Opinnäytetyö AMK

Konetekniikka

2024

Antti Saarela

Henkilöstön hätähälytysjärjestelmän päivitys

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö AMK | Tiivistelmä

Turun ammattikorkeakoulu

Konetekniikka

2024 | 37 sivua

Antti Saarela

Henkilöstön hätähälytysjärjestelmän päivitys

Opinnäytetyön tavoitteena oli perehtyä turva-automaatioon ja sen standardeihin, direktiiveihin ja säädöksiin sekä tutustua ohjelmoitaviin logiikoihin ja turvakomponentteihin, joiden pohjalta uusi henkilöstön hätähälytysjärjestelmä suunniteltaisiin. Vanha henkilöstön hätähälytysjärjestelmä oli tehtaan alkuperäinen vuodelta 1983, joten järjestelmä uusittiin nostattamaan järjestelmän luotettavuutta sekä tehtaan turvallisuutta.

Työssä käytiin läpi turva-automaatioon liittyvistä direktiiveistä sekä standardien SFS EN-ISO 13849-1 sekä SFS EN-ISO 12100 asettamat vaatimukset turva-automaation suunnitteluun, kuten riskien arviointi, suoritustasot, vaarallinen keskimääräinen vikaantumisaika, diagnostiikan kattavuus sekä yhteisvikaantumista estävät toimenpiteet. Näiden perusteella arviointiin järjestelmän vaadittava suoritustaso. Tämän jälkeen syvennyttiin automaation logiikoihin, turvakomponentteihin sekä ohjelmointiin, jonka jälkeen järjestelmä suunniteltiin. Suunnittelussa kuvailtiin vanhaa järjestelmää ja uuden järjestelmän vaatimuksia, tehtiin ristien arviointi, kerrottiin automaatioväylien rakenteesta, uuden järjestelmän komponenteista, logiikan liitännöistä, kelpuutuksesta sekä dokumentoinnista.

Lopputuloksena oli kattava ja tiivis ohjeistus henkilöstön hätähälytysjärjestelmän päivittämiseen, jota voidaan hyödyntää minkä tahansa turva-automaatiojärjestelmän suunnitteluun. Tämä mahdollistaa myös muidenkin tehtaiden turvallisuuden kehityksen ja luotettavuuden.

Asiasanat:

Automaatio, ohjelmoitava logiikka, riskien arviointi, standardit, suunnittelu, turvallisuus.

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Mechanical Engineering

2024 | 37 pages

Antti Saarela

Design of personnel emergency alarm system

The aim of the thesis was to delve into safety automation and its standards, directives, and regulations, as well as to get familiar with programmable logics and safety components on which the new personnel emergency alarm system would be designed from. The old personnel emergency alarm system was the original factory model from 1983, so the system was renewed to enhance its reliability and the safety of the factory.

The thesis covered the requirements for safety automation design set by directives related to safety automation and standards SFS EN-ISO 13849-1 and SFS EN-ISO 12100, such as risk assessment, performance levels, mean time to dangerous failure, diagnostic coverage, and common cause failures. Based on these, the required performance level of the system was evaluated. Subsequently, attention was given to automation logic, safety components, and programming, after which the new system was designed. The design described the old system and the requirements of the new system, performed a risk assessment, explained the structure of automation networks, outlined the components of the new system, logic interfaces, validation, and documentation.

The result was a comprehensive and concise guide for updating the personnel emergency alarm system, which can be utilized in designing any safety automation system and enabling the development and reliability of safety in other factories as well.

Keywords:

Automation, design, risk assessment, safety, standards, programmable logic.

Sisältö

Kuvat

Taulukot

Käytetyt lyhenteet tai sanasto

CCF	Common Cause Failure
DC	Diagnostic Coverage
Direktiivi	Euroopan unionin ohjeistus yhdenmukaisiin lainsäädäntöihin.
EMC	Sähkömagneettinen yhteensopivuus
I/O	Input/Output
MTTFd	Mean Time to Dangerous Failure
PL	Performance Level
PLC	Programmable Logic Controller, ohjelmoitava logiikka.
PLr	Required Performance Level
SIL	Safety Integration Level.
TIA	Totally Integrated Automation
UPS	Uninterruptible Power Supply

1 Johdanto

Turvallisuus on lähivuosina noussut pintaan monessa yrityksessä. Välttämällä tapaturmia ja noudattamalla sääntöjä, yritykset takaavat turvallisen työympäristön sekä työntekijöille, että myös ympäristölle ja luonnolle. Turvallisuuteen liittyy monia eri tekijöitä, kuten henkilöstön turvaus, vaarallisten aineiden käsittely ja varastointi, laitteiden toimivuuden varmistaminen, direktiivit ja lainsäädännöt sekä eri vaatimuksia järjestelmälle ja sen komponenteille. Vanhojen tehtaiden tulee noudattaa uusia turvallisuusstandardeja ja päivittämään laitteita ja järjestelmiä ajan tasalle.

Tässä opinnäytetyössä käsitellään henkilöstön hätähälytysjärjestelmän päivitystä sekä perehdytään turva-automaatioon. Työn tarkoitus on syventyä turva-automaation eri standardeihin, säädöksiin ja turvallisuusluokkiin, logiikan toimintaan turvallisuuden näkökulmasta sekä antaa ohjeistus toimivan henkilöstön hätähälytysjärjestelmän suunnitteluun toimeksiantajalle sekä yleismallina minkä tahansa turva-automaationjärjestelmän suunnitteluun.

Toimeksiantajana työlle toimii PCAS Finland, joka on Seqens konserniin kuuluva lääketeollisuuden yritys, joka on Suomen ensimmäinen lääkeaineita valmistava yritys. Yritys aloitti lääkeaineiden valmistuksen vuonna 1962 nimellä Leiras, jonka jälkeen ranskalainen konserni PCAS osti Leiraksen vuonna 2003. Vuonna 2016 PCAS yhdisti konsernin Novacapin kanssa, jonka nimi vaihdettiin 2018 ja tunnetaan nykyään nimellä Seqens. Turun tehdas on rakennettu uudestaan 1983. (Seqens 2024.) Seqens-konsernin liikevaihto vuonna 2021 on 31,5 miljoonaa. Konsernilla on 24 tehdasta ympäri maailmaa, jotka työllistävät 3200 työntekijää. PCAS valmistaa pääsääntöisesti lääkkeiden vaikuttavia aineita. (Seqens 2024.)

2 Turvallisuuden direktiivit, standardit ja lainsäädäntö

Lääketeollisuudessa ollaan päivittäin tekemisissä syövyttävien, hapettavien ja räjähtävien aineiden kanssa, toimitaan isojen laitteiden parissa sekä käytetään suuria paineita. Prosessiteollisuuden turvallisuudelle ei ole vain yhtä säädöstä tai lakia, vaan säädöksiä on useita, joita noudattamalla saadaan aikaan turvallinen kokoonpano.

Direktiiveillä tarkoitetaan Euroopan unionin antamia ohjeita, joilla yhdenmukaistetaan jäsenvaltioiden lainsäädäntöjä. Direktiivien tavoite on antaa valmistajille ohjeistus turvallisten koneiden valmistukseen ihmisten, koneiden sekä ympäristön kannalta. Näin direktiiviä noudattavat tuotteen voivat liikkua vapaasti Euroopassa. (Metropolia 2017.)

2.1 Konedirektiivi

Konedirektiivi eli Euroopan parlamentin ja neuvoston direktiivi 2006/42/EY määrittelee vaatimukset koneiden suunnittelulle, valmistukselle ja käytölle Euroopan maissa. Konedirektiivi määrittää vaatimukset erilaisten koneiden ja laitteiden turvallisuudelle, riskien arvioinnille ja vähentämiselle sekä ohjeille ja dokumenteille. Konedirektiiviä noudattavat tuotteet täyttävät kaikki vaatimukset ja riskiarvioinnit. Tuotteiden tulee olla CE-merkittyjä ja sen mukaisia. (Konedirektiivi 2006/42/EY.)

Konedirektiiviin sisältyy standardeja, joita tulee noudattaa. Standardien tarkoitus on asettaa yhteiset ja hyväksytyt käytännöt eri valmistajien välille. Standardit antavat pohjan, jonka avulla voidaan varmistaa tuotteiden, palveluiden ja järjestelmien laatu, turvallisuus ja tehokkuus eri toimialoilla. Turvallisuuden standardien tarkoitus on suojata ihmisiä, ympäristöä ja koneita vaaratilanteilta ja tuoda turvaa, sekä mahdollistaa muuten vaarallisten töiden teon.

Standardin ISO 12100 mukaan standardit jaetaan A-, B- ja C-tyypin standardeihin:

- A-tyypin standardit tarjoavat perustan turvallisuudelle, sisältäen suunnitteluperiaatteet ja yleiset näkökohdat erilaisille koneille sovellettaviksi.
- B-tyypin standardit keskittyvät tiettyyn turvallisuusnäkökohtaan tai suojaustekniseen laitteeseen, jota voidaan hyödyntää eri koneryhmissä:

    - B1-tyypin standardeissa tarkastellaan erityisiä turvallisuusnäkökohtia, kuten melutasoa, turvaetäisyyksiä ja pintalämpötilaa.
    - B2-tyypin standardeissa käsitellään suojausteknisiä laitteita, kuten kaksin käsin hallintalaitteita, koneen toimintaan kytkentälaitteita, kosketuksen tunnistavia laitteita ja suojia.
- C-tyypin standardit keskittyvät tietyn koneen tai koneiden ryhmän yksityiskohtaisiin turvallisuusvaatimuksiin.

2.1.1 SFS-EN ISO 12100. Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen.

SFS-EN ISO 12100 on olennainen A-tyypin standardi, joka antaa kattavan käsityksen peruskäsitteistä, periaatteista ja menetelmistä, jotka ovat keskeisiä turvallisten koneiden suunnittelussa. Se tarjoaa suunnittelijoille selkeät ohjeet riskien arvioinnista ja niiden minimoimisesta. Nämä ohjeet pohjautuvat laajaan asiantuntemukseen koneiden suunnittelusta, käytöstä, poikkeuksellisista tilanteista ja niihin liittyvistä riskeistä. Lisäksi standardi käsittelee riskin suuruuden ja merkityksen arvioinnin, vaarojen tunnistamisen koneen eri elinkaaren vaiheissa sekä keinoja vaarojen poistamiseksi tai riskin asianmukaiseksi pienentämiseksi. (SFS-EN ISO 12100.)

