Olli Järvenpää

Toiminnallisen turvallisuuden edellytykset

Teatteritekniikan konesovellusten ohjausjärjestelmille

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Sähkötekniikka
Insinöörityö
1.5.2012

Tekijä Otsikko Sivumäärä Aika	Olli Järvenpää Toiminnallisen turvallisuuden edellytykset Teatteritekniikan konesovellusten ohjausjärjestelmille 38 sivua 1.5.2012
Tutkinto	insinööri (AMK)
Koulutusohjelma	sähkötekniikka
Suuntautumisvaihtoehto	sähkövoimatekniikka
Ohjaajat	yksikön päällikkö Tapio Lähteinen lehtori Jari Ijäs

Insinöörityössä selvitettiin konedirektiivin 2006/42/EY sekä valtioneuvoston asetuksen 400/2008 ja niihin harmonisoitujen standardien keskeisimmät vaatimukset koneille ja niiden ohjausjärjestelmille. Työn tilaajana oli Insta Automation Oy.

Lähtökohtana työlle oli teatteritekniset laitteet, joille laadittiin riskianalyysimalli standardin SFS-EN ISO 12100 mukaisesti. Riskianalyysi tehtiin tankonostinkoneelle.

Riskianalyysia laadittaessa oli otettava huomioon standardin SFS-EN ISO 13849-1 asettamat vaatimukset koneiden toiminnalliselle turvallisuudelle, erityisesti koneiden turvallisuuteen liittyvien ohjausjärjestelmien kyvylle suorittaa turvatoimintoja. Kykyä suorittaa turvatoiminto mitataan standardissa suoritustasoilla (PL).

Tankonostimen turvallisuuteen liittyvän ohjausjärjestelmän vaatimustenmukaisuutta tutkittiin SISTEMA-ohjelmistotyökalun avulla. Samalla selvitettiin SISTEMA:n käytettävyyttä Insta Automation Oy:n suunnitteluosastossa. SISTEMA:n avulla etsittiin vanhojen normien mukaisesti suunnitellun tankonostimen turvallisuuteen liittyvän ohjausjärjestelmän osat, joita tuli kehittää, jotta nykyvaatimukset toteutuisivat.

Työn tuloksena saatua tankonostimen riskianalyysia tullaan käyttämään Insta Automation Oy:n teatteriteknisissä projekteissa riskianalyysimallina. Insinöörityön aikana käytetty SISTEMA-ohjelmistotyökalu otetaan käyttöön Insta Automation Oy:n suunnitteluosaston apuvälineenä koneiden ohjausjärjestelmien suunnittelussa.

Avainsanat	turvallisuuteen liittyvä ohjausjärjestelmä, toiminnallinen turvallisuus, SISTEMA, turvatoiminnon suoritustaso

Author	Olli Järvenpää
Title	Requirements of Functional Safety for Control Systems of Stage Machinery
Number of Pages	38 pages
Date	1st May 2012
Degree	Bachelor of Engineering
Degree Programme	Electrical Engineering
Specialisation option	Electrical Power Engineering
Instructors	Tapio Lähteinen, Business Unit Manager Jari Ijäs, Senior Lecturer

This Bachelor's thesis investigates the requirements of the machine directive 2006/42/EC of the European Commission, and the decree 400/2008 of the Finnish Council of State, for machines and machine control systems. This Bachelor's thesis was made for Insta Automation.

The objective in this Bachelor's thesis was to make a risk analysis–example for stage machinery, according to the principles of the directive–harmonized standard EN ISO 12100. The risk analysis was carried out for a bar hoist –machine.

The requirements for safety related parts of the control system are described in harmonized standard EN ISO 13849-1, and had be taken into account in the risk analysis. According to the standard, all the safety functions, carried out by the safety related part of the control system, have to be determined a performance level (PL) to achieve a functional safety of a machine.

In this Bachelor's thesis, the performance levels of the safety related parts of the control system were measured with SISTEMA –software tool. The usability of SISTEMA in Insta Automation was clarified during the thesis. SISTEMA was used to point out the parts of the safety related control system that needed improvement due to current requirements.

The result of this thesis is a risk analysis, made for the bar hoist -machine and its control system. It will be used as an example of a risk analysis in the stage machinery projects of Insta Automation. SISTEMA –software tool will be used in Insta Automation design, as an assistance tool in the control system designing process.

Keywords	Safety related control system, functional safety, SISTEMA, performance level of safety function

Sisällys

Lyhenteet ja käsitteet

CCF *Common Cause Failure*; yhteisvikaantuminen. Jos samasta syystä aiheutuu useampia vikoja, on niitä tarkasteltava yksittäisenä vikana. Yhteisvikaantumisen arvioinnin menetelmä on esitelty standardin SFS-EN ISO 13849-1 liitteessä F.

DCavg *Diagnostic Coverage average*; diagnostiikan kattavuuden keskiarvo, toisin sanoen järjestelmän valvonnan kattavuuden keskiarvo prosentteina, mitä voidaan arvioida muun muassa vika- ja vaikutusanalyysin avulla. Standardissa SFS-EN ISO 13849-1 liitteessä E esitellään yksinkertaistettu menetelmä DCavg-arvon määrittämiseksi.

EY Euroopan yhteisö; nykyään osa Euroopan Unionia (EU).

FMEA *Failure Modes and Effects Analysis*; vika- ja vaikutus analyysi, ks. VVA.

MTTFd *Mean Time To dangerous Failure*; vaarallinen keskimääräinen vikaantumisaika vuosissa mitattuna; määritellään jokaiselle komponentille ja ohjausjärjestelmän kanavalle standardin SFS-EN ISO 13849-1 esittelemien menetelmien mukaisesti.

PL *Performance Level*; suoritustaso, jolla arvioidaan turvallisuuteen liittyvän ohjausjärjestelmän kykyä suorittaa turvatoiminto. Standardi SFS-EN ISO 13849-1 esittelee myös yksinkertaistetun menetelmän PL-tason määrittämiseksi.

PLr *required Performance Level*; riskianalyysissä määritelty PL-taso, jonka turvallisuuteen liittyvän ohjausjärjestelmän osan suorittama turvatoiminto vähintään tulisi yltää.

S/E/OE sähköinen/elektroninen/ohjelmoitava elektroninen järjestelmä.

SIL *Safety Integrity Level*; turvallisuuden eheyden taso TET on standardien IEC 61508 ja IEC 62061 määrittelemä taso, jota vastaa PL-taso. Standardissa SFS-EN ISO 13849-1 on esitelty vastaavuustaulukko näiden arvojen vertailua varten.

TET turvallisuuden eheyden taso; engl. SIL.

Vna valtioneuvoston asetus.

VVA vika- ja vaikutusanalyysi; riskin arvioinnin muoto, jota käytetään muun muassa toimintavarmuuden arvioinnissa; engl. FMEA.

1 Johdanto

Tässä insinöörityössä selvitetään nykyisten koneturvallisuusdirektiivin ja asetusten vaatimuksia koneen ohjausjärjestelmän osalta, ja mitä koneen valmistajan täytyy ottaa suunnittelussa huomioon. Työn lähtökohtana on teatteriprojektien sähkökäyttöiset näyttämötekniset koneet, joista tankonostimelle jalostettiin nykyvaatimusten mukainen riskianalyysimalli. Ideana oli, että tätä mallia voitaisiin hyödyntää myös muiden koneiden riskianalyysipohjana tai -mallina.

Riskianalyysimalli laadittiin Insta Automation Oy:n suunnitteluosaston kokonaistoimitushankkeiden tarpeisiin. Insta Automation Oy:n kokonaistoimitukset kattavat investoinnin koko elinkaaren; suunnittelun, valmistuksen, asennukset ja ylläpidon.

Suomen teatterit ovat monesti vielä näyttämätekniikaltaan vanhanaikaisia, ja monia teattereita odottaa saneeraus. Insta onkin yksi Suomen johtava teatteritekniikan asiantuntija, joka toimittaa laadukasta ja nykyaikaista sekä ennen kaikkea turvallista näyttämötekniikkaa.

Uuden riskianalyysin laatimisen lisäksi työn aikana selvitetään SISTEMA-ohjelmistotyökalun käyttöönottoa Insta Automation Oy:n suunnitteluosastossa. Käytännössä ohjelmistoon tutustutaan koestamalla vanhojen suunnitteluperiaatteiden mukaan toteutetun tankonostimen ohjausjärjestelmän suoritustasot nykyvaatimukset huomioon ottaen.

Työn tavoitteiden mukaisesti työssä perehdytään aluksi uuteen konedirektiiviin sekä koneturvallisuuden standardeihin. Näiden pohjalta esitellään uusi tankonostimen riskianalyysimalli.

2 Insta Automation Oy

Työn tilaajana on Insta Automation Oy. Insta Automation Oy on osa suurempaa Insta Group Oy:tä, johon kuuluu myös Insta DefSec Oy. Insta Group Oy on tamperelainen perheyrityskonserni, joka on toiminut sähkö- ja automaatioalojen monella eri osa-alueella vuodesta 1960 [1].

Insta Automation Oy on erikoistunut monelle sähkö- ja automaatioalojen eri osa-alueelle prosessiteollisuudesta vesihuoltoon ja aina teatteritekniikkaan asti. Insta DefSec Oy on erikoistunut puolustus-, turvallisuus- ja tietoturvateknologiaan.

Insta Automation Oy:ssä on oma suunnitteluosasto, keskusvalmistusosastonsa sekä asennuspalvelunsa, joista kaikki osallistuvat kokonaistoimitusprojekteihin. Insta Automation Oy:n teatteritekniikan kokonaistoimitusprojekteissa on koneiden ohjausjärjestelmien suunnittelu perustunut standardiin SFS-EN 954-1. Tämä standardi kumottiin uuden konedirektiivin myötä vuonna 2006 ja korvattiin standardilla SFS-EN ISO 13849-1. Kuitenkin SFS-EN 954-1 standardin vaatimustenmukaisuusolettamusta jatkettiin aina 31.12.2011 asti tarkoittaen, että sitä oli mahdollista siihen asti soveltaa. Nykyään standardin SFS-EN 954-1 mukaan ei voi suunnitella koneen ohjausjärjestelmää, joka täyttäisi kaikki nykyiset koneturvallisuusvaatimukset.

Tilaajan tarve uuden riskianalyysin laatimiseksi

SFS-EN 954-1 vaatimustenmukaisuusolettamuksen päättyminen tarkoitti konevalmistajien, kuten Instan kannalta sitä, että uuteen SFS-EN ISO 13849-1 koneturvallisuusstandardiin on perehdyttävä ja sen vaatimuksia noudatettava. Koneturvallisuusstandardi SFS-EN ISO 13849-1 asettaa lisävaatimuksia koneiden ohjausjärjestelmille, jotka on otettava huomioon jo riskianalyysia tehdessä. Tämän takia riskianalyysit on uusittava ja koneisiin on mahdollisesti tehtävä muutoksia.

Tämän insinöörityön tavoitteina oli perehtyä konedirektiiviin 2006/42/EY, standardeihin SFS-EN ISO 12100 ja SFS-EN ISO 13849-1 sekä laatia niiden pohjalta ohjeistus riskianalyysin luomisesta. Uuden koneturvallisuusdirektiivin ja uusien koneturvallisuusstandardien vaatimukset oli otettava huomioon.

Ohjeistus riskianalyysin laatimiseksi päädyttiin toteuttamaan valmiina riskianalyysimallina teatteritekniikan tankonostinkoneelle, jota voidaan käyttää hyväksi myös muissa koneissa, varsinkin teatteritekniikan sovelluksissa.

Vanha riskianalyysi, joita teatteritekniikan kokonaistoimituksissa tehtiin, oli kaksiosainen. Insta Automation Oy teki riskianalyysin ohjausjärjestelmän osalta, ja Instan yhteistyökumppani Ypäjän Metalli Oy suoritti mekaniikan osuuden riskianalyysistä. Ypäjän Metalli Oy suunnittelee ja mitoittaa, toimittaa ja asentaa näyttämömekaanisten koneiden mekaniikan, kuten vaihteistot, vaijerit, pyörästöt jne. Tämän työn tuloksena yhdistettiin molemmat riskianalyysit yhdeksi kokonaisuudeksi ja otettiin huomioon uudet määräykset ohjausjärjestelmän osalta. Koska riskianalyysi kattoi myös mekaniikan osuuden, tehtiin työn aikana yhteistyötä Ypäjän Metallin konesuunnittelijoiden kanssa.

Uusi riskianalyysi yhdisti koneen kahden eri osan mekaniikan ja ohjausjärjestelmän riskianalyysit yhdeksi yhtenäiseksi analyysiksi toteuttaen sen SFS-EN ISO 12100 mukaisesti ja otti myös huomioon SFS-EN ISO 13849-1 ohjausjärjestelmälle asettamat vaatimukset. Työssä käytettiin hyväksi teknisen raportin SFS-ISO/TR 14121-2 esimerkkejä riskianalyysin laatimiseksi.

