viittaavat A-, B- tai toisiin C-tyypin standardeihin, joita tulee suunnittelussa noudattaa. Tilanteet, joissa ei ole C-tyypin standardia käytettävissä, voidaan suunnittelussa noudattaa B-luokan standardin vaatimuksia. Konedirektiivin asettamia vaatimuksia riskien hallinnasta ei käsitellä B ja C-tyypin standardeissa, vaan se on toteutettava soveltamalla A-tyypin standardia ISO 12100. [29]

Pyörillä liikkuvalle työkoneen ohjaukselle on määritelty oma C-luokan standardi ISO 5010. Standardi ei ole harmonisoitu, eikä se kata kaikkia pyörillä liikkuvia koneita, vaan sitä voidaan soveltaa esimerkiksi metsä- ja kaivoskoneissa. Vastaavasti traktoreita ja tienkunnostuskoneita koskevat standardit vaativat ohjauksen täyttävän standardin SFS-EN 12643 vaatimukset, jotka vahvasti pohjautuvat kansainväliseen standardiin ISO 5010. Suurimmat eroavaisuudet standardien välillä koskevat ajonopeuksia sekä sähköisen ohjauksen ja lisäohjauselementtien erityisvaatimuksia, joita ei esitellä standardissa SFS-EN 12643. Lisäksi standardi SFS-EN 12643 määrittelee vaatimukset vain yli 20 km/h nopeudelle. [4, 35-38]

## 3.1 Suomen ajoneuvolaki ja Euroopan komission asetukset

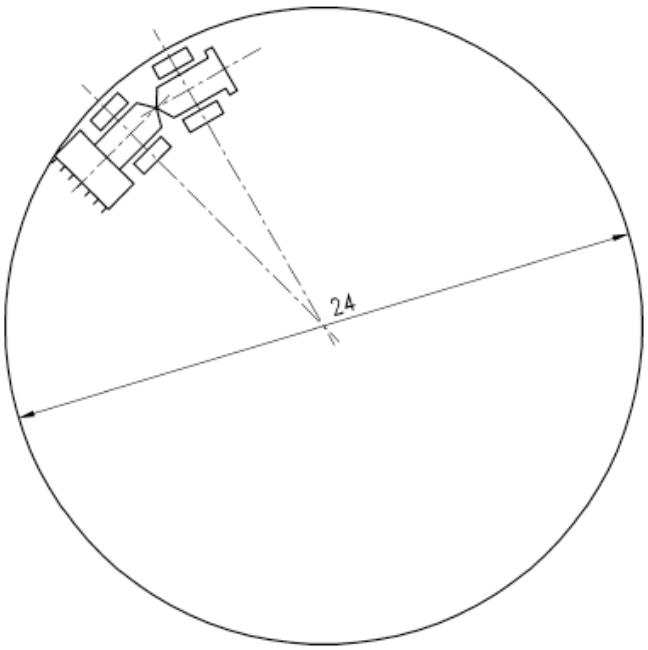
Tieliikenteessä ja muualla käytettävien ajoneuvojen tekniset vaatimukset sekä tyyppihyväksynnät määritellään ajoneuvolaissa. Yleiseltä liikenteeltä eristetyltä alueella toimiviin ajoneuvoihin lakia sovelletaan vain tietyin osin, joihin kuuluvat esimerkiksi turvallisuusvaatimukset sekä ajoneuvon kuntoa, rekisteröintiä ja katsastusta koskevat pykälät. Ajoneuvolain tekniset vaatimukset ovat hyvin suppeat, ja sen turvallisuussäädökset pohjaavatkin hyvin vahvasti EY-tyyppihyväksyntään. Esimerkiksi ohjauslaitteiston vaatimuksena on luotettava ja varmatoiminen ohjauslaite, joka todennetaan ajoneuvoa koskevien direktiivien ja asetusten vaatimusten täyttymisellä. [39] Ajoneuvoa koskevat vaatimukset riippuvat ajoneuvon tyypistä, ja sen rakenteellisesta maksiminopeudesta. Esimerkiksi tieliikenteessä moottorityökoneiden sekä maa- ja metsätaloustraktoreiden suurin sallittu nopeus on 40 km/h, pois lukien b-luokan nopeat traktorit, joiden suurin sallittava nopeus on tietyin edellytyksin jopa 80 km/h. [40]

Maa- ja metsätaloudessa käytettävien traktoreiden hyväksyntä määritellään Euroopan komission asetuksessa 167/2013. Asetusta sovelletaan itse ajoneuvoihin sekä käytettäviin osakokonaisuuksiin, kuten ohjausyksiköihin. Ohjauksen osalta asetus jakaa ajoneuvot traktoreihin, joiden rakenteellinen nopeus on alle 40 km/h, sekä nopeisiin traktoreihin, joiden rakenteellinen nopeus on yli 40 km/h. Nopeiden traktoreiden ohjausvaatimukset määritellään maksiminopeudesta riippuen UN/ECE E-säännön 79 ja

standardin ISO 10998:2008 mukaisesti. Vastaavasti traktoreilla, joiden rakenteellinen nopeus on alle 40 km/h, ohjausvaatimukset määritellään asetuksessa 2015/208. Valmistajat voivat halutessaan kuitenkin noudattaa nopeiden traktoreiden vaatimuksia asetuksen 2015/208 sijaan. [6]

Traktoreiden ohjauksen vaatimuksia käsitellessä on ensimmäisenä selvitettävä ohjauslaitteen tyyppi. Ohjauslaitteeseen luetaan sisältyvän kaikki kulkusuunnan muuttamiseen vaikuttavat komponentit, kuten hallintalaite, ohjausvaihde sekä ohjattavat pyörät. Käsikäyttöinen ohjauslaite saa kaiken tehonsa käyttäjän lihasvoimasta, minkä vuoksi se soveltuu ainoastaan erittäin kevyiden ajoneuvojen ohjaamiseen. Tehostettu ohjauslaite hyödyntää käyttäjän lihasvoiman lisäksi erillistä tehon lähdettä, joka voi olla esimerkiksi hydraulinen tai sähköinen järjestelmä. Täysin tehostettu ohjauslaite saa kaiken ohjaukseen tarvittavan voiman erillisestä tehon lähteestä, tällöin voidaan puhua myös servo-ohjatusta järjestelmästä. [6] Steer by wire -ohjaus on edellä mainitun mukaisesti täysin tehostettu ohjauslaite.

Ohjauksen hallintalaitteelle tarkoitetaan ajoneuvon ohjaukseen käytettävää komponenttia, kuten ohjauspyörää tai ohjausvipuja. Asetuksessa 2015/208 ohjauksen hallintalaitteen riittävä toiminnallisuus varmistetaan kuvassa 8 esitetyllä testiradalla, jossa ajoneuvon on tasaisella nopeudella saavutettava halkaisijaltaan 24 m kääntöympyrä. Testin suoritus nauhoitetaan, ja kuljettajan käyttämän ohjausvoiman sekä ohjauksen keston on pysyttävä määriteltyjen rajojen sisällä. Ohjausvoima ei saa normaali tilanteessa ylittää 250 N, eikä tehostetun ohjauksen ensisijaisen tehonlähteen vikaantuessa yli 600 N. Vastaavasti vaadittavan kääntösäteen saavuttamiseen kulutettu aika ei saa ylittää viittä sekuntia, ja tehonlähteen vikaantumistilanteessa yli kahdeksaa sekuntia. Testi suoritetaan kertaalleen sekä oikealle että vasemmalle puolelle käännettäessä. [6]




***Kuva 8.*** *Ohjauksen kääntöympyrärata [35]*

Ohjausvaihteella tarkoitetaan hallintalaitteen sekä ohjattavien pyörien välillä olevia komponentteja, pois lukien lisä- tai erityistehoa tuottavat lisälaitteet, kuten hydraulipumput, paineakut ja sähkömoottorit. Traktorin ohjausvaihde ei asetuksen 2015/208 mukaan olla sähkökäyttöinen tai täysin pneumaattinen. Huomioitava on, että asetuksen 2015/208 vaatimukset käsittävät servo-ohjauslaitteiden osalta vain täysin hydraulisen ohjausvaihteen järjestelmät. [6]

Tehostettujen sekä servo-ohjauslaitteiden osalta ohjaus on pystyttävä säilyttämään tehonlähteen vikaantuessa. Tehostetun ohjauksen osalta se voidaan saavuttaa mekaanisen tai hydraulisen kytkennän kautta, mikäli vaadittavat ohjausvoimat eivät ole liian suuria. Servo-ohjauslaitteiden tapauksessa se tarkoittaa järjestelmään lisättävää ylimääräistä tehonlähdettä, joka tuottaa vaadittavan ohjausvoiman ensisijaisen tehonlähteen vikaantuessa. Järjestelmän on ilmoitettava käyttäjälle vikaantumisesta äänimerkin tai visuaalisen merkin avulla. Kuvassa 8 esitelty testirata on pystyttävä suorittamaan myös varateholähdettä hyödyntäen. Testi suoritetaan kertaalleen molempiin suuntiin kääntäen. [6]

UN/ECE sääntö E79 on laadittu erityisesti kuljettajaa avustavien automaattisten toimintojen, kuten kaistaohjauksen ja avustetun pysäköinnin, turvallisuusvaatimusten määrittämiseksi. Sääntöä sovelletaan yli 60 km/h nopeudella ajaviin ajoneuvoihin, mukaan lukien nopeat traktorit. Vuonna 2017 julkaistussa revisiossa 3 määritellään automaattiset ohjaustoiminnot kuuteen eri kategoriaan:

- Kategoria A: Korkeintaan 10 km/h nopeudessa toimiva toiminto, joka avustaa kuljettajaa alhaisilla nopeuksilla tai pysäköinnissä.
- Kategoria B1: Toiminto, joka avustaa kuljettaa säilyttämään ajokaistan vaikuttamalla ajoneuvon sivuttaisliikkeeseen
- Kategoria B2: Kuljettajan aktivoima toiminto, joka säilyttää ajokaistan vaikuttamalla ajoneuvon sivuttaisliikkeeseen ilman lisäkomentoja kuljettajalta.
- Kategoria C: Kuljettajan aktivoima toiminto, joka kykenee suorittamaan yksittäisen sivuttaisliikkeen, kuten kaistan vaihdon.
- Kategoria D: Kuljettajan aktivoima toiminto, joka kykenee tunnistamaan mahdollisuuden yksittäiselle sivuttaisliikkeelle, mutta voi suorittaa sen vasta saatuaan kuljettajalta vahvistuksen.
- Kategoria E: Kuljettajan aktivoima toiminto, joka kykenee jatkuvasti määrittämään mahdollisia sivuttaisliikkeitä, sekä suorittamaan niitä ilman kuljettajan vahvistusta.

Jokainen kategoria vaatii kuljettajan toiminnan sekä läsnäolon ajoneuvossa, eikä säännössä määritellä täysin ilman kuljettajaa olevia ajoneuvoja. Vaatimusten osalta säännössä 79 huomioidaan vain kategorioiden A ja B1 toiminnot, mikä kuvastaa hyvin lainsäädännön puutteita koskien ajoneuvojen itseohjautumista ja etäohjausta. Itseohjautuvia robottiautoja on kuitenkin mahdollista testata tieliikenteessä viranomaisten myöntämän poikkeusluvan turvin. Suomessa VTT:n Marilyn-robottiauto on ensimmäinen Trafin poikkeusluvan saanut robottiauto [41].

## 3.2 Pyörillä liikkuvien työkoneiden ohjausvaatimukset

Standardeissa ISO 5010 ja SFS-EN 12643 käsitellään pyörillä liikkuvien työkoneiden ohjauksen vaatimuksia. Standardin SFS-EN 12643 pohjana käytetään standardin ISO 5010 vaatimuksia, ja suurimmat eroavaisuudet niiden välillä koskevat eri nopeusalueiden sekä sähköisen ohjauksen vaatimuksia, joita ei käsitellä standardissa SFS-EN 12643. Tämän vuoksi tässä kappaleessa käsitellään vain standardin ISO 5010 vaatimuksia.

Standardia ISO 5010 sovelletaan suuriin työkoneisiin, kuten kuormaajiin, metsäkoneisiin ja kaivureihin. Standardin sisältö voidaan karkeasti jakaa kahtia: vaatimuksiin ja todentamiseen. Vaatimusten osalta standardi määrittelee yleiset, ergonomiset sekä suorituskyvylliset vaatimukset. Standardissa esiteltävät testiradat ovat tarkoin määriteltyjä, ja niiden tarkoitus on todentaa koneen ohjauksen täyttävän standardissa

esitetyt vaatimukset. Kaikkia ohjausjärjestelmiä koskeviin yleisiin vaatimuksiin sisältyvät muun muassa hydraulipiiriä ja ohjauksen toimivuutta koskevat vaatimukset. Yleisiä vaatimuksia täydentävät erilliset vaatimukset lisäohjauselementtien ja sähköisen tiedonsiirron käytöstä, jotka ovat riippuvaisia ohjausjärjestelmän tyypistä. [4] Tässä osiossa tarkastellaan standardin esittämiä sähköiseen ohjaukseen, nopeusrajoituksiin, hallintalaitteiden ja hätäohjaukseen liittyviä vaatimuksia.

### 3.2.1 Yleiset nopeusrajoitukset

Standardissa koneen nopeuteen vaikuttavat vaatimukset ovat riippuvaisia ohjausjärjestelmän rakenteesta. Yleisiä nopeuteen liittyviä vaatimuksia ovat ohjauksen asteittainen ja moduloitu säätäminen, jotka varmennetaan suorittamalla liitteessä A esiteltävä testirata 1 standardissa esiteltävien vaatimusten mukaisesti. [4]

Standardissa määritellään kolme eri nopeusaluetta: enintään 10 km/h, yli 10 km/h sekä yli 20 km/h käytettäessä sähköstä ohjausta. SBW-ohjausjärjestelmälle tiukimmat vaatimukset asettavatkin sähköisen ohjauksen erityisvaatimukset, jotka pohjautuvat sähköisiä ohjausjärjestelmiä koskeviin standardeihin, kuten ISO 13849-1:een ja IEC 62061:een. [4] Taulukossa 1 esitellään standardissa ISO 5010 mainittuja suoraan nopeuteen liittyviä vaatimuksia.

**Taulukko 1.** *Nopeusrajoitukset [4, 37]*

| | ≤10 km/h | > 10 km/h | > 20 km/h | > 30 km/h |
|---|---|---|---|---|
| ISO 13849-1 | x | x | x | x |
| Ohjauksen asteittainen säätö | | x | x | x |
| Ohjauksen moduloitu säätö | | x | x | x |
| Turvallinen tila | | x | x | x |
| Ohjattavuus vikaantumisen jälkeen | | | x | x |
| Hätäohjaus | (x) | (x) | (x) | x |

Taulukon tiedot koskevat sähköistä ohjausta käyttäviä koneita. Yli 30 km/h vaatimuksia ei standardissa ISO 5010 mainita, vaan hätäohjaus vaatimus on metsäkoneiden standardista SFS-EN ISO 11850. Käytännössä katsoen, ohjattavuuden säilyminen vikaantumisen jälkeen kuitenkin vaatii rinnakkaisen ohjauskanavan, jolloin myös hätäohjaukselta vaadittava toissijainen teholähde on pakollinen. Standardin ISO 13849-

1 vaatimukset riippuvat koneelta vaadittavasta suoritustasosta, jolloin esimerkiksi rinnakkainen ohjauskanavarakenne voi olla pakollinen myös alhaisemmilla nopeuksilla. [4, 34, 37] Ohjausjärjestelmien vaatimuksia käsitellään kappaleessa 5, ja standardin ISO 5010 mukaista hätäohjausta käsitellään kappaleessa 3.2.3.

### 3.2.2 Sähköinen ohjaus

Standardissa suositellaan käyttämään ohjaukseen muista järjestelmistä erillisiä tehonlähdeitä sekä virtapiirejä. Täysin muista toiminnoista irrallinen ohjausjärjestelmä aiheuttaa valmistajalle ylimääräisiä kustannuksia sekä lisäisi järjestelmän kompleksisuutta, mikä voidaan välttää käyttämällä prioriteettiohjausta. Prioriteettiohjauksessa ainoastaan hätäohjaus ja hätäpysäytys saavat normaalia ohjausta korkeamman prioriteetin. Mikäli ohjauksen tehon lähdettä hyödynnetään koneen muissa alajärjestelmissä, niissä tapahtuvat vikaantumiset käsitellään ohjauksen tehon lähteen vikaantumisena, mikä on huomioitava riskianalyysia tehtäessä. [4]

Sähköistä tiedonsiirtoa käyttävien järjestelmien tulee täyttää soveltuvin osin standardin ISO 15998, ISO 13849 tai IEC 62061 vaatimukset. Kyseiset standardit käsittelevät kaikki sähköisen ohjausjärjestelmän suorituskykyjä, ja ovat tässä yhteydessä toistensa korvaavia. Tässä työssä tarkastellaan tarkemmin standardin ISO 13849 asettamia vaatimuksia, ja niitä käsitellään kappaleessa 5.

Turvallisen tilan tarkoituksena on aktivoitua vikaantumistilanteissa, kuten esimerkiksi ohjaussignaalin katketessa. Sen tavoitteena on estää odottamattomat liikkeet sekä potentiaalisesti vaaralliset tilanteet vikaantumisen tapahtuessa. Turvallinen tila on vaadittava ominaisuus koneilta, joiden ajo nopeus ylittää 10 km/h. Koneen vikaantumisen johtaessa ohjauksen menettämiseen, koneen on siirryttävä turvalliseen tilaan ja pysähdyttävä. Vikaantumisesta on ilmoitettava koneen käyttäjälle visuaalisesti tai äänimerkin avulla. [4]

Yksinkertainen turvallinen tila ei ole riittävä yli 20 km/h nopeudella liikkuville koneille, sillä koneen on säilytettävä ohjauskykynsä yksittäisen vikaantumisen tapahtuessa. Standardissa vaatimukset määritellään seuraavasti:

a. Ohjauskyky on säilyttävä yksittäisen vikaantumisen jälkeen
b. Tarkoituksettoman ohjauksen todennäköisyys on minimoitava
c. Operaattoria on varoitettava vikaantumisen sattuessa

Vikaantumiseksi katsotaan kaikki 80 %:n keskimääräisellä diagnostiikan kattavuudella havaitut vikaantumiset. Yllä mainitut kohdat a-c tulee lisäksi todentaa relevantilla

riskianalyysillä, kuten esimerkiksi vika ja vaikutusanalyysillä (engl. Failure mode and effects analysis, FMEA) tai vikapuuanalyysillä (engl. Fault tree analysis, FTA). [4] Ohjattavuuden säilyttäminen yksittäisen vikaantumisen jälkeen asettaa ohjausjärjestelmälle korkeat vaatimukset, joita käsitellään tarkemmin kappaleessa 5. Käytännössä yli 20 km/h nopeus on saavutettavissa vain käyttämällä rinnakkaisia ohjauskanavoita ja tehonlähteitä.