2.1.2 SFS-EN ISO 13849-1. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osat. Osa 1. Yleiset suunnitteluperiaatteet

SFS-EN ISO 13849-1, joka perustuu ISO 12100 -standardiin, on merkittävä B1-tyypin standardi. Se tarjoaa selkeät ohjeet turvallisuuteen liittyvien ohjausjärjestelmän osien suunnitteluun ja integrointiin, kattaen myös ohjelmistosuunnittelun ja niihin liittyvät vaatimukset. Standardi käsittelee turvallisuuteen liittyviä ohjausjärjestelmän osia, jotka toimivat tiheässä vaatetilassa ja jatkuvassa toiminnassa, riippumatta käytetystä teknologiasta tai energiamuodosta. (SFS-EN ISO 13849-1.)

2.1.3 SFS-EN IEC 62061. Koneturvallisuus. Turvallisuuteen liittyvien ohjausjärjestelmien toiminnallinen turvallisuus.

SFS-EN IEC 62061 on suunniteltu palvelemaan konesuunnittelijoita, ohjausjärjestelmien valmistajia sekä muita turvallisuuteen liittyvien

ohjausjärjestelmien määrittelyyn, suunnitteluun ja hyväksymiseen osallistuvia tahoja. Standardissa esitellään lähestymistapa ja vaatimukset, jotka ovat tarpeen vaaditun suorituskyvyn saavuttamiseksi. Tämä helpottaa turvatoimintojen määrittelyä riskien pienentämiseksi. (SFS-EN IEC 62061.)

2.2 Pienjännitedirektiivi

Pienjännitedirektiivi eli Euroopan parlamentin ja neuvoston direktiivi 2006/95/EY kattaa sähkölaitteet, jotka käyttävät 50–1000 V vaihtovirtaa tai 75–1500 V tasavirtaa. Tämän direktiivin päätarkoitus on suojata laitteita ja niiden käyttäjiä sekä varmistaa, että laitteet ovat yhteensopivia Euroopan markkinoilla. Sähkölaitteiden on täytettävä vaatimukset suunnittelun, rakenteen, eristystason, liitäntöjen ja käyttöohjeiden suhteen, ja ne on varustettava CE-merkinnällä. (Pienjännitedirektiivi 2014/35/EU.)

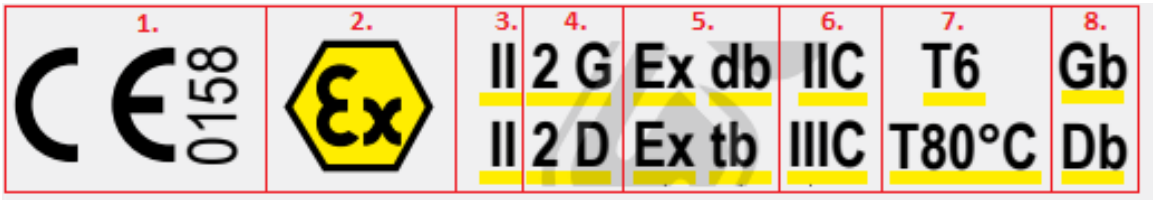
2.3 EMC-direktiivi

Euroopan parlamentin ja neuvoston direktiivi 2004/108/EY, tunnetaan myös EMC-direktiivinä, on suunniteltu varmistamaan sähköisten ja elektronisten laitteiden sähkömagneettinen yhteensopivuus ja asettamaan vaatimukset niiden toiminnalle sähkömagneettisessa ympäristössä. Tavoitteena on turvata laitteiden toimivuus sekä vähentää sähkömagneettisten häiriöiden vaikutusta. EMC-direktiivi koskee kaikenlaisia laitteita, joihin sähkömagneettinen häiriö voi vaikuttaa, kuten automaatiojärjestelmän komponentit ja viestintälaitteet sekä tietokoneet. (EMC-direktiivi 2004/108/EY.)

2.4 Räjähdysvaaralliset tilat

ATEX-laitedirektiivi eli Euroopan parlamentin ja neuvoston direktiivi 2014/34/EU koskee laitteita, jotka soveltuvat räjähdysvaarallisiin tiloihin. ATEX-laitteiden valmistajien tulee noudattaa direktiivin vaatimuksia. Räjähdysvaarallisella tilalla tarkoitetaan tilaa, jossa ilmenee räjähtäviä aineita, kuten kaasuja, höyryjä, pölyä tai helposti syttyvää ainetta, jotka voi aiheuttaa räjähdysvaaran normaalipaineisen ilman kanssa. Räjähdysten estämiseksi tulee räjähdysvaarallisissa tiloissa selvittää vakituiset tai väliaikaiset syttymislähteet, jotka voivat aiheuttaa palavan aineen tai kaasun syttymisen. Tilassa olevien pintojen lämpötila ei tule ylittää tilassa säilytettävien aineiden syttymislämpötilaa, edes laitteiden vikaantuessa. ATEX-tiloissa tulityöt ovat

ainoastaan sallittuja, jos tilassa ei ole eikä tule olemaan räjähdyksen vaaraa ja tulityön ohjeita noudatetaan huolellisesti. Tilassa olevat säiliöt, putkistot ja laitteet, joihin on mahdollista syntyä staattista sähkövarausta, on maadoitettava ja potentiaalitasattava. (Finlex 2012.)



Kuva 1. ATEX-merkinnät (Schischek).

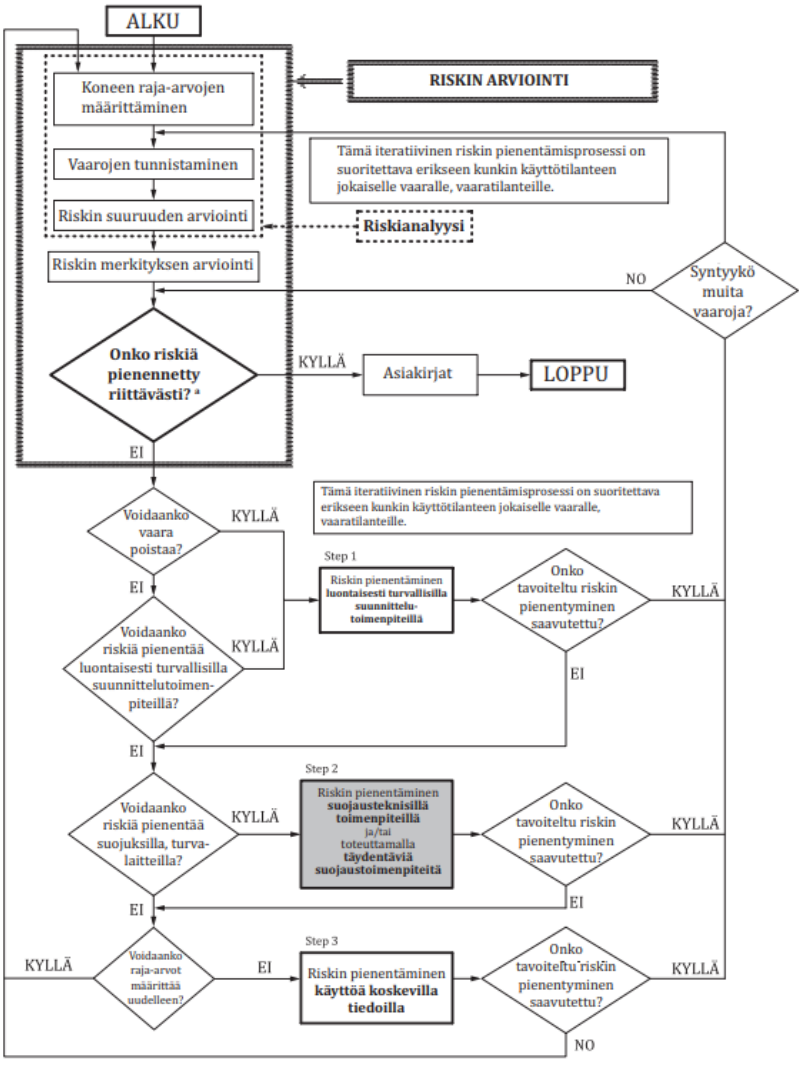
Kuvassa 1 nähdään esimerkki ATEX-laitteiden merkinnöistä, joista saadaan tietoon, mihin laite soveltuu (Schischek):

1. CE-merkintä ja ilmoitettu laitos – CE-merkintä on valmistajan antama merkki, joka takaa tuotteen täyttäneen tietyt EU-direktiivin asettamat vaatimukset. Ilmoitettu laitos arvioi tuotteet EU-direktiivin kanssa ja hoitaa vaatimuksenmukaisuustodistuksen sekä auttaa CE-merkinnän hankkimisessa.
2. Räjähdyssuojatunnus
3. Laiteryhmä – Luokan I laitteet ovat suunnattu kaivosteollisuuteen ja luokan II laitteet muihin kuin kaivosteollisuuden laitteisiin.
4. Laiteluokka – Laiteluokat 1–3 määräytyvät käytetyn tilan mukaan, kuten ilmeneekö tilassa räjähtäviä kaasuja tai pölyä ja kuin usein kaasua tai pölyä tilassa ilmenee. G tarkoittaa kaasuja ja D tarkoittaa pölyä.
5. Räjähdyssuojatunnus ja Ex-rakenne – Räjähdyssuojatunnus on aina Ex, mutta Ex-rakenne vaihtelee käyttökohteen mukaan. Esimerkiksi tulenkestävä luokitus on Exd ja öljysuojattu luokitus on Exo. Rakenteen jälkeen voi olla myös kirjaimet a, b tai c, jotka kertovat, mihin tilaluokkaan (zone) laite soveltuu.
6. Räjähdysryhmä – Ryhmät IIA, IIB ja IIC ovat kaasuille ja määräytyvät tilassa olevien kaasujen ja lämpötilaluokituksen mukaan. Ryhmät IIIA, IIIB ja IIIC ovat tarkoitettu pölylle ja määräytyvät sen mukaan, onko pöly syttyvää ja johtaako pöly sähköä vai ei.
7. Lämpötilaluokka – Lämpötilaluokka kertoo räjähtävän aineen syttymislämpötilan. Kaasujen kanssa luokitus tulee ilmoittaa luokan merkinnällä, kun taas pölyjen kanssa merkataan luokan syttymislämpötila.
8. Laitteen suojataso – Suojataso kertoo, onko kyseessä kaasu vai pölysuojaus sekä laitteen tilaluokan.