3 Koneen riskianalyysille asetetut vaatimukset

3.1 EY-konedirektiivin vaatimukset koneille ja niiden ohjausjärjestelmille

Euroopan Parlamentin ja Neuvoston direktiivin 2006/42/EY myötä laadittiin Suomessa valtioneuvoston asetus, Vna 400/2008, joka antaa koneille ja niiden ohjausjärjestelmille tiettyjä vaatimuksia. Asetus tekee lakisääteiseksi muun muassa riskin arvioinnin jokaiselle koneelle. Riskin arvioinnissa asetuksen mukaan koneen toimittajan on tehtävä seuraavat asiat:

> - määritettävä koneen raja-arvot, joihin sisältyvät tarkoitettu käyttö sekä kohtuudella ennakoitavissa oleva väärinkäyttö;
>
> - tunnistettava koneen mahdollisesti aiheuttamat vaarat ja niihin liittyvät vaaratilanteet;
>
> - arvioitava riskin suuruus ottaen huomioon mahdollisen vamman tai terveyshaitan vakavuus ja todennäköisyys;
>
> - arvioitava riskin merkitys sen määrittämiseksi, onko riskiä tämän direktiivin tavoitteen mukaisesti pienennettävä; ja
>
> - poistettava vaarat tai pienennettävä näihin vaaroihin liittyviä riskejä soveltamalla suojaustoimenpiteitä. [2, Liite I.]

Asetus vaatii koneen toimittajan toimittamaan asiakkaalleen koneesta tekniset asiakirjat, joihin kuuluu myös riskin arviointia koskevat asiakirjat. Riskien arvioinnista on löydyttävä:

> i) luettelo olennaisista terveys- ja turvallisuusvaatimuksista, jotka koskevat konetta,
>
> ii) niiden suojaustoimenpiteiden kuvaus, jotka on toteutettu tunnistettujen vaarojen poistamiseksi tai riskien pienentämiseksi ja tarvittaessa maininta koneeseen liittyvistä jäännösriskeistä. [2, Liite VII:A.]

Asetus antaa ehdot myös ohjausjärjestelmälle seuraavasti;

> Ohjausjärjestelmät on suunniteltava ja rakennettava sellaisiksi, että ne estävät vaaratilanteiden syntymisen. Ennen kaikkea ne on suunniteltava ja rakennettava sellaisiksi, että:
>
> - ne kestävät tarkoitetut käyttörasitukset ja ulkoiset vaikutukset;

- ohjausjärjestelmän laitteisto- tai ohjelmistovika ei aiheuta vaaratilanteita;

- virheet ohjausjärjestelmän logiikassa eivät aiheuta vaaratilanteita; ja

- kohtuudella ennakoitavissa oleva inhimillinen erehdys käytön aikana ei aiheuta vaaratilanteita.

Erityistä huomiota on kiinnitettävä seuraaviin seikkoihin:

- kone ei saa käynnistyä odottamattomasti;

- koneen ominaisarvot eivät saa muuttua hallitsemattomasti, jos tällainen muutos saattaa aiheuttaa vaaratilanteita;

- koneen pysähtymistä ei saa estää, jos pysäytyskäsky on jo annettu;

- mikään koneen liikkuva osa tai koneen kiinni pitämä kappale ei saa pudota tai sinkoutua;

- minkään liikkuvan osan automaattinen tai käsikäyttöinen pysäyttäminen ei saa estyä;

- turvalaitteiden on pysyttävä täysin toimintakykyisinä tai annettava pysäytyskäsky; ja

- turvallisuuteen liittyviä ohjausjärjestelmän osia on käytettävä yhtenäisellä tavalla koneiden tai osittain valmiiden koneiden muodostamaan koko kokoonpanoon.

Langattomassa ohjauksessa on aikaansaatava automaattinen pysäytys, jos oikeita ohjaussignaaleja ei saada tai jos yhteys menetetään. [2, Liite I: 1.2.]

Toisin sanoen tämä asetus antaa selkeät lähtökohdat konekohtaisen riskianalyysin tekemiseen. Ohjausjärjestelmälle on annettu tarkat ja yksiselitteiset määräykset, jotka toteutetaan noudattamalla direktiivin kanssa harmonisoituja standardeja.

3.2 Standardointijärjestöt ja niiden tunnukset

Tässä työssä esiintyy eri standarditunnuksia kuten IEC ja SFS. Nämä ovat eri standardointijärjestöjen tunnuksia, joita on selvitetty taulukossa 1 (ks. seur. s.).

Taulukko 1. Eri standardisointijärjestöjä ja niiden tunnuksia sekä toimialoja

	Tekniikka	Tunnus
Maailma	ISO	ISO
	Sähkö ja elektroniikka	
Maailma	IEC	IEC
Eurooppa	CENELEC	EN
Suomi	SESKO	SFS

Kansainvälisiä standardeja laativat IEC- ja ISO-järjestöt. ISO (*International Organization for Standardization*) on tekniikan eri alojen rajat ylittävä järjestö, kun taas IEC (*International Electrotechnical Commission*) on sähkö ja elektroniikka- alan standardointijärjestö.

CENELEC (*European Committee for Electrotechnical Standardization*) on eurooppalainen sähkö- ja elektroniikka-alan järjestö, jonka standardeista n. 75 % perustuu IEC-standardeihin. SESKO on suomalainen sähkö- ja elektroniikka-alan standardointijärjestö, joka osallistuu tiiviisti Suomen edustajana IEC:n ja CENELEC:n standardointitoimintaan. [3.]

Suomessa SESKO:n kanssa yhteistyössä toimii myös MetSta ry eli Metalliteollisuuden Standardisointiyhdistys ry, joka pitää muun muassa yllä koneturvallisuusstandardien uudistumisten seurantapalvelua internetissä sekä julkaisee verkkoartikkeleita koneturvallisuuteen liittyen.

3.3 Koneturvallisuuteen liittyvät standardit ja niiden tyypitykset

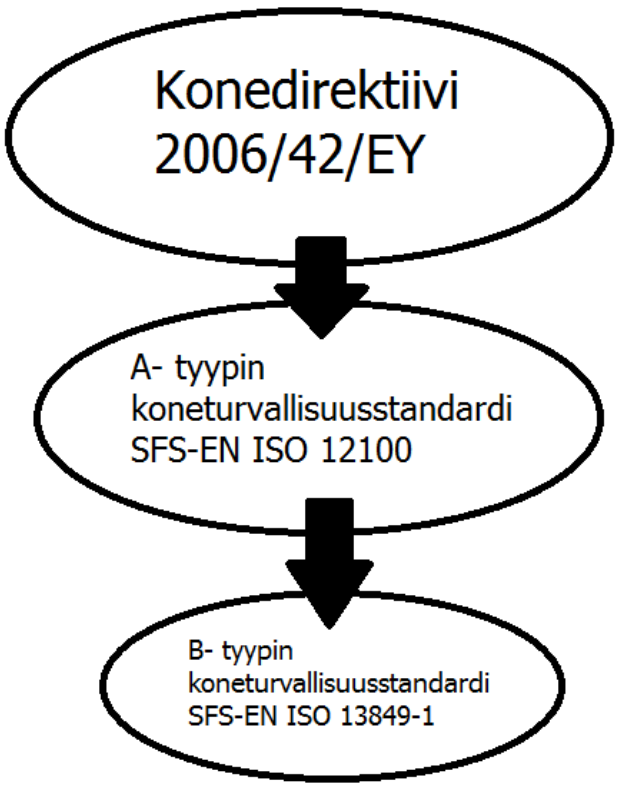
Koneturvallisuusstandardit jaetaan neljään eri tyyppiin: A-, B1-, B2- ja C -tyypin standardeihin. A-tyypin standardi on perusstandardi, jota sovelletaan kaikkiin koneisiin kuten SFS-EN ISO 12100 (Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen).

B-tyypin standardi on koneturvallisuuden ryhmästandardi, jossa käsitellään yhtä turvallisuusnäkökohtaa tai suojausteknistä laitetta, ja jota voidaan käyttää useassa koneessa.

B-tyyppi jaetaan vielä B1- ja B2-tyyppeihin, joista B1-standardit koskettavat yksittäisiä turvallisuusnäkökohtia ja B2-standardit koskettavat yksittäisiä turvalaitteita. Standardi SFS-EN ISO 13849-1 (Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet) on B1-tyypin standardi, jossa käsitellään koneturvallisuutta ohjausjärjestelmän näkökulmasta, ja joka määrittelee suuren osan tämän työn riskianalyysin vaatimuksista.

C-tyypin standardit ovat konekohtaisia tai koneryhmäkohtaisia standardeja. Tässä työssä ei käsitellä C-tyypin standardeja, sillä tankonostimille ei ole olemassa konekohtaista standardia.

Standardien tyyppijaottelun tarkoitus on se, että B- ja C-tyypin standardit on tehty A-tyypin standardien periaatteiden mukaisiksi, mutta ne tarkentavat ja yksityiskohtaistavat vaatimuksia ja riskin pienentämisen keinoja. Koneturvallisuusstandardit, joita tässä työssä esitellään, ovat harmonisoituja konedirektiivin kanssa ja niiden keskinäinen suhde esitellään kuvassa 1. [4.]



Kuva 1. Insinöörityössä sovellettujen koneturvallisuusstandardien suhde konedirektiiviin

Koneturvallisuusstandardin SFS-EN ISO 12100 keskeisimmät vaatimukset koneen riskianalyysille

Koneturvallisuusstandardi SFS-EN ISO 12100 on vuonna 2010 uudistettu standardi, johon on yhdistetty entiset SFS-EN ISO 12100-1- sekä SFS-EN ISO 12100-2 -koneturvallisuusstandardit, sekä SFS-EN ISO 14121-1: Riskin arvioinnin periaatteet. Tekninen raportti SFS-EN ISO/TR 14121-2 on edelleen voimassa, mutta jätetty uuden SFS-EN ISO 12100 -standardin ulkopuolelle. Tekninen raportti sisältää riskin arviointia koskevia esimerkkejä sekä käytännön opastusta.

Riskien arviointiin kuuluu riskianalyysi ja riskien merkityksen arviointi. Riskianalyysi sisältää seuraavat asiakokonaisuudet, jotka esitellään SFS-EN ISO 12100-standardissa:

- koneen raja-arvot
- vaarojen tunnistus
- riskin suuruuden arviointi.

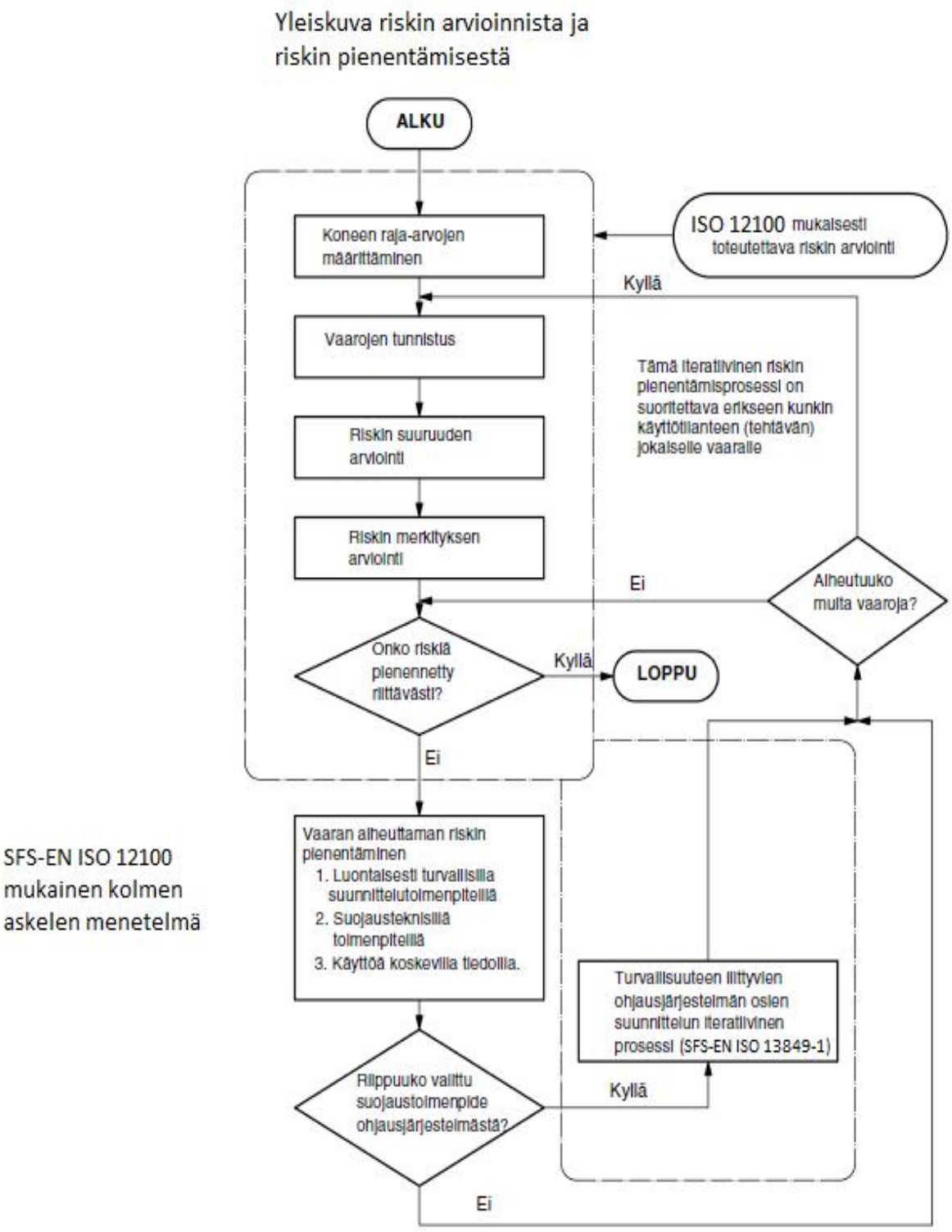
Riskianalyysin avulla voidaan arvioida riskien merkitystä, joista taas päätellään, tarvitseeko riski pienentämistä. Tässä työssä riskianalyysiin sisällytettiin myös riskin pienentämiseen käytetyt toimenpiteet ja riskin merkityksen arviointi.