### 3.2.3 Hätäohjaus

Koneen ohjauksessa käytettävän tehon lähteen vikaantuessa tai moottorin pysähtyessä voidaan ohjaus säilyttää hätäohjausjärjestelmän avulla. Hätäohjausjärjestelmä ei ole täysin rinnakkainen ohjausjärjestelmä, vaan kyseessä on rinnakkaista tehonlähdettä hyödyntävä järjestelmä. Rinnakkaisena tehon lähteenä voidaan käyttää esimerkiksi sähköakkuja, hydraulipumppua tai paineakkuja. Ohjauksen normaalin tehonlähteen vikaantumisesta koneen on ilmoitettava kuljettajalle visuaalisesti tai äänimerkin avulla. [4]

Standardissa ISO 5010 hätäohjausjärjestelmää ei määritellä pakolliseksi yhteenkään ohjausjärjestelmään, mutta esimerkiksi sähköistä ohjausta käyttävien koneiden on säilytettävä ohjattavuus vikaantumistilanteessa, mikäli koneen sallittu ajonopeus ylittää 20 km/h. Sen lisäksi myös muut koneen suunnittelussa huomiotavat standardit voivat vaatia hätäohjauksen, kuten esimerkiksi metsäkoneiden turvallisuusstandardi SFS-EN ISO 11850, joka vaatii standardin ISO 5010 vaatimusten mukaisen hätäohjausjärjestelmän koneilta, joiden ajonopeus ylittää 30 km/h. [4, 37]

Hätäohjausjärjestelmä voidaan toteuttaa joko täysin erillisenä järjestelmällä, tai prioriteettiohjauksella, jolloin hätäohjauksen tehon lähdettä voidaan hyödyntää myös muissa toiminnoissa. Hätäohjauksella on kuitenkin oltava muita toimintoja korkeampi prioriteetti, hätäpysäytystä lukuun ottamatta. Hätäohjauksen toiminta todennetaan normaalin ohjauksen tavoin standardissa ISO 5010 määritellyn testiradan 1 mukaisesti. Erona ovat erilaiset vaatimukset ohjausvoimassa, ohjausajassa sekä ajonopeudessa. Hätäohjauksen tehonlähteen vasteen sopivuus todennetaan testiradalla 2 simuloimalla normaalin ohjauksen tehonlähteen vikaantuminen, minkä jälkeen koneen on kyettävä suorittamaan 90 asteen käännös. Hätäohjauksen on toimittava myös taaksepäin ajattaessa, mikäli ajoneuvon korkein sallittu nopeus on yli 20 km/h. [4] Standardin ISO 5010 testirata 2 esitellään liitteessä A.

### 3.2.4 Ohjauselementit

Ohjauselementillä tarkoitetaan toimilaitetta, jonka avulla kuljettaja välittää ohjauskäskyt koneelle. Tyypillisiä ohjauselementtejä ovat ohjauspyörät ja ohjausvivut. Koneessa voidaan hyödyntää useampaa ohjauselementtiä, joista valitun ensisijaisen ohjauselementin on kaikissa olosuhteissa oltava koneen ohjaajan käytettävissä. Ohjauselementin ohjaussuunnan on luonnollisesti oltava yhtenäinen ajoneuvon kääntymissuuntaan. Erityyppisille ohjauselementeille on määritelty suurimmat ja pienimmät sallitut käyttövoimat, jotka esitellään taulukossa 2.

**Taulukko 2.** *Ohjauselementin käyttövoimat [4]*

| Ohjaustoiminto | Ohjausvoimat | | |
|---|---|---|---|
| | Max. | Normaali | Min |
| **Käsi** | | | |
| - **Vipu, eteen/taakse** | 230 | 80 | 20 |
| - **Vipu, sivuttain** | 100 | 60 | 15 |
| **Sormenpää** | | | |
| - **Vipu tai kytkin** | 20 | 10 | 2 |

Paniikkiolosuhteita varten, standardissa ISO 5010 määritellään voimat, jotka ohjauselementin on kestettävä. Ohjauspyörältä vaadittava arvo on 900 N, ja taulukon 2 ohjauselementeiltä vaadittava arvo on maksimiohjausvoima kaksinkertaisena. Esimerkiksi sivuttain toimivan vivun on kestettävä vähintään 200 N ohjausvoima. [4]

Käytettävän ohjauselementin on täytettävä standardin ISO 10968 vaatimukset, jossa käsitellään ohjauselementin perusominaisuuksia, kuten ohjaussuuntaa sekä ohjauselementin sijoittamista ajoneuvoon. Ohjauselementit, jotka välittävät ohjaussignaalin sähköisesti tulee lisäksi täyttää sähkömagneettista yhteensopivuutta tarkastelevan standardin ISO 13766-1:2018 sekä maansiirtokoneiden turvallisuus standardisarjan SFS-EN ISO 19014 vaatimukset. [4] Standardi ISO 19014 korvaa aiemmin käytössä olleen standardin ISO 15998:2008, ja koostuu 5 osasta, joista osat 2, 4 ja 5 ovat toistaiseksi valmistelu vaiheessa.

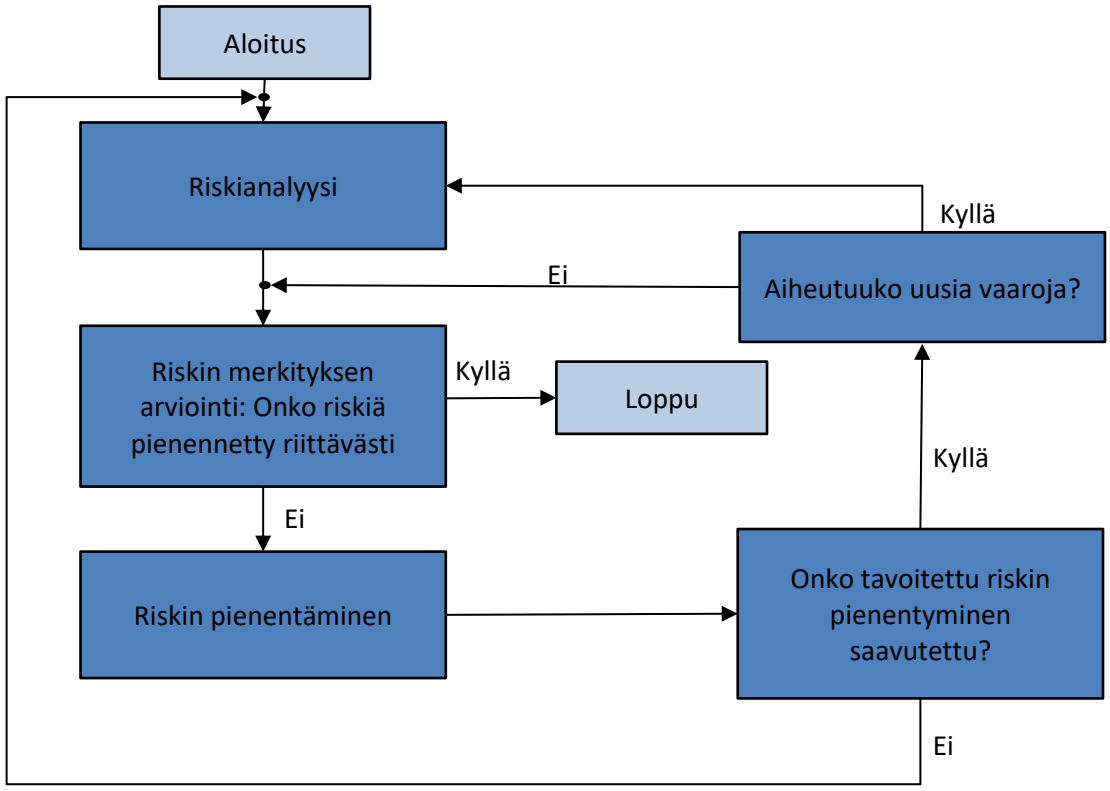
Ajoneuvoissa voidaan hyödyntää myös ylimääräisiä ohjauselementtejä, joille voidaan määrittää eri nopeusalueita verrattuna ensisijaiseen ohjauselementtiin. Sitä voidaan hyödyntää esimerkiksi sovelluksissa, jotka käyttävät maantieajossa eri ohjauselementtiä kuin esimerkiksi maastossa tai työmaalla. Koneen suurin sallittava nopeus lisäohjauselementtiä käytettäessä määritetään normaalin ohjauksen tavoin testiradalla. Vikaantumistilanteita varten lisäohjauselementtejä hyödyntävän koneen tulee suorittaa lisäksi erillinen standardissa ISO 5010 määritelty esteenväistämistestirata, joka esitellään liitteessä A. Korkeimmillaan lisäohjauselementin ollessa aktiivisena koneen

nopeus voi olla sama kuin ensisijaista ohjauselementtiä käytettäessä. Koneen on myös ilmoitettava kuljettajalle visuaalisesti tai äänimerkin avulla lisäohjauselementin ollessa aktiivisena. [4]

# 4. RISKIN ARVIOINTI JA PIENENTÄMINEN

Koneiden turvallisuussuunnittelun perustana käytetään konedirektiivissä ja standardissa ISO 12100 esiteltyä riskin arviointia, minkä pohjalta voidaan määrittää koneeseen sovellettavat turvallisuusvaatimukset. Riskin arviointi suositellaan tehtävän työryhmässä, joka sisältää eri alojen osaamista ja kokemusta. Työryhmässä tulisi olla riittävä tietämys ja kokemus koneen teknisistä ominaisuuksista, ymmärrys vaadittavista turvallisuussäännöksistä ja käyttöä koskevista inhimillisistä tekijöistä sekä tietoa vastaavan kaltaisten koneiden tapaturmatiedoista.[5, 42]

Standardissa ISO 12100 esitellyn riskin arvioinnin ja pienentämisen prosessi koostuu kolmesta päävaiheesta: riskianalyysistä, riskin merkityksen arvioinnista sekä riskin pienentämisestä. Riskien arviointi ja pienentäminen on iteratiivinen prosessi, jonka yksinkertaistettu malli esitetään kuvassa 9. Iteratiivisella prosessilla tarkoitetaan toimenpiteiden toistuvaa suorittamista, kunnes haluttu lopputulos on saavutettu. Prosessia suorittaessa on huomioitava koneen koko elinkaari, johon sisältyvät kyvykkyys suorittaa toiminnot, käytettävyys sekä valmistus-, käyttö ja purkukustannukset.




***Kuva 9.*** *Yksinkertaistettu riskin arvioinnin ja pienentämisen prosessi [5]*

Riskianalyysi sisältää koneen raja-arvojen määrittämisen, vaarojen tunnistamisen ja tunnistettujen riskien suuruuden arvioinnin. Analyysista saatujen tietojen avulla voidaan arvioida riskin merkitystä, ja päättää riskin pienentämisen tarve sekä toimenpiteet riskien minimoimiseksi. Riskien pienentämisen ensisijainen tavoite on poistaa kokonaan analyysissä havaitut vaaratilanteet. Sen ollessa mahdotonta, voidaan tarvittaessa turvautua suojausteknisiin toimenpiteisiin riskin pienentämiseksi. [5] Seuraavissa kappaleissa tarkastellaan prosessin eri osa-alueiden sisältöä.

## 4.1 Riskianalyysi

Koneen aiheuttamat vaarat kartoitetaan riskianalyysin avulla. Analyysi koostuu koneen raja-arvojen määrittämisestä, vaarojen tunnistamisesta ja havaittujen riskien suuruuden arvioinnista. Koneen raja-arvojen määrittämisellä pyritään kartoittamaan koneen fyysiset ominaisuudet, suorituskyky, ennakoitavissa oleva väärinkäyttö sekä käyttöympäristö, joiden avulla voidaan tunnistaa mahdolliset riskitekijät. Standardissa ISO 12100 raja-arvot jaetaan neljään ryhmään: käyttö-, tila- ja aikarajoihin sekä muihin raja-arvoihin. [5, 42]

Käyttörajoihin määritetään koneen tarkoituksen mukainen käyttö sekä ennakoitavissa oleva väärinkäyttö. Niihin määritetään kaikki koneella suoritettavat tehtävät, koneen hyödyntäjiltä ja kunnossapitäjiltä vaadittavat osaamistasot sekä fyysiset ominaisuudet, ja arvioitava muiden henkilöiden altistuminen koneen käytöstä johtuville vaaroille. [42] Raja-arvoon määritellään myös toimenpiteet ennakoitavissa olevaan väärinkäyttöön, kuten esimerkiksi koneen käytön suojaaminen salasanalla. Tilarajoihin määritetään koneen käyttöympäristö, liikkeiden laajuudet, tehonsyöttö, koneen käytön vaatima tila sekä käyttö- että huoltotoiminnan aikana ja käyttäjä-kone rajapinta. Raja-arvoihin voidaan määritellä myös koneelle sopimattomat ympäristöt, kuten esimerkiksi palo- tai räjähdysvaaralliset tilat. Aikarajoihin määritetään koneelle suositeltavat huoltovälit sekä -toimenpiteet. Koneen kuluvien osien eliniän arvioinnissa voidaan hyödyntää standardissa ISO 13849-1 esitettyä $T_{10D}$-arvoa, johon komponenttien toiminta-aika rajoitetaan. Muut raja-arvot sisältävät käytännössä loput mahdolliset koneen käyttöön vaikuttavat tekijät, joita ovat esimerkiksi käsiteltävän materiaalin ominaisuudet ja väliaineelta vaadittavat puhtausluokat. Huomioitavana on myös koneen käyttöympäristön arviointi, kuten koneen kosteuden-, pölyn- ja eri lämpötilojen sietokyky. [5]

Vaarojen tunnistaminen on koneen turvallisuuden kannalta kriittinen vaihe, sillä vasta vaarojen tunnistamisen jälkeen voidaan arvioida vaarojen aiheuttamien riskien suuruutta ja toteuttaa vaadittavat toimenpiteet vaarojen poistamiseksi tai aiheutuvien riskien

alentamiseksi siedättävälle tasolle. Tunnistamisessa tulee huomioida ihmisten vuorovaikutus, koneen mahdolliset toimintatilat, ennakoitavissa oleva koneen väärinkäyttö sekä käyttäjän tarkoittamaton käyttäytyminen. Vaarat voidaan kuvata tehtäväkohtaisesti huomioimalla koneen elinkaaren vaihe, suoritettavat tehtävät, tilarajoissa määritetyt vaaravyöhykkeet, aiheutuva vaara ja vaaratilanne, sekä vaaraan johtava tapahtuma. [5] Liikkuvan työkoneen törmäykseen liittyvää vaaratilannetta voidaan kuvata alla olevan esimerkin mukaisesti:

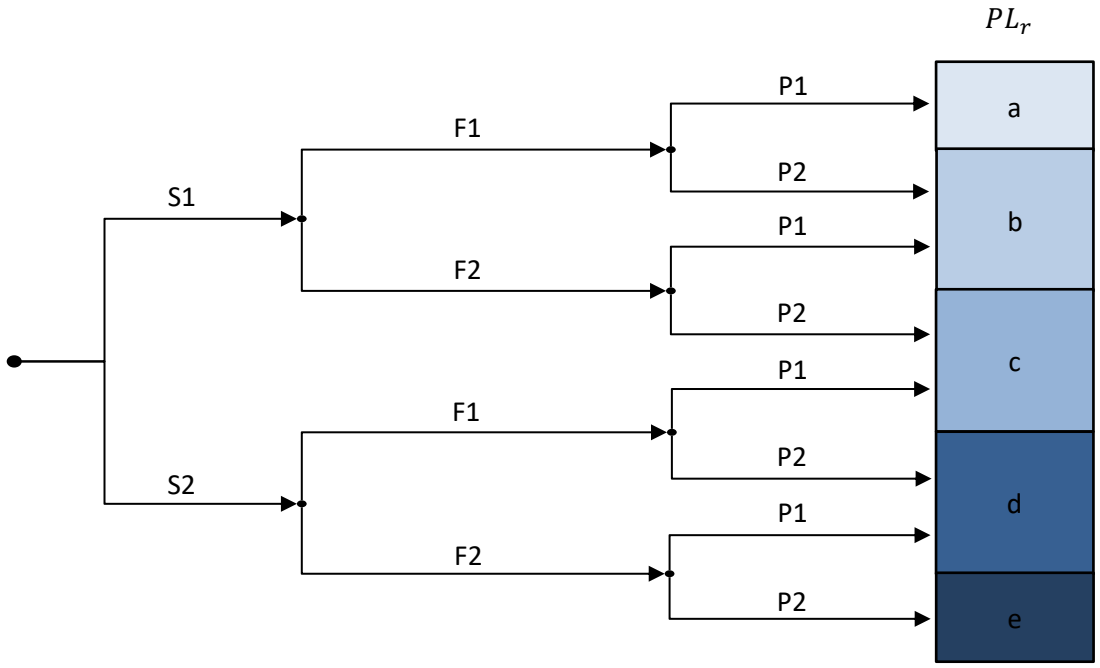
- Elinkaari: Käyttövaihe
- Vaaravyöhyke: Työskentelyvyöhyke
- Aiheutuva vaara: Yliajetuksi tuleminen
- Vaaratilanne: Kuljettaja ja muut koneen liikkeelle altistuvat henkilöt
- Vaarallinen tapahtuma: Ohjauksen menetys vikaantumisen seurauksena, ohjauksen menettäminen inhimillisen virheen seurauksena, koneen ulkopuolisen henkilön tai toisen koneen liike katvealueella.

Kaikki koneeseen liittyvät vaarat on huomioitava ja dokumentoitava, vaikka siedettävä riskitaso olisi jo saavutettu turvallisuussuunnittelun tai suojausteknisten toimenpiteiden seurauksena. Yksittäinen vaara voi olla seurausta useasta eri tekijästä ja vaarallisesta tapahtumasta, minkä vuoksi on tärkeätä tarkastella jokaista vaarallista tapahtumaa erikseen. [5]

Riskin suuruutta arvioidaan vaarasta aiheutuvan vamman vakavuuden, vaaralle altistumisen taajuuden/keston sekä vaaran välttämisen/vahingon rajoittamisen mahdollisuuden funktiona. Arviointiin on olemassa useita eri työkaluja, jotka tyypillisesti pohjautuvat riskimatriisiin, riskigraafiin, numeeriseen pisteytykseen tai edellä mainittujen menetelmien yhdistelmiin. [5] Tässä kappaleessa käsitellään riskigraafiin perustuvaa arviointia, joka esitellään standardissa ISO 13849-1. Kuvan 10 riskigraafi on standardissa ISO 13849-1 esitetty yksinkertainen menetelmä, joka soveltuu erityisesti äkillisten vaaratilanteiden arviointiin. Riskin arviointi tuottaa riskigraafin mukaisesti koneelta vaadittavan suoritustason arvon a-e, joista a kuvaa alhaisinta ja e korkeinta riskiä. [5, 34]

Riskin suuruuden arviointi aloitetaan arvioimalla vamman vakavuus. Lieviä vammoja (S1) ovat tavallisesti palautuvia vammoja, kuten esimerkiksi ruhjeet ja haavaumat. Vakaviksi vammoiksi (S2) luokitellaan palautumattomat vammat kuten raajojen irti leikkautuminen ja kuolema. Huomioitava on myös vahingon laajuus, eli aiheutuuko vaarasta vammoja yhdelle vai useammalle henkilölle. Vaaralle altistumisen kestoksi

ja/tai taajuudeksi valitaan arvo F1 (harvoin) ainoastaan, mikäli vaaralle kertyvä altistumisaika on alle 5 % kokonaiskäyttöajasta, ja taajuus on maksimissaan kerran 15




minuutissa. Muissa tapauksissa luokaksi on valittava toistuvasti vaaralle altistumista kuvaava arvo F2.