3 Riskin arviointi ja riskin pienentäminen

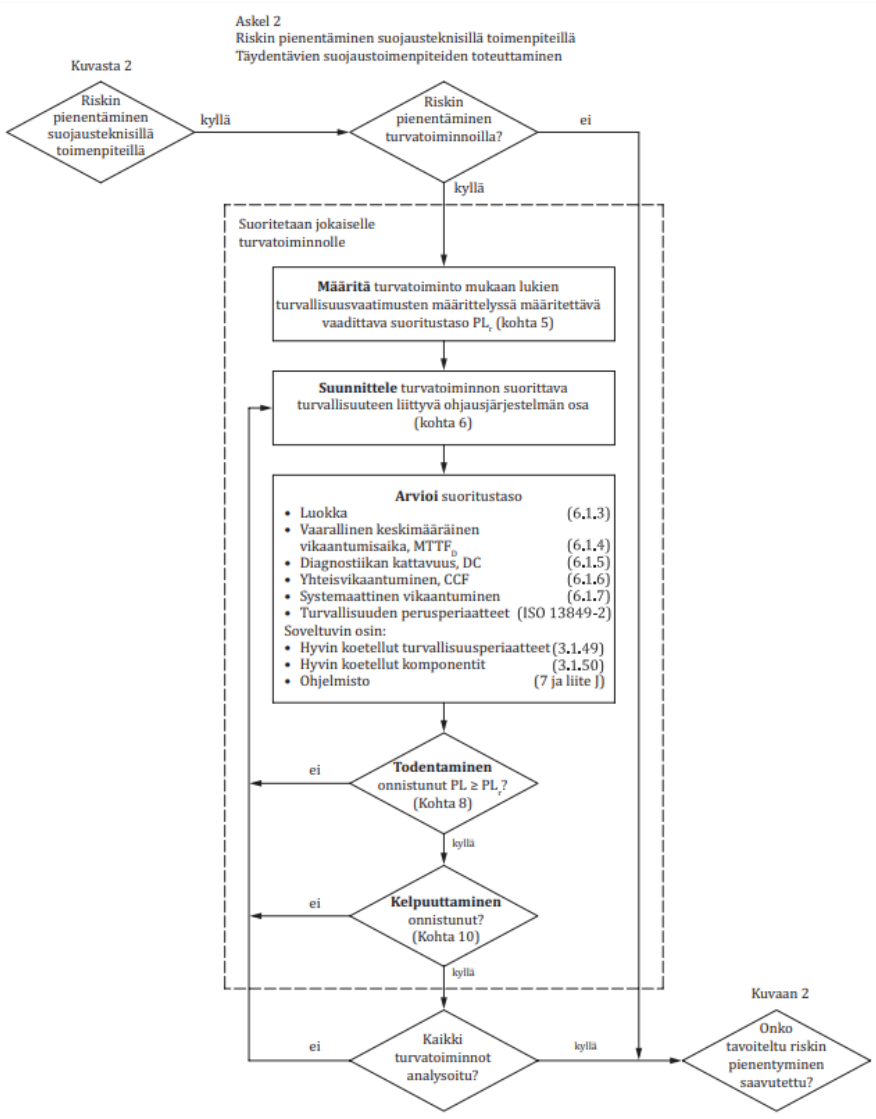
Riskien arvioinnilla pyritään löytämään järjestelmästä vaarat, arvioimaan ne ja tekemään tarvittavat muutokset takaamaan turvallisuuden. Riskien arvioinnin suorittamiseen tarvitaan tietoa seuraavasti (SFS-EN ISO 12100, 17–18):

- kuvaus koneesta, kuten tieto koneen koko elinkaaren vaiheista, koneen rakennuspiirustukset sekä käytetyt energianlähteet ja niiden järjestäminen
- sovellettavat säädökset sekä asiaankuuluvat standardit ja tekniset eritelmät
- aikaisemmat kokemukset vastaavista koneista ja niiden tapaturmista, vioista, terveyshaittoja tai muuta, joka tulisi huomioida uudessa koneessa.



Kuva 2. Riskin pienentämisprosessi (SFS-EN ISO 13849-1. 2023, 22).

Kuvassa 2 esitetään riskien pienentämisprosessi. Ensimmäisen riskiarvioinnissa tehdään riskianalyysi, joka sisältää raja-arvojen määrittämisen, vaarojen tunnistamisen sekä riskin suuruuden arvioinnin. Tämän jälkeen arvioidaan riskin merkitys ja tarkastellaan, onko riski riittävän pieni. Jos riski on liian suuri, jatketaan seuraaviin kuvan 2 kysymyksiin ja vastataan niihin riskin arvioinnin perusteella. Riskin pienentämisprosessi voidaan joutua tekemään useaan kertaan, jotta saavutetaan haluttu turvallisuus. Kun riski on tarpeeksi pieni, voidaan tehdä tarpeelliset dokumentoinnit tehdyistä muutoksista. Prosessi toistetaan erikseen jokaiselle riskille. Jos kuvan 2 kohtaan ”Voidaanko riskiä pienentää suojauksilla, turvalaitteilla?” vastataan kyllä, voidaan riskiä pienentää kuvan 3 mukaisesti:



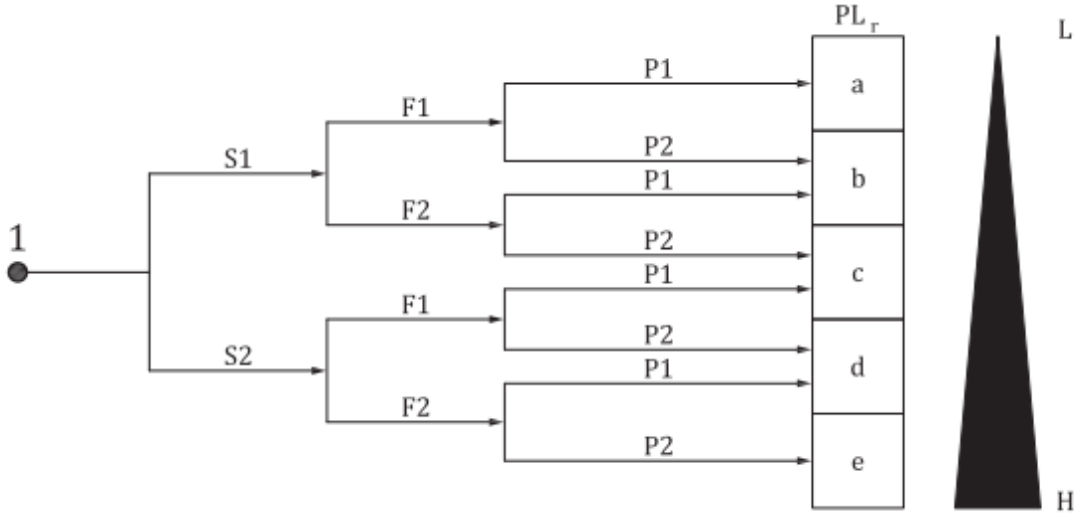
Kuva 3. Riskin pienentämisen prosessi ohjausteknillisin toimenpitein (SFS-EN ISO 13849-1. 2023, 24).

Kuvassa 3 esitetään riskin pienentämisprosessi ohjaustekniikalla ja määritetään vaadittava suoritustaso, suunnitellaan ohjausjärjestelmä ja arvioidaan suoritustaso. Suoritustason arvioinnin jälkeen tarkastellaan, onko suoritustaso vähintään yhtä suuri kuin vaadittava suoritustaso. Viimeiseksi ohjausjärjestelmä kelpuutetaan ja analysoidaan, jotta voidaan varmistaa, että kaikki toiminnot ovat turvallisia ja luotettavia. Prosessi suoritetaan jokaiselle turvatoiminnolle erikseen.

3.1 Suoritustasot

Suoristustasojatyyppejä on kaksi, joista ensimmäinen on PL-suoritustaso. PL-suoritustaso (Performance Level) kertoo turvakomponenttien vaarallisen vikaantumisen mahdollisuudesta. Komponentin valmistaja on yleensä ilmoittanut komponentin suoritustason tai se on laskettavissa, jos suoritustaso ei ole tiedossa. (SFS-EN ISO 13849-1.)

Toinen suoristustasojatyyppi on PLr-suoritustaso (Required Performance Level), joka kertoo mahdollisten riskien ja vahinkojen suuruudesta ja niiden toistuvuudesta yhtä turvatoimintoa kohden. PLr-taso on vaadittava suoritustaso, joten PL-suoritustaso tulee olla vähintään yhtä suuri tai suurempi kuin PLr-taso. PL- ja PLr-suoritustasot jaetaan viiteen eri luokkaan, joista PL a -luokassa on pienin riski eikä vahingot ole suuria ja PL e-luokassa riskit ovat todennäköisiä ja suuria.



Kuva 4. PLr-tason määritys (SFS-EN ISO 13849-1. 2023, 85).

Kuvassa 9 näkyy, kuinka PLr-arvo saadaan selville. S-haarassa mietitään vamman vakavuutta, F-haarassa altistumistaajuutta sekä kestoa ja P-haarassa vaaran välttämisen mahdollisuutta. Esimerkiksi jos laitteella olisi suuri riski aiheuttaa vammaa (S2), riski tapahtuisi harvoin (F1) ja riskin välttäminen olisi mahdollista (P1), olisi laitteen turvaluokitus PLr c. (SFS-EN ISO 13849-1.)

3.2 SIL-luokitus

PL	SIL (ks. tiedot standardista IEC 62061:2021) tiheiden vaateiden tai jatkuva toiminta-tapa
a	ei vastaavuutta
b	1
c	1
d	2
e	3
HUOM. 1 Suoritustasolla PL a ei ole vastaavuutta turvallisuuden eheyden tasojen asteikon kanssa ja suoritustasoa PL a käytetään pääasiassa lieviin ja tavallisesti palautuviin vammoihin johtavien riskien pienentämiseen. HUOM. 2 PL e vastaa turvallisuuden eheystasoa SIL 3, joka on määritelty suurimmaksi koneissa tavallisesti käytettäväksi tasoksi.	

Taulukko 1. PL- ja SIL-luokitusten yhteys (SFS-EN ISO 13849-1. 2023, 39).