Standardi SFS-EN ISO 12100 on harmonisoitu konedirektiiviin, eli se on yhtenäistetty konedirektiivin keskeisten vaatimusten kanssa. Jos kone on suunniteltu harmonisoidun standardin periaatteiden mukaan, täyttää se myös konedirektiivin keskeiset vaatimukset. SFS-EN ISO 12100 esittelee niin sanotun kolmen askeleen menetelmän riskin pienentämiseksi (ks. seur. s.)

Standardin SFS-EN ISO 12100 esittelemän menetelmän kolme askelta ovat

1. *askel:* luontaisesti turvalliset toimenpiteet
    - koneen suunnittelussa toteutetut turvallisuustoimenpiteet
    - esimerkiksi sähköisten osien kosketussuojaaminen, akselien kotelointi yms.
2. *askel:* suojaustekniset toimenpiteet ja täydentävät suojaustoimenpiteet
    - koneen turvallisuutta lisäävät toimenpiteet ja suojalaitteet
    - esimerkiksi ovirajat, valoverhot, sallintapainikkeet yms.
3. *askel:* käyttöä koskevat tiedot
    - koneen varoituskyltit, valo- ja äänivaroitukset yms.
    - käyttöohjeet.

Jos turvallisuutta ei saavuteta kolmen askeleen menetelmällä, tai jos suojalaitteista on aiheutunut uusia riskitekijöitä, on ne arvioitava alusta alkaen ja mietittävä koneen turvallisuustaso uudelleen. Yleiskuva riskin arvioinnin iteratiivisesta prosessista esitetään kuvassa 2 (ks. seur. s.).



Kuva 2. Yleiskuva riskin arvioinnista ja sen pienentämisestä SFS-EN ISO 12100 mukaisesti, lähdekuvaa muokattu [5, s. 32]

Lisäksi standardin SFS-EN ISO 12100 vaatimuksena on, että koneen kaikki riskit on pienennettävä siten, että koneen tarkoituksellinen käyttö ei häiriinny riskin pienentämisen menetelmistä. Tämä tarkoittaa käytännössä sitä, että koneen on voitava suoriutua siitä työstä, jota varten se on suunniteltu ilman, että suojalaitteet häiritsevät jollakin tavalla sen normaalia käyttöä.

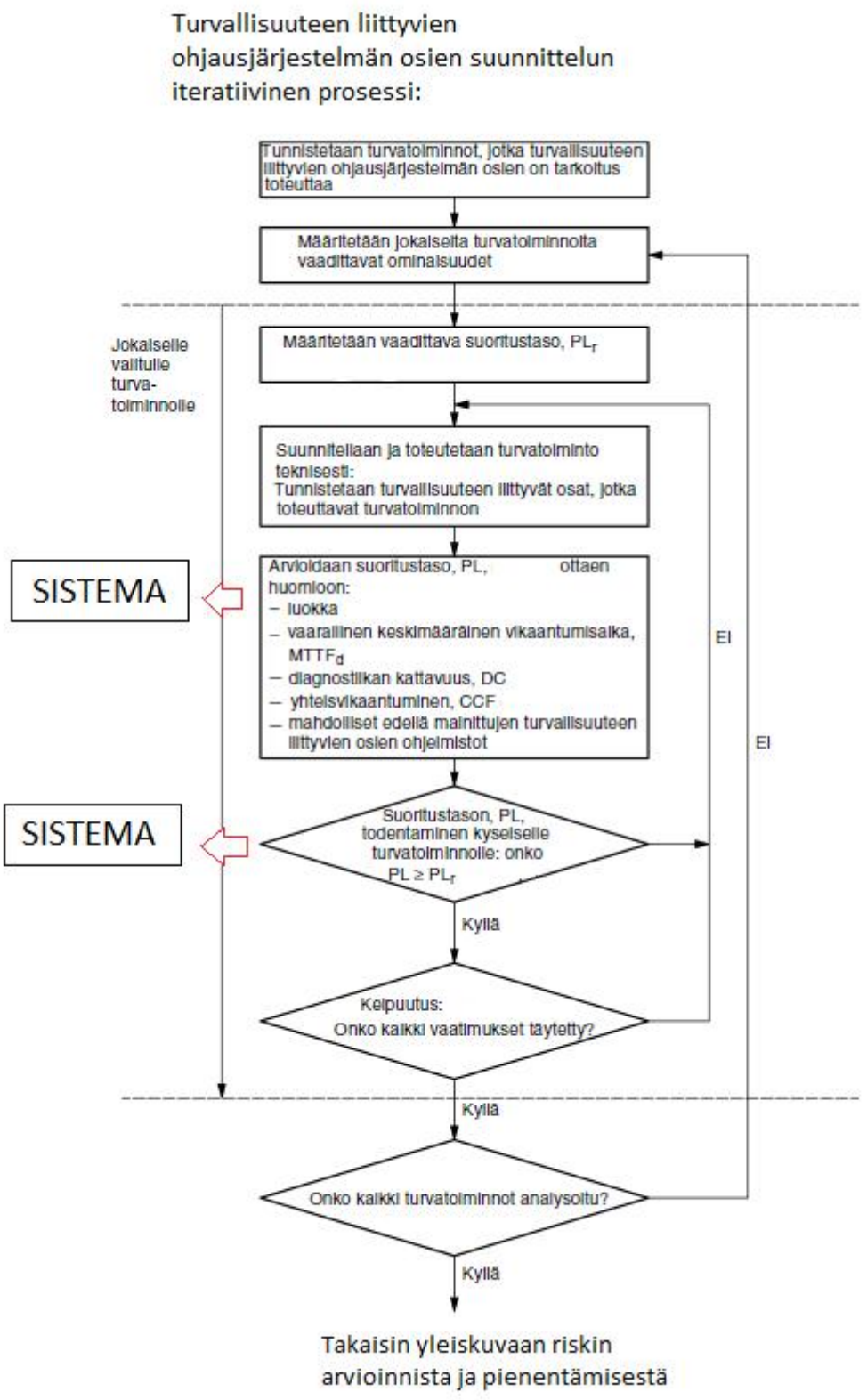
Standardin SFS-EN ISO 13849-1 koneen ohjausjärjestelmälle asettamat keskeiset vaatimukset

Standardi SFS-EN ISO 13849-1 määrittelee ohjausjärjestelmälle entistä tarkemmat vaatimukset kuin aikaisempi jo kumottu standardi SFS-EN ISO 954-1. Standardi SFS-EN ISO 13849-1 määrittelee suoritustasot, eli PL-tasot (*performance level*), turvallisuuteen liittyvien ohjausjärjestelmien kyvylle suorittaa turvatoiminto.

Jokaiselle turvatoiminnolle, joka suoritetaan turvallisuuteen liittyvän ohjausjärjestelmän osan tai niiden yhdistelmän avulla, määritellään riskianalyysin perusteella vaadittava PLr-taso (*required Perfofmance Level*). Koneen valmistaja tai markkinoille saattajan on varmistuttava, että koneen turvatoiminnot täyttävät koneen riskianalyysissa määritellyt PLr-tasot. Toisin sanoen koneen valmistaja todentaa jokaisen turvatoiminnon toteuttaman PL-tason. PL-tason täytyy vähintään olla sama kuin vaadittu PLr-taso. PL-tasot ovat a:sta e:hen, missä e on kaikista suurimman riskin pienentämiseen vaadittu suoritustaso.

Aiemmin esitetyssä yleiskuvassa riskin arvioinnin iteratiivisesta prosessista (kuva 2) kysytään turvatoiminnon riippuvuutta ohjausjärjestelmästä. Jos turvatoiminto toteutetaan turvallisuuteen liittyvää ohjausjärjestelmää hyväksikäyttäen, sen suunnitteluun on esitetty standardissa SFS-EN ISO 13849-1 oma iteratiivinen prosessikaavio. Tämä kaavio palaa takaisin yleiskuvaan riskin arvioinnin iteratiivisesta prosessista, kun kaikki turvatoiminnot on analysoitu.

Turvallisuuteen liittyvien ohjausjärjestelmien osien suunnittelun iteratiivinen prosessi esitetään kuvassa 3 (ks. seur. s.), johon on tämän työn hahmottamisen kannalta lisätty lisähuomautus kohtiin, joissa työn aikana on käytetty SISTEMA-ohjelmistotyökalua.



Kuva 3. Turvallisuuteen liittyvien ohjausjärjestelmän osien suunnittelussa käytettävä iteratiivinen prosessi ja SISTEMA-ohjelmistotyökalun hyödyntäminen, lähdekuvaa muokattu [5, s. 38]

Turvallisuuteen liittyvien ohjausjärjestelmien osien suoritustasojen arvioimiseksi on valmistajan määriteltävä koneen turvatoiminnolle seuraavia näkökohtia:

- vaarallinen keskimääräinen vikaantumisaika, MTTFd (*Mean Time To dangerous Failure*), joka arvioidaan jokaiselle yksittäiselle komponentille sekä kanavalle
- diagnostiikan kattavuus, DCavg (*Diagnostic Coverage average*)
- yhteisvikaantuminen, CCF (*Common Cause Failure*)
- arkkitehtuuri nimettyjen rakenteiden mukaan, eli luokka
- turvatoiminnon käyttäytyminen vikatilanteessa (tai -tilanteissa)
- turvallisuuteen liittyvä ohjelmisto (tässä työssä ei käsitellä ohjelmointia)
- systemaattinen vikaantuminen (esim. ohjelmistojen kopioinnista aiheutuvat)
- kyky toteuttaa turvatoiminto ennakoitavissa olevissa ympäristöolosuhteissa (ympäristöolosuhteet käsitellään koneen riskianalyysin kohdassa *koneen raja-arvot*).

Standardi SFS-EN ISO 13849-1 esittää PL-tasojen arviointiin yksinkertaistetun menetelmän, joka perustuu nimettyihin rakenteisiin eli luokkiin (*categories*). Nämä nimetyt rakenteet (B, 1, 2, 3, 4) täyttävät määrätyt suunnittelukriteerit ja käyttäytymisen vikatilanteissa, ja ne ovat ensi kerran esitelty vanhassa standardissa SFS-EN 954-1.

PL-tason määrittämiseksi on nimettyjen rakenteiden lisäksi huomioitava turvatoiminnon MTTFd-arvo, DCavg-arvo sekä CCF-arvo. Nämä arvot määritellään turvatoiminto- tai komponenttikohtaisesti, ja ne ovat yleensä laitevalmistajien teknisissä tiedostoissa, tai ne voidaan arvioida itse, esimerkiksi SISTEMA-ohjelmaa apuna käyttäen.

Järjestelmän rakenteella on ratkaiseva merkitys siihen, mihin PL-tasoon päästään. Luokkien mukainen arkkitehtuuri on yleensä kuvattu lohkokaavioesityksenä (ks. kuva 4, s. 15).

Nimettyjen rakenteiden määritelmät ovat

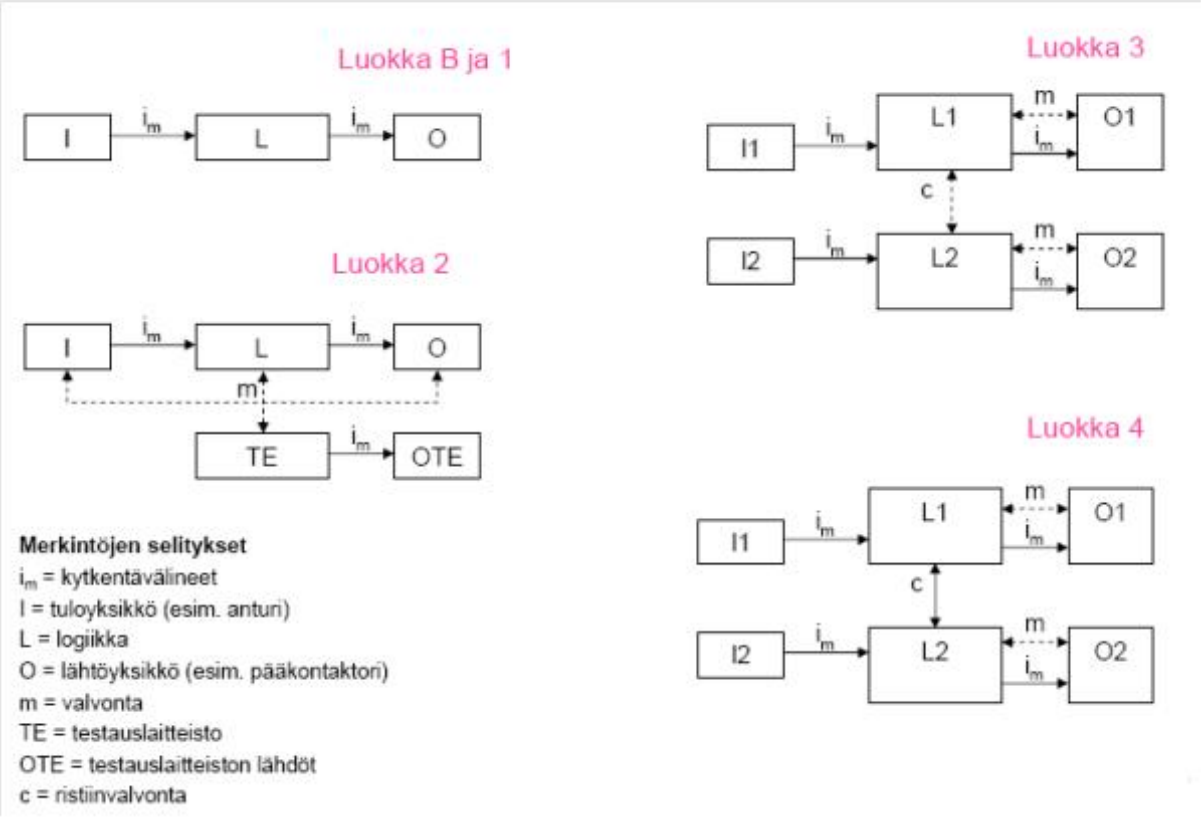
- *luokka B:* yleisiä tuvallisuusperiaatteita (suojamaadoitus, eristyksen valvonta, jännitepiikkien vaimennus yms.) on noudatettava. Käyttö- ja ympäristöolosuhteet on otettava huomioon käytettävissä komponenteissa. Vaarallisten vikaantumisten välinen keskimääräinen aika, MTTFd-arvo, on oltava 3−30 vuotta.