***Kuva 10.*** *Riskigraafi [34]*

Vaaran välttämisen mahdollisuutta voidaan arvioida esimerkiksi sen syntymisen nopeuden, käytön valvonnan ja aiempien turvallisuuskokemuksien perusteella. Mikäli vaaratilanteessa on mahdollista vähentää vaaran vaikutusta tai välttää vaara täysin, valitaan riskigraafista arvo P1. Muussa tapauksessa on valittava arvo P2. Vaaran välttämisen mahdollisuuteen voidaan vaikuttaa esimerkiksi merkinantolaitteilla ja käyttäjien koulutuksella. [34]

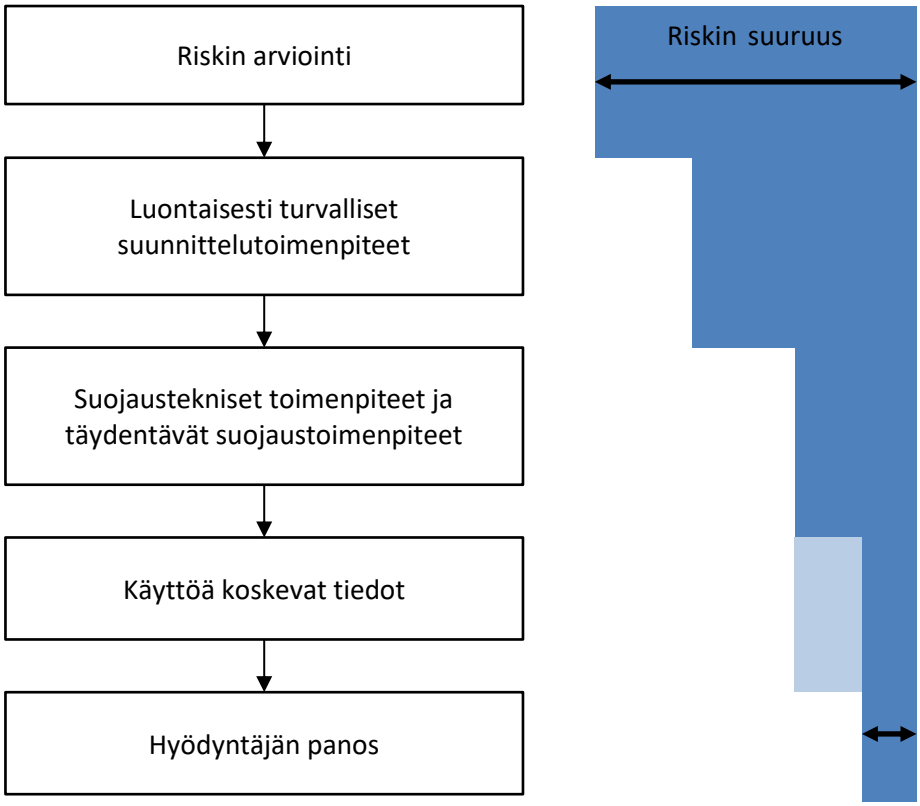
## 4.2 Riskin merkityksen arviointi ja pienentäminen

Iteratiivisen riskin arviointi prosessin viimeinen askel on riskin merkityksen arviointi. Riskien merkitystä arvioitaessa on huomioitava kaikki mahdolliset toimintaolosuhteet, suojaustoimenpiteiden yhteensopivuus ja niiden aiheuttamat uudet vaarat sekä mahdolliset jäännösriskit. Koneen tai sen osien riskien arvioinnissa voidaan hyödyntää toisten koneiden ja koneen osien riskitietoja, olettaen niiden olevan vertailukelpoisia niin teknisesti, noudatettavien standardien että olosuhteiden osalta. Riskin arviointi katsotaan suoritetuksi, mikäli saavutetun riskitason voidaan dokumentoidusti osoittaa olevan riittävän alhainen. [5]

Riskin pienentäminen on kolmivaiheinen hierarkkinen prosessi, jonka vaiheita ovat luontaiset turvalliset suunnittelutoimenpiteet, suojaustekniset toimenpiteet ja riskin pienentäminen käyttöä koskevien tietojen avulla. Prosessin jokaisella askeleella riskiä pyritään pienentämään mahdollisimman paljon, kuten kuvassa 11 esitetään. Ensisijaisena tavoitteena on poistaa havaittu vaara kokonaan turvallisten suunnittelumenetelmien avulla. Mikäli havaittua vaaraa ei ole mahdollista täysin poistaa, riskin minimoinnissa voidaan hyödyntää suojausteknisiä ja täydentäviä suojaustoimenpiteitä. [5]

Luontaisilla turvallisilla suunnittelumenetelmillä tarkoitetaan koneen rakenteellisia ominaisuuksia, jotka vaikuttavat vaaratilanteiden muodostumiseen. Koneen käyttäjän näkyvyyden parantaminen ja katvealueiden pienentäminen peileillä, liikenopeuksien rajoittaminen, ylikuorman aiheuttamien rasitusten estäminen paineenrajoitusventtiileillä sekä ergonomisten periaatteiden huomioiminen ovat esimerkkejä luontaisesta turvallisesta suunnittelusta. Suunnittelussa on myös huomioitava koneen elinkaareen kuuluvien huoltotoimenpiteiden suorittamisen helppous ja minimoitava vaara-alueilla suoritettavien kunnossapitotoimenpiteiden määrä. Ohjausjärjestelmiä koskevia turvallisia suunnittelunäkökohtia käsitellään standardeissa ISO 13849-1, jota tarkastellaan tämän työn kappaleessa 5. Prosessin ensimmäinen askel on tehokkain keino riskien pienentämiseen, sillä suojalaitteiden käyttäminen lisää mahdollisia vikaantumiskohteita, ja käyttöä koskevat tiedot kuten varoituskilvet ja varoituslaitteet vain ilmoittavat mahdollisesta vaarasta.[5]

Suojausteknisiin ja täydentäviin toimenpiteisiin voidaan turvautua, mikäli luontaisilla turvallisilla suunnittelutoimenpiteillä ei saavuta riittävää riskin pienentämistä. Turvalaitteiden valitsemisessa ja suunnittelussa on huomioitava vaaravyöhykkeelle pääsyn tarve normaalin toiminnan aikana, sekä pyrittävä estämään turvalaitteiden toimimattomaksi tekeminen. Hyviä esimerkkejä turvalaitteista ovat rajakytkimet, valoverhot sekä tuntomatot. Turvalaitteet voivat aiheuttaa uusia turvallisuusriskejä, jotka ovat huomioitava kuvassa 9 esitetyn riskien arvioinnin ja pienentämisen prosessin mukaisesti.[5]




***Kuva 11.*** *Riskin pienentämisen prosessi [5]*

Mikäli kahden ensimmäisen askeleen jälkeen riskiä ei ole pienennetty riittävälle tasolle, jäännösriskistä on selvästi ilmoitettava käyttäjälle. Riskin luonteesta riippuen, siitä voidaan ilmoittaa esimerkiksi koneen mukana toimitettavissa asiakirjoissa tai varoituskilvin. Kirjallisen ilmoituksen lisäksi riskin ilmoittamisessa voidaan hyödyntää erilaisia merkinanto ja varoituslaitteita. Käyttöä koskevat tiedot eivät alenna riskiä ilman koneen hyödyntäjän omaa panosta, jonka suuruutta kuvataan kuvassa 11 vaaleansinisellä. Tämänkaltaisia toimenpiteitä ovat esimerkiksi koneen suunnittelijan käyttöä koskevien tietojen noudattaminen, koneen käytön valvonta sekä käyttäjien ja muiden koneen toimintaan vaikuttavien henkilöiden koulutus. [5]

# 5. OHJAUSJÄRJESTELMÄ

Koneen riskin pienentämisessä hyödynnetään turvatoimintoja suorittavia ohjausjärjestelmän suojausteknisiä laitteita, joita kutsutaan turvallisuuteen liittyviksi ohjausjärjestelmän osiksi (engl. Safety Related Parts of Control System, SRP/CS). Turvatoimintoa suorittava ohjausjärjestelmä voi koostua yhdestä tai useammasta osasta. Tyypillinen yksinkertainen turvatoimintoa suorittava järjestelmä voidaan pilkkoa tulo-, logiikka- ja lähtöyksikköön sekä näiden välisiin liitäntävälineisiin. Kyseisten osien suunnittelussa ja toteutuksessa on noudatettava edellisessä kappaleessa esitellyn standardin ISO 12100 periaatteita. Suunnittelussa on myös huomioitava koneen tarkoitetun käytön lisäksi ennakoitavissa olevia väärinkäyttötilanteita. [34]

Ohjausjärjestelmän kykyä suorittaa turvatoiminto voidaan arvioida standardissa ISO 13849-1 esiteltyjen suoritustasojen (engl. Performance Level, PL) ja standardissa IEC 62061 esiteltyjen turvallisuuden eheyden tasojen (engl. Safety Integrity Level, SIL) avulla. Suoritustasot jaetaan viiteen eri luokkaan a-e, joista a on matalin ja e korkein. Vastaavasti SIL-tasot ovat määritelty vaativuusjärjestyksessä luokkiin 1-4. Korkeinta luokkaa 4 pidetään tarpeettoman vaativana, eikä sitä käytetä koneturvallisuuden sovelluksissa [43](s. 147). Tasoa SIL 4 käytetään lähinnä prosessiteollisuudessa, jolloin vikaantumisella voi olla katastrofaalisia seurauksia. Standardien erilaisista määritelmistä huolimatta, suoritustasot ovat käännettävissä turvallisuuden eheyden tasoiksi standardista ISO 13849-1 löytyvän käännöstaulukon avulla. Ohjausjärjestelmää suunnitellessa standardeja ei kuitenkaan voida käyttää rinnakkain, vaan se on tehtävä käyttämällä ainoastaan toista mainituista standardeista. [34, 44] Tässä diplomityössä tarkastellaankin ohjausjärjestelmää lähinnä ISO 13849-1 mukaisesti, ja standardin IEC 62061 sisältöä tarkastellaan vain täydentävin osin.

Suoritustason määrittämisprosessissa on arvioitava sekä määrällisiä että laadullisia näkökohtia. Suoritustaso lasketaan määrällisten arvojen pohjalta, mutta myös suoritustasolle ominaisten laadullisten näkökulmien on täytyttävä, jotta ohjausjärjestelmä läpäisisi standardin ISO 13849-2 mukaisen kelpuutusprosessin. Määrällisiin näkökohtiin sisältyvät:

- Ohjauskanavan rakenne
- Ohjauskanavan ja sen osien vikaantumisajat
- Diagnostiikan kattavuus
- Yhteisvikaantuminen,

joita käsitellään kappaleessa 5.1 yhdessä standardissa ISO 13849-1 esitetyn suoritustason määrällisen arvioinnin yksinkertaisen lähestymistavan kanssa. Vastaavasti laadullisiin näkökohtiin luetaan:

- Ohjelmisto
- Turvatoimintojen käyttäytyminen vikaantumistilanteissa
- Kyky toteuttaa turvatoiminto
- Ympäristöolosuhteet,

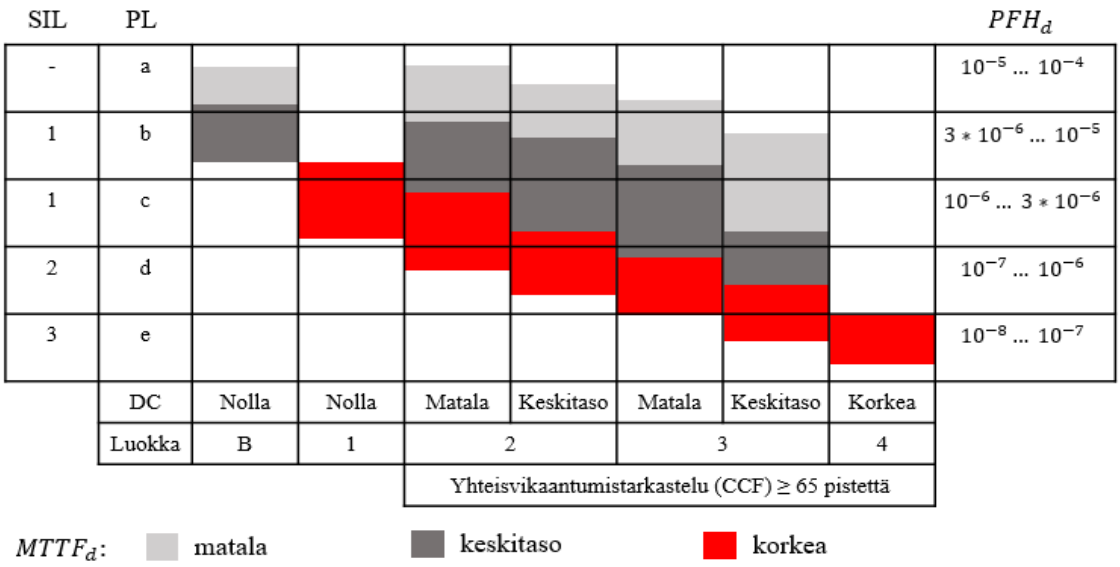
joita käsitellään kappaleessa 5.2. [34] Turvatoimintojen suoritustasojen määrittäminen vaatii merkittävästi laskentaa, useiden suoritustasokohtaisten vaatimusten täyttämistä sekä tarkkaa dokumentointia, minkä vuoksi suunnittelussa on edullista hyödyntää tietokoneavusteisia ohjelmia. Kappaleessa 5.3 esitellään standardin ISO 13849-1 vaatimuksiin pohjautuvan SISTEMA-ohjelman ominaisuuksia.

## 5.1 Määrälliset näkökohdat

Turvatoiminnon suoritustason määrittämisen ensimmäinen askel on vaarasta aiheutuvan riskin suuruuden arvioiminen, joka standardissa ISO 13849-1 arvioidaan kuvassa 10 esitetyn riskigraafin avulla. Ohjausjärjestelmän todellisen suoritustason on saavutettava vähintään riskin arvioinnissa todettu vaadittava suoritustaso. Suoritustason määrälliseen arviointiin vaikuttavat tekijät ovat:

- Keskimääräinen odotettavissa oleva aika vaaralliseen vikaantumiseen (engl. Mean Time to dangerous Failure, $MTTF_d$)
- Vaarallisen vikaantumisen todennäköisyys tuntia kohden (engl. Probability of dangerous failure per hour, $PFH_d$)
- Luokka
- Diagnostiikan kattavuus (engl. Diagnostic Coverage, DC).
- sekä ohjausjärjestelmän luokasta riippuen, yhteisvikaantumisen tarkastelu.

Kuvassa 12 esitetään suoritustasojen ja turvallisuuden eheystasojen, sekä niihin vaikuttavien tekijöiden keskinäisiä suhteita. [34]




***Kuva 12.*** *Suoritustasoon vaikuttavien tekijöiden keskinäinen suhde [34]*

Kuvassa 12 näkyvät suoritustasojen rajat ovat häilyvät, eikä sen pohjalta voida tehdä lopullisia johtopäätöksiä suoritustasoista. Se antaa kuitenkin hyvin selkeän kuvan eri suoritustasojen vaatimuksista. Esimerkiksi vaadittavan suoritustason ollessa PLd, ohjausjärjestelmän rakenteen on vähintään oltava luokkaa 2, diagnostiikan kattavuus voi alhaisimmillaan olla tasolla matala, keskimääräisen vikaantumisajan on oltava lyhyimmillään keskitasoa ja yhteisvikaantumisen tarkastelusta on saavutettava 65 pistettä. Eri suoritustasojen tarkat arvot esitellään standardin ISO 13849-1 liitteessä K, jonka arvot pohjautuvat ohjauskanavan rakenteeseen, vikaantumisaikaan sekä diagnostiikan keskimääräiseen kattavuuteen [5]. Seuraavissa alakappaleissa käsitellään suoritustasoon vaikuttavia tekijöitä tarkemmin.

### 5.1.1 Vikaantumisaika ja -taajuus

Keskimääräinen odotettavissa oleva aika vaaralliseen vikaantumiseen voidaan määrittää sekä yksittäisille komponenteille että useammista komponenteista koostuville kanaville ja ohjausjärjestelmille. Käytännössä $MTTF_d$-arvo kuvaa komponentin vikaantumisherkkyyttä ajan funktiona, ja sille on määritelty kolme tasoa:

- Matala: 3 vuotta ≤ $\boldsymbol{MTTF_d}$ < 10 vuotta
- Keskitaso: 10 vuotta ≤ $\boldsymbol{MTTF_d}$ < 30 vuotta
- Korkea: 30 vuotta ≤ $\boldsymbol{MTTF_d}$ < 100 vuotta

Kappaleessa 5.1.4 esiteltävien rakenteiden 1-3 mukaisten yksittäisten kanavien ja ohjausjärjestelmien korkein sallittu $MTTF_d$ -arvo on rajoitettu 100 vuoteen. Rakenteen 4 mukaisilla kanavoilla vastaava arvo on 2500 vuotta. [34]

$MTTF_d$ -arvot tyypillisesti saadaan komponentin valmistajalta, mikäli arvoja ei ole saatavilla, voidaan ne määrittää standardin ISO 13849-1 liitteessä C olevien taulukko arvojen avulla. Valmistaja voi ilmoittaa vikaantumisajan myös $B_{10D}$-arvona, joka kuvaa toimintajaksojen lukumäärää ennen kuin 10 % komponenteista on vaarallisesti vikaantunut. $B_{10D}$-arvoa käytetään usein komponenttien yhteydessä, joiden vikaantuminen ei ole riippuvainen ajasta, vaan toimintojen lukumäärästä. Tällaisia komponentteja ovat esimerkiksi sähkömekaaniset ON/OFF kytkimet.[43](s.133) $B_{10D}$-arvoon perustuva vikaantumisaika voidaan laskea kaavojen (9) ja (10) avulla.

$$MTTF_d = \frac{B_{10D}}{0{,}1 * n_{op}}, \tag{9}$$

jossa $n_{op}$ kuvaa keskimääräistä vuosittaista toimintajaksojen lukumäärää. Sitä voidaan arvioida kaavan (10) mukaisesti:

$$n_{op} = \frac{d_{op} * h_{op} * 3600 \frac{s}{h}}{t_{toimintajakso}}, \tag{10}$$

jossa $d_{op}$ on keskimääräinen toiminta-aika (päivää vuodessa), $h_{op}$ keskimääräinen toiminta-aika (tuntia päivässä), ja $t_{toimintajakso}$ kahden peräkkäisen toimintajakson alkamisajankohdan välinen keskimääräinen aikaväli (sekuntia per toimintajakso). $MTTF_D$-arvon lisäksi komponentille on määritettävä toiminta-aika $T_{10D}$, mihin mennessä 10 % komponenteista on vaarallisesti vikaantunut. $T_{10D}$-arvo lasketaan arvojen $B_{10D}$ sekä $n_{op}$ suhteena, ja se rajoittaa komponentin toiminta-ajaksi 10 % määritellystä $MTTF_D$-arvosta.