SIL-tasot kuuluvat standardiin IEC 62061:2021, mutta niitä silti käyttää taulukon 1 mukaisesti PL-suoritustason kanssa. SIL-taso kertoo, kuinka mahdollisten riskien ja vahinkojen suuruudesta ja niiden toistuvuudesta. SIL-tasoja on kolme, joista SIL1 on epäluotettavin taso ja SIL3 turvallisin taso. Mitä vaarallisempi tuotannon prosessi on kyseessä, sitä vaativampi ja luotettavampi turvallisuusvaatimusten on oltava. Taulukossa 2 näkyy, kuinka usein virheitä saa tapahtua eri SIL-tasoilla. Esimerkiksi SIL3-tasolla virheitä saa tapahtua jatkuvasti käytettävillä laitteilla kerran 10–1000 miljoonasta tai satunnaisesti käytettävissä laitteissa kerran 1–10 tuhannesta. (Metropolia 2015.)

Virheen todennäköisyys		
Turvallisuuden eheyden taso	Toimintapa - Tarvittaessa (on demand)	Toimintapa - Jatkuva
SIL 4	$\geq 10^{-5} \ldots < 10^{-4}$	$\geq 10^{-9} \ldots < 10^{-8}$
SIL 3	$\geq 10^{-4} \ldots < 10^{-3}$	$\geq 10^{-8} \ldots < 10^{-7}$
SIL 2	$\geq 10^{-3} \ldots < 10^{-2}$	$\geq 10^{-7} \ldots < 10^{-6}$
SIL 1	$\geq 10^{-2} \ldots < 10^{-1}$	$\geq 10^{-6} \ldots < 10^{-5}$

Taulukko 2. SIL-tason virheen todennäköisyys (Metropolia 2015).

3.3 Vaarallinen keskimääräinen vikaantumisaika

Vaarallinen keskimääräinen vikaantumisaika (MTTFd) kertoo, kuinka kauan kestää, että järjestelmän yhteen komponenttiin tulee vaarallinen virhe. MTTFd-arvon laskentaan käytetään käytettävyyden määrää ja B10d-arvoa. B10d-arvo on valmistajan antama arvo, joka kertoo, montako toimintoa komponentti pystyy toteuttamaan ennen kuin 10 % niistä vikaantuu (SFS-EN ISO 13849-1. 2023, 94). MTTFd-arvona käytetään ensisijaisesti valmistajan ilmoittamaa arvoa. Jos valmistaja ei ole ilmoittanut komponentin MTTFd-arvoa tai se ei ole saatavilla, voidaan arvo laskea käyttäen standardin SFS-EN ISO 13849-1 (2023, 94–95) mukaisesti:

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

jossa

$$n_{op} = \frac{d_{op} \times h_{op} \times \frac{3600s}{h}}{t_{cycle}}, \tag{2}$$

jossa

h_{op} on keskimääräinen toiminta-aika, tuntia päivässä

d_{op} on keskimääräinen toiminta-aika, päivää vuodessa

t_{cycle} on keskimääräinen toiminta-aika komponentin kahden peräkkäisen toimintajakson välillä (esim. venttiilin avaaminen) sekunteina per toimintajakso.

$MTTF_D$	
Kunkin kanavan merkintä	**Kunkin kanavan vaihteluväli**
pieni	3 vuotta ≤ $MTTF_D$ < 10 vuotta
keskimääräinen	10 vuotta ≤ $MTTF_D$ < 30 vuotta
suuri	30 vuotta ≤ $MTTF_D$ < 100 vuotta[a]

HUOM. 1 Kunkin kanavan $MTTF_D$-arvojen vaihteluvälien valinta perustuu nykytekniikan mukaisista kenttähavainnoista saatuihin vikataajuuksiin ja ne muodostavat tietyntyyppisen logaritmisen asteikon, joka sopii logaritmiseen suoritustason asteikkoon. Todellisissa alajärjestelmissä jokaisen kanavan $MTTF_D$-arvoja, jotka ovat alle kolme vuotta, ei oleteta esiintyvän, koska tämä tarkoittaisi, että yhden vuoden kuluttua noin 30 % markkinoilla olevista järjestelmistä vikaantuisivat ja ne pitäisi korvata. Minkään kanavan $MTTF_D$-arvoa yli 100 vuotta ei hyväksytä, koska suuria riskejä varten olevat alajärjestelmät eivät saisi olla riippuvaisia yksistään komponenttien luotettavuudesta. Alajärjestelmien vahvistamiseksi systemaattisia ja satunnaisia vikaantumisia vastaan tarvitaan täydentäviä keinoja, kuten redundanssia ja testausta. Käytännön syistä vaihteluvälit rajoitetaan kolmeen. Jokaisen kanavan $MTTF_D$-arvon rajoittaminen enintään 100 vuoteen koskee alajärjestelmän yksittäistä kanavaa, joka toteuttaa turvatoiminnon. Korkeampia $MTTF_D$-arvoja voidaan käyttää yksittäisille komponenteille (ks. taulukko D.1).

HUOM. 2 Tässä taulukossa esitettävien raja-arvojen tarkkuuden oletetaan olevan 5 %.

[a] Luokassa 4 $MTTF_D$-arvon rajana on 2500 vuotta.

Taulukko 3. MTTFd-arvon kanavat (SFS-EN ISO 13849-1. 2023, 48).

Kun MTTFd-arvo on selvillä, voidaan tarkistaa MTTFd-arvon kanava taulukosta 3. MTTFd-arvot jaetaan pieneen, keskimääräiseen ja suureen kanavaan. Kanavaa hyödynnetään suoritustason laskentaan.

3.4 Diagnostiikan kattavuus

Diagnostiikan kattavuus (DC)	
Merkintä	**Vaihtelualue**
nolla	DC < 60 %
pieni	60 % ≤ DC < 90 %
keskimääräinen	90 % ≤ DC < 99 %
suuri	99 % ≤ DC

Taulukko 4. DC-arvo (SFS-EN ISO 13849-1. 2023, 49).

Taulukossa 4 esitetään diagnostiikan kattavuuden eri ryhmät vaihteluvälin perusteella. Diagnostiikan kattavuus (DC) kertoo, kuinka paljon järjestelmä havaitsee järjestelmässä ilmeneviä vaarallisia vikoja. PL-arvon laskemiseen voidaan käyttää DC-keskiarvoa DC_{avg}, esimerkkiarvoja tai järjestelmän yksittäisen komponentin pienintä DC-arvoa. (SFS-EN ISO 13849-1.)

DC_{avg} voidaan laskea standardin SFS-EN ISO 13849-1 (2023,105) mukaan seuraavasti:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \cdots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \cdots + \frac{1}{MTTF_{DN}}}, \quad (3)$$

jossa

DC_{avg} on keskimääräinen diagnostiikan kattavuus

DC_n on kyseisen komponentin diagnostiikan kattavuus

$MTTF_{Dn}$ on kyseisen komponentin vaarallinen keskimääräinen vikaantumisaika.

3.5 Yhteisvikaantuntumista estävät toimenpiteet

Nro	Yhteisvikaantumista estävä toimenpide	Pisteet
1	erottelu/erottaminen	15
2	erilaisuus (diversiteetti)	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	5
5	koulutus	5
6	ympäristöolosuhteet	
6.1	sähkömagneettisten häiriöiden tai nestemäisen väliaineen epäpuhtauksien estäminen	25
6.2	muut vaikutukset	10
	yhteensä	[mahdolliset maksimipisteet 100]

Kokonaispisteet	Toimenpiteet yhteisvikaantumisen välttämiseksi
65 tai enemmän	Täyttää vaatimukset
vähemmän kuin 65	Ei täytä vaatimuksia ⇒ tee lisätoimenpiteitä

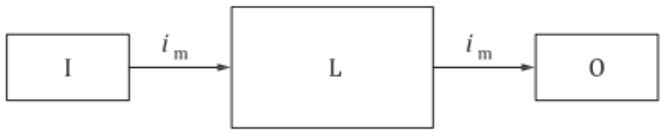
Taulukko 5. CCF-taulukko (SFS-EN ISO 13849-1. 2023, 107).

Taulukossa 5 esitetään yhteisvikaantuntumista estävät toimenpiteet (CCF) standardin SFS-EN ISO 13849-1 mukaisesti. Arvo kertoo laitteen yksittäisistä vioista, joiden seurauksena laite vikaantuu. Jokaisen taulukon kohdasta katsotaan, toteutuuko menetelmän vaatimukset, jolloin kohdasta saadaan kaikki taulukon kohdan pisteet. Jos vaatimukset eivät täyty, ei kohdasta voi antaa pisteitä. Kaikkien kohtien pisteet lasketaan lopuksi yhteen. Pisteiden summaksi täytyy saada vähintään 65 pistettä, jotta laskelmia voidaan jatkaa. Jos pisteitä tulee alle 65, tarvitsee järjestelmään lisätä jokin menetelmä, josta ei saatu aikaisemmin pisteitä. (SFS-EN ISO 13849-1.)

3.6 Suoritustasojen luokat

Laskennan kulmakivenä toimivat luokat, joiden tarkoitus on antaa perusta järjestelmän vaadittaville komponenteille komponenttien vikakestoisuuden mukaan. Luokka valitaan järjestelmän laajuuden ja halutun turvallisuuden tason perusteella. Luokkia on viisi, joista B on alhaisin ja 4 korkein. Jokainen luokka noudattaa aina luokan B vaatimuksia oman luokan vaatimusten lisäksi. (SFS-EN ISO 13849-1. 2023, 39.)

3.6.1 Luokka B



Selite

i_m	Liitäntävälineet
I	tuloyksikkö (esim. anturi)
L	logiikka
O	lähtöyksikkö (esim. pääkontaktori)

Kuva 5. Luokan B järjestelmärakenne (SFS-EN ISO 13849-1. 2023, 43).

Kuvassa 4 näkyy luokan B järjestelmärakenne. Luokassa B ei tarvitse ottaa huomioon DC_{avg}- tai CCF-arvoja ja MTTFd-arvo on oltava vähintään matala. Järjestelmä on suunniteltava ja rakennettava noudattaen asiaankuuluvia standardeja. Suurin suoritustaso luokan B järjestelmässä on PL b. Järjestelmän vikaantuessa alatoimintoja voi menettää. (SFS-EN ISO 13849-1. 2023, 42.)