- *luokka 1:* on noudatettava luokan B vaatimuksia sekä hyvin koeteltuja komponentteja ja hyvin koeteltuja turvallisuusperiaatteita (ylimitoittaminen, pakkotoimisuus yms.). MTTFd on oltava 30−100 vuotta. [6, s. 143.]

- *luokka 2:* on noudatettava luokkien B ja 1 vaatimuksia, sekä koneen ohjausjärjestelmän on koetettava turvatoimintojen toimivuus tietyin väliajoin. MTTFd on oltava 3−100 vuotta vaaditun PL-tason mukaan.

- *luokka 3:* on noudatettava luokkien B ja 1 vaatimuksia. Yksittäinen vian sattuessa ohjausjärjestelmän on pystyttävä suorittamaan turvatoiminto, ja mahdollisuuksien mukaan yksittäinen vika on havaittava, useammat viat on aina havaittava. MTTFd on oltava 30−100 vuotta vaaditusta PL-tasosta riippuen. DCavg-arvo, eli diagnostiikan kattavuus on oltava vähintään 60−99 %, yhteisvikaantumisen (CCF) todennäköisyys oltava pieni (CCF-arvon määrittäminen; SFS-EN 13849-1; Liite F).

- *luokka 4:* on noudatettava luokkien B ja 1 vaatimuksia. Turvatoimintoa ei saa menettää vaikka järjestelmässä olisi yksi vika. Kaikkien vikojen on paljastuttava, eli vikoja ei saa kertyä järjestelmään, ilman että käyttäjä niistä tietää. Jos vikoja kuitenkin kertyy, ne eivät saa aiheuttaa turvatoiminnon menettämistä. Käytännössä tarkoittaa järjestelmän kahdennusta, sekä itse- että ristivalvontaa. MTTFd on oltava 30−100 vuotta, DCavg on oltava 99−100 % ja yhteisvikaantumisen (CCF) todennäköisyys on oltava pieni. [6, s. 144.]



Kuva 4. Standardin SFS-EN 13849-1 määrittelemien nimettyjen rakenteiden eli luokkien lohkokaavioesitykset [7, s. 21]

Käytännössä luokan 3 ja 4 välinen ero jää valvonnan, eli diagnostiikan kattavuuden suuruuteen. Luokka 4 vaatii järjestelmältä käytännössä täydellistä vikojen automaattista valvontaa.

Luokat B, 1 ja 2 ovat yksikanavaisia ja luokat 3 ja 4 kahdennettuja eli redundanttisia. Luokissa 3 ja 4 on kaksi erillistä toisistaan riippumatonta toimivaa kanavaa, jotka pystyvät suorittamaan turvatoiminnon. Toisin sanoen luokat 3 ja 4 ovat kaikista kalleimmat toteuttaa, mutta niillä päästään korkeimpaan suoritustasoon.

Luokkien lisäksi turvallisuuteen liittyvän ohjausjärjestelmän osan saavuttamaan PL-tasoon vaikuttavat muutkin arvot, joita standardi SFS-EN ISO13849-1 määrittelee:

- MTTFd eli vaarallinen keskimääräinen vikaantumisaika. Sen määrittämiseksi voidaan käyttää valmistajan antamia arvoja, SFS-EN 13849-1 liitteiden C ja D antamia karkeita likiarvoja tai valita 10 vuotta. Kymmenen vuoden MTTFd-arvo ei kata vaativia turvallisuusehtoja.

MTTFd-arvo jaotellaan vaarallisten vikaantumisten vaihteluvälin mukaan matalaan, keskimääräiseen ja korkeaan tasoon taulukon 2 mukaisesti.

Taulukko 2. Keskimääräisen vaarallisen vikaantumisajan jaottelu eri tasoihin

MTTFd	Vaihteluväli
matala (*low*)	3−10 vuotta
keskimääräinen (*medium*)	10−30 vuotta
korkea (*high*)	30−100 vuotta

Eri suoritustasoilla on eri vaatimukset MTTFd-arvon suuruudelle. Esimerkiksi PL e -taso vaatii aina korkean MTTFd-arvon.

- DCavg eli diagnostiikan kattavuus tarkoittaa turvatoiminnon kykyä havaita vikoja. Standardin SFS-EN 13849-1 Liitteessä E annetaan karkeita arvioita DCavg-arvolle eri komponenteilla, eri tilanteissa sekä laskentakaava, joka perustuu paljastettujen vaarallisien vikaantumisten sekä kaikkien vaarallisten vikaantumisten suhteena [6, s.159]. SISTEMA-työkalu on tässä tilanteessa erittäin hyödyllinen apuväline, sillä siinä on standardin mukainen taulukko/työkalu diagnostiikan kattavuuden arviointiin.

  DCavg-arvo jaotellaan taulukon 3 mukaisesti. Vaadittu arvo riippuu pääosin vaaditusta PL-tasosta (PLr) ja määritellystä luokasta.

Taulukko 3. Diagnostiikan kattavuuden eri tasot ja prosentuaaliset arvot

DC avg	Vaihtelualue
nolla (none)	< 60 %
matala (low)	60−90 %
keskimääräinen (medium)	90−99 %
korkea (high)	99−100 %

- CCF eli yhteisvikaantuminen. Yhteisvikaantuminen tarkoittaa kahta tai useampaa erillistä vikaa, joiden syy (aiheuttaja) on sama. CCF-arvon määrittelyä varten SFS-EN 13849-1 Liite F esittelee pisteytystaulukon, jossa kysytään järjestelmän suunnittelussa käytettyjä keinoja yhteisvikaantumisten estämiseksi.

Käytetyistä menetelmistä saa pisteitä, joiden maksimi on 100. Luokissa 2, 3 ja 4, jotka vaativat pientä todennäköisyyttä yhteisvikaantumisen tapahtumiseen, on saatava vähintään 65 pistettä. [8.]

Taulukko 4. CCF-arvon määrittämiseksi tarvittavat osatekijät [8]

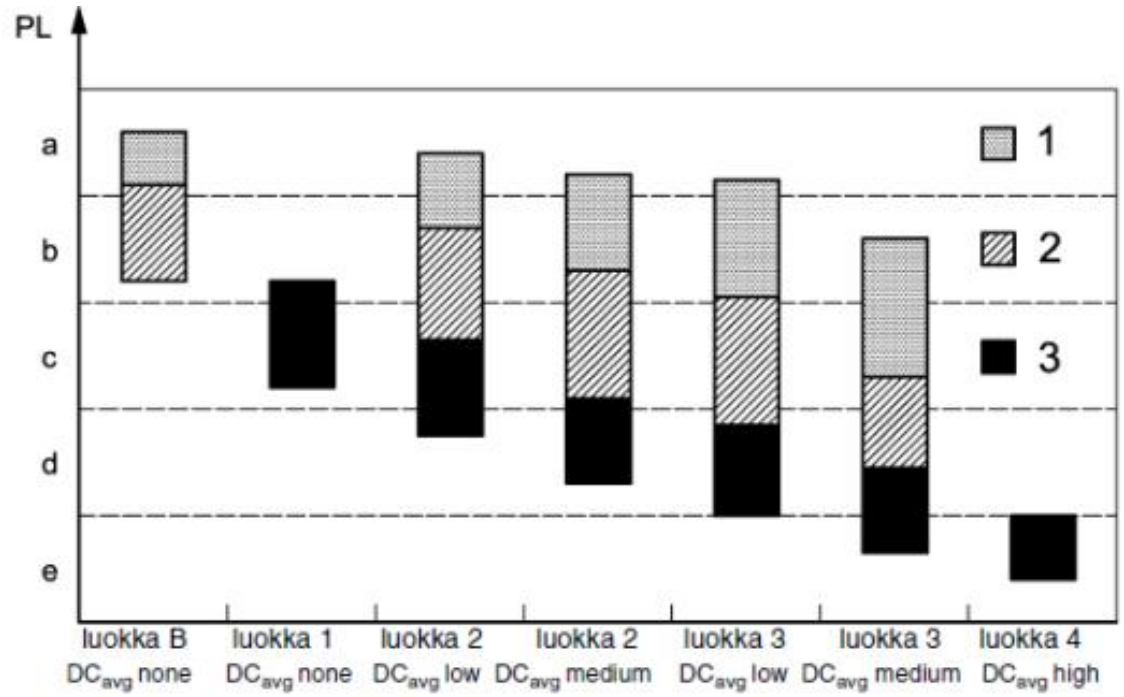
Kriteerit	Pisteet
–Erottelu	15 p.
–Diversiteetti	20 p.
–Suunnittelu	15 p.
–Koetellut komponentit	5 p.
–FMEA	5 p.
–Ammattitaito	5 p.
–Ympäristöolosuhteet (EMC)	25 p.
–Muut	10 p.

CCF-arvoa varten standardissa SFS-EN 13849-1 on tarkemmin selvitetty kriteerit. Matti Sundquistin yksinkertaistamassa taulukossa (taulukko 4), on esitetty keskeiset vaatimukset yhteisvikaantumisen arvioimiseksi. Lyhenne FMEA tarkoittaa vika- ja vaikutusanalyysia (suomeksi lyhenne on VVA), joka on eräs tapa arvioida riskejä, sekä vikaantumisen todennäköisyyttä.

Edellä esitetyt osatekijät on nidottava yhteen vaaditun suoritustason mukaan. Esimerkiksi, jos riskianalyysissa todetaan jonkin riskin pienentämiseen tarkoitetun turvatoiminnon vaadittavaksi suoritustasoksi PLr e, on tämän turvatoiminnon suorittavien turvallisuuteen liittyvien ohjausjärjestelmän osien täytettävä tietyt vaatimukset (kuva 5, ks. seur. s.).

Suoritustason e vaatiman rakenteen on oltava luokkaa 3 tai 4 eli kahdennettu ja valvottu. Valvonnan kattavuuden (DCavg) on oltava turvatoiminnon muodostavasta järjestelmän osan luokasta riippuen keskimääräinen tai korkea. Sen lisäksi molempien turvatoiminnon suorittavien kanavien (kahdennus, luokan 3 ja 4 vaatimus) vaarallinen keskimääräinen vikaantumisaika on oltava pitkä (30−100 vuotta), eli MTTFd-arvon on oltava korkea.

Näiden vaateiden täytyttyä on tarkasteltava CCF-arvo turvatoiminnolle, standardin SFS-EN 13849-1 taulukon F.1 mukaan, pisteiden on oltava vähintään 65. Lisäksi ohjelmointiin liittyvät vaatimukset, sekä ennakoitavat ympäristöolosuhteet on otettava tässä vaiheessa huomioon. Kaikkien vaatimusten täytyttyä voidaan sanoa, että turvatoiminnon suoritustaso on PL e ja vastaa näin ollen vaadittua tasoa PLr e.