Edellä mainitut arvot koskevat vain yksittäisiä komponentteja. Suoritustason määrittämistä varten on selvitettävä jokaisen kanavan keskimääräinen vaarallinen vikaantumisaika. Turvallisuustoimintoa suorittava kanava koostuu useista komponenteista, jolloin kokonaisen kanavan vikaantumisaika voidaan määrittää kaavan (11) avulla:

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}}, \tag{11}$$

jossa $MTTF_d$ on koko kanavan ja $MTTF_{di}$ yksittäisen komponentin vikaantumisaika. Turvatoimintoa suorittava ohjausjärjestelmä voi koostua useammasta eri ohjauskanavasta, jolloin puhutaan kahdennetuista, eli redundanttisista ohjauskanavoista. Tämän seurauksena ohjauskanavien vikaantumisajat voivat poiketa toisistaan. Ohjausjärjestelmän suoritustasoa arvioitaessa on mahdollista käyttää

ainoastaan yhtä yhteistä arvoa. Ohjausjärjestelmän vikaantumisaikana voidaan hyödyntää myös symmetroitua arvoa, joka lasketaan kaavan (12) mukaisesti:

$$MTTF_d = \frac{2}{3}\left[MTTF_{\mathrm{d1}} + MTTF_{\mathrm{d2}} - \frac{1}{\frac{1}{MTTF_{\mathrm{d1}}} + \frac{1}{MTTF_{\mathrm{d2}}}}\right], \quad (12)$$

jossa $MTTF_{d1}$ ja $MTTF_{d2}$ ovat eri kanavan vaarallinen keskimääräinen vikaantumisaika. Symmetrointia voidaan hyödyntää vain, mikäli redundanttiset kanavat ovat toisistaan riippumattomia. Vaihtoehtoisesti turvatoimintoa suorittavan ohjausjärjestelmän vikaantumisaikana voidaan pahimman oletuksen periaatteen mukaisesti käyttää heikomman ohjauskanavan arvoa. [34]

Vaarallisen vikaantumisen todennäköisyys tuntia kohden, $PFH_d$, on yleinen vikaantumistaajuutta kuvaava yksikkö. Tarkasteltaessa yksittäisiä komponentteja tai yksikanavaisia ohjausjärjestelmiä, $MTTF_d$- ja $PHF_d$-arvojen välillä on kaavan (13) mukainen selkeä yhteys.

$$PFH_d = \frac{1}{X * MTTF_d} \quad (13)$$

jossa X on tuntien lukumäärä yhdessä vuodessa (8760 h). Tyypillisesti $PFH_d$ -arvoa käytetään kokonaisen ohjausjärjestelmän vikaantumisen mittarina, jolloin huomioidaan myös ohjausjärjestelmän rakenne ja diagnostiikka. Standardin ISO 13849-1 liitteessä K esitellään kattava taulukko, jonka avulla $PFH_d$-arvo voidaan määrittää $MTTF_d$-arvon pohjalta kaikille standardin ISO 13849-1 luokille. Taulukon $PFH_d$-arvot ovat laskettu standardin SFS-EN 62061 kappaleessa 6 esiteltyjen määritelmien mukaisesti. [34, 44]

### 5.1.2 Diagnostiikan kattavuus

Turvatoimintoa suorittavan ohjausjärjestelmän luotettavuutta mitataan diagnostiikan kattavuudella (engl. Diagnostic coverage, DC). Standardissa ISO 13849-1 diagnostiikan kattavuudelle on määritelty neljä eri tasoa, jotka esitellään taulukossa 3. Alhaisimmalla tasolla, eli alle 60 %:n diagnostiikan kattavuudella ei ole järjestelmän luotettavuuden kannalta suurta merkitystä, minkä vuoksi se ei ole sallittu arvo kaksi- tai useampikanavaisissa ohjausjärjestelmissä. Taulukossa esittävien rajojen tarkkuus on 5 %.

**Taulukko 3.** *Diagnostiikan kattavuus [27]*

| Merkintä | Vaihtelualue |
|---|---|
| Nolla/Ei lainkaan | DC < 60 % |
| Matala | 60 % ≤ DC < 90 % |
| Keskitaso | 90 % ≤ DC < 99 % |
| Korkea | 99 % ≤ DC |

Ohjausjärjestelmän yksittäisen osan diagnostiikan kattavuutta mitataan havaittujen vaarallisten vikaantumisen ja kaikkien vaarallisten vikaantumisen taajuuksien suhteena kaavan (14) mukaisesti

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_D}, \tag{14}$$

joka ilmaisee havaittavien vaarallisten vikaantumisten $\lambda_{DD}$ prosentuaalisen osuuden suhteessa havaitsemattomiin vikaantumisiin $\lambda_D$. Diagnostiikan kattavuus määritetään usein vika- ja vaikutusanalyysin avulla, ja se on usein saatavilla komponentin valmistajalta.

Standardin ISO 13849-1 liitteessä E esitellään yksinkertainen lähestymistapa diagnostiikan kattavuuden arviointiin, jossa arvioidaan useita lähtöyksikön, logiikan ja tuloyksikön valvonnan toimenpiteitä, kuten suoran-, epäsuoran ja ristiinvalvonnan vaikutusta diagnostiikan kattavuuteen. Standardin esittämät toimenpiteet esitellään kokonaisuudessaan liitteessä B.

Kokonaisen ohjausjärjestelmän diagnostiikan kattavuutta kutsutaan keskimääräiseksi diagnostiikan kattavuudeksi, ja se voidaan laskea kaavan 15 mukaisesti

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{\mathrm{d}1}} + \frac{DC_2}{MTTF_{\mathrm{d}2}} + \cdots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{\mathrm{d}1}} + \frac{1}{MTTF_{\mathrm{d}2}} + \cdots + \frac{1}{MTTF_{dN}}}, \tag{15}$$

jossa $DC_1$, $DC_2$ ja $DC_N$ ovat yksittäisten osien diagnostiikan kattavuudet. Diagnostiikan kattavuutta arvioitaessa on oleellista huomioida, ettei sillä tarkoiteta testauslaitteen, kuten tilavuusvirtasensorin, vaan mitattavan komponentin, kuten venttiilin, diagnostiikan kattavuutta. Testaamattoman komponentin diagnostiikan kattavuus on nolla, mutta sen vikaantumisaika sisällytetään ohjausjärjestelmän keskimääräisen diagnostiikan kattavuuden arviointiin. [34]

### 5.1.3 Yhteisvikaantuminen

Kahden tai useamman kohteen samanaikainen vikaantumista yksittäisen tapahtuman seurauksena kutsutaan yhteisvikaantumiseksi (engl. Common cause failure, CCF). Ohjausjärjestelmän kohdalla yhteisvikaantuminen on aina turvallisuusriski, sillä jokaisen kanavan samanaikainen vikaantuminen johtaa ohjauksen menettämiseen. Ohjausjärjestelmän vikasietoisuustila kuvaa sen kykyä säilyttää ohjattavuus yksittäisen vikaantumisen tapahtuessa. Esimerkiksi yksikanavaisen ohjausjärjestelmän tapauksessa vikasietoisuustaso on nolla, jolloin ensimmäisen vikaantuminen johtaa turvatoiminnon menettämiseen. Vastaavasti kaksikanavaisen ohjausjärjestelmän vikasietoisuus taso on 1, ja kolmikanavaisen ohjausjärjestelmän vikasietoisuuden taso on 2. Sen vuoksi, yhteisvikaantumista estävien toimenpiteiden arviointi määritellään ainoastaan luokille 2-4. [34, 43]

Kanavien yhteisvikaantumisen voi laukaista useat tekijät, kuten ohjelmistovirheet, sähkömagneettiset häiriöt ja ulkoisen voiman aiheuttama kaapeleiden katkeaminen. Ohjausjärjestelmän yhteisvikaantumista estäviä toimenpiteitä arvioidaan standardin ISO 13849-1 liitteen F pisteytysprosessin avulla, joka esitellään taulukossa 4.

***Taulukko 4.*** *Pisteytysprosessi ja yhteisvikaantumista estävien toimenpiteiden määrällinen arviointi [34]*

| Nro. | Yhteisvikaantumista estävä toimenpide | Pisteet |
|---|---|---|
| 1 | Erottelu/erottaminen | |
| | Signaalireittien fyysinen erottaminen, esimerkiksi:<br>— johdotuksen/putkituksen erilleen sijoittaminen<br>— oikosulkujen ja avointen piirien paljastaminen dynaamisella testauksella<br>— jokaisen kanavan signaalireittien erillinen suojaaminen<br>— riittävät ilma- ja pintavälit painetuissa piirilevyissä. | 15 |
| **2** | **Erilaisuus (diversiteetti)** | |
| | Erilaisten teknologioiden, toteutustapojen tai fyysisten periaatteiden käyttö, esimerkiksi:<br>— ensimmäinen kanava toteutetaan elektronisesti tai ohjelmoitavalla elektroniikalla ja toinen kanava sähkömekaanisesti kiinteästi langoitettuna<br>— turvatoimintojen eri kanavien erilainen käynnistystapa (esim. asema, paine, lämpötila) ja/tai<br>— muuttujien digitaalinen ja analoginen mittaaminen (esim. etäisyys, paine tai lämpötila) ja/tai eri valmistajien komponentit. | 20 |
| **3** | **Suunnittelu, soveltaminen ja kokemukset** | |
| 3.1 | Suojaustoimenpiteet ylijännitteelle, ylipaineelle, ylivirralle, liian korkealle lämpötilalle jne. | 15 |
| 3.2 | Käytetyt komponentit ovat hyvin koeteltuja | 5 |
| **4** | **Arviointi ja analyysit** | |
| | Turvallisuuteen liittyvien ohjausjärjestelmän osien jokaiselle osalle on tehty vika- ja vaikutusanalyysi ja sen tulokset on otettu huomioon suunnittelussa yhteisvikaantumisen estämiseksi. | 5 |
| **5** | **Pätevyys ja koulutus** | |
| | Suunnittelijat koulutetaan ymmärtämään yhteisvikaantumisten syyt ja | 5 |
| **6** | **Ympäristöolosuhteet** | |
| 6.1 | Likaantumisen ja sähkömagneettisten häiriöiden (EMC, engl. electromagnetic compability) estäminen sähköisissä/elektronisissa järjestelmissä yhteisvikaantumisten estämiseksi soveltuvien standardien mukaisesti (esim. IEC 61326–3–1).<br><br>Pneumaattiset- ja hydrauliset järjestelmät: väliaineen suodatus, likaisen imuilman estäminen ja paineilman kuivatus, esim. komponentin valmistajan esittämien väliaineen puhtausvaatimusten mukaisesti.<br><br>HUOM. Yhdistetyt sähköiset ja hydrauliset tai pneumaattiset järjestelmät: olisi otettava huomioon molemmat edellä mainittavat näkökohdat | 25 |
| 6.2 | Muut vaikutukset<br><br>Kaikkien asiaan liittyvien ympäristövaikutusten välttämiseksi on otettava huomioon sietokyky, esim. lämpötila, iskut, tärinä, kosteus (asiaankuuluvien standardien erittelyn mukaisesti). | 10 |
| | **Yhteensä** | **100** |

| Kokonaispisteet | Toimenpiteet yhteisvikaantumisen välttämiseksi (ks. a) |
|---|---|
| 65 tai enemmän | Täyttää vaatimukset |
| Vähemmän kuin 65 | Ei täytä vaatimuksia, vaatii lisätoimenpiteitä |

a. Jos teknologiset toimenpiteet eivät ole asiaan kuuluvia, tähän sarakkeeseen liittyviä pisteitä voidaan tarkastella kokonaisvaltaisessa laskelmassa.

Pisteytysprosessi on jaettu kahdeksaan osa-alueeseen. Pisteiden saavuttamiseksi, kunkin osa-alueen kaikkien vaatimusten on täytyttävä, jolloin arvioinnin kohteelle voidaan merkitä ainoastaan joko täydet pisteet tai nolla pistettä. Tarkastelussa oletetaan yhteisvikaantumisalttiuden (β) olevan korkeintaan 2 %. Yhteisvikaantumisalttius kuvaa yhteisvikaantumisten prosenttiosuutta kaikista vikaantumisista. [45]

### 5.1.4 Kanavien rakenteet

Ohjausjärjestelmien rakenteet luokitellaan viiteen luokkaan vaativuusjärjestyksessä: B, 1, 2, 3 ja 4. Luokat B ja 1 ovat täysin yksikanavaisia rakenteita, jotka menettävät turvatoiminnon hallinnan yksittäisen vikaantumisen seurauksena. Luokka 2 on yksikanavainen rakenne, joka sisältää turvatoimintoa säännöllisesti tarkastelevan testauslaitteiston. Myös luokan 2 ohjausjärjestelmien vikasietoisuustila on nolla, mutta diagnostiikan avulla järjestelmä voidaan saattaa turvalliseen tilaan vikaantumisen tapahtuessa. Luokat 3 ja 4 ovat redundanttisia järjestelmiä, jotka säilyttävät ohjattavuuden yksittäisen vikaantumisen sattuessa.

Ohjausjärjestelmän kanavien rakenteilla on merkittävä vaikutus suoritustasoon, ja ohjausjärjestelmän rakenne tyypillisesti määräytyy vaadittavan suoritustason mukaan. Luokkien rakenteissa huomioidaan myös edellä käsiteltyjä ominaisuuksia, kuten diagnostiikan kattavuutta sekä keskimääräistä vaarallisen vikaantumisen aikaa. Huomioitava on, etteivät luokkien 3 ja 4 rakenteet välttämättä ole fyysisesti rinnakkaisia kanavoita, vaan sisältävät rinnakkaisia ominaisuuksia, joiden ansiosta vikasietoisuustaso on vähintään 1.

**Luokat B ja 1** ovat rakenteeltaan yksikanavaisia ohjausjärjestelmiä, joka koostuu tulo-, logiikka- ja lähtöyksiköstä, kuten kuvassa 13 esitellään. Osien välisiä liitäntävälineitä kuvataan tekijällä $i_m$. Ominaista molemmille luokille on diagnostiikan puuttuminen, sekä ohjauksen menettäminen jo ensimmäisen vikaantumisen seurauksena. Luokka B (Basic) on perusluokka, jonka vaatimukset koskevat myös luokkia 1-4. Saavuttaakseen luokan B vaatimukset, ohjausjärjestelmän suunnittelussa on noudatettava yleisiä turvallisuuden perusperiaatteita niin, että järjestelmä ja sen osat, kestävät odotettavissa olevat käyttökuormitukset, käsiteltävien aineiden vaikutukset sekä muut merkittävät ulkoiset vaikutukset. Luokan B ohjausjärjestelmät voivat parhaimmillaan saavuttaa suoritustason b.

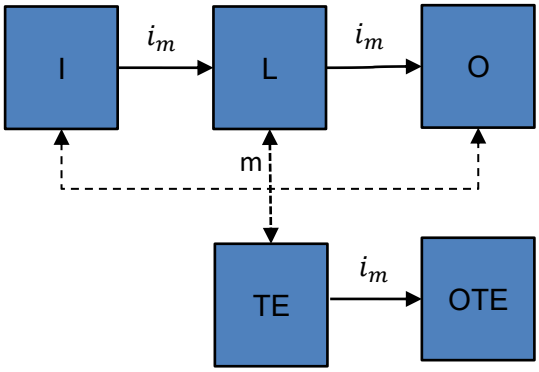

I Tuloyksikkö
L Logiikka
O Lähtöyksikkö
$i_m$ Liitäntävälineet

***Kuva 13.*** *Luokkien B & 1 mukainen rakenne [34]*

Luokan 1 ohjausjärjestelmä täyttää kaikki luokan B vaatimukset. Niiden lisäksi ohjausjärjestelmässä on käytettävä hyvin koeteltuja komponentteja sekä hyvin koeteltuja turvallisuusperiaatteita, kuten varmuuskertoimien käyttöä. Kyseisiä vaatimuksia sovelletaan myös luokissa 2-4. Tämän lisäksi luokan 1 vikaantumisajan on oltava tasolla korkea eli vähintään 30 vuotta, minkä ansiosta luokan 1 ohjausjärjestelmällä saavutetaan suoritustaso c, joka on yhtä tasoa korkeampi kuin luokalla B. Tarkemmat kuvaukset yleisistä ja hyvin koetelluista turvallisuuden perusperiaatteista esitellään standardin ISO 13849-2 liitteissä A, B, C ja D.

**Luokan 2** ohjausjärjestelmä on rakenteeltaan myös yksikanavainen, mutta sen yhteydessä on turvatoimintojen testauslaitteisto, kuten kuvasta 14 nähdään. Turvatoimintojen tarkastus toteutetaan aina koneen käynnistyksen yhteydessä, sekä ennen jokaista ohjausjärjestelmällä ohjattavaa toimintajaksoa. Turvatoiminnot sallivat käyttötoiminnan, mikäli vikoja ei tarkastuksen yhteydessä paljastunut. Mikäli vika paljastuu tarkastuksessa, testauslaitteiston ulostulosignaali (OTE) käynnistää tarvittavan ohjaustoiminnon, esimerkiksi. turvatilan tai varoituksen.

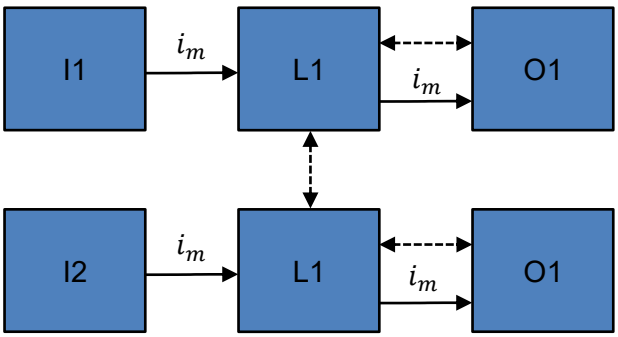
Luokan 2 rakenteella korkein saavutettava suoritustaso on PLd, joka on toisiksi korkein suoritustaso. Suurin ongelma luokan 2 rakenteessa on korkea testaustaajuus. Turvatoimintojen tarkastus tulee suorittaa vähintään 100 kertaa jokaista toimintoa kohden, minkä vuoksi luokan 2 rakenne soveltuu huonosti jatkuva toimisiin laitteisiin. [34]




| | |
|---|---|
| I | Tuloyksikkö |
| L | Logiikka |
| O | Lähtöyksikkö |
| $i_m$ | Liitäntävälineet |
| m | Valvonta |
| TE | Testauslaitteisto |
| OTE | Testauslaitteiston lähdöt |

***Kuva 14.*** *Luokan 2 mukainen rakenne [34]*

**Luokat 3 ja 4** ovat kaksi- tai useampi kanavaisia ohjausjärjestelmiä, joiden rakenne esitellään kuvassa 15. Redundanttisten kanaviensa ansiosta, molempien luokkien vikasietoisuustaso on vähintään 1, jolloin ohjattavuus säilyy yksittäisen vikaantumisen seurauksena. Käytännössä katsoen, luokka 4 on identtinen luokan 3 kanssa, mutta sen diagnostiikan kattavuus on korkeampi, ja sen jokaisen kanavan $MTTF_d$ -arvon täytyy olla tasolla korkea. Kuvassa 15 esiintyvät katkoviivat kuvastavat luokan 3 heikompaa diagnostiikan tasoa. Mallinnettaessa luokan 4 rakenne, kuvataan logiikoiden keskinäistä sekä logiikoiden ja ulostulojen välistä valvontaa yhtenäisellä viivalla. [34]




| | |
|---|---|
| I1, I2 | Tuloyksiköt |
| L1, L2 | Logiikat |
| O1,O2 | Lähtöyksiköt |
| $i_m$ | Liitäntävälineet |
| m | Valvonta |

***Kuva 15.*** *Luokkien 3 ja 4 rakenne [34]*

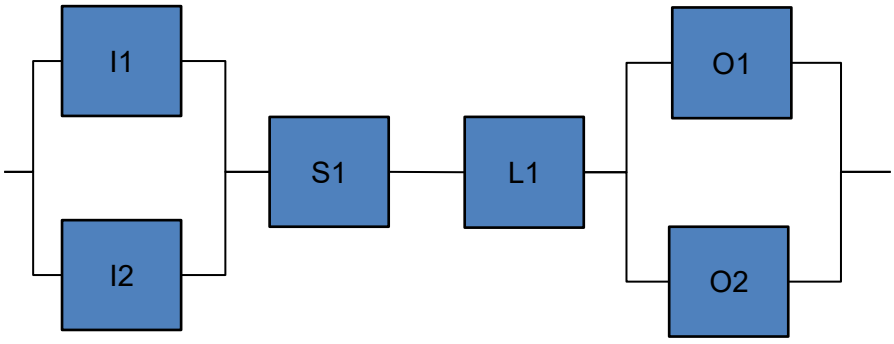
Luokilla 3 ja 4 korkein saavutettavissa oleva suoritustaso on e, joka on korkein saavutettavissa oleva taso. Rinnakkaisilla kanavoilla voidaan saavuttaa korkeammat suoritustasot kuin yksikanavaisilla rakenteilla. Ne eivät kuitenkaan automaattisesti takaa korkeampaa suoritustasoa, kuten kuvasta 12 huomataan. Hyvin koetelluista komponenteista rakennetulla yksikanavaisella ohjausjärjestelmällä voidaan saavuttaa korkeampi suoritustaso kuin heikommista komponenteista rakennetulla kaksikanavaisella ohjausjärjestelmällä.