3.6.2 Luokka 1

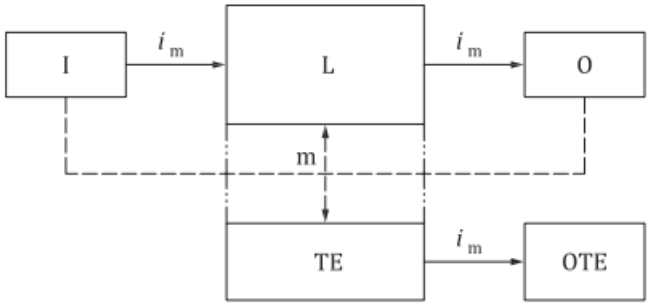
Selite

i_m Liitäntävälineet
I tuloyksikkö (esim. anturi)
L logiikka
O lähtöyksikkö (esim. pääkontaktori)

Kuva 6. Luokan 1 järjestelmärakenne (SFS-EN ISO 13849-1. 2023, 43).

Kuvassa 5 näkyy luokan 1 järjestelmärakenne. Luokan 1 järjestelmässä on luokan B vaatimusten lisäksi käytettävä luotettavia komponentteja käyttäen hyvin koeteltuja turvallisuusperiaatteita. Luokassa 1 ei tarvitse ottaa huomioon DC_{avg}- tai CCF-arvoja ja MTTFd-arvo on oltava vähintään suuri. Suurin suoritustaso luokan 1 järjestelmässä on PL c. Järjestelmän vikaantuessa turvatoimintoja voi menettää. (SFS-EN ISO 13849-1. 2023, 43.)

3.6.3 Luokka 2



Selite

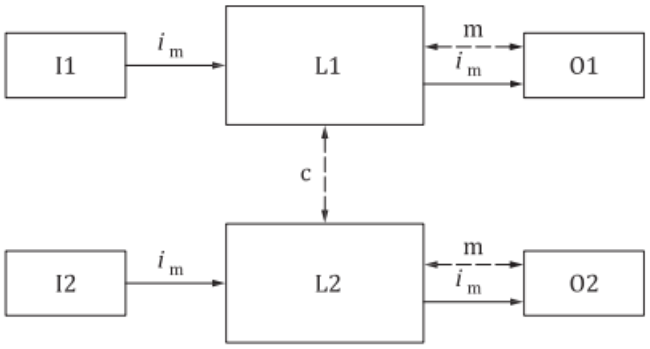
i_m Liitäntävälineet
I tuloyksikkö (esim. anturi)
L logiikka
m valvonta/testaus
O lähtöyksikkö (esim. pääkontaktori)
TE testauslaitteisto
OTE testauslaitteiston lähdöt

Katkoviivat esittävät kohtuudella mahdollista vikojen paljastamista.

Kuva 7. Luokan 2 järjestelmärakenne (SFS-EN ISO 13849-1. 2023, 45).

Kuvassa 6 näkyy luokan 2 järjestelmärakenne. Luokan 2 järjestelmässä on luokan B vaatimusten lisäksi oltava järjestelmän testaus säännöllisin väliajoin. Testaukset on tehtävä esimerkiksi ennen uutta työkiertoa, ennen liikkeiden alkamista tai käytön aikana, jos se ei aiheuta riskejä ja se koetaan tarpeelliseksi. Luokassa 2 tulee ottaa huomioon DC_{avg}- tai CCF-arvot ja vaadittava MTTFd-arvo määräytyy vaadittavan PLr-suoritustason mukaan. Suurin suoritustaso luokan 2 järjestelmässä on PL d. Järjestelmän vikaantuessa vika tunnistetaan testillä. (SFS-EN ISO 13849-1. 2023, 43–44.)

3.6.4 Luokka 3



Selite

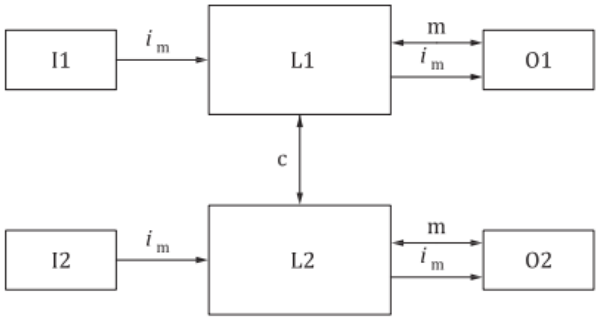
i_m	Liitäntävälineet	L1, L2	logiikka
c	ristiinvalvonta	m	valvonta
I1, I2	tuloyksikkö (esim. anturi)	O1, O_2	lähtöyksikkö, esim. pääkontaktori tai voimansiirtojärjestelmä

Katkoviivat esittävät kohtuudella mahdollista vikojen paljastamista.

Kuva 8. Luokan 3 järjestelmärakenne (SFS-EN ISO 13849-1. 2023, 46).

Kuvassa 7 näkyy luokan 3 järjestelmärakenne. Luokan 3 järjestelmässä on luokan B vaatimusten lisäksi kestettävä yksittäinen vika ilman alatoiminnon menettämistä ja jos mahdollista, yksittäinen vika on tunnistettavissa ennen seuraavaa vikaantumista. Kaikkia vikoja ei tarvitse tunnistaa, jonka takia havaitsemattomien vikojen kasvaessa järjestelmä saattaa menettää toimintoja. Luokassa 3 tulee ottaa huomioon DC_{avg}- tai CCF-arvot ja vaadittava MTTFd-arvo määräytyy vaadittavan PLr-suoritustason mukaan. Suurin suoritustaso luokan 3 järjestelmässä on PL e. (SFS-EN ISO 13849-1. 2023, 45.)

3.6.5 Luokka 4



Selite

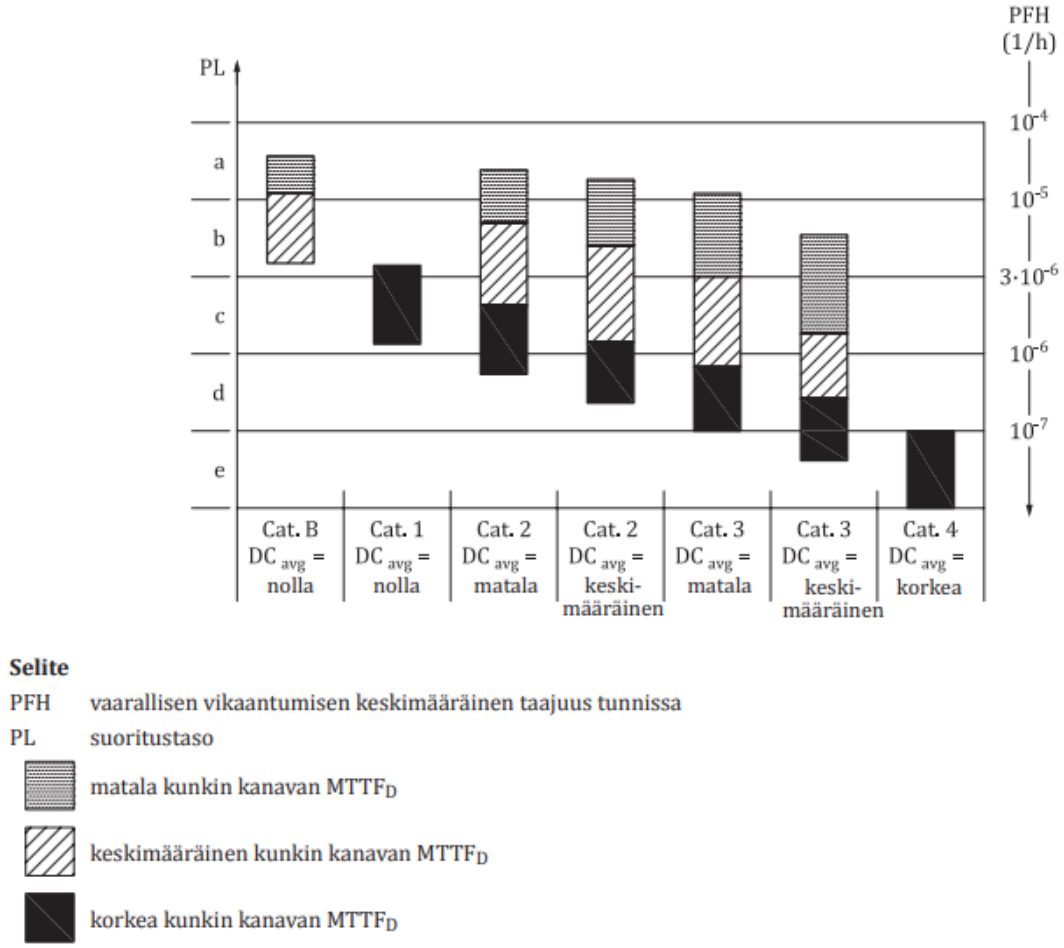
i_m	Liitäntävälineet	L1, L2	logiikka
c	ristiinvalvonta	m	valvonta
I1, I2	tuloyksikkö (esim. anturi)	O1, O_2	lähtöyksikkö, esim. pääkontaktori tai voimansiirtojärjestelmä

Yhtenäiset viivat valvontatoiminnoissa (m) esittävät diagnostiikan kattavuutta, jonka taso on korkeampi kuin luokkaan 3 kuuluvassa nimetyssä rakenteessa.

Kuva 9. Luokan 4 järjestelmärakenne (SFS-EN ISO 13849-1. 2023, 47).

Kuvassa 8 näkyy luokan 4 järjestelmärakenne. Luokan 4 järjestelmässä on luokan B vaatimusten lisäksi kestettävä yksittäinen vika ilman turvatoiminnon menettämistä ja yksittäinen vika on tunnistettavissa esimerkiksi järjestelmän käynnistyessä tai työkierron päättyessä. Kaikkia vikoja ei tarvitse tunnistaa, mutta kerääntyvät viat eivät saa aiheuttaa turvatoiminnon menettämistä. Luokassa 4 tulee DC_{avg}-arvon olla suuri, CCF-arvo on otettava huomioon ja vaadittava MTTFd-arvo on oltava korkea. Suurin suoritustaso luokan 4 järjestelmässä on PL e. (SFS-EN ISO 13849-1. 2023, 46.)

3.7 Suoritustason arviointi



Kuva 10. PL-suoritustason arviointi (SFS-EN ISO 13849-1. 2023, 51).