Merkintöjen selitykset:

PL	suoritustaso
1	kunkin kanavan $MTTF_d$ = matala (low)
2	kunkin kanavan $MTTF_d$ = keskimääräinen (medium)
3	kunkin kanavan $MTTF_d$ = korkea (high)

Kuva 5. Luokkien, MTTFd- ja DCavg-arvojen, sekä niiden yhteisvaikutuksesta saatavan PL-tason riippuvuus [5, s. 52]

Standardien SFS-EN ISO 13849-1, IEC 61508 ja IEC 62061 välinen suhde

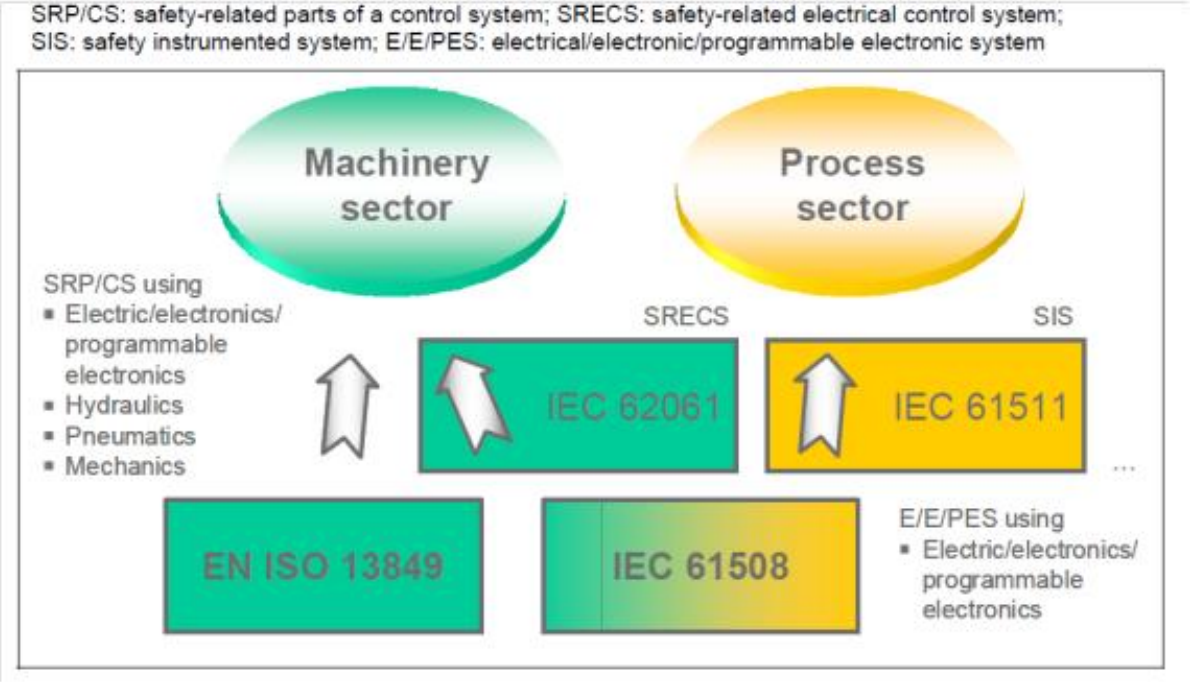
IEC 61508 (B-tyypin standardi) on yleisesti käytetty sähköisten/ elektronisten/ ohjelmoitavien elektronisten (S/E/OE) turvallisuusjärjestelmien standardisarja (7 osaa) ja siihen liittyy koneturvallisuusstandardi IEC 62061. Standardisarja IEC 61508 esittelee koneen turvallisuuteen liittyvän elinkaarimalli -ajattelun sekä toiminnallisen turvallisuuden käsitteen, johon myös standardi SFS-EN ISO 13849-1 tähtää.

Toiminnallinen turvallisuus tarkoittaa kokonaisturvallisuutta, joka saavutetaan turvallisuuteen liittyvien järjestelmien sekä ulkoisten riskin vähennyskeinojen suunnitellulla toiminnalla. Toisin sanoen toiminnallinen turvallisuus saavutetaan turvatoimintojen toimiessa oikein sekä muiden riskin vähennyskeinojen, kuten varoituskilpien, turvallisuuskoulutusten, ohjeiden yms. onnistuessa. [9.]

Toiminnallisen turvallisuuden täyttymisen arvioimiseksi täytyy järjestelmille määrittää turvallisuuden eheyden taso TET (englanniksi SIL). TET-tasoja on neljä. Mitä korkeampi TET-taso on, sitä suuremmalla todennäköisyydellä turvatoiminto toimii oikein. Koneturvallisuuden puolella käytetään yleensä TET 1–3 -tasoja. TET 4 -taso on laadittu sellaisen riskin pienentämiseksi, minkä seuraukset voivat olla katastrofaaliset. Esimerkiksi ydinteollisuudessa sekä rautatieliikenteessä käytetään kaikkia neljää tasoa. Yksittäisen koneen ei yleensä katsota voivan aiheuttaa katastrofaalisen suurta vaaraa.

IEC 61508 on yleisesti käytetty standardisarja muun muassa prosessiteollisuudessa. Siitä johdettua koneturvallisuusstandardia IEC 62061 on hyödyllistä käyttää sellaisissa olosuhteissa, joissa käytetään IEC 61508:n mukaisia turvallisuusperiaatteita. Esimerkiksi prosessiteolliseen ympäristöön suunnitellun yksittäisen koneen yhteydessä voi olla hyödyllistä käyttää IEC 62061 -standardia.

Saksalaisessa työturvallisuuteen liittyvässä raportissa (*BGIA report 2/2008*) esitellään yksinkertainen kaavio standardien SFS-EN ISO 13849-1 ja IEC 61508 (sekä siitä johdettujen kone ja prosessiteollisuuden standardien IEC 62061 ja IEC 61511) sovellusaloista (kuva 6, ks. seur. s.).



Kuva 6. Standardien EN 13849-1 ja IEC 61508 soveltamisalat [10]

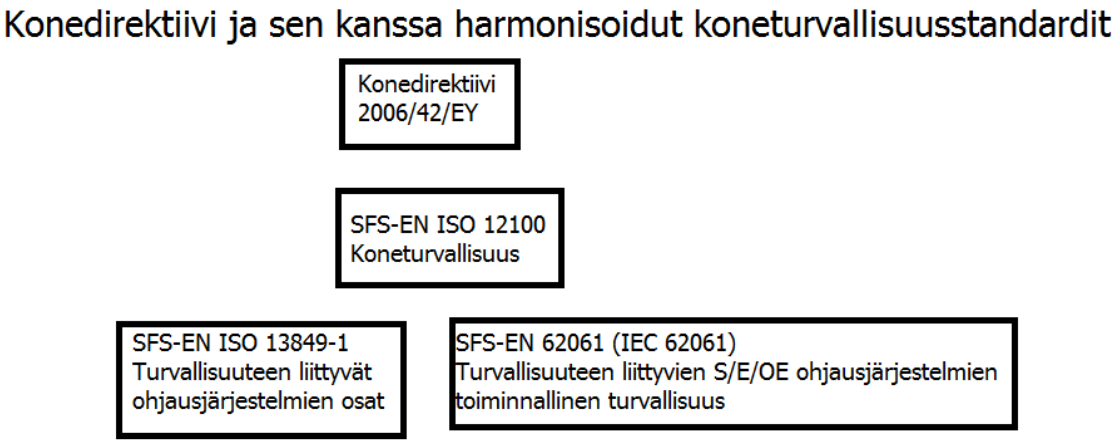
Yleensä soveltamisalasta riippuu, käyttääkö SFS-EN ISO 13849-1 vai IEC 62061 -standardia. Standardi SFS-EN 13849-1 esittelee vastaavuustaulukon (taulukko 5) toiminnallisen turvallisuuden eri mittareiden eli PL- ja TET-tasojen (SIL) välillä.

Taulukko 5. PL-tasojen (SFS-EN 13849-1) ja SIL-tasojen (IEC 61508-1) välinen vastaavuus [5, s.44]

PL	SIL (IEC 61508-1, tiedoksi) tiheiden vaateiden tai jatkuvan toiminnan tapa
a	Ei vastaavuutta
b	1
c	1
d	2
e	3

Standardin esittämä vastaavuustaulukko ei ole täysin aukoton, mutta tärkeimpien turvallisuusvaatimusten osalta vertailu on mahdollinen. Standardi IEC 61508 ei ole harmonisoitu standardi konedirektiivin 2006/42/EY kanssa, mutta siihen perustuva koneturvallisuuteen keskittyvä IEC 62061 (SFS-EN 62061) on harmonisoitu direktiivin kanssa (ks. kuva 7).

Toisin sanoen konevalmistajat saavat soveltamisalasta riippuen päättää kumpaa harmonisoitua standardia, SFS-EN ISO 13849-1 vai SFS-EN 62061 (IEC 62061), käyttävät. Myös koneen tilaaja saattaa asettaa vaatimuksia sen suhteen, kumman standardin mukaista turvallisuusluokitusta käytetään.



Kuva 7. EY-konedirektiivin kanssa yhdenmukaiset koneturvallisuusstandardit

IEC 62061 -standardin käyttö vaatii standardin hyvää osaamista, myös IEC 61508 on tunnettava. Nämä standardit keskittyvät sähköisten/ elektronisten/ ohjelmoitavien elektronisten järjestelmien turvallisuuteen, kun taas SFS-EN ISO 13849-1 on sovellettavissa myös muille tekniikanaloille, kuten hydraulisiin, pneumaattisiin ja mekaanisiin järjestelmiin.

Standardi SFS-EN ISO 13849-1 esittelee suositustaulukon (taulukko 6, ks. seur. s.) eri tekniikoiden soveltamisaloista näillä kahdelle eri standardilla. Kyseisessä taulukossa näytetään, mitä teknologian käyttöä on käsitelty, ja mille turvallisuuden tasolle kullakin tekniikalla päästään.

Taulukko 6. Standardien SFS-EN ISO 13849-1 ja IEC 62061 soveltamissuositukset [5,s.12]

	Turvallisuuteen liittyvien ohjaustoimintojen toteutuksessa käytettävä teknologia	ISO 13849-1	IEC 62061
A	Muut kuin sähköiset, esim. hydrauliset	X	Ei käsitellä
B	Sähkömekaaniset, esim. releet ja/tai yksinkertainen elektroniikka	Rajoitettu nimettyihin rakenteisiin [a] ja enintään suoritustasolle PL e	Kaikki rakenteet ja enintään turvallisuuden eheyden tasolle SIL 3
C	Monimutkainen elektroniikka, esim. ohjelmoitavat järjestelmät	Rajoitettu nimettyihin rakenteisiin [a] ja enintään suoritustasolle PL d	Kaikki rakenteet ja enintään turvallisuuden eheyden tasolle SIL 3
D	A yhdessä B:n kanssa	Rajoitettu nimettyihin rakenteisiin [a] ja enintään suoritustasolle PL e	X [c]
E	C yhdessä B:n kanssa	Rajoitettu nimettyihin rakenteisiin (ks. huomautus 1) ja enintään suoritustasolle PL d	Kaikki rakenteet ja enintään turvallisuuden eheyden tasolle SIL 3
F	C yhdessä A:n kanssa tai C yhdessä A:n ja B:n kanssa	X [b]	X [c]
X tarkoittaa, että kyseistä kohtaa käsitellään sarakkeen otsikossa mainitussa kansainvälisessä standardissa			
[a] Nimetyt rakenteet määritellään kohdassa 6.2, jotta voidaan esittää yksinkertaistettu lähestymistapa suoritustason määrälliseen arviointiin. [b] Monimutkainen elektroniikka: käytetään nimettyjä rakenteita standardin ISO 13849 tämän osan mukaisesti suosituskyvyn tasolle PL d asti tai mitä tahansa rakennetta standardin IEC 62061 mukaisesti. [c] Muissa kuin sähköisissä teknologioissa käytetään alajärjestelminä standardin ISO 13849 tämän osan mukaisia osia.			

Tämä työ käsittelee sähköistä toteutusta, joten molemmat standardit ovat käyttökelpoisia. Instan teatteriprojekteissa on joissain tapauksissa käytetty myös IEC 61508 ja IEC 62061 mukaisia periaatteita, mutta tämä työ, kuten on jo mainittukin, on tehty SFS-EN ISO 13849-1 esittelemien vaatimuksien mukaisesti.

3.4 SISTEMA-ohjelmistotyökalu

SISTEMA-ohjelmalla voidaan todentaa ohjausjärjestelmän suoritustaso, joiden laskemiseen ohjelma käyttää Markovin dynaamisia malleja. SISTEMA on ilmaisohjelma, joka on kehitetty Saksan työterveyden ja työturvallisuuden laitoksen toimesta (suom. Sundcon Oy). SISTEMA on kehitetty helpottamaan riskien arviointiprosessia sekä koneen turvallisuuden eheyden suunnittelua, ja näin ollen ohjaamaan konevalmistajia standardien käyttöön konesovelluksissa.

SISTEMA on ohjelmistotyökalu, joka pohjautuu täysin standardiin SFS EN ISO13849-1. Täytyy muistaa, että PL- ja SIL-tasoja voidaan vertailla keskenään, mutta turvallisuuslaskennat on tehtävä aina vaaditun standardin asettamien ehtojen mukaisesti. Jos esimerkiksi tilaaja vaatii IEC 62061 -standardin mukaisen SIL-luokituksen, ei sen määrittämiseksi voi käyttää SISTEMA-ohjelmaa, jonka laskenta perustuu SFS-EN ISO 13849-1 -standardin PL-tasojen määrityksiin, vaan silloin on käytettävä standardin IEC 62061 (sekä IEC 61508) mukaisia laskentakaavoja.

SISTEMA-mallinnus käytännössä aloitetaan, kun riskianalyysin perusteella on määritelty vaadittava PL-taso (PLr-taso). PLr-tason perusteella tiedetään, mitä vaatimuksia järjestelmälle (ja sen yksittäisille turvatoiminnoille, sekä turvatoimintojen toteuttaville komponenteille) on asetettu. Tämän jälkeen voidaan käyttää laitevalmistajien julkaisemia SISTEMA-kirjastoja, eli tietokantoja, joista löytyy turvallisuuteen käytettävien komponenttien määritellyt tiedot. Nämä voidaan joissain tapauksissa määrittää myös itse SISTEMA-ohjelman *hyvät insinöörikäytännöt* -aputoiminnon avulla. SISTEMA:n avulla voidaan jo suunnitteluvaiheessa valita sopivat komponentit koneturvallisuuden varmistamiseksi.

SISTEMA-mallinnuksesta voidaan myös tulostaa raportti, jossa todetaan saavuttiko järjestelmä vaaditun suoritustason vai ei. Tämä voidaan liittää esimerkiksi asiakkaalle annettaviin dokumentteihin.

Tässä työssä SISTEMA-ohjelmistotyökalua käytettiin todentamaan riskianalyysissä määritellyt vaadittavat PLr-tasot tankonostimen turvatoiminnoille. Ohjelman avulla selvitettiin, toteutuuko nykyisen SFS-EN 13849-1 vaatima turvallisuuden taso tällä hetkellä jo suunnitellussa koneessa, jonka suunnittelulähtökohtana on ollut vanha standardi SFS-EN 954-1.