### 5.1.5 Yhdistettyjen osien kokonaissuoritustaso

Turvatoimintoa suorittava ohjausjärjestelmän osa koostuu tyypillisesti useammista eri komponenteista/alajärjestelmistä, jolloin järjestelmän rakennetta tarkastellaan lohkomenetelmän mukaisesti sarjan tai rinnankytkentänä. Alhaalta ylös lähestymistavan mukaisesti on ensin selvitettävä komponenttien ja ohjauskanavien suoritustasot, joiden avulla muodostetaan lopullinen turvatoimintoa suorittavan ohjausjärjestelmän suoritustaso.

Turvatoimintoa suorittavan ohjausjärjestelmän suoritustason laskemista varten on määriteltävä ohjausjärjestelmän luokka, sekä laskettava kanavien keskimääräiset vaaralliset vikaantumisajat ja ohjausjärjestelmän keskimääräinen diagnostiikan kattavuus. Luokkien 2, 3 ja 4 osalta suoritetaan lisäksi yhteisvikaantumisen arviointi, joka esiteltiin taulukossa 4. Turvatoiminnon saavuttamaa suoritustasoa voidaan arvioida kuvan 12 avulla, tarkat lukuarvot ovat luettavissa standardin ISO 13849-1 liitteestä K.

Kuvassa 16 esitellään eräs kaksikanavainen ohjausjärjestelmä, joka koostuu sensorista (S1), ohjausyksiköstä (L1) sekä kahdesta tulosta (I1, I2) ja lähdöstä (O1, O2). Ohjausyksikkö sekä sensori ovat rakenteeltaan redundanttisia, jolloin kokonaisen ohjausjärjestelmän luokaksi saadaan 3 tai 4, riippuen diagnostiikan kattavuudesta. Järjestelmän ensimmäinen ohjauskanava koostuu osista I1-S1-L1-O1, ja vastaavasti toinen ohjauskanava koostuu osista I2-S1-L1-O2.



***Kuva 16.*** *Eräs turvatoiminnon suorittava ohjausjärjestelmä*

Ohjauskanavien suoritustasojen laskentaa varten on tiedettävä sen osien rakenteiden luokat, vikaantumisajat sekä diagnostiikan kattavuudet. Kuvan 16 ohjausjärjestelmän osien arvoiksi ilmoitetaan:

- I1 ja I2
    - Luokka: 1
    - $MTTF_d$: 50
    - DC: 90 % (epäsuora valvonta)
- S1 ja L1
    - Luokka: 3
    - $MTTF_d$: 100
    - DC: 95 %
- O1
    - Luokka: 1
    - $MTTF_d$: 150 vuotta
    - DC: 90 % (epäsuora valvonta)
- O2
    - Luokka: 1
    - $MTTF_d$: 100 vuotta
    - DC: 90 % (epäsuora valvonta)

Ohjauskanavoille voidaan laskea yhteiset vikaantumisajat sijoittamalla lukuarvot kaavaan (11), jolloin arvoiksi saadaan:

$$\frac{1}{MTTF_{d1}} = \frac{1}{50\ vuotta} + \frac{1}{100\ vuotta} + \frac{1}{100\ vuotta} + \frac{1}{150\ vuotta} = \frac{0{,}047}{vuosi},$$

joka vastaa 21,4 vuotta, ja

$$\frac{1}{MTTF_{d2}} = \frac{1}{50\ vuotta} + \frac{1}{100\ vuotta} + \frac{1}{100\ vuotta} + \frac{1}{100\ vuotta} = \frac{0{,}05}{vuosi},$$

joka vastaa 20 vuotta. Vikaantumisajat poikkeavat toisistaan, jolloin kokonaisen ohjausjärjestelmän vikaantumisaika voidaan symmentroida kaavan (12) mukaisesti, jolloin saadaan

$$MTTF_d = \frac{2}{3}\left[21{,}4 + 20 - \frac{1}{\frac{1}{21{,}4} + \frac{1}{20}}\right] = 20{,}7\ vuotta,$$

joka standardin määritysten mukaan vastaa keskitasoista vikaantumisaikaa. Ohjausjärjestelmän keskimääräinen diagnostiikan kattavuus saadaan selville sijoittamalla molempien ohjauskanavoiden lukuarvot kaavaan (15), jolloin saadaan

$$DC_{avg} = \frac{\frac{0{,}9}{50} + \frac{0{,}9}{50} + \frac{0{,}95}{100} + \frac{0{,}95}{100} + \frac{0{,}95}{100} + \frac{0{,}95}{100} + \frac{0{,}9}{150} + \frac{0{,}9}{100}}{\frac{1}{50} + \frac{1}{50} + \frac{1}{100} + \frac{1}{100} + \frac{1}{100} + \frac{1}{100} + \frac{1}{150} + \frac{1}{100}} = 0{,}92,$$

joka vastaa keskitasoista diagnostiikan kattavuutta. Ohjausjärjestelmän rakenteen, vikaantumisajan ja keskimääräisen diagnostiikan kattavuuden arvon avulla voidaan standardin ISO 13849-1 liitteestä K suoritustasoksi lukea arvo d. Määrällisen arvioinnin lisäksi ohjausjärjestelmän on täytettävä myös muita vaatimuksia, kuten hyvin koeteltujen komponenttien ja turvallisuusperiaatteiden käyttämistä, systemaattisten vikaantumisten arviointia ja ohjelmistojen turvallisuusvaatimusten noudattamista. [34]

## 5.2 Suoritustason laadulliset näkökohdat

Järjestelmältä vaadittavia laadullisia näkökohtia ei voida arvioida yhtä yksi selitteisesti kuin edellä tarkasteltuja määrällisiä näkökohtia. Laadulliset näkökohdat vaikuttavat järjestelmän käyttäytymiseen, ja niihin sisältyvät turvallisuuteen liittyvä ohjelmisto, systemaattinen vikaantuminen, ympäristöolosuhteet sekä järjestelmän käyttäytyminen vikatilanteissa. Seuraavissa kappaleissa tarkastellaan systemaattisten vikaantumisten ja turvatoimintoihin liittyvien ohjelmistojen ominaisuuksia sekä vaatimuksia.

### 5.2.1 Systemaattinen vikaantuminen

Vikaantumisia, jotka tapahtuvat aina tietyissä olosuhteissa, kutsutaan systemaattiseksi vikaantumiseksi. Tyypillisiä systemaattisen vikaantumisen syitä ovat esimerkiksi valmistus ja kokoonpano virheet, suunnitteluvirheet sekä vääränlainen kunnossapito ja/tai käyttö. Lisäksi tehon syötön katkeaminen sisältyy systemaattisen vikaantumisen tarkasteluun. Simuloinnilla ja testaamisella voidaan tunnistaa järjestelmän systemaattiset virheet, mutta käytännössä suunnitteluvaiheessa ei ole mahdollista simuloida jokaista vikaantumiseen johtavaa tapahtumaa. Hyödyntämällä standardissa

ISO 13849-2 esiteltyjä turvallisuuden perusperiaatteita suunnittelussa voidaan kuitenkin vaikuttaa systemaattisten vikaantumisten lukumäärään.

Suunnittelussa tulee huomioida koneen käyttövaatimusten lisäksi myös käyttöympäristön vaatimukset, kuten kosteus, lämpötila, tärinä sekä sähkömagneettiset häiriöt, joita voidaan hyödyntää koneen mitoituksessa ja sopivien materiaalien sekä valmistustapojen valinnassa. Komponenttien valinnassa on huomioitava yhteensopivuus järjestelmän muiden osien kanssa, sekä hyödynnettävä valmistajan tarjoamia tuotetietoja ja asennusohjeita. Valmistus sekä kokoonpano virheistä aiheutuviin vikaantumisiin voidaan puuttua tarkistamalla käytössä olevan laadunhallintajärjestelmän toimivuus. Standardissa ISO 13849-2 liitteissä A ja D esitellään turvallisuuden perusperiaatteet sekä hyvin koetellut turvallisuusperiaatteet teknologia ja komponenttikohtaisesti. [34, 46]

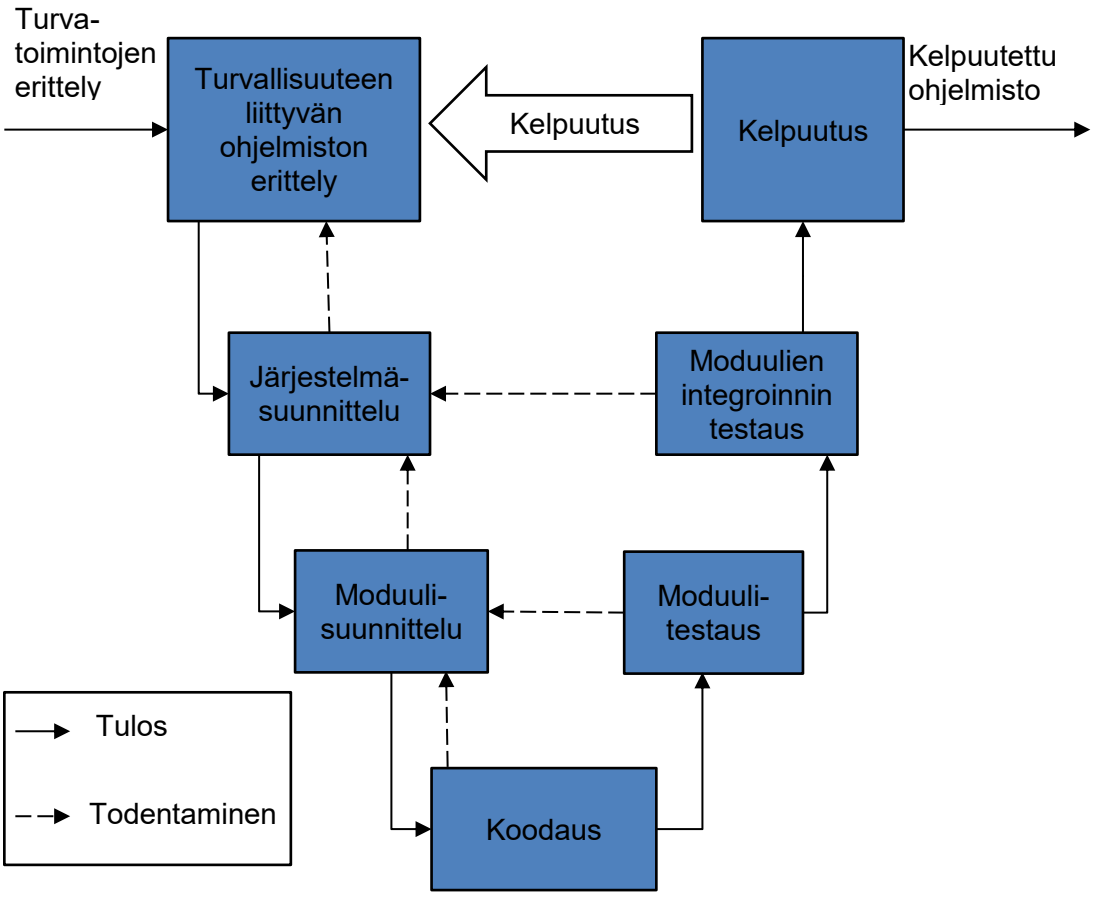
Systemaattisen vikaantumisen riskiä voidaan alentaa myös lisäämällä laitteiston monimuotoisuutta, suorittamalla vika-vaikutusanalyysi sekä tarkistamalla valmistuksen laadunhallintajärjestelmä. Yhteisvikaantumiset ovat usein seurausta systemaattisesta vikaantumisesta. Hyödyntämällä eri komponentteja tai teknologioita redundanttisissa kanavoissa voidaan myös madaltaa sekä systemaattisten että yhteisvikaantumista aiheuttavien virheiden riskiä. Erilaisten kanavoiden käytössä kuitenkin lisää järjestelmän kompleksisuutta, mikä saattaa aiheuttaa muita turvallisuusriskejä. [34, 47]

### 5.2.2 Ohjelmiston turvallisuusvaatimukset

Turvallisuuteen liittyvät ohjelmistot voidaan jakaa sovellusohjelmistoihin ja sulautettuihin ohjelmistoihin. Sovellusohjelmistot tyypillisesti hyödyntävät rajoitetun käskykannan ohjelmointikieltä, kuten tikapuukieltä tai toimilohkokaaviota, mutta se on toteutettavissa myös rajoittamattomalla ohjelmointikielellä, jolloin ohjelmiston on noudatettava sulautetulle ohjelmistolle asetettuja vaatimuksia. Sulautetuissa ohjelmistoissa käytetään rajoittamattoman käskykannan ohjelmointikieliä, kuten C++:aa tai Pythonia. [34]

Standardissa ISO 13849-1 esitellään molemmille ohjelmistotyypeille vaatimukset, jotka ovat yhdenmukaisia standardin IEC 62061 vaatimusten kanssa. Vaatimusten ensisijainen tavoite on luoda ymmärrettävää, luettavaa, testattavaa sekä ylläpidettävää ohjelmistoa. Tavoitteen saavuttamiseksi, standardissa esitellään ohjelmistosuunnittelussa käytettävä V-malli, joka koostuu useasta eri suunnittelun, toteutuksen sekä todentamisen eri vaiheista. Mallia voidaan hyödyntää sekä sovellusohjelmistojen, että sulautettujen ohjelmistojen suunnittelussa. [34]

Ohjelmistosuunnittelussa käytettävä V-malli on iteratiivinen prosessi, jossa edellisten vaiheiden tuotosten toimivuus todennetaan seuraavissa työvaiheissa. Todentamisen suorittaa suunnitteluun kuulumaton ulkopuolinen henkilö. V-mallin suurin etu on prosessin selkeä rakenne, joka soveltuu hyvin selkeästi määriteltyjen ohjelmistojen suunnitteluun. Mallin haittapuolena on heikko joustavuus vaatimusten muuttuessa. Puhtaasti V-mallin mukaisesti toteutetusta ohjelmista saadaan käyttäjän/asiakkaan palautetta vasta ohjelmiston kelpuutusvaiheessa. Tällöin riskinä on, että asetetut vaatimukset eivät vastaa todellista tarvetta, jolloin tarpeettomien tai viallisten vaatimusten täyttämiseen on turhaan käytetty resursseja. Toiminnallisissa ohjelmistoissa voi olla edullisempaa hyödyntää ketterää ohjelmistokehitystä, jossa suunnittelu, toteutus sekä todentamien ovat jatkuvaa iteratiivista toimintaa, jolloin suunnitelmia on helpompi muokata todellisten tarpeiden mukaiseksi. Ketterää ohjelmistokehitystä on toistaiseksi käytetty toiminnallisissa funktioissa, eikä turvatoimintojen suunnittelussa. Toiminnallisissa ohjelmistoissa asiakkaan tarpeet sekä nopea toimitus ovat ensisijaisia, vastaavasti turvatoimintojen suunnittelussa oleellisinta on turvallisuus ja luotettavuus sekä todelliset tarpeet. V-malli tarjoaa turvatoimintojen suunnitteluun selkeän ja helposti dokumentoitavan lähestymistavan, minkä vuoksi se on laajasti käytössä. [48] Yksinkertaistettu V-malli esitellään kuvassa 17.




***Kuva 17.*** *Ohjelmiston turvallisuuselinkaaren yksinkertaistettu V-malli [34]*

V-mallissa varsinainen ohjelmointi tehdään vasta koodaus-vaiheessa, jota edeltävät toimenpiteet ovat ohjelmistosuunnittelua. Vastaavasti V-mallin oikealla puolella olevat tehtävät koskevat ohjelmiston laadun todentamista ja kelpuutusta. Suunnittelun ensimmäisessä vaiheessa eritellään turvallisuuteen liittyvät toiminnot sekä tarkastellaan kunkin turvatoiminnon vaatimuksia, kuten vaadittavia suoritustasoja, arkkitehtuureja ja diagnostiikkojen toteutusta. Asetettujen vaatimusten suositellaan olevan ainutlaatuisia, yksiselitteisiä, todennettavissa olevia sekä helposti ymmärrettäviä. Lopulta vaatimukset ovat dokumentoitava todentamista varten. [49]

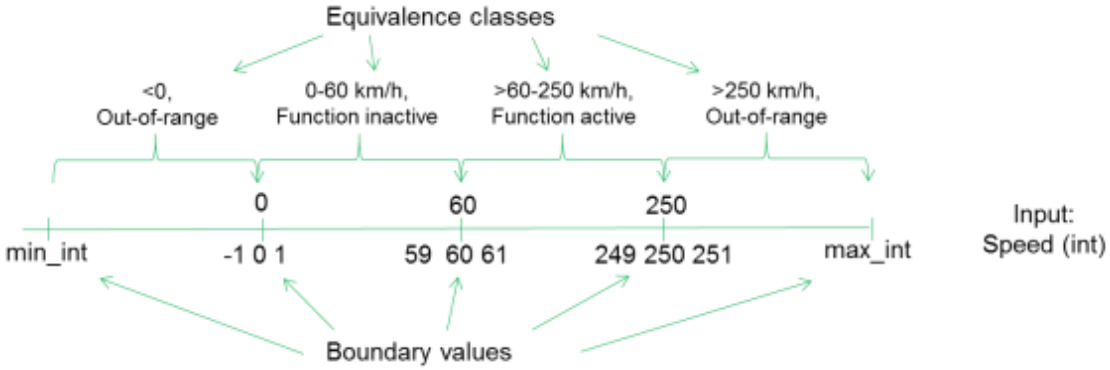
Järjestelmä ja moduulisuunnittelussa luodaan ylätason suunnitelma ohjelmiston toiminnallisuudesta. Suunnittelussa hyödynnetään modulaarista rakennetta, mikä yksinkertaistaa huomattavasti ohjelmiston rakennetta sekä helpottaa ohjelmiston toimivuuden testaamista ja vianetsintää. Turvatoimintojen erottaminen muista toiminnoista on suositeltavaa sekä yksinkertaisemman ja helpommin todennettavissa olevan rakenteen että turvallisuuden kannalta. Sovellusohjelmistojen, joissa käytetään rajoitetun käskykannan ohjelmointikieltä, suunnittelussa on hyödynnettävä turvatoimintojen data- ja ohjelmavuo puolimuodollisia menetelmiä, kuten tila- ja vuokaavioita. Saavuttaakseen yksinkertaisen rakenteen, ohjelmistossa käytettävien

toimilohkojen koodin kokoa on rajoitettava, ja kukin toimilohko voi sisältää vain yhden tulo- ja lähtökohdan. Ohjelmistossa tulisi hyödyntää kolmivaiheista rakennetta, joka koostuu tulo-, prosessointi- ja lähtökohdasta. Rajoittamatonta ohjelmointikieltä hyödyntäville sulautetuille ohjelmistoille ei aseta rakenteellisesti vastaavia vaatimuksia. Ohjelmistossa on kuitenkin hyödynnettävä toimintaan soveltuvia ohjelmointikieliä sekä käytännössä varmoiksi osoittautuneita tietokoneavusteisia työkaluja. Rajoittamatonta ohjelmointikieltä käytettäessä on huomioitava standardin ISO 13849-1 vaatimusten kattavan vain suoritustasot PLa-PLd, jolloin PLe voidaan saavuttaa noudattamalla IEC 61508-3 turvallisuuden eheyden tasolle SIL3 asettamia vaatimuksia. [34, 49]