Kuvassa 10 näkyy taulukko, jonka perusteella suoritustaso arvioidaan. Suoritustason arviointiin tarvitaan järjestelmän luokka, DC_{avg}- sekä MTTFd-arvot. Jos luokka on 2 tai suurempi, tarvitaan myös CCF-arvo luokan laskentaan. Jos MTTFd-arvoa ei ole annettu, luokissa b, 2 ja 3 voidaan käyttää MTTFd-arvoa 10 vuotta ja luokassa 1 MTTFd-arvoa 30 vuotta, mutta suurin saavutettava suoritustaso on tällöin PL c. Arviointiin voidaan myös käyttää standardin SFS-EN ISO 13849-1 (2023, 130–133) liitettä K. (SFS-EN ISO 13849-1. 2023, 52.)

4 Turva-automaatiojärjestelmä

Turva-automaatio on yleensä muusta automaatiosta riippumaton järjestelmä, jonka tarkoituksena on suojata työntekijöitä, laitteita sekä ympäristöä vaarallisilta tekijöiltä. Turva-automaatio on oma järjestelmä, jotta järjestelmä toimii luotettavasti jopa vikatilanteen tullen eikä muu automaatiojärjestelmä häiritse turvalaitteiden toimintaa. Sen avulla toteutetaan tuotannon lukitukset ja suojaukset, jotka ovat kriittisiä ja tuodaan tuotanto turvalliseen tilaan tai estää tuotantoa pääsemästä vaaralliseen tilaan. (Tukes 2023.)

Turva-automaatiossa on monia osa-alueita, jotka vaikuttavat kokonaisjärjestelmän suunnitteluun ja toimintaan. Turva-automaatiota koskevat erilaiset standardit ja säädökset, joiden vaatimusten perusteella turva-automaatiojärjestelmä suunnitellaan ja määritetään miten sen kuuluisi toimia. Direktiivit ja lainsäädännöt ohjeistaa laitteiden valmistajia valmistamaan tuvallisia tuotteita, jotka ovat yhdenmukaisia ja turvallisia. (Metropolia 2023.)

4.1 Ohjelmoitava logiikka

Kuva 11. Siemens SIMATIC ohjelmoitava logiikka (Siemens c).

Kuvassa 11 on esimerkki ohjelmoitavasta logiikasta. Ohjelmoitava logiikka tai PLC (Programmable Logic Controller) on tietokone, joka ohjaa automaatioprosesseja. Logiikkaan liitetään sisääntuloihin (input) ohjaavia laitteita, kuten painikkeita tai antureita, joiden tieto prosessoidaan. Tiedon perusteella ohjataan laitteita, kuten huomiovaloja tai releitä ulostuloilla (output) tehdyn ohjelman mukaisesti. Monessa logiikassa prosessori on omana yksikkönä, johon liitetään lisämoduuleja. Moduuleja on monia erilaisia, kuten:

- relemoduuleita: Relemoduuleilla saadaan ohjattua releitä logiikan avulla.
- analogisia tai digitaalisia sisään- ja ulostulomoduuleita: Analogiset viestit ovat tyypillisesti jänniteviestejä 0–10 V tai virtaviestejä 4–20 mA. Virtaviesti sietävät häiriöitä paremmin kuin jänniteviesti, jonka takia virtaviesti on yleisemmin käytetty. Virtaviesti kertoo myös yhteyden toimivuudesta. Pienin virtaviesti on 4 mA, joka kertoo, että yhteys kenttälaitteelle on ehjä. (PR electronics)
- väylämoduuleita: Mahdollistaa logiikan yhdistämisen esimerkiksi Profinet-verkkoon, jonka kautta hälytykset tai muut tiedot voidaan ohjata prosessin ohjausjärjestelmään tai muille logiikoille. Myös näyttöpäätteiden yhdistäminen logiikalle tapahtuu väylän kautta.

Turvalogiikat ovat vastaavia kuin normaalit logiikat, mutta niissä on paljon turvallisuuteen liittyviä ominaisuuksia, jotka takaavat järjestelmän toimivuuden sekä tekevät siitä turvallisen joka tilanteessa. Vaikka turvalogiikkaan tulisi vika, sen on jätettävä järjestelmä aina turvalliseen tilaan. Standardisarja EN 61508 takaa sähköisten, elektronisten ja ohjelmoitavien elektronisten turvallisuuteen liittyvien järjestelmien toiminnallisen turvallisuuden. (Control Design 2003.)

Turvalogiikka voi olla osa ohjausjärjestelmää tai erillinen yksikkö, joka liitetään ohjausjärjestelmään. Se toimii samalla tavalla kuin perinteinen ohjelmoitava logiikka. Riippuen käytetystä järjestelmästä, turvallisuuslogiikka voidaan liittää suoraan väylään tai erillisen yksikön kautta, mikä mahdollistaa sen toiminnan seurannan ja yksinkertaisemman kaapeloinnin. (MRO Electric 2022.)

4.2 Turvakomponentit

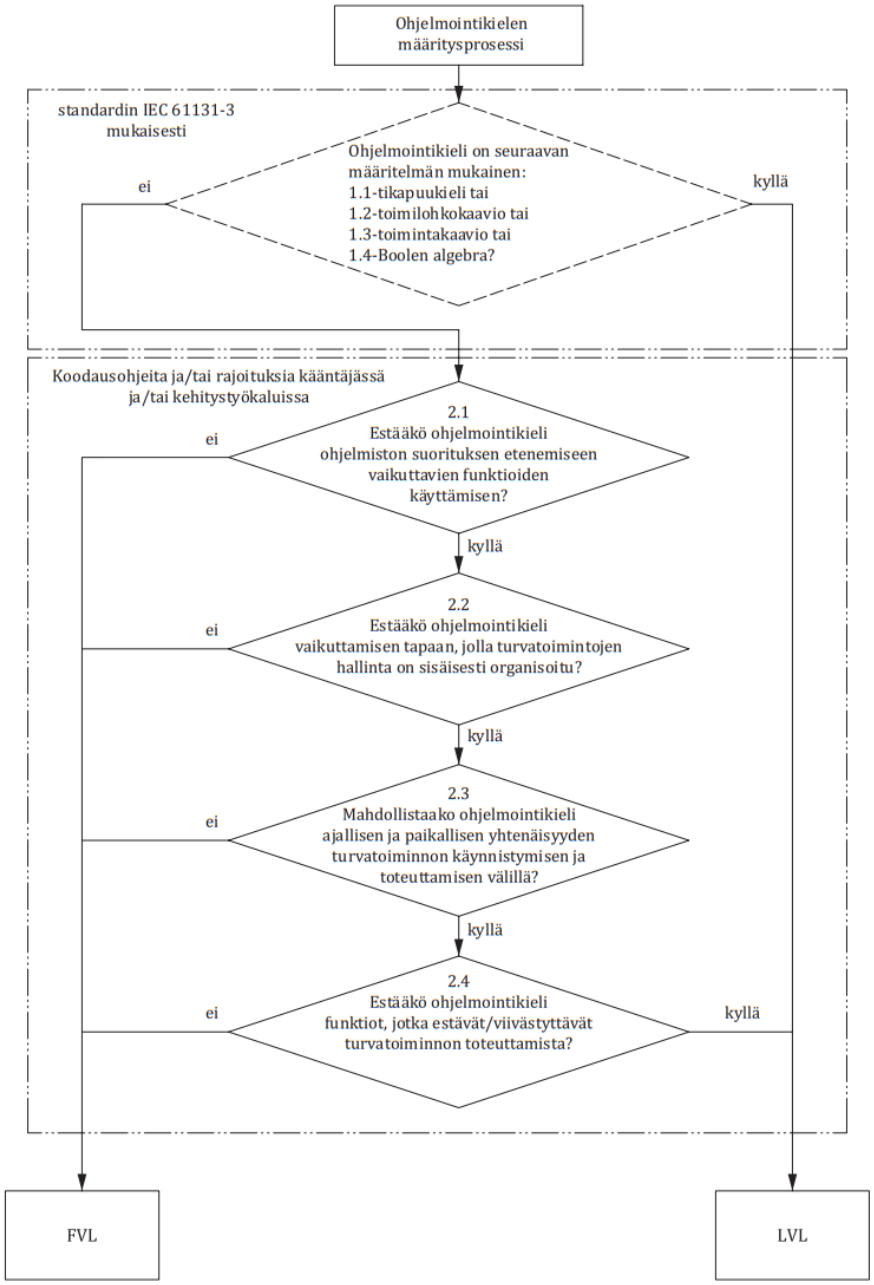
Turvakomponentit ovat tyypillisesti luotettavampia komponentteja ja kestävät paremmin haastavia olosuhteita. Siemensin SIMATIC-tuoteperheen avulla turvakomponentteja voidaan yhdistää normaalien komponenttien kanssa, jolloin vanha automaatiojärjestelmä on helppo muuttaa turva-

automaatiojärjestelmäksi. SIMATIC mahdollistaa laitteiden yhteensopivuuden luotettavasti väyliä hyödyntäen. Turvakomponentit ovat tyypillisesti merkattu keltaisella värillä. (Siemens a.)

Kommunikointi laitteiden välillä tehdään kenttäväylillä tai turvaväylillä. Kenttäväylä on digitaalinen tietoliikennejärjestelmä, joka mahdollistaa selkeän ja yksinkertaisen kaapeloinnin tai langattoman tiedonsiirron, parantaa vikadiagnostiikkaa ja yhteensopivuutta sekä helpottaa kokoonpanon muunneltavuutta. Turvaväylää voidaan käyttää omana väyläratkaisuna tai kenttäväylään lisättynä ominaisuutena. Turvaväylä käyttää omia turvaprotokollakerroksia, joiden avulla voidaan valvoa järjestelmän yhteyksiä ja varmistaa signaalin eheys. (Sundquist, M.)

4.3 Ohjelmointi

Logiikan ohjelmoinnissa käytetään tyypillisesti logiikan valmistajan omaa sovellusta. Siemens TIA Portal on lisenssipohjainen ohjelmointiympäristö, johon on integroitu Siemensin aikaisempia sovelluksia, kuten STEP 7, WinCC, SINAMICS Startdrive, SIMOCODE ES ja SIMOTION SCOUT TIA. TIA Portaalin avulla voidaan luoda automaatiojärjestelmä virtuaalisesti ja testata ohjelmiston sekä komponenttien yhteensopivuus ja toimivuus ennen fyysisen järjestelmän rakentamista. Tiedostot voidaan jakaa pilvipalvelun kautta muille jäsenille joustavuuden ja laadun varmistamiseksi. (Siemens b.)