3.5 Näyttämömekaniikka

Näyttämömekaniikka tarkoittaa teatteritekniikkaa. Näyttämömekaniikka mahdollistaa lavasteiden noston ja laskemisen, esiripun liikkeen, pyörivän näyttämön, nousevat ja laskevat lattiat yms. Toisin sanoen puhutaan teatteriesityksen lavasteiden ja tehosteiden tekniikasta. Tällaista tekniikka on käytössä teattereissa sekä muun muassa TV-studioissa ja loistoristeilijöillä.

Näyttämömekaniikan koneistaminen vaatii huolellista riskien arviointia, sillä kohteena on teatteri, jossa työskentelevät pääsääntöisesti teatterialan ammattilaiset, eivätkä tekniikan asiantuntijat. Tämä lisää painetta koulutuksille ja käyttöohjeille. Riskianalyysissä tällaiset seikat on otettava huomioon.

Koneiden käyttäjien lisäksi näyttämöalueella liikkuu paljon muuta henkilökuntaa, kuten näyttelijöitä, puvustajia, maskeeraajia ynnä muita sellaisia henkilöitä, joiden toiminta saattaa aiheuttaa ennalta arvaamattomia riskejä. Nämä seikat asettavat myös rajoituksia, kuten kulkurajoituksia konetiloihin ja huoltosilloille. Tämä lisää valvonnan ja suojaustoimien tarvetta.

Ohjausjärjestelmä tällaisessa kohteessa, jossa saattaa esiintyä useita erilaisia koneita tai koneryhmiä, kuten tankonostimia, pistenostimia, pyörönäyttämö, lattianostimia jne. täytyy olla turvallinen ja luotettava. Ohjausjärjestelmä voi ohjata jopa kymmeniä taajuusmuuttajakäyttöjä. Riskianalyysin perusteella on selvitettävä turvallisuustoimenpiteet.

Koneiden yhteiskäyttö on esitysten aikana yleistä, joten ohjausjärjestelmälle on suunniteltu käyttöliittymä, joka mahdollistaa mm. ryhmäajoja ja ennalta ohjelmoituja ajoja. Tarkat ajoitukset sekä paikoitukset esityksen aikana ovat perusvaatimus.

Koneiden ohjaus vaatii joissakin tilanteissa useampaa ohjaajaa, siksi ohjauspaikkoja on useita, kuten myös ohjauspaneeleita. WLAN- ja radiotekniikkaa käytetään hyväksi langattomassa ohjauksessa.

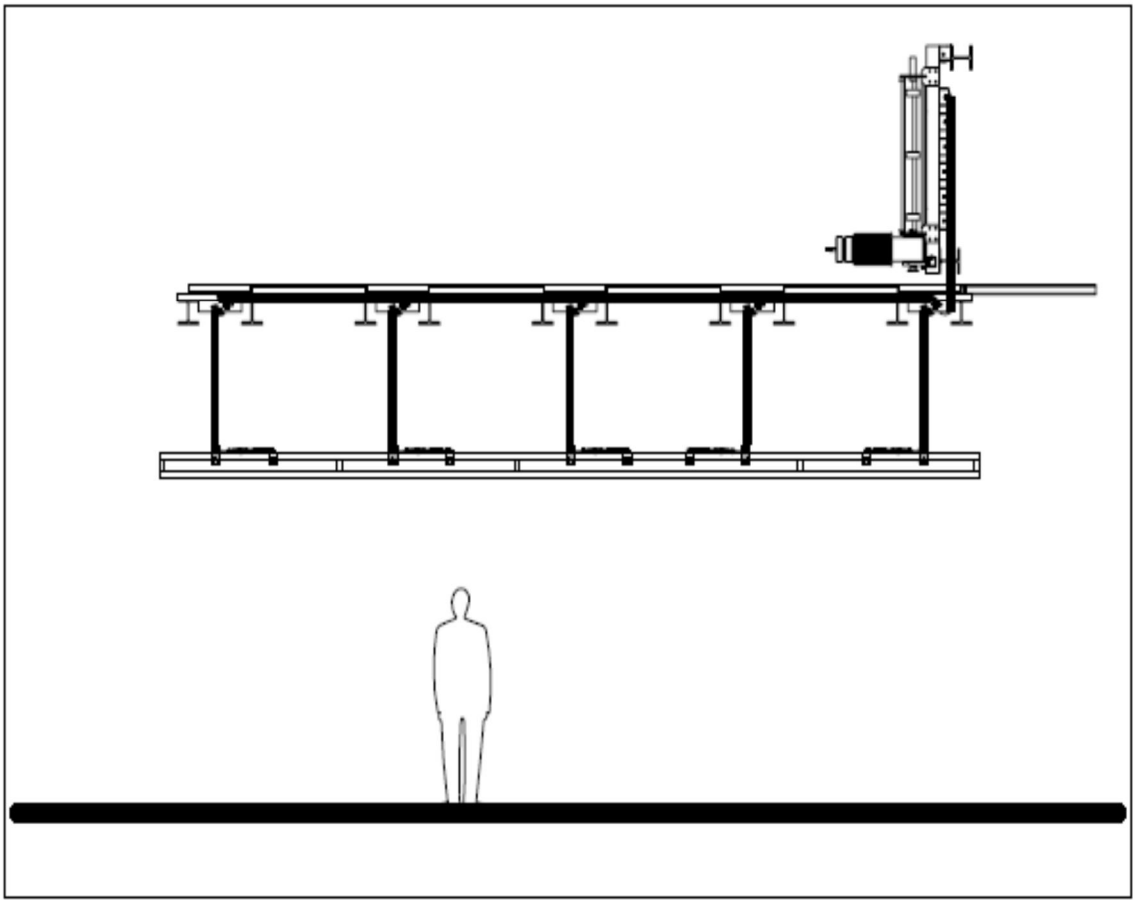
Ohjausjärjestelmän on nidottava kaikki koneet yhteen ja turvatoimintojen on oltava riittävät. Esimerkiksi hätäpysäytys-toiminnon on pysäytettävä useita koneita yhtä aikaa, sillä vaaratilanteen sattuessa usein muiden koneiden liike saattaa aiheuttaa lisää vaaratilanteita.

Tankonostin

Insinöörityössä oli tarkoituksena laatia riskianalyysimalli näyttämöteknisille laitteille. Tämä toteutettiin siten, että malli olisi samalla valitun koneen valmis riskianalyysi. Riskianalyysimallin koneeksi valittiin tankonostin, sillä se on varsin yleinen kone teatterihankkeissa. Yhdessä teatterissa saattaa olla kymmeniä tankonostimia.

Tankonostimella nostetaan ja lasketaan muun muassa lavasteita ja taustoja, jonka takia sitä kutsutaan myös lavastenostimeksi. Tankonostin on kone, jolla on taajuusmuuttajaohjattu, jarruilla varustettu sähkömoottori. Taajuusmuuttajaa ohjaa ohjaus- ja turvalogiikat. Tankonostimen moottori pyörittää vaijerirumpua.

Vaijerirumpuun on kiinnitetty vaijeri, joka kiinnittyy eri taljojen kautta useaan eri paikkaan tankoa tasapainon saavuttamiseksi. Kun moottori pyörittää vaijerirumpua, rumpu joko kerää tai päästää vaijeria, jolloin tanko laskee ja nousee riippuen valitusta moottorin pyörimissunnasta. Tankonostimen periaatepiirros esitetään kuvassa 8 (ks. seur. s.).



Kuva 8. Tankonostimen periaatepiirros [11]

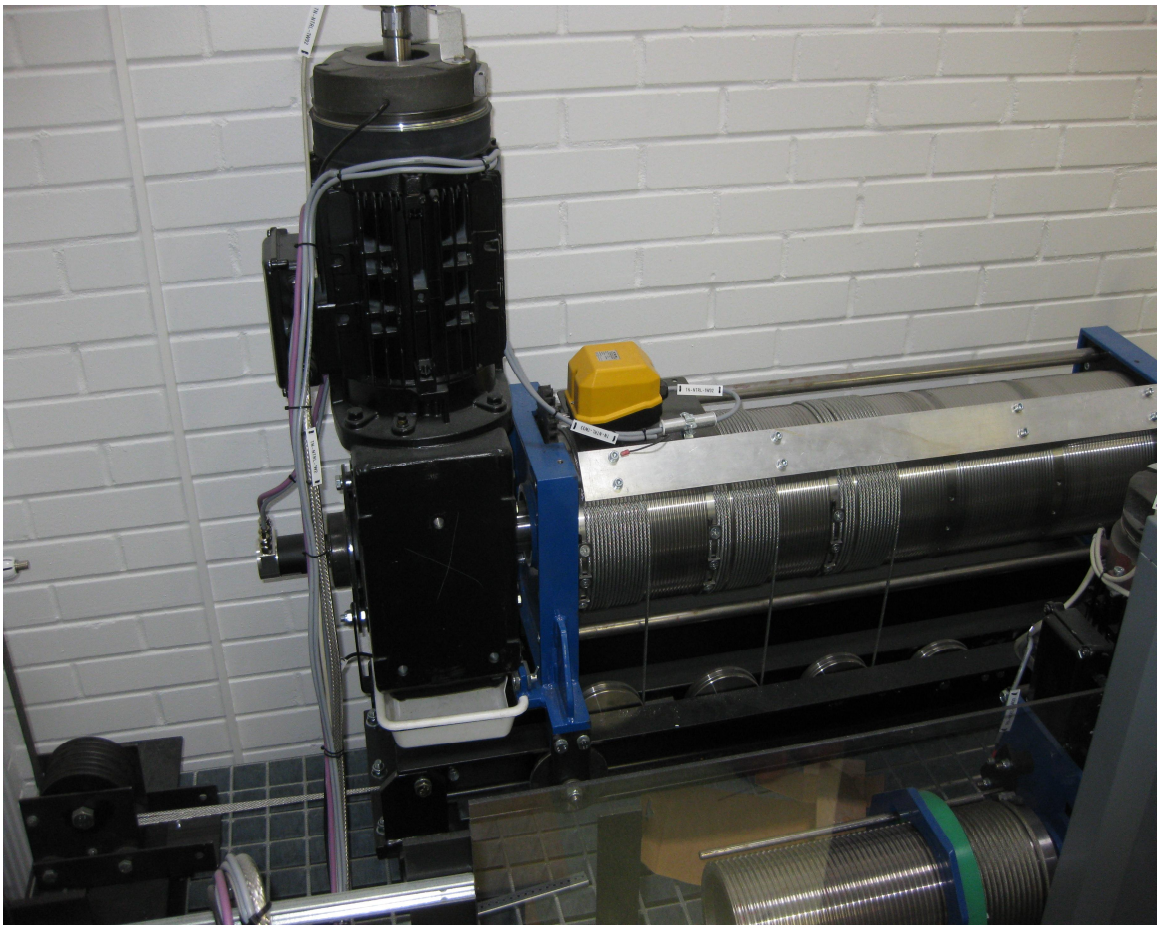
Tankonostimen ohjaaminen vaatii ohjaajalta valvontaa. Teattereissa tankonostimien koneet sijoitetaan niin sanotulle köysiullakolle, joka sijaitsee näyttämön yläpuolella. Tanko liikkuu vaijereiden varassa näyttämön yläosassa. Ajonaikaisen valvonnan tulisi yltää koko ajoalueelle, jotta vältyttäisiin tankojen takertumisista kiinteisiin esteisiin tai ihmisiin.

Konetta ohjataan esitysten aikana pääosin pääohjauspaneelilla manuaalisesti tai ennalta määrätysti automaattiajolla. Insta Automation Oy:n tiloissa Tampereella on rakennettu demolaitteisto testaus- ja koulutustarpeisiin. Demolaitteiston pääohjauspaneeli esitetään kuvassa 9 (ks. seur. s.).

Kuva 9. Insta Automation Oy:n demolaitteiston pääohjauspaneeli [11]

Ohjauspaneeliin tuodaan kaikki tarvittavat tiedot koneesta ja sen tilasta. Konetta ohjaava henkilö näkee paneelistaan muun muassa liikenopeuden, korkeuden ja kuorman massan. Koneen kaikki hälytykset nähdään suoraan ohjauspaneelista.

Tankonostimen moottori sijoitetaan konetilaan teatterin köysiullakolle. Tämä tila on yleensä valvottu tai lukittu, sillä siellä liikkuminen ja oleskelu koneiden käytön aikana voi olla vaarallista. Ajettavan tankonostimen vaijerirumpu (ks. kuva 10 seur. s.) saattaa aiheuttaa esimerkiksi takertumisvaaran.



Kuva 10. Insta Automation Oy:n demolaitteiston tankonostimen koneistus ja vaijerirumpu [11]

Kuvassa 10 on esitetty Instan demolaitteiston tankonostimen sähkömoottori, vaihde sekä vaijerirumpu. Koneessa on rajapaketti ajo- ja turvarajoja varten sekä anturit pyörimisnopeuden, paikoituksen sekä kuorman massan määrittämiseen. Myös esimerkiksi törmäystilanteita varten koneessa on löysän köyden vahti, joka pysäyttää moottorin.

Tankonostimen kattokoneistoon kuuluu taittopyöriä ja niiden kiinnityksiä. Moottorin akselin jälkeen voimansiirto tapahtuu rummun vaijerien avulla, jotka kiinnittyvät tankoon. Insta Automation Oy:n demolaitteiston tankonostimen esitetään kattokoneistus kuvassa 11 (ks. seur. s.).