Koodaukselle asetetut vaatimukset ovat vahvasti riippuvaisia käytettävästä ohjelmointikielestä. Ohjelmakoodille asetettavat vaatimukset riippuvat useasta tekijästä kuten ohjelmointikielestä, ohjelmoitavasta järjestelmästä ja turvavaatimusten kriittisyydestä. Rajoittamattoman sekä rajoitetun käskykannan ohjelmointikielille asetetaan standardissa ISO 13849-1 vain perusvaatimukset, kuten ohjelmoinnin toteuttamisen modulaarista ja rakenteellista koodausta noudattaen, ja käytettävien moduuleiden kokojen rajoittaminen. Ohjelmoinnissa onkin hyödynnettävä muita soveltuvia ohjelmointistandardeja sekä -sääntöjä kuten esimerkiksi standardia IEC 61508-7, jonka noudattamista vaaditaan PLe-tason ohjelmistoilta. Ohjelmointiohjeena voidaan hyödyntää esimerkiksi MISRA-C -säännöstöä, joka koostuu yli sadasta C-kielelle asetetusta pakollisesta, vaadittavasta sekä suositeltavasta vaatimuksesta. [48, 49]

Ohjelmiston testaus kuvastaa hyvin V-mallin iteratiivista rakennetta. Mallissa on yksinkertaistuksen vuoksi kuvattu ainoastaan moduuli- sekä moduulien integroinnin testaus, mutta ohjelmiston koodia on järkevää testata heti, kun se on mahdollista. Vastaavasti ohjelmiston suunnittelun aikaista testaamista kutsutaan mallissa todentamiseksi. Testaaminen jaetaan tyypillisesti niin kutsuttuihin black box- ja white box -testauksiin. Black box -testauksessa tutkitaan ohjelmiston toiminnallisuutta ja verrataan saatuja tuloksia suunnittelussa asetettuihin vaatimuksiin. Testauksessa tutkitaan ulostulo yksiköiden arvoja erilaisilla syötearvoilla, jolloin varsinaista prosessointiyksikköä, joka suorittaa toiminnon, kuvataan mustana laatikkona. Toisin sanoen, menetelmässä ei tarkastella varsinaista ohjelmointikoodia, vaan testataan erilaisten syötteiden aiheuttamia tuloja. Eräs black box -testausmenetelmä on jakaa testitapaukset ekvivalenssiluokkiin, jolloin ohjelmaan syötetään vääriä, eli raja-arvojen ulkopuolisia, ja oikeita syötteitä. Ekvivalenssiluokkajakomenetelmää voidaan laajentaa raja-arvo -analyysillä, jossa testataan ohjelmiston toimivuutta sen ääriarvoilla. Raja-arvo -analyysissa valitaan arvot raja-arvojen molemmilta puolilta, jolloin voidaan olettaa

toiminnallisuuden pysyvän rajojen sisällä samana.[49] Esimerkiksi kuvan 18 järjestelmässä toiminnallisuus testataan arvoilla -1, 0, 1, 59 ja 60, joiden palauttaessa toiminnon epäaktiivisuustilan, voidaan olettaa toiminnon olevan epäaktiivinen välillä 0-60.




***Kuva 18.*** *Black box -testaus [49]*

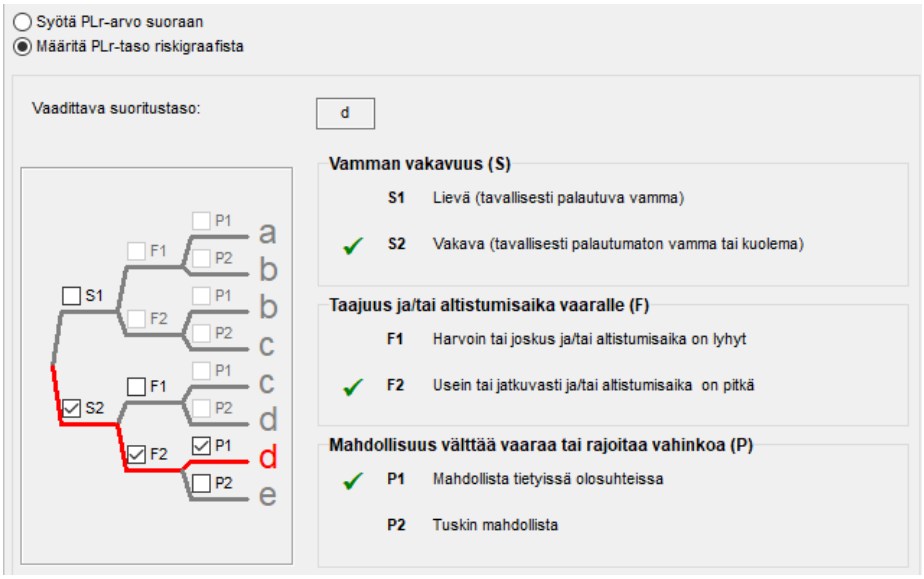
White box -testaus on edellistä huomattavasti kattavampi ja laajempi testausmenetelmä. Testissä tunnetaan ohjelman sisältämä koodi ja mahdolliset syötteet, minkä ansiosta voidaan testata ohjelman kaikki haarat ja ohjelmapolut. Grey box -testaus on edellisten välimuoto. Siinä testaajalla on tiedossa ohjelman rakenne, mutta varsinainen testaus suoritetaan black box -testauksen tavoin. Rajoittamattoman käskykannan ohjelmointikieltä käyttävän turvatoimintoa suorittavan ohjelmiston testauksessa hyödynnetään black box -testausta suoritustasoilla PLa-PLb, ja grey box -testausta suoritustasoilla PLc-PLd. Vastaavasti rajoitetun käskykannan ohjelmointikieltä käytettäessä testaus toteutetaan black box -testeillä. [34, 46, 49, 50]

V-mallin testauksessa hyödynnetään Bottom up -strategiaa. Menetelmässä testataan ensin alimman tason moduulit yksittäin, ja edetään taso kerrallaan ylöspäin. Lopulta moduulien yhteensopivuus varmennetaan, minkä jälkeen ohjelmisto on testattu.

## 5.3 SISTEMA

Monimutkaisten turvatoimintoja suorittavien ohjausjärjestelmien suunnittelu ja määrällinen arviointi on laskennallisesti raskasta, minkä vuoksi suunnittelun tueksi on luotu tietokoneavusteisia ohjelmistoja. Yksi suosituimmista ohjelmistoista on saksalaisen IFA:n (saks. Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung) luoma SISTEMA, jonka perustana käytetään standardin ISO 13849-1 vaatimuksia. Ohjelma on ilmaiseksi ladattavissa IFA:n sivuilta, ja siihen on ladattavissa komponenttitietoja useilta eri valmistajilta.

Ohjelma sisältää kuusi eri hierarkiatasoa: projekti, turvatoiminto, alajärjestelmä, kanava, lohko ja elementti. Projektilla viitataan ylimpään tarkastelun alla olevaan osaan, mikä tyypillisesti on kone tai vaaravyöhyke. Tiedoston sisälle voidaan määritellä projektin perustiedot, kuten projektin luojat, vaiheet ja muu dokumentaatio. Turvatoimintoihin määritellään vaadittava suoritustaso, jonka muodostamisessa voidaan hyödyntää standardin mukaista kuvan 19 riskigraafia. Lisäksi turvatoiminnoille voidaan määritellä dokumentaatio, joka sisältää muun muassa turvatoiminnon tyypin, turvatoiminnon laukaisevan tekijän sekä turvallisen tilan määritelmän. [51]

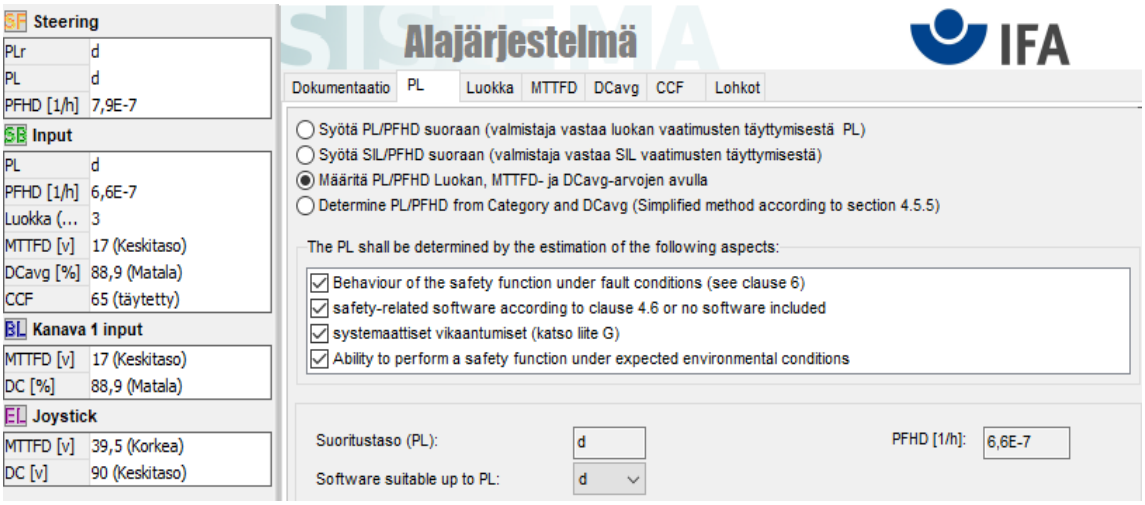



***Kuva 19.*** *SISTEMA-turvatoiminnon riskigraafi*

Turvatoiminto koostuu yhdestä tai useammasta alajärjestelmästä, jotka voidaan määritellä itse tai ladata valmistajan sivuilta valmiita alajärjestelmiä, jolloin valmistaja vastaa alemman hierarkian kohtien vaatimusten täyttymisestä. Manuaalisesti määriteltynä alajärjestelmät voivat olla rakenteeltaan yksi tai kaksikanavaisia, ja vikaantumisaikojen sekä keskimääräisten diagnostiikan kattavuuksien lukuarvot voidaan syöttää suoraan alajärjestelmään. Vaihtoehtoisesti lukuarvot voidaan laskea lohkoissa ja elementeissä määriteltävien tietojen perusteella. Alajärjestelmien järjestyksellä ei ole laskennan kannalta merkitystä, sillä SISTEMA:an merkittyjen alajärjestelmien katsotaan olevan sarjaan kytkettyjä. Lisäksi kaksikanavaisia ohjausjärjestelmiä koskeva yhteisvikaantumisen arviointi suoritetaan alajärjestelmän sisällä. [51]

Kanavat eivät sisällä turvatoiminnon suorittamiseen liittyvää toiminnallista tietoa, vaan niiden tehtävä on selkeyttää ohjausjärjestelmän rakennetta. Kanavat koostuvat lohkoista, joiden määrittelyssä on myös mahdollista hyödyntää valmistajan sivuilta ladattavia tietoja, tai vaihtoehtoisesti määrittää tiedot manuaalisesti valmistajan antamista tiedoista. Tyypillisiä lohkoja ovat ohjausjärjestelmän mekaaniset osat,

hydrauliventtiilit sekä yksinkertaiset ohjausyksiköt. Lohkot voidaan pilkkoa yhteen tai useampaan elementtiin, joiden vikaantumisajoista muodostetaan lohkon oma $MTTF_d$-arvo. Esimerkiksi sähkömekaaninen ohjausvipu on lohko, jonka sähköinen ja mekaaninen vikaantumisaika voidaan kuvata erillisillä elementeillä. [51]




***Kuva 20.*** *Turvatoiminnon suoritustason määrillinen ja laadullinen arviointi SISTEMA-ohjelmalla*

SISTEMA laskee jokaisen turvatoimintoon osallistuvan osan ja koko ohjausjärjestelmän arvot automaattisesti, mikä mahdollistaa valittujen komponentin sopivuuden nopean arvioinnin. Ohjelma huomioi määrällisten vaatimusten lisäksi turvatoiminnolta vaadittavat laadulliset toimenpiteet, kuten kuvassa 20 esitellään. SISTEMA:an ei ole sisäänrakennettu tarkkoja laadullisten näkökohtien arviointia, mutta käyttäjä voi määritellä ne itse, ja liittää tarpeelliset dokumentit alajärjestelmä-kansioon. [51]

# 6. STEER BY WIRE -JÄRJESTELMIÄ

Liikkuvissa työkoneissa vaadittavat ohjausvoimat ovat suuria, minkä vuoksi niissä käytetään hydraulisesti tehostettuja ohjausjärjestelmiä. Steer by wire -teknologia mahdollistaa sekä mekaanisen että hydraulisen yhteyden poistamisen ohjaamon ja pyörien väliltä, mikä yksinkertaistaa koneen rakennetta, mahdollistaa ergonomisemman ohjauksen sekä laskee ohjaamon melutasoa [52]. Hydraulinen ohjaus voidaan toteuttaa venttiiliohjauksella, jolloin toimilaitteille johdetaan ohjaukseen vaadittava tilavuusvirta venttiileiden avulla. Ohjaus voidaan toteuttaa myös pumppuohjauksella, jolloin ohjausliikkeeseen vaikutetaan säätämällä pumpun kierrostilavuutta ja pyörimisnopeutta. Seuraavissa osioissa käsitellään venttiiliohjattuja järjestelmää, jonka toimilaitteina on ristiinkytketyt differentiaalisylinterit.

Venttiiliohjatussa järjestelmässä koneen ohjausvaihteeseen kuuluvat ohjauselementti, ohjausyksikkö, venttiili sekä sylinterin asemaa mittaava sensori. Ohjausyksikkö toimii järjestelmän aivoina, ja sen tehtävänä on välittää kuljettajan käskyt venttiilille. Ohjausyksikön ohjelmoitavuus mahdollistaa erisuuruisen ohjauksen välityssuhteen eri nopeusalueille, minkä avulla voidaan lyhentää ohjaajalta vaadittavan ohjausliikkeen laajuutta, sekä parantaa ohjaustyön ergonomisuutta [53]. Järjestelmän vaatimuksista ja rakenteesta riippuen, se sisältää yhden tai useamman ohjausyksikön. Ohjauskäskyt voidaan välittää ohjausyksiköllе esimerkiksi ohjausvivulla tai ohjauspyörällä.

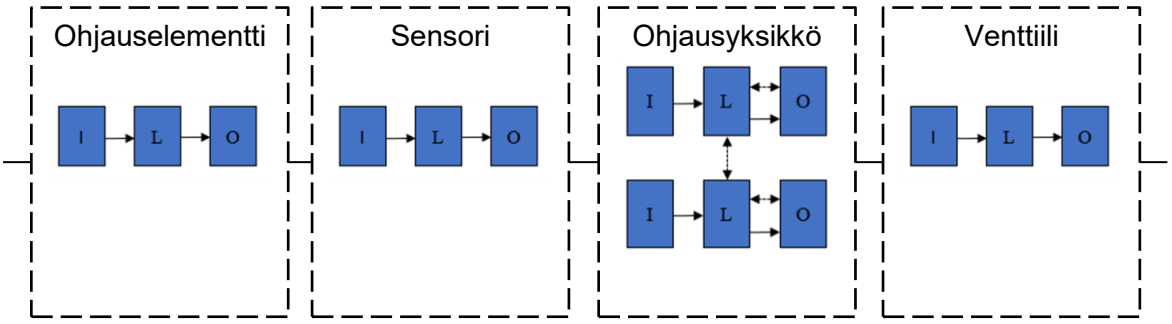
Koneen ohjausta koskevat vaatimukset esitetään Euroopan Unionin direktiiveissä ja asetuksissa, joiden tukena hyödynnetään eri standardoimisyhdistysten laatimia standardeja. Noudattamalla konetta koskevia yhdenmukaistettuja standardeja, voidaan osoittaa koneen täyttävän lainsäädännössä asetetut vaatimukset. Standardiin ISO 5010 kuuluvien Steer by wire-ohjausta hyödyntävien työkoneiden ohjauksen vaatimukset ovat riippuvaisia sekä vaadittavasta suoritustasosta että ajonopeudesta. Jokaisen SBW-ohjausta hyödyntävän työkoneen on täytettävä ohjausjärjestelmiä käsittelevän standardin kuten ISO 13949-1, IEC 62061 tai ISO 15998 vaatimukset. Hyödynnettäessä standardia ISO 13849-1, koneelta vaadittava suoritustaso voidaan määrittää kappaleessa 4.3 esitellyn kolmiasteisen menettelyn mukaisesti. Vastaavasti ajonopeuksia koskevat vaatimukset voidaan jakaa kolmeen eri luokkaan alle 10 km/h, 10-20 km/h ja yli 20 km/h.

Koneissa, joiden korkein ajonopeus on alle 20 km/h ja vaadittava suoritustaso on a-c, on mahdollista hyödyntää yksinkertaista yksikanavaista ohjausta. Yli 10 km/h nopeudella

operoivien koneiden on vikaantumistilanteessa kuitenkin saavutettava turvallinen tila, joka on luotavissa luokan 2 rakenteella. Yli 20 km/h nopeudella ajettavien koneiden on säilytettävä ohjattavuus yksittäisen vikaantumisen tapahtuessa, mikä käytännössä tarkoittaa redundanttisia ohjauskanavoita. Seuraavissa kappaleissa tarkastellaan yksi- ja useampikanavaisia SBW-järjestelmiä.

## 6.1 Yksikanavainen järjestelmä

Pyörillä liikkuvien koneiden standardin ISO 5010 vaatimukset voidaan täyttää yksikanavaisella ohjausjärjestelmällä, mikäli koneelta vaadittava suoritustaso on korkeintaan PLc, ja nopeus on alle 20 km/h. Vikaantumistilanteessa koneen ohjaus menetetään, ja ohjausjärjestelmän on siirryttävä turvalliseen tilaan, mikäli koneen maksiminopeus ylittää 10 km/h. Ohjausjärjestelmän yksikanavaisella rakenteella tarkoitetaan standardissa ISO 13849-1 määriteltyjä luokkia B, 1 ja 2. Luokan 2 rakenne sisältää testauslaitteiston, jota voidaan hyödyntää esimerkiksi turvallisen tilan luomisessa. Koneissa, joiden vaadittava suoritustaso on PLc ja maksiminopeus alle 10 km/h, voidaan hyödyntää luokan 1 rakennetta, jollainen esitellään kuvassa 21.




***Kuva 21.*** *Yksikanavainen ohjausjärjestelmä*

Ohjauskanavan komponentit voivat kuvan 21 mukaisesti koostua eri luokista, jotka yhdessä muodostavat ohjauskanavan luokan. Turvatoimintoa suorittavan yksikanavaisen ohjausjärjestelmän suoritustason arvioidaan komponenttien $PFH_d$- tai $MTTF_d$- arvojen avulla. Kanavan määrällisessä arvioinnissa ei tarvitse huomioida diagnostiikan kattavuutta eikä yhteisvikaantumista. Ohjauskanavan keskimääräinen vaarallinen vikaantumistaika voidaan laskea

$$\frac{1}{MTTF_d} = \frac{1}{MTTF_{d,ohjausel.}} + \frac{1}{MTTF_{d,\text{Sensori}}} + \frac{1}{MTTF_{d,\text{Ohjausyks.}}} + \frac{1}{MTTF_{d,venttiili}}, \quad (16)$$

jolloin kanavan $MTTF_d$-arvo on oltava vähintään 39 vuotta saavuttaakseen suoritustason PLc. Jokaiselle kanavan komponentille on määritettävä toiminta-aika, jonka puitteissa komponentti on vaihdettava saavutetun suoritustason säilyttämiseksi. Toiminta-aikaa

arvioidaan $T10_D$-arvona, johon mennessä 10 % komponenteista on vaarallisesti vikaantunut. Ohjausvivun kaltaisten sähkömekaanisten laitteiden vikaantumisajat lasketaan usein komponentin $B_{10D}$-arvon ja vuosittaisten käyttökertojen avulla:

$$MTTF_d = \frac{B_{10D}}{0{,}1 * n_{op}}, \tag{18}$$

ja toiminta-aika rajoitetaan 10 % lasketusta vikaantumisajasta.