Kuva 12. Ohjelmointikielen valinta (SFS-EN ISO 13849-1. 2023, 62).

Kuva 12 toimii oppaana logiikan ohjelmointikielen valinnassa. Turvallisuuden näkökulmasta ohjelmisto tulee olla luotettava ja yhteensopiva kaikkien järjestelmän komponenttien kanssa. Väärin ohjelmoitu järjestelmä voi johtaa virheelliseen toimintaan tai aiheuttaa vaaroja ihmisille, komponenteille tai ympäristölle. Ohjelmointikielet jaetaan rajoitetun- ja rajoittamattoman käskykannan ohjelmointikieliin. Rajoitetuissa ohjelmointikielissä ohjelma tulisi suunnitella ymmärrettäväksi ja keskittyä vain toteutuviin sovelluksiin virheiden minimoimiseksi. Yleisimmät rajoitetut ohjelmointikielet ovat tikapuukieli,

toimilohkokaavio, toimintakaavio sekä Boolen algebra. Rajoittamattomilla ohjelmointikielillä voidaan ohjelmoida järjestelmässä mitä tahansa ja tehdä laajempia ja monimutkaisempia kokoonpanoja. Rajoittamattomia ohjelmointikieliä käytetään sulautetuissa ohjelmistoissa, mutta harvemmin sovellusohjelmistoissa. Tyypillisiä rajoittamattomia ohjelmistokieliä on Ada, C, C++, Java ja SQL.

5 Järjestelmän suunnittelu

Tehtaan nykyinen henkilöstön hätähälytysjärjestelmä on tehtaan alkuperäinen vuodelta 1983, jonka ohjaus on toteutettu releillä. Järjestelmän toimivuus alkaa olemaan epäluotettava iän ja tekniikan takia, joten järjestelmä on hyvä uusia. Nykyisestä järjestelmästä säästetään mahdollisimman paljon vanhoja komponentteja, kuten hätäseis-painikkeita ja huomiolaitteita. Releohjaus vaihdetaan moderniin turvalogiikkaan, joka takaisi luotettavan ja pitkäaikaisen toiminnan sekä tuo lisäominaisuuksia, jotka eivät ole mahdollisia nykyisellä järjestelmällä. Lisäksi järjestelmään olisi mahdollista asentaa näyttöpäätteitä, joista näkisi reaaliaikaista tietoa järjestelmän tilasta tai hälytyksen sijainnin. Turvalogiikka mahdollistaa myös automaattiset hälytykset työntekijöiden matkapuhelimiin tekstiviestin välityksellä sekä helpottaa tulevaisuuden päivityksien tekoa.

Päivityksen alussa tarvitaan tieto, mitkä ovat järjestelmän vaatimukset ja mitä järjestelmältä halutaan. Kyseiselle järjestelmälle on vaatimuksina vähintään 80 sisääntuloa ja 32 ulostuloa, suosien SIL3-luokitusta komponenteille, mahdollisuus laajentaa järjestelmää tulevaisuudessa sekä tekstiviestit hälytyksistä työntekijöiden matkapuhelimiin. Tehtaalla on myös paljon ATEX-luokiteltuja tiloja, jotka tulee ottaa huomioon. Toimeksiantaja halusi myös UPS-virtalähteen järjestelmälle. UPS on laite, joka syöttää tasaisen sähkövirran laitteille jopa sähkökatkojen aikana. UPS-laitteissa on akku, johon se vaihtaa automattisesti verkkovirran katketessa. UPS voi myös suodattaa verkkovirrasta tulevia jännitepiikkejä tai häiriötä. UPS-laitteen akusto mitoitetaan riittämään noin kolmeksi tunniksi.

5.1 Riskien arviointi

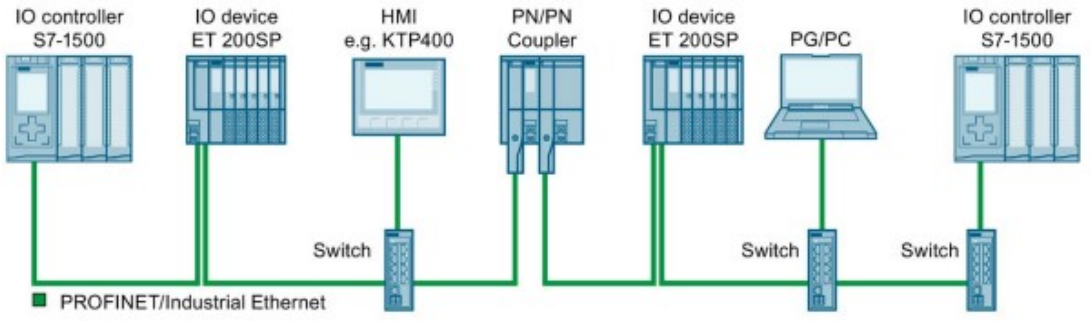
Riski	Vaaratilanne	S (Vakavuus)	F (Taajuus)	P (Mahdollisuus välttää)	PLr
Ohjelmointivirhe	Hälytyksen toimintahäiriö	S1	F2	P1	b
Ohjelmointivirhe	Virheellinen hälytys	S1	F2	P1	b
Räjähdysvaara	ATEX-tilassa syttyvä räjähdys	S2	F1	P1	c
Laiterikko	Hätäseis-napin vajaatoiminta	S2	F1	P2	d
Laiterikko	Hälytyslaitteen vajaatoiminta	S1	F1	P2	b

Taulukko 6. Järjestelmän riskien arviointi.

Järjestelmässä ilmenevät riskit ovat pääsääntöisesti pieniä järjestelmän käyttötarkoituksen ja vähäisten laitteiden takia, mutta riskejä kuitenkin on. Taulukossa 6 on esitetty järjestelmään kohdistuvat riskit, niiden vakavuus, taajuus sekä välttämisen mahdollisuus kappaleen 3.2 mukaisesti. Suurin

laskennallinen vaadittava suoritustaso on PLr d. Tämä tarkoittaa sitä, että järjestelmän komponenttien suoritustaso tulee olla PL d tai korkeampi. Jotta tämä on mahdollista, järjestelmä tulee olla vähintään luokan 2 mukainen. Luokassa 2 järjestelmässä tulee olla vaarallisten virheiden testaus. Diagnostiikan kattavuus tulee olla vähintään matala, joka tarkoittaa, että vähintään 60 % vaarallisista virheistä täytyy tulla ilmi testauksen aikana. Komponenttien suurin keskimääräinen vikaantumisen taajuus tunnissa on standardin SFS-EN ISO 13849-1 (2023,132) mukainen.

5.2 Väylät



Kuva 13. Väyläkytkentä (SiePortal 2019).

Kommunikointi laitteiden välillä tapahtuu Profinet-väylää pitkin kuvan 13 esimerkin mukaisesti. Järjestelmän laitteet yhdistetään kytkimelle, joka yhdistää laitteet väylään. Kytkimeltä väylä yhdistyy PN/PN-kytkimelle, joka mahdollistaa usean järjestelmän kommunikoinnin samassa väylässä. PN/PN-kytkimeltä väylä yhdistetään muun tehtaan automaatiojärjestelmään, jolla voidaan kerätä dataa ja valvoa kaikkien järjestelmien tilannetta tai historiaa. (SiePortal 2019.)

5.3 Järjestelmän uudet komponentit

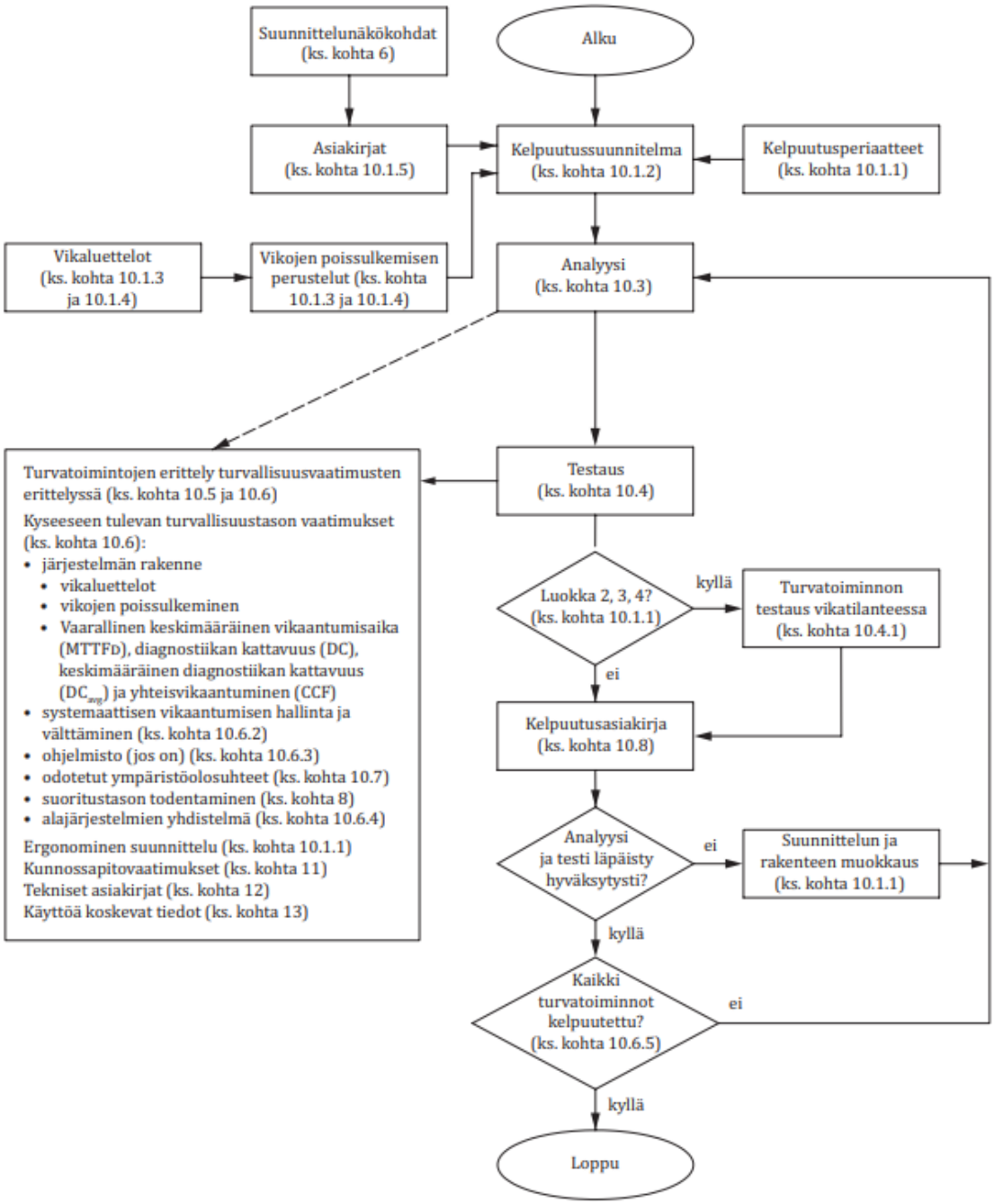
Järjestelmään valitaan Siemensin turvalogiikka, koska logiikka on yritykselle tuttu, helposti laajennettavissa sekä asiakastukea on helppo saada muihin valmistajiin verrattuna. Prosessoriksi valitaan Siemensin 1512SP F-1 PN, jonka I/O-portteja laajennetaan SIMATIC ET 200SP turvamoduuleilla. Moduuleita voidaan lisätä tulevaisuudessa, jos laitteita halutaan lisätä järjestelmään. Kaikki uudet komponentit kykenevät suoritustasoon PL e tai SIL 3 sekä keskimääräinen vikaantumisen taajuus tunnissa on suoritustasojen mukaiset. Lisäksi uusi järjestelmä yhdistetään tehtaan muuhun automaatioverkostoon