Kuva 11. Insta Automation Oy:n demolaitteiston tankonostimen tanko, sekä katon vaijeripyörästöt [11]

Kuvien 9-11 demolaitteisto on rakennettu siten, että kone sähkömoottoreineen sekä sähkökeskuksineen (myös taajuusmuuttaja) ovat lattiatasolla, ja vaijeri kulkee lattiasta kattoon, kunnes lopulta kiinnittyy tankoon. Teattereissa koneet ovat yleensä ylhäällä köysiullakolla, jolloin ne eivät ole näyttämötasolla kenenkään tiellä. Muuten kuvien demolaitteisto on pääosin samanlainen kuin teattereissa yleensä käytetyt tankonostimet.

4 Tankonostimen riskianalyysin laadinta ja vaiheet

Tankonostimen riskianalyysissa jouduttiin tekemään tiettyjä oletuksia koneen käyttöön liittyen. Esimerkiksi riskianalyysia laadittaessa ei voitu ottaa huomioon tankoon ripustettavien lavasteiden kiinnityksiä, jotka ovat käyttäjän vastuulla. Lisäksi oli oletettava, että käyttäjä noudattaa käyttö-, huolto ja turvaohjeita, ja että näyttämöalueella työskentelevät henkilöt tiedostavat koneista aiheutuvat vaarat. Lisäoletuksena oli, että ainoastaan katsomoalueella on kouluttamattomia henkilöitä.

Riskianalyysissa kuvattiin tankonostimella tehtävä työ sekä määriteltiin koneen tarkoitettu käyttö. Konetta ei ole tarkoitettu ihmisten nostoon. Näyttelijöiden nostamiseen ja siirtoon esityksen aikana tarkoitetut koneet eivät kuulu konedirektiivin 2006/42/EY soveltamisalaan.

Instan kokonaistoimitusprojektien luovutusaineistoon kuuluu jokaisen koneen tarkempi toimintaperiaatteen kuvaus. Koneen ja sen toiminnan hahmottamiseksi on riskianalyysissa esitelty suunnittelun lähtökohdat, kuten mekaanisen mitoituksen periaatteet, sähkönsyöttö, sähkömoottorin koko, tangon liikenopeus, maksimi kuormitus tangolle jne.

Riskianalyysissa mainitaan koneen vaatimustenmukaisuudet voimassa oleviin turvallisuusmääräyksiin ja standardeihin, joita käytetään teatteritekniikkaan soveltuvin osin. Konedirektiivin 2006/42/EY lisäksi koneen suunnittelussa noudatetaan myös pienjännitedirektiiviä 2006/95/EY sekä EMC-direktiiviä 2004/108/EY ja näitä soveltavia standardeja. Insta toimittaa aina koneidensa mukana myös säädösten vaatiman vaatimustenmukaisuusvakuutuksessa, jossa on eriteltynä kaikki noudatetut normit ja standardit.

Koneen raja-arvojen määrittäminen

Koneen käytöstä on määritelty tarkoitettu käyttö ja käyttäjät sekä kohtuudella ennakoitavissa oleva väärinkäyttö, kuten ylikuormaus. Kohtuudella ennakoitavat väärinkäytöt ovat vaaratekijäluettelossa otettu huomioon. Esimerkiksi ylikuormaamisen estämiseksi koneessa on punnitusanturi, jolloin koneen käyttäjä näkee tankoon asetetun kuorman massan. Moottorissa on kaksi sähkömekaanista jarrua, joiden toiminta on toisistaan

riippumatonta. Jarrut ovat mitoitettu siten, että yhdenkin jarrun momentti riittää kantamaan 1,25 -kertaisen ylikuorman.

Koneen vaatimat fyysiset tilarajat ja aikarajat on määritelty, kuten myös koneen käyttöluokitus. Käyttöluokitus on tarkennettu ajoittaiskäyttökertoimella. Koneen raja-arvoista vielä äänentasot ja koneen aiheuttama tärinä, sekä sähkönsyötön rajat että käyttöolosuhteet ovat myös määritelty riskianalyysissä.

Raja-arvojen määrittämiseen tiedot on kerätty edellisen teatteriprojektin tankonostin -koneiden arvojen perusteella. Raja-arvot määräytyvät jokaisessa projektissa tapauskohtaisesti koneelle vaaditun kuormitettavuuden, nopeuden yms. ominaisuuksien perusteella. Koneen kaikki raja-arvot on määritelty koneen koko elinkaaren eri vaiheille.

Vaarojen tunnistaminen

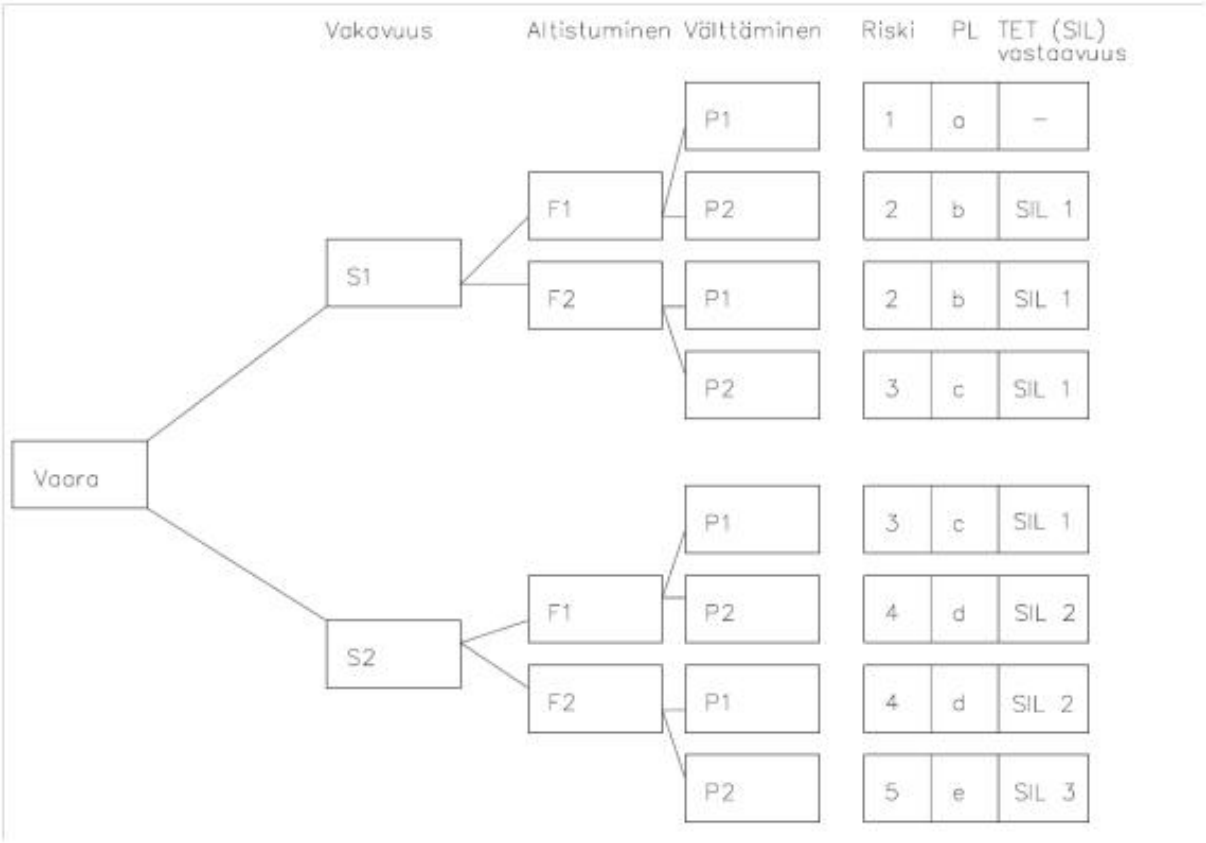
Vaaratekijöiden aiheuttamien riskien arviointiin on käytetty vika- ja vaikutusanalyysia (VVA). Vaaratekijät on luetteloitu, ja niiden aiheuttamat riskit on kuvattu. Yleisimmät onnettomuusskenaariot sekä kaikki yksittäiset vaaratekijät on käsitelty, kuten myös koneen vikaantumiseen liittyvät olennaiset vaaratilanteet.

Vaarojen tunnistamista varten on riskianalyysissa tarkastellun järjestelmän laajuus rajattu. Tarkastelussa määritelty kone koostuu mekaanisista ja sähköisistä osista sekä sen ohjausjärjestelmästä.

Vaaratekijäluettelon mukaiset jäännösriskit sekä niiden minimointi on käsitelty. Kaikki riskit on turvatoiminnoilla saatettu hyväksyttävälle tasolle, ja lisäturvallisuutta on tuotu ohjeistuksilla ja varoitusmerkinnöillä.

Riskin suuruuden arviointi

Riskianalyysia tehdessä on määriteltävä, mihin riskien arviointi perustuu. Tankonostimen riskianalyysi perustuu vika- ja vaikutusanalyysiin sekä riskigraafiin, jonka mukaan määritellään jokaiselle vaaratekijälle erikseen riskin suuruus (ks. kuva 12).



Kuva 12. Riskigraafi, vaaratekijöiden riskien arvioimiseksi

Jos turvallisuuteen liittyvä ohjausjärjestelmä suorittaa turvatoiminnon vaaratekijän aiheuttamalle riskille, on sille määriteltävä suoritustaso PL, jota voidaan verrata standardin IEC 62061 mukaiseen TET-tasoon. Tämän riskigraafin idea riskin suuruuden arvioimiseksi esitellään standardissa SFS-EN ISO 13849-1. Myös muut menetelmät riskin suuruuden arvioimiseksi ovat sallittuja.

Riski muodostuu graafin perusteella vamman vakavuuden (S), vaaralle altistumisen (F) ja vaaran välttämisen mahdollisuuden mukaan (P).

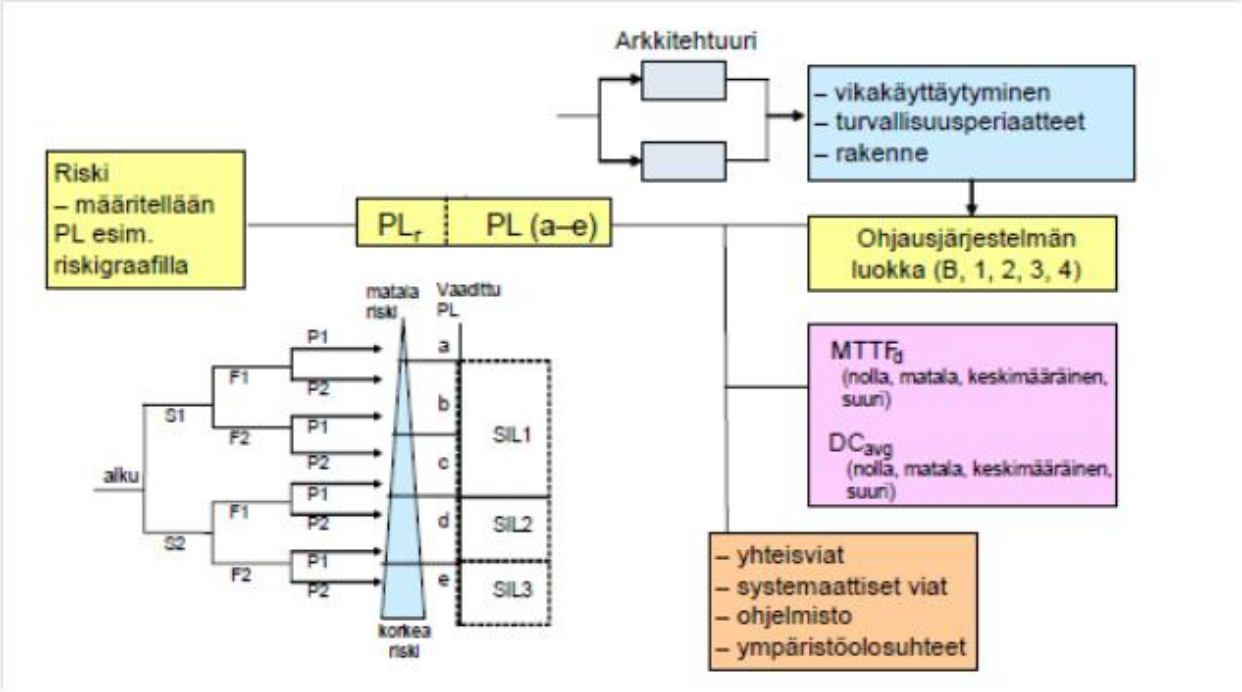
- S vaaran aiheuttaman vamman vakavuus on
    - S1 lievä (tavallisesti palautuva vamma)
    - S2 vakava (tavallisesti palautumaton vamma tai kuolema)

- F vaaralle altistumisen taajuus ja/tai kesto on
    - F1 harvoin...toisinaan ja/tai lyhyt altistumisaika
    - F2 toistuvasti...jatkuvasti ja/tai pitkä altistumisaika

- P mahdollisuus välttää vaaraa tai rajoittaa vahinkoa on
    - P1 mahdollista tietyissä olosuhteissa
    - P2 tuskin mahdollista.

Näistä osatekijöistä voidaan arvioida suoraan riskin suuruus. Vaaratekijän aiheuttaman riskin suuruuden mukaan määritellään turvatoimenpiteet riskin pienentämiseksi, sekä turvatoiminnon toteutustapa.