Vikaantumisaikojen avulla voidaan arvioida ohjauskanavan määrällistä suoritustasoa, minkä lisäksi on huomioitava laadulliset vaatimukset, kuten toimenpiteet systemaattisen vikaantumisen estämiseksi, ohjelmiston vaatimukset sekä kanavan kyky suorittaa turvatoiminto odotettavissa ympäristöolosuhteissa. Ohjelmoitavan logiikan on myös oltava valmistajan puolesta turvallisuusluokiteltu. [34]

## 6.2 Redundanttinen järjestelmä

Yli 20 km/h maksiminopeudella ajavilta koneilta vaaditaan vikasietoisuustasoa 1, mikä tarkoittaa koneen ohjattavuuden säilymistä yksittäisen vikaantumisen seurauksena. Se on mahdollista saavuttaa ainoastaan redundanttisilla, eli rinnakkaisilla, ohjausjärjestelmillä. Standardissa ISO 13849-1 esitetyt redundanttiset luokat 3 ja 4 ovat rakenteeltaan identtiset, ja eroavat toisistaan vain diagnostiikan kattavuudessa, joka on luokalla 4 korkeampi. Ohjausjärjestelmän erittäin korkeaa diagnostiikkaa on haastavaa saavuttaa, minkä vuoksi tässä kappaleessa käsitellään luokan 3 rakennetta, jolla voidaan saavuttaa suoritustaso PLd.

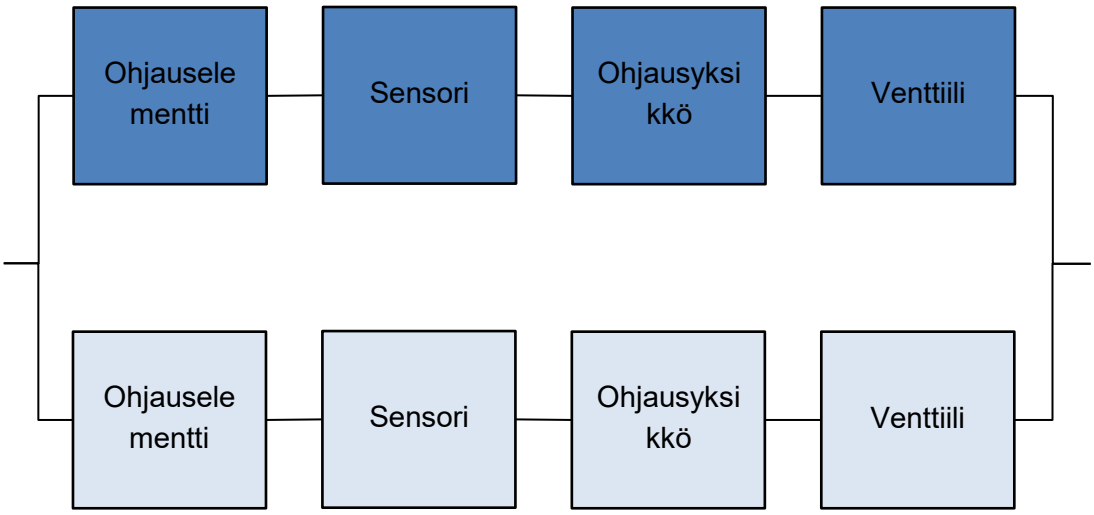
Luokan 3 ohjausjärjestelmä koostuu kuvan 22 mukaisesti kahdesta ohjauskanavasta. Ensisijaisena ohjauskanavana toimii tummansininen kanava, jonka vikaantuessa kuljettajan ohjauskäskyt välitetään pyörille toissijaisen ohjauskanavan kautta, jota esitetään kuvassa 22 vaaleansinisenä. Redundanttiset kanavat eivät välttämättä koostu fyysisesti täysin erillisistä osista, mutta niiden on sisällettävä redundanttisia ominaisuuksia, jotta vikaantumistaso 1 saavutetaan [34]. Fyysisesti erillisten osien käyttäminen kuitenkin lisää ohjausjärjestelmän erilaisuutta, mikä pienentää yhteisvikaantumisen riskiä.

Luokan 3 redundanttisilla ohjauskanavoilla voidaan saavuttaa suoritustaso PLd sekä matalalla 60-90 % tai keskitason 90-99 % diagnostiikan kattavuudella. Ohjausjärjestelmässä, jossa diagnostiikan kattavuus on matala, kanavien yhdistetyn vikaantumisajan on oltava vähintään 24 vuotta. Korkean diagnostiikan kattavuuden järjestelmissä alhaisin sallittu vikaantumisaika on lähes puolet lyhempi, 13 vuotta.

Riittävä diagnostiikan kattavuus voidaan saavuttaa esimerkiksi ristiin valvonnalla, sekä asemasensoreiden avulla epäsuoralla valvonnalla.

Kuvassa 22 esitetyn redundanttisen ohjausjärjestelmän kanavat koostuvat ohjauselementistä, sylinterin asemasensorista, ohjausyksiköstä sekä solenoidista, joka ohjaa venttiilin avautumista. Kanavat ovat keskenään identtiset, ja voivat sisältää samoja komponentteja.

Ohjauselementteinä voidaan hyödyntää ohjausvivun ja ohjauspyörän yhdistelmää, jolloin ohjausvivun on täytettävä kappaleessa 3.2.4 esitellyt lisäohjauselementin vaatimukset. Järjestelmässä voidaan hyödyntää myös yhtä ainoata ohjauselementtiä, jonka sisään on rakennettu vaadittava redundanttisuus esimerkiksi useamman rinnakkaisen sensorin avulla. Myös sylinterin asemasensori ja järjestelmän ohjausyksikkö voivat olla fyysisesti samat komponentit molemmissa kanavoissa. Vikasietoisuustason saavuttamiseksi on huomioitava redundanttisuus myös ohjauskanavan teholähteissä.




***Kuva 22.*** *Redundanttinen järjestelmä*

Eri valmistajien ohjausyksiköitä ja erilaisia ohjelmistoja käyttämällä madalletaan yhteisvikaantumisen riskejä, mutta samalla kasvatetaan järjestelmän kompleksisuutta. Täysin identtisillä ohjauskanavoilla on kuitenkin mahdollista saavuttaa vaadittavat 65 pistettä standardin ISO 13849-1 yhteisvikaantumisen arvioinnista.

Luokan 3 ohjausjärjestelmän suoritustason määrittämiseksi on selvitettävä yksittäisten kanavien keskimääräinen vikaantumisaika sekä diagnostiikan kattavuus, minkä jälkeen arvioidaan turvatoimintoa suorittavan ohjausjärjestelmän yhteisvikaantumisen todennäköisyys. Kanavan vikaantumisaika määritellään samoin kuin edellisen

kappaleen yksikanavaisen järjestelmän tapauksessa. Ohjausjärjestelmän suoritustasoa arvioitaessa voidaan vikaantumisaikana käyttää vain yhtä arvoa, minkä vuoksi kanavien vikaantumisaikojen poiketessa toisistaan, voidaan yhteinen vikaantumisaika symmentroida kappaleessa 5 esitellyn kaavan (12) mukaisesti.

Ohjausjärjestelmän keskimäärästä diagnostiikan kattavuutta arvioitaessa on huomioitava kaikkien kanavoiden jokaisen osan vikaantumisaika sekä diagnostiikan kattavuus kappaleessa 5 esitellyn kaavan (15) mukaisesti. Komponenteille kuten ohjausyksiköille ja sensoreille valmistaja usein ilmoittaa diagnostiikan kattavuuden, jota voidaan hyödyntää kokonaisen ohjausjärjestelmän keskimääräisen diagnostiikan arvioinnissa. ISO 13849-1 esiteltyä yksinkertaistettua diagnostiikan kattavuuden arviointia voidaan hyödyntää valmistajan ilmoittamien tietojen puuttuessa. Esimerkiksi sylinterin asemasensorin avulla voidaan epäsuorasti valvoa ohjausvipua sekä venttiiliä, jolloin molemmille osille saavutetaan 90-99 % diagnostiikan kattavuus.

Ohjausjärjestelmän rakenteen, keskimääräisen vaarallisen vikaantumisajan ja diagnostiikan kattavuuden määrittämisen lisäksi on arvioitava ohjauskanavoiden yhteisvikaantumisen riski. Taulukossa 4 on esitelty yhteisvikaantumista estävien toimenpiteiden pisteytysprosessi, josta on saavutettava vähintään 65 pistettä. Ohjausjärjestelmän on aiemmin määriteltyjen määrällisten vaatimusten lisäksi täytettävä laadullisten näkökohtien vaatimukset, joihin sisältyvät ohjelmistolle, systemaattiselle vikaantumiselle sekä toimintaympäristön asetetut vaatimukset.

# 7. YHTEENVETO

Tämän diplomityön tavoitteena oli kartoittaa lainsäädännön ja standardien steer by wire -ohjaukselle asettamia vaatimuksia. Suomen lainsäädäntö ei ohjauksen osalta aseta ajoneuvoille lisävaatimuksia, mutta edellyttää ajoneuvon tyyppihyväksyntää, mikä käytännössä tarkoittaa EU:n lainsäädännön mukaista suunnittelua. Lainsäädännön vaatimukset pohjautuvat konedirektiiviin, ja ovat täytettävissä yhdenmukaistettuja standardeja noudattamalla. Lainsäädännössä määriteltävät vaatimukset ja käytettävät standardit ovat konekohtaisia, minkä vuoksi työn ensimmäisessä osiossa tarkasteltiin erilaisia ohjausmenetelmiä.

Lainsäädännön tukena käytettävät standardit luokitellaan kolmelle tasolle: A-, B- ja C-tyyppiin. Tässä työssä tarkasteltujen off-road -työkoneiden SBW-ohjaukseen liittyvät oleellisimmat standardit ovat:

- A-tyypin standardi: SFS-EN ISO 12100. Tämä käsittelee turvallisuuden ja suunnittelun perusperiaatteita sekä koneiden riskien arviointia
- B-tyypin standardi: SFS-EN ISO 13849. Standardissa paneudutaan koneen ohjausjärjestelmien ominaisuuksiin ja vaatimuksiin, ja on verrattavissa sähköisiä ohjausjärjestelmiä käsittelevään standardiin EN 62061.
- C-tyypin standardi: ISO 5010. Standardissa esitellään pyörillä liikkuvien työkoneiden ohjaukselle asetettuja yleisiä vaatimuksia.

Standardien asettamat vaatimukset steer by wire -ohjaukselle ovat riippuvaisia koneelta vaadittavasta turvallisuudesta sekä koneen suurimmasta ajonopeudesta. Alan standardeissa turvallisuutta kuvataan suoritustasoilla, kuten tässä työssä, tai turvallisuuden eheyden tasoilla, jota käytetään erityisesti ohjausyksiköiden arvioinnissa. Koneelta vaadittava suoritustaso voidaan määrittää koneen käytöstä aiheutuvien riskien arvioinnin avulla.

Koneen ajonopeudelle on määritelty kolme eri tasoa: alle 10 km/h, 10-20 km/h, yli 20 km/h. Asetetut nopeusrajat eivät suoraan ole kytköksissä koneelta vaadittavaan suoritustasoon, minkä vuoksi SBW-ohjaukselle vaatimuksia ei voida yksiselitteisesti esittää, vaan jokaista konetyyppiä on tarkasteltava yksittäin.

Ohjausjärjestelmät voidaan karkeasti jakaa yksikanavaisiin ja redundanttisiin ohjausjärjestelmiin. Yksikanavainen ohjausjärjestelmän rakenne on mahdollinen suoritustasoon c asti. Vaadittaessa korkeampaa suoritustasoa, ohjausjärjestelmän

rakenteen on oltava vähintään kaksikanavainen. Yli 10 km/h nopeus vaatii järjestelmältä turvallista tilaa, mikä on mahdollista saavuttaa diagnostiikan avulla. Yksinkertaisimmillaan se voidaan toteuttaa luokan 2 mukaisella rakenteella, mutta korkean testaustaajuuden takia, se soveltuu huonosti jatkuvatoimisiin koneisiin. Yli 20 km/h nopeudella ajavien koneiden on säilytettävä ohjaus yksittäisen vikaantumisen seurauksena, mikä on saavutettavissa ainoastaan redundanttisilla ohjauskanavoilla.

# LÄHTEET


[1] J. Chang, M. Li, X. Bai, The Development of Engineering Vehicles Steer - by-Wire System, Atlantis Press, pp. 1763-1767.

[2] Fly-By-Wire (1980-1987), Airbus, Saatavissa: https://www.airbus.com/company/history/aircraft-history/1980-1987.html.

[3] Douglas F LeRoy, Steer-by-wire challenges hydraulics, Machine Design, Vol. 78, Iss. 15, 2006, pp. 52. Saatavissa: https://search.proquest.com/docview/217185426.

[4] ISO 5010, Earth-moving machinery - Rubber-tyred machines - Steering requirements, International Organization for Standardization, 2007, pp. 13.

[5] SFS-EN ISO 12100, Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen, in: 3, Suomen standardoimisliitto SFS, Helsinki, 2011, pp. 186.

[6] Komission delegoitu asetus (EU) 2015/208, 2014. Saatavilla: http://data.europa.eu/eli/reg_del/2015/208/oj.

[7] P. Pfeffer, H. Ulrich, Introduction and History, in: M. Harrer, P. Pfeffer (ed.), Steering Handbook, Springer International Publishing, Cham, 2017, pp. 1-25.

[8] R.N. Jazar, Steering Dynamics, in: R.N. Jazar (ed.), Vehicle Dynamics: Theory and Application, Springer New York, New York, NY, 2014, pp. 387-495.

[9] H. Sakai, T. Matsuo, S. Murayama, H. Hoshino, R. Nagashima, Geometry of a Four-Wheel-Steered Off-Road Vehicle, Journal of Forest Engineering, 1989, pp. 7-14. Saatavissa: https://journals.lib.unb.ca/index.php/IJFE/article/viewFile/10055/10311.

[10] M. Trzesniowski, Steering Kinematics, in: M. Harrer, P. Pfeffer (ed.), Steering Handbook, Springer International Publishing, Cham, 2017, pp. 63-90.

[11] J. Balkwill, Performance vehicle dynamics: engineering and applications, Elsevier Science, Saint Louis, 2017, pp. 197-239.

[12] Johansson Cris, T. Stockel Martin, Auto Suspension and Steering, A4, 3rd Edition, 3rd ed. Goodheart-Willcox, 2010, 167-194 p.

[13] B. Heißing, M. Ersoy, Chassis Components, in: B. Heißing, M. Ersoy (ed.), Chassis Handbook: Fundamentals, Driving Dynamics, Components, Mechatronics, Perspectives, Vieweg+Teubner, Wiesbaden, 2011, pp. 149-381.

[14] Types Of Power Steering, Saatavissa: http://www.aboutpowersteering.com/types.php.

[15] Meihua Tai, Pushkar Hingwe, M. Tomizuka, Modeling and control of steering system of heavy vehicles for automated highway systems, IEEE/ASME Transactions on Mechatronics, Vol. 9, Iss. 4, 2004, pp. 609-618. Saatavissa: https://ieeexplore.ieee.org/document/1372520.

[16] Recirculating Ball Typer Steering Gears, Ningbo Cie Industry And Trade Co., LTD, Saatavissa: http://www.ddb-tech.com/recirculating-ball-type-steering-gears-02.htm.

[17] M-serier Power Steering Service Manual, R.H. Sheppard Company Inc, Saatavissa: http://www.rhsheppard.com/wp-content/uploads/2014/08/mseriesmanual.pdf.

[18] Steering catalog, in: C-STOV-MC001-E2, Eaton Corporation, 2011, pp. 100.

[19] Steering, General, Steering Components, in: BC00000096en-US0401, Danfoss, 2017, pp. 60.

[20] TYPICAL STEERING WITH ORBITROL, Eaton, Saatavissa: http://www.eaton.com/EatonComJapan/e-index/Products/EFPL/SteeringControlUnit/TypicalSteeringwithOrbitrol/index.htm.

[21] HGF Series, Hydrostatic Steering Unit, in: Catalog HY13-1560-002/US, Parker Hannifin Corporation, Greeneville, 2003, pp. 20.

[22] HR46x Metsäharvesteri, Sampo Rosenlew Ltd, Saatavissa: http://www.samporosenlew.fi/upload/esitteet/samporosenlew_hr46x_2016_fi_web.pdf.

[23] N. Daher, M. Ivantysynova, Energy analysis of an original steering technology that saves fuel and boosts efficiency, Energy Conversion and Management, 2014, pp. 1059-1068.

[24] S. Haggag, A. Rosa, K. Huang, S. Cetinkunt, Fault tolerant real time control system for steer-by-wire electro-hydraulic systems, Mechatronics, Vol. 17, Iss. 2, 2007, pp. 129-142. Saatavissa: http://www.sciencedirect.com.libproxy.tut.fi/science/article/pii/S0957415806001036.

[25] G. Genta, L. Morello, Control of the Chassis and ‘by Wire’ Systems, in: G. Genta, L. Morello (ed.), The Automotive Chassis: Vol. 2: System Design, Springer Netherlands, Dordrecht, 2009, pp. 429-495.

[26] Rondeau Geoff, Steer-by-Wire Systems with Integrated Torque Feedback Improve Steering Performance and Reduce Cost, Industrial Utility Vehichle & Mobile Equipment, Vol. 21, Iss. 13, 2009, pp. 3.

[27] Balakrishnan Jyothis, Steer By Wire In Agricultural Tractors, International Journal of Scientific & Engineering Research, Vol. 4, Iss. 7, 2013, pp. 1303-1310.

[28] HY-STEER; Electro-hydraulic Steering Systems, in: E 10.116.9.0/04.15, HYDAC International GMBH, 2015, pp. 15.

[29] T. Siirilä, Koneturvallisuus 2, EU:n direktiivien ja standardien soveltaminen käytännössä, 2nd ed. Inspecta Koulutus Oy, 2008, 462 p.

[30] Euroopan parlamentin ja neuvoston direktiivi 2006/42/EY. Konedirektiivi, 2006.

[31] Avain standardien maailmaan, SFS-Käsikirja 1, Suomen Standardoimisliitto SFS ry, Helsinki, 2018, 48 p.

[32] T. Siirilä, Koneturvallisuus 1, EU-määräysten mukainen koneiden turvallisuus, 2nd ed. Inspecta Koulutus Oy, 2008, 431 p.

[33] Koneturvallisuuden standardit, Suomen standardoimisliitto SFS ry, 2015, Saatavissa: https://www.sfs.fi/files/63/Koneturvallisuusesite2015web.pdf.

[34] SFS-EN ISO 13849-1, Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet, in: 3, Suomen Standardisoimisliitto SFS, Helsinki, 2016, pp. 197.