kenttäväylää hyödyntäen. Tehtaan automaatioverkostosta tulee väyläkaapeli Siemensin SCALENCE XB208-kytkimelle, johon kaikki uuden järjestelmän laitteet kytketään väyläkaapelilla.

5.4 Logiikan liitännät

Järjestelmän pääsääntöiset laitteet ovat sisääntuloina hätäseisnapit ja ulostuloina huomiolaitteita, kuten hälytyskelloja sekä huomiovalot ympäri tehdasta. Hätäseisnappeja on sijoitettu tehtaan käytäville sekä jokaisen huoneen jokaiseen kerrokseen. Turvallisuuden ja toiminnan takaamiseksi hätäseisnapeille tulee kahdennus, joka tarkoittaa sitä, että jokaiselle napille tulee neljä johdinta. Nämä johtimet jaetaan napin kahdelle kontaktorille, jotta toisen kontaktorin vikaantuessa napin painallus huomataan logiikalla. Jos logiikka huomaa vain toisen kontaktorin aktivoituneen, voidaan siitä tehdä vikailmoitus automaatiojärjestelmään. Huomiolaitteille ei koettu tarvetta kahdentaa. Laitteiden toiminta tulee tällöin tarkistaa säännöllisin väliajoin.

5.5 Kelpuutus



Kuva 14. Kelpuutusprosessi (SFS EN-ISO 13849-1. 2023, 70).

Kelpuutuksen tarkoitus on varmistaa, että järjestelmä täyttää turvallisuusvaatimukset ja järjestelmä toimii niin kuin kuuluukin. Kuvassa 14 esitetään kelpuutusprosessin vaiheet. Kelpuutuksen alussa tehdään kelpuutussuunnitelma, joka kattaa kelpuutusprosessin vaatimukset, kuten

testausten aikaiset toiminta- ja ympäristöolosuhteet, käytettävät testit ja analyysit sekä kelpuutusprosessin vaiheiden vastuuhenkilöt. Analyysiin sisältyy turvatoimintojen erittely, niiden ominaisuudet sekä turvallisuuden eheyden määrittely, vaarallinen keskimääräinen vikaantumisaika, keskimääräinen diagnostiikan kattavuus ja yhteisvikaantuminen sekä perustelut laskelmiin valutuista arvoista, vikaluettelot sekä vikojen poissulkemisen perustelut. Analyysin ja testauksen jälkeen tehdään kelpuutusasiakirja ja varmistetaan, että kaikki analyysit ja testit on läpäisty hyväksytysti sekä kaikki turvatoiminnot kelpuutettu. (SFS EN-ISO 13849-1. 2023, 71–80).

5.6 Dokumentointi ja ohjelmointi

Dokumentointi on keskeinen osa päivitysprosessia, sillä se mahdollistaa järjestelmän ymmärtämisen, ylläpidon ja kehittämisen eri vaiheissa. Dokumentoinnilla varmistetaan, että järjestelmän toiminta, rakenne ja käyttöönotto ovat selkeitä ja säädösten mukaisia. Dokumentaation tulisi kattaa laajasti järjestelmän toiminnallisuudet, rajapinnat, komponenttien tekniset ominaisuudet, kytkentä- ja piirikaaviot, testausmenetelmät ja tulokset, käyttöohjeet sekä mahdolliset rajoitukset ja varoitukset. Näin varmistetaan turva-automaation tehokas käyttö ja ylläpito sekä mahdollistetaan jatkokehitys ja integraatio muihin järjestelmiin.

Turva-automaation ohjelmointi on vaativaa paljon aikaa ja resursseja. Kirjoittajan vähäisen kokemuksen takia sekä ohjelmoinnin laajuuden takia ohjelmointia ei suoritettu tässä työssä. Ohjelmointi ulkoistetaan ammattilaisten tehtäväksi, jotta järjestelmästä saadaan turvallinen ja toimiva kokoonpano.

6 Yhteenveto

Opinnäytetyön tavoitteena oli tutustua turva-automaatioon liittyviin standardeihin ja direktiiveihin, joiden pohjalta suunniteltaisiin uusi henkilöstön hätähälytysjärjestelmä tehtaalle tai mihin tahansa turva-automaatiojärjestelmään. Lopputuloksena saatiin selkeä ja kattava ohjeistus turva-automaatiojärjestelmän suunnittelusta sekä huomioitavista osa-alueista. Työssä pyrittiin pysymään aihealueessa sekä keskittymään oleelliseen. Aihe on kuitenkin niin laaja, että työstä oli pakko jättää yksityiskohtia pois, joilla saattaa olla merkitystä lopullisessa järjestelmässä. Automaatiojärjestelmän ohjelmoinnista kerrottiin myös yleisellä tasolla, vaikkei sitä työssä suoritettu.

Opinnäytetyössä esitetyt periaatteet, standardit, ja suunnittelumallit toimivat alustavana lähtökohtana myös muissa erilaisissa turva-automaatioratkaisujen toteuttamisessa ja kehittämisessä. Tämä mahdollistaa turva-automaatiojärjestelmien tehokkaamman kehityksen ja soveltamisen erilaisiin tarpeisiin, edistäen samalla monimutkaisen järjestelmän turvallisuutta ja luotettavuutta.

Lähteet

Control Design 2003. Learn to Trust Safety PLCs. Viitattu 22.8.2023. https://www.controldesign.com/safety/safety-controllers/article/11377976/programmable-logic-controllers-learn-to-trust-safety-plcs

Euroopan parlamentin ja neuvostondirektiivi 2006/42/EY.

Euroopan parlamentin ja neuvostondirektiivi 2014/30/EU.

Euroopan parlamentin ja neuvostondirektiivi 2014/35/EU.

Finlex. 2012. Valtioneuvoston asetus vaarallisten kemikaalien teollisen käsittelyn ja varastoinnin turvallisuusvaatimuksista. Viitattu 14.7.2023. https://www.finlex.fi/fi/laki/ajantasa/2012/20120856#L1

Sunquist, M. Teollisuusautomaation standardit Osio 8: Turvaväylät ja niiden valinta: tekninen raportti IEC/TR 62513. Sesko.

Metropolia 2015. Turvallisuuden ja eheystasojen määrittäminen TET, SIL. Viitattu 22.8.2023. https://wiki.metropolia.fi/pages/viewpage.action?pageId=291247389

Metropolia 2017. Direktiivit ja lainsäädäntö. Viitattu 7.7.2023. https://wiki.metropolia.fi/pages/viewpage.action?pageId=291247315

MRO Electric 2022. What is a PLC. Viitattu 23.2.2024. https://www.mroelectric.com/blog/what-is-a-plc/

Schischek. Labelling/Classification of electric exposion proof ATEX equipment according to ATEX 2014/34/EU. Viitattu 24.1.2024. https://www.schischek.com/pdf/ATEX-Classification-Labelling-of-Electric-Equipment.pdf

Seqens 2024. Viitattu 19.2.2024. https://www.seqens.com/

SiePortal 2019. SIMATIC Bus links PN/PN coupler. Viitattu 29.2.2024. https://support.industry.siemens.com/cs/document/44319532/simatic-bus-links-pn-pn-coupler?dti=0&lc=en-FI

SFS-EN IEC 62061. 2021. Koneturvallisuus. Turvallisuuteen liittyvien ohjausjärjestelmien toiminnallinen turvallisuus. Helsinki. Suomen Standardisoimisliitto SFS ry.

SFS-EN ISO 12100. 2010. Koneturvallisuus. Yleiset suunnitteluperiaatteet, riskin arviointi ja riskin pienentäminen. Helsinki. Suomen Standardisoimisliitto SFS ry.

SFS-EN ISO 13849-1. 2023. Koneturvallisuus. Turvallisuuteen liittyvät ohjausjärjestelmien osa. Osa 1: Yleiset suunnitteluperiaatteet. Helsinki. Suomen Standardisoimisliitto SFS ry.

Siemens a. SIMATIC Safety Integrated – machine safety seamlessly integrated. Viitattu 2.3.2024. https://www.siemens.com/global/en/products/automation/topic-areas/safety-integrated/factory-automation/offering/simatic-safety.html

Siemens b. Totally Integrated Automation Portal – Always ready for tomorrow. Viitattu 5.3.2024. https://www.siemens.com/global/en/products/automation/industry-software/automation-software/tia-portal.html

Siemens c. 6ES7512-1SM03-0AB0 Catalog. Viitattu 26.3.2024. https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7512-1SM03-0AB0

Tukes a. CE-merkintä. Viitattu 24.1.2024. https://tukes.fi/tuotteet-ja-palvelut/ce-merkinta

Tukes b. Räjähdysvaarallisten tilojen laitteet – Atex. Viitattu 24.1.2024. https://tukes.fi/teollisuus/rajahdysvaaralliset-tilat/rajahdysvaarallisten-tilojen-laitteet-atex