Jos turvatoiminto toteutetaan turvallisuuteen liittyvällä ohjausjärjestelmällä, määritellään vaadittava PLr-taso, joka myöhemmin todennetaan esimerkiksi SISTEMAA apuna käyttäen. Riskianalyysi ja riskinarviointi ovat osa koneen suunnitteluprosessia, johon kuuluu myös turvatoimintojen suunnittelu. Ohjausjärjestelmän toteuttamien turvatoimintojen suunnittelu perustuu koneen riskianalyysin asettamiin vaatimuksiin (ks. kuva 13 seur. s.).



Kuva 13. Suoritustason PL arvioinnissa huomioitavat seikat [7, s.20]

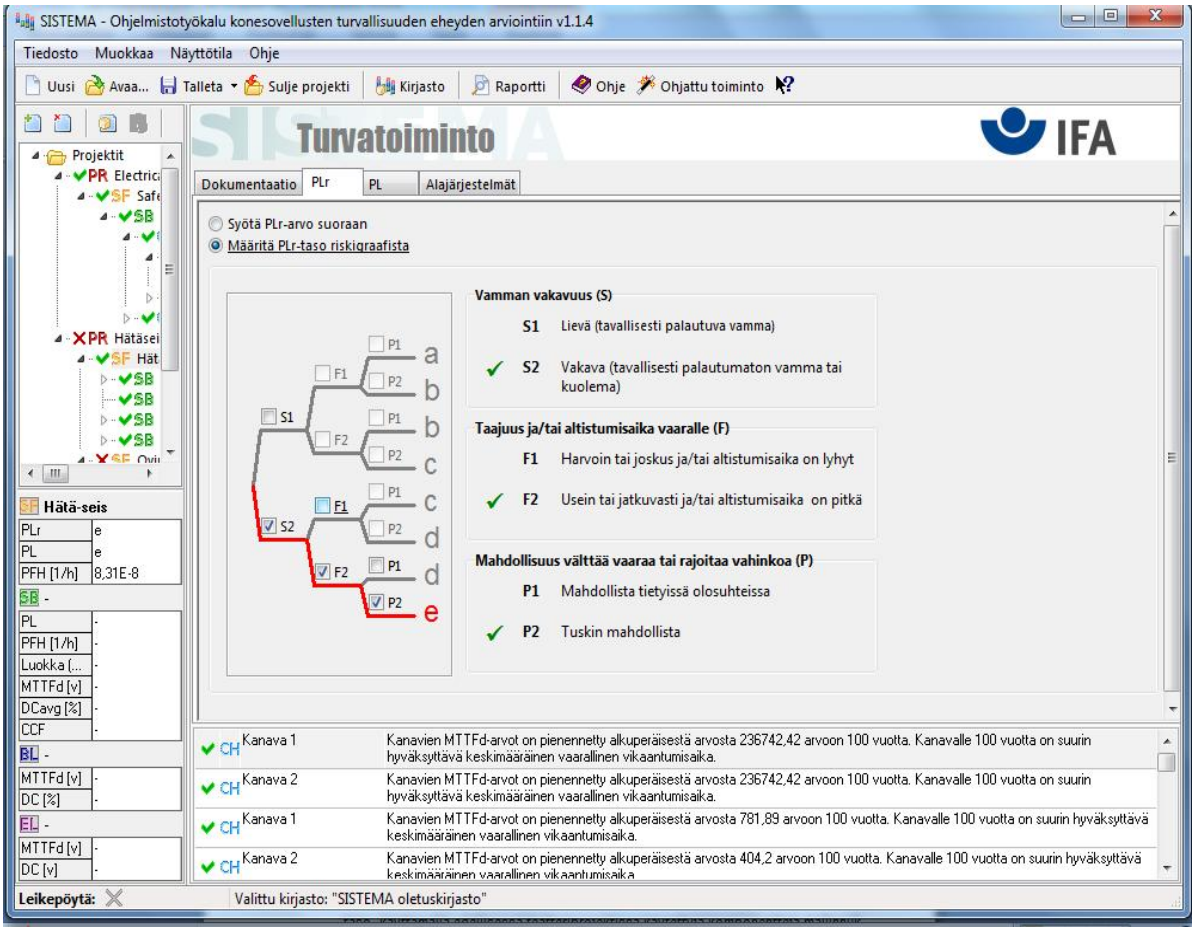
Kuvassa 13 on esitetty tiivistettynä riskinarvioinnin kulkukaavio turvatoiminnon suoritustason arvioinnista, ja mitä asioita on turvallisuuteen liittyvän ohjausjärjestelmän suunnittelussa otettava huomioon määritetyn PLr-tason saavuttamiseksi.

Riskin pienentäminen ja SISTEMAN hyödyntäminen

Riskianalyysin perusteella tankonostimen suurimmat riskit liittyvät konetilassa (usein köysiullakolla) sijaitsevien koneiden vaijerirumpuihin ja -taittopyörästöihin, jotka koneen käydessä pyörivät ja saattavat aiheuttaa takertumisvaaran tai puristumisvaaran aiheuttaen esimerkiksi sormen menettämisen. Tällainen vamma on pysyvä (S2).

Koneet käyvät useaan kertaan teatteriesityksen aikana, joten vaaralle voi teoriassa joku altistua usein ja toistuvasti (F2). Koneita ohjataan näyttämötasolta, ja jos ei tiedä esimerkiksi, mitkä lavasteet liikkuvat esityksen, voidaan ajatella, että konetilassa liikkuvan henkilön on hyvin vaikeata välttää koneiden liikkeestä aiheutuvat vaarat (P2).

Näin saadaan koneen vaijerirummun aiheuttamalle vaaratekijälle riskigraafin perusteella riskin suuruudeksi 5. Jos turvatoiminto toteutetaan turvallisuuteen liittyvällä ohjausjärjestelmällä, vaaditaan siltä graafin perusteella PL e -taso (PLr e), jotta riski pienenisi hyväksyttävälle tasolle. PLr-tasojen määrittely voidaan kuvan 14 mukaisesti tehdä myös SISTEMA-ohjelmassa.



Kuva 14. SISTEMA-ohjelmistotyökalun käyttäminen turvatoiminnon PLr-tason määrittämiseksi

Konetilassa liikkuminen ei ole tarpeellista koneiden käytön aikana, joten suojatoimenpiteenä vaara-alueella liikkuminen estetään koneiden ollessa käynnissä. Tämä toteutetaan esimerkiksi konetilan eristävällä turvaportilla, johon asennetaan kulkua valvova oviraja. Tällöin turvatoiminnon toteuttaa turvallisuuteen liittyvä ohjausjärjestelmä.

SISTEMA-ohjelmaa hyväksikäyttäen määriteltiin tämän turvatoiminnon toteuttama PL-taso, käyttämällä edellisessä teatteriprojektissa käytettyjä komponentteja mallinnuksessa. Turvaportin oviraja oli pakkotoiminen ja siinä oli tuplakoskettimet.

Pakkotoiminen oviraja on silloin, kun sen koskettimet toimivat suoraan mekaanisesti. Pakkotoimiset koskettimet toimivat silloinkin kun ne ovat esimerkiksi hitsautuneena asentoonsa.

Turvarajan asematieto ohjattiin turvalogiikalle, joka on kahdennettu. Turvalogiikka ohjaa koneen hätäpysäytystilaan riskianalyysissä määritellyn pysäytysluokan 1 mukaisesti. Pysäytysluokka 1 tarkoittaa moottorin pyörimisnopeuden hidastettua alasajoa, sekä syötön poiskytkentää. Kone on pysäytettävä rampilla mekaniikan kestävyyden vuoksi.

Pysäytysluokka 1 toteutetaan siten, että turvalogiikka ohjaa samanaikaisesti taajuusmuuttajaa, sekä aikaviivästettyä kontaktoria. Taajuusmuuttaja saa tiedon hätäpysäytyksestä ja ajaa moottoria siihen asetetun ramppiajan mukaan ja pitää momentin yllä niin kauan kunnes molemmat jarrut ovat kiinni. Tähän kuluvan ajan jälkeen kontaktori katkaisee koneen sähkönsyötön.

Tällä tavoin kahdennettu ja valvottu järjestelmä mallinnettuna SISTEMA-ohjelmalla tietyillä komponenttivalinnoilla toteuttaa turvatoiminnon PL e -tason mukaisesti ja vastaa tällöin TET 3 -tasoa.

Riskianalyysiin liitetään SISTEMA:n raportti määriteltyjen turvatoimintojen PL-tason kattamisesta. Tästä on tarkoitus tehdä käytäntö Insta Automation Oy:n teatteriprojektien riskianalyyseja tehdessä. On kuitenkin huomioitava, ettei SISTEMA-ohjelma ota mitään vastuuta turvatoimintojen toimivuudesta, vaan edelleen kaikki vastuu pysyy koneen valmistajalla ja markkinoijalla.

5 Yhteenveto

SISTEMA-ohjelmistotyökalun tai jonkin muun apuohjelman käyttö ohjausjärjestelmien suunnitteluvaiheessa riskianalyysin määrittelemän suoritustason saavuttamiseksi on suositeltavaa. Standardi SFS-EN ISO 13849-1 antaa tarkat vaatimukset eri suoritustasojen saavuttamiseksi, ja monet muuttujat on otettava jo käytettävien komponenttien tasolla huomioon.

Laite- ja komponenttivalmistajilta löytyy kohtalaisen laajat kirjastot omista tuotteistaan, joita voidaan mallintaa SISTEMA-ohjelmalla. Tällä tavoin voidaan määrittää ilman matemaattista laskentaa turvallisuuteen liittyvän ohjausjärjestelmän suorittamien turvatoimintojen suoritustaso standardin SFS-EN ISO 13849-1 vaatimusten mukaisesti. Ilman apuohjelmaa PL-tasojen määrittäminen turvatoiminnoille on erittäin työlästä ja hidasta, toisin sanoen kallista.

On muistettava, että täsmällinen riskianalyysi on tärkeä turvallisuuden kannalta, mutta se on vain osa pitkää suunnitteluprosessia, jonka lopputuloksena on valmis vaatimustenmukainen kone. Kaikki apuvälineet, kuten SISTEMA ja sen kaltaiset ohjelmistot, ovat omiaan nopeuttamaan ja tehostamaan koko suunnitteluprosessia.

Työssä tarkasteltu tankonostin täyttää konedirektiivin vaatimukset. Kuitenkin insinöörityön riskianalyysin pohjalta tehdyn SISTEMA-mallinnuksen avulla tankonostimen turvallisuuteen liittyvän ohjausjärjestelmän heikoimmat lenkit paikannettiin ja joitakin komponenttivalintoja pohdittiin uudestaan.

SISTEMA-ohjelman ansiosta riskianalyysi sidotaan tiiviimmin muuhun suunnitteluun. Tällöin koneen riskianalyysille tulee lisää painoarvoa sekä luotettavuutta.

Insinöörityössä tehtyä tankonostimen riskianalyysia on tarkoitus käyttää Insta Automation Oy:n tulevissa teatteriprojekteissa riskianalyysimallina, jota jalostetaan projekti- ja konekohtaisesti. SISTEMA-ohjelmistotyökalu on tarkoitus ottaa käyttöön Insta Automation Oy:n suunnitteluosaston apuvälineenä.

Lähteet

1 Sähköinen messuesite, Insta Group Oy. <http://www.insta.fi/insta_automation/esitteet/> Päivitetty 29.9.2010. Luettu 10.4.2012.

2 Valtioneuvoston asetus 400/12.6.2008 koneiden turvallisuudesta.

3 Suomen sähkö- ja elektroniikka-alojen standardointijärjestö Sesko ry, verkkoaineisto. <http://www.sesko.fi/portal/fi/standardisointijarjestelma/>. Luettu 10.4.2010.

4 Metalliteollisuuden standardoimisyhdistys, MetSta ry, verkkojulkaisu. <http://www.metsta.fi/ipubs/html/machinery/standards/05-00-00.html>. Päivitetty 14.10.2009. Luettu 10.4.2012.

5 SFS-EN ISO 13849-1: Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1: Yleiset suunnitteluperiaatteet. Helsinki: Suomen Standardisoimisliitto. 28.12.2009.

6 Siirilä, Tapio. 2009. Koneturvallisuus III: Ohjausjärjestelmät ja turvalaitteet. Helsinki: Fimtekno Oy.

7 Hietikko, Marita & Malm, Timo & Alanen, Jarmo. 2009. Koneiden ohjausjärjestelmien toiminnallinen turvallisuus: Ohjeita ja työkaluja standardien mukaisen turvallisuusprosessin luomiseen. VTT -tiedote 2485. Espoo: VTT.

8 Sundquist, Matti. 12.4.2010. Ohjelmistotyökalun Sistema käyttö koneiden turvatoimintojen suunnittelussa. Verkkoartikkeli Nro 4/2010. MetSta ry. <http://www.metsta.fi/ipubs/docs/machinery/articles/2010_nro_004.pdf>. Luettu 20.4.2012

9 Sundquist, Matti. Teollisuusautomaation standardit: Osio 2. Verkkodokumentti, Sesko ry. < http://www.sesko.fi/attachments/ohjeet/osio_2.pdf>. Luettu 10.4.2012.

10 BGIA report 2/2008e: Functional safety of machine controls, application of EN ISO 13849-1, p. 19. 2nd edition, 6.2009. Germany, Berlin: German Social Accident Insurance (DGUV)

11 Insta Automation Oy