[35] SFS-EN 12643, Earth moving machinery - Rubber-tyred machines - Steering requirements (ISO 5010:1992 modified), Suomen standardoimisliitto SFS, 2014, pp. 15.

[36] SFS-EN 1889-1. Machines for underground mines. Mobile machines working underground. Safety. Part 1: Rubber tyred vehicles. Suomen Standardisoimisliitto SFS ry, 2011, pp. 46.

[37] SFS-EN ISO 11850, Machinery for forestry, General safety requirements, Suomen Standardisoimisliitto SFS, Helsinki, 2012, pp. 32.

[38] SFS-EN 474-1:2007 + A5:2018, Earth moving machinery - Safety - Part 1: General requirements, Suomen Standardoimisliitto SFS, 2018, pp. 60.

[39] Ajoneuvolaki 2002/1090, 2002. Saatavissa: https://www.finlex.fi.

[40] Asetus ajoneuvojen käytöstä tiellä, 1992. Saatavissa: https://www.finlex.fi.

[41] Robottiauto Marilyn osaa ajaa jo yksin, Aamulehti, 2017.

[42] SFS-ISO 10968:2017, Suomen standardoimisliitto SFS, Helsinki, 2017, pp. 18.

[43] SFS-ISO/TR 14121-2, Koneturvallisuus. Riskin arviointi. Osa 2: Käytännön opastusta ja esimerkkejä menetelmistä, Suomen standardoimisliitto SFS, Helsinki, 2013, pp. 80.

[44] T. Siirilä, Koneturvallisuus 3, Ohjausjärjestelmät ja turvalaitteet, 2nd ed. Inspecta Koulutus Oy, 2009, 472 p.

[45] SFS-EN 62061 Koneturvallisuus. Turvallisuuteen liittyvien sähköisten, elektronisten ja ohjelmoitavien elektronisten ohjausjärjestelmien toiminnallinen turvallisuus, Suomen standardoimisliitto, Helsinki, 2005, pp. 199.

[46] S. Hauge, S. Håbrekke, M. Lundteigen, Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook, Sintef, Trondheim, 2003, 50 p.

[47] SFS-EN ISO 13849-2, Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. OSA 2: KELPUUTUS, in: 3, Suomen standardoimisliitto SFS, Helsinki, 2014, pp. 165.

[48] M. Gentile, A.E. Summers, Random, systematic, and common cause failure: how do you manage them? Process Safety Progress, Vol. 25, Iss. 4, 2006, pp. 331-338.

[49] Malm Timo, Vuori Matti, Rauhamäki Jari, Vepsäläinen Timo, Koskinen Johannes, Seppälä Jari, Virtanen Heikki, Hietikko Marita, Katara Mika, Safety-critival

software in machinery applications, VTT, Espoo, 2011, 63-111 p. Saatavissa: https://www.vtt.fi/inf/pdf/tiedotteet/2011/T2601.pdf.

[50] Söderberg Andreas, Hedberg Johan, Folkesson Peter, Jacobson Jan, Safety-related Machine Control Systems using standard EN ISO 13849-1, RISE Reserch Institutes of Sweden, Borås, 2018, 98 p. Saatavissa: www.diva-portal.org/smash/get/diva2:962662/FULLTEXT01.pdf.

[51] Tuomas Kautto, Ohjelmistotestaus ja siinä käytettävät työkalut, 1996, Saatavissa: http://www.mit.jyu.fi/opiskelu/seminaarit/ohjelmistotekniikka/testaus/#RTFToC29.

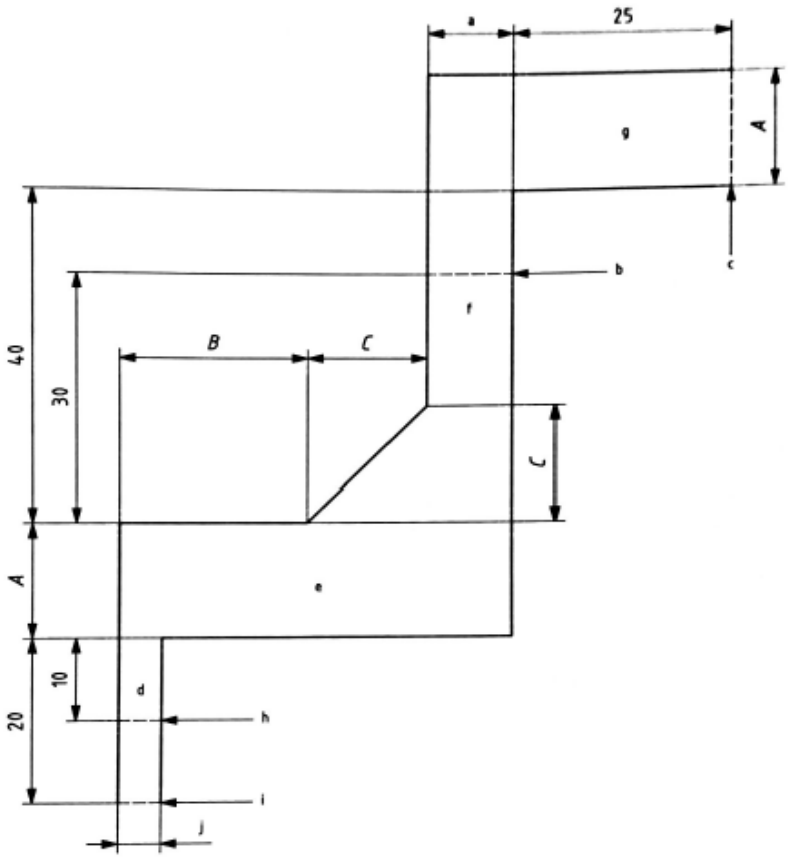
[52] Huelke Michael, Lungfiel Andy, Hauke Mikael, The SISTEMA Cookbook 5, 1st ed. Deutche Gesetzliche Unfallversicherung e. V. (DGUV), Berlin, 2014, 66 p.

[53] Steer by wire, Parker Hannifin, Saatavissa: http://solutions.parker.com/LP=8970.

[54] L. He, G.Y. Chen, H.Y. Zheng, Fault tolerant control method of dual steering actuator motors for steer-by-wire system, International Journal of Automotive Technology, Vol. 16, Iss. 6, 2015, pp. 977-987. Saatavissa: https://doi.org/10.1007/s12239-015-0100-8.

# LIITE A: STANDARDIN ISO 5010 OHJAUKSEN TESTIRADAT

Dimensions in metres




**Course dimensions**

$A$ = 1,1 times the tyre circle or 14 m, whichever is the larger

$B$ = 1,75 times the tyre circle or 22 m, whichever is the larger

$C$ = twice the maximum wheelbase or 15 m, whichever is the smaller

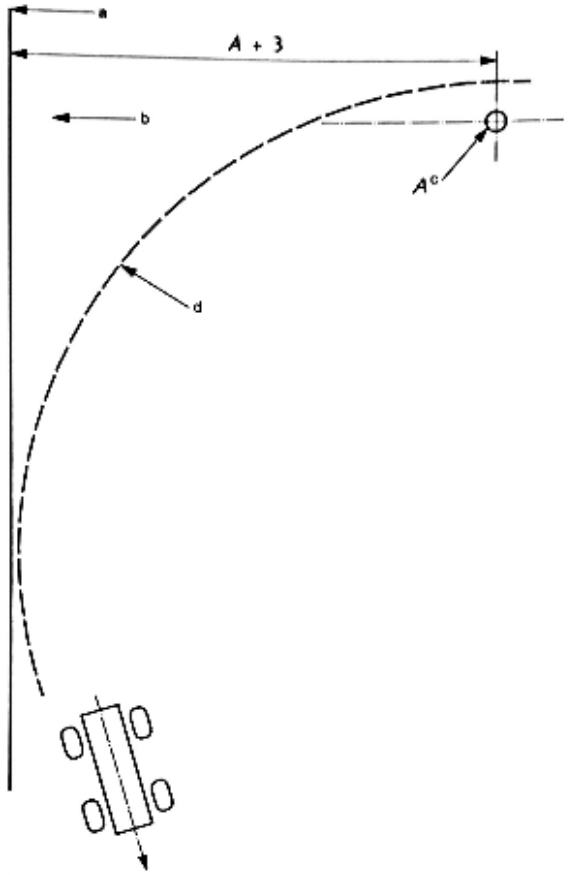
**Course length**

Machines with a tyre circle of less than 12 m, all wheeled dozers and all graders shall start the test at "Start 1" and terminate the test at "Finish 1". All other machines shall start the test at "Start 2" and terminate the test at "Finish 2".

a 2,5 times maximum width over tyres.
b Finish 1.
c Finish 2.
d Corridor 3.
e Corridor 4.
f Corridor 2.
g Corridor 1.
h Start 1.
i Start 2.
j 1,25 times maximum width over tyres.

**Figure 1 — Steering test course**

Dimensions in metres




**Key**

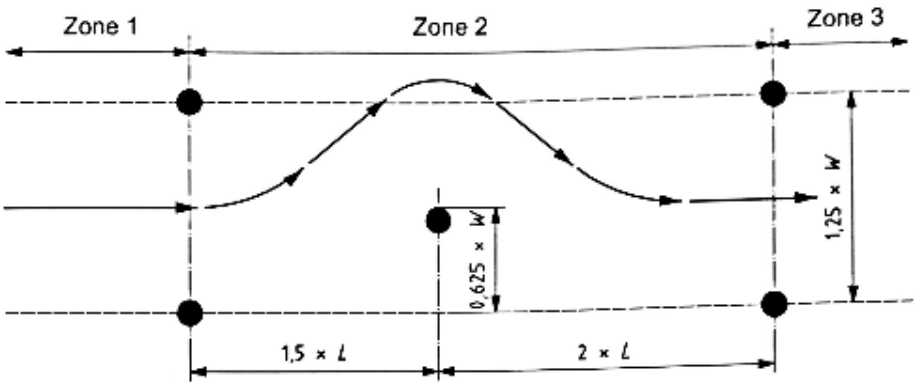
$A$ = 1,1 times the tyre circle or 14 m, whichever is the larger

a Perpendicular to original direction of travel.

b Original direction of travel.

c Point A: forward axle location at initiation of steering control movement (see 10.3.8).

d Outside line of tyres.




None of the cones shall be run over.

The machine shall be controllable as a comparable machine with a steering-wheel as operating element and shall provide the same level of safety and efficiency.

Zone 1: The maximum speed should be realized in zone 1. The machine shall enter zone 2 centered between the cones and parallel to the course. Speed may only be reduced after the front edge of the machine has reached the first group of cones.

Zone 2: In this zone, the operator is permitted to do anything that is required for keeping or reducing speed, except for using the brakes. The machine shall swerve around the single cone; additional manoeuvres are not permitted (e.g. a loop turn).

Zone 3: In this zone, the operator may use the brakes after the wheel centre of the front tyre has passed the cones. The machine shall be able to stay within the course until coming to a complete stop.

**Key**

*L* total length of machine (e. g. for wheeled loaders, length between counterweight and cutting edge of bucket, with bucket in transport position)

*W* total width of machine, measured across bucket

# LIITE B: DIAGNOSTIIKAN KATTAVUUDEN ARVIOINTI

Standardin ISO 13849-1 liitteessä E esitellyt yksinkertaistetun diagnostiikan arvioinnin toimenpiteet.

| Toimenpide | Diagnostiikan kattavuus (DC) |
|---|---|
| **Tuloyksikkö** | |
| Tulosignaalien dynaamisten muutosten aikaansaama jaksottainen testauksen käynnistys | 90 % |
| Mielekkyyden tarkistus (esim. käyttämällä sulkeutuvia ja avautuvia mekaanisesti yhdistettyjä koskettimia) | 99 % |
| Tulojen ristiinvalvonta ilman dynaamista testausta | [AC] 0...99 % riippuen kuinka usein sovelluksessa tapahtuu signaalin tilamuutos [AC] |
| Jos oikosulkuja ei voida paljastaa, tulosignaalien ristiinvalvonta yhdessä dynaamisen testauksen kanssa, (useille I/O-yksiköille) | 90 % |
| Tulosignaalien ja logiikan (L) väliarvojen ristiinvalvonta ja ohjelman suorituksen tilapäinen looginen ohjelmallinen valvonta sekä pysyvien vikojen ja oikosulkujen paljastaminen (useille I/O-yksiköille) | 99 % |
| Epäsuora valvonta (esim. valvonta painekytkimellä, toimilaitteiden aseman sähköinen valvonta) | 90...99 % riippuen sovelluksesta |
| Suora valvonta (esim. ohjausventtiilien asennon sähköinen valvonta, sähkömekaanisten laitteiden valvonta mekaanisesti yhdistetyillä kosketinelementeillä) | 99 % |
| Vikojen paljastuminen prosessin kautta | 0...99 % riippuen sovelluksesta: tämä toimenpide ei yksistään ole riittävä vaadittavalle suoritustasolle $PL_r$ e. |
| Anturien joidenkin ominaisuuksien valvonta (vasteaika, analogisten signaalien vaihtelualue, kuten sähköinen vastus, kapasitanssi) | 60 % |
| **Logiikka** | |
| Epäsuora valvonta (esim. valvonta painekytkimellä, toimilaitteiden aseman sähköinen valvonta) | 90...99 % riippuen sovelluksesta |
| Suora valvonta (esim. ohjausventtiilien asennon sähköinen valvonta, sähkömekaanisten laitteiden valvonta mekaanisesti yhdistetyillä kosketinelementeillä) | 99 % |
| Logiikan toiminnan yksinkertainen tilapäinen valvonta (esim. ajastinvahti, jolloin liipaisukohdat ovat logiikan ohjelmassa) | 60 % |
| Logiikan toiminnan tilapäinen ja looginen valvonta ajastinvahdilla, jolloin testauslaitteet tarkistavat logiikan käyttäytymisen mielekkyyttä | 90 % |
| Käynnistyksen itsetestaus piilevien vikojen paljastamiseen logiikan osissa (esim. ohjelma ja datamuistit, tulo- ja lähtöportit, rajapinnat) | 90 % (riippuen testaustekniikasta) |
| HUOM. 1 Muita arviointimenetelmiä diagnostiikan kattavuudelle: katso esimerkiksi standardin IEC 61508–2:2010 taulukot A.2...A.15. | |
| HUOM. 2 Jos logiikalle vaaditaan diagnostiikan kattavuutta "keskitaso (medium)" tai "korkea (high)", on muuttuvalle muistille, kiinteälle muistille ja prosessointiyksikölle kullekin sovellettava vähintäänkin yhtä toimenpidettä, jolla saadaan diagnostiikan kattavuus tasolle 60 %. Tässä taulukossa lueteltujen toimenpiteiden lisäksi voi olla myös muita käytettävissä olevia toimenpiteitä. | |
| HUOM. 3 Toimenpiteissä, jossa diagnostiikan kattavuuden vaihtelualue on annettu (esim. vikojen paljastuminen prosessin kautta) oikea DC-arvo voidaan määrittää ottamalla huomioon kaikki vaaralliset vikaantumiset ja päättämällä sen jälkeen, mitkä niistä havaitaan diagnostiikan kattavuuden toimenpiteillä. Epäselvissä tapauksissa vika- ja vaikutusanalyysin olisi oltava diagnostiikan kattavuuden arvioinnin lähtökohtana. | |

| | |
|---|---|
| Valvontalaitteiden reaktiokyvyn tarkistus (esim. ajastinvahti), joka toteutetaan pääkanavalla käynnistyksen yhteydessä tai kun tulee vaade turvatoiminnolle tai kun ulkoinen signaali vaatii turvatoimintoa tuloihin liitettävien laitteiden kautta | 90 % |
| Dynaaminen periaate (kaikkien logiikan komponenttien on vaihdettava tilaa "PÄÄLLE – POIS – PÄÄLLE" kun turvatoimintoa vaaditaan), esimerkiksi releillä toteutettu toimintaankytkennän ohjauspiiri | 99 % |
| Kiinteä muisti: yhden sanan pituinen varmenne (8 bittiä) | 90 % |
| Kiinteä muisti: kahden sanan pituinen varmenne (16 bittiä) | 99 % |
| Muuttuva muisti: RAM-testin suorittaminen käyttämällä redundanttista dataa, esimerkiksi lippuja, markkereita, vakioita, ajastimia ja näiden datojen ristikkäinen vertailu | 60 % |
| Muuttuva muisti: käytettävien datan muistipaikkojen luettavuus- ja kirjoittamiskyvyn tarkistus | 60 % |
| Muuttuva muisti: RAM-komponenttien valvonta muunnellulla Hamming-koodilla tai RAM-komponentin itsetestaus (esim."galpat" tai "Abraham") | 99 % |
| Prosessointiyksikkö: itsetestaus ohjelmallisesti | 60 % ... 90 % |
| Prosessointiyksikkö: koodattu prosessointi | 90 % ... 99 % |
| Vikojen paljastuminen prosessin kautta | 0...99 % riippuen sovelluksesta: tämä toimenpide ei yksistään ole riittävä vaadittavalle suoritustasolle $PL_r$ e. |
| **Lähtöyksikkö** | |
| Yhden kanavan lähtöjen valvonta ilman dynaamista testausta | 0...99 % riippuen siitä, kuinka usein sovelluksessa muutetaan signaalia |
| Lähtöjen ristiinvalvonta ilman dynaamista testausta | 0...99 % riippuen siitä, kuinka usein sovelluksessa muutetaan signaalia |
| Lähtöjen ristiinvalvonta dynaamisella testauksella ilman oikosulkujen paljastumista | 90 % |
| Lähtösignaalien ja logiikan (L) väliarvojen ristiinvalvonta sekä ohjelman suorituksen tilapäinen looginen ohjelmallinen valvonta sekä pysyvien vikojen ja oikosulkujen paljastaminen (useille I/O-yksiköille) | 99 % |
| Redundanttinen signaalin sulkupolku toimilaitteiden valvonnalla joko logiikan tai testauslaitteen avulla | 99 % |
| Epäsuora valvonta (esim. valvonta painekytkimellä, toimilaitteiden aseman sähköinen valvonta) | 90...99 % riippuen sovelluksesta |
| Vikojen paljastuminen prosessin kautta | 0...99 % riippuen sovelluksesta: tämä toimenpide ei yksistään ole riittävä vaadittavalle suoritustasolle $PL_r$ e. |
| Suora valvonta (esim. ohjausventtiilien asennon sähköinen valvonta, sähkömekaanisten laitteiden valvonta mekaanisesti yhdistetyillä kosketinelementeillä) | 99 % |

HUOM. 1 Muita arviointimenetelmiä diagnostiikan kattavuudelle: katso esimerkiksi standardin IEC 61508–2:2010 taulukot A.2...A.15.

HUOM. 2 Jos logiikalle vaaditaan diagnostiikan kattavuutta "keskitaso (medium)" tai "korkea (high)", on muuttuvalle muistille, kiinteälle muistille ja prosessointiyksikölle kullekin sovellettava vähintäänkin yhtä toimenpidettä, jolla saadaan diagnostiikan kattavuus tasolle 60 %. Tässä taulukossa lueteltujen toimenpiteiden lisäksi voi olla myös muita käytettävissä olevia toimenpiteitä.

HUOM. 3 Toimenpiteissä, jossa diagnostiikan kattavuuden vaihtelualue on annettu (esim. vikojen paljastuminen prosessin kautta) oikea DC-arvo voidaan määrittää ottamalla huomioon kaikki vaaralliset vikaantumiset ja päättämällä sen jälkeen, mitkä niistä havaitaan diagnostiikan kattavuuden toimenpiteillä. Epäselvissä tapauksissa vika- ja vaikutusanalyysin olisi oltava diagnostiikan kattavuuden arvioinnin lähtökohtana.